PENETRATION TEST REPORT

DATE

Prepared for:

COMPANY

123 Main Street
Knoxville, TN 37932

AVERTIUM

Making Your World a Safer Place

The information contained within this report is considered proprietary and is Confidential Information. Inappropriate and unauthorized disclosure of this report or portions of it could result in significant damage or loss. This report should be distributed to individuals on a Need-to-Know basis only. Paper copies should be locked up when not in use. Electronic copies should be stored offline and protected appropriately.

NOTICE:

This report is subject to the terms of the Master Services Agreement or other master agreement executed by Avertium and the client to which this report is delivered ("MSA") and the SOW or Order that describes the services which resulted in the generation of this report.

COPYRIGHT:

Contact Information

Technical Team Lead
Team Member
Security Analyst
Avertium
1 Data Security Way
Virtual Container, Anywhere USA
(865) 244-3500
secure.data@avertium.com

Technical Services Manager
Team Member
Security Analyst
Avertium
1 Data Security Way
Virtual Container, Anywhere USA
(865) 244-3500
secure.data@avertium.com

Account Manager
Team Member
Account Executive
Avertium
1 Data Security Way
Virtual Container, Anywhere USA
(865) 244-3500
secure.data@avertium.com

Avertium Security Assessment Team

Team Member
Job Title

John Doe is a security analyst for Avertium. His primary role consists of conducting network vulnerability assessments, penetration tests, and web application assessments but also performs firewall configuration audits, wireless assessments, and social engineering engagements. He has more than 10 years of experience in the technical field in roles such as database design, field device support, help desk, IT asset management, programming, and information security.

Certification and Training

John holds a Bachelor of Science in Information Technology with a focus on Information System Security. He has obtained several Global Information Assurance Certifications (GIAC). These certifications include GIAC Security Essentials Certification (GSEC), GIAC Certified Incident Handler (GCIH), and GIAC Certified Intrusion Analyst (GCIA). Additionally, he has completed the Penetration Testing with Kali course and holds a CompTIA A+ certification.

Table of Contents

List of Tables and Figures

Executive Summary

Avertium (assessment team) was contracted by COMPANY Corporation (COMPANY) to complete a network security assessment which involved an external Network Vulnerability Assessment/Penetration Test (NVA/PT) and an internal NVA/PT, and web application assessment. The assessment team was tasked with identifying and verifying vulnerabilities in the information security architecture of the COMPANY network, along with identifying and reporting on enhancements that could improve its overall security posture.

Three (3) phases were employed for this security assessment. The first phase was an external NVA/PT that was completed under a limited knowledge scenario to represent a “hacker’s perspective.” The only information supplied to the assessment team was the target external Internet Protocol (IP) addresses. The second phase of the assessment was an internal NVA/PT completed from an unauthorized user’s perspective. The only information supplied to the assessment team was the target internal IP addresses. The third phase of the assessment was a web application assessment. This phase was completed from both an unauthenticated user’s perspective and an authenticated user’s perspective. Client supplied the assessment team with target Uniform Resource Locators (URLs) and credentials for the authenticated portion of the task.

The assessment team identified a few areas of concern during the assessment. A summary of these concerns is given below:

External NVA

1. One (1) host utilizing an unsupported version of the Windows operating system
2. One (1) host with a vulnerable version of Remote Desktop Protocol (RDP) allowing remote code execution
3. Two (2) Digital Video Recorder (DVR) hosts with default or easily guessed credentials

Internal NVA

1. Four (4) hosts supporting a Microsoft Server Message Block (SMB) service using a vulnerable version
2. Eight (8) hosts utilizing the SMB protocol with packet signing disabled
3. One (1) host running a web server that has reached end-of-life status
4. Thirty-three (33) instances on hosts running a vulnerable version of VMWare's ESXi 4.X operating system
5. Two (2) hosts utilizing a service with a vulnerable version of Microsoft's Schannel security package
6. One (1) host using an unsupported version of Microsoft Internet Information Services (IIS)
7. Three (3) hosts using a vulnerable version of Dropbear Secure Shell (SSH) Server
8. Four (4) hosts utilizing a vulnerable version of Microsoft's Hypertext Transfer Protocol (HTTP) protocol stack
9. Two (2) hosts utilizing an unsupported operating system

Web Application Assessment

1. One (1) application vulnerable to Structured Query Language (SQL) injection
2. Two (2) applications vulnerable to reflected Cross-site Scripting (XSS)
3. One (1) application using an insecure frame
4. One (1) application using an out of date JavaScript library

5. One (1) application found to have directory listing enabled
6. Two (2) applications using Transport Layer Security (TLS) version 1.0

External PT

1. DVR accessed using default credentials allowing for remote live video viewing
2. Code execution on remote host compromising the external network

Internal PT

1. MS17-010 exploited and code executed resulting in remote host compromise
2. Upgrade Windows hosts to a newer operating system
3. Sensitive documents accessed from file shares using recovered credentials
4. Usernames and encrypted passwords intercepted via Broadcast Message Spoofing
5. User account with Domain Administrator privileges are broadcast over the internal network paired with SMB signing disables allows for remote hosts to be compromised using the SMBRelay attack

Web Application PT

1. User information extracted from the application's backend database using SQL injection
2. Files were accessed via directory listing
3. Pop-up alerts were executed with XSS

Based on the identified concerns, the assessment team makes the following recommendations:

External NVA

1. Upgrade host to a supported operating system
2. Restrict access to RDP from the Internet and upgrade host to a supported operating system
3. Restrict access to DVR devices from the Internet and implement complex passwords on accounts

Internal NVA

1. Install Microsoft Security Update indicated in MS17-010
2. Implement mandatory SMB signing on all hosts
3. Upgrade operating system to a supported version
4. Upgrade the hosts to the latest supported version of ESXi
5. Upgrade the hosts to the latest supported version of ESXi
6. Disable SMB Version 1 on hosts and utilize SMB Version 2 and 3
7. Install Microsoft Security Update indicated in MS14-066
8. Upgrade operating system to a supported version
9. Upgrade to latest supported version of Dropbear SSH software
10. Install Microsoft Security Update indicated in MS15-034
11. Upgrade operating systems to supported version

Web Application Assessment

1. Modify code to implement parameterized queries as well as proper input validation
2. Modify code to perform input validation and output encoding on all user input
3. Secure framed content in a sandbox, and disable all unused features
4. Update the affected library to the latest supported version
5. Disable global directory listing
6. Disable support for TLS version 1.0 and only support TLS 1.1 or higher instead

External PT

1. Restrict access to DVR devices from the Internet and implement complex passwords on accounts
2. Restrict access to RDP from the Internet and upgrade host to a supported operating system

Internal PT

1. Install Microsoft Security Update indicated in MS17-010
2. Upgrade hosts to a newer Windows operating system
3. Analyze the data stored on the network to ensure documents containing sensitive data are properly disposed of or encrypted
4. Reduce the number of NBNS/LLMNR messages
5. Enable and enforce SMB packet signing

Web Application PT

1. Modify code to implement parameterized queries as well as proper input validation
2. Disable global directory listing
3. Modify code to perform input validation and output encoding on all user input

Correct implementation of the recommendations contained in this report and the recommendations found in the documents listed in Appendix B, along with continued diligence on the part of COMPANY administrators, will result in an improved security posture. It should be noted that the data included within this report represents only a snapshot in time. Best practice recommends periodic security assessments are conducted.

1 Introduction

1.1 Overview

Avertium (assessment team) was contracted by COMPANY Corporation (COMPANY) to complete a network security assessment which involved an external Network Vulnerability Assessment/Penetration Test (NVA/PT), an internal NVA/PT, and a web application assessment. The assessment team was tasked with identifying and verifying vulnerabilities in the information security architecture of the COMPANY network along with identifying and reporting on enhancements that could improve its overall security posture.

Two (2) phases were employed for this security assessment. The first phase was an external NVA/PT that was completed under a limited knowledge scenario to represent a “hacker’s perspective.” The only information supplied to the assessment team was the target external Internet Protocol (IP) addresses. The second phase of the assessment was an internal NVA/PT completed from an unauthorized user’s perspective. The only information supplied to the assessment team was the target internal IP addresses.

1.2 Purpose and Scope

The assessment team was tasked to identify and verify vulnerabilities in the information security architecture of the evaluated network and along with identifying and reporting on enhancements that could improve their overall security. This security testing effort was conducted with emphasis on the actual state of the systems examined and not simply the adequacy of any supporting documentation.

Two (2) phases were employed for this security assessment. The first phase was an external NVA/PT that was completed under a limited knowledge scenario to represent a “hacker’s perspective.” The only information supplied to the assessment team was the target external Internet Protocol (IP) addresses. The second phase of the assessment was an internal NVA/PT completed from an unauthorized user’s perspective. The only information supplied to the assessment team was the target internal IP addresses.

Phase 1:External NVA/PT – With respect to Phase 1, the external NVA/PT, all testing was completed from Avertium headquarters in Knoxville, Tennessee, between December 1, 2017 and December 15, 2017. The source IP addresses used by the assessment team were in the 169.130.146.48/28 and 205.232.71.80/28 address ranges. Table 1 contains the provided target external IP address.

Table 1: Target External IP Address

192.168.20.100

Phase 2: Internal NVA/PT – With respect to Phase 2, the internal NVA/PT, all testing was completed using a system connected to the COMPANY network at its location in Knoxville, TN between December 1, 2017 and December 15, 2017. The assessment team's internal IP address used during testing was 10.10.200.5. Table 2 contains the provided target internal IP address range.

Table 2: Target Internal IP Address

10.10.200.0/24

Phase 2: Internal NVA/PT – With respect to Phase 3, the web application assessment, all testing was completed from Avertium headquarters in Knoxville, Tennessee, between December 1, 2017 and December 15, 2017. The source IP addresses used by the assessment team were in the 169.130.146.48/28 and 205.232.71.80/28 address ranges. contains the provided target URLs.

Table 3: Target Web Application URLs

https://mysite.com	https://yoursite.com

1.3 Methodology

Avertium has developed an assessment testing methodology that has been adapted to both commercial and government environments with very effective results. The objective of a security assessment is to examine the subsystems, components, and security mechanisms composing the network infrastructure and identify weaknesses. To that end, the security testing approach for an **external or internal network vulnerability assessment and penetration test** consists of eight key stages:

Security Architecture Review – Supporting system architecture and design documentation for the target system is reviewed for the purpose of identifying network entry/exit points, information flows, and security mechanisms. This review assists in threat identification, vulnerability test construction and development of penetration profiles, determining network test points, and the scope of network boundaries to be included in testing. This step may be bypassed during "zero knowledge" approaches.

Vulnerability Analysis Test Plan – Prior to testing, a test plan may be written to document the strategy for testing activities specific to the environment. The test plan includes a categorical presentation of security checks to be performed, identification of key systems, networks, and devices to be tested, identification of automated tools to be used in the tests, and manual test procedures.

Network Mapping and Data Collection – This activity is concerned with the collection of data regarding standard network devices, protocols, and services. The tools and techniques applied are designed to not affect normal computer and network operations. Computer and network related information to be collected includes:

Host discovery scan - Avertium uses an eight-pass methodology to discover IP addressable devices. The first pass is an ICMP echo-request. The other paths are focused TCP/SYN scans, targeting the most common TCP ports used. This allows the consulting team to find nearly 100% of the IP addressable devices. Those devices that do not respond or those that are prevented from responding (behind firewalls, transparent devices, etc.) to ICMP echo-requests will usually respond to requests to initiate a session on a port that they have open. On the other hand, devices that are not running any of the 30 most common services may still respond to ICMP echo-requests. The unique combination of devices gathered using this technique will represent a snapshot of the IP addressable devices in scope. There may be other devices on the network that will not be accounted for. Devices that are configured to only respond to particular IP addresses for instance, will not respond to any of the consulting team's queries. Obviously, devices not connected to the network at the time of testing, or are powered down will not be included in the final report of discovery. The output of this scan will be included as an appendix to the main report.

- Service scanning (port scanning)
- Banner checking
- Operating system identification and version information
- Device data (e.g., SNMP information)
- File sharing information (e.g., NFS and SMB/CIFS shares)
- Accounts, passwords, security and auditing policies
- IP addresses (active and inactive)
- DNS zone information
- Identification of trust relationships
- Routing information (e.g., RIP)

Threat Model Identification – Before conducting vulnerability assessment and penetration testing activities, identification of threat models is required. Information gathered from the security architecture review and data collection stages can be useful in determining the most likely threats to a network. Common threat models are frequently based on: external malicious users (hackers), external semi-trusted users (Internet banking customers), and internal (trusted) users. Threat models then guide security-testing activities based on the likelihood of an attack and help in assessing the risk/severity of the vulnerabilities. In addition, the threats and vulnerabilities experienced by the client in the last 12 months will be considered.

Vulnerability Identification – The vulnerability identification stage of testing includes targeting specific host and network facilities for exposure to security weaknesses (i.e., exploitation of vulnerabilities). During this stage, both automated tools and manual methods are used to catalog network and system vulnerabilities against available vulnerability databases. Sources of these vulnerability databases include, but are not limited to, open sources such as CERT, NVD, OSVDB, BugTraq, and hacker channels. In addition, Avertium will perform a limited vulnerability assessment of any Web applications discovered, including the following categories:

- XSS (Cross Site Scripting)
- SQL Injection
- Default Usernames/Passwords

- Directory Traversal
- Clients Apps (downloads) that can be decompiled/reverse engineered to gain access to systems

Penetration Testing – The goal of penetration testing is to determine if the protective controls of a given system can be bypassed. At this stage of testing, attempts are made to circumvent security controls by devising penetration profiles using acquired target information and vulnerability identification results. The penetration tests are conducted using information collected during the network mapping and data collection stage and from the review of the system architecture documentation. Penetration profiles are devised for the target system based on the security architecture review and vulnerability identification results. With successful penetrations, Avertium will purposefully leave behind the forensic evidence of a system break-in (compromise) or provide alternate evidence.

Network Segmentation Testing – Segmentation testing is conducted to confirm the needed isolation between subnets/networks. Network segmentation is evaluated from the perspective of a normal user outside of the segment of concern. The client provides the assessment team with the target IP address ranges used within the segment of concern and/or the applicable firewall configurations. This assessment ensures systems that store, process, or transmit sensitive data are isolated from those that do not.

Analysis and Reporting – Test results are analyzed and incorporated into a report addressing the vulnerabilities present in the network, network devices, and specific systems. The potential impact of vulnerability will be discussed and may be used as input for further risk analyses. In addition to describing the security posture of the network, the report will provide recommendations for safeguarding systems to ensure continued secure operations including tools, policies, procedures, and information sources.

Vulnerability Reporting Tool (Gauntlet) – Because we use multiple scanning tools in our testing methodology, Avertium developed a unique reporting tool to correlate information from various network scanning tools to provide a common vulnerability description and severity rating.

1.4 Document Overview

Section 2, Assessment Findings, includes details concerning the vulnerabilities identified during this testing effort, as well as recommendations. Section 3, Conclusions, provides a summary of the recommendations contained in the body of the report.

2 Assessment Findings

2.1 Overview

This section discusses the vulnerabilities and areas of concern discovered during the Client security assessment. The first section, titled *Summary of Findings*, provides a concise list of the most severe vulnerabilities and areas of concern identified during the assessment. Following the *Summary of Findings*, the remainder of Section 2 is divided into three (3) major parts: *External NVA/PT, Internal NVA/PT, and Web Application Assessment.*

2.2 Summary of Findings

The assessment team identified a few areas of concern during the assessment. A summary of these concerns is given below:

External NVA

1. One (1) host utilizing an unsupported version of the Windows operating system
2. One (1) host with a vulnerable version of Remote Desktop Protocol (RDP) allowing remote code execution
3. Two (2) Digital Video Recorder (DVR) hosts with default or easily guessed credentials

Internal NVA

1. Four (4) hosts supporting a Microsoft Server Message Block (SMB) service using a vulnerable version
2. Eight (8) hosts utilizing the SMB protocol with packet signing disabled
3. One (1) host running a web server that has reached end-of-life status
4. Thirty-three (33) instances on hosts running a vulnerable version of VMWare's ESXi 4.X operating system
5. Two (2) hosts utilizing a service with a vulnerable version of Microsoft's Schannel security package
6. One (1) host using an unsupported version of Microsoft Internet Information Services (IIS)
7. Three (3) hosts using a vulnerable version of Dropbear Secure Shell (SSH) Server
8. Four (4) hosts utilizing a vulnerable version of Microsoft's Hypertext Transfer Protocol (HTTP) protocol stack
9. Two (2) hosts utilizing an unsupported operating system

Web Application Assessment

1. One (1) application vulnerable to Structured Query Language (SQL) injection
2. Two (2) applications vulnerable to reflected Cross-site Scripting (XSS)
3. One (1) application using an insecure frame
4. One (1) application using an out of date JavaScript library
5. One (1) application found to have directory listing enabled
6. Two (2) applications using Transport Layer Security (TLS) version 1.0

External PT

1. DVR accessed using default credentials allowing for live video viewing across the Internet

2. Code execution on remote host compromising the external network

Internal PT

1. MS17-010 exploited and code executed resulting in remote host compromise
2. Plain text credentials for COMPANY\Administrator extracted from a compromised host resulting in total compromise of the COMPANY Windows domain
3. Sensitive documents accessed from file shares using recovered credentials
4. Usernames and encrypted passwords intercepted via Broadcast Message Spoofing
5. User account with Domain Administrator privileges are broadcast over the internal network paired with SMB signing disables allows for remote hosts to be compromised using the SMBRelay attack

Web Application PT

1. User information extracted from the application's backend database using SQL injection
2. Files were accessed via directory listing
3. Pop-up alerts were executed with XSS

Detailed information about the findings from the assessment can be found in the following sections.

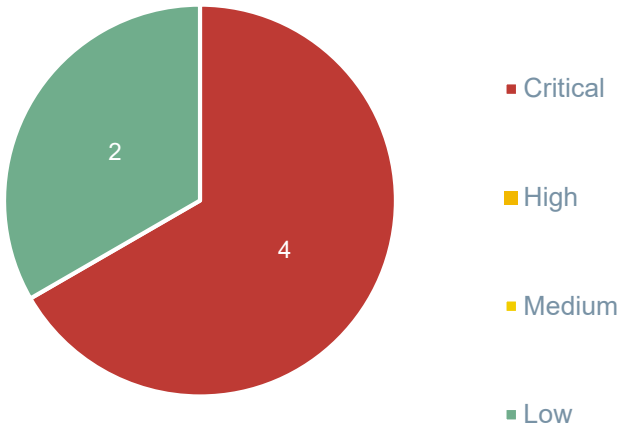
2.3 External NVA/PT

Initial scans against the target IP addresses produced a list of one (1) interesting (i.e. had at least one open port accessible from the Internet) host to examine for the external assessment (refer to Appendix D).

2.3.1 External NVA Findings

The scan results identified four (4) critical-severity, zero (0) high-severity, zero (0) medium-severity, and two (2) low-severity vulnerabilities as shown in Figure 1 below.

Figure 1: External Vulnerabilities by Severity



A ***complete*** and detailed listing of the vulnerabilities identified during the external NVA can be found in the external vulnerability documents referenced in Appendix B - Supporting Documents. ***Some*** of the more severe vulnerabilities identified by the assessment team are detailed in the following sections

2.3.1.1 Default or Easily Guessed DVR Credentials (CVSS: 9.4 - Critical)

The assessment team identified two (2) hosts (192.168.20.100:81/tcp and 192.168.20.100:82/tcp) with default or easily guessed credentials. The DVR device allowed full management access using a default or easily guessed password. Access to the device allowed for viewing of live and recorded video data. Access to live video can allow an attacker to accomplish surveillance and gather information. Access to stored video data can allow an attacker to delete video that would otherwise lead to proof of physical access by attacker. Some DVR systems can also allow the attacker to gain full system access to device and pivot into an internal network.

The assessment team recommends changing username and password credentials to non-default complex values of at least sixteen (16) characters in length. If external or Internet access is required to system, recommend restricting with VPN technology.

2.3.1.2 Remote Desktop Protocol Remote Code Execution Vulnerability (CVSS: 10.0 - Critical)

The assessment team identified one (1) host (192.168.20.100:1/tcp) with a vulnerable version of RDP allowing remote code execution. A remote code execution vulnerability exists in how RDP handles requests if the RDP server has Smart Card authentication enabled. An unauthenticated, remote attacker can exploit this, via a specially crafted application, to execute arbitrary code with full user privileges.

The assessment team recommends updating the operating system to a supported version. Microsoft has provided security updates for older Operating System versions as a work around if needed. If systems can't be updated, ensure access to host from Internet is disabled.

2.3.1.3 Unsupported Operating System (CVSS: 8.3 - Critical)

The assessment team identified one (1) host (192.168.20.100:1/tcp) utilizing an unsupported operating system. The installed operating system is Windows Server 2003 R2 (refer to Figure 2). Support for this operating system ended on July 14, 2015. Unsupported operating systems do not receive updates or security patches. This leaves the affected host indefinitely vulnerable to attacks identified after the end-of-life date.

Figure 2: Unsupported OS

The assessment team recommends the affected host be upgraded to a supported operating system.

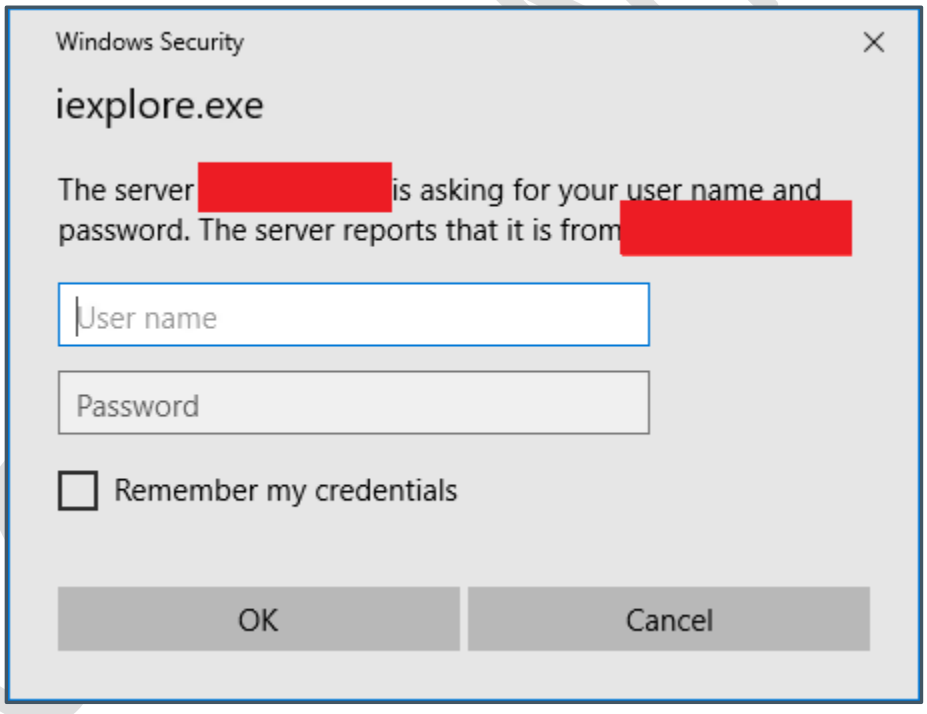
2.3.2 External PT Findings

The assessment team conducted a penetration test against the target external network. During this PT, the assessment team attempted to leverage the vulnerabilities discovered during the external NVA to exploit vulnerable systems, obtain sensitive information, and generally mimic the actions of an attacker with a targeted motivation to compromise the network.

2.3.2.1 Default Credentials on DVR System

The assessment team identified two (2) DVR systems running on 192.168.20.100:1/tcp and 192.168.20.100:82/tcp. The assessment team browsed to the two (2) services with a standard web browser and were prompted for a username and password. The login prompt provided the model number for the DVR system. The model number provided the information the assessment team needed to research default credentials (refer to Figure 3).

Figure 3: Login Prompt on DVR



The assessment team was able to login to the DVR system with default admin credentials and access live video (refer to Figure 4) as well as stored video. With full admin access, the assessment team had access to erase all stored video content (refer to Figure 5).

Figure 4: Live Video

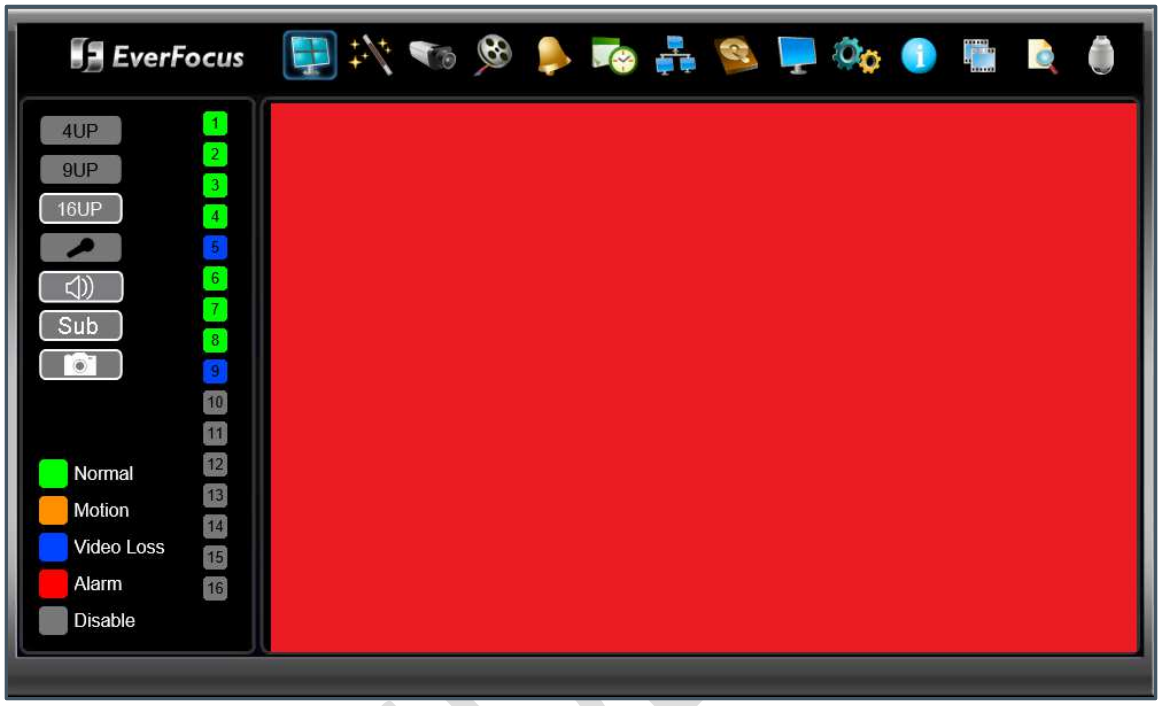
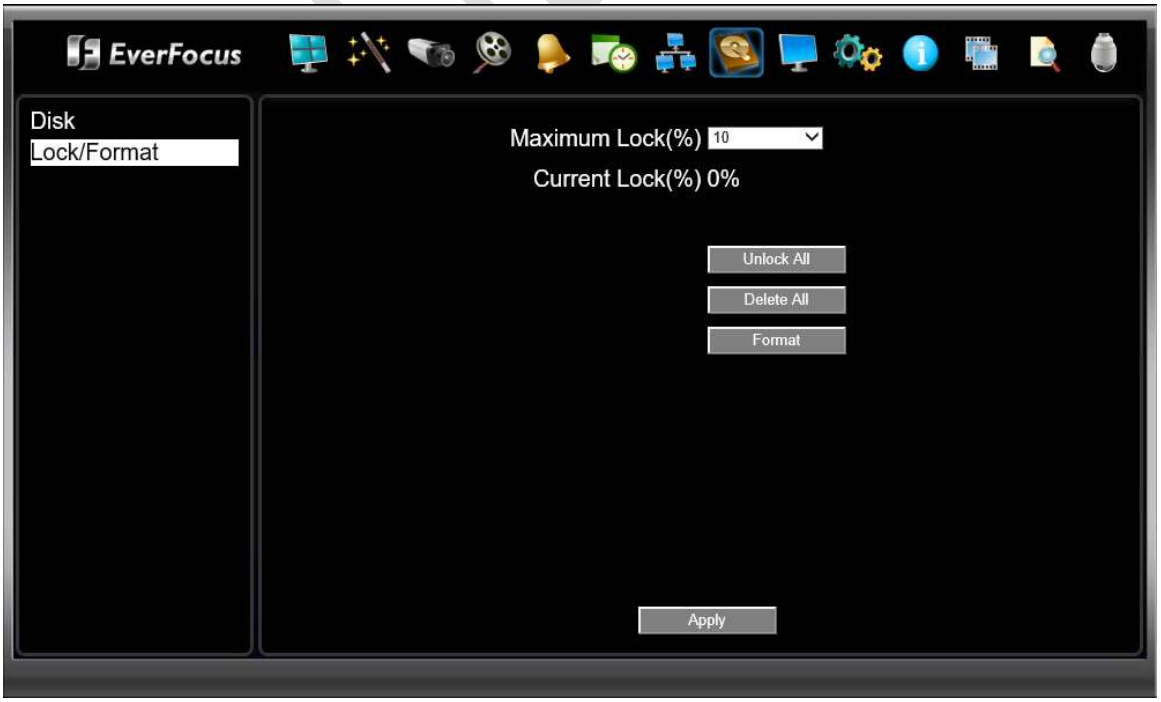


Figure 5: Video Data Erase Screen



The assessment team recommends changing username and password credentials to non-default complex values of at least sixteen (16) characters in length. If external or Internet access is required to system, recommend restricting with VPN technology.

2.3.2.2 Remote Code Execution on Server 2003 via Vulnerable Remote Desktop Protocol

The assessment team identified a host (192.168.20.100:1/tcp) with a vulnerable version of RDP. The vulnerable host was running Windows Server 2003, an end of life operating system from Microsoft. The assessment team utilized publicly available tools to exploit the system and accomplish remote code execution. Figure 6 provides output of a session received from 192.168.20.100 after exploitation. Figure 6 also shows an output of processes that were currently running at the time. The assessment team would typically provide an output identifying the IP address of the host, but in this case, the system became unstable shortly after compromise. Further exploit of the system was not accomplished due to potential instability of the system.

Figure 6: Remote Access Shell

```
[-] Handler failed to bind to [redacted]:443:-  -
[*] Started reverse TCP handle[redacted]443
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to [redacted]
[*] Meterpreter session 4 opened ([redacted] at 2017-08-10 11:17:09 -0400

meterpreter > ps

Process List
============

 PID   PPID  Name                          Arch  Session  User                          Path
 ---   ----  ----                          ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                        x64   0        NT AUTHORITY\SYSTEM
 304   4     smss.exe                      x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 344   652   wmiprvse.exe                  x64   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\wbem\wmiprvse.exe
 352   304   csrss.exe                     x64   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
```

NOTE: This exploit was accomplished via the Internet. This means that an attacker from anywhere in the world could have exploited this vulnerability previously. The assessment team recommends inquiring with Avertium about performing a Data Breach Threat Analysis (DBTA) to ensure the existing environment has not been compromised or is in the process of being compromised.

The assessment team recommends updating the operating system to a supported version. Microsoft has provided security updates for older Operating System versions as a work around if needed. If systems can't be updated, ensure access to host from Internet is disabled.

2.3.3 Post Penetration Cleanup

The assessment team recommends rebooting host 192.168.20.1 to clear memory resident exploit code used by the assessment team.

2.3.4 Testing Limitations

There were no limitations for the external phase of the assessment.

2.3.5 Tools

The assessment team utilized various commercial and open source tools to scan the external hosts for vulnerabilities and attempted to exploit identified vulnerabilities. Tools used include:

- Nessus Vulnerability Scanner
- NMAP
- OpenSSL
- Web Browsers (Internet Explorer, Firefox, Chrome)

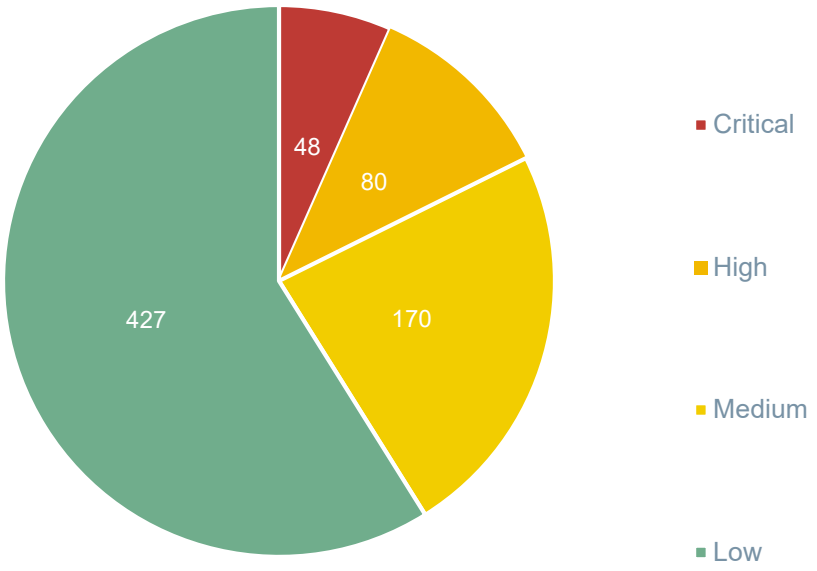
2.4 Internal NVA/PT

Initial scans against the target IP addresses produced a list of eighty-three (83) interesting (i.e. had at least one open port accessible on the network) hosts to examine for the internal assessment (refer to Appendix E).

2.4.1 Internal NVA Findings

The scan results identified forty-eight (48) critical-severity, eighty (80) high-severity, one-hundred seventy (170) medium-severity, and four-hundred twenty-seven (427) low-severity vulnerabilities as shown in Figure 7 below.

Figure 7: Remote Access Shell



A ***complete*** and detailed listing of the vulnerabilities identified during the internal NVA can be found in the internal vulnerability documents referenced in Appendix B - Supporting Documents. ***Some*** of the more severe vulnerabilities identified by the assessment team are detailed in the following sections.

2.4.1.1 Security Update for Windows SMB Version 1 Service (MS17-010) (CVSS: 9.3 - Critical)

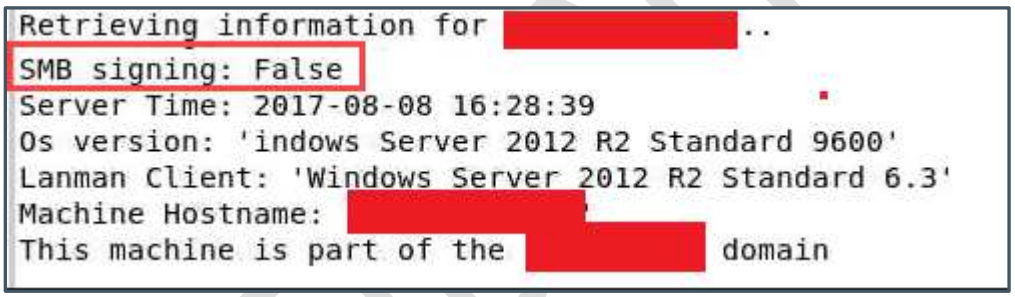
The assessment team identified four (4) hosts (10.10.200.1:1/tcp, 10.10.200.4:2/tcp, 10.10.200.44:3/tcp, and 10.10.200.55:4/tcp) supporting a Microsoft SMB service using a vulnerable version. The vulnerability occurs due to the way SMB version 1 handles specially crafted requests. This could allow code execution if an attacker sends specially crafted packets to the affected server.

The assessment team recommends ensuring that the patch identified in Microsoft security bulletin MS17-010 has been applied.

2.4.1.2 SMB Packet Signing Disabled (CVSS: 5.0 - Critical)

The assessment team identified eight (8) hosts (refer to Table 3) utilizing the SMB protocol with packet signing disabled (refer to Figure 8). Packet signing ensures messages between the client and server are authentic. When packet signing is disabled, SMB packets can be modified in-transit to facilitate man-in-the-middle attacks.

Figure 8: SMB Signing Disabled



The assessment team recommends the affected hosts be configured to always use SMB packet signing.

Table 4: Hosts with SMB Packet Signing Disabled

10.10.200.1:1/tcp	10.10.200.34:1/tcp	10.10.200.3:1/tcp	10.10.200.42:1/tcp
10.10.200.44:1/tcp	10.10.200.53:1/tcp	10.10.200.55:1/tcp	10.10.200.57:1/tcp

2.4.1.3 End-of-Life Web Server Status (CVSS: 8.3 - High)

The assessment team identified one (1) host (10.10.200.1:1/tcp) running a web server that has reached end-of-life status. The installed version is Microsoft IIS 5.1 and ended support on April 8, 2014. The affected web server service will no longer receive updates that mitigate security flaws or vulnerabilities. Attackers continue to find new flaws and develop exploits for older software versions. Using end-of-life web software puts hosts at a greater risk than those that will receive security patches if a new flaw is found.

The assessment team recommends that administrators upgrade the operating system to a supported version, which will also update the web service to a supported version.

2.4.1.4 VMware ESXi 4.X Multiple Vulnerabilities (High)

The assessment team identified Thirty-three (33) instances on hosts running a vulnerable version of VMWare's ESXi operating system. There are many known vulnerabilities ranging from denial of service to arbitrary code execution (refer to Table 4). Reference the supporting documentation for a detailed list of the common vulnerability and exposures (CVEs) for the hosts.

The assessment team recommends that the affected hosts be upgraded to the latest supported version of ESXi. Additionally, installing the patches from VMware will mitigate the identified vulnerabilities.

Table 5: VMware ESXi 4.X Vulnerabilities

Severity	CVSS	Vulnerability	Affected Hosts
High	10.0	VMware ESX / ESXi NFC and Third-Party Libraries Multiple Vulnerabilities (VMSA-2013-0003) (remote check)	2
High	7.9	VMware ESX / ESXi Guest OS Local Privilege Escalation (VMSA-2013-0014) (remote check)	2
High	10.0	VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2013-0012) (remote check)	2
High	9.3	VMware ESX / ESXi vSphere Client RCE (VMSA-2014-0003)	2
High	10.0	VMware ESX / ESXi Third-Party Libraries Multiple Vulnerabilities (VMSA-2011-0013) (remote check)	2
High	8.5	VMware ESX Multiple Vulnerabilities (VMSA-2010-0013) (remote check)	1
High	10.0	VMware ESX Multiple Vulnerabilities (VMSA-2010-0015) (remote check)	1
High	7.2	VMware ESX Privilege Escalation (VMSA-2010-0017) (remote check)	1
High	7.2	VMware ESX / ESXi Tools Update Privilege Escalation (VMSA-2010-0018) (remote check)	1
High	10.0	VMware ESX / ESXi Authentication Service and Third-Party Libraries Multiple Vulnerabilities (VMSA-2013-0001) (remote check)	2
High	7.2	VMware ESX / ESXi Third-Party Libraries Multiple Vulnerabilities (VMSA-2011-0004) (remote check)	2
High	10.0	VMware ESX / ESXi Third-Party Libraries Multiple Vulnerabilities (VMSA-2011-0003) (remote check)	1
High	9.3	VMware ESX / ESXi libxml2 Multiple Vulnerabilities (VMSA-2012-0012) (remote check)	2

High	7.2	VMware ESX / ESXi VMCI Privilege Escalation (VMSA-2013-0002) (remote check)	2
Medium	4.4	VMware ESX / ESXi Arbitrary File Modification (VMSA-2013-0016) (remote check)	2
Medium	6.8	VMware ESX / ESXi libxml2 RCE (VMSA-2013-0004) (remote check)	2
Medium	7.8	VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2011-0007) (remote check)	2
Medium	6.9	VMware ESX / ESXi Third-Party Libraries Multiple Vulnerabilities (VMSA-2013-0009) (remote check)	2
Medium	7.5	VMware ESX Multiple Vulnerabilities (VMSA-2010-0019) (remote check)	2

2.4.1.5 Microsoft Schannel Improper Packet Processing (MS14-066) (CVSS: 10.0 - High)

The assessment team identified two (2) hosts (10.10.200.1:1/tcp and 10.10.200. 5:1/tcp) utilizing a service with a vulnerable version of Microsoft's Schannel security package. Schannel is used with Microsoft products to provide authentication and to secure private communication through encryption. This vulnerability is due to Schannel improperly handling specially crafted packets. A remote unauthenticated attacker could execute code on an affected host by sending a specially crafted packet, potentially leading to a complete compromise. It is important to note that at the time of the assessment, exploit code is not publicly available.

The assessment team recommends ensuring that the patch identified in Microsoft security bulletin MS14-066 has been applied.

2.4.1.6 Microsoft Unsupported Version Detection (CVSS: 8.3 - High)

The assessment team identified one (1) host (10.10.200.3:1/tcp) using an unsupported version of Microsoft IIS. Support for Microsoft IIS version 6 ended July 14, 2015. The affected operating system will no longer receive updates that mitigate security flaws or vulnerabilities. Attackers continue to find new flaws and develop exploits for older operating systems. Using end-of-life applications puts hosts at a greater risk than those that will receive security patches if a new flaw is found.

The assessment team recommends that affected systems be upgraded to a supported operating system.

2.4.1.7 Dropbear SSH Multiple Vulnerabilities (CVSS: 10.0 - High)

The assessment team identified three (3) hosts (10.10.200. 8:1/tcp, 10.10.200.9:22/tcp, and 10.10.200.110:1/tcp) using a vulnerable version of Dropbear SSH server. The installed version of Dropbear SSH was identified as being out-of-date and is possibly vulnerable to authentication bypass attacks and arbitrary code execution. Reference the supporting documentation for a full list of the Common Vulnerabilities and Exposures (CVEs) for this version of Dropbear SSH. The assessment team recommends upgrading to the latest supported version of Dropbear SSH or contacting the vendor for fix.

2.4.1.8 Microsoft HTTP.sys Improper Packet Processing (MS15-034) (CVSS: 10.0 - High)

The assessment team identified four (4) instances on hosts (10.10.200.1:1/tcp, 10.10.200.2:2/tcp, 10.10.200.3:1/tcp, and 10.10.200.4:1/tcp) utilizing a vulnerable version of Microsoft's HTTP protocol stack. The protocol stack found in HTTP.sys improperly parses packets, potentially leading to remote code execution. Microsoft has assigned this vulnerability a severity rating of critical. An attacker can craft a packet to exploit this vulnerability and subsequently compromise the host.

The assessment team recommends installing the patch identified in the Microsoft Security Bulletin MS15-034.

2.4.1.9 Unsupported Operating System (High)

The assessment team identified two (2) hosts (10.10.200.1 and 10.10.200.2) utilizing an unsupported operating system. Refer to Table 7 for the list of unsupported operating systems discovered. Unsupported operating systems do not receive updates or security patches. This leaves the affected hosts indefinitely vulnerable to attacks identified after the end-of-life date.

The assessment team recommends that the affected hosts be upgraded to a supported operating system.

Table 6: Unsupported Operating Systems

Severity	CVSS	Vulnerability	Affected Hosts
High	8.3	Unsupported Linux/Unix Operating System	10.10.200.1
High	8.3	Microsoft Windows Server 2003 End-of-Life Status	10.10.200.2

2.4.2 Internal PT Findings

The assessment team conducted a penetration test against the target internal network. During this PT, the assessment team attempted to leverage the vulnerabilities discovered during the internal NVA to exploit vulnerable systems, obtain sensitive information, and generally mimic the actions of an attacker with a targeted motivation to compromise the network.

2.4.2.1 Initial Compromise of COMPANY Domain

The assessment team identified that 10.10.200.2 was running an unsupported operating system and was vulnerable (refer to section 2.4.1.1) to an SMB Version 1 exploit titled “Eternalromance.” The assessment team was able exploit the system (refer to Figure 9) and gain full system access (refer to Figure 10).

Figure 9: Eternalromance Exploit

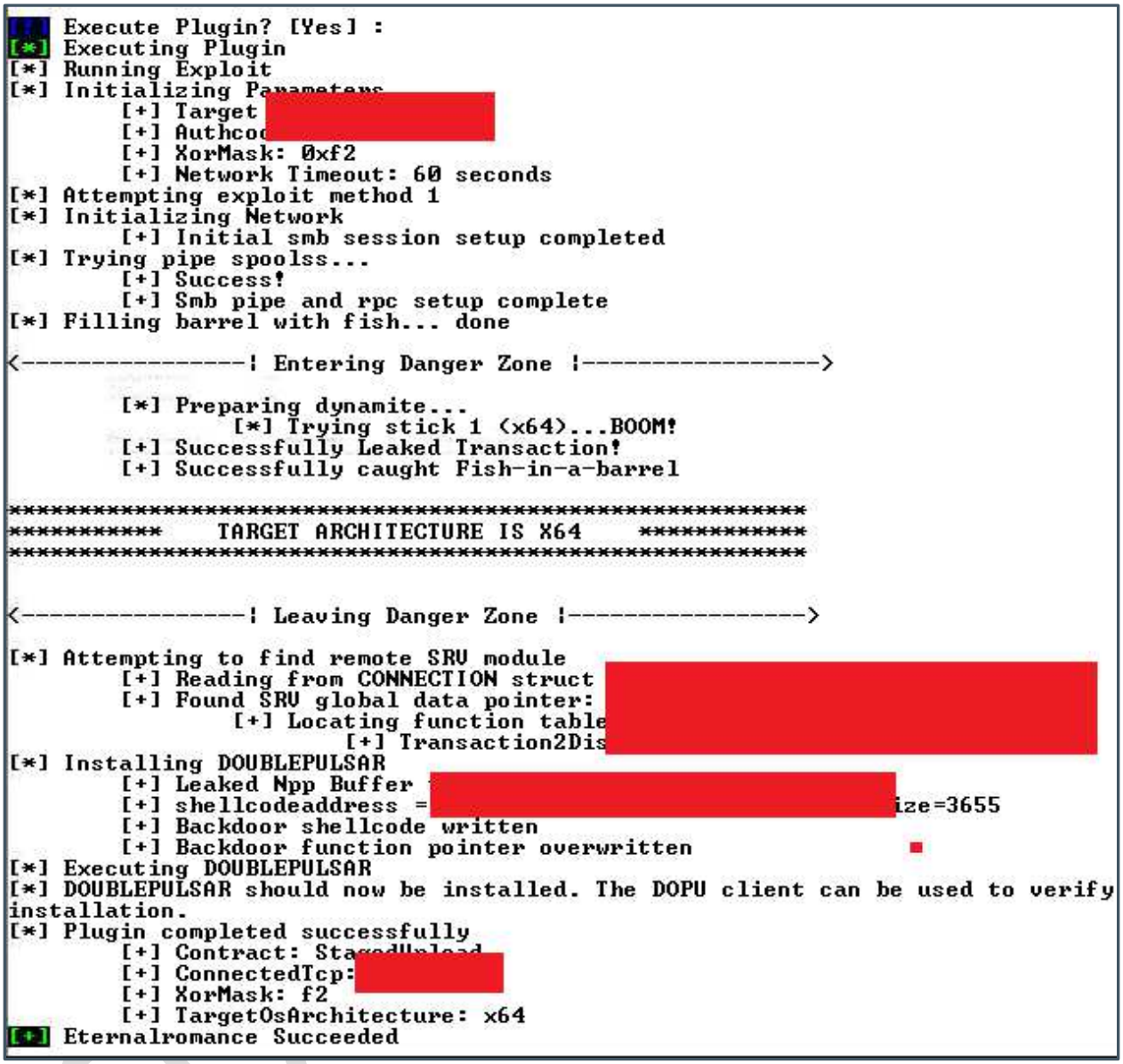
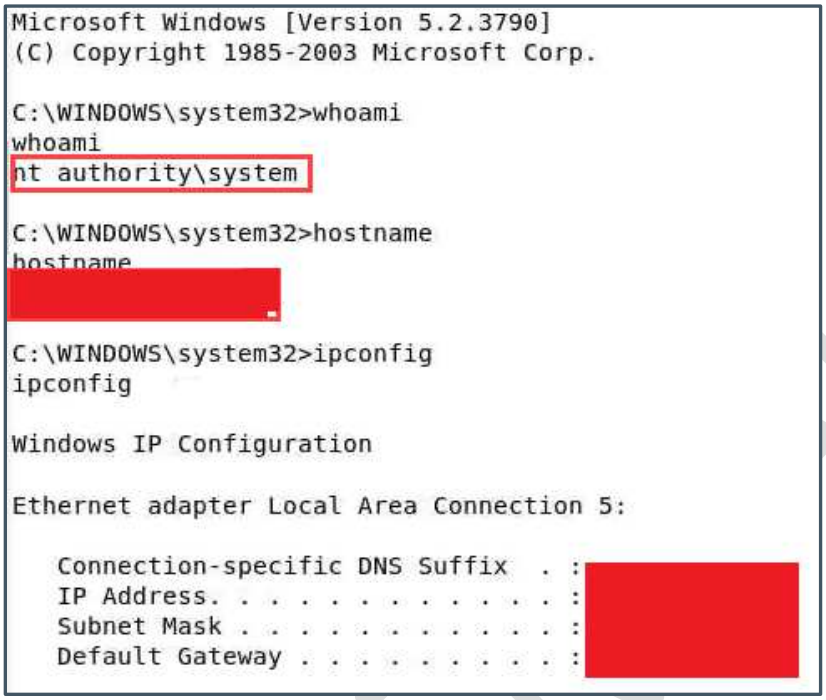


Figure 10: Proof of Compromise



The assessment team recommends ensuring that the patch identified in Microsoft security bulletin MS17-010 has been applied.

2.4.2.2 Credential Theft on 10.10.200.1 (SERVER)

After gaining full system access to 10.10.200.1, the assessment team utilized their new access to steal credentials in memory that could be used to further exploit the environment. The assessment team was able to steal many credentials, one being the “Administrator” account for the COMPANY domain (refer to Figure 11).

Figure 11: Credential Theft (redacted)

The assessment team recommends upgrading Windows hosts to a newer operating system. Operating systems of at least Windows 8.1/Server 2012R2 or greater contain protection mechanism that prevent a malicious user's ability to extract most plaintext passwords from memory. Additionally, the security updates discussed in Microsoft's KB2871997 article should be applied to all hosts. A Protected Users security group, an Active Directory 2012 R2 Functional Level enhancement, should be implemented to control its member's authentication capabilities to better protect their credentials. Alternatively, set the value of the following registry key to zero (0) to prevent the host from storing plaintext credentials in memory:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential

The assessment team also recommends that administrators have separate accounts used to perform administrative functions. Administrators should utilize Restricted Admin mode when making RDP connections to network resources. This will prevent their credentials from being loaded into memory on the target host. Additional information regarding Restricted Admin mode can be found in Microsoft Security Advisory 2871997. A Privileged Access Workstations (PAWs) architecture should be implemented and used to perform sensitive tasks.

The assessment team recommends reviewing the guidelines published at the locations listed below and implementing compensating controls:

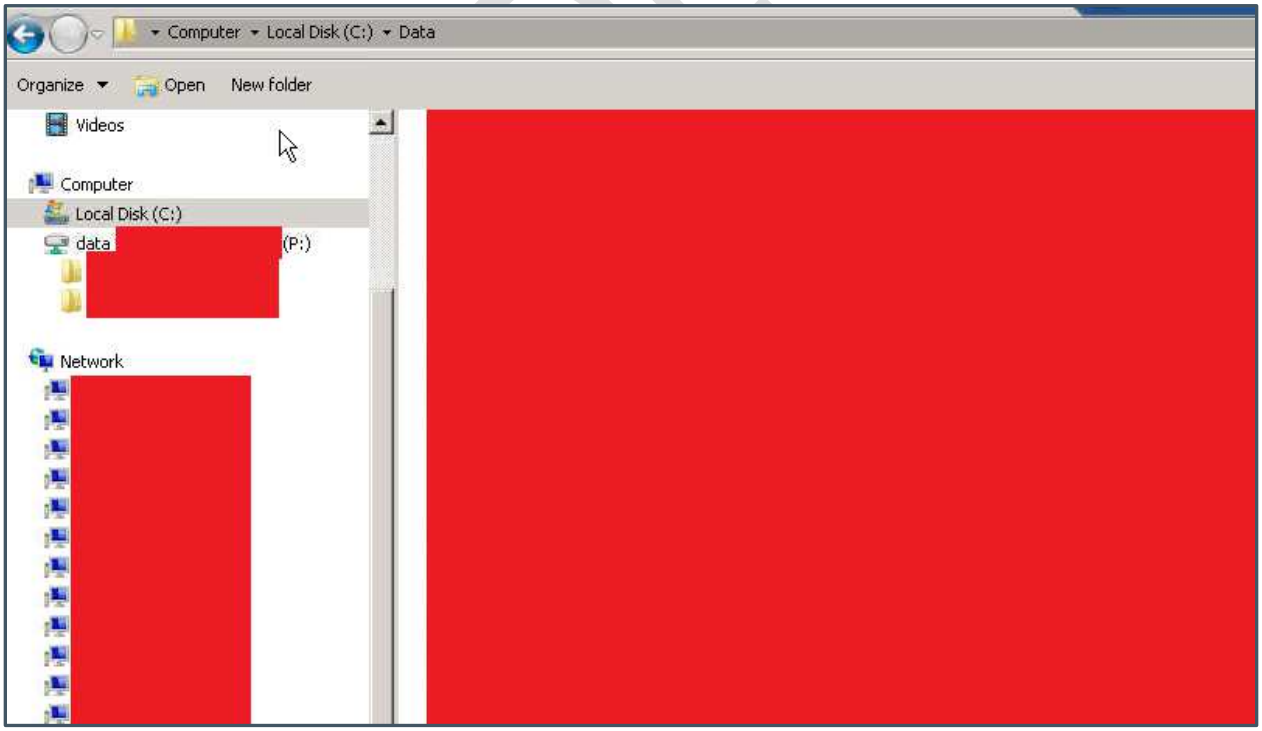
- https://support.microsoft.com/en-us/kb/2871997
- https://technet.microsoft.com/en-us/security/dn920237.aspx
- https://technet.microsoft.com/en-us/library/dn408190.aspx
- https://www.microsoft.com/en-us/download/confirmation.aspx?id=36036
- https://technet.microsoft.com/en%ADUS/library/mt634654.aspx
- https://technet.microsoft.com/en-us/library/dn466518.aspx

The assessment team also recommends enabling the "'Account is sensitive and cannot be delegated" user account configuration option for high privilege accounts. This will prevent Windows Access Tokens from being stolen and used to access network resources with privilege accounts. All changes should be tested first to ensure they do not impact business operations in a negative manner. Additional information can be found here: *https://blogs.technet.microsoft.com/poshchap/2015/05/01/security-focus-analysing-account-is-sensitive-and-cannot-be-delegated-for-privileged-accounts/*

2.4.2.3 Sensitive Data Discovery on COMPANY Domain

Utilizing the COMPANY/Administrator account, the assessment team was able to gain access to data across the COMPANY domain. The assessment team discovered numerous sensitive documents including the items shown in Figure 12.

Figure 12: Sensitive Data Discovery



The assessment team recommends that COMPANY analyze the data stored on the network to ensure documents containing things such as social security numbers or login credentials are properly disposed of or encrypted to provide appropriate access.

2.4.2.4 Broadcast Message Spoofing

The assessment team conducted a Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBNS) message spoofing attack on the 10.10.200.0/4 network. This attack listens for clients attempting to resolve a host name using the LLMNR or NBNS protocols and responds with the address of the attacker's host. After the requesting client receives a response back to the query from the attacker, it will attempt to authenticate, providing the attacker with a username and encrypted password hash. The assessment team exploited these requests and subsequently obtained the unique password hash shown in Figure 13 for user (*COMPANY/user*).

Figure 13: Broadcast Message Spoofing Captured Hash Example

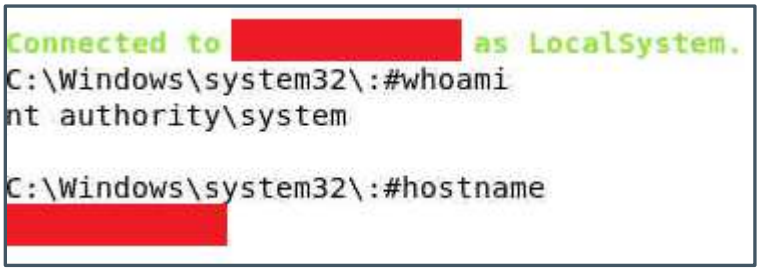
The presence of NBNS/LLMNR messages on a network is not a vulnerability as the protocols are operating as intended. The number of NBNS/LLMNR messages can be reduced by ensuring the presence of a DNS entry for the name attempting to be resolved. Additionally, an entry in a device's 'hosts' file will prevent NBNS/LLMNR messages from being broadcasted to the network when attempting to resolve a name. The assessment team recommends disabling both the NBNS and LLMNR protocols if feasible. Alternatively, the assessment team recommends monitoring the network for NBNS/LLMNR messages and configuring the host to resolve the name through DNS or its hosts file. It should be noted that sometimes the host is looking for a network resource that it communicated with at one time, but is no longer available. If this is the case, configure the host to quit attempting to connect to that resource.

2.4.2.5 SMB Relay Attack

By leveraging the attack described in the Broadcast Message Spoofing section (2.4.2.7), the assessment team was able to exploit the LLMNR/NBNS authentication requests by performing an SMB relay attack that targeted the host at 10.10.200.3. SMB authentication traffic was sent to this server by the assessment team with the credentials for (COMPANY\Administrator), and as a result, intercepting and relaying the request using the tools Responder and MultiRelay (refer to Figure 14). A remote shell session was established with SYSTEM level privileges (refer to Figure 15).

Figure 14: SMB Relay Attack

Figure 15: Proof of Compromise



SMB Relay attacks can be mitigated by enabling SMB signing for all clients and servers. This prevents an attacker from performing man-in-the-middle attacks by relaying user credentials. The following registry key can be modified to require SMB message signing: HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature

For additional information on SMB signing, and recommendations on securing SMB communications, please reference the following link: https://technet.microsoft.com/en-us/library/cc731957(v=ws.11).aspx

2.4.3 Testing Limitations

There were no limitations for the internal phase of the assessment.

2.4.4 Tools

The assessment team utilized various commercial and open source tools to scan the internal hosts for vulnerabilities and attempted to exploit identified vulnerabilities. Tools used include:

- Nessus Vulnerability Scanner
- Metasploit
- NMAP
- OpenSSL
- Fierce
- Pipal
- Responder
- Impacket
- Mimikatz
- Hashcat
- Burp Suite
- PowerTools
- Veil Framework
- PSTools
- Sparta
- dirb

- Nikto
- Hydra
- SSLScan
- enum4linux.pl
- snmpwalk
- Web Browsers (Internet Explorer, Firefox, Chrome)
- Built-In Windows Tools (i.e. cmd.exe, powershell.exe, mstsc.exe, explorer.exe, vssadmin.exe)

2.4.5 Post Penetration Testing Cleanup

The assessment team recommends rebooting the hosts 10.10.200.1 and 10.10.200.3 to remove memory resident exploits utilized during the assessment.

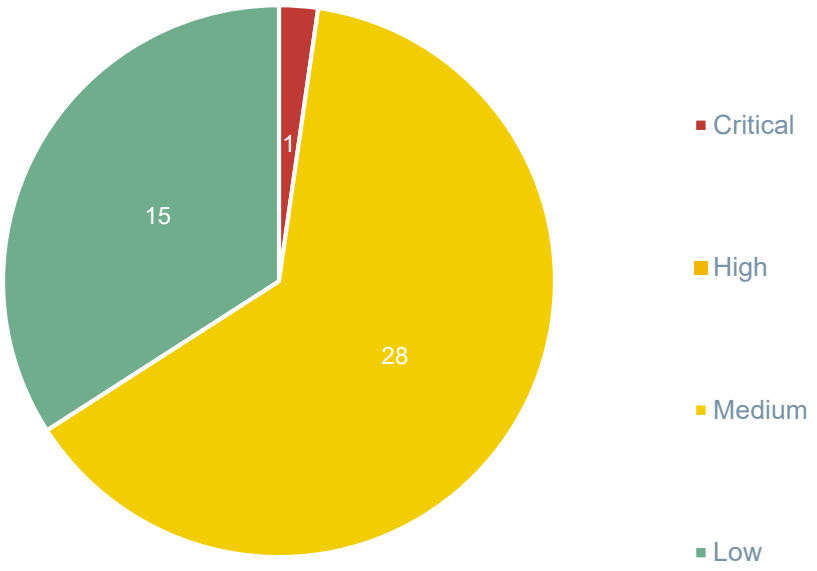
2.5 Web Application Assessment

The assessment team evaluated two (2) web applications for vulnerabilities during this assessment. Twenty-five (25) dynamic pages were evaluated for this web application assessment

2.5.1 Web Application Assessment Findings

The scan results identified one (1) critical-severity, zero (0) high-severity, twenty-eight (28) medium-severity, and fifteen (15) low-severity vulnerabilities as shown in below.

Figure 16: Web Application Vulnerabilities by Severity



A ***complete*** and detailed listing of the vulnerabilities identified during the web application assessment can be found in the vulnerability documents referenced in Appendix B - Supporting Documents. ***Some*** of the more severe vulnerabilities identified by the assessment team are detailed in the following sections.

2.5.1.1 SQL Injection (CVSS: 9.4 - Critical)

The assessment team identified one (1) application (mysite.com:443/tcp) vulnerable to structured query language injection. SQL injection is a code-based vulnerability that is found when user-controlled data is used to build SQL queries. An attacker can supply valid SQL characters and modify the SQL statement that is sent to the database. Various attacks can be delivered via SQL injection including reading or modifying critical application data, interfering with application logic, escalating privileges within the database, and even in some cases executing operating system commands. Figure 17 below can be used as a proof of concept:

Figure 17: SQLi Proof-of-Concept

The assessment team recommends that code modifications be made to implement parameterized queries as well as proper input validation for all fields that are used for interaction with a database. Parameterized queries help prevent SQL injection by creating placeholders for the user supplied data and putting those placeholders within an already constructed SQL statement. This prevents an attacker from editing the SQL statement itself. In addition, taking a "white-listing" approach to input validation helps mitigate SQL injection. For example, there should be no reason for a field to accept valid SQL language characters when that field needs only to accept alphanumeric characters. In addition, it is recommended that steps be taken to harden the database server itself to prevent data from being accessed inappropriately. For more information on mitigating SQL injection, please see the following Open Web Application Security Project's article:
https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

2.5.1.2 Cross-Site Scripting (CVSS: 6.4 - Medium)

The assessment team identified one (1) host (yoursite.com:443/tcp) vulnerable to XSS. XSS is an input injection vulnerability that is found when there is inadequate server-side input validation and/or inadequate output encoding of user-supplied data. An attacker can use XSS to send malicious JavaScript to an unsuspecting user. Because the browser interprets the script as coming from a trusted source, the malicious script can access cookies, session tokens, or other sensitive information retained by the browser and used within that site. This vulnerability can even be used to inject HTML into the valid webpage. If successful, XSS vulnerabilities can be exploited to manipulate or steal cookies, create requests that can be mistaken for those of a

valid user, compromise confidential information, or execute malicious code on end user systems.

The assessment team recommends that developers pay attention to fields within a web application that can be modified by a malicious user. Any area of input within the web application that is reflected back to the browser should have proper input validation at a server-side code level and should have the output encoded to reduce the risk associated with malicious input. For more information on preventing XSS, see the Open Web Application Security Project's article referenced below:
https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

2.5.1.3 Insecure Frame (CVSS: 4.3 - Medium)

The assessment team identified one (1) host (yoursite.com:443/tcp) using an insecure frame. Frames are generally used to host content from other domains or from the same domain. Since framed content can change without knowledge or consent, the principle of least privilege should be applied. Improperly framed elements may contain malicious elements that can affect users of the parent site.

The assessment team recommends that framed content be secured within an iFrame sandbox which allows granular control over the frame's abilities. All unused features should be disabled

2.5.1.4 Vulnerable JavaScript Library (Medium)

The assessment team identified two (2) applications (mysite.com:443/tcp and yoursite.com:443/tcp) using an out of date JavaScript library. The identified version of Prototype JavaScript Library was 1.5.1.1 and allows developers to use functions that create XSS conditions. Client-side script execution can allow an attacker to access cookies, session tokens, or other sensitive information retained by the browser.

The assessment team recommends upgrading the affected library to the latest version.

2.5.1.5 Directory Listing (CVSS: 6.1 - Medium)

The assessment team identified one (1) application (yoursite.com:443/tcp) with directory listing enabled. The */files* directory was found to have directory listing enabled. With this feature enabled, an attacker is able to view all files and folders in the affected directory. The directories can potentially contain sensitive information such as customer data, employee data, or source code.

The assessment team recommends configuring the affected web server to globally disable directory listing.

2.5.1.6 TLS Version 1.0 Protocol Detection (CVSS: 5.8 - Medium)

The assessment team identified two (2) applications (mysite.com:443/tcp and yoursite.com:443/tcp) using TLS version 1.0. This version of TLS suffers from several cryptographic flaws. An attacker may be able to exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Figure 18: Supported on https://mysite.com

```
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA
Accepted  TLSv1.0  256 bits  DHE-RSA-AES256-SHA
Accepted  TLSv1.0  256 bits  DHE-RSA-CAMELLIA256-SHA
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  256 bits  CAMELLIA256-SHA
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA
Accepted  TLSv1.0  128 bits  DHE-RSA-AES128-SHA
Accepted  TLSv1.0  128 bits  DHE-RSA-CAMELLIA128-SHA
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  128 bits  CAMELLIA128-SHA
Accepted  TLSv1.0  112 bits  ECDHE-RSA-DES-CBC3-SHA
Accepted  TLSv1.0  112 bits  EDH-RSA-DES-CBC3-SHA
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA
Accepted  TLSv1.0  128 bits  RC4-SHA
```

The assessment team recommends disabling support for TLS version 1.0 and only supporting TLS 1.1 or higher instead.

2.5.2 Web Application PT Findings

The assessment team conducted a penetration test against the target web applications. During this PT, the assessment team attempted to leverage the identified vulnerabilities to exploit the application, obtain, obtain sensitive information, and generally mimic the actions of an attacker with a targeted motivation to compromise the web applications.

2.5.2.1 SQL Injection

The assessment team exploited the SQL injection vulnerability to extract the *users* database table from the MySQL database as shown below in Figure 19.

Figure 19: Users Database Table (redacted)

user_id	email	username	password	last_name	first_name	db_admin
1	[redacted]	root	...ES[redacted]1%21...	Root	Mr.	1
2	[redacted]					0
3	[redacted]					0

2.5.2.2 Directory Listing

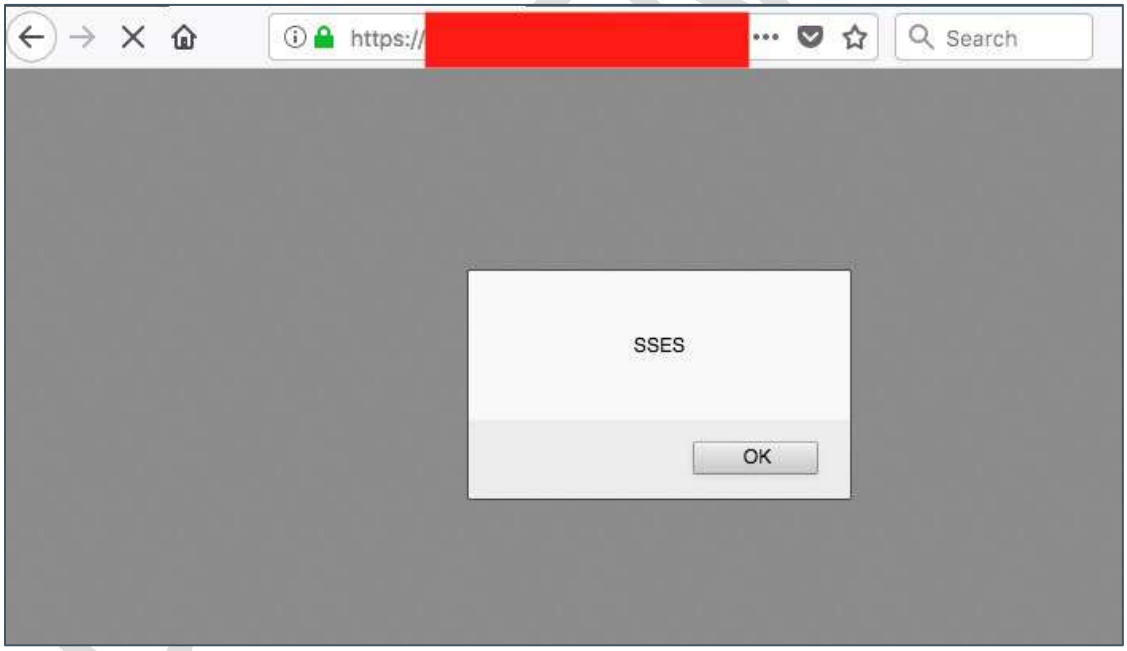
The assessment team exploited the directory listing enabled vulnerability to access the files listed in *https://yoursite.com/files/* (see Figure 20).

Figure 20: Directory Listing on *https://yoursite.com*

2.5.2.3 Cross-Site Scripting

The assessment team exploited the XSS vulnerability on *https://mysite.com* to execute a popup alert in a web browser (see Figure 21).

Figure 21: XSS on https://mysite.com



2.5.3 Web Application PT Findings

There were no limitations for the web application assessment. Client was required to submit a penetration testing request form to Amazon to get authorization before any testing could be started

2.5.4 Tools

The assessment team utilized various commercial and open source tools to scan the target web application(s) for vulnerabilities and attempted to exploit identified vulnerabilities. Tools used include:

- Nessus Vulnerability Scanner
- Netsparker
- Burp Suite
- Web Browsers (Internet Explorer, Firefox, Chrome)

3 Conclusion

Based on the analysis of the test results, the security posture of the evaluated network needs some improvements. A summary of the assessment team's recommendations for items needing remediation is given below:

External NVA

1. Upgrade host to a supported operating system
2. Restrict access to RDP from Internet and upgrade host to a supported operating system
3. Restrict access to DVR devices from Internet and implement complex passwords on accounts

Internal NVA

1. Install Microsoft Security Update indicated in MS17-010
2. Implement mandatory SMB signing on all hosts
3. Upgrade operating system to a supported version
4. Upgrade the hosts to the latest supported version of ESXi
5. Upgrade the hosts to the latest supported version of ESXi
6. Disable SMB Version 1 on hosts and utilize SMB Version 2 and 3
7. Install Microsoft Security Update indicated in MS14-066
8. Upgrade operating system to a supported version
9. Upgrade to latest supported version of Dropbear SSH software
10. Install Microsoft Security Update indicated in MS15-034
11. Upgrade operating systems to supported version

Web Application Assessment

1. Modify code to implement parameterized queries as well as proper input validation
2. Modify code to perform input validation and output encoding on all user input
3. Secure framed content in a sandbox, and disable all unused features
4. Update the affected library to the latest supported version
5. Disable global directory listing
6. Disable support for TLS version 1.0 and only support TLS 1.1 or higher instead

External PT

1. Restrict access to DVR devices from the Internet and implement complex passwords on accounts
2. Restrict access to RDP from the Internet and upgrade host to a supported operating system

Internal PT

1. Install Microsoft Security Update indicated in MS17-010
2. Upgrade hosts to a newer Windows operating system
3. Analyze the data stored on the network to ensure documents containing sensitive data are properly disposed of or encrypted
4. Reduce the number of NBNS/LLMNR messages
5. Enable and enforce SMB packet signing

Web Application PT

1. Modify code to implement parameterized queries as well as proper input validation
2. Disable global directory listing
3. Modify code to perform input validation and output encoding on all user input

Correct implementation of the recommendations contained in this report and the recommendations found in the documents listed in Appendix B, along with continued diligence on the part of COMPANY administrators, will result in an improvement of the security posture of the evaluated network.

It should be noted that the data included within this report represents only a snapshot in time. Best practice recommends periodic security assessments are conducted.

APPENDIX A: Acryonyms

CVSS	Common Vulnerability Scoring System
DBTA	Data Breach Threat Analysis
DNS	Domain Name Services
DOM	Document Object Model
DVR	Digital Video Recorder
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IIS	Internet Information Services
IP	Internet Protocol
LLMNR	Link Local Multicast Name Resolution
MitM	Man in the Middle
NBNS	Netbios Name Resolution
NVA	Network Vulnerability Assessment
PAW	Privileged Access Workstation
PCI	Payment Card Industry
PT	Penetration Test
RCE	Remote Code Execution
RDP	Remote Desktop Protocol
SMB	Server Message Block
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniformed resource Locator
VPN	Virtual Private Network
XSS	Cross-Site Scripting

APPENDIX B: Supporting Documents

This report is accompanied with several supporting documents. These documents are listed below along with a short description of each.

External Vulnerability Matrix

Filename: COMPANY 2017 External Vulnerability Matrix.xls
Description: A spreadsheet detailing which vulnerabilities are present on each external host. Network and system administrators tasked with remediation can utilize this matrix as a checklist.

External Vulnerability Listing

Filename: COMPANY 2017 External Vulnerability Listing.pdf
Description: A list of each vulnerability identified during the external network security assessment along with a short synopsis, the recommended remediation, any references, and a list of the affected hosts.

Internal Vulnerability Matrix

Filename: COMPANY 2017 Internal Vulnerability Matrix.xls
Description: A spreadsheet detailing which vulnerabilities are present on each internal host. Network and system administrators tasked with remediation can utilize this matrix as a checklist.

Internal Vulnerability Listing

Filename: COMPANY 2017 Internal Vulnerability Listing.pdf
Description: A list of each vulnerability identified during the internal network security assessment along with a short synopsis, the recommended remediation, any references, and a list of the affected hosts.

Web Vulnerability Matrix

Filename: COMPANY 2017 Web Vulnerability Matrix.xls
Description: A spreadsheet detailing which vulnerabilities are present on each web application. Network and system administrators tasked with remediation can utilize this matrix as a checklist.

Web Vulnerability Listing

Filename: COMPANY 2017 Web Vulnerability Listing.pdf
Description: A list of each vulnerability identified during the web application assessment along with a short synopsis, the recommended remediation, any references, and a list of the affected hosts.

APPENDIX C: Assignment of Risk Levels

Risk to an information system can be expressed as the expected loss as a result of 1) potential attacks to the information system; 2) vulnerabilities of the information system to those attacks; and 3) consequences of the attacks succeeding. The risk assessment is the evaluation of these potential attacks and vulnerabilities taken together with the resulting consequences if an attack were to succeed. The risk assessment process involves a study of these aspects to determine the likelihood of loss or consequence, and the expected effectiveness of security measures. The risk assessment allows managers to develop more effective security programs.

The risk levels associated with vulnerabilities in this report should be considered in the context of the application environment and perceived threat. These identifiers are not intended to be absolute values of risk; rather, these identifiers are intended as an indicator of severity of vulnerability. Five levels of risk are used:

Critical Risk – A vulnerability that is trivial to exploit (requires no special access conditions), and whose exploitation could have a catastrophic impact on the confidentiality, integrity, or availability of a critical system or application.

High Risk – A vulnerability that is fairly easy to exploit, and whose exploitation could result in a compromise of an application's confidentiality, integrity, or availability.

Medium Risk – A vulnerability that is complex to exploit (may require specialized access conditions, may require authentication), or may result in only a partial impact on an application's confidentiality, integrity, or availability upon exploitation.

Low Risk – A vulnerability that is more difficult to exploit (has a significant number of access conditions), or whose exploitation results in only a minor impact on an application's confidentiality, integrity, or availability.

Informational – A finding that includes discovered network devices, systems, or service information. These findings do not represent network vulnerabilities but could be leveraged by an attacker to indirectly assist in other network attacks.

APPENDIX D: External NVA/PT – Interesting Hosts

IP Address	Hostname	Open TCP Port(s)	Open UDP Port(s)
192.168.20.1	---	25, 3398, 443, 80, 81, 82, 8443	500

APPENDIX E: Internal NVA/PT – Interesting Hosts

IP Address	Hostname	Open TCP Port(s)	Open UDP Port(s)
10.10.200.1	---	22, 443, 80	67
10.10.200.2	---	427, 443, 5989, 80, 8000, 8100, 902	---
10.10.200.1	---	135, 139, 1723, 1801, 2103, 2105, 2107, 3268, 3269, 3388, 3389, 389, 443, 445, 464, 5000, 5001, 53, 593, 6004, 6005, 6006, 6007, 6008, 6012, 6014, 6017, 6022, 6048, 6049, 6075, 6079, 6126, 636, 80, 88	123, 137, 500, 53, 5355
10.10.200.3	---	1720, 411, 443, 80, 8443, 9080	123, 53, 69
10.10.200.4	---	1049, 1056, 1061, 1333, 135, 1380, 139, 1593, 1661, 1820, 1850, 21, 2142, 2150, 2330, 2686, 3002, 3255, 3398, 3563, 445, 5800, 5900	137, 1434
10.10.200.5	---	1500, 1501, 21, 23, 80, 9	69
10.10.200.6	---	135, 1366, 139, 25, 3389, 443, 445, 5800, 5900, 6002, 80, 8080, 993	123, 137, 1434
10.10.200.7	---	80	---
10.10.200.8	---	427, 443, 5989, 80, 8000, 8100, 902	123
10.10.200.9	---	427, 443, 5989, 80, 8000, 8100, 902	123
10.10.200.10	---	427, 443, 5989, 80, 8000, 8100, 902	427
10.10.200.11	---	1029, 1030, 1032, 1057, 1058, 1062, 135, 139, 1894, 1895, 3412, 445, 4452, 4545, 5454	137
10.10.200.12	---	135, 139, 1433, 2383, 2443, 3389, 3443, 443, 445, 4456, 4545, 49152, 49153, 49154, 49155, 49160, 49176, 49243, 49244, 5454, 5801, 5802, 5803, 80, 8443	137, 5355
10.10.200.13	---	139, 23000, 445	1022, 1023, 137, 138, 161, 34611, 427, 5353, 57102, 58014, 65471

APPENDIX F: Disclaimer

This document and its contents do not constitute, and are not a substitute for, legal advice. The outcome of a Security Risk Assessment should be utilized to ensure that diligent measures are taken to lower the risk of potential weaknesses be exploited to compromise data.

Although the Services and this report may provide data that Client can use in its compliance efforts, Client (not Avertium) is ultimately responsible for assessing and meeting Client's own compliance responsibilities. This report does not constitute a guarantee or assurance of Client's compliance with any law, regulation or standard.