



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

Header 1

[List View](#)

General Information

Contact

Default Values

Discount

Document Information

Clarification Request

Procurement Folder: 1369290

Procurement Type: Central Master Agreement

Vendor ID: VS0000045522

Legal Name: CyVantage LLC

Alias/DBA: CyVantage

Total Bid: \$110,430.00

Response Date: 03/28/2024

Response Time: 13:27

Responded By User ID: CyVantage

First Name: Sheri

Last Name: Donahue

Email: sdonahue@cyvantage.cor

Phone: 5026493102

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: 1

Total of All Attachments: 1



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 ESR03282400000005562	1

VENDOR
VS0000045522
CyVantage LLC

Solicitation Number: CRFQ 0705 LOT2400000009
Total Bid: 110430
Response Date: 2024-03-28
Response Time: 13:27:42
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				33129.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Website Penetration Testing				11043.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Internal/Client-Side Network Penetration Testing				49693.50

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Wireless Penetration Testing				16564.50

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

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

1 COMPANY OVERVIEW

CyVantage LLC specializes in the design of cyber resiliency programs. Rooted in Department of Defense methodologies, the programs are for experienced cyber aggressors and defenders operating under real-time, complex, and highly stressful environments. We currently work with government and commercial clients to improve and maintain the operational readiness of tactical response capabilities for a wide spectrum of enterprises.

Our team of cyber security experts leverages expertise from close association with the Department of Defense, the Department of Homeland Security, and the Intelligence Community. In addition to a strong partner network of cyber experts from across a wide range of industries, our personnel are capable of supporting a variety of multifaceted problem sets, from simple intrusions to state sponsored Advanced Persistent Threats (APT).

The CyVantage cadre and our strong partner network of additional subject matter experts, from across a wide range of industries, have been on the forefront of many key activities, including:

- Cyber defense assessments to assess an organization's cyber defense program—people, processes, and technology-and its ability to defend against and respond to advanced adversaries
- Exercise development from small-scale tabletops for CEOs and flag-level officers, to technical drills for attackers and defenders, to large-scale national exercises, to challenges on all aspects of national power
- Training on cyber warfare, intelligence support to cyber warfare, exercise planning, contingency planning, top-level domain operations, Computer Incident Response Team & Fusion Center Operations, Cyber-Red Teaming, intrusion monitoring, enterprise cyber defense, insider detection, and detecting advanced persistent threats
- Incident response and developing Concepts of Operation against advanced cyber threats
- Strategic consulting and policy development, using our experience at the highest levels of government and private-public sector partnerships to help organizations define their cyber security postures
- Business Resiliency and Mission Assurance to guide enterprises in performing risk assessments and developing contingency plans focusing on their most critical operations and information assets.

CyVantage is a successor company to Delta Risk LLC founded by Robert Schmidt in 2003.

In 2015 Delta Risk was purchased by Diamond Holdings in a private equity deal led by Sec. Michael Chertoff (DHS Ret.) and Gen. Michael Hayden (NSA, CIA, Air Force, Ret.) and was subsequently sold to Motorola Solutions.

2 PRIOR PROJECTS

The following examples highlight the CyVantage and Delta Risk past performance and experience that CyVantage utilizes for its clients. The personnel responsible for these efforts are now under the CyVantage umbrella and are simply referred to collectively as “CyVantage”.

Demonstrated expertise conducting technical security assessments. CyVantage currently performs cybersecurity assessments of commercial networks, information systems, and key cybersecurity processes. These assessments include social engineering activities, physical security assessments, wireless security audits, and configuration reviews of critical security appliances including firewalls and perimeter routers. We have conducted specialized risk assessments focusing on identification and mitigation of advanced persistent cyber threats for two large, multinational companies: a large mining company, and an international banking and finance company. We oversaw the successful execution of advanced network security assessments of onboard networks in commercial aircraft. We provided technical subject matter experts in advanced wireless penetration testing, general network vulnerability assessment methodologies, and formal test and validation activities. As project leads for the multi-organization teams, we managed the teams’ interactions with the commercial aircraft company and the FAA. Our support included validating threat assessments, identifying appropriate test scenarios, and overseeing execution of a test plan by the penetration test team. Because of these experiences, our team members understand the importance of controls in the operational context within which they are implemented – an insight we will leverage in our development efforts to ensure products that are both innovative and advanced.

James Mulvenon

Chairman of the Board of the Cyber Conflict Studies Association

Scientific Research/Analysis Director Peraton Labs

8401 Colesville Road

Suite 400

Silver Spring, MD 20910

Phone: 703-868-4324

James.mulvenon@peraton.com

Engaged in Feb. 2016 and work ongoing

Summary of Work

The Cyber Conflict Studies Association is a 503(c)1 non-profit entity organized to promote and lead a diversified research and intellectual development agenda to advance knowledge in the cyber conflict field.

CCSA is committed to developing academic programs and communities in the U.S. and abroad. Members of the leadership at CyVantage represent the original plank holders of the association and work continuously to promote the following strategic objectives.

1. Function as the connective tissue for the community studying cyber conflict;
2. Providing a venue for academic dialog and study of economic, policy, and other strategic issues surrounding the threat of cyber conflict;
3. Promoting enhanced discourse on the strategic implications of cyber conflict;
4. Providing cross-functional venues where cyber conflict issues can be discussed among professionals from academia, government, industry, etc.;
5. Serving as a coordinating vehicle through which related organizations (including government organizations) may solicit productive dialog from the cross-functional members of the group;
6. Providing an outlet for the publication of professional articles, position papers, and analysis;
7. Support the framing and promotion of national policy concerning all aspects of cyber conflict;
8. Cooperating with other organizations and institutions involved with other aspects of national security affairs to serve as a resource for them on cyber conflict issues.

Keith Zecchini
Chief Technology Officer
Woolpert Inc.
4454 Idea Center Boulevard
Dayton, OH 45430
Phone: 937.461.5660
Keith.Zecchini@Woolpert.com

Engaged in March of 2020 and ongoing

Summary of Work

CyVantage was engaged by Woolpert Inc. to analyze previous Pen testing and Cyber Security Assessments. After review CyVantage then help formulate a new comprehensive Cyber strategy. Through the discovery process, which included an internal gap assessment, audit, and internal/external pen testing. CyVantage identified weaknesses, overall strengths and updated policies and best practices. CyVantage continues to provide consulting services and acts as a technical resource for Woolpert.

Angela Haun
ONG-ISAC
Executive Director
Houston, TX
703-439-4728
info@ongisac.org

Engaged with January 2019 and ongoing consulting services

ONG-ISAC Mission

ONG-ISAC serves as a central point of coordination and communication to aid in the protection of exploration and production, transportation, refining, and delivery systems of the ONG industry, through the analysis and sharing of trusted and timely cyber threat information, including vulnerability and threat activity specific to ICS and SCADA systems.

1. CyVantage worked with Ms. Haun and the ONG-ISAC to execute an industry wide Cyber Exercise. CyVantage crafted the top-level scenario and assisted during the exercise.
2. The notional attack scenario was designed to highlight several key take-aways:
 - o – An authorized activity such as a maintenance action can result in disruption to energy operations.
 - o – Malware can mask the true operational state of a process under automated control.
 - o – Intelligent field points such as PLCs contain instruction sets sufficient to execute a wide range of malware.
 - o – Insufficient communications between operations centers and business units can hamper the investigation and analysis of seemingly routine outages and other anomalous system behaviors.

3 TEAM MEMBERS

Senior Account Executives

Robert Schmidt

Mr. Schmidt spent the first 15 years of his career as a member of the commodity and options exchanges in Chicago, holding several appointments, including Chairman SPX, Chairman FLEX, Financial Planning, Business Conduct, Arbitration, Floor Officials, and Facilities Task Force committees. In 2003, he was asked by the White House to serve as an SME for the finance sector and 'Red Team' during the White House's Livewire cyber exercise and has since helped large financial institutions and law firms develop strategies which address the risks presented by Advanced Persistent Threat (APT) actors. He is a founding Board Member of the Cyber Conflict Studies Association (CCSA), a guest lecturer for Johns Hopkins Graduate School in Intelligence Analysis, a member of the Atlantic Council, and formerly the President of the InfraGard National Members Alliance (INMA). In 2012, Mr. Schmidt served as a financial services Subject Matter Expert (SME) in support of the FEMA/DHS National Level Exercise – the first Tier 1 national exercise to examine a response to a large-scale cyber-attack against critical infrastructures.

Mr. Schmidt oversees the development of the industry engagement strategy.

Chris Fogle; CISSP

As Principal and a Founding Partner of CyVantage, Chris Fogle has over 25 years of experience in the diverse areas of cyber security, emergency management, and contingency planning and operations. He is a senior subject matter expert in cyber exercises, and a leader in advancing the art of preparing staff and organizations for cyber operations. In the U.S. Air Force, he developed and executed the first BLACK DEMON network defense exercise that included “live network play” using simulated adversary forces and realistic network ranges; and he led the design and development of an exercise for an international Computer Emergency Response Team (CERT) organization to orient over 100 heavy-industries and financial sector companies on operations to counter advanced and persistent threats.

In 2012, he was tapped to lead development of the scenario and gameplay for the Federal Emergency Management Agency’s National Level Exercise which – for the first time ever – focused on a national response to a simulated major cyber incident. In addition to technical scenario elements, he was the architect of the unique “edge scripted” gameplay that enabled the successful integration of disparate objectives across many federal departments and agencies, critical infrastructures, and State government entities.

Mr. Fogle leads operations.

Project Team

See **Appendix B** for Project Team Resumes and Certifications

4 TESTING

4.1 EXTERNAL NETWORK PENETRATION TEST

- 4.1.1** CyVantage will conduct reconnaissance of external effects to determine the location of vendor owned perimeter servers based on open research conducted against the Internet,
- 4.1.2** CyVantage will conduct port and vulnerability scanning to determine any open services or weaknesses that may be exploitable by an external adversary,
- 4.1.3** CyVantage will document and categorize any vulnerabilities found based on data known about the organization (critical infrastructure, business purposes, mission statement, etc.),
- 4.1.4** CyVantage will exploit (in accordance with client/vendor agreements) any weaknesses discovered in attempts to traverse from an external to internal position,
- 4.1.5** CyVantage will catalog all successful efforts and methods of exploitation. Additionally, the agent will document any vulnerabilities found that were not exploited.

SOCIAL ENGINEERING/PHISHING TEST

4.1.6 Our engagements provide detailed analysis of the current state of our clients' situational awareness and cybersecurity annual training through identifying potential phishing vulnerabilities. Phishing, a form of cyber deception, is a tactic that aims to trick individuals into divulging sensitive personal or professional information, which can range from login credentials to financial information or corporate data. Phishing often takes place through seemingly innocuous but manipulative electronic communications, typically emails, masquerading as legitimate messages from trusted sources. This deceptive practice poses a significant threat to individual and corporate data security. If successful, these attacks can lead to unauthorized system access, disruption of business operations, financial loss, and severe reputational damage.

4.1.7 Importance of Phishing Training and Impact - A key reason why phishing poses such an ominous threat is due to its potential to be highly targeted and personalized, often known as spear-phishing, making it extremely difficult to detect. Despite advancements in cybersecurity technology and awareness training, phishing attacks continue to pose serious challenges due to their evolving sophistication and the human factor that is often exploited.

4.1.8 CyVantage Threat Score - The CyVantage Threat Score (CTS) serves as a metric for establishing the current security posture of an organization against social engineering and phishing attacks. The table below illustrates the potential level of resilience an organization can demonstrate when all elements of an engagement (click through rates, campaign development potential, phishing reporting response times and more) are analyzed. The resultant can be found at the top of this report (next to the Executive Summary Title). Please note, these ratings are based on examination of a target user base in a given time and does not guarantee that the same sample base will be as resilient or vulnerable to phishing attacks in the future. As threatscapes evolve so does the human physique.

4.2.3.1 Highly Resilient - Individuals at this level have extensive knowledge and experience in recognizing phishing attempts, including the most sophisticated ones. They consistently apply best practices in cybersecurity, regularly update their security measures, and are proactive in seeking information on the latest threats. They are highly unlikely to fall for phishing attacks, and their resilience can be attributed to continuous learning and diligent application of security measures.

4.2.3.2 Low Risk - These individuals have a strong understanding of phishing threats and regularly engage in safe online behavior. They can recognize most common phishing attempts and use robust security measures. However, they may still fall prey to highly advanced, targeted attacks due to a minor lapse in judgement or cutting-edge techniques employed by

attackers.

4.2.3.3 Mild Risk - Individuals at level 3 are generally aware of the phishing threats and usually employ good cybersecurity practices. However, they might be fooled by highly personalized spear-phishing or whaling attacks. They use security measures like two-factor authentication and strong passwords but may lack advanced security knowledge, like recognizing SSL certificates or using encrypted communication.

4.2.3.4 Moderately Vulnerable - At this level, individuals have a basic understanding of phishing threats but are inconsistent in applying security practices. They may occasionally fall for sophisticated phishing attempts, often due to lapses in judgement, rush, or stress. Their security measures may be in place but are not regularly updated or reviewed.

4.2.3.5 High Risk - Individuals at this level display a fundamental lack of awareness about phishing attacks, often opening unsolicited emails and clicking on unfamiliar links without hesitation. They may freely provide sensitive information and do not utilize, or are unaware of, basic security measures like two-factor authentication or secure password practices.

4.2 WEBSITE PEN TEST

4.2.1 CyVantage will conduct a Website and Application Penetration Assessment against the external facing web application architecture. The intent of an application assessment is to dynamically identify and assess the impact of potential security vulnerabilities within the application. During this assessment, both manual and automated testing tools and techniques will be employed to discover and exploit possible vulnerabilities.

4.2.2 All testing activities will be conducted against the development environment to limit the impact of any service disruptions.

4.2.3 Testing will be conducted from both an unauthenticated and authenticated context. Unauthenticated testing examines the exterior security posture of an application and looks for vulnerabilities that do not require authentication to exploit, while authenticated tests focus on discovering and exploiting vulnerabilities on portions of the internal application that are only accessible after successful authentication. Assessors were provided both a regular user and an administrative user account to assess the internal security controls of the application.

4.3 INTERNAL/CLIENT-SIDE NETWORK PEN TEST

4.3.1 CyVantage will conduct reconnaissance of internal effects to determine the security posture of the organization from the position of having compromised at least one asset within the network,

4.3.2 CyVantage will conduct port and vulnerability scanning to determine any open

services or weaknesses that may be exploitable by an insider or external adversary. NOTE: "Port scanning" may be tweaked depending on the agreed upon terms. For engagements, specifically testing Security Operation Center (SOC) response times and metrics, more manual (less noisy) techniques will be used,

- 4.3.3** CyVantage will document and categorize any vulnerabilities found based on data known about the organization (critical infrastructure, business purposes, mission statement, etc.),
- 4.3.4** CyVantage will exploit (in accordance with client/vendor agreements) any weaknesses discovered in attempts to traverse the network,
- 4.3.5** CyVantage will attempt to access other segments (VLANs, PVLANS, domains, etc.),
- 4.3.6** CyVantage will attempt lateral movement between compromised assets (if successful),
- 4.3.7** CyVantage will catalog all successful efforts and methods of exploitation. Additionally, the agent will document any vulnerabilities found that were not exploited

4.4 WIRELESS PEN TEST

- 4.4.1** CyVantage will perform attacks emulating real world operator methodologies without prior authentication to the scoped wireless networks,
- 4.4.2** During the assessment, multiple attack methods will be used against all access points (APs),
- 4.4.3** CyVantage will test the possible over-transmittal of wireless network signals by measuring signal strength from various locations around the Lottery facilities.

4.5 REPORTING

Executive Summary Reports will be provided to the Lottery upon conclusion of each assessment. Each report will include an overview of all test results, a summary of the scope and approach, findings, key strengths and recommendations for improvement.

CyVantage will conduct a presentation with the Lottery discussing all vulnerabilities found, major areas of concern, remediation strategies, general practices and the overall impact to the organization given this newly discovered information. The presentation will be delivered remotely (via teleconference or web-conference).

CyVantage will securely transmit the preliminary report containing all information regarding the execution of the engagement. This report will include findings, data,

technical analysis of the infrastructure tested, the position from which the engagement was executed and mitigation strategies to bolster the posture of the network by eliminating any weaknesses found.

A sample report is included as **Appendix C**.

5 CONTRACT MANAGER

Contract Manager: Sheri Donahue

Telephone Number: (502) 649-3102

Fax Number: N/A

Email Address: SDonahue@CyVantage.com

**APPENDIX A
Pricing Page**

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	\$4,141.13	\$33,129.00
2	4.2	Website Penetration Testing	8	\$1,380.38	\$11,043.00
3	4.3	Internal/Client-Side Network Penetration Testing	8	\$6,211.69	\$49,693.50
4	4.4	Wireless Penetration Testing	8	\$2,070.57	\$16,564.50
TOTAL BID AMOUNT					\$110,430.00

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:	CyVantage, LLC
Vendor Address:	4899 Montrose Blvd., Suite 1801, Houston, TX 77006
Email Address:	RSchmidt@CyVantage.com
Phone Number:	(312) 203-8307
Fax Number:	N/A
Signature and Date:	Robert Schmidt, 28 March 2024

APPENDIX B

Project Team Resumes and Certifications

TITLE: SENIOR SECURITY ADVISOR

YEARS OF EXPERIENCE: 20+ YEARS

SENIOR CONSULTANT DEVELOPING ADVANCED NETWORK DEFENSE FRAMEWORKS—INTEGRATING NETWORK SECURITY, SURVIVABILITY/RESILIENCY, RISK ASSESSMENT, TACTICS & TRAINING PROGRAMS, AND CYBER EXERCISE DESIGN METHODOLOGIES. TECHNICAL LEADER AND INNOVATOR IN CYBER WARFARE OPERATIONS. MILITARY INFORMATION OPERATIONS EXPERIENCE WITH UNDERSTANDING OF ADVERSARY TACTICS AND THEIR APPLICATION TO DEFENSIVE OPERATIONS. EXPERIENCE WITH NETWORK VULNERABILITY AND OPERATIONS SECURITY ASSESSMENTS, EFFECTIVE RISK REMEDIATION, AND TRAINING CURRICULUM DEVELOPMENT IN OFFENSIVE AND DEFENSIVE NETWORK TACTICS. EXPERIENCE PREPARING PAPERS AND PRESENTATIONS FOR TECHNICAL AND NON-TECHNICAL AUDIENCES.

SKILL SET: CARNEGIE MELLON SEI REGISTERED CYBERSECURITY COMPLIANCE VALIDATION (CCV) PROGRAM TEAM MEMBER. CERTIFIED CHIEF INFORMATION SECURITY OFFICER (C|CISO). CERTIFIED INFORMATION SYSTEM SECURITY PROFESSIONAL (CISSP). CERTIFIED ETHICAL HACKER (C|EH). SECURITY+. NETWORK+. PROJECT+. EXPERT KNOWLEDGE OF CYBER EXERCISING, OFFENSIVE CYBER TACTICS DEVELOPMENT, CONTINUITY PLANNING, BUSINESS RESILIENCY, NETWORK AND SECURITY CENTER OPERATIONS, NETWORKING TECHNOLOGIES AND TOPOLOGIES, SYSTEM ADMINISTRATION, INFORMATION SYSTEMS SECURITY ANALYSIS, PENETRATION TESTING, AND VULNERABILITY TESTING. EXPERT KNOWLEDGE OF AIR FORCE COMPUTER SECURITY AND INFORMATION PROTECTION. ABILITY TO ESTABLISH AND MAINTAIN EFFECTIVE WORKING RELATIONSHIPS WITH A VARIETY OF INDIVIDUALS AND GROUPS, BOTH CONTRACTOR AND GOVERNMENT STAFFS, TECHNICAL AND MANAGERIAL.

DEGREE	INSTITUTION
MS BS	UNIVERSITY OF SOUTHERN CALIFORNIA MAJOR: COMPUTER SCIENCE — ROBOTICS & AUTOMATION, 2000
	ILLINOIS INSTITUTE OF TECHNOLOGY MAJOR: ELECTRICAL ENGINEERING, CUM LAUDE, 1997

TECHNICAL TRAINING/CERTIFICATIONS

- ISC2 CERTIFIED INFORMATION SYSTEM SECURITY PROFESSIONAL (CISSP) - 2011
- EC-COUNCIL, CERTIFIED CHIEF INFORMATION SECURITY OFFICER (C|CISO) - 2013
- EC-COUNCIL, CERTIFIED ETHICAL HACKER (C|EH) (2006)
- COMPTIA PROJECT+ (2010)
- COMPTIA SECURITY+ (2006)
- COMPTIA NETWORK+ (2007)
- MICROSOFT CERTIFIED PROFESSIONAL (1999)
- INFORMATION OPERATIONS FUNDAMENTALS COURSE (2007)
- RED TEAM OPERATOR COURSE, LACKLAND AFB (2004)
- COMPUTER NETWORK OPERATIONS COURSE, LACKLAND AFB (2003)
- ADVANCED COMPUTER NETWORK OPERATIONS COURSE, LACKLAND AFB (2004)

EXPERIENCE

VICE PRESIDENT 9+ YEARS CYBER SECURITY PROFESSIONAL SERVICES COMPANY

Provides adversary perspective and threat knowledge to cybersecurity initiatives. Provides strategic advice and forward looking thought to senior Department of Defense (DoD) executives on cybersecurity issues. Applies DoD methods & lessons learned to improving private and commercial enterprise cyber defenses—resulting increase in National capacity for homeland cyber defense. Consults with US and international clients in government and commercial sectors on cybersecurity matters. Developed enterprise cybersecurity assessment framework promoting objective evaluations with cross-organization comparable metrics. Developed Domain Name System (DNS) threat training for international audience of internet domain registry operators. Organized first-ever DNS Security, Stability, and Resiliency Symposium, to bring

broad spectrum of stakeholders together to discuss DNS risks and brainstorm remediation strategies. Led development of and instructed first-ever DNS registry operator technical security workshop. Led development of the Registry Operations Curriculum, a three-course program totaling 15 days of technical training, merging existing ad-hoc efforts and providing a comprehensive training framework for DNS registry operators. Developed advanced cyber exercise templates that included scripting adversary actions, network diagnostics, incident response, and forensics of exercising organizations. Delivered workshops in-person and through online venues around the world focusing on operational, hands-on cybersecurity training.

CHIEF OF NETWORK WARFARE OPERATIONS 2 YEARS U.S. AIR FORCE WARFARE CENTER

Developed network warfare operations strategy for brand-new unit, building capability from the ground up, and aligning two geographically separated units with dynamic adversary replication mission. Led efforts to create virtual environments for network penetration and target replication for use in Joint, Air Force, and internal exercises and training. Created and instructed new network warfare aggressor training curriculum covering the spectrum of network warfare operations. Executed red cell tasks as network and Information Operations (IO) opposition forces (OPFOR) during TERMINAL FURY and RED FLAG exercises. Instructed Air Force combat forces worldwide in adversary threats, remediation strategies, and offensive and defensive network tactics to include response actions for malware intrusions, data tampering, and unauthorized system entry; secure firewall implementations, inbound/outbound SMTP filtering/relay, e-mail filtering, and VPN use. Directed software development teams in the creation and advancement of computer network exploitation and attack tools. Recognized as Association of Old Crows Defensive Information Warfare Individual of the Year for 2007.

CHIEF OF WEAPONS & TACTICS 4 YEARS AIR FORCE INFORMATION OPERATIONS AGGRESSORS

Directed team of nine active duty, reserve, and civilian personnel in developing information warfare capabilities for use in increasing network defense capacity and secure network and system administration. Led 25+ network vulnerability engagements which included in depth penetration testing and 10+ multi-discipline vulnerability assessments, coordinating execution, scope, timeline and logistics with internal teams, customer and external agencies. Executed red cell tasks as network OPFOR during TERMINAL FURY, BLUE FLAG, BULLWARK DEFENDER and BLACK DEMON exercises. Initiated redesign of software toolset to provide simultaneous assessment of multiple locations, increasing assessment capability 15X. Designed standardized, redundant reach-back network servers between three separate units, providing constant capability in event of a failure at one location. Launched threat representative ability to conceal network assessment actions, ensuring a fair assessment of the entire Air Force network security chain. Developed new vulnerability assessment reporting software, providing standardized, streamlined, visual summary in customer friendly format. Trained and certified incoming team chiefs through academics, hands-on lab work, and on-the-job training.

TITLE: SENIOR SECURITY ENGINEER

YEARS OF EXPERIENCE: 14+ YEARS

SENIOR CONSULTANT DEVELOPING ADVANCED NETWORK DEFENSE FRAMEWORKS—INTEGRATING NETWORK SECURITY, RISK ASSESSMENT, TACTICS & TRAINING PROGRAMS, AND CYBER EXERCISE DESIGN METHODOLOGIES. SUBJECT MATTER EXPERT IN DoD AND USAF CYBER PROTECTION TEAMS, EXERCISES, PENETRATION TESTING, CYBERSECURITY, VIRTUAL RANGES BASED ON CYPHERPATH'S SOFTWARE DEFINED INFRASTRUCTURE (SDI) PLATFORM AND VMWARE'S ESX PLATFORM, PROVIDING INSIGHT TO ENTERPRISES AND GOVERNMENTS ON CYBERSECURITY ISSUES. EXTENSIVE OPERATIONS AND MANAGEMENT EXPERIENCE LEADING WORLD-WIDE DEPLOYED TACTICAL NETWORKS AND ENTERPRISE SYSTEMS SUCH AS THE DoD GLOBAL INFORMATION GRID (GIG). EXTENSIVE TEACHING AND COURSE DEVELOPMENT EXPERIENCE IN THE FIELD OF CYBERSECURITY. PROVEN TEAM LEADER WITH TECHNICAL, OPERATIONAL AND ADMINISTRATIVE LEADERSHIP EXPERIENCE.

SKILL SET: CARNEGIE MELLON SEI REGISTERED CYBERSECURITY COMPLIANCE VALIDATION (CCV) PROGRAM TEAM MEMBER AND LEAD. CERTIFIED NSA RED TEAM OPERATOR AND INSTRUCTOR. EXPERT KNOWLEDGE OF CYBER EXERCISING, OFFENSIVE CYBER TACTICS DEVELOPMENT, NETWORK AND SECURITY CENTER OPERATIONS, NETWORKING TECHNOLOGIES AND TOPOLOGIES, SYSTEM ADMINISTRATION, INFORMATION SYSTEMS SECURITY ANALYSIS, PENETRATION TESTING, AND VULNERABILITY TESTING. EXPERT KNOWLEDGE OF DoD GLOBAL INFORMATION GRID DESIGN, COMPUTER SECURITY AND INFORMATION PROTECTION. ABILITY TO ESTABLISH AND MAINTAIN EFFECTIVE WORKING RELATIONSHIPS WITH A VARIETY OF INDIVIDUALS AND GROUPS, BOTH CONTRACTOR AND GOVERNMENT STAFFS, TECHNICAL AND MANAGERIAL.

DEGREE

INSTITUTION

BS CLARKSON UNIVERSITY

MAJOR: COMPUTER SCIENCE, 2000

EXPERIENCE

DIRECTOR & SENIOR CYBERSECURITY CONSULTANT CYBER SECURITY PROFESSIONAL SERVICES COMPANY

5+ YEARS

TECHNICAL TRAINING/CERTIFICATIONS

- USAF Blue Team operator course, 2012
- USAF CYBERSPACE 300, 2011
- COMPTIA SECURITY+ - 2010
- NSA/CSS RED TEAM BOOT CAMP, 2008

Technical subject matter expert (SME) on DHS FEMA National Level Exercise 2012 (NLE) Scenario Team. Designed and wrote technical scenario to drive simulated cyber-attack on Federal and State Department and Agencies. Designed and taught courses on Windows Penetration Testing, Mobile Device Security, and Incident Response to Federal Department and Agencies as part of the FedCTE program sponsored by the Department of State and the Department of Homeland Security. Designed and taught courses on Certified Information Security Manager (CISM) certification, DMZs, Linux Security, and CompTIA A+ certification as part of SEI's FedVTE program. Created training environment for US-CERT's GFIRST conference. Created threats and vulnerabilities to train participants in detecting and mitigating an adversary. SEI Team Lead and Evaluator for the Department of Homeland Security and Carnegie Mellon's Software Engineering Institute in developing and executing Cybersecurity Capability Validations of Federal Agency's in support of the Office of Management and Budget's (OMB) Trusted Internet Connection initiative. Lead evaluator of applications for ICANN's generic top level domains (gTLDs) initiative. Developed methodology for evaluating National Capitol Region states, counties, and their organizations alignment to NIST's Framework for Improving Critical Infrastructure Cybersecurity and providing recommendations on how to improve their procedures and processes. SME on SEI's STEP platform. In this role, supported SEI by installing, managing, and developing content in support of US Cyber Command's (USCC) CYBER FLAG exercise, Cyber Protection Team exercises, and Marine Forces Cyberspace Command's (MARFORCYBER) exercises.

DOD GIG OPERATIONS MISSION LEAD 2 YEARS USCYBERCOM, NSA

Prioritized Network Operation Missions for the DoD GIG, oversaw fix actions and provided situational awareness to leadership for 7M computers, 15K networks, and 20K telecommunication circuits across the globe directly supporting the war fighter. Standardized and defined USCYBERCOM reporting guidelines for DoD GIG infrastructure to quickly identify critical failures. Created a standardized training plan for the 24/7 Mission Lead position and certified 6 new operators. Ensured active Network Defense of the GIG by working closely with the NSA Threat Operation Center (NTOC) and the Defense Information Systems Agency (DISA) to develop mitigation of cyber advisories and unauthorized network access attempts

RED TEAM SERVICES BRANCH CHIEF 2 YEARS NSA RED TEAM, NSA

Developed and directed training and certification of 100+ NSA Red Team cyber operators supporting the defense of the DoD GIG. Created NSA Red Team Services branch to support the joint certification and accreditation process for all DoD Red Teams. Created and taught NSA Red Team seminar for 300 officers at USAF Advanced Communication Officer School. Helped shape USAF first Cyber 300 course to develop strategic focus for integration and application of cyberspace capabilities.

DEPUTY CHIEF OF SYSTEMS 1 YEAR IRAQ TRAINING & ADVISORY MISSION-INTEL TRANSITION TEAM

Captured requirements and implemented plans to extend Iraqi Intelligence Network throughout ministries and military bases. Directly trained, assisted and led Iraqi technicians in designing and installing 2 separate LANs to support Intel Training School. Advised senior Iraqi officials on developing an advanced network architecture and maintaining strong network security practices.

OPERATIONS TEAM LEAD 2 YEARS NSA RED TEAM

Led Red Team operations against multiple DoD networks and identified vulnerabilities to increase cybersecurity. Certified Red Team operator and analyst; taught UNIX systems and exploitation for NSA Red Team Boot Camp.

EXCHANGE OFFICER / SENIOR NETWORK SYSTEMS ENGINEER, 3 YEARS U.S. AIR FORCE

Technical authority for the Canadian Forces entire Windows 2003 Active Directory domain of 100 servers and 98K workstations. Maintained lab to perform testing for all changes and created implementation guidance for system administrators. Engineered deployable hardware/software solution to extend domain into war zone with slow links and frequent disconnects.

TITLE: SENIOR CYBER SECURITY INFRASTRUCTURE PROFESSIONAL

YEARS OF EXPERIENCE: 13+ YEARS

CONSULTANT DEVELOPING ADVANCED NETWORK DEFENSE FRAMEWORKS—INTEGRATING NETWORK SECURITY, CYBER EXERCISE DESIGN METHODOLOGIES. CYBER RANGE TECHNICIAN, RESPONSIBLE FOR CREATING OPERATIONALLY RELEVANT CYBER ENVIRONMENTS FOR OPERATION, TEST, AND EVALUATION OF AIR FORCE CYBER TOOLS. COMMUNICATIONS INTEGRATOR; SPECIAL DUTIES INCLUDED PROTOTYPING AND EMPLOYING ADVANCED SECURE TECHNOLOGIES FOR THE DoD COMMUNITY. COMMUNICATIONS PROJECT LEAD, PROVIDED DAY-TO-DAY ONSITE COMMUNICATIONS DESIGN AND PROJECT IMPLEMENTATION OVERSIGHT FOR DEPLOYED JOINT TASK FORCE. NETWORK MANAGER, RESPONSIBLE FOR THE 24/7 SUPPORT AND UPKEEP OF MULTIMILLION DOLLAR CRITICAL INFRASTRUCTURE FOR A JOINT DoD ELEMENT. NETWORK ENGINEER, DESIGNING AND EMPLOYING CYBER DEFENSE LAB TO ENHANCE NETWORK DEFENSE CAPABILITIES AGAINST ADVANCED PERSISTENT THREATS. SUBJECT MATTER EXPERT IN DoD AND USAF CYBER PROTECTION TEAMS, EXERCISES, PENETRATION TESTING, CYBERSECURITY, VIRTUAL RANGES BASED ON CYPHERPATH’S SOFTWARE DEFINED INFRASTRUCTURE (SDI) PLATFORM AND VMWARE’S ESX PLATFORM, PROVIDING INSIGHT TO ENTERPRISES AND GOVERNMENTS ON CYBERSECURITY ISSUES.

SKILL SET: CARNEGIE MELLON SEI REGISTERED CYBERSECURITY COMPLIANCE VALIDATION (CCV) PROGRAM TEAM MEMBER. EXPERT KNOWLEDGE OF CYBER EXERCISES, NETWORKING TECHNOLOGIES AND TOPOLOGIES, SYSTEM ADMINISTRATION, AND INFORMATION SYSTEMS SECURITY ANALYSIS. EXPERT KNOWLEDGE OF AIR FORCE COMPUTER SECURITY AND INFORMATION PROTECTION. ABILITY TO ESTABLISH AND MAINTAIN EFFECTIVE WORKING RELATIONSHIPS WITH A VARIETY OF INDIVIDUALS AND GROUPS, BOTH CONTRACTOR AND GOVERNMENT STAFFS, TECHNICAL AND MANAGERIAL.

DEGREE	INSTITUTION
--------	-------------

BS PARK UNIVERSITY
MAJOR: BUSINESS MANAGEMENT, 2010

TECHNICAL TRAINING/CERTIFICATIONS
<ul style="list-style-type: none">• SANS – SEC505 SECURING WINDOWS WITH POWERSHELL AND THE CRITICAL SECURITY CONTROLS – 2015• COMPTIA LINUX+ - 2014• INTRODUCTION TO BREAKINGPOINT – 2011• OPNET: INTRODUCTION TO MODELER - 2010• COMPTIA SECURITY+ - 2010• CISCO SECURING NETWORKS WITH PIX AND ASA - 2007• NSA OPERATIONAL INFORMATION ASSURANCE PRINCIPLES COURSE – 2006

EXPERIENCE

SENIOR CYBERSECURITY CONSULTANT CYBER SECURITY PROFESSIONAL SERVICES COMPANY 5 YEARS

Developed squad level on-demand on-demand exercises for DoD Cyber Protection Teams (CPTs) within SEI’s Stimulation, Training, and Exercise Platform (STEP). Utilized a mixture of enterprise and open source software and SEI collaboration tools to create technical and administrative content based upon squad level standard operating procedures (SOPs) to include training objectives, scenario events, and knowledge assessments. On-demand exercises provided teams with in-depth knowledge on the use, configuration, and application of devices in addition to identifying and managing security risks to protect enclaves. Exercise developer for 40+ on-demand comprehensive scenarios within the STEP used to evaluate operational leadership roles within DISA’s Joint Information Environment (JIE) Enterprise Operations Centers (EOCs). Utilized role based Knowledge, Skills, and Abilities (KSAs) to assess each participant’s ability to react to scripted EOC events simulated in the STEP. In support of the Internet Corporation for Assigned Names and Numbers (ICANN), provided onsite education on cyber threats and network security training to small country code Top-level Domain (TLD) operators. Designed cyber exercise scenarios and provided range development support to an international security center in an effort to enhance the country’s network defense capabilities against advanced persistent threats. Coordinated and advised US DHS on best practices to implement Information Security Continuous Monitoring (ISCM) across 120+ Departments & Agencies in the US Government.

TEST RANGE ENGINEER 2 YEARS CYBER SECURITY ENGINEERING SERVICES COMPANY

Responsible for sustaining the Air Force's Combat Information Transport System (CITS) network defense test ranges. Provided input and test support/data analysis during the drawdown of the Air Force's Automated Security Measurement System (ASIM). Lead range engineer in the range development and support during the OT&E of the Air Force's next generation information operations platform security appliance.

TEST INTEGRATOR 4 YEARS CYBER SECURITY ENGINEERING SERVICES COMPANY

Test network engineer responsible for testing cutting edge information assurance technologies. Assisted in the procurement and network design of over \$3M of information technology equipment utilized for High Assurance Internet Protocol Encryptor (HAIPe) 3.x research and development. Supported the test and development of NSA certified Type-1 encryption initiatives for the airborne warfighter.

PROJECT LEAD 1 YEAR CYBER SECURITY ENGINEERING SERVICES COMPANY

Technical lead responsible for the day-to-day communications support of a 200-member Joint Task Force element. Provided communications oversight, project implementation, and systems support for a multitude of ruggedized deployed communications systems. Provided cost/benefit analysis to senior staff members to meet information technology budget requirements.

NETWORK ADMINISTRATOR 2 YEARS CYBER SECURITY ENGINEERING SERVICES COMPANY

Shift lead and senior network administrator for network operations at Camp Victory, Iraq. Provided theatre network administration services for a large-scale rigorous network of 50,000 users. Responsible for maintaining, operating, and installing Cisco related devices throughout regional complex infrastructure.

INFRASTRUCTURE TECHNICIAN 1 YEAR CYBER SECURITY ENGINEERING SERVICES COMPANY

Lead infrastructure technician responsible for all maintaining site's Tandberg infrastructure and administration. Provided daily monitoring and analysis on Cisco core infrastructure services valued at \$2M. Responsible for documenting and maintaining the documentation and visual layout for network services provided to all users within the Air Force's Air Intelligence Agency.

NETWORK MANAGER 6 YEARS NSA - TEXAS

Engineered campus-wide NIPRNET and SIPRNET Gigabit Cisco infrastructure upgrade. Served as shift lead and responsible for the configuration, operation, security, restoration, service improvements and updates of high bandwidth data/voice circuits. Monitored status and performance of transmission and switching systems, local and wide area networks, and subscriber equipment. Implemented and completed rollover of site's legacy IP format to a new NSA mandated addressing scheme.

TITLE: SENIOR CONSULTANT

YEARS OF EXPERIENCE: 20+ YEARS

SENIOR CONSULTANT CONDUCTING ADVANCED SECURITY ASSESSMENTS OF CRITICAL INFRASTRUCTURES AGAINST VARIOUS NETWORK DEFENSE FRAMEWORKS—INTEGRATING NETWORK SECURITY, SURVIVABILITY/RESILIENCY, RISK ASSESSMENT, TACTICS & TRAINING PROGRAMS, AND CYBER EXERCISE DESIGN METHODOLOGIES. TECHNICAL LEADER AND INNOVATOR IN CYBER WARFARE OPERATIONS. MILITARY INFORMATION OPERATIONS EXPERIENCE WITH UNDERSTANDING OF ADVERSARY TACTICS AND THEIR APPLICATION TO DEFENSIVE OPERATIONS. EXPERIENCE WITH NETWORK VULNERABILITY AND OPERATIONS SECURITY ASSESSMENTS, EFFECTIVE RISK REMEDIATION, AND TRAINING CURRICULUM DEVELOPMENT IN OFFENSIVE AND DEFENSIVE NETWORK TACTICS. EXPERIENCE PREPARING PAPERS AND PRESENTATIONS FOR TECHNICAL AND NON-TECHNICAL AUDIENCES.

SKILL SET: CERTIFIED CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA). CERTIFIED INFORMATION SYSTEM SECURITY PROFESSIONAL (CISSP). CERTIFIED ETHICAL HACKER (C|EH). CERTIFIED EXPERT PENETRATION TESTER (CEPT). EXPERT KNOWLEDGE OF CYBER EXERCISING, OFFENSIVE CYBER TACTICS DEVELOPMENT, CONTINUITY PLANNING, BUSINESS RESILIENCY, NETWORK AND SECURITY CENTER OPERATIONS, NETWORKING TECHNOLOGIES AND TOPOLOGIES, SYSTEM ADMINISTRATION, INFORMATION SYSTEMS SECURITY ANALYSIS, PENETRATION TESTING, AND VULNERABILITY TESTING.

DEGREE	INSTITUTION
PHD MBA BS	NORTHCENTRAL UNIVERSITY BUSINESS ADMINISTRATION, INFORMATION SECURITY. COMPLETED 39 HOURS. STARTED DISSERTATION.
	WEBSTER UNIVERSITY, 1996 MAJOR: BUSINESS ADMINISTRATION
	UNITED STATES AIR FORCE ACADEMY, 1993 MAJOR: COMPUTER RESOURCE & INFORMATION MANAGEMENT, DISTINGUISHED GRADUATE

PATENTS

SYSTEMS AND METHODS FOR A SIMULATED NETWORK ENVIRONMENT AND OPERATION THEREOF. US 2009/0319247 A1. DECEMBER 24, 2009

SYSTEMS AND METHODS FOR AUTOMATED BUILDING OF A SIMULATED NETWORK ENVIRONMENT. US 2009/0319647 A1. DECEMBER 24, 2009

SYSTEMS AND METHODS FOR A SIMULATED NETWORK TRAFFIC GENERATOR. US 2009/0319248 A1. DECEMBER 24, 2009

SYSTEMS AND METHODS FOR NETWORK MONITORING AND ANALYSIS OF A SIMULATED NETWORK. US 2009/0319249 A1. DECEMBER 24, 2009

SYSTEMS AND METHODS FOR RECONSTITUTION OF NETWORK ELEMENTS IN A SIMULATED NETWORK. US 2009/0319906 A1. DECEMBER 24, 2009

SYSTEMS AND METHODS FOR A SIMULATED NETWORK ATTACK GENERATOR. US 2009/0320137 A1. DECEMBER 24, 2009

TECHNICAL TRAINING/CERTIFICATIONS

- CEI: CERTIFIED EC-COUNCIL INSTRUCTOR
- LPT: LICENSED PENETRATION TESTER
- CRISC: CERTIFIED IN RISK & INFORMATION SYSTEMS CONTROL
- CISA: CERTIFIED INFORMATION SYSTEMS AUDITOR
- CISSP: CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
- PMP: PROJECT MANAGEMENT PROFESSIONAL

- CEPT: CERTIFIED EXPERT PENETRATION TESTER
- CSSA: CERTIFIED SCADA SECURITY ARCHITECT
- CEH: CERTIFIED ETHICAL HACKER
- CWAPT: CERTIFIED WEB APP PENETRATION TESTER

EXPERIENCE

PRINCIPAL / WHITE HAT HACKER / TRAINER 2014 – PRESENT (COMPANY REDACTED)

Provide holistic approach to security, facilitating cost-effective security control analysis, based on assessed risk. Provide vulnerability assessment, penetration testing (technical & social engineering), & security audit expertise. Develop customized curriculum & deliver content for numerous courses, including CISSP, CEH, and Security+. Provide malware analysis and reverse engineering services for incident response and security research. Provide expertise in cyberwar exercise simulator and system design, development, deployment, and sustainment. Develop computer network defense training scenarios for use in exercises, simulations, research, and events.

VICE PRESIDENT, SECURITY PRODUCTS / CONSULTANT. 2010–2014 (COMPANY REDACTED)

Responsible for manufacturing, distribution, marketing, & sales to migrate security products from R&D to market. Responsible for managing relationships with vendors, resellers, distributors, clients, & subcontractors. Planned & successfully implemented company wide CRM to effectively manage customer relationships/campaigns. Created, grew, & managed penetration testing & security assessment business for aircraft manufacturing industry. Managed budget, resources, schedules, and deliverables as PM on both commercial and government contracts.

DIRECTOR, RESEARCH & DEVELOPMENT 2008–2010 (COMPANY REDACTED)

Responsible for the design, development, and architectural review of new technologies, services, and products. Managed team of 15 technical experts responsible for researching & developing new security products & services. Responsible for introducing a profitable line of products into a company that was 100% service-oriented. Provided guidance & strategies to achieve technical advancement in security training, exploitation, & virtualization. Regularly provided project & technological updates to CEO, CTO, senior management, and Board of Directors.

CHIEF ENGINEER 2005–2008 (COMPANY REDACTED)

Managed technical teams and key projects ranging from innovative research projects to systems integration. Developed strategies & technical plans to market HAIPE v2 cryptography hardware based on FPGA integrated circuit technology. Led team in Systems Development Lifecycle process to assess requirements and develop innovative solutions. Provided vision, engineering support, curriculum development, & instructor support for cyber warfare training. Analyzed current cyber warfare training market & designed an innovative 75% hands-on profitable course.

NETWORK INFORMATION ASSURANCE OFFICER 2004-2005 (COMPANY REDACTED)

Responsible for the operational security of the DISA management enclave for the Global Information Grid (GIG). Managed CyberGuard firewall, Securify IDS, ITA, and HAIPE encryptors for Element Management Systems. Worked with Pacific and Europe theatres to ensure security measures were effectively implemented globally. Developed and briefed DISA Program Management Office personnel on information security recommendations.

SENIOR INFORMATION SECURITY CONSULTANT 2002-2004 (COMPANY REDACTED)

Designed & maintained VPN for Air Force-wide security exercises conducted over operational network backbone. Developed and standardized defense simulator architecture to include firewalls, switches, routers, servers, & IDS.

Developed information security attack scenarios for quarterly training & annual DoD-wide cybersecurity exercises. Lead engineer responsible for information security architecture for worldwide network defense simulators.

SENIOR INFORMATION ASSURANCE ENGINEER / MICROSOFT CERTIFIED TRAINER. 1999-2002 (COMPANY REDACTED)

Developed the business plan and stood up a successful Microsoft CTEC business unit within the company. Analyzed, troubleshot, & optimized network infrastructures and enterprise designs for Air Force worldwide sites. Evaluated network security & implemented security tools and countermeasures at Air Force worldwide sites. Upgraded firewalls/proxy servers & migrated DHCP, WINS, & DNS to Windows 2000 at Air Force worldwide sites.

PRESIDENT 2000-2002 (COMPANY REDACTED)

Provided corporate vision, created business model, and developed business and marketing plans. Responsible for all company day-to-day operations, ranging from customer relations to accounting. Expanded company operations from \$10k to over a quarter million in annual revenue in less than two years.

NETWORK ENGINEER. 1997-1999 US AIR FORCE

Designed & installed local & wide area computer & telecommunications networks for twenty worldwide sites. Trained network security administrators & implemented network security programs at twelve Air Force bases. Troubleshot network-related problems both remotely and locally for over twenty worldwide sites. Managed crypto equipment (KIV-7 and KG-184s) for Scott Air Force Base Secret LAN.

TITLE: SENIOR Security Engineer 2

YEARS OF EXPERIENCE: 16+ YEARS

CURRENT MANAGING DIRECTOR OF SPECIAL OPERATIONS AND PREVIOUS DIRECTOR OF OFFENSIVE SECURITY, SENIOR OFFENSIVE SECURITY ENGINEER, PENETRATION TESTER, RED TEAM OPERATOR, AND CYBERSECURITY CONSULTANT WITH 20+ YEARS OF EXPERIENCE IN A NETWORK SECURITY CAPACITY. I HAVE HAD THE HONOR OF WORKING IN MULTIPLE SECTORS WITHIN THE IT AND CYBERSECURITY FIELDS (RETAIL, BIOTECHNOLOGY, BANKING AND FINANCE, CYBERSECURITY SERVICE PROVIDER (CSSP) OPERATIONS, MEDICAL AND OFFENSIVE SECURITY), AND AS A RESULT, I BRING A STRONG CUSTOMER-ORIENTED PERSPECTIVE TO MY WORK WHILE STILL MAINTAINING A SET OF HIGHLY TECHNICAL SKILLS. I AM A PREVIOUSLY CLEARED (HELD FROM 2010 – 2020) PROFESSIONAL AND AM CURRENTLY DEPARTMENT OF DEFENSE DIRECTIVE (DoDD) 8140 (FORMERLY 8570) COMPLIANT IN THE FOLLOWING ROLES: IAT III, IAM III, IASAE II, CSSP ANALYST/INFRASTRUCTURE SUPPORT/INCIDENT RESPONDER/AUDITOR.

SKILL SET: (ISC)2 Certified Information Systems Security Professional (CISSP), GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), Offensive Security Certified Expert (OSCE), Offensive Security Certified Professional (OSCP), Offensive Security Wireless Professional (OSWP), eLearnSecurity Mobile Application Penetration Tester (eMAPT), Amazon Web Services (AWS) Certified Cloud Practitioner (CCP), EC-Council Certified Ethical Hacker (CEH), EC-Council Certified Network Defense Architect (CNDA), IACRB Certified Penetration Tester (CPT), CompTIA Security+, Network+, A+

DEGREE	INSTITUTION
BA	UNIVERSITY OF MARYLAND MAJOR: CRIMINOLOGY AND CRIMINAL JUSTICE

CERTIFICATIONS

- (ISC)2 CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)
- GIAC EXPLOIT RESEARCHER AND ADVANCED PENETRATION TESTER (GXPN)
- OFFENSIVE SECURITY CERTIFIED EXPERT (OSCE)
- OFFENSIVE SECURITY CERTIFIED PROFESSIONAL (OSCP)
- OFFENSIVE SECURITY WIRELESS PROFESSIONAL (OSWP)
- eLEARNSECURITY MOBILE APPLICATION PENETRATION TESTER (eMAPT)
- AMAZON WEB SERVICES (AWS) CERTIFIED CLOUD PRACTITIONER (CCP)
- EC-COUNCIL CERTIFIED ETHICAL HACKER (CEH)
- EC-COUNCIL CERTIFIED NETWORK DEFENSE ARCHITECT (CNDA)
- IACRB CERTIFIED PENETRATION TESTER (CPT)
- COMPTIA SECURITY+, NETWORK+, A+

CURRENT TRAINING

- Altered Security Academy Red Team Expert Labs (CRTE, January 2022 – Present)
- Altered Security Academy Active Directory Labs (CRTP, February 2020 – Present)
- Offensive Security Advanced Web Attacks and Exploitation (OSWE Labs, July 19, 2020 – August 19, 2020)
- eLearnSecurity Web Application Penetration Testing Extreme v2 (WAPTX, January 2020 – Present)
- Offensive Security Advanced Web Attacks and Exploitation (OSWE, February 2019 – May 2019)
- eLearnSecurity Penetration Testing Extreme (PTX, October 2018 – January 2019)
- eLearnSecurity Mobile Application Security Tester (MASPT v2, October 1, 2018 – February 1, 2019)
- Programming Mobile Applications for Android Handheld Systems: Part 1 and Part 2 (June 19 – July 19, 2017, University of Maryland/Coursera)
- eLearnSecurity Web Application Penetration Testing Extreme (WAPTX, November 4, 2016 – February 12, 2017)
- Offensive Security Labs (Pentesting with Kali (PWK), October 31, 2016 – November 30, 2016)
- eLearnSecurity Advanced Reverse Engineering of Software (ARES, December 2015 – February 2016)
- Offensive Security Certified Expert (OSCE, Cracking the Perimeter (CTP), February 3, 2013 – March 3, 2013)
- SANS Exploit Researcher and Advanced Penetration Tester (GXPN) (June 15, 2013 – June 22, 2013; SANSFIRE DC 2013) / NetWars Tournament (June 17 – 18, 2013; SANSFIRE DC 2013)
- Offensive Security Certified Professional (OSCP, Pentesting with BackTrack Labs, January 2013
 - April 2013, December 2011 - March 2012)
- Offensive Security Wireless Attacks – Wifu v3.0 (OSWP, Wireless Penetration Testing, August 2012 – December 2012)

EXPERIENCE

MANAGING DIRECTOR OF OFFENSIVE SECURITY SPECIAL OPERATIONS 2023 – PRESENT (COMPANY REDACTED)

- Manager of the Cloud Alliance Security Assessment (CASA) and Mobile Application Security Assessment (MASA) Teams (Google Authorized Partner)
- Manager of the Social Engineering Services (SES) Unit
- Manager of the Special Operations Unit (Red Team)

DIRECTOR OF OFFENSIVE SECURITY OPERATIONS 2022–2023 (COMPANY REDACTED)

- Manager of the Google Designated Security Assessment (GDSA) Team
- Manager of the Compliance Penetration Testing Team
- Manager of Special Projects
- Ensures all requirements are met per assessment and enforces all MOCA standards in authorizing customers the ability to use Google Restricted Scopes
- Conducts market research and implements new offensive security practices and techniques, tactics and procedures to continually improve testing effectiveness and accuracy.
- Identifies emerging cyber security specialties and community needs and builds business units to address these needs
- Develops business strategies to scale each penetration testing operations through innovative career development initiatives and promotion within.

SENIOR OFFENSIVE SECURITY ENGINEER 2020–2021 (COMPANY REDACTED)

- Strong knowledge of AWS and/or Google Cloud Compute from an attacker perspective
- Strong experience utilizing and attacking secOps / techOps tooling, infrastructure, and automation
- Build disposable, repeatable, and verifiable red team infrastructure for ad-hoc engagements
- Work with 3rd party vendors to carefully test their products without causing outages or incidents
- Develop, implement, and communicate vulnerability mitigation strategies to development teams
- Work solo and collaboratively while delivering simultaneous projects on a deadline
- Think like an attacker and solve complex problems with expertise and ingenuity
- Give presentations and represent Okta in private or public venues

SENIOR RED TEAM OPERATOR 2017–2020 (COMPANY REDACTED)

- Conducts in-depth full scope Red Team engagements within the digital, social, and physical realms of security to include the execution of Network and Web Application Penetration Testing, Intelligence Gathering, Physical Security Assessments, Mobile Security Assessments and Social Engineering Engagements.
- Researches, engineers, and develops innovative tactics, techniques, and procedures (TTPs) for adversarial activity.
- Lead other senior, mid, and junior red team operators in targeted commercial and High Value Asset (HVA) engagements.
- Serves as a member of a surge team that assists engagements during times of need. The domains involved include but are not limited to: Digital Forensics, Threat hunting, Reverse Engineering, Programming, and Incident Response and Handling.
- Provides internal training and mentorship to mid and junior level penetration testers and red team operators.
- Interfaces with clients and senior management to design, scope and coordinate engagement parameters and assert compliance with Rules of Engagement (RoE).
- Designs and delivers executive and technical level engagement briefings

SENIOR SECURITY CONSULTANT 2014-2017 (COMPANY REDACTED)

- Led Web Application Penetration Testing (WAPT) planning, execution, and outbrief engagement briefings for federal and commercial entities.
- Technical Lead for multi-national threat emulation squad exercises and assessments. Conducted threat emulation activity planning, demonstration and execution in support of federal agencies. (2016)
- Created and administered virtual theatres used by federal agencies to conduct global exercises.
- Anticipated and analyzed customer exercise scenario development requirements to assess feasibility of execution parameters.
- Met with vendor staff and aided in the deployment of war games hardware and data to client site.
- Designed extensible and modular programs to facilitate the automation of validation operations across projects and analyze cloud SIEM events.
- Implemented project deliverables and assists with compliance program design.
- Engaged in Business Development acquisitions and developed proposals for submittal towards new contractual awards.
- Coordinated workflow and delivery of client deliverables and milestones with upper management at all levels as well as other client representatives/contractors on assigned project parameters/tasks.

LEAD ENGINEER / SENIOR PENETRATION TESTER 2013-2014 (COMPANY REDACTED)

- Conducted enterprise system, network, and web application penetration testing for clients ranging from commercial clients to large federal agencies and provided recommended controls and countermeasures to reduce risk.
- Automated penetration testing discovery phase efforts through the creation of scripts and tools which allowed penetration testers to conduct in-depth data analysis of returned artifacts in a timely manner.
- Performed data and trends analysis to correlate pentest findings to effectiveness metrics which helped define and assess active defense programs and the overall security posture of target clients.
- Performed retesting of mitigated vulnerabilities to ensure proper mitigation strategies are being executed and implemented.
- Created, executed, and modernized penetration testing procedures and Rules of Engagement (RoE) documentation which defined the scope of operations for scheduled penetration testing engagements.
- Engaged in meetings with senior risk management staff on a daily basis to ensure findings were accurate and accounted for.
- Documented risk management strategies to improve agency efficiency with penetration testing and vulnerability analysis.
- Consulted with internal client-team administrators and developers to help them understand and implement server hardening and secure application development principles and best practices.
- Created daily, weekly, and monthly status reports detailing the business impact of penetration testing findings on the client network infrastructure.
- Prepared contract deliverables with visibility of client Directors, Executive, and Commissioners.
- Interviewed potential penetration testing candidates for placement within our firm's offensive security division.

CYBERSECURITY SERVICE PROVIDER (CSSP) ANALYST/AUDITOR 2011-2013 (COMPANY REDACTED)

- Analyzed and evaluated anomalous network and system activity using malware package knowledge of UNIX- and Microsoft Windows-based computer systems and intrusion detection software.
- Reviewed logs daily from server systems, security tools, and network traffic analyzers to determine anomalies.
- Compiled information and prepared technically detailed incident reports on a daily/weekly/periodic basis on the events and incidents detected in the course of network monitoring.
- Conducted open source intelligence research and analyzed threat intelligence on new attack vectors, malware campaigns, and system vulnerabilities.
- Responded to incidents as required by the COR, with nonscheduled services, to ensure 24/7 continuity of operations of the CSSP.

- Assisted in the troubleshooting and problem-solving of a wide variety of critical networking issues.
- Implemented network blocks on perimeter routers, firewalls, and switches to triage or preempt malware replication and impending or active cyber attacks.
- Suggested and implemented modifications to access control lists, signatures, and tools to prevent and mitigate intrusions.
- Collaborated with members of the Information Assurance Management (IAM) team on daily policy issues.
- Developed recommendations to standard operating procedures (SOPs) used by the CSSP.
- Assisted the Agent of the Certification Authority (ACA) on Certification and Accreditation (C&A) engagements through technical review of asset configurations as well as interview of on-site experts to ensure DIACAP/STIG compliance (*NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems*).
- Trained and mentored new analysts on incident response procedures, network forensics, and DoD directives.

PROGRAM ANALYST / TECHNICAL SUPPORT SPECIALIST 2008-2009 (COMPANY REDACTED)

- Member of the BSI-II software (ca BIG Bronze Certified) testing, training, and technical support team.
- Created, proofed, and executed test scripts for software validation in software development life cycles.
- Developed and created user-manual entries for the end-user help system.
- Executed Role Based Access Control (RBAC) measures through the creation and maintenance of new and existing user accounts and permissions.
- Performed daily software testing of the BSI-II client and worked directly with application development team to ensure software functionality met customer requests/requirements.
- Trained internal and external end-users on software usage and its business applications over the phone or in-person.
- Provided end-user technical support to intramural labs contracted by several Federal agencies for software development changes and new releases.

TITLE: SENIOR SECURITY ENGINEER / PENETRATION TESTER

YEARS OF EXPERIENCE: 17+ YEARS

SENIOR SECURITY ENGINEER IN THE CYBER SECURITY INDUSTRY SINCE 2007, WHERE HE HAS FOCUSED PRIMARILY ON RISK AND VULNERABILITY ASSESSMENTS, PENETRATION TESTING, AND HANDS ON SECURITY TRAINING. SUPPORTED US MARINE CORPS FORCES CYBERSPACE, U.S. CYBER COMMAND, AND THE US AIR FORCE IN DEVELOPING TRAINING PROGRAMS AND EXERCISES FOR CYBER PROTECTION TEAMS. PERFORMED SECURITY ASSESSMENTS FOR FORTUNE 500 COMPANIES, GOVERNMENT AGENCIES, AND PRESIDENTIAL CAMPAIGN OFFICES. BEFORE ENTERING THE CYBER SECURITY INDUSTRY, SPENT SEVERAL YEARS AS A WEB APPLICATION DEVELOPER AND MANAGER OF SOFTWARE ENGINEERING. SERVED SIX YEARS IN THE U.S. MARINE CORPS RESERVES WHERE HE DEPLOYED TO THE AL ANBAR PROVINCE OF IRAQ IN SUPPORT OF OPERATION IRAQI FREEDOM. AFTER LEAVING THE MARINES, TRANSITIONED TO THE TEXAS AIR NATIONAL GUARD AS A CYBER INTELLIGENCE ANALYST WHERE HE SUPPORTED AIR FORCE CYBER DEFENSE INITIATIVES AND THE AIR FORCE'S PREMIER NATIONAL GUARD CYBER PROTECTION TEAM. PARTICIPATES HEAVILY IN CAPTURE THE FLAG EVENTS, BOTH LOCALLY AND INTERNATIONALLY. HAS DEVELOPED AND LED MULTIPLE LOCAL CAPTURE THE FLAG EVENTS DURING INDUSTRY SECURITY CONFERENCES.

SKILL SET: HOLDS A BACHELOR OF SCIENCE IN COMPUTER SCIENCE FROM SAM HOUSTON STATE UNIVERSITY, HAS HIS COMPTIA SECURITY+ AND NETWORK+ CERTIFICATION, AND IS CURRENTLY PURSUING HIS OFFENSIVE SECURITY CERTIFIED PROFESSIONAL (OSCP) CERTIFICATION

DEGREE

BS (UNIVERSITY REDACTED)

MAJOR: COMPUTER SCIENCE, EMPHASIS ON INFORMATION ASSURANCE, 2011

MEMBER OF THE SAM HOUSTON ASSOCIATION OF COMPUTER SCIENCE

TECHNICAL TRAINING/CERTIFICATIONS

- COMPTIA NETWORK+ & SECURITY+
- SANS ICS 415
- CURRENTLY PURSUING OFFENSIVE SECURITY CERTIFIED PROFESSIONAL (OSCP)

EXPERIENCE

FOUNDER / CYBER SECURITY CONSULTING COMPANY 2022-PRESENT (COMPANY REDACTED)

Founder and principal consultant of a cyber security consulting and managed service provider that specializes in offensive security. Additionally providing small and medium business with a turn-key cyber security solution for the management and monitoring of assets and data.

DIRECTOR AND SECURITY ARCHITECT 2022-2023 (COMPANY REDACTED)

Built and managed a team of offensive security engineers who performed penetration tests, security control validation exercises, threat hunting, and managed threat intelligence. Responsible for the vision and direction of building each of these programs from the ground up, including defining SLAs and SOPs, creating and maintaining a budget, onboarding vendors through the legal and risk management process, and establishing metrics to be presented to the board of directors and Cyber Security steering committee. Acted as the SME for security architecture during projects like migrating IAM providers and building a new Point-of-Sale System.

PENETRATION TESTER 2018-2022 (COMPANY REDACTED)

Participates in penetration tests, including web applications, hardware, network, and social engineering. Assessments include a Scope of Work, assessment period, risk rating, and a reporting process. Reports are generated and presented to the customer to provide high level remediation process and severity of findings, as well as a recommended timeline for remediation. Actively engages in quarterly CTF training and presents demonstrations on emerging tactics, techniques, and procedures. Previous demo discussions have included bypassing application white-listing, host-based C2, and RFID spoofing and cloning.

CHIEF CONSULTANT & CISO 2017-2018 (COMPANY REDACTED)

Tasked with developing a new cyber security consulting practice, focusing on vulnerability assessments, penetration testing, red team engagements, and general security program assessments. Responsibilities included developing customer onboarding processes, documenting engagement processes and procedures, establishing deliverables, and identifying marketing avenues. In addition to customer facing responsibilities, duties included developing an internal cyber security program, in accordance with NIST 800-53. Participated customer speaking events, training sessions, and writing marketing papers. Risk and vulnerability assessments were conducting using the NIST Risk Management Framework and tools such as Nessus. Penetration tests were conducted both internally and externally, typically in black box scenarios.

CYBERSECURITY CONSULTANT 2014-2017 (COMPANY REDACTED)

Performed penetration tests, security assessments, and risk assessments for commercial and federal customers including the Department of Homeland Security, United States Cyber Command, and Marine Corps Cyber Command. Federal customers were assessed in accordance with FISMA and NIST SP 800-53 documentation, while commercial customers were typically assessed in accordance with the Critical Security Framework, ISO 27001, or NEC/SIP guidance. Penetration tests generally consist of three elements, a phishing campaign, an external assessment, and an internal (authenticated) assessment.

Responsible for developing cyber security training scenarios, both as table top exercises and in virtual training environments, by incorporating training requirements from the customer, deploying the necessary virtual infrastructure, and developing automated scenarios ranging from network security and host defensive operations, forensic analysis and incident response, to offensive activities. Cyber security training scenarios were developed in a large scale virtual environment, and were designed to simulate as realistic networks as possible. This included architecting and deploying networks with thousands of user nodes and every possible technical solution – internal/external DNS, Exchange servers, Active Directory, DLP, and Proxy servers.

Additional responsibilities included the management and development of cyber security related competitions and workshops for industry or customer conferences (BSides Houston and San Antonio, HouSecCon, EUCL, Code Jam San Antonio, and Cyber Patriots).

Served as company ICS SME during consulting and training engagements. Leveraged the Critical Infrastructure Framework, NIST guidance, and NERC CIP to conduct security assessments, vulnerability assessments, and governance reviews.

CYBERSECURITY ANALYST & GROUP MANAGER 2013-2014 (COMPANY REDACTED)

Responsible for enterprise architecture strategic planning and integration for a data center consolidation effort with the VA. Provided analysis of current state enterprise architecture, IT policies, and processes, from which a plan of deliverables was developed for the customer. The focus of the enterprise architecture strategic planning was on high reliability, traceability, standards compliance, and exceeding the customer's timeline. This included establishing traffic flow and patterns for both user and server traffic, establishing a network design for the final consolidation, and working with application owners to create implementation plans. This data center migration primarily focused on the VAs DLP, Exchange, internal DNS, Active Directory, and Proxy solutions.

CYBER INTELLIGENCE ANALYST 2010-2016 USAF

Responsibilities ranged from developing network defense tactics to researching and presenting current cyber threats to squadron and wing level command. Squadron level Client Support Technician, operating in accordance with DoD 8570.01-m. Conducted troop level training in areas such as CompTIA Security+ and related topics. Provided expert analysis for the design of several test networks for the purpose of network defense tactics development. Acted as the ICS SME during group level training exercises (Cyber Guard 2014 and 2015, Cyber Shield 2015) by both technically defending customer assets and coordinating a defensive plan with Cyber Protection Teams, industry representatives, and federal organizations.

MANAGER OF WEB ENGINEERING & SECURITY 2011-2012 (COMPANY REDACTED)

Primary responsibility was leading the web-engineering group in the development and maintenance of a web application, which consisted of over 2Gb per second of daily traffic and millions of users. This included participating in high-level design, planning and coordination, and the execution of development throughout the entire software lifecycle. Took direction from the Director of Engineering and Executive Officers to achieve critical business and strategic goals. Additional duties included administrative role of managing employees, such as coordinating vacation days or overtime, performance reviews, and hiring process. Developed and administered hiring pre-screen test which aided in filtering dozens of unqualified candidates.

Additional responsibilities included writing of standards and practices for application security, coordinating penetration tests and vulnerability assessments of applications, working with third party PCI and vulnerability auditors, and providing customer support. Responsible for keeping up to date with relevant exploits and zero-day threats, and patching/refactoring these threats if necessary.

SECURITY ANALYST & APPLICATION DEVELOPER 2010-2011 (COMPANY REDACTED)

Responsibilities included development of web-based applications in support of WM Security Operations Center. Applications were database driven and solely developed full cycle from initial design to maintenance period. Aided in several large-scale system administration projects, notably an off-site redundancy system in the event of catastrophic failure. This required an in-depth analysis of enterprise architecture, and how it impacted the business. This system leveraged server mirroring of SQL databases and network load balancing. Other system administration duties were network monitoring, developing backup processes and procedures, maintenance of production and development servers, and security impact analysis.

JUNIOR APPLICATION DEVELOPER 2005-2008 (COMPANY REDACTED)

Extensive development of Content Management Systems to provide clients with a custom user interface for various dynamic applications. CMS developed using PHP5, CSS, JavaScript, HTML, JSON, AJAX, and SQL. Developed web applications that focused on dynamic usage. Emphasis was placed on object-oriented programming, optimization of code to provide quick project turn around, and a desirable user interface experience. All databases were set up, maintained, and optimized using phpMyAdmin, Control Panel, and MySQL. Regular maintenance included Cron Jobs, regular backups, and export as CSV. Training provided clients with use of interactive web applications, such as Content Management Systems.

CompTIA

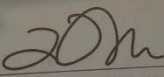
ADVANCING THE GLOBAL IT INDUSTRY

Alexander Cobblah

has successfully completed the requirements to be recognized as



CAREER ID


TODD THIBODEAUX
President & CEO

May 25, 2011

DATE CERTIFIED



C | E H
Certified Ethical Hacker™

Certified Ethical Hacker

THIS IS TO ACKNOWLEDGE THAT

Alexander Cobblah

bearing the membership ID [REDACTED] for
CEH Version 6

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

EC-Council

JAY BAVISI, PRESIDENT

March 18, 2011

DATE

International Information System Security Certification Consortium

The (ISC)² Board of Directors hereby awards

Alexander Cobblah

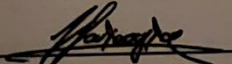
the credential of

Certified Information Systems Security Professional[®]

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

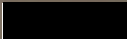


Zachary Tudor - Chairperson



Yiannis Pavlosoglou - Secretary




Certification Number

Jul 1, 2021 - Jun 30, 2024
Certification Cycle

Certified Since 2012

(ISC)²





IACRB

Information Assurance Certification Review Board

Certified Penetration Tester

On April 13, 2011 the Information Assurance Certification Review Board has awarded this title to:

Alexander Cobblah

For completing the training and passing the CPT exam.

Janet Billings

Janet Billings
Certification Director



Global Information Assurance Certification
presents this certification to:

Alexander Cobblah

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

GIAC EXPLOIT RESEARCHER AND ADVANCED PENETRATION TESTER
- GXPN

Received on this date 2013/11/1 and valid through 2025/11/30



Analyst number:




Jeff Frisk, Director
Global Information Assurance Certification



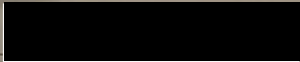
CompTIA

ADVANCING THE GLOBAL IT INDUSTRY

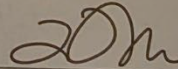
Alexander Cobblah

has successfully completed the requirements to be recognized as

CompTIA
Network+
CERTIFIED



CAREER ID

A handwritten signature in black ink.

TODD THIBODEAUX
President & CEO

June 10, 2010

DATE CERTIFIED



THIS IS TO ACKNOWLEDGE THAT

Alexander Cobblah

IS CERTIFIED AS A

OSCE

(Offensive Security Certified Expert)

AND HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND CRITERIA
FOR SAID CERTIFICATION THROUGH EXAMINATION ADMINISTERED BY
OFFENSIVE SECURITY.

THIS CERTIFICATION EARNED ON

27th of September 2014



A handwritten signature in black ink, appearing to read "Mati".

Mati Aharoni

PRESIDENT AND CHIEF EXECUTIVE OFFICER

This certificate may be verified by contacting orders@offensive-security.com using the certificate holders student ID [REDACTED]

OFFENSIVE SECURITY

THIS IS TO ACKNOWLEDGE THAT

Alexander Cobblah

IS CERTIFIED AS A

OSCP

(Offensive Security Certified Professional)

AND HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND CRITERIA
FOR SAID CERTIFICATION THROUGH EXAMINATION ADMINISTERED BY
OFFENSIVE SECURITY.

THIS CERTIFICATION EARNED ON

21st of September 2013



Mati Aharoni

PRESIDENT AND CHIEF EXECUTIVE OFFICER

This certificate may be verified at www.offensive-security.com using the certificate holders student ID _____

OFFENSIVE security

THIS IS TO ACKNOWLEDGE THAT

Alexander Cobblah

IS CERTIFIED AS A

OSWP

(Offensive Security Wireless Professional)

AND HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND CRITERIA
FOR SAID CERTIFICATION THROUGH EXAMINATION ADMINISTERED BY
OFFENSIVE SECURITY.

THIS CERTIFICATION EARNED ON

3rd of December 2012



OFFENSIVE
security

Mati Aharoni

PRESIDENT AND CHIEF EXECUTIVE OFFICER

This certificate may be verified at www.offensive-security.com using the certificate holders student ID [REDACTED]

CompTIA.

ADVANCING THE INDUSTRY

Alexander Cobblah

has successfully completed the requirements to be recognized as

CompTIA
Security+
CERTIFIED

CAREER ID


TODD THIBODEAUX
President & CEO

June 17, 2010

DATE CERTIFIED

APPENDIX C
Sample Report

CONFIDENTIAL



Test Inc. External Network Penetration

Engagement Report

Delivered To

John Doe
1234 Main St.
Springfield, NA 12345
123-456-7890
test@testinc.com

Delivered January 20th, 2023

Executive Summary

Engagement

Test Inc., pursuant to the CyVantage/Test Inc. MSA; Appendix B SOW, engaged CyVantage LLC to perform a network vulnerability assessment against Test Inc. identified external facing components. In order to evaluate the current posture of the external interfaces, CyVantage conducted a hybrid black/grey box validation operation. The test was conducted “blind” (without knowledge of any credentials to any component outside of VPN access). The level of aggression was well below the threshold of an Advanced Persistent Threat (APT) but well within the purview of most malicious actors (ransomware, etc.). In addition, the test was technically based and absent of any “social engineering” efforts. The overall objective of the test was to determine whether Test Inc.’s external networks were properly managed and functioning according to industry standards and best practices.

Results

Multiple findings were discovered (7 in total) ranging in severity from Medium to Critical. CyVantage recommends minor changes that can prove powerful in closing gaps in some of the vulnerabilities observed and improve Test Inc.’s overall best practices. CVSS 3.3 and NIST SP 800-53 were heavily consulted during this engagement as they serve as free standing, government issued, general practices and compliance guides trusted by numerous organizations around the world.

Recommendations

The CyVantage report details the business impact and proposed mitigation strategy for each observed finding. The report also includes detailed references and ultimately all the artifacts generated by the test. The core recommendations primarily fall into two categories: 1) Update & Maintain specific software, and 2) Replace outdated encryption protocols.

Specific Recommendations:

- 1) Update through patch and configuration management processes Test Inc.’s version of PHP to the latest supported version (8.1.0) and enable ongoing evaluations to keep up to date with emerging threats.
- 2) Update appliance software identified (see page 14).
- 3) Disable all instances of SSLv3 and associated ciphers. Move toward the use of newer protocols TLS v1.2 and v1.3 (see page 16 & 18)
- 4) Disable password authentication to externally accessible resources. Enable a trusted PKI certificate in conjunction with MFA (if this method of communication is necessary).
- 5) Secure headers across hosted web services (see page 20).
- 6) Perform general patch management (see page 22).
- 7) Perform regular annual Penetration Testing and Vulnerability Assessments

Conclusion

As a general rule the configuration established by Test Inc. shows a dedication to creating and maintaining a “defense in depth environment” pursuant to best practices. Relatively minor patches, configurations, updates, and adaptations will enhance Test Inc.’s defensive posture. Ongoing assessments and evaluations (followed by action on remediation) will further fortify Test Inc.’s infrastructure.

This page has been intentionally left blank

Disclaimer

The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published, or redistributed without the prior written consent of Test Inc.. The findings expressed are in good faith and while every care has been taken in preparing these documents, CyVantage LLC makes no representations and gives no warranties of any kind with respect to these documents. CyVantage LLC its subsidiaries, employees and agents cannot be held liable for the misuse of the information and risk recommendations found in this document.

All information found in this document is **CONFIDENTIAL**.

Document Versioning Changelog			
Author	Version	Date	Notes
George Washington	1.0	1/9/2023	Initial Documentation and Submission
Abraham Lincoln	2.0	1/16/23	Revisions
Alexander Hamilton	3.0	1/20/23	Revisions
Benjamin Franklin	4.0	1/21/23	Final

TABLE OF CONTENTS

1	INTRODUCTION	8
2	OBJECTIVE.....	8
3	SCOPE	8
4	PENETRATION TESTING ENGAGEMENT SUMMARY	10
4.1	TOP PORTS	10
4.2	FINDING STATUS	11
4.3	SUMMARY OF FINDINGS	11
5.	PRELIMINARY FINDINGS	12
5.1	CRITICAL FINDINGS	13
5.1.1	PHP Remote Code Execution Vulnerability (Version 7.x.).....	13
5.2	HIGH FINDINGS	15
5.2.1	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Read-Only Path Traversal.....	15
5.2.2	Use of Legacy Encryption Protocols (SSLv3).....	17
5.2.3	Administrative Console Externally Accessible (Password Authentication Enabled).....	18
5.3	MEDIUM FINDINGS.....	19
5.3.1	Use of Legacy Encryption Protocols (TLS 1.0)	19
5.3.2	Cross Frame Scripting (XFSv2)	20
5.3.3	General Patch Management.....	23
5.4	LOW FINDINGS	25
6	CONCLUSION	26
7	APPENDICES.....	27
7.1	APPENDIX A: TOOLS INVENTORY.....	28
7.2	APPENDIX B: SSL VPN CONCENTRATORS.....	28
7.3	APPENDIX C: CRUSH FTP HTTP SERVER	30
7.4	APPENDIX D: IIS EXPOSURE.....	30
7.5	APPENDIX E: CHECK POINT SECUREMATE HOSTNAME DISCLOSURE.....	31
7.6	APPENDIX F: LOG4J	32

TABLE OF FIGURES AND TABLES

Figure 1 – EOL Chart	14
Figure 2 – Unauthenticated download of translation table	16
Figure 3 – Translation Table	16
Figure 4 - SSLv3 detected (SSLSCAN)	17
Figure 5 - Attempt to log in as root to SSH interface	18
Figure 6 – TLS v1.0 detected (SSLSCAN)	19
Figure 7 – JavaScript blocking XFSv2 execution	20
Figure 8 – Emulated login page using direct Test Inc. URIs	22
Figure 9 – jQuery 1.7.1 found	24
Figure 10 – VPN Concentrator #1	29
Figure 11 – VPN Concentrator #2	29
Figure 12 - Attempt at unauthenticated XSS detected and failed	30
Figure 13 – IIS Servers which expose default page	30
Figure 14- IIS default page sample	31
Figure 15- CheckPoint SecuRemote validation request (Nessus Output)	31
Figure 16- Result from Log4Jscan (Nessus Output)	32
Table 1- Scope	8
Table 2 -Top Ports Summary	10
Table 3- Summary of Findings	11
Table 4- Vulnerabilities Discovered	11
Table 5- Sample Pentesting Toolkit	28

1 INTRODUCTION

CyVantage LLC has been tasked with conducting a network vulnerability assessment against identified Test Inc. external facing components. In order to evaluate the current posture of the external assets (interfaces), CyVantage LLC conducted a hybrid black/grey box validation operation. During this engagement, the tester was not provided credentials to any component outside of VPN access and relied on a Kali machine (for offensive security tool use) to execute testing efforts. This network penetration test serves as a starting point for discovery into the current posture of the Test Inc. enterprise. The targeted asset ranges can be found below.

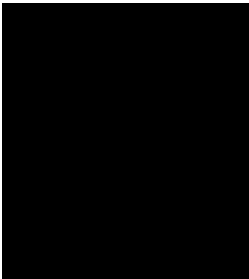
2 OBJECTIVE

Our objective was to determine whether Test Inc. external networks were properly managed and functioning according to industry standards and best practices. Our review scope covered: approved network security system baselines, security standards, and security policies. Validation of automated scanning findings were conducted to ascertain the true posture of the network. To accomplish our objective, we performed automated scans using industry recognized tools (such as NMAP, Burp Suite Professional, and proprietary CyVantage processes) to test the current system configurations and policies in place across the scoped network spaces and compared the results against best practices, hardening standards, and documented discrepancies. CVSS 3.3 and NIST SP 800-53 were heavily consulted during this engagement as they serve as free standing, government issued, general practices and compliance guides trusted by numerous organizations around the world. The NIST guide can be found here:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

3 SCOPE

The scope of this engagement was identified as the following assets:

External IPs	
Test Inc.	

--	--	--

Black Out Times	
EST	24/7

4 PENETRATION TESTING ENGAGEMENT SUMMARY

Upon commencement of the engagement, the tester was not provided any credentials to Test Inc.'s system. Pre-authentication system scanning was conducted and identified several compliance based vulnerabilities.

The next sections will detail the structure of reporting and the findings discovered. The findings detailed in future sections of this report will serve as recommendations to bolster the defensive posture of the targeted network devices, servers, and applications. Naturally, environments vary from organization to organization and it is recommended that Change Management be followed in accordance with organizational policies when attempting to implement any of the mitigation recommendations.

Multiple findings were discovered (**7** in total) ranging from Medium to Critical on CyVantage's severity scale (1 Critical, 3 High and 3 Medium). The severity is determined by the impact to the organization in relation to the complexity of exploitation.

The configuration established by Test Inc. shows a dedication to creating and maintaining a defense in depth environment pursuant to best practices however, small changes can prove powerful in closing gaps in some of the best practices observed.

4.1 TOP PORTS

Listed below are the five most common services and ports detected during the discovery phase of this engagement:

Port Number	Protocol	Service Use	Instances
22	TCP	SSH	1
53	TCP	Domain Name Services (DNS)	2
80	TCP	HTTP (Web Services)	9
443	TCP	HTTPS (Web Services)	14
8080	TCP	Proxy	1

Table 1 - Top Ports Summary

4.2 FINDING STATUS

Listed below are the statuses that are assigned to vulnerabilities discovered during this penetration test. This allows for the creation of metrics that can be used to monitor the progress of remediation efforts:

Closed This designation signifies the remediation of a cited vulnerability.

Open This designation signifies a finding has been newly discovered or currently exists within the scope of the current assessment at the time of report delivery.

4.3 SUMMARY OF FINDINGS

Detailed below is a chart listing the number of vulnerabilities discovered per risk rating category. In this engagement, only the most pertinent and confirmed vulnerabilities have been presented for evaluation and discussion:

Rating	Open	Closed	Total
Critical	1	0	1
High	3	0	3
Medium	3	0	3
Low	0	0	0

Table 2 - Summary of Findings

Vulnerability Number	Vulnerability Name	Severity	Status
C1	PHP Remote Code Execution Vulnerability (Version 7.x.)	Critical	Open
H1	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Read-Only Path Traversal	High	Open
H2	Use of Legacy Encryption Protocols (SSLv3)	High	Open
H3	Administrative Console Externally Accessible (Password Authentication Enabled)	High	Open
M1	Use of Legacy Encryption Protocols (TLS 1.0)	Medium	Open
M2	Cross Frame Scripting (XFSv2)	Medium	Open

M3	General Patch Management	Medium	Open
----	--------------------------	--------	------

Table 3 - Vulnerabilities Discovered

5. PRELIMINARY FINDINGS

The following section details the vulnerabilities discovered during the course of this engagement. Penetration testing engagements serve as tests conducted in a “snapshot” timeframe and findings discovered within that time may later be mitigated throughout the course of delivery of this document. In addition, systems integration, the addition/connection of new or legacy systems, and the inclusion of networks from mergers/acquisitions may also profoundly effect Test Inc.’s’ network security posture but would be outside of the purview of this test.

5.1 CRITICAL FINDINGS

5.1.1 PHP Remote Code Execution Vulnerability (Version 7.x.)		
CWE ID(s): 1104, 1035	Status: Open	Risk: Critical
Affected hosts and URL(s): <div></div>		

Description: The affected host harbors a version of PHP which is notorious for allowing remote code execution (RCE) within its subsystem. The versions detected (7.0.9) are no longer supported by PHP and have reached End of Life (EOL).

***Detection
Request***

POST /components/vdv/core/view/login_check.php HTTP/1.1

Host: [REDACTED]

Content-Length: 0

Accept: */*

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36

X-Requested-With: XMLHttpRequest

Origin: http://[REDACTED]

Referer: http://[REDACTED]/

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Cookie: PHPSESSID=ui53j4gcaseu0nksvc3nmar1n0

Connection: close

Response

HTTP/1.1 200 OK

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Content-Type: text/html; charset=UTF-8

Expires: Thu, 19 Nov 1981 08:52:00 GMT Server:

Microsoft-IIS/10.0

X-Powered-By: PHP/7.0.9

Date: Mon, 10 Jan 2023 01:14:46 GMT

Connection: close

Content-Length: 0

NOTE: While most exploitation in regards to these effects occurs in NGINX hosting instances, the framework itself inherently has numerous vulnerabilities.

Business Impact: If the correct attack conditions are met, the affected server would be at risk of full compromise as adversarial users would be able to execute commands in the context of the compromised service. PHP has the ability to read and write code leaving the server's integrity at high risk.

Mitigation Strategy Recommendation: Through patch and configuration management processes, update this version of PHP to the latest supported version (8.1.0). Ensure quarterly or annual evaluation of software suites in use and keep up to date with emerging threats against coding languages and frameworks in use by Test Inc.'s enterprise environment.

References:

- <https://www.php.net/supported-versions.php>
- <https://www.zdnet.com/article/nasty-php7-remote-code-execution-bug-exploited-in-the-wild/>
- <https://www.appdynamics.com/blog/engineering/php-7-vulnerabilities-you-cant-ignore/>
- <https://blog.qualys.com/product-tech/2019/10/30/php-remote-code-execution-vulnerability-cve-2019-11043>

Evidence:

Currently Supported Versions

Branch	Initial Release		Active Support Until		Security Support Until	
7.4	28 Nov 2019	2 years, 1 month ago	28 Nov 2021	1 month ago	28 Nov 2022	in 10 months
8.0	26 Nov 2020	1 year, 1 month ago	26 Nov 2022	in 10 months	26 Nov 2023	in 1 year, 10 months
8.1	25 Nov 2021	1 month ago	25 Nov 2023	in 1 year, 10 months	25 Nov 2024	in 2 years, 10 months

Or, visualised as a calendar:



Key

Active support	A release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made.
Security fixes only	A release that is supported for critical security issues only. Releases are only made on an as-needed basis.
End of life	A release that is no longer supported. Users of this release should upgrade as soon as possible, as they may be exposed to unpatched security vulnerabilities.

Figure 1 - EOL Chart

5.2 HIGH FINDINGS

5.2.1 Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Read-Only Path Traversal		
CVE ID(s): CVE-2020-3452	Status: Open	Risk: High
Affected hosts and URL(s): [REDACTED] (unauthenticated)		
Description: Any user on the Internet can exploit this vulnerability to read sensitive data on the Cisco device affected. As a proof of concept, the translation table was downloaded from the device.		
Business Impact: As this is unrestricted access which can be committed globally, users of all skill levels can obtain this information for use in planning nefarious activities in the future.		
Mitigation Strategy Recommendation: Update to the latest version of the appliance software which includes a roll up for this specific vulnerability.		
References: <ul style="list-style-type: none">• https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt03598• https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-asaftd-ro-path-KJuQhB86.html• https://www.rapid7.com/blog/post/2020/07/23/cve-2020-3452-cisco-asa-firepower-read-only-path-traversal-vulnerability-what-you-need-to-know/• https://twitter.com/aboul3la/status/1286012324722155525		
Evidence:		

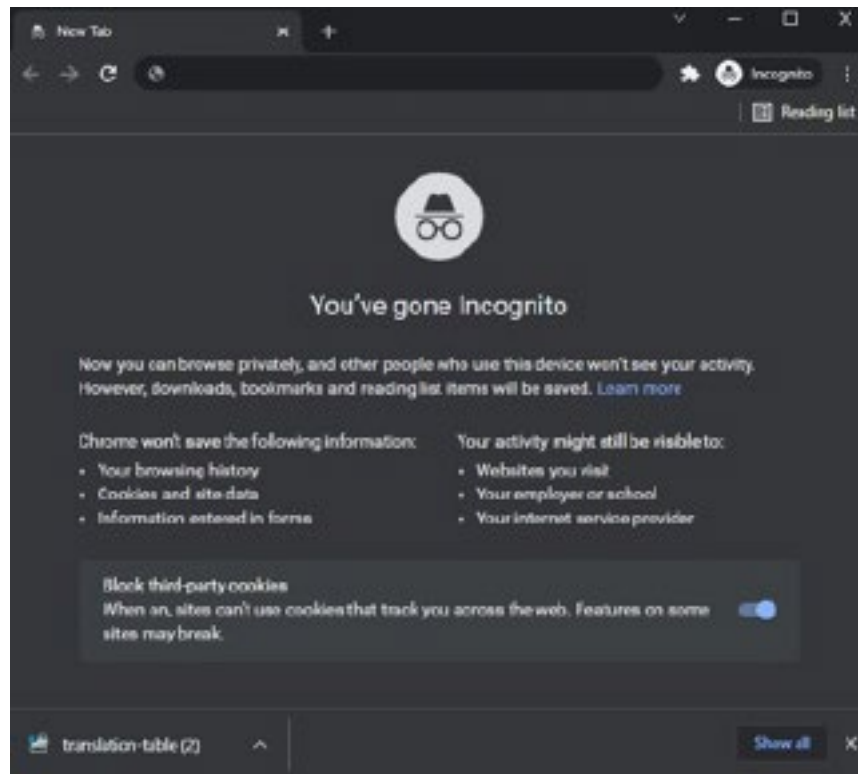


Figure 2 - Unauthenticated download of translation table

```
translation-table (2) - Notepad
File Edit Format View Help
-- Copyright (C) 2006-2018 by Cisco Systems, Inc.
-- Created by otrizna@cisco.com

dofile("/+CSCOE+/include/common.lua")
dofile("/+CSCOE+/include/browser_inc.lua")

local function compare(a,b) return a["order"]<b["order"] end;
function INTERNAL_PASSWORD_ENABLED(name)
    return false;
end

function CONF_VIRTUAL_KEYBOARD(name)
    return false;
end

no_inheritance = false
custom_profile=""
asdm_custom_file = ""

function SetSessionData(index,name,value)

    local f1
    f1=io.open("/sessions/"..index.."/session_data","w")
    if f1 then
        io.set_metadata_int(f1,name,value)
        f1:close()
    end
end
```

Figure 3 - Translation Table


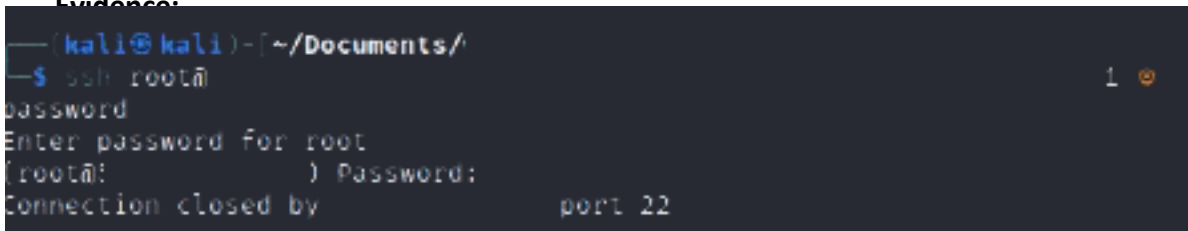
5.2.2 Use of Legacy Encryption Protocols (SSLv3)		
CWE ID(s): 1035, 326	Status: Open	Risk: High
<p>Affected hosts and URL(s):</p> <div></div>		
<p>Description: SSLv3 is an unsupported and programmatically weak encryption protocol. Using SSLv3 increases the attack surface on the hosting target and leaves the target vulnerable to attacks (such as POODLE) which seek to decrypt valid transactions through the manipulation of Oracle Padding.</p>		
<p>Business Impact: If an adversary conducts a successful “man in the middle campaign”, they can reasonably replace the padding with the session cookie block and it can be sent to the server in order to guess the last byte of the session cookie. This begins a process of downgrading the protocol to extract confidential data from the weakly encrypted stream.</p>		
<p>Mitigation Strategy Recommendation: Disable all instances of SSLv3 and associated ciphers. Move towards use of newer protocols (TLS v1.2 and v1.3).</p>		
<p>References:</p> <ul style="list-style-type: none"> https://cwe.mitre.org/data/definitions/326.html https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/ 		
<p>Evidence:</p>  <pre> (kali@kali)-[~] \$ sslls Version: 2.0.11-static OpenSSL 1.1.1n-dev xx XXX xxxx Connected to 130 Testing SSL server on port 443 using SNI name helmet.wpengine.com SSL/TLS Protocols: SSLv2 disabled SSLv3 enabled TLSv1.0 enabled TLSv1.1 enabled TLSv1.2 enabled TLSv1.3 disabled </pre>		

Figure 4 – *SSLv3 detected (SSLSCAN)*

5.2.3 Administrative Console Externally Accessible (Password Authentication Enabled)		
CWE ID(s): 309	Status: Open	Risk: High
<p>Affected hosts and URL(s):</p> <div></div>		
<p>Description: Password authentication is enabled on an externally facing interface (SSH). This access is not restricted by a PKI requirement or through network access control mechanisms.</p> <p>Business Impact: An adversary is able to test an arbitrary amount of passwords against the interface to include that of the root user.</p> <p>Mitigation Strategy Recommendation: Disable password authentication to externally accessible resources. If required to facilitate this method of communication, a trusted PKI certificate in conjunction with MFA should be enabled.</p> <p>References:</p> <ul style="list-style-type: none"> https://cwe.mitre.org/data/definitions/309.html <p>Evidence:</p>  <pre> (kali@kali)~\$ ssh root@ password Enter password for root (root@:) Password: Connection closed by port 22 </pre>		
<p><i>Figure 5 - Attempt to log in as root to SSH interface</i></p>		

5.3 MEDIUM FINDINGS

5.3.1 Use of Legacy Encryption Protocols (TLS 1.0)		
CWE ID(s): 326	Status: Open	Risk: Medium
Affected hosts and URL(s): [REDACTED]		
<p>Description: Weak ciphers and protocols are enabled on the target server. At the time of writing, TLS 1.3 and TLS 1.2 are the strongest protocols for facilitating secure transactions between clients and target servers.</p> <p>Business Impact:</p> <p>Using protocols that are insecure, unsupported, and currently have vulnerabilities can be actively exploited. Combined with weaknesses in their implementations these protocols increase the attack surface of the web application and server. Common attacks degrade the encryption encapsulating customer and user requests leaving overall integrity of communications at risk in man-in-the-middle situations. Exploits (such as Heartbleed), can leak memory directly from server processes without the need for user interaction.</p> <p>Mitigation Strategy Recommendation: It is recommended that these ciphers be disabled and focus be put on bolstering the current implementation of TLS 1.2 across all affected entities.</p>		
<p>References:</p> <ul style="list-style-type: none">• https://cwe.mitre.org/data/definitions/326.html• https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001)• https://www.acunetix.com/vulnerabilities/web/tls-1-0-enabled/		

Evidence:

```
(kali㉿kali)-[~]
$ sslscan .static.ctl.one 1 x
Version: 2.0.11-static
OpenSSL 1.1.1n-dev xx XXX xxxx

Connected to

Testing SSL server .static.ctl.one on port 443 using SNI name
.static.ctl.one

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    enabled
TLSv1.1    enabled
TLSv1.2    enabled
TLSv1.3    disabled
```

Figure 6 - TLS v1.0 detected (SSLSCAN)

5.3.2 Cross Frame Scripting (XFSv2)		
CWE ID(s): 644, 16	Status: Open	Risk: Medium
Affected hosts and URL(s): [REDACTED] [REDACTED] [REDACTED]		

Description: The application server does not have elements such as the X-Frame-Options and X-Content-Type-Options configured within its responses to user requests. As a result, images and resources can be directly referenced by nefarious websites without hinderance.

Key Locations:

- <https://1.1.1.1/Account>
- <https://1.1.1.1/Account/Register>
- <https://1.1.1.1/Account/RetrieveInfo>
- <https://2.2.2.2/account/Register>
- <https://2.2.2.2/account/RetrieveInfo>

Sample Response:

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5

X-UA-Compatible: IE=8
X-AspNetMvc-Version: 3.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET

Date: Sun, 09 Jan 2023 22:57:01 GMT

Connection: close
Content-Length: 6141
```

At the moment, [REDACTED] and [REDACTED] do not have the proper headers to deflect this attack however, inline JavaScript conditioning is passively protecting these sites for the moment.

Figure 7 - JavaScript blocking XFSv2 execution

Business Impact: In its current configuration, adversaries can reference objects (such as images from the site) in phishing campaigns. An example of exploitation would be creating a

site that fully emulates the victim server. All images referenced would be valid, and the site would appear to be real. Users would then be sent emails or communications asking users to “log in” to the respective site. The user could then fall victim to a keylogger and redirected to the actual site without leaving a hint of suspicion.

Mitigation Strategy Recommendation: It is recommended that Test Inc. secure headers across all hosted web services. The following headers, at a minimum, should be appropriately configured:

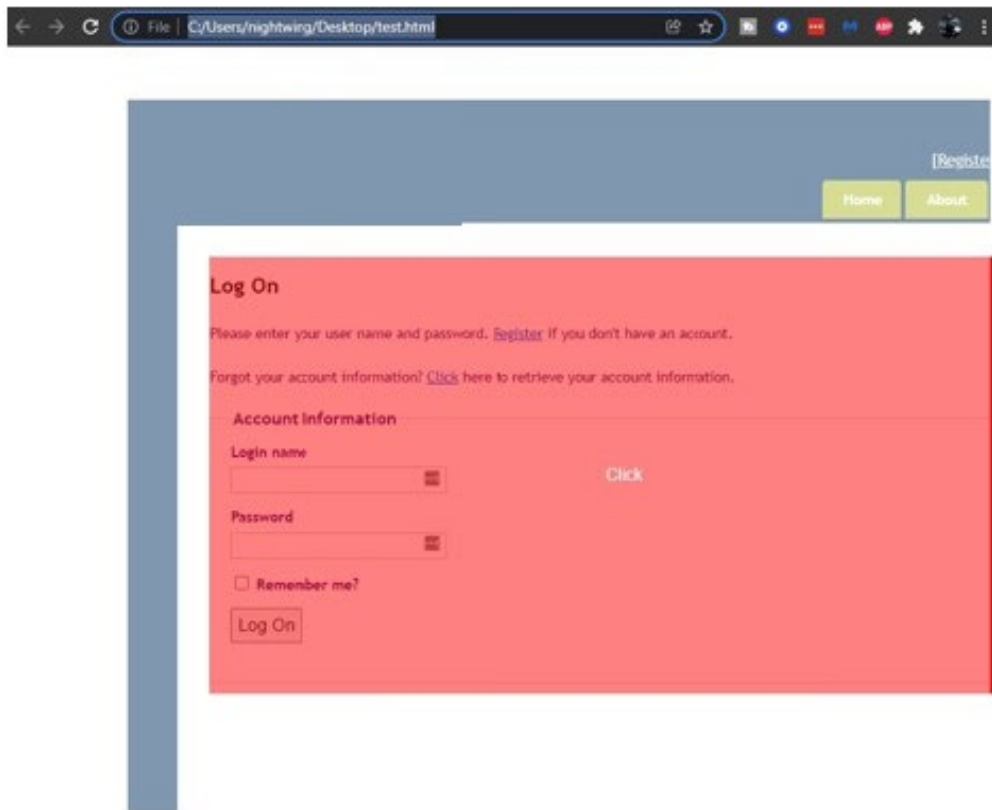
- X-XSS-Protection
- Content-Security-Policy
- Strict-Transport-Security
- Pragma
- Cache-Control
- X-Content-Type-Options
- X-Frame-Options
- Access-Control-Allow-Origin

References:

- https://www.owasp.org/index.php/HTTP_Strict_Transport_Security
- <https://www.veracode.com/blog/2014/03/guidelines-for-setting-security-headers>
- https://owasp.org/www-community/attacks/Cross_Frame_Scripting
- https://www.owasp.org/index.php/OWASP_Secure-Headers_Project

Evidence:

Please see the next page for evidence regarding this finding.



5.3.3 General Patch Management		
CWE ID(s): 1035	Status: Open	Risk: Medium
<p>Affected hosts and URL(s):</p> <div style="background-color: black; height: 1.2em; width: 100%;"></div> <p>10.10.10.10(Host)</p>		
<p>Description: The affected host uses outdated software and services which contain vulnerabilities that could be easily exploited by adversarial forces. The following versions of outdated software were detected during this engagement:</p> <p style="text-align: center;">jQuery</p> <p style="text-align: center;">Detected Version: 1.7.1 Current Version: 3.6.0</p> <p style="text-align: center;">IIS</p> <p>Detected Version: 8.5 Current Version: 10.0.x</p> <p>Business Impact: Use of outdated and unpatched software can not only put the hosting asset at risk but may also put the integrity of customer data at risk.</p>		
<p>Mitigation Strategy Recommendation: Update this software suite to match the up-to-date servers in the enterprise (10.0.x).</p>		
<p style="text-align: center;">References:</p> <ul style="list-style-type: none"> • https://jquery.com/download/ (jQuery) • https://cwe.mitre.org/data/definitions/1035.html • https://snyk.io/vuln/npm:jquery • https://cwe.mitre.org/data/definitions/1035.html • https://techcommunity.microsoft.com/t5/itops-talk-blog/windows-server-101-hardening-iis-via-security-control/ba-p/329979 		
<p>Evidence:</p> <p>10.101.101.10</p>		

Powered-By: ASP.NET

Date: Sun, 09 Jan 2023 22:59:16 GMT

Connection: close
Content-Length: 3844

5.4 LOW FINDINGS

No Low findings were detected during this engagement.

6 CONCLUSION

A Defense in Depth strategy is imperative to the successful implementation of any security program. Test Inc.'s efforts to secure and protect the confidentiality, integrity, and availability of its employee and customer data is demonstrated by the work that has been put into reducing the attack surfaces on its application servers. Many of the vulnerabilities found can be easily remediated and it is recommended that any proposed changes go through Test Inc.'s Change Management process. Regular annual Penetration Testing and Vulnerability Assessments are also recommended as part of the ongoing analysis of the organizations current Continuous Device Monitoring. These efforts will enhance Test Inc.'s continued success in fortifying its enterprise infrastructure.

7 APPENDICES

The following sections serve as supplemental pages of information pertaining to elements of the engagement that may or may not be covered in the initial report.

7.1 APPENDIX A: TOOLS INVENTORY

Listed below is a sample set of the tools that are typically used during engagements. This list is non-exhaustive:

Tool Name	Domain	Description
Burp Suite Professional	Web Application Penetration Testing	<p>Burp Suite Professional is a top tier extensible program which allows penetration testers and network defense agents to conduct dynamic and manual web application testing.</p> <p>For more information, please see the following link: https://portswigger.net/burp</p>
OWASP Zed Attack Proxy (ZAP)	Web Application Penetration Testing	<p>This OWASP project serves to distribute software that can be used to automate the assessing of target vulnerabilities within a web application and server instance.</p> <p>More information can be found here: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project</p>
Cloud Services	Web Application/Network Penetration Testing	<p>General cloud service providers hosted the virtual instances used to harbor harvested data, launch exploits, and maintain reverse handlers.</p>
Domain Registration Services (Google/GoDaddy)	Web Application Penetration Testing	<p>These service providers are a sample of entities that provide domain services. Creation of domains that are similar to that of the target entity is critical to execution of a successful penetration testing or red teaming operation.</p> <p>To purchase domains, please contact the respective vendor:</p> <p>Amazon – https://aws.amazon.com/getting-started/tutorials/get-a-domain/ Google – https://domains.google.com/ GoDaddy - https://www.godaddy.com/domains/domain-name-search</p>
Open VAS	Network Penetration Testing	<p>This tool is open source and can be used to conduct baseline network vulnerability assessments.</p> <p>For more information, please visit: http://www.openvas.org/</p>
NMAP	Network/Web Application Penetration Testing	<p>NMAP serves as a network protocol swiss army exploitation and scanning tool.</p> <p>For more information, please visit: https://nmap.org/</p>

Kali Linux	Web/Network	<p>This suite of offensive security and forensic tools is a must have for penetration testers at all levels. The suite comes pre-compiled for VMware, Virtual Box or use as an ISO.</p> <p>For more information on Kali, please visit the following website: https://www.kali.org/</p>
Manual Testing	All	Experience in various industries and exposure to various application types and vulnerabilities

Table 4 - Sample Pentesting Toolkit

7.2 APPENDIX B: SSL VPN CONCENTRATORS



Figure 11 - VPN Concentrator #2

7.3 APPENDIX C: CRUSH FTP HTTP SERVER

Certain versions of this particular software suite suffer from multiple vulnerabilities to include Cross Site Scripting (XSS) and Remote Code Execution. The following exploits were attempted in the link below and yielded reprimand from perimeter devices:



Figure 12 - Attempt at unauthenticated XSS detected and failed

7.4 APPENDIX D: IIS EXPOSURE

The following assets are still showing the default IIS page on port 80. This gives adversaries an inadvertent confirmation as to a Microsoft Windows Operating System distribution being in use in the environment:

Hostname	Port	Protocol	State	Version
5	80	tcp	open	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
2	80	tcp	open	Microsoft IIS httpd 10.0
1	80	tcp	open	Microsoft IIS httpd 10.0
1	80	tcp	open	Microsoft IIS httpd 10.0
1	80	tcp	open	Microsoft IIS httpd 10.0
1	80	tcp	open	Microsoft IIS httpd 10.0
1	80	tcp	open	Microsoft IIS httpd 10.0

Figure 13 - IIS Servers which expose default page

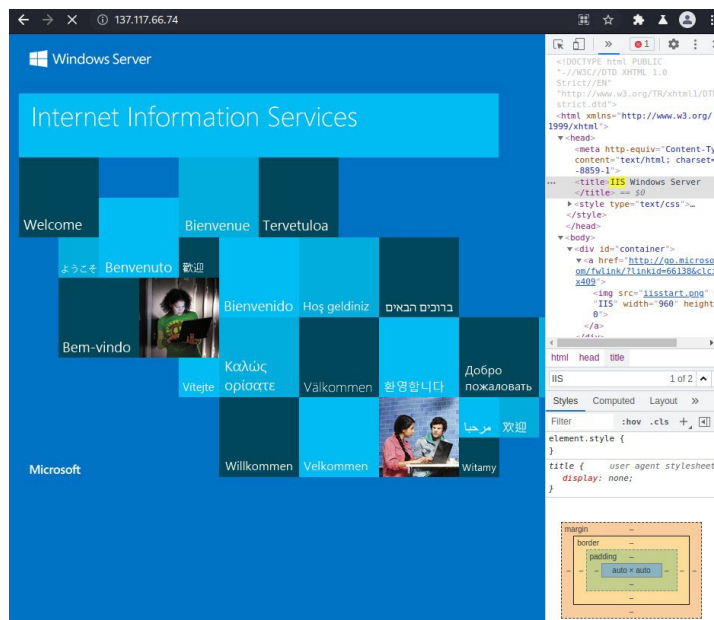


Figure 14 – IIS default page sample

7.5 APPENDIX E: CHECK POINT SECUREMOTEL HOSTNAME DISCLOSURE

Please validate the following result in your environment. Communicating with the port directly did not yield the returned data.

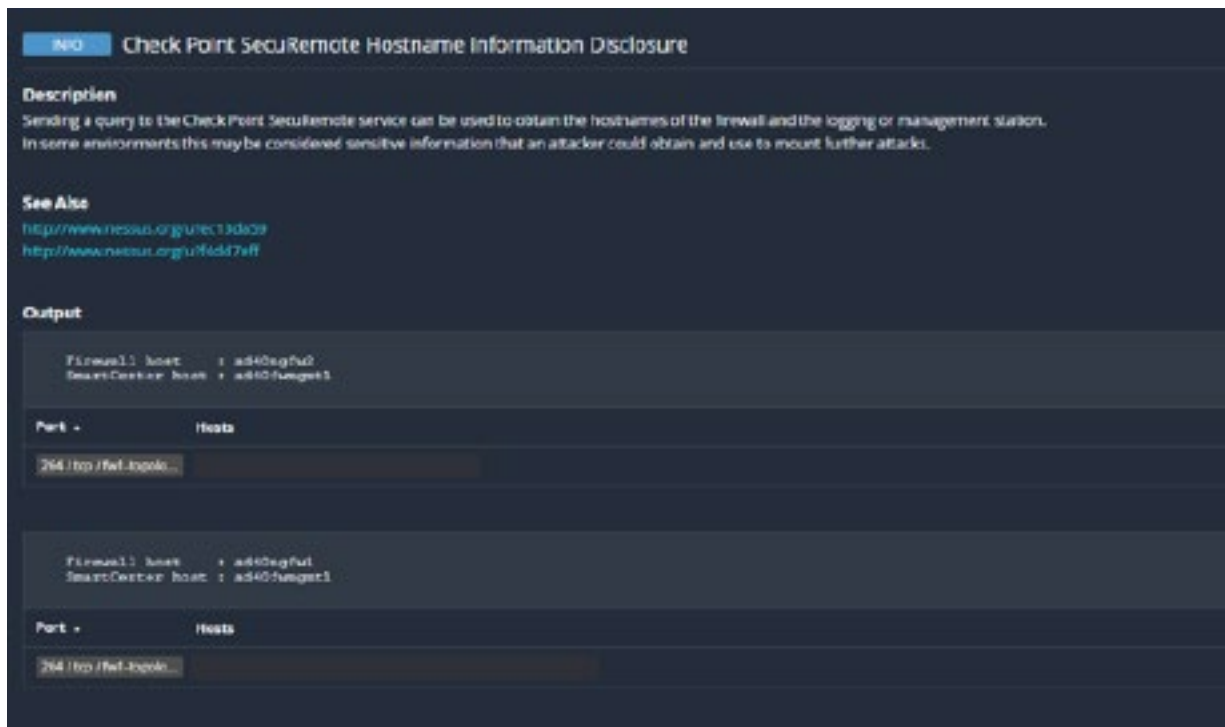


Figure 15 – CheckPoint SecuRemote validation request (Nessus Output)

7.6 APPENDIX F: LOG4J

The LOG4J Plugin was run against the scoped assets and did not yield a positive result for infection.



Figure 16 – Result from Log4J scan (Nessus Output)