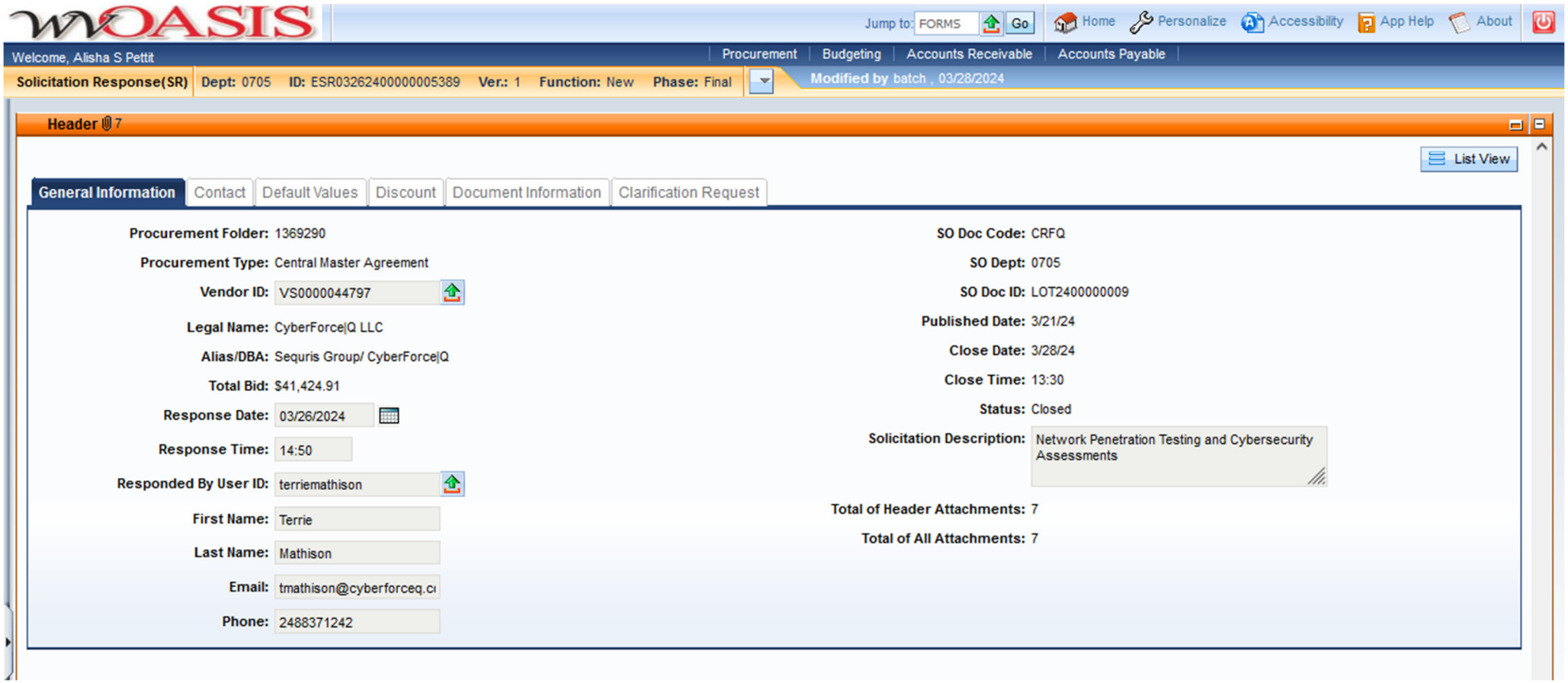
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency 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.


wvOASIS
Jump to: FORMS Go
Home
Personalize
Accessibility
App Help
About
Welcome, Alisha S Pettit
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR)
Dept: 0705
ID: ESR03262400000005389
Ver.: 1
Function: New
Phase: Final
Modified by batch , 03/28/2024
Header 7
List View
General Information
Contact
Default Values
Discount
Document Information
Clarification Request
Procurement Folder: 1369290
Procurement Type: Central Master Agreement
Vendor ID: VS0000044797
Legal Name: CyberForce|Q LLC
Alias/DBA: Sequris Group/ CyberForce|Q
Total Bid: $41,424.91
Response Date: 03/26/2024
Response Time: 14:50
Responded By User ID: terriemathison
First Name: Terrie
Last Name: Mathison
Email: tmathison@cyberforceq.c
Phone: 2488371242
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: 7
Total of All Attachments: 7

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 ESR03262400000005389	1

VENDOR

VS0000044797
CyberForce|Q LLC

Solicitation Number: CRFQ 0705 LOT2400000009

Total Bid: 41424.91000000000349245965480 **Response Date:** 2024-03-26 **Response Time:** 14:50:51

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				9196.72

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Eternal Network Penetration Testing

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				9916.72

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Website Penetration Testing

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				17393.44

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Internal/Client-Side Network Penetration Testing

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				4918.03

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Wireless Penetration Testing

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

CYBERFORCE

RESPONSE PROPOSAL

Prepared For
West Virginia Lottery

Solicitation No. CRFQ0705
Network Penetration Testing and Cybersecurity Assessment

March 25, 2024

47911 Halyard Drive, Suite #110
Plymouth, MI 48170
www.cyberforceq.com
Office 248.837.1400 | Fax 248.837.1401

TABLE OF CONTENTS

COVER LETTER

March 25, 2024

State of West Virginia
Department of Administration – Purchasing Division
Attn: Brandon Barr
2019 Washington Street East
PO Box 50130
Charlston, WV 25305-0130

RE: Request for Proposal for Network Penetration Testing and Cybersecurity Assessments

With the State of West Virginia having a goal of supporting cybersecurity improvement with the West Virginia Lottery, it is a pleasure to be considered as a cybersecurity partner for your community. As a government organization collaborating with the West Virginia Lottery, we know providing services, sound initiatives, and safe practices are your top priority. CyberForce|Q relates to that goal, as we continue to be a "Collective force for good," protecting cybersecurity systems across the nation. As a leading provider of cybersecurity solutions, with over 28 years of experience, our organization will deliver services with deep expertise proven methodologies to meet and exceed your expectations and requirements.

Included in this response, you will find responses that meet and exceed your goals of:

- Providing the West Verginia Lottery with comprehensive Penetration Testing Assessments
- Providing recommendations for improvements
- Resources for effective and efficient project management
- Team with extensive experience with government agencies

Eric Eder will also serve as the Contract Manager for this engagement.

We are excited to share our passion of improving cybersecurity with your organization and look forward to the opportunity of achieving success together, as a cybersecurity partner.

Sincerely,

Eric S. Eder

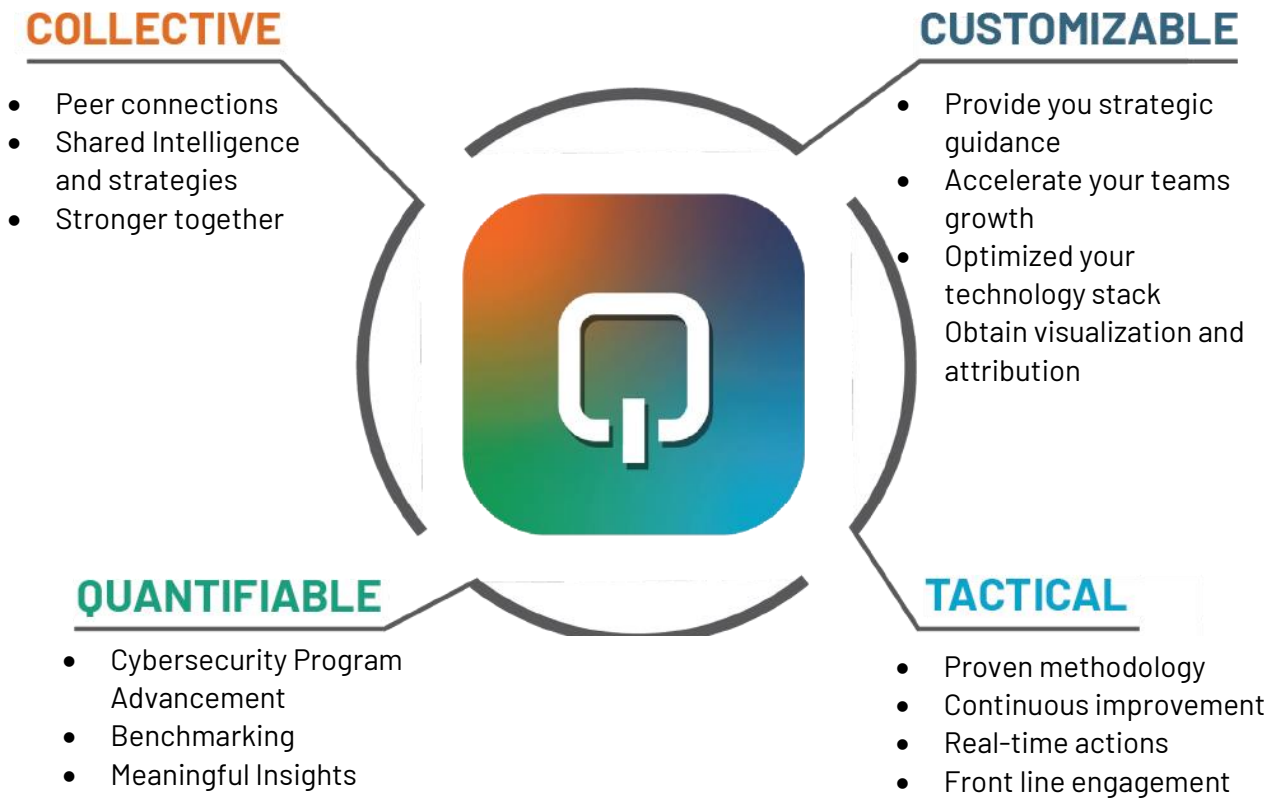
Eric S. Eder
Founder and President, CyberForce|Q
47911 Halyard Road, Suite 110
Plymouth, MI 48170
Phone: (248)837-1400

3. QUALIFICAITONS

CyberForce|Q has provided information security services for over 28 years. We architect and implement quantifiable cybersecurity programs for organizations of all sizes. We have performed hundreds of penetration tests and have deep, documented expertise and certifications that meet and exceed your requirements.

3.1 GENERAL OVERVIEW

CyberForce|Q provides a wide range of services to a diverse group of organizations including government entities, educational organizations, healthcare entities, manufacturing enterprises, and both public and private organizations. By providing technology-agnostic solutions, CyberForce|Q's goal is to enhance the current capabilities of the organizations we work with, by integrating our services with your current technologies and systems. Every organization is unique, which is why we meet you where you are in your cybersecurity journey, and tailor our solutions to your needs.



EXPERIENCE IN PROVIDING PENTRATION TESTING SERVICES

CyberForceQ has performed penetration testing for large government organizations, educational institutions, and civilian companies all across the nation. We perform penetration testing for the following services:

- Internal network penetration testing
- External network penetration testing
- Wireless penetration testing
- Web application penetration testing
- Mobile application penetration testing
- IoT penetration testing
- Red team assessments
- Tabletop Exercises
- Social engineering (electronic and physical)

Our security consulting team will demonstrate real-world attacks on your network, devices, web applications, infrastructure, and personnel to expose your hidden security risks and steps to remediate any weaknesses. With 28 years of IT and security experience, we have performed hundreds of penetration tests for a wide variety of industries. Our experts have the ability to perform internal and external testing, making sure even physical locations are secure.

Our company is headquartered in Plymouth Township, Michigan. Our primary data center is in Grand Rapids, Michigan. We have offices and an additional data center in Phoenix, Arizona. CyberForceQ is a US based company, and we are able to perform both virtual and on-site operations. We have operational and sales representation in Michigan, New York, Texas, Arizona, and Colorado.

3.2 PROFESSIONAL REFERENCES

As a cybersecurity company dedicated to protecting our partners, CyberForce|Q only discloses names of customers who have expressly agreed to be mentioned as a reference to external sources. As a trusted partner of several organizations, we are glad to have these individuals share their experience of our services and capabilities with you.

CyberForce|Q References:

Reference #1: **Commonwealth of Massachusetts – Executive Office of Education**
Contact: Ken Klau, Senior IT Program and Portfolio Manager
Phone: (781)605-4121
Email: Kenneth.klau@mass.gov
Address: 75 Pleasant Street, Malden, MA 02148

Services Provided: Penetration Testing assessment services provided for 11 higher education institutions. Massachusetts Executive Office of Education requested an External and Internal Assessment and Penetration testing. All 11 institutions needed individual kickoff calls and scheduling. A deadline for completion was required by the EOE and was met by our team before the deadline. We provided each institution with a comprehensive report and recommendations for improvements, detailed to include critical, high, medium, and low findings. Our services allowed us to provide actionable plans for each institution for improving their cybersecurity posture. A redacted report was provided to the EOE for their review. Our team has been rehired in 2024 to conduct an additional 8 educational institutions for external and internal assessment and penetration testing.

Client Engagement: 2023 – Current

Reference #2: **City of Southfield, Michigan**
Contact: Rene Hinojosa, Director of Technology
Phone: (248)796-5000
Email: rhinojosa@cityofsouthfield.com
Address: 26000 Evergreen, Southfield, MI 48077

Services Provided: Q|FRAME™ Cybersecurity Risk Assessment Services, Government Security Operations Center (GovSOC) and SIEM services provider, and firewall management services.

Program Outcomes and Advancement: Through our Q|FRAME™ assessment we provide measurable organizational data used to provide operational cybersecurity policies, procedures,

and guidance. The GovSOC provides 24x7x365 cybersecurity continuous monitoring and alerting, providing continuous improvement in their cybersecurity posture. Through monitoring, our services include preventing, detecting, analyzing, and responding to cybersecurity incidents. Further threat detection, event triage, and incident response action are key components of our SOC.

Client Engagement: 2003 - Current

Reference #3: **Oakland School Districts**
Contact: Ryan Velzy, Director of Technology
Phone: (248)209-2439; Fax: (248)209-2085
Email: ryan.velzy@oakland.k12.mi.us
2111 Pontiac Lake Road, Waterford Twp., MI 48328

Services Provided: Penetration Testing services for 29 school districts. Included External, Internal, Web Application and Phishing Social Engineering. This engagement included 1,500 servers and 15,000 other networked devices; 700 public IP addresses; 15 Web Applications with the social engineering testing for 22,000 employees. Our services assisted the school district in implementing plans for remediation and improvement in their security posture.

Start/End Date: 5/1/2021 – 12/15/2021

CyberForceQ was selected as a cybersecurity solutions provider by the following associations:

Association	Scope of Services
Commonwealth of Massachusetts MASSACHUSETTS STATEWIDE CONTRACT ITS78: Data, Cybersecurity, and Related Audit, Compliance, and Incident Responses Services	CyberForceQ was selected as a statewide contractor for Data, Cybersecurity, and Related Audit, Compliance, and Incident Response Services for the Commonwealth under a statewide contract as a provider for entities in Massachusetts.
Washington State Purchasing Program WSIPC Inspired by education. Empowered by technology.	CyberForceQ is a proud awarded vendor for WSIPC RFP 22-05 Managed Security Solutions and 21-04 Security Awareness Training Solutions. As a vendor of a competitively bid contract we offer comprehensive cybersecurity programs for schools.
BuyBoard National Purchasing Cooperative BuyBoard	As an awarded vendor for Cybersecurity Assessments, Products and Related Services for the BuyBoard National Purchasing Program, CyberForceQ can offer BuyBoard members competitive pricing, through a trusted procurement process, with reduced costs.
State of New York, Erie 1 BOCES erie boces	Cybersecurity Assessments for New York school districts, providing baseline assessments to help schools become compliant with the EdLaw (2-d) requirement.
Michigan Health and Hospital Association (MHA) MHA Michigan Health & Hospital Association	We are an endorsed business partner of MHA, being chosen as one of their recommended cybersecurity partners, after thorough research of our capabilities and offerings.
State of Michigan and MiDEAL STATE OF MICHIGAN MiDEAL www.michigan.gov/mideal	Cybersecurity Assessment partner for their member organizations, which include schools, government, and community entities, to provide baseline assessment and monthly advisory sessions.
Michigan Economic Development Corporation and the Michigan Defense Center MEDC MICHIGAN ECONOMIC DEVELOPMENT CORPORATION	Cybersecurity Compliance Consulting Services for Michigan businesses seeking assistance in achieving NIST 800-171 for CMMC compliance.

3.3 OUR TEAM

The assigned Account Representative will be John Reilly and the assigned Project Specialist is Jason Zaffuto. Each of our business partners are paired with a dedicated Participant Success Liaison to have a consistent point of contact for your continued operations. Our team is dedicated to your project and to providing professionalism when working with clients. We commit to bring our core values of Authenticity, Positivity, BOLD Contribution, Collaboration, and Collective Innovation to your project.

All penetration testing is conducted by Jason Zaffuto, who is highly experienced and accredited in information technology and security. His methodology includes understanding the client's business needs, in order to execute work that meets and exceeds client requirements. In addition, Jason adds value through continual insights and consultative advice, assisting clients based on their industry and current practices.

Jason has over 20 years of experience and his areas of expertise include penetration testing, ethical hacking, security research, and systems administration. He has held positions as an Army Paratrooper, Military Intelligence Electronic Warfare Systems Maintainer, System Engineer (at NASA's Stennis Space Center), and as an NSA Systems Administrator and Intelligence Contractor.

Eric Eder

Eric Eder founded CyberForce|Q over 28 years ago and currently serves as President and CEO. He has extensive experience in account and engagement management, providing technical and strategic advice to clients and team members. In his role, Eric works directly with organizations to help them advance their cybersecurity programs and leads a talented group of information security professionals in providing exceptional quality service.

Eric is a certified cybersecurity professional with certifications related to health services, city government, and education, among others. He is also a board member of the Michigan Healthcare Cybersecurity Council (MiHCC) – a nonprofit corporation supporting the citizens, patients, workforce, and students of Michigan by protecting the critical healthcare information infrastructure. Eric earned a bachelor's degree with distinction from the University of Michigan and a master's in International Management from Thunderbird, The American Graduate School of International Management. He also holds Chartered Financial Analyst (CFA) and Chartered Alternative Investment Analyst (CAIA) designations.

Jason Zaffuto

Jason is responsible for performing all Penetration Testing for CyberForce|Q. He has over 20 years of experience working with electronics, information technology, and security, with extensive expertise in offensive security. Jason has held positions as an Army Paratrooper, Military Intelligence Electronic Warfare Systems Maintainer, System Engineer (at NASA's Stennis Space Center), and as an NSA Systems Administrator and Intelligence Contractor. In addition, Jason is highly accredited, holding many certifications including NSA, CompTIA, and Microsoft affiliated certifications.

Terrie Mathison

Terrie is the Business Operations Coordinator of CyberForce|Q and I hold a central position in upholding and enhancing client satisfaction. I actively engage in close collaboration with Sales, Marketing, and Operations Teams to streamline the client experience, facilitating swift and efficient project delivery. Leveraging over three decades of experience in customer operations, I will ensure meticulous execution of Project Management for your team. Consistently achieving on-time and on-budget project deliverables.

John Reilly

Based in Michigan, John is the National Business Development lead for CyberForce|Q. John has been helping clients drive efficiency in cybersecurity operations and providing clients with strategic and tactical cybersecurity solutions for the last 10 years. John is passionate about serving the under resourced and helping organizations prioritize their cybersecurity needs. He strives to assist organizations with advancing their cybersecurity program by designing plans to reduce risk that fit each participant's unique cybersecurity goals. Building trust and collaboration with his clients is one of his strongest skills.

3.4 CERTIFICATIONS

Jason holds the following certifications:

NSA IEM/IAM – Certified NSA InfoSec Evaluation Methodology / InfoSec Assessment Methodology	**ECSA** – EC-Council Certified Security Analyst
A+ - CompTIA A+	**CEH** – EC-Council Certified Ethical Hacker
Network+ - CompTIA Net+	**MCP** – Microsoft Certified Professional
Security+ - CompTIA Sec+	**MCSE+S** – Microsoft Certified Systems Engineer with Security Specialization
OSWE - Offensive Security Web Expert	**MCSA** – Microsoft Certified Systems Administrator
OSCP – Offensive Security Certified Professional	**MCT** – Microsoft Certified Trainer
GIAC – Penetration Tester (GPEN)	**ECSA –** Certified Security Analyst
LPT – EC-Council Licensed Penetration Tester	
CISSP – Certified Information Systems Security Professional	

3.5 PENETRATION TESTING METHODOLOGY

CyberForce|Q brings decades of experience providing security, privacy, and compliance services and conducting security assessments for government and educational institutions. We have in-depth knowledge of a broad range of application regulations that position us to conduct the information security penetration testing. Operating as a "collective force for good", our goal is to advance the cybersecurity of our clients and protect them against potential threats. With our focus on collective innovation and continuous improvement, we assist our partners with consistently strengthening their cybersecurity programs and staying compliant. Using this methodology, we can elevate the security of the West Virginia Lottery with our service offerings.

The engagement will provide a holistic penetration test, incorporating assessments of external network, website, wireless, and internal/client-side environments. Adherence to the Center for Internet Security (CIS) methodology serves as the foundation for rigorous evaluation. Leveraging techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide, each facet of the Lottery's infrastructure will undergo meticulous scrutiny. The external network assessment will scrutinize perimeter defenses for vulnerabilities like misconfigurations and outdated software, while the website evaluations target common OWASP Top 10 vulnerabilities such as injection flaws and broken authentication. The wireless assessments aim to uncover weaknesses in Wi-Fi security protocols, and internal/client-side testing delves into potential insider threats and vulnerabilities stemming from end-user interactions. By synergizing these methodologies, the penetration test will provide a comprehensive view of the Lottery's security posture, empowering stakeholders with actionable insights to bolster defenses and mitigate risks effectively.

3.6 BACKGROUND CHECKS

As a Cybersecurity firm, we use a third-party paid service. Our background checks are exhaustive. We use B&B Reporting, Inc. for our background checks, which includes the following:

- Social Security Verification
- Sex Offender Registry
- Office of Foreign Assets Control (OFAC)
- OIG/LEIE Exclusion List
- Prior Employment Verification
- Personal and Professional References
- Educational Verification
- Criminal History
- Motor Vehicle Records
- Credit History
- Procedure

Per West Virginia Lottery's requirements, CyberForce|Q will provide names, addresses and fingerprint information for a law enforcement background check prior to the award.

3.7 NON-DISCLOSURE AGREEMENT

CyberForce|Q has signed the Non-Disclosure Agreement.

4. MANDATORY REQUIREMENTS

CyberForce|Q has over 28 years of experience delivering cybersecurity and penetration testing services. Having conducted hundreds of tests We will meet and exceed West Virginia Lottery's mandatory requirements with experience, capability, structured approach, and execution.

CyberForce|Q will employ a four-phased structure methodology for the penetration test that begins with reconnaissance, where information gathering techniques such as open-source intelligence (OSINT) and network scanning are employed to identify potential entry points and vulnerabilities. Subsequently, mapping involves the systematic exploration and enumeration of discovered assets, services, and network topology to construct a comprehensive blueprint of the target environment. The discovery phase entails the active probing and validation of vulnerabilities and weaknesses identified during mapping, utilizing tools and techniques tailored to the specific context. Finally, exploitation leverages the insights gained to simulate real-world attacks, effectively penetrating the target systems to demonstrate the potential impact of security breaches and provide actionable recommendations for remediation. This structured approach ensures a thorough assessment of the organization's security posture, equipping Lottery stakeholders with insights to fortify defenses against evolving cyber threats.

4.1. EXTERNAL NETWORK PENETRATION TEST

Network: 1 Public Live Systems
Consultant Presence: 100% Remote

The purpose of external penetration testing is to identify, evaluate, and address any potential or existing security issues, which cyber criminals may use to gain access to a company's information systems and illegally obtain proprietary information.

Our External penetration testing will provide a four-phased approach that will include reconnaissance, mapping, discovery, exploitation, and a social engineering exercise. We will:

- Identifying and assessing all Internet-facing assets a criminal hacker could use as potential entry points into your network.
- Assess the effectiveness of your firewalls and other intrusion-prevention systems.
- Establish whether an unauthorized user with the same level of access as your customers and suppliers can gain access to your systems via the external network.
- Critical business resources such as external portals that allow access to internal systems, or to sensitive company data, are specifically tested. This phase exploits observed vulnerabilities, and identifies what information is being exposed to outsiders through your perimeter systems. We will look to gain access to sensitive information and discover methods an attacker could use to attack your clients or users. In quality external pen testing, the security professional conducting the assessment will replicate the activities of real hackers, including executing exploits to attempt to gain control of systems. We will also test the extent of any weaknesses discovered to see how far a malicious attacker could burrow into your network and what the business impact of a successful attacker would be. We will identify network security flaws.
- Exploitation will include a social engineering exercise. This phase is designed to convince your employees to release sensitive data through our customized phishing attacks. If any data is obtained which could be leveraged for additional attacks, an attempt will be made to pivot into other systems or directly obtain critical data. This situational assessment for your employees will expose gaps in process, procedures, and general security awareness. We will test up to 200 users, as you've identified in our project kickoff meeting.
- Reconnaissance will include WHOIS, ARIN and DNS lookups (public and entities server), OSINT searches, list building, metadate analysis.
- Mapping will include Network Discovery, Port and Protocol Scanning, O/S Version Scanning
- Discovery will include Vulnerability Scanning, Enumerating Network Services, Username and Email Enumeration
- Exploitation will include the using vulnerability information to gain access to additional access, privileged access, and using compromised systems, pivot to other in-scope systems for testing.

CyberForce|Q will not conduct DoS attacks in this phase of testing. **Heavy load brute forced attacks will only be performed with prior lottery approval.** We will notify West Virginia Lottery of any High-Risk vulnerabilities or service disruption immediately. All findings, risks and remediation recommendations will be prioritized and provided through the executive and technical reports.

CyberForce|Q will provide a Findings Presentation to the Lottery management team after the External Penetration Test is concluded. The presentation will provide an overview of the strengths, weaknesses, and vulnerabilities found in the test.

4.2. WEBSITE AND WEB APPLICATION PENETRATION TEST

Applications: 1 website and no web applications to date
Consultant Presence: 100% Remote

CyberForce|Q will simulate as a malicious actor attacking your web applications using techniques outlined by OWASP, SANS CEW Top 25, and CERT Secure Coding. This will be in-depth manual application testing which enables us to find what scanners may miss. An information gathering phase consists of reconnaissance, server fingerprinting, application enumeration, and more. Information gathering efforts result in a compiled list of metadata and raw output to obtain as much information about the application as possible. The purpose of this step is to map the in-scope application and prepare for threat identification, collectively.

Testing will be from both inside and outside the network ensuring the industry accepted vulnerability and penetration testing approach of ISO 27001, NIST SP 800-115. CyberForce|Q's penetration tester will attempt to exploit against all types of vulnerabilities that give access to private data, cardholder data, and sensitive information. We will compile and develop a plan for exploitations, analyze the impact and potential exploitable vulnerabilities, and select the best methods and tools to properly exploit each suspected vulnerability.

Further, during the manual exploitation of the vulnerabilities identified, we will determine the level of risk and level of exploitation possible, capture logs and evidence of proof of exploitation (this includes images, screenshots, and configurations). We will notify the client of any Critical and High findings upon discovery. We then provide Executive Summary and Technical reports, rating the risk findings, and providing clear and actionable reporting. We will deliver the report through encryption and present our findings to you in an online meeting.

Our Website and Web Application penetration testing will provide a four-phased approach that will include reconnaissance, mapping, discovery, and exploitation. We will also determine static and dynamic page counts.

- Reconnaissance will include WHOIS, ARIN, and DNS lookups (both public and entity), OSINT searches, password list building, information gathering of from the lottery's web applications, and metadate analysis.
- Mapping will include SSL/TLS Analysis, Virtual Hosting & Load Balancer Analysis, software Configuration Discovery, HTTP Options Discovery, Web Application Spidering, Directory Browsing, Web Application Flow, and Session analysis.
- Discovery will include Vulnerability Scanning, Username and Email Enumeration, Identification of Werb Application Specific and Web Service Specific Vulnerabilities, the Identification of Authentication and Authorization Issues and Bypasses

- Exploitation will include Brute Force Logins, exploiting vulnerable systems, and pivoting to gain access to other in-scope systems.

CyberForce|Q will conduct DoS attacks in this phase of testing per the mandatory requirement. We will notify West Virginia Lottery before the attack commences and of any High-Risk vulnerabilities immediately upon discovery.

CyberForce|Q will provide a Findings Presentation to the Lottery management team after the Website and Web Application Penetration Test is concluded. The presentation will provide an overview of the strengths, weaknesses, and vulnerabilities found in the test.

4.3. INTERNAL NETWORK PENETRATION TEST

Consultant Presence: 100% On-site Services
Locations: 8

Network: 132 Services; 230 Windows OS Endpoints
Consultant Prescence: Consultant on-site

The goal of this phase is to exploit observed vulnerabilities and identify what information is being exposed to outsiders, after receiving full disclosure of the internal configurations, including source code, IP address, diagrams, and network protocols.

CyberForce|Q will attempt to find and exploit vulnerabilities of a system to steal or compromise the organization's information. This testing is a real scenario that happens often in organizations where a malicious actor gains a foothold on an internal asset and exploits it. The malicious actor could be a present or former employee or an external entity that has acquired internal server login credentials. Testing will be performed on-site at each location per the mandatory requirements.

Our Internal Network penetration testing will provide a four-phased approach that will include reconnaissance, mapping, discovery, and exploitation:

- Reconnaissance will identify software versions along with potentially useful software configurations or settings, identify any anti-malware, firewall, and IDS products on the system, gather information about the network, and verify the ability to execute scripts or third-party programs.
- Mapping and Discovery will include identifying possible vulnerabilities affecting the provided host and determining the possibility of receiving and executing various malicious payloads. When a vulnerability is found on a server or network device that relates to device configuration, a configuration review will be conducted.
- Exploitation will include attempts to bypass anti-malware solutions and security restrictions, escape restricted environments, and escalate privileges.

CyberForce|Q will notify West Virginia Lottery of any High-Risk/Critical vulnerabilities immediately. All findings, risks and remediation recommendations will be prioritized and provided through the executive and technical reports.

CyberForce|Q will provide a Findings Presentation to the Lottery management team after the Internal Penetration Test is concluded. The presentation will provide an overview of the strengths, weaknesses, and vulnerabilities found in the test.

4.4. WIFI PENETRATION TESTING

Consultant Presence: 100% On-site Services
Locations: 8

This simulates a malicious actor attacking your web application using techniques outlined by OWASP, to exploit against all types of vulnerabilities that give access to private data, cardholder data, and sensitive information. A wireless penetration test will detect, and exploit security controls employed by various wireless technologies and standards, weak security protocols, and misconfigured access points. Gathering and cracking Pre-Shared Keys (PSKs), exploiting vulnerable technologies like WEP and WPA/WPA2, and building rogue access points to attack misconfigured WPA2/Enterprise settings are all utilized techniques. Our penetration testers will also map out your wireless network and notify you of any existing rogue access points. We will also test your guest wireless network for proper segmentation and guest isolation.

Our WiFi penetration testing will provide a four-phased approach that will include reconnaissance, mapping, discovery, and exploitation:

- Reconnaissance will include WHOIS, ARIN, and DNS lookups (both public and entity), OSINT searches, password list building, information gathering of from the lottery's web applications, and metadate analysis.
- Mapping will include Sniffing, War Walk, Identification of Rogu Access Points
- Discovery will include AP Attacks, Client Attacks, applicable DoS attacks with prior Lottery approval.
- Bluetooth/Zigbee/SDR Attacks where applicable and with prior Lottery approval

CyberForce|Q will provide a Findings Presentation to the Lottery management team after Wireless Penetration Test is concluded. The presentation will provide an overview of the strengths, weaknesses, and vulnerabilities found in the test.

ENGAGEMENT DELIVERABLES

This engagement will require dynamic interaction between CyberForce|Q and the client team, in order to meet the outlined goals. Specific roles and accountabilities are defined as follows:

CyberForce|Q	Client	Collaborative
Report High Risk vulnerabilities immediately Will provide weekly status updates Develop and deliver project plan and outline with project dates and times Conduct Q&A session with consultant to discuss process, findings, and recommendations Create and present final report at the end of each phase Can provide Letter of Attestation, if needed	Access to IT managers and IT staff to define basic data sets and elements Obtain written authorization from all third-party service providers prior to testing For internal testing, install virtual machine for remote testing Provide IP addresses and URLs as needed Provide credentials for applications, as necessary	Participation in onsite and web-based meetings Participation in Phase Kick-Off (30-60 minutes): establish timelines, training schedule, review client requirements Participation in Weekly Status Calls (30 minutes) Review final report together If needed, Teams channel is established for consistent communication.

REPORTING AND DOCUMENTATION

Upon the completion of each test type of the Ethical Hacking Assessment, CyberForceIQ will provide the client with reports detailing all the vulnerabilities that were identified, the risk level of the vulnerability (**High, Medium, Low, Informational**), and the recommended course of action in order to remediate each of the vulnerabilities. A sample report will be provided electronically as part of the RFP submission.

Risk Level	Recommendation
High Risk	Pose a serious, immediate threat to the confidentiality, integrity, and availability of the environment and its users, the exploitation of these findings would lead to the compromise of security. These findings should take the highest priority when considering your remediation efforts.
Medium Risk	Pose a threat to the environment and its use, these vulnerabilities are not necessarily immediately exploitable, but should be given serious consideration when remediating. An attacker could use medium level vulnerabilities to enumerate information and could lead to further attacks to compromise the environment and its users.
Low Risk	Do not pose a serious or immediate threat to the environment but is not recommended exposure. These vulnerabilities should not be ignored and should be considered when looking to secure your environment from attacks and compromise.
Informational	Interesting facts that were found during the assessment that pose no obvious risk to the environment but should be taken into consideration.

The reports will be delivered to meet your requirements of an Executive Summary Report and a separate Technical Report. The components are detailed below:

Section	Definition
Executive Report	High-level overview of the in-depth security assessment .
Statement of Work	An overview of the client specified parameters for the assessment and the responsibilities of each party.
Results	An overview of the objectives that were met during the in-depth vulnerability assessment (i.e., unauthorized access obtained to environment, information resource, personal identifiable information was disclosed).
Analysis and Recommendations	An overview of the number of findings with their associated risk ratings. Detailed actionable steps to remediate or mitigate identified vulnerabilities will be provided.
Technical Report	We will provide a technical report of the finding of our security assessment.
Conclusion	The outcome of the Security Assessment will be a deliverable report with all the findings, steps to mitigation, with actionable project plan for your use.
Methodology	A summary of our in-depth vulnerability assessment methodology is given, detailing the phases that are taken from beginning to the end of the assessment.
Technical Report: Security Analysis and Recommendations	The core of the report gives detailed technical insight on the vulnerabilities that were identified, and the recommended remediation steps to eliminate the threats.

FINDINGS PRESENTATION

Upon completion of each test of the project, CyberForce|Q will deliver a comprehensive Findings Presentation to the Lottery management team, aimed at offering a detailed overview of the findings, insights, and recommendations garnered during the assessment phase. This presentation serves as a pivotal moment for stakeholders to gain a deeper understanding of the cybersecurity landscape surrounding their operations.

The presentation will begin with a concise summary of the project scope, methodologies employed, and the key objectives set forth at the project's outset. This sets the stage for a thorough examination of the strengths, weaknesses, and vulnerabilities uncovered throughout the assessment process.

Each aspect of the presentation will be meticulously structured to ensure clarity and relevance. The strengths identified within the lottery's existing cybersecurity infrastructure will be highlighted, emphasizing areas where robust defense mechanisms are already in place. This acknowledgment aims to reinforce positive practices and serve as a foundation for further improvement.

Conversely, weaknesses and vulnerabilities discovered within the system will be meticulously outlined, accompanied by detailed explanations of their potential impact and implications. By shining a light on these areas, the presentation aims to foster a proactive approach to cybersecurity, empowering the Lottery management team to address vulnerabilities before they can be exploited by malicious actors.

Moreover, the presentation will not only identify weaknesses but also provide strategic recommendations for remediation. These recommendations will be tailored to the specific needs and capabilities of the Lottery, offering practical steps to strengthen their cybersecurity posture effectively.

Throughout the presentation, CyberForce|Q will leverage its expertise to provide actionable insights and strategic guidance, enabling the Lottery management team to make informed decisions to mitigate risks effectively. Additionally, the presentation will emphasize the importance of ongoing vigilance and adaptation in the face of evolving cyber threats, advocating for a proactive approach to cybersecurity management.

Ultimately, the presentation serves as more than just a documentation of findings; it represents a collaborative effort between CyberForce|Q and the Lottery management team to safeguard critical assets and uphold the integrity of their operations in an increasingly complex digital landscape.

CYBERFORCE

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	$1,149.59 -	$9,196.72
2	4.2	Website Penetration Testing	8	$1,149.59	$9,916.72
3	4.3	Internal/Client-Side Network Penetration Testing	8	$2,174.18	$17,393.44
4	4.4	Wireless Penetration Testing	8	$614.75 -	$4,918.03
				TOTAL BID AMOUNT	$40,704.91 -

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:	CyberForce|Q LLC
Vendor Address:	47911 Halyard Rd. Suite 110, Plymouth, MI 48170
Email Address:	eric@cyberforceq.com
Phone Number:	248.837.1400
Fax Number:	248.837.1401
Signature and Date:	Eric S. Eder 03/25/2024

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

MUTUAL NON-DISCLOSURE AGREEMENT

This Mutual Non-Disclosure Agreement ("Agreement") is entered into by and between the West Virginia Lottery, with its principal offices located at 900 Pennsylvania Avenue Charleston, WV 25302 ("Lottery"), and _____, with its principal offices located at _____ ("Party of the second part"), with an Effective Date of _____. Lottery and Party of the second party also are referred to herein individually as a "party", or collectively as the "parties".

WHEREAS, the parties to this Agreement may wish to exchange certain information related to the provision of certain information or communication technology services by one party of interest to the other party; and

WHEREAS, the parties agree that improper disclosure of either party's Confidential Information, as defined below, by the other party could cause material harm to the party whose Confidential Information was improperly disclosed;

NOW THEREFORE, in order to protect certain Confidential Information that may be disclosed between the parties, Lottery and Alpha agree to maintain the confidentiality of the Confidential Information as follows:

I. **Definition of Confidential Information**. The "Confidential Information" disclosed under this Agreement is defined as follows:

Any data or information that is proprietary to the disclosing party and not generally known to the public, whether in tangible or intangible form, whenever and however disclosed, including, but not limited to: (i) any marketing strategies, plans, financial information, or projections, operations, sales estimates, business plans and performance results relating to the past, present or future business activities of such party, its affiliates, subsidiaries and affiliated companies; (ii) plans for products or services, and customer or supplier lists; (iii) any scientific or technical information, invention, design, process, procedure, formula, improvement, technology or method; (iv) any concepts, reports, data, know-how, works-in-progress, designs, development tools, specifications, computer software, source code, object code, flow charts, databases, inventions, intellectual property, and trade secrets; (v) solicitation for proposals, responses to proposals, bids, or information disclosed in connection with such solicitation, response, or bid; (vi) any other information that should reasonably be recognized as confidential information of the disclosing party.

II. **Disclosure Period and Term**. This Agreement protects against the disclosure of Confidential Information which is disclosed between the parties during each party's performance of its obligations associated with that certain CRFQ Agreement executed between the parties on _____ (the "Effective Date") and 3 year(s) after the termination of such Agreement ("Disclosure Period"). Therefore, the duty of a recipient of Confidential Information to protect such Confidential Information disclosed under this Agreement begins on the Effective Date and expires 3 year(s) after the end of Disclosure

Period. Upon termination of this Agreement or upon the disclosing party's request, the recipient shall cease use of Confidential Information and return or destroy it.

III. **Use of Confidential Information**. A party hereunder receiving Confidential Information shall use such Confidential Information solely for the purposes of, as applicable to the recipient, understanding current business activities of a party, soliciting a proposal for certain information technology services, responding to such proposal solicitation, reviewing solicitation responses, tendering a bid, or discussions or negotiations related to such solicitation, proposal, or bid.

IV. **Protection of Confidential Information**. Each party shall not disclose the Confidential Information of the other party to any third party. The recipient shall protect the Confidential Information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination or publication of the Confidential Information as the recipient uses to protect its own confidential information of a like nature. A recipient shall restrict disclosure of Confidential Information to its employees, provided that such employees (i) have a need to know, and (ii) are bound by obligations of confidentiality equally as restrictive as the terms of this Agreement.

V. **Exclusions**. This Agreement imposes no obligation upon the recipient with respect to Confidential Information which: (a) was in the recipient's possession before receipt from the disclosing party; (b) is or becomes a matter of public knowledge through no fault of the recipient; (c) is rightfully received by the recipient from a third party without a duty of confidentiality; (d) is disclosed by the disclosing party to a third party without a duty of confidentiality on the third party; (e) is independently developed by the recipient; (f) is disclosed under operation of law; or (g) is disclosed by the recipient with the disclosing party's prior written approval.

VI. **Miscellaneous.** Neither party to this Agreement shall acquire any intellectual property rights nor any other rights under this Agreement except the limited right to use as set forth in this Agreement. This Agreement does not prevent either Party from competing with one another for work or clients unless the parties specifically agree otherwise, in writing, as to a specific client. Each disclosing party warrants and represents that the Confidential Information and other information provided which is necessary to the purposes described hereunder, are true and correct to the best of the disclosing party's knowledge and belief. Nothing in this Agreement shall be construed to preclude either party from developing, using, marketing, licensing, and/or selling any software or other material that is developed without reference to the Confidential Information.

VII. **Export Administration**. Each party to this Agreement agrees to comply fully with all relevant export laws and regulations of the United States and other countries to assure that no Confidential Information or any portion thereof is exported, directly or indirectly, in violation of such laws.

VIII. **No Obligation to Purchase or Offer Products or Services**. Neither party has an obligation under this Agreement to purchase or otherwise acquire any service or item from

the other party. Neither party has an obligation under this Agreement to commercially offer any products using or incorporating the Confidential Information. The disclosing party may, at its sole discretion, offer such products commercially and may modify them or discontinue such offerings at any time.

IX. **General.** The parties do not intend that any agency or partnership relationship be created between them by this Agreement. This Agreement sets forth the entire agreement with respect to the Confidential Information disclosed herein and supersedes all prior or contemporaneous agreements concerning such Confidential Information, whether written or oral. All additions or modifications to this Agreement must be made in writing and must be signed by both parties. This Agreement and all matters arising out of or relating to this Agreement shall be governed by the laws of the State of West Virginia. The parties agree that the information provided as allowed by this Agreement will not contain any proprietary technical or confidential contractual information, or any financial information related to the relationship between Alpha and its partners. As a result, damages will not be included as a remedy.

The undersigned authorized representatives of each party have agreed to be legally bound by the terms of this Agreement as of the Effective Date shown above.

WEST VIRGINIA LOTTERY

By: _____

Name: _____

Title: _____

_____ **(VENDOR)**

By:_____

Name: _____

Title: _____

CYBERFORCE

Sample Client Name

Penetration Testing Sample Presentation

SCOPE OF SERVICES REVIEW

PHASE 01	Scoping & Pre-Engagement	• Define success criteria
PHASE 02	Reconnaissance	• Information gathering & discovery • Device and OS enumeration • Port scanning • Network sniffing
PHASE 03	Discover & Vulnerability Assessment	• Vulnerability detection • Authentication testing • Data validation • Configuration management
PHASE 04	Exploitation	• Vulnerability verification • False positives and false negatives elimination
PHASE 05	Analysis & Reporting	• Analyze and consolidate findings to report vulnerabilities

EXECUTIVE SUMMARY

Date of Testing – 10/1/2021 – 10/31/2021

Overview: This test was designed to provide [Customer Name] with an independent, point-in-time assessment of internal network vulnerabilities from the perspective of a malicious actor in accordance with CIS Controls and NIST guidelines.

Assessment Synopsis:

During the assessment, CyberForce|Q used an SMB relay attack against systems that did not require SMB signing and obtained Local Administrator hashes and credentials for servers and user workstations. With the Local Administrator credentials, CyberForce|Q could escalate to NT\SYSTEM privileges, disable services, such as Cylance Protect, and pull cleartext Domain Administrator passwords from memory.

Using the privileged credentials, CyberForce|Q was able to access any server information and share, including financial and Human Resource (HR) records that contained sensitive employee and customer information, such as Social Security Numbers (SSN) and bank account information. CyberForce|Q also found that the Group Policy contained an encrypted password for the Local Administrator account, which a malicious actor could decrypt using a publicly released Microsoft key. Additionally, CyberForce|Q found multiple instances of Windows Server 2003.

ASSESSMENT FINDINGS

KEY FINDINGS AND RECOMMENDATIONS:

Implied Trust Relationship Exploitation

Finding: CyberForce|Q found that user workstations and servers used the same Local Administrator passwords, which allowed CyberForce|Q to move laterally after finding Local Administrator credentials or hashes.

Recommendation: Use the Microsoft LAPS tool to assign unique passwords for each system

Insecure Password Storage in Group Policy

Finding: The Group Policy contained an encrypted password for the Local Administrator account, which a malicious actor could decrypt using a publicly released Microsoft key.

Recommendation: Install the MS14-025 patch and delete the 'groups.xml' file containing the encrypted 'cpassword'

Weak Domain Passwords

Finding: CyberForce|Q discovered that several Domain users, service accounts, and privileged accounts used weak passwords.

Recommendation: Ensure that the default password policy requires a password length based on the guidelines in this report, and train users to use pass phrases

ASSESSMENT FINDINGS

KEY FINDINGS AND RECOMMENDATIONS:

Obsolete Operating System Version in Use

Finding: CyberForce|Q found instances of Windows Server 2003.
Recommendation: Replace obsolete Operating Systems with supported ones

SMB Messaging Signing Not Required

Finding: CyberForce|Q discovered systems with SMB message signing disabled, which allowed CyberForce|Q to perform SMB relay attacks and gain Local Administrator access to the affected system.
Recommendation: Create a Group Policy that requires SMB signing for Windows systems

THREAT RANKING METHODOLOGY

Testing and vulnerability rankings are aligned to industry proven NIST 800-30 threat ranking methodology.

Likelihood \ Impact	Informational	Low	Moderate	High	Critical
High	Informational	Low	Moderate	High	Critical
Moderate	Informational	Low	Moderate	Moderate	High
Low	Informational	Low	Low	Moderate	Moderate

Table 1: Threat Likelihood and Impact

THREAT LIKELIHOOD

- **High:** A malicious actor is highly likely to initiate the threat event.
- **Moderate:** A malicious actor is somewhat likely to initiate the threat event.
- **Low:** A malicious actor is unlikely to initiate the threat event.

THREAT IMPACT

- **Critical:** The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, assets, individuals, and other organizations.
- **High:** The threat event could be expected to have severe or catastrophic adverse effects on organizational operations, assets, individuals, and other organizations.
- **Moderate:** The threat event could be expected to have serious adverse effects on organizational operations, assets, individuals, and other organizations.
- **Low:** The threat event could be expected to have limited adverse effects on organizational operations, assets, individuals, and other organizations.
- **Informational:** The threat event could be expected to have negligible effects on organizational operations, assets, individuals, and other organizations.

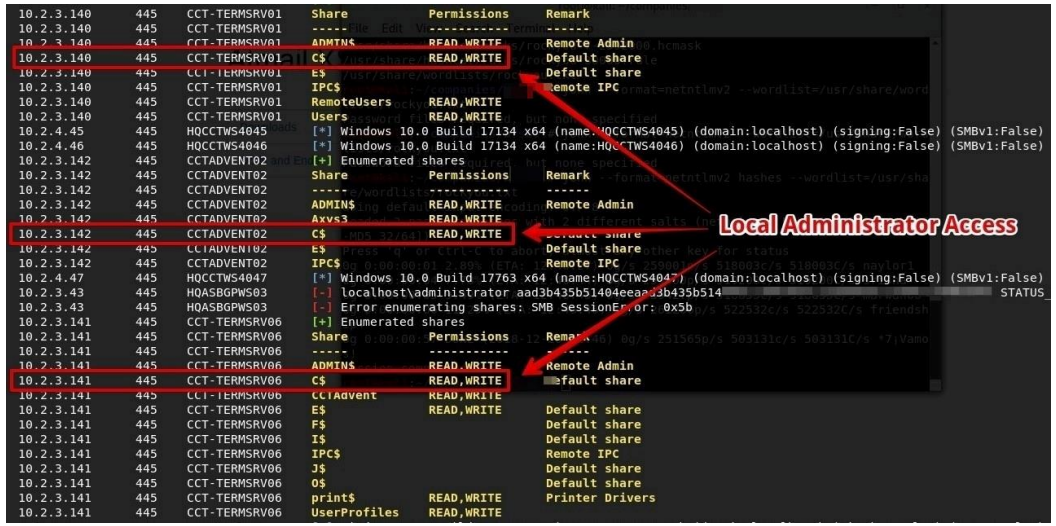
FINDING SUMMARY

Assessment Findings	Risk
Implied Trust Relationship Exploitation	Critical
Insecure Password Storage in Group Policy	Critical
Weak Domain Passwords	Critical
Obsolete Operating System Version in Use	High
SMB Message Signing Not Required	High
Weak Password Policy	High
Excessive Number of Privileged Accounts	High
Weak Local Account Passwords	High
LAN Manager Hashes Recovered	Moderate
Undetected Changes to the Domain Admins Group	Moderate
Insecure Services in Use	Low

FINDING SUMMARY

The following chart provides an overview of NIST scoring and a summary of the findings discovered during the assessment:

CRITICAL THREAT ASSESSMENTS



IMPLIED TRUST RELATIONSHIP EXPLOITATION

NIST Scoring Summary: CRITICAL

Finding Summary

If two accounts share the same password, this creates an 'implied trust relationship' as any user with access to one can access the other. In most cases, these trust relationships are created unintentionally. Implied trust relationships allow for the possibility of access between domains, domain accounts, local accounts, or even networks for malicious actors.

Implied trust relationship exploitation takes these relationships between systems and abuses that trust. For example, a malicious actor could exploit local system or Active Directory domain trust relationships to expand access across an organization's environment.

CRITICAL THREAT ASSESSMENT

Affected Resources

All servers used the same Local Administrator password.
All workstations used the same Local Administrator password.

Recommendations

Isolate hashes, tokens, and passwords. This makes it harder for malicious actors to move between systems. **To do this:**

- Use Microsoft's free Local Administrator Password Solutions (LAPS) tool
- Do not allow shared passwords.
- Disable Local Administrative accounts.
- Turn off network access to unnecessary accounts, including RDP.

Minimize the number of hashes, tokens and passwords malicious actors can access. **To do this:**

- Limit cached credentials.
- Reduce the number of local accounts, especially Administrative ones.
- Limit the number of interactive logons.
- Reboot frequently, if possible.

HIGH, MEDIUM AND LOW FINDINGS

- Two slides would be created for each Threat Assessment
  - Identifying the NIST Scoring Summary
  - Finding Summary
  - Validation Steps with photo, if available.
  - Affected Resources
  - Recommendations
  - References

All presentations would be followed up with a .pdf document of findings and recommendations for securing the exposures exploited in our Penetration Testing. A sample is attached.

CYBERFORCE

REPORT SUMMARY

INTERNAL NETWORK PENETRATION TEST

Prepared for SAMPLE CLIENT

October 1, 2021

47911 Halyard Drive, Suite #110
Plymouth, MI 48170
www.cyberforceq.com

Office: 248.837.1400| Fax: 248.837.1401

TABLE OF CONTENTS

EXECUTIVE SUMMARY

CyberForce|Q conducted an internal network penetration test for [Customer Name] from October 1, 2021 – October 31, 2021. This test was designed to provide [Customer Name] with an independent, point-in-time assessment of internal network vulnerabilities from the perspective of a malicious actor in accordance with CIS Controls and NIST guidelines.

ASSESSMENT SYNOPSIS

During the assessment, CyberForce|Q used an SMB relay attack against systems that did not require SMB signing and obtained Local Administrator hashes and credentials for servers and user workstations. With the Local Administrator credentials, CyberForce|Q could escalate to NT\SYSTEM privileges, disable services, such as Cylance Protect, and pull cleartext Domain Administrator passwords from memory.

Using the privileged credentials, CyberForce|Q was able to access any server information and share, including financial and Human Resource (HR) records that contained sensitive employee and customer information, such as Social Security Numbers (SSN) and bank account information. CyberForce|Q also found that the Group Policy contained an encrypted password for the Local Administrator account, which a malicious actor could decrypt using a publicly released Microsoft key. Additionally, CyberForce|Q found multiple instances of Windows Server 2003.

SCOPE

CyberForce|Q tested eight different class 'C' subnets on the internal network.

CONSTRAINTS

CyberForce|Q was not to perform any exploits that would cause Denial of Service (DoS) issues.

ASSESSMENT DATA

Dates: 10/01/2021 – 10/31/2021
Level of Effort: 31 days
Consultant(s): CyberForce|Q LLC

ASSESSMENT FINDINGS

The following section provides a high-level overview of key assessment findings and recommendations:

KEY FINDINGS

- **Implied Trust Relationship Exploitation:** CyberForce|Q found that user workstations and servers used the same Local Administrator passwords, which allowed CyberForce|Q to move laterally after finding Local Administrator credentials or hashes.
- **Insecure Password Storage in Group Policy:** The Group Policy contained an encrypted password for the Local Administrator account, which a malicious actor could decrypt using a publicly released Microsoft key.
- **Weak Domain Passwords:** CyberForce|Q discovered that several Domain users, service accounts, and privileged accounts used weak passwords.
- **Obsolete Operating System Version in Use:** CyberForce|Q found instances of Windows Server 2003.
- **SMB Message Signing Not Required:** CyberForce|Q discovered systems with SMB message signing disabled, which allowed CyberForce|Q to perform SMB relay attacks and gain Local Administrator access to the affected system.

KEY RECOMMENDATIONS

- **Implied Trust Relationship Exploitation:** Use the Microsoft LAPS tool to assign unique passwords for each system.
- **Insecure Password Storage in Group Policy:** Install the MS14-025 patch and delete the 'groups.xml' file containing the encrypted 'cpassword'.
- **Weak Domain Passwords:** Ensure that the default password policy requires a password length based on the guidelines in this report, and train users to use pass phrases.
- **Obsolete Operating System Version in Use:** Replace obsolete Operating Systems with supported ones.
- **SMB Message Signing Not Required:** Create a Group Policy that requires SMB signing for Windows systems.

THREAT RANKING METHODOLOGY

CyberForce|Q testing, and vulnerability threat rankings are aligned to industry proven NIST 800-30 threat rankings methodology. The following section outlines the NIST-based scoring methodology applied to the assessment findings:

Likelihood \ Impact	Informational	Low	Moderate	High	Critical
High	Informational	Low	Moderate	High	Critical
Moderate	Informational	Low	Moderate	Moderate	High
Low	Informational	Low	Low	Moderate	Moderate

Table 1: Threat Likelihood and Impact

THREAT LIKELIHOOD

- **High:** A malicious actor is highly likely to initiate the threat event.
- **Moderate:** A malicious actor is somewhat likely to initiate the threat event.
- **Low:** A malicious actor is unlikely to initiate the threat event.

THREAT IMPACT

- **Critical:** The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, assets, individuals, and other organizations.
- **High:** The threat event could be expected to have severe or catastrophic adverse effects on organizational operations, assets, individuals, and other organizations.
- **Moderate:** The threat event could be expected to have serious adverse effects on organizational operations, assets, individuals, and other organizations.
- **Low:** The threat event could be expected to have limited adverse effects on organizational operations, assets, individuals, and other organizations.
- **Informational:** The threat event could be expected to have negligible effects on organizational operations, assets, individuals, and other organizations.

LEVEL OF RISK

- **Critical**: The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, assets, individuals, and other organizations.
- **High:** The threat event could be expected to have severe or catastrophic adverse effects on organizational operations, assets, individuals, and other organizations.
- **Moderate:** The threat event could be expected to have serious adverse effects on organizational operations, assets, individuals, and other organizations.

- **Low:** The threat event could be expected to have limited adverse effects on organizational operations, assets, individuals, and other organizations.
- **Informational:** The threat event could be expected to have negligible effects on organizational operations, assets, individuals, and other organizations.

Note: See NIST's comprehensive methodology for more information: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

FINDING SUMMARY

The following chart provides an overview of NIST scoring and a summary of the findings discovered during the assessment:

Assessment Findings	Risk
Implied Trust Relationship Exploitation	Critical
Insecure Password Storage in Group Policy	Critical
Weak Domain Passwords	Critical
Obsolete Operating System Version in Use	High
SMB Message Signing Not Required	High
Weak Password Policy	High
Excessive Number of Privileged Accounts	High
Weak Local Account Passwords	High
LAN Manager Hashes Recovered	Moderate
Undetected Changes to the Domain Admins Group	Moderate
Insecure Services in Use	Low

Table 2: Assessment Findings

ASSESSMENT STORYBOARD

This section explains the steps that CyberForce|Q took to gain Domain Administrator privileges and access to sensitive data.

1. Scan for Systems Not Requiring SMB Signing
2. Perform SMB Relay Attacks
3. Gather Credentials on Systems to Gain Domain Administrator Access
4. Access Sensitive Data on SMB Shares

SCAN FOR SYSTEMS NOT REQUIRING SMB SIGNING

CyberForce|Q started the assessment by scanning for port 445 on all in-scope subnets. CyberForce|Q then used RunFinger.py to find systems with SMB signing disabled, as shown in Figure 1:

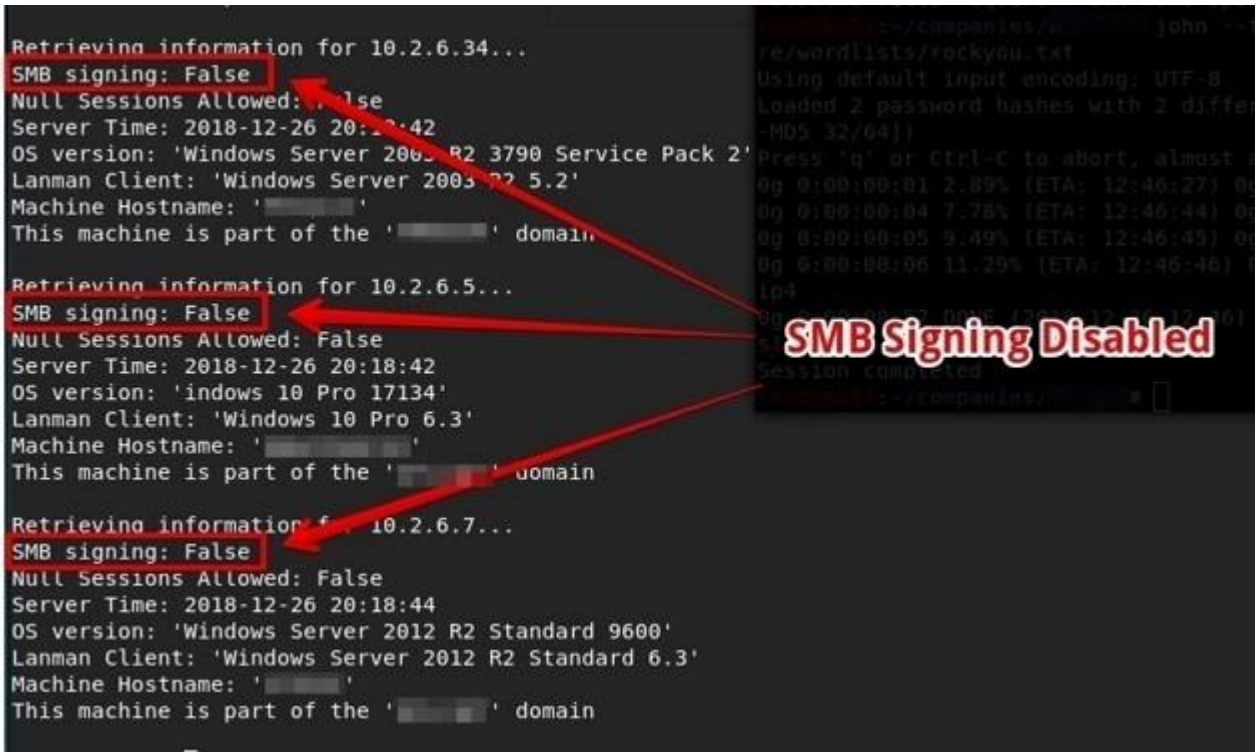


Figure 1: RunFinger.py Output

PERFORM SMB RELAY ATTACKS

Using Responder and ntlmrelayx.py from the Impacket suite, CyberForce|Q relayed NetNTLMv2 hashes from users that were Administrators on systems to gain Local Administrator hashes on targeted systems, as shown in Figure 2:

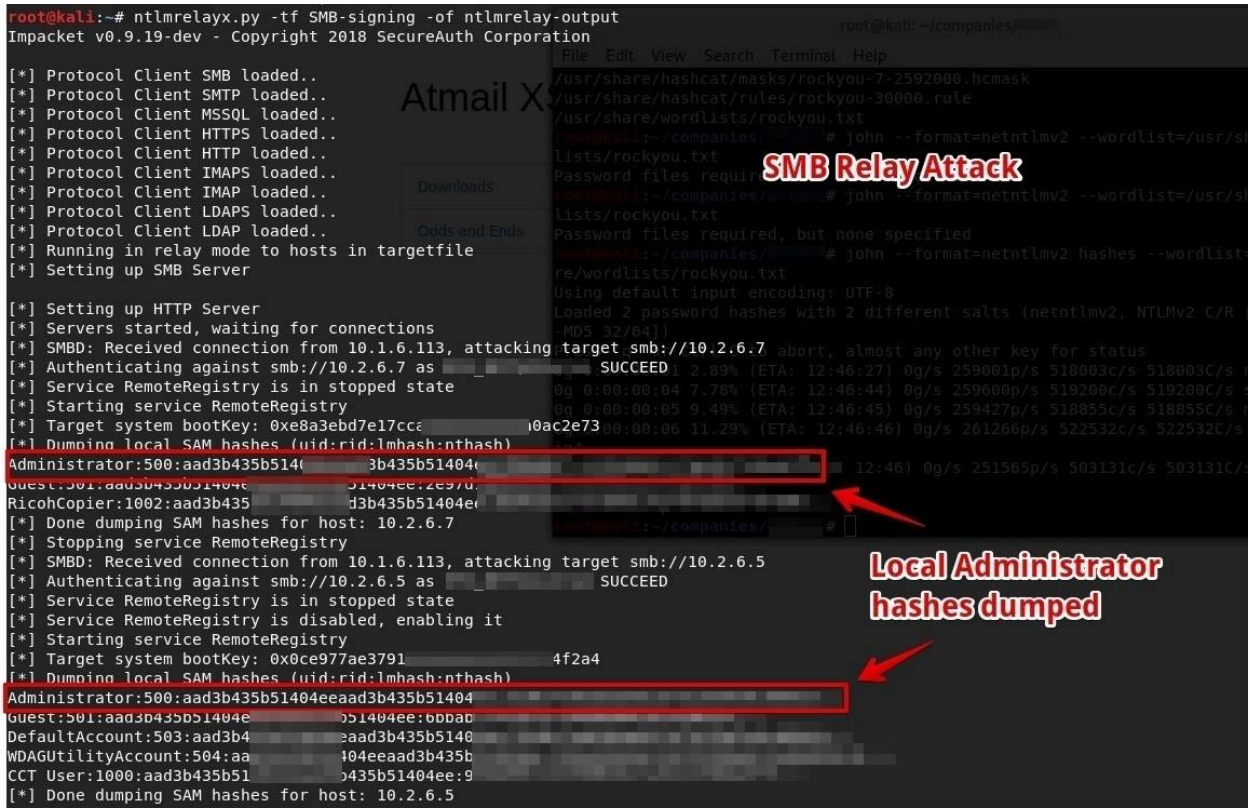


Figure 2: SMB Relay Attack Used to Gain Local Administrator Hashes

After obtaining Local Administrator hashes, CyberForce|Q used CrackMapExec to pass the Administrator hash to all systems in an attempt to discover whether the Local Administrator password was the same on all systems, as shown in Figure 3:

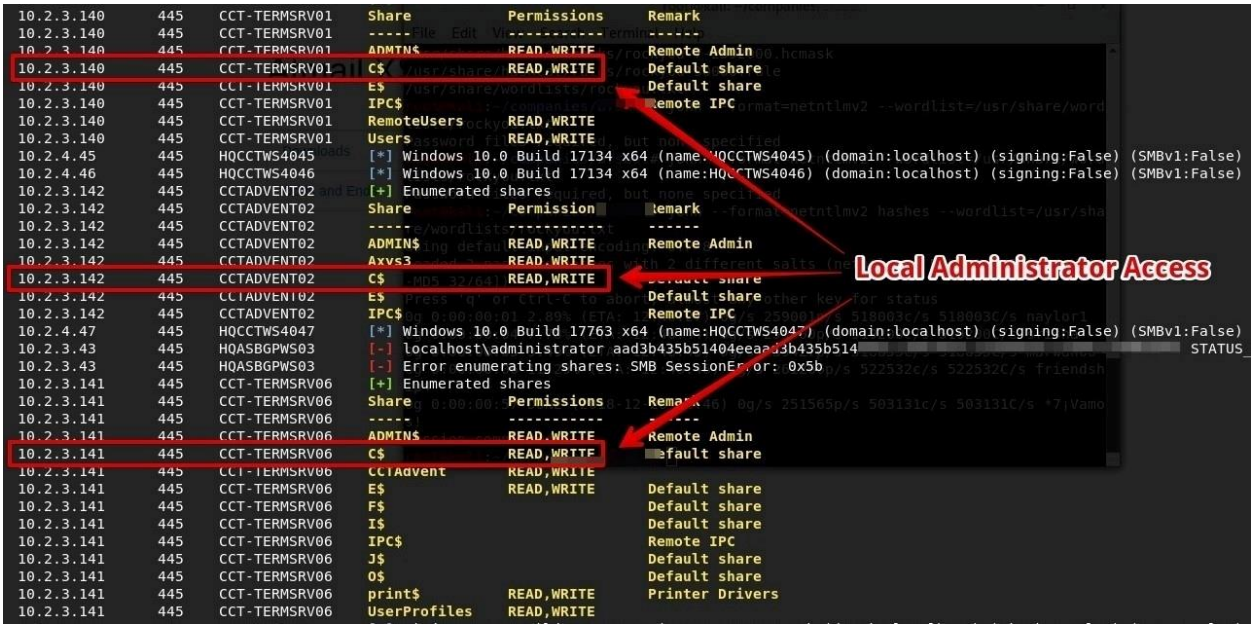


Figure 3: CrackMapExec Output Showing Local Administrator Access

GATHER CREDENTIALS ON SYSTEMS TO GAIN DOMAIN ADMINISTRATOR ACCESS

CyberForce|Q used the 'John the Ripper' tool to quick crack the Local Administrator hashes, and obtain the cleartext password, as shown in Figure 4:

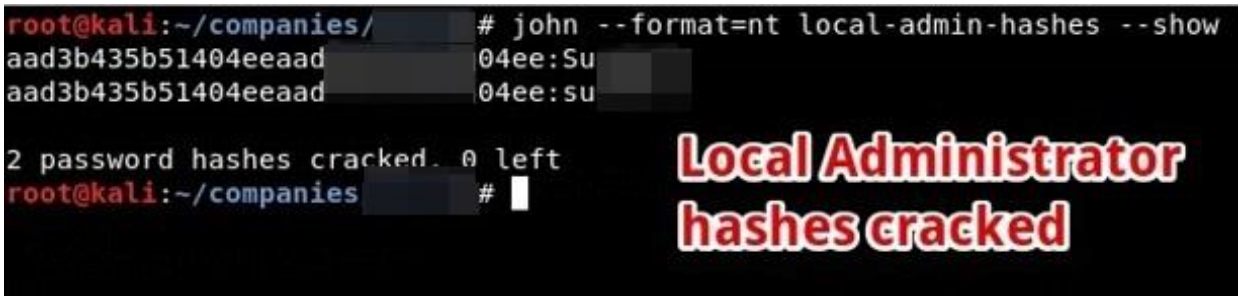


Figure 4: Local Administrator Hashes Cracked

After obtaining the cleartext password, CyberForce|Q used Remote Desktop (RDP) to access a server, as shown in Figure 5:

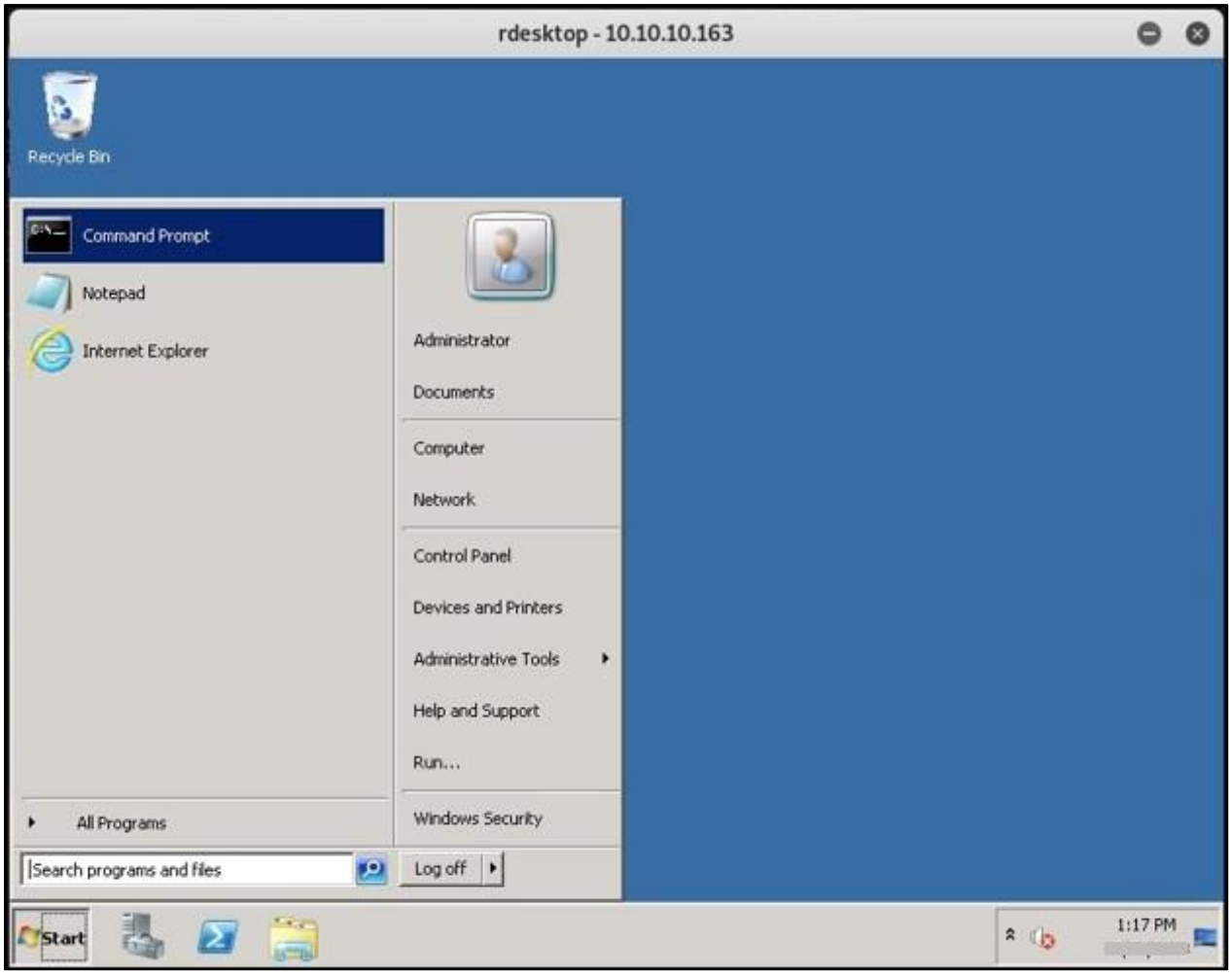


Figure 5: Local Administrator Access to System

Once on the server, CyberForce|Q used PowerShell to escalate from Local Administrator to NT\SYSTEM to temporarily disable the Cylance Protect software. After disabling the Cylance Protect software, CyberForce|Q went to Task Manager and created a dump file of the LSASS process, which contained the cleartext passwords for users that logged into the server. After off-loading the file back to CyberForce|Q system, CyberForce|Q performed analysis, and pulled cleartext passwords using Mimikatz, as shown in Figure 6:

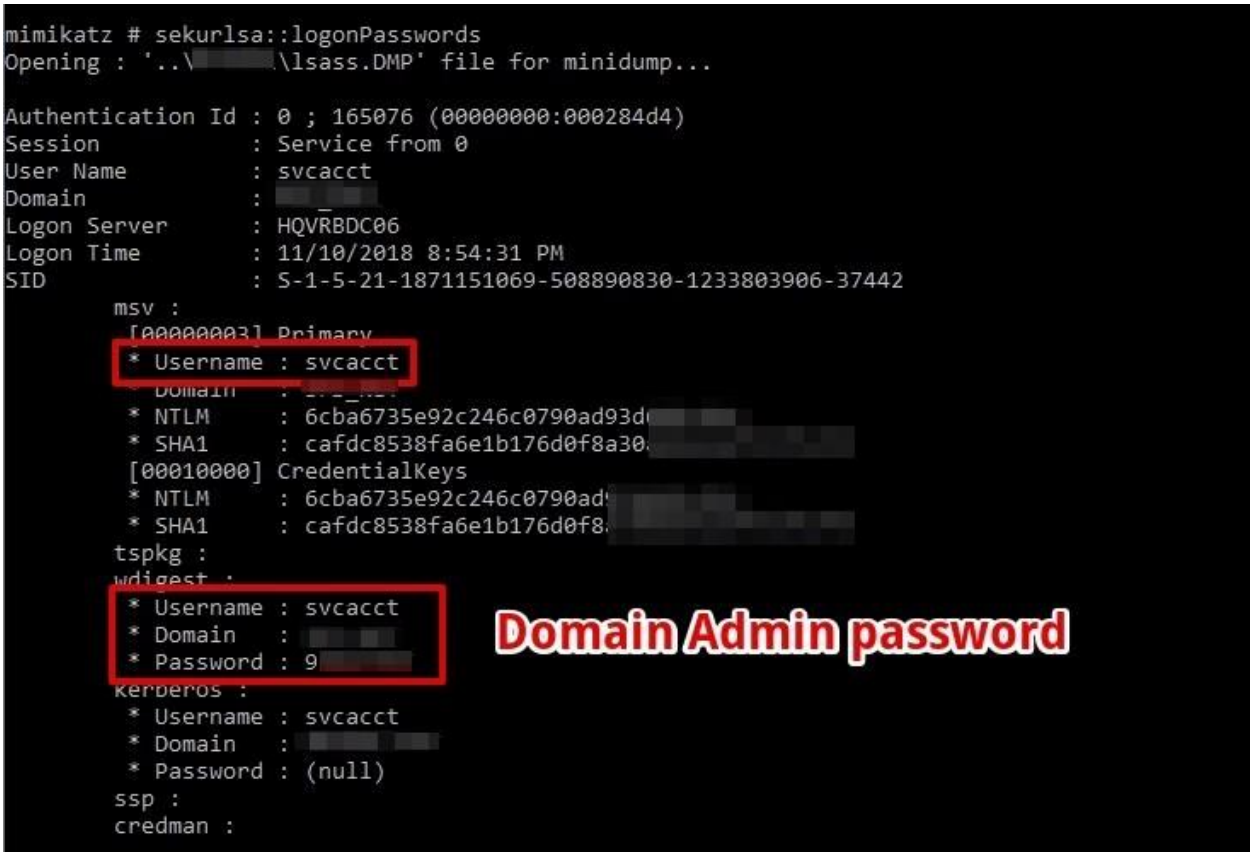


Figure 6: Domain Administrator Credentials Found in Memory

ACCESS SENSITIVE DATA ON SMB SHARES

After gaining Domain Administrator access, CyberForce|Q could enumerate any files on systems, including files with sensitive information, such as SSNs and bank information. Figure 7 shows a document with SSNs inside:

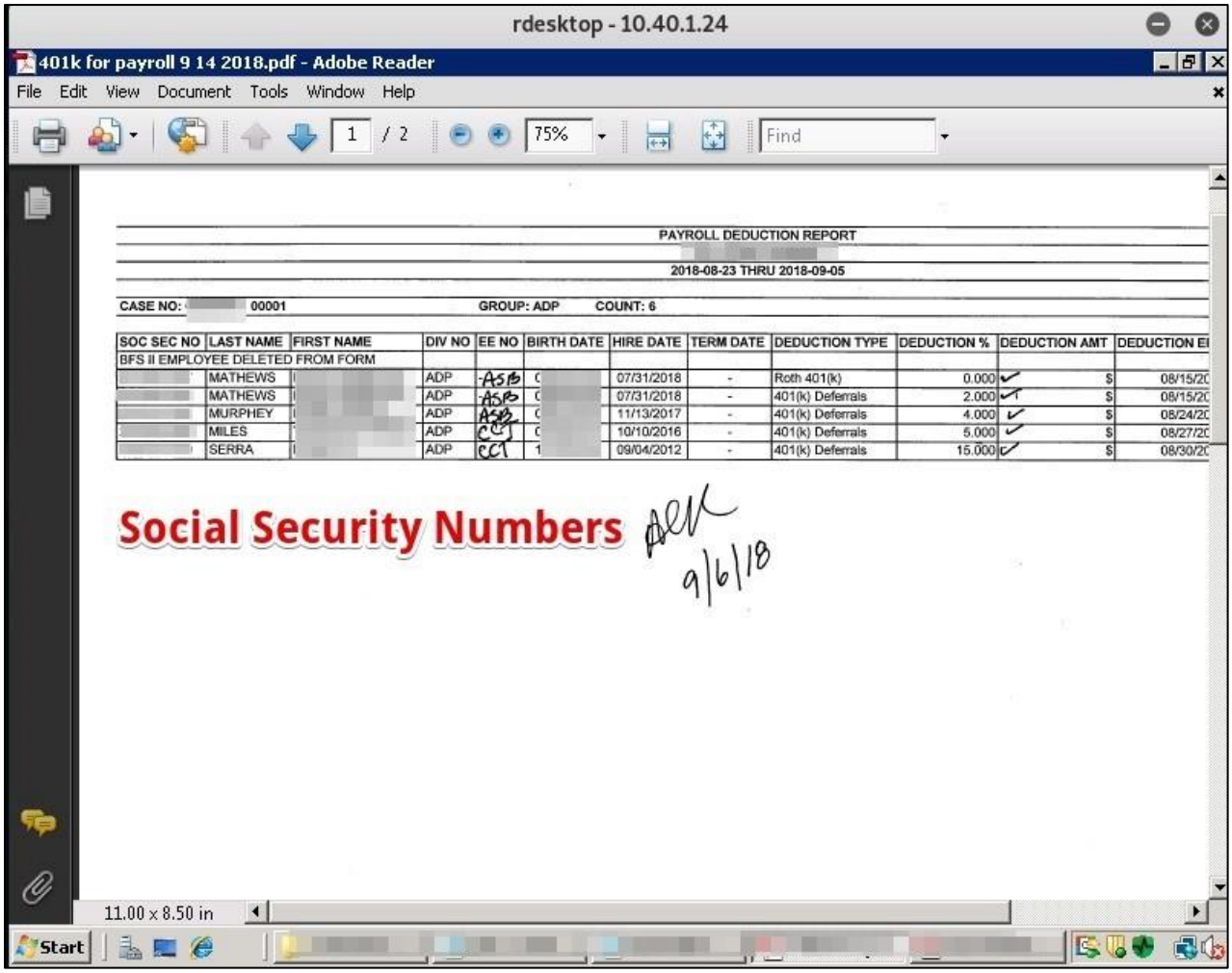


Figure 7: Document with SSNs Inside

Figure 8 shows a Social Security card:

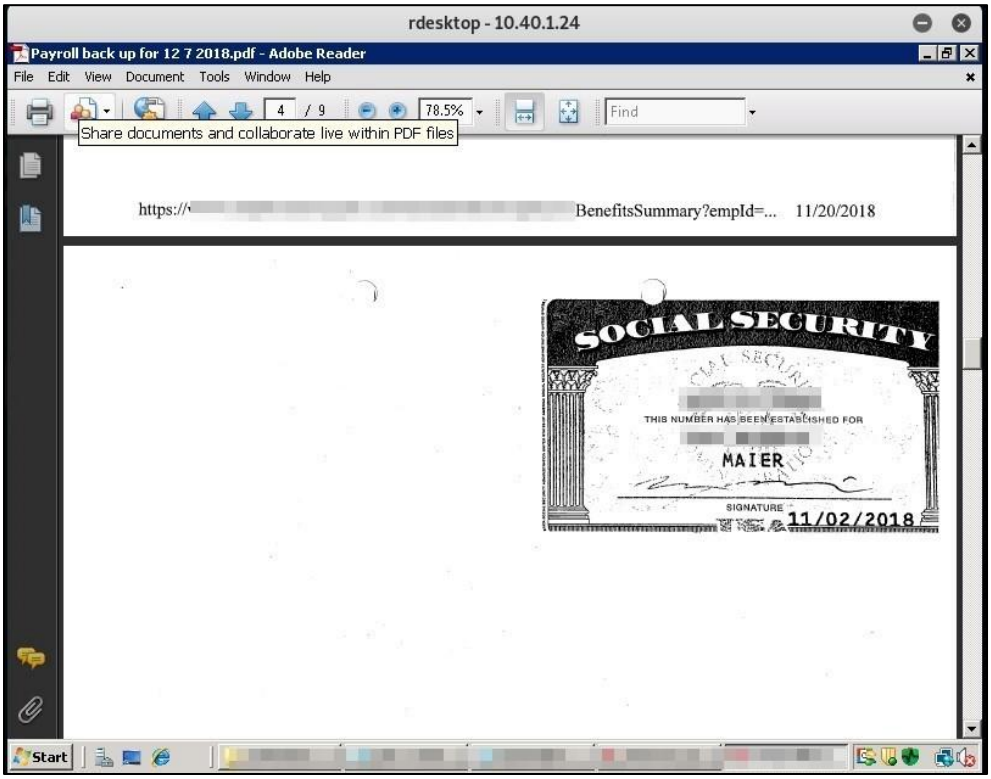


Figure 8: Social Security Card

Figure 9 shows a file with bank account and social security information:

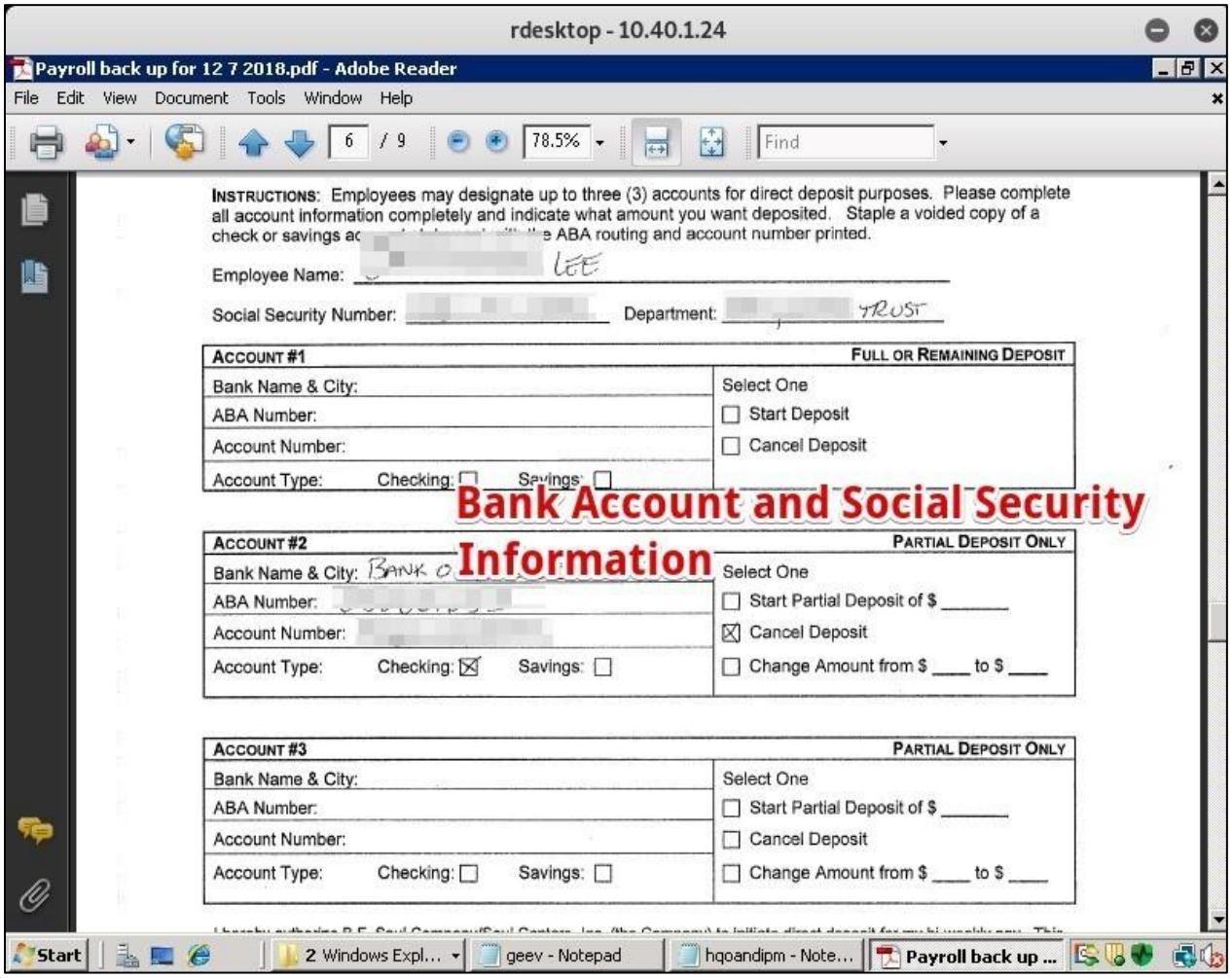


Figure 9: Bank Account and Social Security Information

CRITICAL THREAT ASSESSMENT FINDINGS

IMPLIED TRUST RELATIONSHIP EXPLOITATION

NIST Scoring Summary

Risk	Likelihood	Impact
Critical	High	Critical

CIS Control: Secure Configurations for Hardware and Software

Finding Summary

If two accounts share the same password, this creates an 'implied trust relationship' as any user with access to one can access the other. In most cases, these trust relationships are created unintentionally. Implied trust relationships allow for the possibility of access between domains, domain accounts, local accounts, or even networks for malicious actors.

Implied trust relationship exploitation takes these relationships between systems and abuses that trust. For example, a malicious actor could exploit local system or Active Directory domain trust relationships to expand access across an organization's environment.

If a malicious actor cracks or otherwise obtains a user's password, or if they use a captured password hash in a Pass-the-Hash attack, they can test other accounts and systems within the environment to locate any implied trust relationships.

Validation Steps

Using CrackMapExec, CyberForce|Q passed the Local Administrator hash to all Windows systems, and found that the Local Administrator password was the same, as shown in Figure 10:

```
cme smb -u administrator -d localhost -H [local admin hash] --shares [List of
IPs]
```

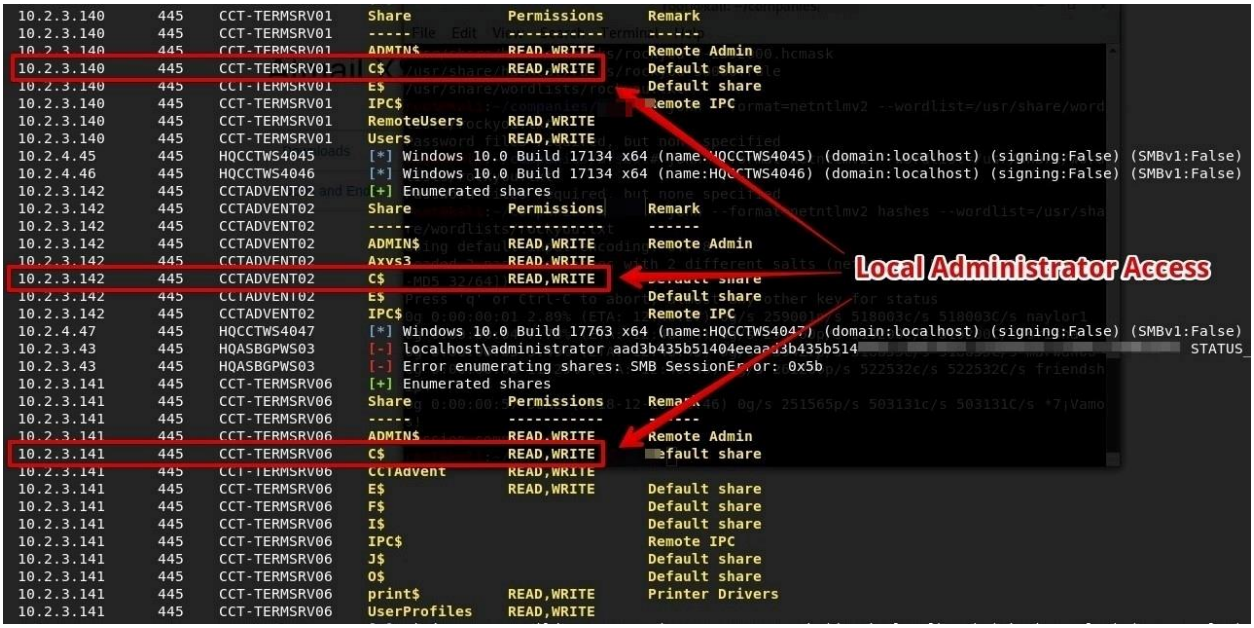


Figure 10: CrackMapExec Output

Affected Resources

- All servers used the same Local Administrator password.
- All workstations used the same Local Administrator password.

Recommendations

Isolate hashes, tokens, and passwords. This makes it harder for malicious actors to move between systems. To do this:

- Use Microsoft's free Local Administrator Password Solutions (LAPS) tool
- Do not allow shared passwords.
- Disable Local Administrative accounts.
- Turn off network access to unnecessary accounts, including RDP.

Minimize the number of hashes, tokens and passwords malicious actors can access. To do this:

- Limit cached credentials.
- Reduce the number of local accounts, especially Administrative ones.
- Limit the number of interactive logons.
- Reboot frequently, if possible.

Limit privilege escalation by protecting privileged account hashes and tokens, especially for Domain Admins. To do this:

- Reduce the number of privileged accounts.
- Provide Administrators with separate non-privileged accounts for normal day-to-day functions.
- Only use privileged accounts on a limited number of more secure and isolated hosts.

Limit lateral movement with:

- Client firewalls, but not Windows firewall set to 'domain' mode.
- Network segmentation.
- Client isolation, using private VLANs.

References

- 'Local Administrator Password Solution', Microsoft, https://technet.microsoft.com/en-us/mt227395.aspx
- 'Local Administrator Password Solution (LAPS)', Microsoft, https://www.microsoft.com/en-us/download/details.aspx?id=46899
- 'Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft', Microsoft, 2014: http://www.microsoft.com/en-us/download/details.aspx?id=36036
- 'Protecting Privileged Domain Accounts: Safeguarding Password Hashes', SANS DFIR, 2012: http://computer-forensics.sans.org/blog/2012/02/21/protecting-privileged-domain-account-safeguarding-password-hashes
- 'Protecting Privileged Domain Accounts: Safeguarding Access Tokens', SANS DFIR, 2012: http://computer-forensics.sans.org/blog/2012/03/21/protecting-privileged-domain-accounts-access-tokens
- 'Windows Credentials Editor (WCE) F.A.Q.', Amplia Security, 2016: http://www.ampliasecurity.com/research/wcefaq.html
- 'Mimikatz', Gentil Kiwi: http://blog.gentilkiwi.com/mimikatz

INSECURE PASSWORD STORAGE IN GROUP POLICY

NIST Scoring Summary

Risk	Likelihood	Impact
Critical	High	Critical

CIS Control: Secure Configurations for Hardware and Software

Finding Summary

Windows Group Policy Preferences (GPP) allows Administrators a greater level of flexibility and can help ease the burden of mass configuration changes. GPP allow for editing of configuration options, up to and including creating user accounts and setting/changing passwords. This feature allows Administrators to deploy and manage applications on client computers, add a Local Administrator account with a set password, map network drives, and add printers.

When adding a new user account or editing a current account, the password that is set is encrypted using a 32-byte AES key. When GPPs are used to set a password, the information is stored on the SYSVOL of the Domain Controller, in a file called 'groups.xml'.

However, Microsoft has since published this AES key in MSDN, which now allows anyone with authenticated access to the network, the ability to capture the Groups.xml file (as it is stored in the SYSVOL, any authenticated user can access it), and decrypt the 'cpassword' value to obtain the plaintext password to access the account that was created or altered via the GPP.

While the Microsoft bulletin MS14-025 was issued to mitigate this vulnerability, it does not remove any already created GPPs. This is due to several reasons, one of which being already existing Group Policy Objects (GPOs) may rely on passwords set in a GPP. Therefore, the mitigation if MS14-025 is already deployed, would be to ensure no GPOs rely on the offending GPP, then fully remove the GPP.

This GPP is commonly used to set Administrative level users, therefore the groups.xml file often contains Local Administrator credentials, which a malicious user could leverage to gain Local Administrative access over workstations and servers.

Validation Steps

Using the Metasploit framework GPP module, CyberForce|Q found a 'groups.xml' file that contained the 'cpassword' encrypted password for the Local Administrator, which CyberForce|Q then decrypted with the Metasploit GPP module, as shown in Figure 11:

```
msfconsole
use scanner/smb/smb_enum_gpp
```

```
set RHOST 10.40.1.24
set SMBUSER administrator
set SMBDOMAIN localhost
set SMBPASS [local admin password]
run
```

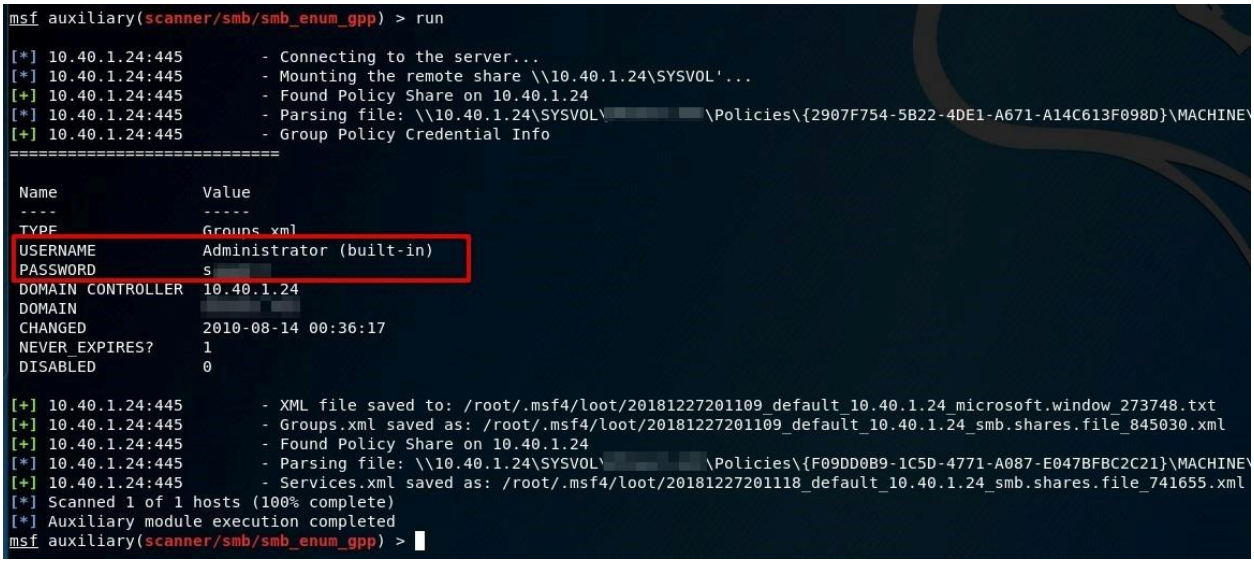


Figure 11: GPP Module Finding the Local Administrator Password

Affected Resources

- All Domain Controllers were affected.
- \\[DC IP]\SYSVOL\[private]\Policies\{2907F754-5B22-4DE1-A671-A14C613F098D}\MACHINE\Preferences\Groups\Groups.xml

Recommendations

Do not use Group Policy to store and/or configure Local Administrator or other passwords across the Windows domain. Ensure that Microsoft Windows patch MS14-025 is installed on all Domain Controllers. This patch will remove the capability to store encrypted passwords in Group Policy Preference.xml file groups.

However, this does not apply to any GPP files already on the network. Any existing passwords stored in Group Policy must be removed. Use Metasploit's 'smb_enum_gpp' module, and the script from Microsoft's MS14-025 page, or manually search the SYSVOL for stored credentials.

References

- 'Pentesting in the Real World: Group Policy Pwnage' Artifice Security Blog, 2016: https://community.Artifice

Security.com/community/services/blog/2016/07/27/pentesting-in-the-real-world-group-policy-pwnage

- 'SMB Group Policy Preference Saved Passwords Enumeration', Artifice Security Metasploit: https://www.Artifice Security.com/db/modules/auxiliary/scanner/smb/smb_enum_gpp
- 'MS14-025: Vulnerability in Group Policy Preferences could allow elevation of privilege', Microsoft Support, 2014: http://support.microsoft.com/kb/2962486
- 'Local Administrator Password Solution', Microsoft Technet, 2016: https://technet.microsoft.com/en-us/mt227395.aspx

WEAK DOMAIN PASSWORDS

NIST Scoring Summary

Risk	Likelihood	Impact
Critical	High	Critical

CIS Control: Secure Configurations for Hardware and Software

Finding Summary

A password's strength is a measure of how easy it is to crack or guess. This means that a short password without a complex variety of characters is weak, and so is a password made up of the word 'password', the company name, or the season and year, as in 'Winter2018'.

A malicious actor using a program like hashcat could crack a weak hash in seconds, or minutes. A stronger password can take days, weeks, or longer.

If a malicious actor cracks the password hash for an account with Administrative access on the network, they could leverage that account to gain unauthorized access to critical or sensitive systems, documents, or configurations.

Validation Steps

CyberForce|Q downloaded the 'NTDS.dit' password hash file from the Domain Controller and cracked the hashes using hashcat. Of the 2,467 hashes downloaded, CyberForce|Q cracked 1,889 using common wordlists, as shown in Figure 12:

```
hashcat -m 1000 [hashes] [wordlist]
```

Figure 12: hashcat Cracked Passwords

Using the pipal password analyzer tool, CyberForce|Q performed analysis and found common passwords in use, as shown in Figure 13:

```
Total entries = 1852
Total unique entries = 1153

Top 10 passwords
network1234! = 141 (7.61%)
network123! = 137 (7.4%)
network = 119 (6.43%)
network9862 = 109 (5.89%)
Passw0rd = 69 (3.73%)
Supp0rt = 18 (0.97%)
Cct2010 = 12 (0.65%)
$HEX[526f6d616e73333a3230] = 12 (0.65%)
9I8U7Y6T = 9 (0.49%)
network12345! = 9 (0.49%)

Top 10 base words
network = 599 (32.34%)
passw0rd = 74 (4.0%)
supp0rt = 22 (1.19%)
hayadams = 13 (0.7%)
hex[526f6d616e73333a = 12 (0.65%)
holiday = 11 (0.59%)
i8u7y6t = 10 (0.54%)
winter = 8 (0.43%)
december = 7 (0.38%)
welcome = 7 (0.38%)
```

Figure 13: Password Analysis Results

Affected Resources

- 1,889 of 2,467 Passwords Cracked Due to Weak Passwords.

Recommendations

CyberForce|Q recommends several strategies to mitigate the risk of users creating and using weak passwords:

First, identify all privileged accounts, including users in the 'Domain Admin' group of Active Directory, and any local accounts configured with Local Administrator privileges on critical systems. These accounts create the highest risk if compromised. Create a separate password policy for these accounts and configure them with the strongest passwords possible.

Second, consider implementing an Active Directory password-auditing add-on to create a blacklist of words that users cannot include in their passwords. The blacklist should include commonly used words, such as the company name, seasons and months, and the word 'password'.

Third, consider increasing the password requirements within Active Directory to require longer and more complex passwords. A stronger password policy typically:

1. Does not allow significant portions of the user's account name, company name or full name.
2. Requires at least 12-character lengths. Administrator accounts should be at least 16 characters, and service accounts should be at least 20 characters long.
3. Contains characters from at least three of the following categories:
    a. Uppercase characters (A through Z)
    b. Lowercase characters (a through z)
    c. Base-10 digits (0 through 9)
    d. Special characters (for example, &, $, #, %)

Even with Windows password complexity and length requirements, users can set passwords in common, easily guessable formats. When training users to create passwords, CyberForce|Q recommends encouraging them to think in terms of 'passphrases' and not passwords. The user can create a strong password from an easy-to-remember sentence, and then substitute numbers and symbols for letters or words. For example, the sentence, 'To be or not to be, that is the question' could be changed to '2bORnot2bth@sthe?', resulting in a long, complex password.

When resetting passwords or creating passwords for new accounts, IT should also avoid using consistent or simple password formats, as users may leave accounts configured with those passwords, or follow that format as an example.

References

- 'Password must meet complexity requirements', Microsoft Technet, 2012: https://technet.microsoft.com/en-us/library/hh994562(v=ws.10).aspx
- 'Password Tips from a Pen Tester: 3 Passwords to Eliminate', Artifice Security Blog: https://blog.Artifice Security.com/2018/05/10/password-tips-from-a-pen-tester-3-passwords-to-eliminate/
- 'Forget Passwords, Use Passphrases for Extra Security', PC Magazine, 2013: http://www.pcmag.com/article2/0,2817,2419274,00.asp
- 'How Do I Create a Strong Password?', Webroot: https://www.webroot.com/us/en/home/resources/tips/getting-started/beginners-how-do-i-create-a-strong-password

HIGH THREAT ASSESSMENT FINDINGS

OBSOLETE OPERATING SYSTEM VERSION IN USE

NIST Scoring Summary

Risk	Likelihood	Impact
High	High	High

CIS Control: Continuous Vulnerability Assessment and Remediation

Finding Summary

Obsolete Operating System versions pose a significant threat to an organization when not replaced with current patched solutions. The Operating System is no longer supported by the vendor, meaning that the vendor has moved all resources onto a new project and will not patch any security vulnerabilities. This Operating System will no longer receive patches or updates.

Any security vulnerabilities discovered after an obsolete Operating System becomes unsupported will not be fixed. A malicious actor could exploit those vulnerabilities at any time.

Validation Steps

CyberForce|Q used RDP to confirm that obsolete Operating Systems were in use, as shown in Figure 14 and Figure 15:

```
mstsc 10.10.10.129
```

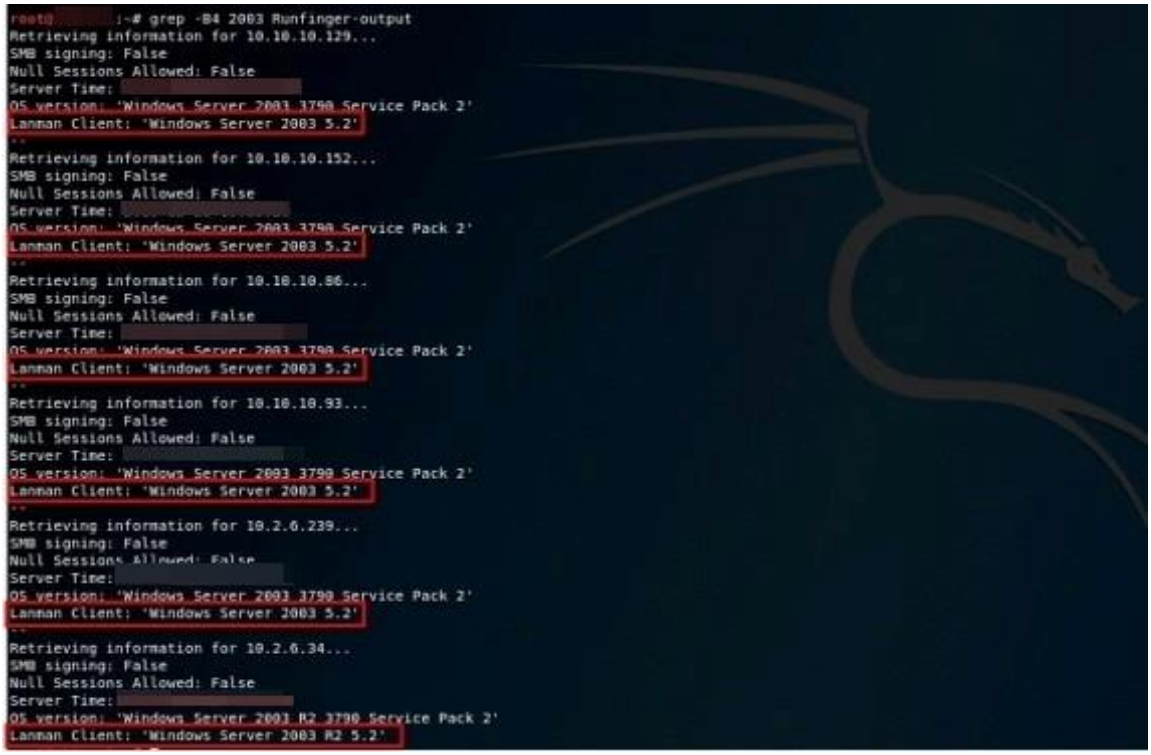


Figure 14: Runfinger Finding Windows Server 2003 Servers

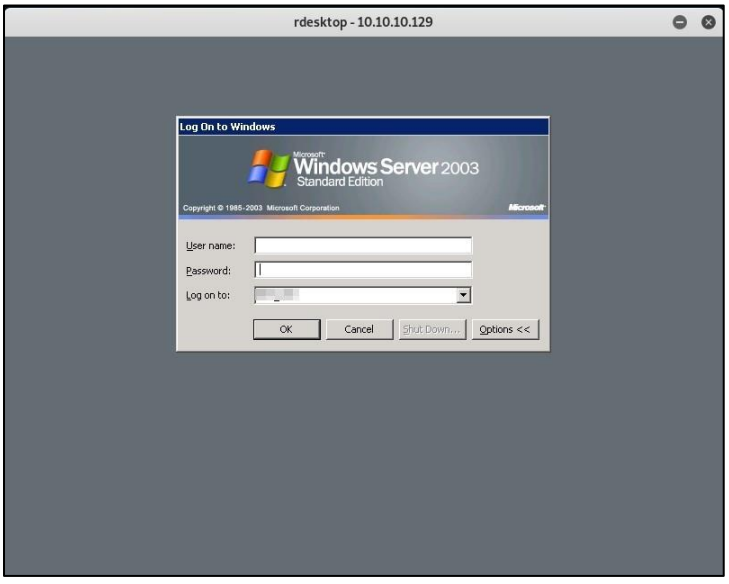


Figure 15: Windows Server 2003

Affected Resources

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		

Recommendations

Upgrade all obsolete Operating System versions to the current patched version.

If this is not possible, CyberForce|Q recommends isolating unsupported systems and systems with known vulnerabilities from the rest of the network by disabling unnecessary services, restricting network traffic using firewalls and access control lists, and by ensuring that credentials are not reused with other systems on the network.

References

- 'The Risks of Running Obsolete Software, Part 1', TechGenix http://techgenix.com/risk-running-obsolete-software-part1/
- 'Obsolete Operating Systems', Red Circle Blog: https://redcircle.blog/2007/11/10/obsolete-operating-systems/

SMB MESSAGE SIGNING NOT REQUIRED

NIST Scoring Summary

Risk	Likelihood	Impact
High	High	High

CIS Control: Secure Configurations for Hardware and Software

Finding Summary

Server Message Block (SMB) is a widely used protocol for sharing access to files, printers, ports, and other system resources. SMB message signing allows a system receiving SMB packets to confirm their authenticity. This is done by digitally signing the communications between the hosts. SMB signing can be configured in one of three ways:

- Disabled entirely (least secure)
- Enabled (but not required)
- Required (most secure)

SMB signing can prevent Man-in-the-Middle attacks against the SMB protocol. When disabled, a malicious actor can send SMB packets that appear to come from valid users. If this user is an Administrative user or in an Administrative group, the malicious actor could even gain a connection to the targeted host as the valid user.

Validation Steps

CyberForce|Q used Runfinger.py, which is part of the Responder tool, to verify SMB signing, as shown in Figure 16:

```
Runfinger.py -i [IP Address]
```

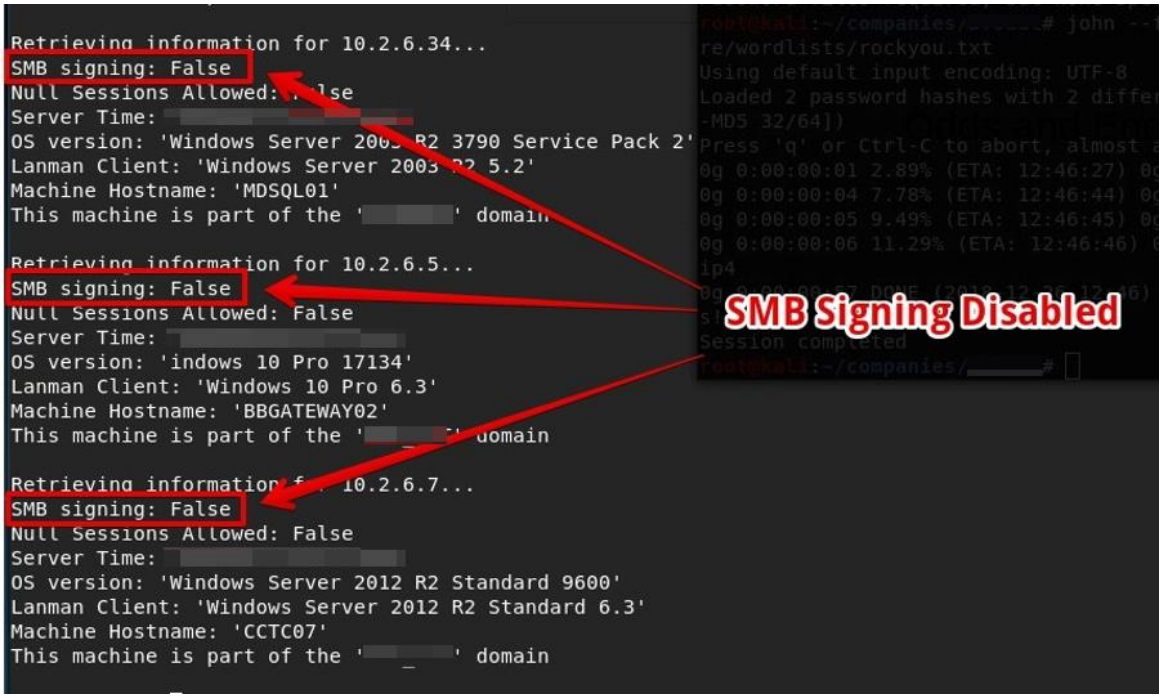


Figure 16: SMB Signing Disabled

Using Responder and ntlmrelayx.py, CyberForce|Q could relay NetNTLMv2 hashes to other systems to gain Local Administrator access, as shown in Figure 17:

Figure 17: ntlmrelayx.py Relaying Hashes to Gain Local Administrator Access

Affected Resources

See Appendix B: Systems with SMB Signing Disabled for a list of affected resources.

Recommendations

Configure your network to require SMB signing. If this is not possible, SMB signing should be enabled.

Microsoft Windows:

Configure the Windows system to enable or require SMB signing as appropriate. The steps required for this are system specific. Consult your vendor instructions or the References section for more information.

Note: Ensure that SMB signing is configured for incoming connections to the server.

Samba:

Configure Samba to enable or require SMB signing, as appropriate. To enable or require SMB signing, open the Samba configuration file, typically 'smb.conf', in the global section, and add the code:

- Enabled: server signing = auto
- Required: server signing = mandatory

For other network configurations, consult the vendor documentation.

References

- 'The Basics of SMB Signing', Microsoft Technet, 2010: http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx
- 'Overview of Server Message Block signing', Microsoft KB, 2017: http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429

WEAK PASSWORD POLICY

NIST Scoring Summary

Risk	Likelihood	Impact
High	Moderate	Critical

CIS Control: Secure Configurations for Hardware and Software

Finding Summary

Password policies regulate requirements, such as minimum length, complexity, threshold, and lockout. A good password policy can prevent malicious actors from gaining unauthorized access through guessing or brute-force attacks. Password strength refers to how easy it would be to crack or guess the password. This means that a short password without a complex variety of characters or variations of common words, such as password, season, or company name, are considered weak.

A malicious actor could attempt to gain access to an authorized user's account by making password guesses, such as season and year combinations, 'service_name1', 'password123', or 'monkey12345'. Alternately, if a malicious actor captured a password hash, they could use a password cracking program, such as hashcat, to attempt to recover the hashed value of the user's password. A weak password could crack in a matter of seconds, or minutes, while a stronger password could take days, weeks, or longer.

If a malicious actor cracks the password hash to an account with Administrative-level access on the network, they could leverage that account to gain unauthorized access to critical or sensitive systems, documents, or configurations.

Validation Steps

CyberForce|Q enumerated the password policy, and found that the password length was only seven characters long, as shown in

Figure 18:

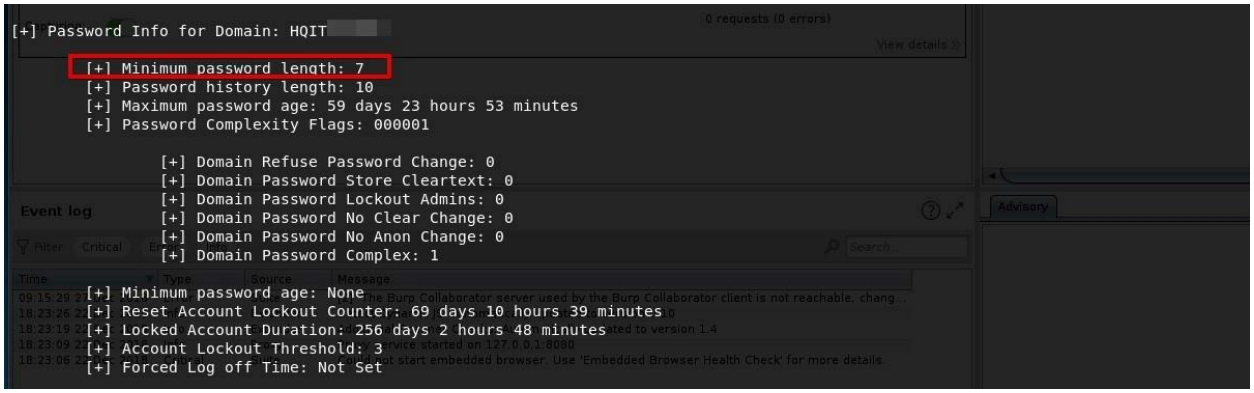


Figure 18: Default Domain Password Policy

Affected Resources

- Default Domain Group Policy

Recommendations

Increase the password policy to require longer and more complex passwords. A stronger password policy typically:

1. Does not allow significant portions of the user's account name, company name or full name
2. Requires at least 12-character lengths. Administrator accounts should be at least 16 characters, and service accounts should be at least 20 characters long.
3. Contains characters from at least three of the following four categories:
    a. Uppercase characters (A through Z)
    b. Lowercase characters (a through z)
    c. Base-10 digits (0 through 9)
    d. Special characters (for example, &, $, #, %)

Even with complexity and length requirements users can still set passwords with common, easily-guessable formats. CyberForce|Q recommends encouraging them to think in terms of 'passphrases' and not passwords. The user can create a strong password from an easy-to-remember sentence. Some examples are:

- CaptainAmerica!My#1Hero
- TheHulk,AWasteOfMuscle?
- SupergirlCouldWhoopSuperman.1

References

- ‘Password must meet complexity requirements’, Microsoft TechNet, 2012: https://technet.microsoft.com/en-us/library/hh994562(v=ws.10).aspx
- ‘Forget Passwords, Use Passphrases for Extra Security’, PC Magazine, 2013: http://www.pcmag.com/article2/0,2817,2419274,00.asp
- 'Password Tips from a Pen Tester: 3 Passwords to Eliminate', Artifice Security Blog: https://blog.Artifice Security.com/2018/05/10/password-tips-from-a-pen-tester-3-passwords-to-eliminate/

EXCESSIVE NUMBER OF PRIVILEGED ACCOUNTS

NIST Scoring Summary

Risk	Likelihood	Impact
High	Moderate	Critical

CIS Control: Boundary Defense

Finding Summary

Administrator, or root, accounts and groups have a high level of access that often make them targets for attacks, such as the 'Domain Admins' group. When a malicious actor targets members of privileged groups, the more accounts in that group, the larger that network's attack surface. When these privileged groups have high memberships the security posture of that network is decreased, due to the higher likelihood of privileged account compromise.

For example, a malicious actor could perform a Man-in-the-Middle attack and wait for a Domain Administrator to authenticate to a system, then capture their password hash and relay or crack it. The more Domain Administrative accounts on the network, the higher the chances that a Domain Administrator user will log on during the attack.

Validation Steps

CyberForce|Q enumerated the 'Domain Admins', 'Enterprise Admins', 'Schema Admins', and 'Administrators' groups, and found an excessive number of users. Figure 19 shows the 'Domain Admins' group:

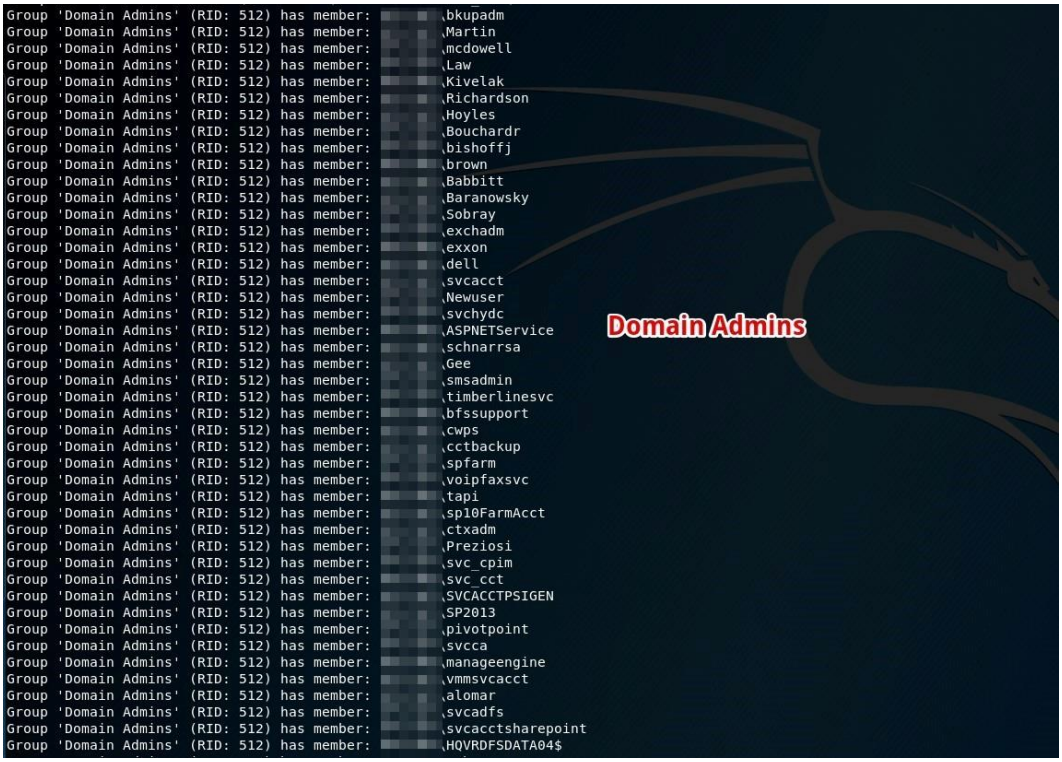


Figure 19: 'Domain Admins' Group

Figure 20 shows the 'Enterprise Admins' group:

Figure 20: 'Enterprise Admins'

Figure 21 shows users in the 'Administrators' group:

Figure 21: 'Administrators' Group Members

Affected Resources

Domain Admins Group
Enterprise Admins Group
Administrators Group

Recommendations

Reduce the number of accounts with Domain Administrator privileges, or other high privilege group, and limit this group as much as possible.

Any account that needs Domain Administrator privileges should be approved by the Chief Information Security Officer (CISO), or someone with a similar level of authority in the organization. The account owner should have a clear and present need for Domain Administrative access.

Review the members of the 'Domain Admin' group at least twice a year and remove accounts unless the privileges are critical for the employee to perform his or her job. Employ the principle of least privilege when deciding what access level each employee needs.

References

- 'Too many admins spoil your security', Infoworld, 2013: http://www.infoworld.com/article/2614271/security/too-many-admins-spoil-your-security.html
- 'How many enterprise admins is too many?', Infoworld, 2010: http://www.infoworld.com/article/2627737/authentication/how-many-enterprise-admins-is-too-many-.html

- 'The Divine Right of Kings: Domain Administrators and your (In)secure Network', SANS, 2001: https://www.sans.org/reading-room/whitepapers/sysadmin/divine-kings-domain-administrators-insecure-network-306

WEAK LOCAL ACCOUNT PASSWORDS

NIST Scoring Summary

Risk	Likelihood	Impact
High	Moderate	Critical

CIS Control: Security Skills Assessment and Appropriate Training to Fill Gaps

Finding Summary

Local accounts on a computer may not have access to other network resources, but a Local Administrative account may have access to information about domain accounts that have accessed that machine. These accounts should be locked down with a strong, hard-to-guess password.

Password strength refers to how easy it would be to crack or guess. This means that a short password without a complex variety of characters is weak, and so is a password made up of the word 'password', the company name, or the season and year, as in 'Winter2019'.

A malicious actor could use a program like Hashcat to attempt to crack a hashed password. A sufficiently weak password may crack in a matter of seconds, or minutes. A stronger password can take days, weeks, or longer. If a malicious actor cracks the password to an account with Administrative-level access on the local system, they could leverage that account to gain unauthorized access to critical or sensitive documents or applications.

Validation Steps

CyberForce|Q cracked the Local Administrator hash, and discovered that the passwords were weak for servers and workstations, as shown in Figure 22:

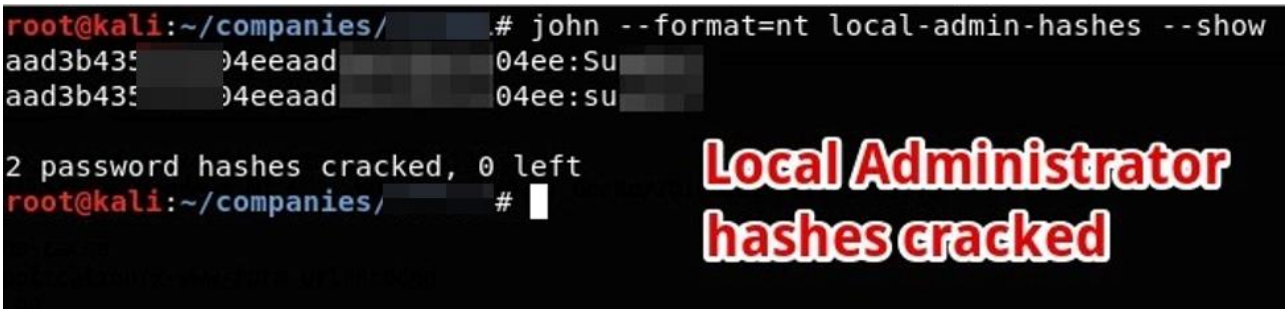


Figure 22: Weak Local Administrator Password

Affected Resources

- All servers and workstations used weak Local Administrator passwords.

Recommendations

Remediating weak passwords on user accounts can be a tedious task. However, CyberForce|Q can recommend several strategies to mitigate the risk of users creating and using weak passwords.

First, identify all privileged accounts, including users in the 'Domain Admin' group of Active Directory, and any local accounts configured with Local Administrator privileges on critical systems. These accounts create the highest risk if compromised. Create a separate password policy for these accounts to ensure they are configured with the strongest passwords possible.

Second, consider implementing an Active Directory password-auditing add-on that will enforce a blacklist of words that users should not include in their passwords. The blacklist should include commonly used words such as the company name, name of seasons and months, and the word 'password'. Blacklisting these words will put a technical control in place to ensure users are not creating passwords with commonly used words.

Third, consider increasing the password requirements within Active directory to require longer and more complex passwords. A stronger password policy typically:

1. Does not allow significant portions of the user's account name, company name or full name
2. Requires at least 12-character lengths. Administrator accounts should be at least 16 characters, and service accounts should be at least 20 characters long.
3. Contains characters from at least three of the following categories:
    a. Uppercase characters (A through Z)
    b. Lowercase characters (a through z)
    c. Base-10 digits (0 through 9)
    d. Special characters (for example, &, $, #, %)

Even with Windows password complexity and length requirements can still allow users to set passwords with common, easily-guessable formats. When training users to come up with passwords, CyberForce|Q recommends encouraging them to think in terms of 'passphrases' and not passwords. The user can create a strong password from an easy-to-remember sentence, and then substitute numbers and symbols for letters or words. For example, the sentence, 'To be or not to be, that is the question' could be changed to '2bORnot2bth@sthe?', resulting in a long, complex password.

When resetting passwords or creating passwords for new accounts, IT should also avoid using of consistent and simple password formats, as accounts could be left configured with those passwords, or users may follow that format as an example.

References

- ‘Password must meet complexity requirements’, Microsoft Technet, 2012: https://technet.microsoft.com/en-us/library/hh994562(v=ws.10).aspx
- 'Password Tips from a Pen Tester: 3 Passwords to Eliminate', Artifice Security Blog: https://blog.Artifice Security.com/2018/05/10/password-tips-from-a-pen-tester-3-passwords-to-eliminate/
- ‘Forget Passwords, Use Passphrases for Extra Security’, PC Magazine, 2013: http://www.pcmag.com/article2/0,2817,2419274,00.asp
- ‘How Do I Create a Strong Password?’, Webroot: https://www.webroot.com/us/en/home/resources/tips/getting-started/beginners-how-do-i-create-a-strong-password

MODERATE THREAT ASSESSMENT FINDINGS

LAN MANAGER HASHES RECOVERED

NIST Scoring Summary

Risk	Likelihood	Impact
Moderate	Moderate	High

CIS Control: Secure Configurations for Hardware and Software

Finding Summary

Before Windows NT, Microsoft LAN Manager and Microsoft Windows used the LAN Manager (LM) password hashing function to store user passwords. When passwords are hashed with the LM hashing algorithm, they are case-insensitive and do not support more than 14 characters. LM hashes separate passwords into two sections after the 7th character. For passwords that are not more than 7 characters, a known hash value represents the blank section. These issues make LM hashes weak against password cracking attempts, such as brute-force and rainbow table attacks.

Microsoft recommends preventing Windows computers from storing an LM hash of any password.

Validation Steps

CyberForce|Q cracked LM hashes from the 'NTDS.dit' Domain Controller hash file, as shown in Figure 23:

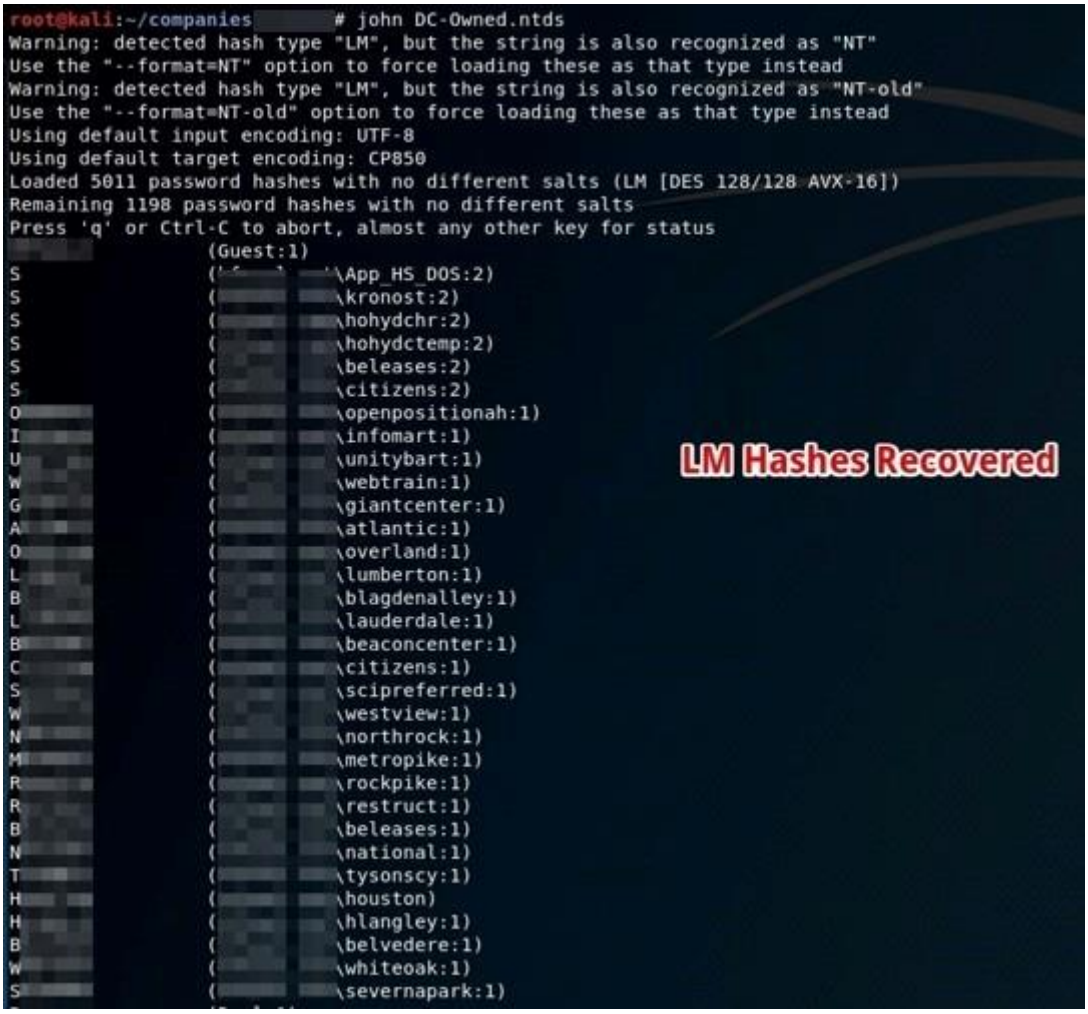


Figure 23: LM Hashes Recovered

Affected Resources

- All Domain Controllers contained LM hashes for the 'NTDS.dit' hash file.

Recommendations

Prevent Windows machines from storing LM Hashes for any password by implementing the NoLMHash Policy, which Administrators can do using Group Policy or by editing the Registry. LM hashes will still be stored for accounts until the user changes their password, which CyberForce|Q recommends forcing users to do after applying the NoLMHash policy.

LM Hashes do not work with passwords that are longer than 15 characters, so implementing a 15-character password policy can also prevent storage of the LM hash.

References

- How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases', Microsoft Support: https://support.microsoft.com/en-us/help/299656/how-to-prevent-windows-from-storing-a-lan-manager-hash-of-your-password

UNDETECTED CHANGES TO THE DOMAIN ADMINS GROUP

NIST Scoring Summary

Risk	Likelihood	Impact
Moderate	Moderate	High

CIS Control: Account Monitoring and Control

Finding Summary

Membership in a network group like 'Domain Admins' should be tightly controlled, and only granted to users with a business need for the level of access that a Domain Administrator or equivalent account can provide. If a new Domain Admin is created, the Network Administrators should know about it.

A malicious actor could create a privileged account or grant special privileges to a regular user's account without anyone noticing. If an unwanted or unauthorized change goes undetected for days or months, the malicious actor may have joined a privileged group, accessed sensitive data, and then unjoined the group without triggering any alerts.

Validation Steps

On the second day of the assessment, CyberForce|Q gained Domain Administrator privileges, and created a new Domain Administrator account on the Domain Controller. In the description section of the account, CyberForce|Q created a 'Did you catch this new account? Email me if so…' message, as shown in Figure 24:

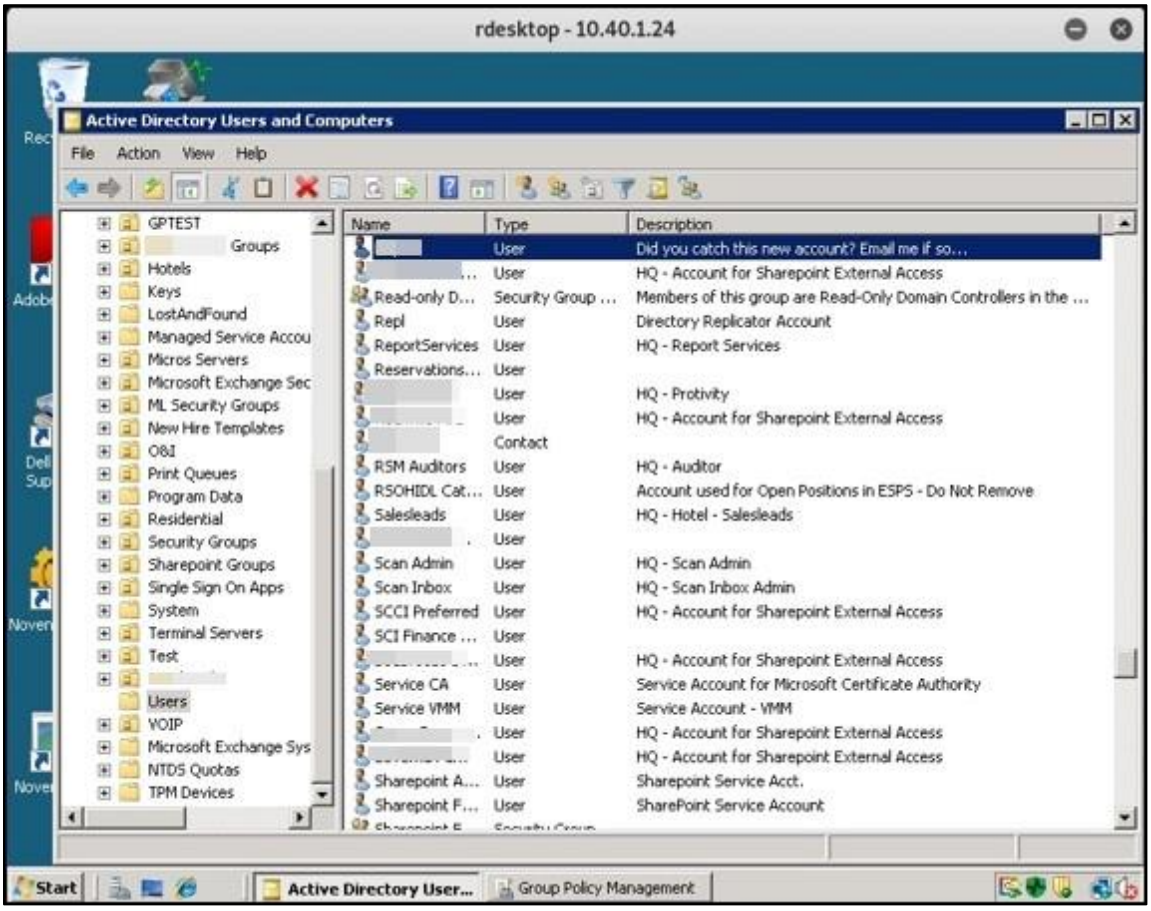


Figure 24: New CyberForce|Q Domain Administrator Account

Note: CyberForce|Q did not receive a response from [Customer Name] by the end of the assessment.

Affected Resources

- CyberForce|Q Account on the Domain Controller

Recommendations

Log and notify IT Administrators of all changes to the 'Domain Admins' group, and any other high-privileged group within Active Directory.

References

- 'How To Configure SCOM To Monitor for Changes To The Domain Admins Group', Microsoft TechNet Blog: http://blogs.technet.com/b/klince/archive/2011/05/18/how-to-configure-scom-to-monitor-for-changes-to-the-domain-admins-group.aspx'

LOW THREAT ASSESSMENT FINDINGS

INSECURE SERVICES IN USE

NIST Scoring Summary

Risk	Likelihood	Impact
Low	Low	Moderate

CIS Control: Continuous Vulnerability Assessment and Remediation

Finding Summary

Insecure services, such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Network Management Protocol (SNMP) transmit user credentials and other sensitive information in cleartext.

A malicious actor intercepting, or 'sniffing' network traffic can capture this unencrypted data transmitted with these services.

Validation Steps

CyberForce|Q found insecure services in use, such as FTP services. Using the tshark tool, CyberForce|Q captured FTP credentials to an FTP system, as shown in Figure 25:

```
root@[redacted]:~# tshark -i eth0 -f "tcp port 21"
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
 /usr/share/wireshark/init.lua:32: dofile has been disabled due to running Wireshark as superuser. See https://wiki.wireshark.org/CaptureSetup/CapturePrivile
eged user.
Capturing on 'eth0'
    1 0.000000000    10.1.5.91 → 10.10.10.102 TCP 74 56082 → 21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=12056113 TSecr=0 WS=128
    2 0.001109105 10.10.10.102 → 10.1.5.91    TCP 74 21 → 56082 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 WS=1 TSval=0 TSecr=12056113
    3 0.001220705    10.1.5.91 → 10.10.10.102 TCP 66 56082 → 21 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=12056114 TSecr=0
    4 0.006791728 10.10.10.102 → 10.1.5.91    FTP 113 Response: 220 RICOH Pro 8110S FTP server (12.75) ready.
    5 0.006870228    10.1.5.91 → 10.10.10.102 TCP 66 56082 → 21 [ACK] Seq=1 Ack=48 Win=29312 Len=0 TSval=12056120 TSecr=1
    6 2.149300451    10.1.5.91 → 10.10.10.102 FTP 78 Request: USER admin
    7 2.149615052 10.10.10.102 → 10.1.5.91    TCP 66 21 → 56082 [ACK] Seq=48 Ack=13 Win=33568 Len=0 TSval=5 TSecr=12058262
    8 2.149749053 10.10.10.102 → 10.1.5.91    FTP 100 Response: 331 Password required for admin.
    9 2.149773153    10.1.5.91 → 10.10.10.102 TCP 66 56082 → 21 [ACK] Seq=13 Ack=82 Win=29312 Len=0 TSval=12058262 TSecr=5
   10 5.156806697    10.1.5.91 → 10.10.10.102 FTP 84 Request: PASS Password123
   11 5.157311599 10.10.10.102 → 10.1.5.91    TCP 66 21 → 56082 [ACK] Seq=82 Ack=31 Win=33562 Len=0 TSval=11 TSecr=12061270
   12 7.516132503    10.1.5.91 → 10.10.10.102 TCP 66 56082 → 21 [FIN, ACK] Seq=31 Ack=82 Win=29312 Len=0 TSval=12063629 TSecr=11
   13 7.516498705 10.10.10.102 → 10.1.5.91    TCP 66 21 → 56082 [ACK] Seq=82 Ack=32 Win=33580 Len=0 TSval=16 TSecr=12063629
   14 10.645287345 10.10.10.102 → 10.1.5.91    FTP 93 Response: 230 User admin logged in.
   15 10.645332245    10.1.5.91 → 10.10.10.102 TCP 54 56082 → 21 [RST] Seq=32 Win=0 Len=0
   16 10.645725546 10.10.10.102 → 10.1.5.91    FTP 103 Response: 221 You could at least say goodbye.
   17 10.645755947    10.1.5.91 → 10.10.10.102 TCP 54 56082 → 21 [RST] Seq=32 Win=0 Len=0
```

Figure 25: FTP Username and Password Captured

Affected Resources

See Appendix C: Insecure Services for a list of affected resources.

Recommendations

Implement a plan to remove all insecure services and replace them with secure alternatives. Use HTTPS instead of HTTP whenever passing sensitive information. Replace

FTP with SFTP, and Telnet with SSH. If using SNMP, ensure SNMPv3 is used to enable encryption. Use authentication with SNMPv3 to ensure data is not modified in transit.

If it is not possible to replace an insecure service, isolate systems required to use the service.

References

- 'Are You Still Using Insecure Network Protocols?' Auvik, 2015: https://www.auvik.com/media/blog/insecure-network-protocols/

APPENDIX A: ASSESSMENT SCOPE OVERVIEW

RULES OF ENGAGEMENT AND ASSUMPTIONS

- No Denial of Service (DoS) attacks.

ACCOUNTS

- No accounts were provided.

SCOPE TARGETS

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

APPENDIX B: SYSTEMS WITH SMB SIGNING DISABLED

IP Addresses with SMB Signing Disabled

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			

APPENDIX C: INSECURE SERVICES

FTP Service

[redacted]			

Telnet Service

[redacted]			

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.

Eric S. Eder, President/Manager
CyberForce|Q LLC
47911 Halyard Rd, Suite 110
Plymouth, MI 48170
Phone: 248.837.1400 Fax: 248.837.1401
Email: eric@cyberforceq.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; 4at this bid or offer is in all respects fair and **wi4out** 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 $ SA-3-62. which automatically voids certain contract clauses that violate State law, and that pursuant to WV. Code SA-3-63. the entity entering into this contract is prohibited from engaging in a boycott against Israel.

CyberForce|Q LLC
(Company)

Eric S. Eder
(Signature of Authorized Representative)

Eric S. Eder, President/Manager
(Printed Name and Title of Authorized Representative)

March 26, 2024
(Date)

248.837.1400 248.837.1401
(Phone Number) (Fax Number)

eric@cyberforceq.com
(Email Address)

ADDENDUM ACKNOWLEDGEMENT FORM

SOLICITATION NO. LOT24-05

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

☒ *Addendum No. 1*

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

CyberForce|Q LLC
Company

Eric S. Eder
Authorized Signature

03/26/2024
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document proc