6300 Corporate Blvd. Suite. 200

Baton Rouge, LA 70809

Phone: 225.612.2122

www.tracesecurity.com

 **INTERNAL PENETRATION TEST REPORT**

<Client Name>

<Date>

TraceSecurity

# TABLE OF CONTENTS

[TABLE OF CONTENTS 2](#_Toc499887857)

[LIST OF FIGURES 3](#_Toc499887858)

[DOCUMENT INFORMATION 6](#_Toc499887859)

[PROJECT DEFINITION 7](#_Toc499887860)

[DEFINITION 7](#_Toc499887861)

[OBJECTIVE 7](#_Toc499887862)

[RULES OF ENGAGEMENT 7](#_Toc499887863)

[TESTING METHODOLOGY 8](#_Toc499887864)

[EXECUTIVE SUMMARY 10](#_Toc499887865)

[EXECUTIVE SUMMARY OF INTERNAL PENETRATION TEST RESULTS 10](#_Toc499887866)

[SECTION 1: NETWORK MAPPING 12](#_Toc499887867)

[SECTION 2: VULNERABILITY IDENTIFICATION 17](#_Toc499887868)

[SECTION 3: PENETRATION TESTING 18](#_Toc499887869)

[NBT-NS and LLMNR Poisoning Attack – High Risk 18](#_Toc499887870)

[Anonymous Access or Missing Credentials – High Risk 20](#_Toc499887871)

[Default CREDENTIALS – High Risk 24](#_Toc499887872)

[Man In The Middle (MITM) Attack Vulnerability via OpenSSL – medium risk 28](#_Toc499887873)

[Remote Session Vulnerability “WannaCry” – medium risk 31](#_Toc499887874)

[Plaintext protocols in use – medium risk 33](#_Toc499887875)

[MS SQL Server DR-Dos Amplification – Medium Risk 35](#_Toc499887876)

[Weak and Insecure Ciphers – Low risk 36](#_Toc499887877)

[CBC Ciphers Detected over ssh – Low Risk 43](#_Toc499887878)

[Post-Exploitation evidence 45](#_Toc499887879)

[APPENDIX 50](#_Toc499887880)

[Additional test results and findings 50](#_Toc499887881)

# LIST OF FIGURES

[Figure 1: Table - Target Ranges and Individual IP addresses provided: 12](#_Toc499887882)

[Figure 2: Summary of Top Open Ports and Services: 12](#_Toc499887883)

[Figure 3: Service Version Scan: SMB TCP Port 445 on Devices Not on a Domain: 13](#_Toc499887884)

[Figure 4: Service Version Scan: SMB TCP Port 445 on Windows 2008 R2 Servers: 13](#_Toc499887885)

[Figure 5: IP SMB Version Scan on Devices with TCP Port 389 Open as Possible Domain Controllers: 13](#_Toc499887886)

[Figure 6: Service Version Scan: SMB TCP Port 445 on Windows 2012 Servers: 14](#_Toc499887887)

[Figure 7: Service Version Scan Example of FTP TCP Port 21: 14](#_Toc499887888)

[Figure 8: Service Version Scan: SSH TCP Port 22: 15](#_Toc499887889)

[Figure 9: Service Version Scan: Telnet TCP Port 23: 15](#_Toc499887890)

[Figure 10: Example NetScan Results on Targeted Subnets: 16](#_Toc499887891)

[Figure 11: High and Medium Vulnerabilities from TraceCSO Scanner Results: 17](#_Toc499887892)

[Figure 12: Poisoning Attack Example Performed on the 172.16.0.0/24 Subnet with Captured Hash 19](#_Toc499887893)

[Figure 13: Hash Cracking Attempts on Captured Credentials: 19](#_Toc499887894)

[Figure 15: Table - Anonymous LDAP Enumeration on Multiple Hosts: 20](#_Toc499887895)

[Figure 16: Anonymous LDAP Enumeration Example on 172.16.2.18: 20](#_Toc499887896)

[Figure 17: Anonymous LDAP Enumeration on 172.16.3.18 Showing Renamed Administrator Account: 21](#_Toc499887897)

[Figure 18: System Properly Configured to Prevent Anonymous LDAP Lookups at 172.16.2.76: 21](#_Toc499887898)

[Figure 19: Anonymous Administrator Access to HP Printer Located at https://172.16.2.50: 21](#_Toc499887899)

[Figure 20: Table - Anonymous Read Access to FTP Services on Multiple Devices: 22](#_Toc499887900)

[Figure 21: Anonymous Read Access Example to FTP Services on 192.168.10.5: 22](#_Toc499887901)

[Figure 22: Anonymous Access over Telnet TCP Port 23 from Version Scan on Multiple Devices: 23](#_Toc499887902)

[Figure 23: “Password is not set” message on Multiple Devices over Telnet: 23](#_Toc499887903)

[Figure 24: Anonymous Access Connection Example to Telnet TCP Port 23 on 172.16.2.50: 23](#_Toc499887904)

[Figure 25: Table - SNMP “read-write” Login with Default Community Strings on Multiple Hosts: 24](#_Toc499887905)

[Figure 26: SNMP “read-write” Login Example with Default Community Strings on Multiple Hosts: 25](#_Toc499887906)

[Figure 27: Table - Default SNMP Community Strings on HP Printers Reveal Usernames from Print Logs: 25](#_Toc499887907)

[Figure 28: SNMP Community Strings Example on HP Printers Reveal Usernames from Print Logs: 26](#_Toc499887908)

[Figure 29: Default Admin Credentials Accepted on AudioCodes located at http://172.16.0.212: 26](#_Toc499887909)

[Figure 30: Table - Default Credentials Accepted Polycom Device Located on Multiple Devices: 26](#_Toc499887910)

[Figure 31: Default Credentials Accepted Polycom Device Located at https://192.168.101.188: 27](#_Toc499887911)

[Figure 32: Table - OpenSSL MITM Attack Vulnerability Confirmed on Multiple Devices over TCP Port 443: 28](#_Toc499887912)

[Figure 33: OpenSSL MITM Attack Vulnerability Confirmed on Multiple Devices over TCP Port 443: 29](#_Toc499887913)

[Figure 34: OpenSSL MITM Attack Vulnerability Confirmed on Multiple Devices over TCP Port 443: 30](#_Toc499887914)

[Figure 35: Table - EternalBlue or WannaCRY Vulnerability Found on Multiple Hosts: 31](#_Toc499887915)

[Figure 36: EternalBlue or WannaCRY Vulnerability Found on 172.16.6.191: 31](#_Toc499887916)

[Figure 37: Failed Attempt to Start a Remote Session through MS17\_010 Exploit on 172.16.0.31 31](#_Toc499887917)

[Figure 38: Failed Attempt to Start a Remote Session through MS17\_010 Exploit on 172.16.6.191 32](#_Toc499887918)

[Figure 39: Plaintext Protocol Found on http://172.16.5.30 that Accepts Login Credentials: 33](#_Toc499887919)

[Figure 40: Plaintext Protocol Found on http://172.16.8.71 that Accepts Login Credentials: 33](#_Toc499887920)

[Figure 41: Table - Telnet Version Scan on Multiple Devices with TCP Port 23 Open: 34](#_Toc499887921)

[Figure 42: Telnet Version Scan on Multiple Devices with TCP Port 23 Open: 34](#_Toc499887922)

[Figure 28: DRDoS Amplification probable on XXXX: 35](#_Toc499887923)

[Figure 43: Table - Insecure Protocols Detected on Multiple Hosts with SSLv2 Accepted: 36](#_Toc499887924)

[Figure 44: Table - Insecure Protocols Detected on Multiple Hosts with SSLv3 Accepted: 37](#_Toc499887925)

[Figure 45: Table - Insecure Protocols Detected on Multiple Hosts with TLSv1.0 Accepted: 38](#_Toc499887926)

[Figure 46: Table - Insecure Protocols Detected on Multiple Hosts with TLSv1.1 Accepted: 39](#_Toc499887927)

[Figure 47: Table - Weak & Insecure Protocols Detected on Multiple Hosts with TLSv1.1 Accepted <128bit: 40](#_Toc499887928)

[Figure 48: Table - Weak & Insecure Protocols Detected on Multiple Hosts with TLSv1.1 Accepted ADH/RC4/AECDH: 40](#_Toc499887929)

[Figure 49: Table - Weak & Insecure Protocols Detected on Multiple Hosts with TLSv1.2 Accepted <128bit: 41](#_Toc499887930)

[Figure 50: Table - Weak & Insecure Protocols Detected on Multiple Hosts with TLSv1.2 Accepted ADH/RC4/AECDH: 41](#_Toc499887931)

[Figure 51: Table - Insecure Session Renegotiation Supported on Multiple Hosts: 42](#_Toc499887932)

[Figure 52: Table - Nmap Scans Revealing the use of CBC Ciphers on Multiple Hosts: 43](#_Toc499887933)

[Figure 53: Nmap Scan Example revealing the use of CBC Ciphers on Multiple Hosts: 44](#_Toc499887934)

[Figure 54: Account Numbers Located on 172.16.6.12 by Accessing Shares with Compromised Credentials: 45](#_Toc499887935)

[Figure 55: Credit Card Numbers Located on Share Accessed with Compromised Credentials: 45](#_Toc499887936)

[Figure 56: Check Image Located on Share Accessed with Compromised Credentials: 46](#_Toc499887937)

[Figure 57: Example of Users and Descriptions Extracted via Anonymous LDAP Lookup: 46](#_Toc499887938)

[Figure 58: Loan Documents Located on Share Accessed with Compromised Credentials: 47](#_Toc499887939)

[Figure 59: Folders Located on http://172.16.0.248 using Directory Tools that Lead to Member Information: 47](#_Toc499887940)

[Figure 60: Member Information Located with Directory Search Tools on 172.16.0.248 Anonymously: 47](#_Toc499887941)

[Figure 61: Receipts Located on Share Accessed with Compromised Credentials: 48](#_Toc499887942)

[Figure 62: Report CSV Export Option Found with Directory Search Tools with Anonymous Access: 48](#_Toc499887943)

[Figure 63: Report Exported Anonymously from Server Located at 172.16.0.248: 49](#_Toc499887944)

[Figure 65: Default Login Attempted on http://172.16.0.212: 50](#_Toc499887945)

[Figure 66: Default Login Attempted on https://172.16.0.213: 51](#_Toc499887946)

[Figure 67: Password Attack on Enumerated Accounts (anonymously) on 172.16.2.18: 51](#_Toc499887947)

[Figure 68: Default Login Attempt on https://172.16.5.75: 52](#_Toc499887948)

[Figure 69: Default Login Attempt on https://172.16.7.83: 53](#_Toc499887949)

[Figure 70: Meterpreter Session Attempt with Compromised Credentials: 53](#_Toc499887950)

[Figure 71: Default Login Attempt at https://172.16.3.15: 54](#_Toc499887951)

[Figure 72: Default Login Attempt at https://172.16.5.22: 54](#_Toc499887952)

[Figure 73: Default Login Attempt at http://172.16.8.71: 55](#_Toc499887953)

[Figure 74: Remote Desktop Login Attempt with Compromised Credentials: 55](#_Toc499887954)

[Figure 75: Remote Desktop Login Attempt with Compromised Credentials on 192.168.201.26: 56](#_Toc499887955)

[Figure 76: VNC None-Auth Vulnerability Check on Devices with TCP Port 5900 Open: 56](#_Toc499887956)

[Figure 77: Table - Full List of Live Devices Found in the Subnets Beginning With “10.”: 57](#_Toc499887957)

[Figure 78: Table - Full List of Live Devices Found in the 172.16.0.0/24 Subnet: 57](#_Toc499887958)

[Figure 79: Table - Full List of Live Devices Found in the 172.16.1.0/24 Subnet: 58](#_Toc499887959)

[Figure 80: Table - Full List of Live Devices Found in the 192.168.101.0/24 & 192.168.205.0/24 Subnets: 58](#_Toc499887960)

[Figure 81: Table - Full List of Live Devices Found in the 172.16.2.0/24 Subnet: 59](#_Toc499887961)

[Figure 82: Table - Full List of Live Devices Found in the 172.16.5.0/24 Subnet: 59](#_Toc499887962)

[Figure 83: Table - Full List of Live Devices Found in the 172.16.6.0/24 Subnet: 59](#_Toc499887963)

[Figure 84: Table - Full List of Live Devices Found in the 172.16.7.0/24 Subnet: 60](#_Toc499887964)

[Figure 85: Table - Full List of Live Devices Found in the 172.16.8.0/24 Subnet: 60](#_Toc499887965)

[Figure 86: Table - Full List of Live Devices Found in the 172.16.9.0/24 Subnet: 60](#_Toc499887966)

[Figure 87: Table - Full List of Live Devices Found in the 172.16.3.0/24 Subnet: 60](#_Toc499887967)

[Figure 88: Table - Full List of Live Devices Found in the 172.16.4.0/24 Subnet: 60](#_Toc499887968)

# DOCUMENT INFORMATION

|  |  |
| --- | --- |
| **Company** | <Client Name> |
| **Document Title** | Internal Penetration Test Report |
| **Date** | <DAte of Report> |
| **Classification** | Confidential |
| **Document Type** | Private |

|  |  |  |
| --- | --- | --- |
| **Document recipients** | | |
| **name** | **title** | **organization** |
| <Contact Name> | <Title> | <Client Name> |

|  |  |  |
| --- | --- | --- |
| **Document History** | | |
| **Date** | **Author** | **Comments** |
| <Date of Report> | TraceSecurity | Final DOCUMENT |

# PROJECT DEFINITION

## DEFINITION

An Internal Penetration Test emulates an attack by attempting to breach systems on the internal network from an attacker’s perspective. For this security testing, the TraceSecurity Information Security Analyst (ISA) attempts to circumvent the security features of a system and may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The ISA works under the same constraints applied to ordinary users.

## OBJECTIVE

The objective of this engagement is to provide an analysis of the current security program and countermeasures implemented at  <Client Name>. This is achieved by predefining a goal (i.e. obtaining administrative access to systems, or obtaining confidential or sensitive information from network resources such as file shares or customer account systems) and reporting whether that goal was achieved, providing proof of obtaining the defined goal, and documenting the exact process.

## RULES OF ENGAGEMENT

Prior to beginning the Internal Penetration Test, several rules of engagement must be predefined so that TraceSecurity does not engage in any “out-of-bounds” behavior or tactics. Please note that a typical attacker will not adhere to this list. Most will implement any and all methods of obtaining information in order to achieve their goal.

**Possible Rules of Engagement**

|  |  |
| --- | --- |
| **Attack Methodology** | **Permitted** |
| Network Mapping : Internal | Received Sign-Off |
| Compromise Communication | Received Sign-Off |

**Tools Used during Engagement**

Many tools that will be utilized in the engagement are available through the Internet. These tools may include mundane programs, such as PING, NSLOOKUP, SAMSPADE, web browsers, and more complex utilities such as:

|  |  |
| --- | --- |
| Port Scanners : Nmap, Propecia, netcat | Anti-Ids : Nmap, hping |
| Penetration framework: metapsploit | Security Scanners : In-House, openvas |
| Sniffers : ettercap, Wireshark, Cain | Information Gathering Utilities : p0f, |
| Password Crackers : Ophcrack | Banner Grabbing Utilities : Netcat |
| web Scanners :, Wikto,NIkto, grendalscan | Various Utilities : netifera, autoscan |

## TESTING METHODOLOGY

* **Information Gathering:** TraceSecurity gathers site-specific information to identify servers, workstations, routers, firewalls, and everything that provides specific information on the target system. This information will help build a picture, or “footprint” of the target’s network. In addition, this information also provides insight into the environment to better prepare for social engineering or other methods of compromise.
* **Enumeration:** During this step, the penetration team attempts to gain more information about the targets, using methods that are more intrusive. Additional information is recorded by trying to connect to network resources.
* **Vulnerability Analysis:** During this phase, the ISA attempts to associate operating systems and applications with identified computers on the network. Depending on network architecture, this may be accomplished using automated tools, such as Nmap, Autoscan, and Lanmap, or using manual techniques, such as Telnet, FTP, or other login banners. Using this information, TraceSecurity creates a list of probable vulnerabilities associated with each potential target system. In addition, automated scripts are developed or compiled to attempt exploitation of vulnerabilities.
* **Definition of Secondary Targets:** Based on information generated by the vulnerability analysis, the TraceSecurity penetration testing team determines the specific objectives that offer a greater possibility of obtaining the final goal or initiative. This is to ensure that secondary targets that were compromised will be reported, even if the primary target is not achieved.
* **Exploitation and Penetration Attacks:** During this phase, system and user information is used to attack the authentication processes of the target systems. Example attack scenarios in this phase include, but are not limited to, buffer overflows, application or system configuration problems, modems, routing issues, DNS attacks, address spoofing, share access, and exploitation of inherent system-trust relationships. Potential vulnerabilities are systematically tested in the order of penetration and detection probability as determined by the members of the TraceSecurity penetration testing team. The strength of captured password files is tested using password-cracking tools. Individual user account passwords may also be tested using dictionary-based, automated login scripts. In the event that an account is compromised, the TraceSecurity ISA will attempt to elevate privileges to that of superuser, root, or administrator level.

Since the goal of TraceSecurity Penetration testing is to determine the extent of vulnerabilities and not simply penetrate a single site system, information discovered on one system may be used to gain access to additional systems that may be "trusted" by the compromised system. Additionally, host-level vulnerabilities may be exploited to elevate privileges within the compromised system to install "sniffers" or other utilities. The ISA will insert a small text file at the highest level directory of each compromised system. If the ISA is unable to gain sufficient privilege to write to the system, a file will be copied from the system. In either case, additional files may be copied during testing if further review is required to determine the sensitivity of information contained on the system. TraceSecurity will maintain detailed records of all attempts to exploit vulnerabilities and activities conducted during the attack phase.

* **Results Analysis:** After initial testing is performed and preliminary data is generated, all information will be reviewed to determine if further analysis is necessary, or if the exploit should be tested further to discover additional information.
* **Final Analysis and Documentation:** TraceSecurity will provide a comprehensive report outlining all discoveries and methods used to obtain the information. An off-site conference call will be scheduled and performed to ensure that all information is clearly understood and a course of action/remediation is implemented. In addition, these results will also be documented in a management-level report that will cover the unannounced penetration testing. Specific details on vulnerabilities will also be provided to site technical personnel.
* **Special Considerations:** TraceSecurity coordinates testing activities with a "trusted agent" in each organization listed on the performance test agreement as appropriate. Each organization should identify an individual to be designated as a trusted agent. More than one trusted agent may be identified at the site. However, the number should be kept to an absolute minimum. All personnel informed of the testing must maintain strict confidentiality to ensure the validity of test results.

The Operations Office will coordinate with trusted agents at the site to identify critical systems that should be excluded from testing activities (e.g. safety systems, major applications undergoing upgrades, or other special evolutions). Specific network addresses and reasons for exclusion should be provided as an attachment to the signed performance test.

The Operations Office must identify any systems or network nodes that are connected to the site network, but not under the direct control and responsibility of the site or Operations Office. These systems will be excluded from testing unless TraceSecurity obtains permission from the system owner.

TraceSecurity will provide <Client Name> with information regarding the systems used for scanning and testing activities to ensure that these are not confused with real attacks.

While TraceSecurity does not attempt to exploit "denial-of-service" vulnerabilities (unless specifically requested by competent authority) and will make every attempt to prevent damage to any information system and its data, some penetration attempt scenarios have the possibility of causing service interruption. In the unlikely event that such an incident occurs, TraceSecurity will work with the trusted agents at the site to determine the nature of the problem and restore the system to its desired state of operation.

All information obtained by TraceSecurity will be protected (to the greatest extent possible) from unauthorized access. In the event that any site personnel (excluding trusted agents) identify TraceSecurity testing activities, site information security personnel should document the detection of activity and take initial actions that would be taken in the case of a real intrusion, including informing the Incident Response Team. If notified by the site of incidents that correspond with penetration testing, the site’s trusted agents must inform the appropriate site information security personnel that the activity identified is part of an authorized test. <Client Name>’s IT Team will also be informed of the detection. In these cases, logs or other evidence of intrusion detection activities should be provided to TraceSecurity for analysis. TraceSecurity testing will then continue as an announced internal network security penetration test without blocking, filtering, or restricting access.

It is the site’s responsibility to restore network computer systems to a secure configuration after TraceSecurity testing. TraceSecurity will assist system administrators as requested during this period of "cleaning up" network computer systems. Cleanup may consist of removing added programs and files, identifying systems whose password files were compromised, and restoring systems to a secure configuration so that no systems are left in a compromised state.

# EXECUTIVE SUMMARY

## EXECUTIVE SUMMARY OF INTERNAL PENETRATION TEST RESULTS

<Client Name>, has just completed a Penetration Test of the internal network.

This engagement utilized real-world tests of how internal adversaries may conduct attempts to gain unauthorized access to <Client Name>’s core information systems, servers, workstations, network equipment, and security devices. This engagement used a combination of widely known and freely available attack methods to complete this test of the internal network.

<Client Name> provided the ISA with internal Internet Protocol (IP) ranges to be tested. These IP addresses are listed in the Network Mapping section of this report. The ISA performed network mapping (enumeration), vulnerability identification, and penetration testing based on the identified vulnerabilities.

Although the analyst was unable to compromise any confidential data on the credit union’s network within the timeframe of this engagement, there were several known vulnerabilities across the organization’s internal network and systems that were validated during this exercise. The analyst was able to gain access and control interfaces of several devices on the credit union’s network. The testing performed by the analyst identified several serious issues that could negatively impact confidentiality, integrity, and availability of the affected systems.

The primary areas of concern are:

* High Risk
  + NBT-NS and LLMNR Poisoning Attack  
    – During the engagement the analyst was able to broadcast a poisoning attack on the local subnet to capture and crack login credentials. TraceSecurity recommends adjusting current network topology and protocols to prevent broadcasting system and user hashes to unauthenticated systems on the network.
  + MS14-025 Vulnerability Allows User Privileged Elevation  
    – The analyst conducted an exploit scan against devices identified as possible Domain Controllers to locate domain admin credentials with a compromised end-user password. TraceSecurity recommends ensuring that all systems are patched and updating according the manufactures’ security bulletins to prevent malicious parties from using documented vulnerabilities to attack systems and resources.
  + Weak/Dictionary Passwords Identified  
    – By conducting a simple password guess attack on usernames extracted from LDAP systems, the analyst was able to confirm the use of a common password for an end user to eventually elevate domain access to the organization’s network. TraceSecurity recommends implementing a strong password enforcement policy with regular audits to ensure effectiveness.
  + Anonymous Access or Missing Credentials  
    – The analyst discovered multiple systems with missing administrative credentials or incomplete security settings. TraceSecurity recommends implementing a device hardening procedure that will ensure all equipment, devices, applications, protocols, and services arFe configured with strong passwords.
  + Default Login Credentials   
    –Access to systems using documented credentials located on the internet. TraceSecurity recommends implementing a device hardening procedure that will ensure all equipment, devices, applications, protocols, and services are configured to remove default credentials and set with unique, strong passwords.
* Medium Risk
  + Multiple IPMI Authentication Vulnerabilities  
    – Systems found using IPMI Authentication possessed one or more vulnerabilities resulting in administrative bypass and password hash enumeration. TraceSecurity recommends removing all Intelligent Platform Management Interface (IPMI) devices as the protocol provides low-level access to systems that can override operation system controls. Required equipment should be configured to follow any documented settings published by the manufacture to reduce the risk of exploitation related to these vulnerabilities.
  + Multiple OpenSSL Vulnerabilities  
    – The analyst confirmed software versions of systems exposed to Denial of Service (DoS) and Man-In-The-Middle (MITM) attacks on the local network. TraceSecurity recommends updating services and protocols to the latest, supported versions by the manufacturer to ensure proper mitigation of known vulnerabilities.
  + Administrative Bypass Vulnerability  
    – Directories were enumerated behind password protected landing pages that contained non-public information accessible to unauthorized users. TraceSecurity recommends auditing all application authentication settings and system permissions to ensure the authentication requirements are effective throughout the site and application. TraceSecurity also recommends implementing periodic tests to ensure hardening standards have been implemented to prevent authentication bypass and related exploits to the hosted applications.
  + Remote Session Vulnerability “WannaCry” MS17-011  
    – Although no remote sessions were successfully connected to the devices mentioned within this report, the vulnerabilities were confirmed and tested. TraceSecurity recommends that the organization subscribe to and implement security patches from software vendors to ensure remote session executions are minimized.
  + Plain-Text Protocol in Use for Authentication  
    – The analyst successfully logged into to multiple interfaces and protocols with built-in or default credentials with a demonstration a plain-text exploit showing credentials in plain-text with WireShark. TraceSecurity recommends disabling all protocols that transmit credentials or other sensitive information in plain-text. Any mission critical services that require plain-text protocols should be incorporated with additional security measures to limit, monitor, log, and alert on access to quickly respond to unauthorized connectivity.
  + MS SQL Dr-DoS Amplification  
    – Systems running MS Sql were found to have anonymous information available to provide an attacker with system information, directory locations and software versions to aid attackers exploiting a Distributed Reflection Denial of Service (DRDoS) conditions against remote hosts. TraceSecurity recommends restricting access to MS Sql servers to any unauthorized traffic.
  + Anonymous Domain Enumeration (LDAP Null Bind)  
    – The analyst conducted a series of anonymous scans to successfully enumerate sensitive information such as usernames, groups, account settings, and permissions from systems supporting LDAP. Most commonly targeted systems are running Microsoft Active Directory. TraceSecurity recommends configuring all LDAP servers and services to require authentication to prevent unauthorized enumeration attempts by malicious parties.
* Low Risk
  + Weak and Insecure Ciphers   
    – Scans conducted by the analyst revealed insecure protocols and encryption bit strengths below 128bit. TraceSecurity recommends updating SSL certificates to use strong ciphers and encryptions of 128bit or higher.
  + CBC SSH Vulnerability  
    – The analyst confirmed software versions of systems exposed to Denial of Service (DoS) and Man-In-The-Middle (MITM) attacks on the local network. TraceSecurity recommends removing all insecure protocols to ensure vulnerabilities are mitigated.

The following information in this report will provide details on the initial network discovery, vulnerability testing, and penetration testing as described in the scope of work and contracted services between TraceSecurity and <Client Name>.

# SECTION 1: NETWORK MAPPING

This section identifies the network resources and services. It is focused on technical aspects of the institution’s network.

The expected results were the following:

* Target IP range(s)
* Host discovery
* Summary of available ports and services
* Operating system(s) identification
* Web server identification

The analyst performed a series of Nmap scans on the specified subnets and IP address ranges in order to identify system types, operating systems, network shares and other critical services that could present a vulnerability to the organization’s network. The following figures detail the mapping process of live systems and open ports and vulnerabilities discovered by TraceSecurity Scanners. The results of this pentest are a partial segment of the client’s internal network and represent an example of like systems and branches throughout the organization. It is advised that the organization take additional steps to ensure the artifacts found by the analyst within this report do not exist in other areas, subnets, branches or like systems maintained by the credit union.

Figure 1: Table - Target Ranges and Individual IP addresses provided:

A full list of live hosts can be found in the appendix of this report.

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.0.0/24  172.16.1.0/24  172.16.2.0/24  172.16.3.0/24  172.16.4.0/24 | 172.16.5.0/24  172.16.6.0/24  172.16.7.0/24  172.16.8.0/24  172.16.9.0/24 | 10.10.10.0/24  10.0.0.0/24  10.0.9.0/24  10.20.36.0/24 | 192.168.201.0/24  192.168.101.0/24  192.168.205.0/24 |

Figure 2: Summary of Top Open Ports and Services:

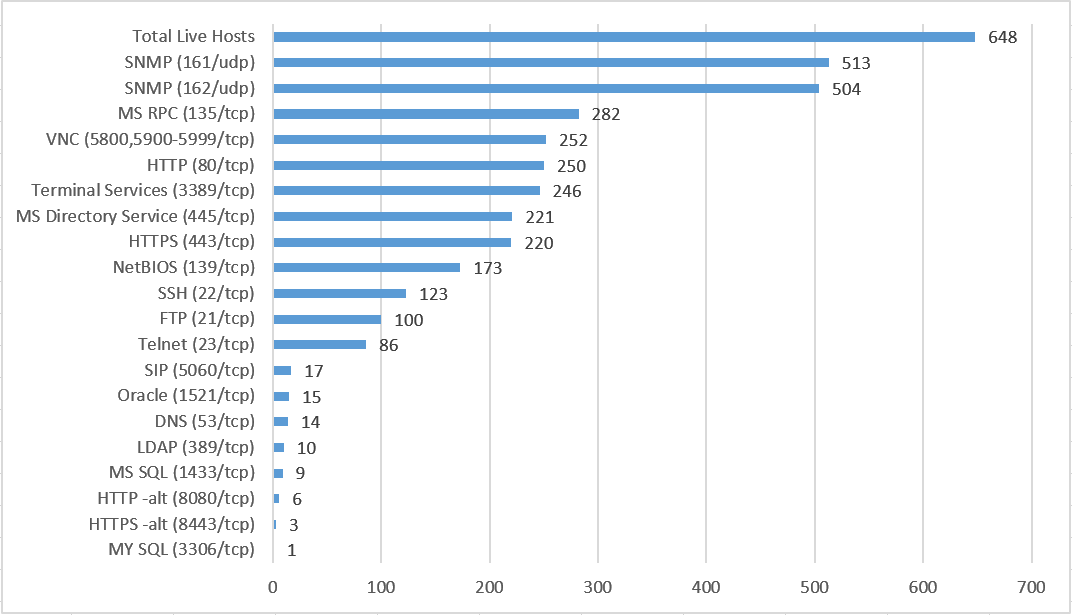


Figure 3: Service Version Scan: SMB TCP Port 445 on Devices Not on a Domain:



Figure 4: Service Version Scan: SMB TCP Port 445 on Windows 2008 R2 Servers:

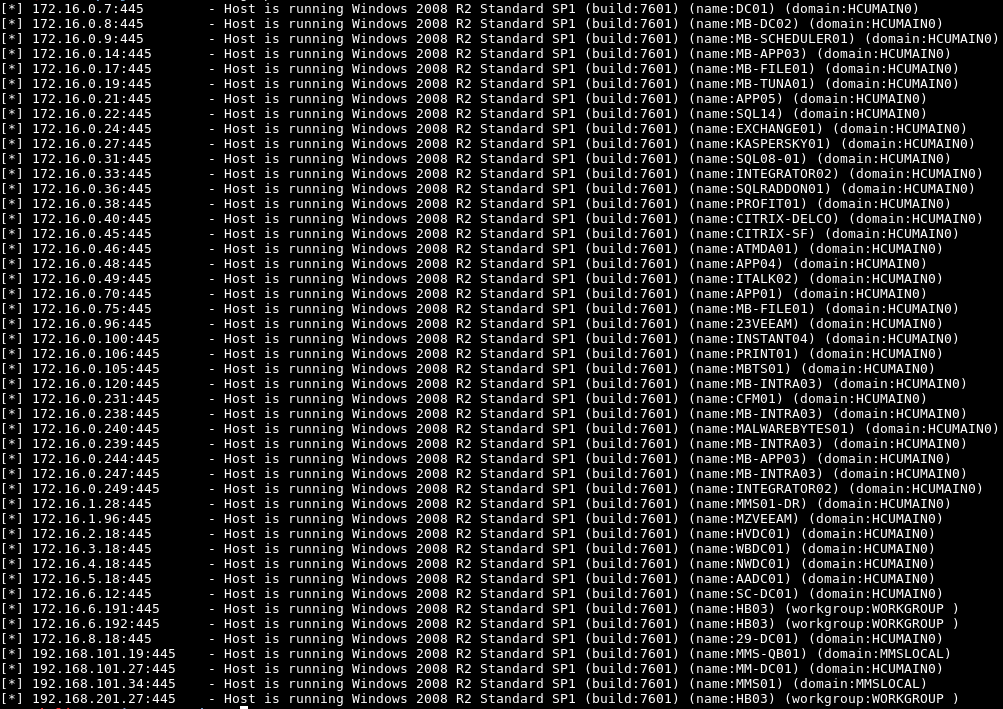


Figure 5: IP SMB Version Scan on Devices with TCP Port 389 Open as Possible Domain Controllers:

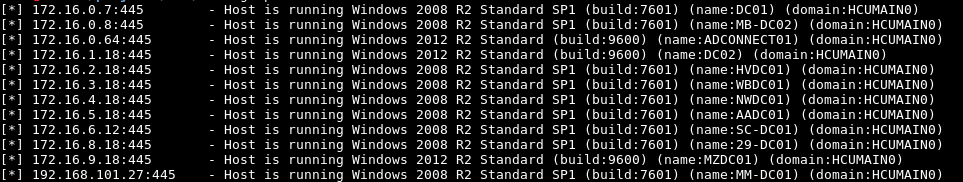


Figure 6: Service Version Scan: SMB TCP Port 445 on Windows 2012 Servers:

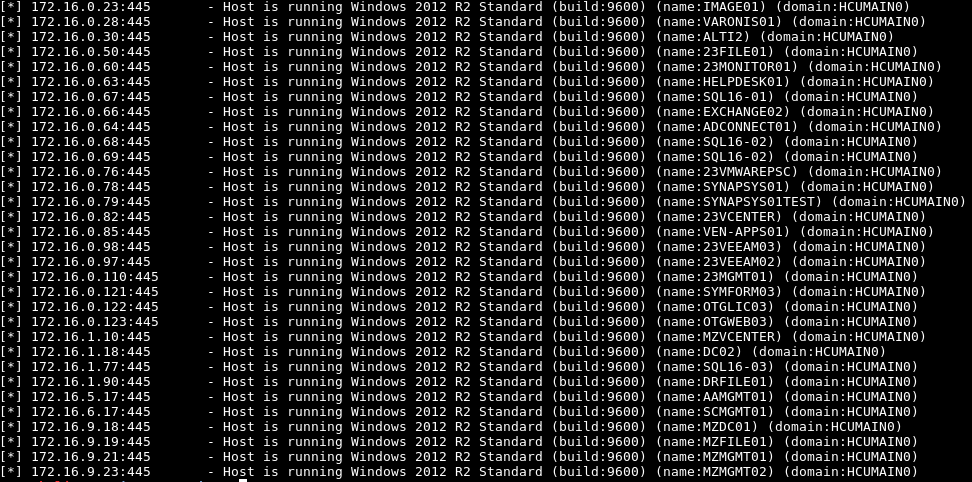


Figure 7: Service Version Scan Example of FTP TCP Port 21:

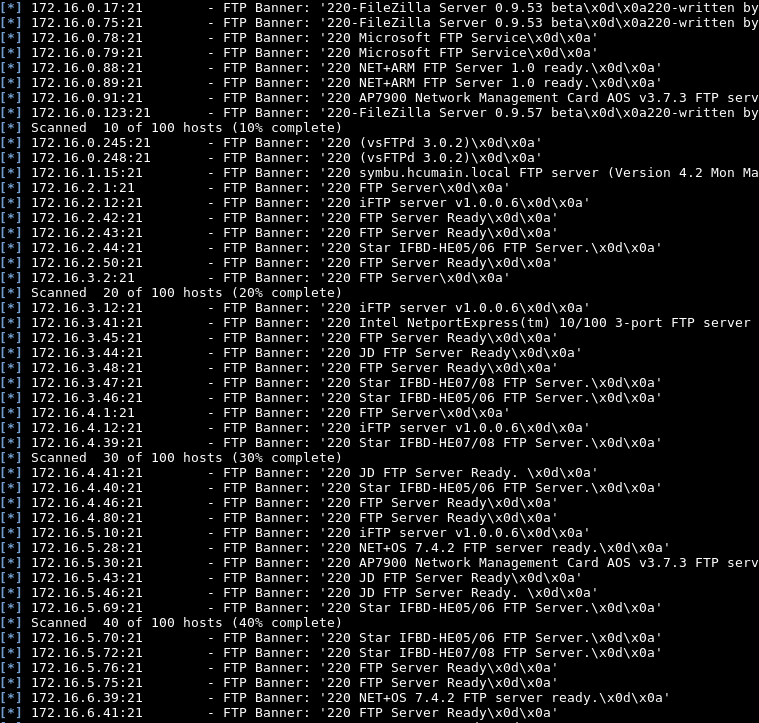


Figure 8: Service Version Scan: SSH TCP Port 22:

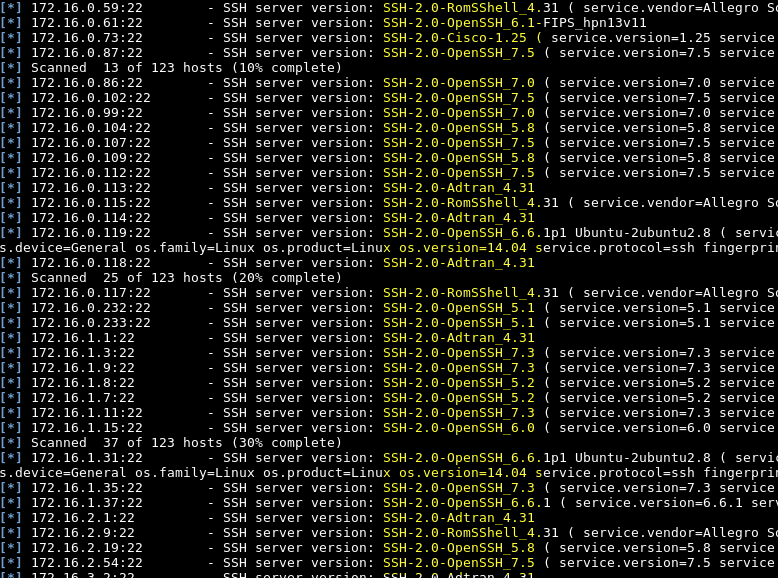


Figure 9: Service Version Scan: Telnet TCP Port 23:

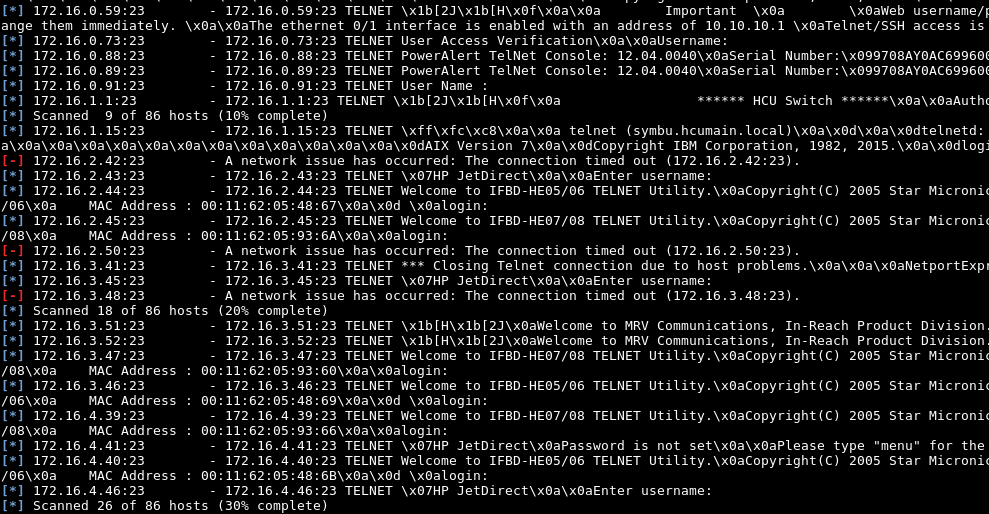
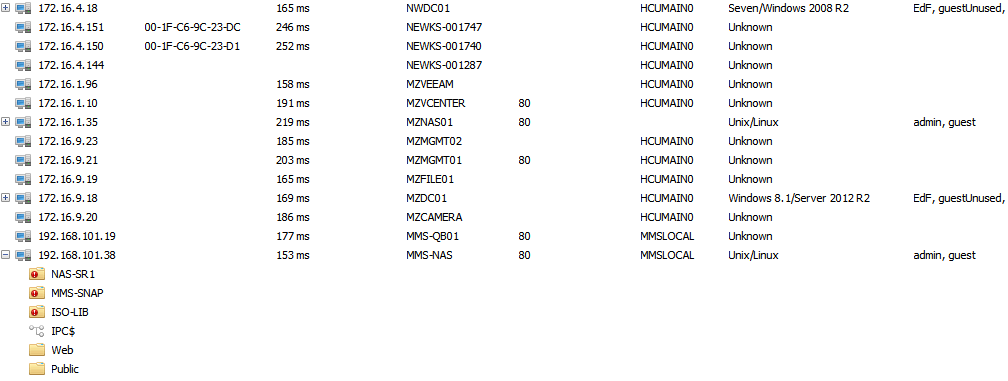


Figure 10: Example NetScan Results on Targeted Subnets:



# SECTION 2: VULNERABILITY IDENTIFICATION

This section utilizes the information from the previous section to identify the existence of the vulnerabilities. During this section, the ISA may have utilized TraceSecurity’s proprietary Cloud Security Officer (CSO) scanners, vulnerability scanners, web application scanners, and other tools, such as Metasploit, to discover vulnerabilities and match them to known exploits.

The goal of this stage was to use information gathered in the previous section of this report to perform a technical assessment of the actual existence of exploitable vulnerabilities. Network analysis identified insecurely configured services and vulnerable software versions. During the vulnerability identification stage, the ISA identified as many positive penetration venues of attack as possible. Examples of vulnerability validation are shown in the following figures. Where applicable, a proof of concept is demonstrated in the penetration testing portion of the report. TraceSecurity recommends reviewing all identified vulnerabilities in the TraceCSO portal and promptly remediating unresolved vulnerabilities.

The research of the vulnerabilities and analysis of the tools’ results indicated the following viable attack vectors are present on the credit union’s internal network. Details of the vulnerabilities can be found in Section 3 below:

* NBT-NS and LLMNR Poisoning Attack
* Anonymous Access or Missing Credentials
* Default System/Application Credentials
* Man In The Middle (MITM) Attack Vulnerability via OpenSSL
* Weak and Insecure Ciphers
* Remote Session Vulnerabilities
* CBC Ciphers over SSH
* Plaintext Authentication Protocols

Figure 11: High and Medium Vulnerabilities from TraceCSO Scanner Results:



The analyst was able to confirm the vulnerabilities located by the TraceCSO scanner throughout the penetration testing phase of the project. The content within this report detail the findings of these vulnerabilities and items found through manual testing.

# SECTION 3: PENETRATION TESTING

This section describes the ISA’s actual attempts to gain unauthorized access by utilizing the discovered ports and services in the previous section of the report. During this stage, the ISA attempted to gain access to sensitive information, exploit configuration problems, buffer overflow vulnerable systems, attempt brute-force and dictionary-based attacks, etc. If basic user privileges are gained, the ISA will attempt to escalate privileges.

The goal of this stage was to compromise vulnerable systems and gain access to sensitive information. Sensitive information includes, but is not limited to, account numbers, names, addresses, social security numbers, passwords, and usernames.

It is important to note that, for the purposes of this report, “external” attackers are considered unauthenticated and unknown third parties, while “malicious insiders,” are considered rogue employees or trusted vendors. Examples might include a remote attacker who gained access through a hypothetical vulnerability in the external network, remote social engineering, or malware, as well as an onsite attacker who gained access through wireless compromise, in-person social engineering, or physical intrusion.

Text figures in this report make use of placeholders, such as “[...],” “[REDACTED],” and “[REDACTED PASSWORD]” to sanitize sensitive information and shorten or snip output for display purposes. Potentially sensitive or confidential information in images or screenshots may be highlighted and made unreadable.

## NBT-NS and LLMNR Poisoning Attack – High Risk

The analyst used a network attack technique to trick local systems on the network into believing the analyst’s testing computer was a legitimate system providing a service requested by other systems and users on the internal network. As a result, these systems provided usernames and password hashes to the analyst to capture for offline cracking.

This technique is known as an NBT-NS (NetBIOS Name Service) and LLMNR (Link-Local Multicast Name Resolution) Poisoning Attack. NBT-NS and LLMNR are components of Microsoft systems allowing systems on the same subnet to help each other resolve hostnames with IP addresses when DNS, or a DNS entry is not available. In this situation, a malicious system could falsely identify itself as a requested system. Once the response is accepted by the victim’s system, authentication credentials are sent to the attacker’s system that contain the username and password hash or clear text password.

The analyst was able to acquire 1 username and password hash on the subnet where the TraceCSO scanner resides. Without installing a TraceCSO Scanner on each of the client’s subnets, the results of this examination are only related to the subnet of 192.168.100.0/24. Although the analyst was unsuccessful in cracking the hash within the contracted period of time, an attacker would be able to continue cracking the captured hash offline until successful.

The results of this portion of the engagement are limited in scope by the isolated entry into the client’s network as a result of a “remote” Internal Penetration Test. An attacker could continue to gather information and decipher hashes from the remaining subnets and attempt to crack those hashes offline until successful, and in turn, use the credentials to further attack the credit union’s network.

TraceSecurity recommends disabling NBT-NS and LLMNR services. If these services are required for business functionality, Trace Security recommends employing automated detection rules that can identify and prevent poisoning attacks.

These requests can be captured, and a spoofed response can be sent back to the victim from the attacking machine. These spoofed responses will tell the victim’s machine to authenticate to the attacker’s machine. Through this process, the attacker is able to capture a password hash. If possible, TraceSecurity recommends eliminating the use of LLMNR to resolve host names if initial DNS queries fail.

The steps to mitigate against the risks due to this vulnerability include enabling the network adapter setting “Disabled NetBIOS over TCP/IP,” unchecking the setting “Automatically detect settings” of the Local Area Network (LAN) settings in Internet Options, and enabling the Group Policy setting labeled “Turn off Multicast Name Resolution.” Additionally, strengthening the organization’s established password policies will also help reduce the likelihood of successfully cracking these hashes. Password requirements should contain the following characteristics, at a minimum:

- At least 15 characters in length

* Be at least 8-10 characters long; ideally longer (especially for administrative accounts)
* Use uppercase and lowercase characters
* Use alpha and numeric characters, including special characters (e.g. !?$£#@%)
* Should not be easily guessable like company names, pets name, etc.
* Not be a word from a common dictionary (e.g. orange, computer, television)
* Not have any part of the username in it
* Change the password every 60-90 days

Figure 20: Disabling LLMNR Using Policy Editor

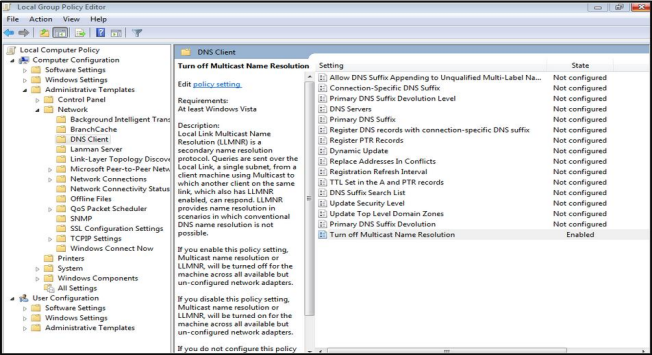


Figure 21: Disable NetBIOS

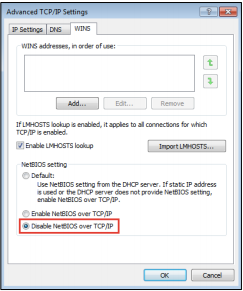


Figure 22: Uncheck “Automatically detect settings”



The following figures demonstrate the poisoning and cracking process along with articles extracted from file servers accessed with the compromised user account or account created.

Figure 12: Poisoning Attack Example Performed on the 172.16.0.0/24 Subnet with Captured Hash

The figure below demonstrates 1 of 6 hashes captured by the analyst during the engagement.

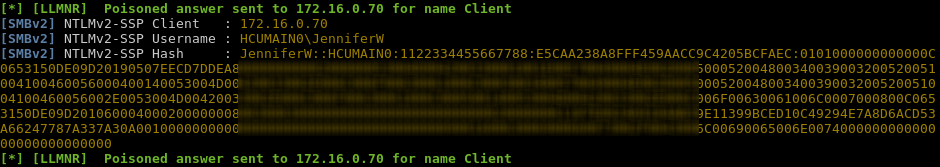
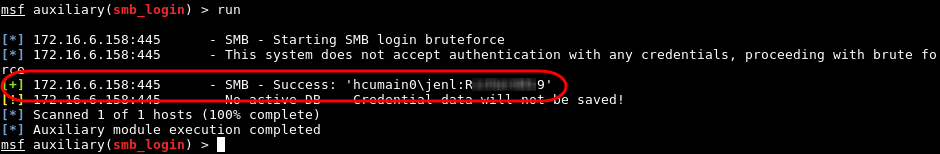


Figure 13: Hash Cracking Attempts on Captured Credentials:

The figure below demonstrates a dictionary password attack against the captured hash with over 58 billion tries per account with 2 matching passwords found. The passwords obtained by the analyst were from different hashes from the same account, resulting in a duplicate password.



***Figure 14: Confirmation of Compromised Credentials with SMB Login:***



## Privilege Elevation Vulnerability MS14-025 – High Risk

Group Policy Preferences are distributed with an XML file containing the settings is written to the SYSVOL share of domain controllers, and computers periodically query the SYSVOL share (authenticating to it using their computer account) for updates to the group policy. Several of the Group Policy Preferences store credentials and passwords with a static key encryption written to the XML file along with the rest of the settings. Details of the key are documented in MSDN: http://msdn.microsoft.com/en-us/library/cc422924.aspx. An attacker with access to the SYSVOL share (which is open to any authenticated user) can obtain the AES encryption key used to encrypt/decrypt passwords set with GPP; allowing the attacker to obtain the credentials.

The analyst used confirmed credentials of non-domain accounts to exploit devices identified as Domain Controls with TCP Port 389 open. By running modules within the Metasploit Framework the analyst was able to quickly extract one or more possible credential sets to further elevate privileged access to take control of the organization’s Domain Controls and access sensitive network storage locations.

TraceSecurity recommends applying updates related to Microsoft Bulletin MS14-025 on all published affected operating systems listed within the bulletin. Additional resources can be found in the Microsoft knowledge base article number 2962486.

Figure 15: Table – Systems Vulnerable to MS14-025 Vulnerability:

|  |  |  |
| --- | --- | --- |
|  |  |  |

Figure 15: Administrative Password Extracted from XML Files located in Sysvol folder on 10.10.10.10:

## Weak/Dictionary Password Vulnerability – High Risk

Insecure passwords present a risk of access by an attacker that would otherwise have limited or no access to systems or resources within the organization’s network. Any network device that an attacker can gain access to poses a risk of lost productivity, network access, and loss of sensitive data.

The analyst conducted a simple test using the password “Spring2018!” to test usernames enumerated during other exploits of this engagement by logging into a confirmed system share on a system with TCP Port 445 open as an SMB Share.

TraceSecurity recommends implementing strong password enforcement along with expiration periods, password retention rules and auditing procedures to periodically verify the effectiveness of the overall password policies maintained by the organization. The following guidelines are useful when developing password policies:

* Be at least 8-10 characters long; ideally longer.
* Use uppercase and lowercase characters
* Use alpha and numeric characters, including special characters (e.g. !?$£#@%)
* Should not be easily guessable like company names, pets name, etc.
* Not be a word from a common dictionary (e.g. orange, computer, television)
* Not have any part of the username in it
* Change the password every 60-90 days

Figure 15: User(s) Confirmed with the password “Spring2018!” during a Brute Force Scan:

## Anonymous Access or Missing Credentials – High Risk

Many devices and services are preconfigured to allow anonymous access that provides many of the functions necessary to easily configure the functionality and security of the equipment before placing them on an organization’s production network. Although these services are configured to allow anonymous access to make installation more convenient during initial configuration efforts; malicious parties will attempt to authenticate to these services anonymously to cause disruption to the client’s network or gather compromising information. Due to the ease of this type of attack, it has been given a high risk rating.

The analyst discovered multiple devices and services that allowed anonymous authentication during the pen-testing phase of the engagement. Although no changes were made to the services detected, per the pre-disclosed rules of engagement, the options are present and considered a high risk for a multitude of vulnerabilities associated with unauthorized access to network devices and services. The analyst gained access to administrative features and enumerated information to help with mapping the client’s internal network to further advance the attack methods during the engagement.

TraceSecurity recommends processing all network devices and services through an advanced hardening procedure to ensure all anonymous configurations have been removed or changed to require strictly encrypted access rights to authorized personnel only.

The following figures demonstrate the anonymous access to devices and information on the client’s network. The examples listed below are only a sample of the effective systems compromised during this phase of the testing, the client should check all devices running the services related to the examples below:

Figure 15: Table - Anonymous LDAP Enumeration on Multiple Hosts:

The following table demonstrates the listing of domain accounts with their descriptions without authentication. Additional systems found during this test with similar vulnerabilities include:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.0.18  172.16.2.18 | 172.16.3.18  172.16.4.18 | 172.16.5.18  172.16.6.12 | 172.16.8.18  192.168.101.27 |

Figure 16: Anonymous LDAP Enumeration Example on 172.16.2.18:

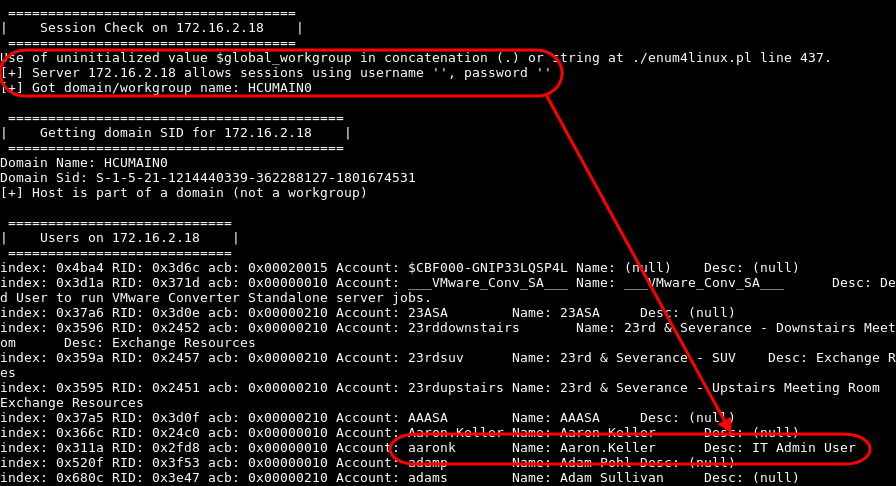


Figure 17: Anonymous LDAP Enumeration on 172.16.3.18 Showing Renamed Administrator Account:

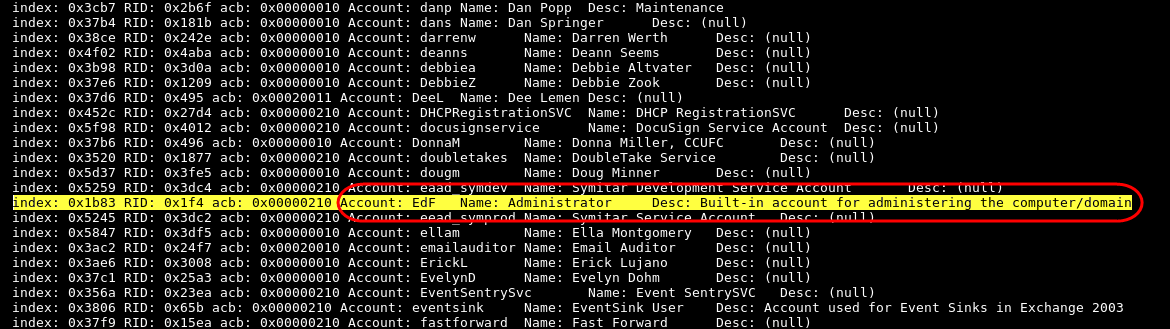


Figure 18: System Properly Configured to Prevent Anonymous LDAP Lookups at 172.16.2.76:

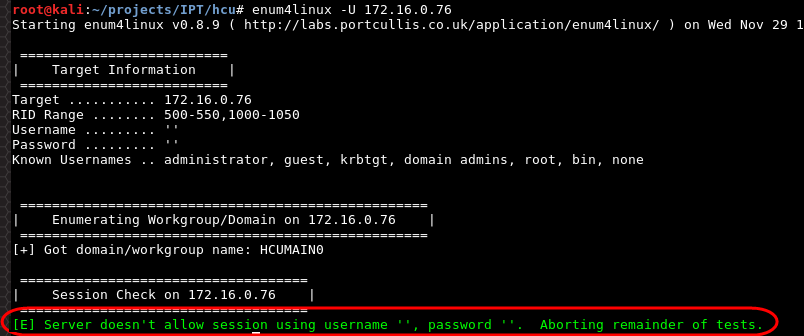


Figure 19: Anonymous Administrator Access to HP Printer Located at https://172.16.2.50:

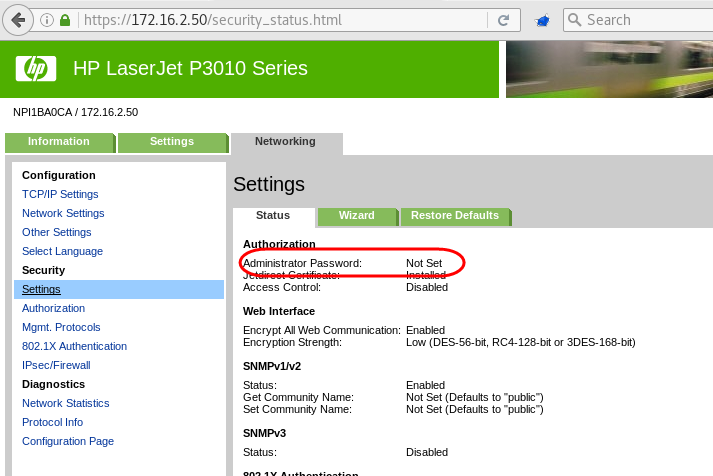


Figure 20: Table - Anonymous Read Access to FTP Services on Multiple Devices:

The specified device shows to have Read access from the scanning results. The analyst attempted to files from the specified devices without success. Although the analyst was unable to access files on the specified systems, the connections were established and any contents placed on this device by an authorized user would be exposed to malicious parties. The affected systems identified are:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.2.42  172.16.2.43  172.16.6.48  172.16.6.54  172.16.6.56  172.16.9.81 | 172.16.6.57  172.16.6.59  172.16.7.76  172.16.7.75  172.16.7.77  172.16.9.75 | 172.16.7.79  172.16.7.82  172.16.7.84  172.16.7.85  172.16.8.42  192.168.101.66 | 172.16.8.43  172.16.9.74  172.16.9.78  172.16.9.83  172.16.9.82  192.168.101.67 |

Figure 21: Anonymous Read Access Example to FTP Services on 192.168.10.5:

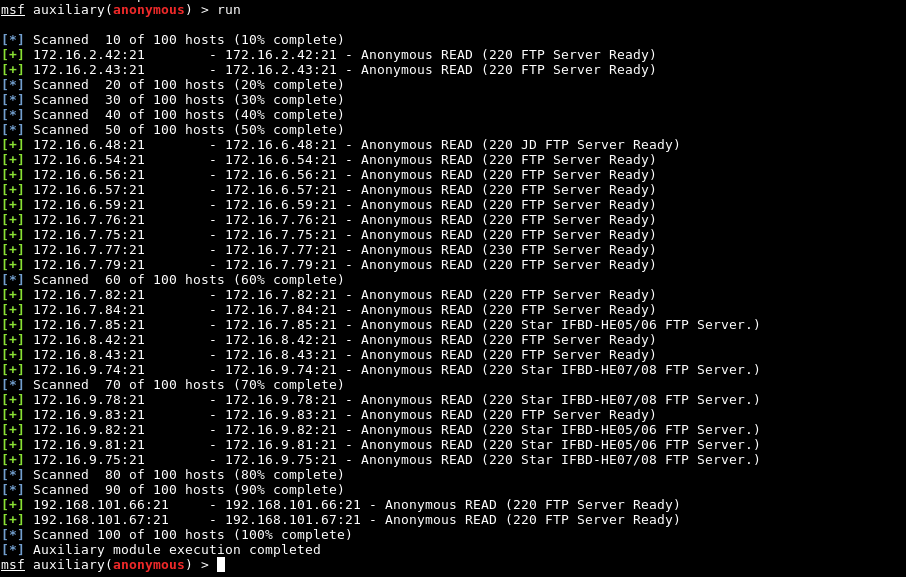


Figure 22: Anonymous Access over Telnet TCP Port 23 from Version Scan on Multiple Devices:

Multiple devices demonstrate the absence of a telnet password. The capability for an attacker to gain control of the specified devices could expose sensitive information or allow a DoS (Denial of Service) to be performed on the private network.

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.2.50  172.16.3.48 | 172.16.4.41  172.16.5.46 | 172.16.7.76  172.16.7.77 | 172.16.9.83 |

Figure 23: “Password is not set” message on Multiple Devices over Telnet:

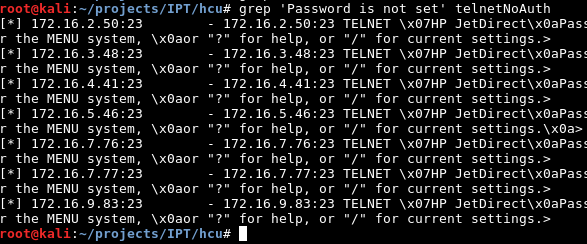
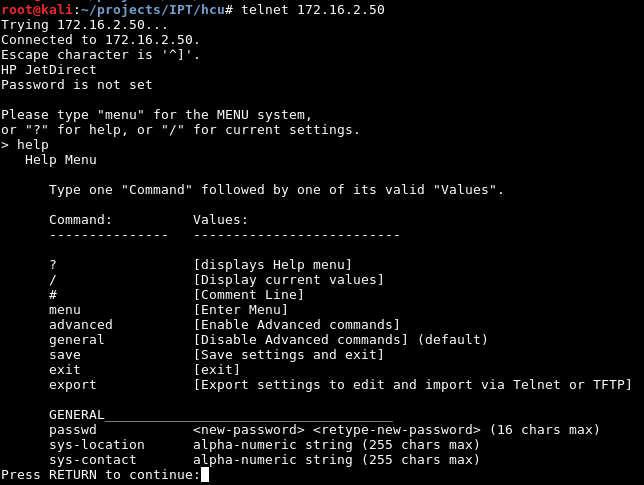


Figure 24: Anonymous Access Connection Example to Telnet TCP Port 23 on 172.16.2.50:



## Default CREDENTIALS – High Risk

Default or factory credentials that are shipped with devices that connect to the network provides an attacker with easily access systems and settings through device manuals and tutorials available to the public over the internet. Once a device is found and a service or manufacture is identified, an attacker will first attempt to login to devices with the manufactures default credential settings to locate quick targets for an attack. Any network device that an attacker can gain access to poses a risk of lost productivity, network access, and loss of sensitive data.

Using common scanner techniques the analyst was able to discover device and/or service identification on the systems identified in this vulnerability that accepted the factory default credentials for access. Although the analyst did not make any changes to the devices per the rules of engagement, the opportunity was available and documented for this report and additional information was extracted from the specified devices to further advance the attack methods.

TraceSecurity recommends establishing a process to ensure that all factory default settings are changed prior to placing a service into production. TraceSecurity also recommends establishing a process to ensure that all factory default settings are changes prior to placing a service into production with strong authentication that restricts access to users with a business need to access the resource. These policies are often referred to as a Systems Hardening Policy, located in the organization’s Systems Security Manual or Procedures.

TraceSecurity recommends updating the existing policies and procedures to include the hardening practices and development testing necessary to secure equipment is secure by replacing the default credentials, installing service packs, and updating to the latest firmware, provided by the manufacture, and testing the device in a safe environment (sand box) or offline mode to ensure that all network devices are secure prior to deployment to the production network.

The following figures show the devices that accepted default credentials:

Figure 25: Table - SNMP “read-write” Login with Default Community Strings on Multiple Hosts:

The figure below is an example excerpt from the scanning conducted by the analyst. The following list of devices were found to have Read and Write access with default SNMP Strings:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.0.212  172.16.4.41  172.16.4.41  172.16.5.68  172.16.5.68  172.16.5.75  172.16.5.75  172.16.6.41 | 172.16.6.41  172.16.6.49  172.16.6.49  172.16.6.57  172.16.6.57  172.16.6.59  172.16.6.59 | 172.16.6.60  172.16.6.60  172.16.7.75  172.16.7.82  172.16.9.83  172.16.9.83  172.16.9.85 | 172.16.9.87  172.16.9.88  172.16.9.86  172.16.9.86  192.168.101.68  192.168.101.68  192.168.101.75 |

Figure 26: SNMP “read-write” Login Example with Default Community Strings on Multiple Hosts:

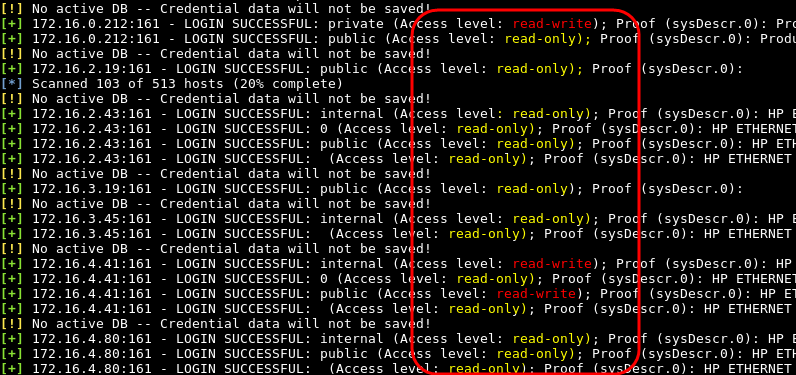


Figure 27: Table - Default SNMP Community Strings on HP Printers Reveal Usernames from Print Logs:

The analyst executed an enumeration tool that targets default SNMP strings to extract information from HP Printers identified during the mapping phase of the penetration test. The figure below demonstrates an expert from the information collected to compile a list of users to advance attack methods. The following list of devices were utilized to extract the usernames and should be reviewed to ensure proper hardening techniques are used to remove default credentials from devices prior to deploying them to the production environment:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.0.104  172.16.0.109  172.16.0.212  172.16.0.213  172.16.0.84  172.16.0.86  172.16.0.91  172.16.0.99  172.16.2.19  172.16.2.42  172.16.2.43  172.16.2.50  172.16.3.19  172.16.3.44  172.16.3.45  192.168.101.68 | 172.16.3.48  172.16.4.19  172.16.4.41  172.16.4.80  172.16.5.19  172.16.5.30  172.16.5.43  172.16.5.49  172.16.5.68  172.16.5.75  172.16.5.76  172.16.6.41  172.16.6.42  172.16.6.43  172.16.6.44 | 172.16.6.49  172.16.6.53  172.16.6.54  172.16.6.56  172.16.6.57  172.16.6.59  172.16.6.60  172.16.7.75  172.16.7.76  172.16.7.77  172.16.7.78  172.16.7.79  172.16.7.82  172.16.7.83  172.16.7.84  192.168.101.75 | 172.16.7.88  172.16.8.42  172.16.8.43  172.16.8.44  172.16.9.83  172.16.9.85  172.16.9.86  172.16.9.87  172.16.9.88  192.168.101.60  192.168.101.63  192.168.101.64  192.168.101.65  192.168.101.66  192.168.101.67 |

Figure 28: SNMP Community Strings Example on HP Printers Reveal Usernames from Print Logs:

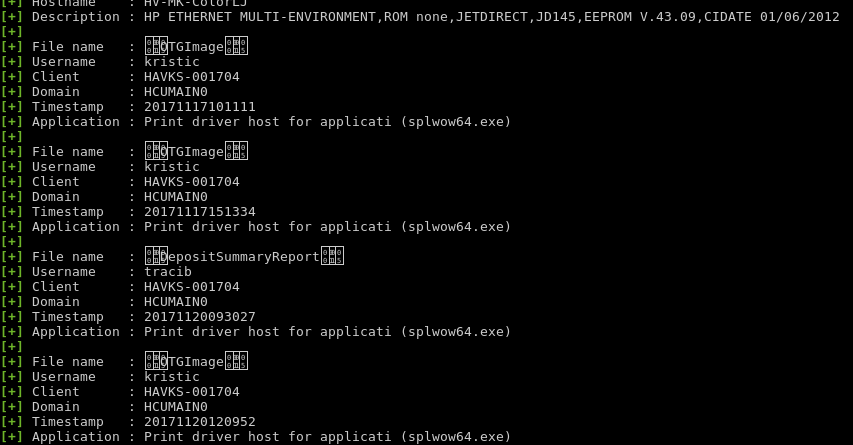


Figure 29: Default Admin Credentials Accepted on AudioCodes located at http://172.16.0.212:

The device in the figure below accepted “Admin” as the username and password to access the administrative features of the application.

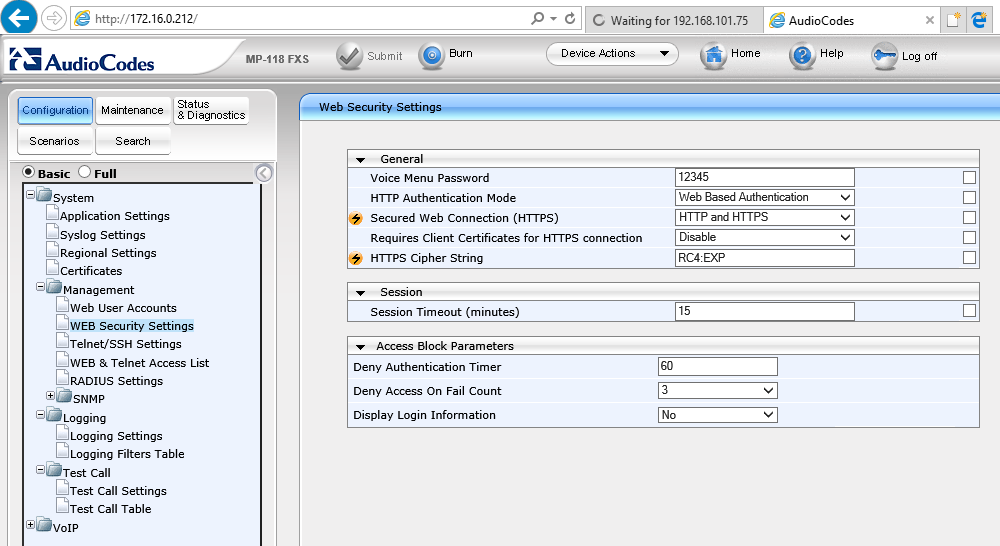
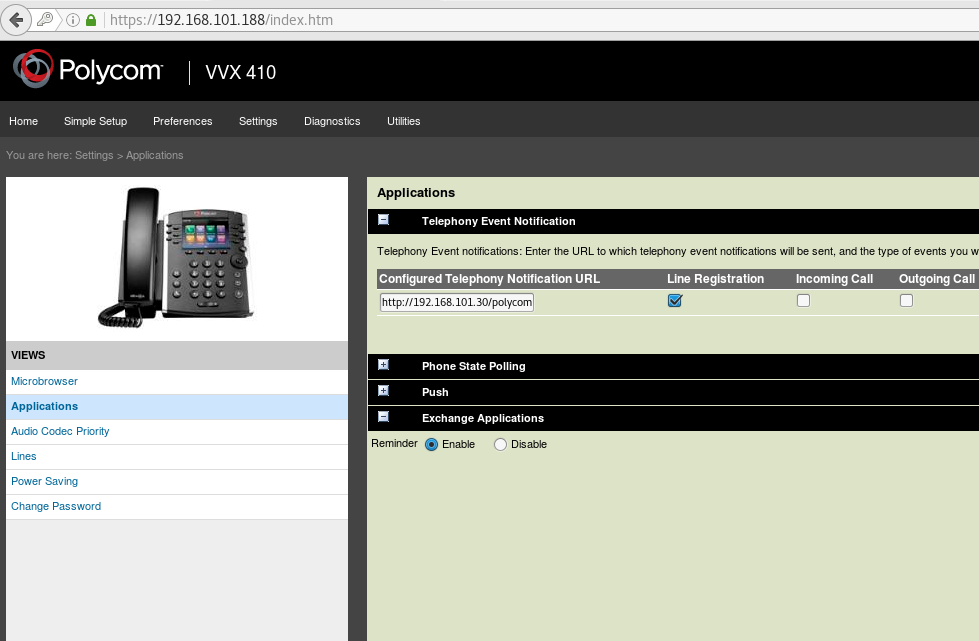


Figure 30: Table - Default Credentials Accepted Polycom Device Located on Multiple Devices:

The image below demonstrates the use of “user” and a password of “123” to access the user features of the phone. The analyst found the following devices running similar applications that should be evaluated for similar vulnerabilities:

|  |  |  |
| --- | --- | --- |
| <https://192.168.101.188/>  <https://192.168.101.135/> | <https://172.16.5.111/>  <https://192.168.101.102/> | <https://192.168.101.122/> |

Figure 31: Default Credentials Accepted Polycom Device Located at https://192.168.101.188:



## Multiple IPMI Authentication Vulnerabilities – medium risk

Intelligent Platform Management Interface (IPMI) is an interface specification adopted by hardware vendors to allow remote administration at the system or firmware level. IPMI run over the Baseboard Management Controller (BMC) which provides access to BIOS, Disks, and other hardware connected to the system’s controller. Remote booting and monitoring as well as limited network services are also available through an exploited system.

The analyst identified server systems on the internal network with UDP port 623 open and was able to confirm exploitable machines without disrupting services during the manual penetration testing engagement. Details provided within this report along with screen captures demonstrate the tools and exploits used to expose systems or reveal systems vulnerable.

TraceSecurity recommends restricting all IPMI traffic to trusted internal networks and devices only though ACLs or routing controls through management VLANS for IPMI traffic. All systems with UDP Port 623 should be evaluated by the organization and mitigated according to the recommendations provided by the manufacture. IPMI traffic should also be implemented as part of an ongoing vulnerability scans for both the unauthenticated, trusted network traffic and all external network traffic for abnormal activity.

Figure 32: Table – Devices Identified on the Network with IPMI UDP Port 623 Open:

## Man In The Middle (MITM) Attack Vulnerability via OpenSSL – medium risk

OpenSSL Man In The Middle (MITM) attacks allow an attacker to issue false CCS packets to both the server and supplicant that cause the master key to return a zero length key that force all connections to the downgraded key allowing the attacker to decipher all communication between the two devices. Once a compromised connection is established the malicious user can collect the decrypted information or alter the information before it is delivered to the receptive device.

The analyst was able to confirm the existence of this vulnerability through a Metasploit module designed to look for this particular issue. The provided screen shots demonstrate the presence of this man-in-the-middle attack that could compromise the confidentiality and integrity of communication between two vulnerable OpenSSL endpoints. The analyst was unable to demonstrate the process necessary to fully exploit this vulnerability within the timeframe of this engagement. The results of the provided scans indicate the presence of OpenSSL versions that are vulnerable.

TraceSecurity recommends upgrading to OpenSSL 1.01 or later. OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master keys. OpenSSL updates to all systems running affected versions of OpenSSL are encouraged.

Figure 32: Table - OpenSSL MITM Attack Vulnerability Confirmed on Multiple Devices over TCP Port 443:

The figure below demonstrates all of the devices found by the analyst with the ChangeCipherSpec vulnerability. The following devices were found to have the CCS vulnerability through the testing results in the figure:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.0.104  172.16.0.109  172.16.0.114  172.16.0.212  172.16.0.213  172.16.1.8  172.16.1.7  172.16.2.19  172.16.2.42  172.16.5.49  172.16.5.75  172.16.7.7 | 172.16.2.43  172.16.3.15  172.16.3.19  172.16.3.45  172.16.3.48  172.16.4.1  172.16.4.14  172.16.4.46  172.16.5.46  172.16.6.41  172.16.9.83 | 172.16.6.42  172.16.6.49  172.16.6.50  172.16.6.54  172.16.6.56  172.16.7.76  172.16.7.77  172.16.7.79  172.16.7.82  172.16.7.84  10.10.10.4 | 192.168.101.18  192.168.101.26  192.168.101.28  192.168.101.42  192.168.101.64  192.168.101.66  192.168.101.68  192.168.101.162  192.168.205.1  192.168.201.9  192.168.201.25 |

Figure 33: OpenSSL MITM Attack Vulnerability Confirmed on Multiple Devices over TCP Port 443:

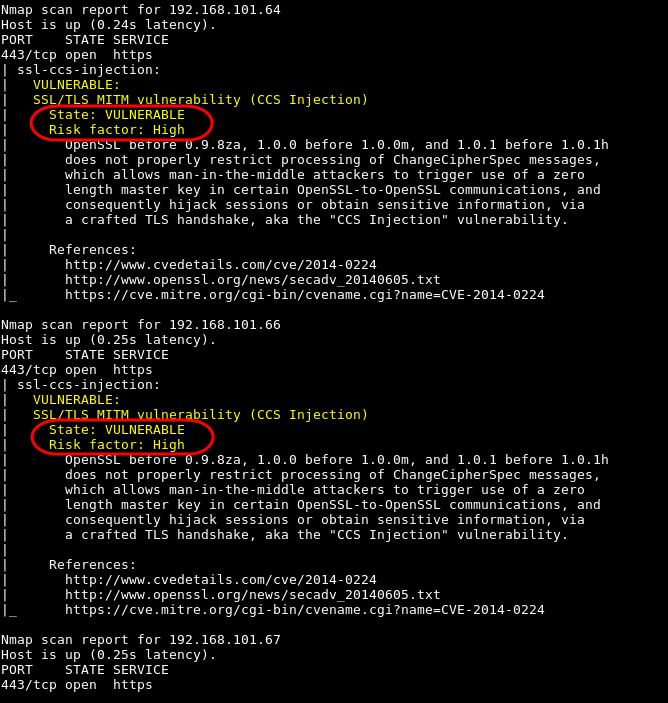
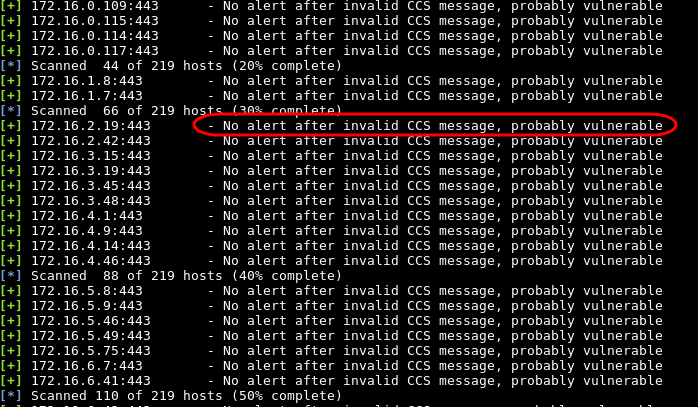


Figure 34: OpenSSL MITM Attack Vulnerability Confirmed on Multiple Devices over TCP Port 443:



## Administrative Bypass Vulnerability – Medium Risk

An attack known as Authentication Bypass allows hackers to avoid authentication, in some cases, to the entire security subsystem or a service or appliance. Most attacks occur on Web sites and can happen due to errors in the design or implementation of a system. Systems vulnerable to authentication bypass exhibit either a failure to enumerate and enforce the access policy or a weak authentication system that allows a valid identity to be forged. Either the Web access control system does not have the full set of URIs that enumerate the application or Web site under attack, or the access control system does not extend to the section of the site that needs protection. If a web application implements access control only on the log in page, the authentication schema could be bypassed. For example, if a user directly requests a different page via forced browsing, that page may not check the credentials of the user before granting access.

The analyst discovered a device running an intranet message board or informational appliance that displayed upcoming events as well as current employee schedules and changes for the day and was able to circumvent the authentication mechanism of the server by conducting a directory enumeration attack and browse directly to the site’ management panel without authentication. Once behind the analyst was at the management interface, they were able to conduct administrative functions without providing credentials. The analyst conducted a rogue post and demonstrated the removal of the rogue post. The activities indicate an erosion in authentication that compromises the integrity of information shared on the intranet site. Although the root folder of the administrative folder required authentication, the sub-directories and related menu items did not enforce authentication during this engagement.

TraceSecurity recommends auditing all application authentication settings and system permissions to ensure the authentication requirements are effective throughout the site and application. TraceSecurity also recommends implementing periodic tests to ensure hardening standards have been implemented to prevent authentication bypass and related exploits to the hosted applications.

The following figures show the devices that are missing credentials:

***Figure 25a: Information Located on Intranet Site at http://XXXX***

***Figure 25b: DirB Search Results on http://XXXX***

The image below demonstrates the location of directories located on the intranet site located on XXXX. The analyst attempted to visit these directories and pages to explore opportunities to compromise the information and attempt to control the system.

## Remote Session Vulnerability “WannaCry” – medium risk

EternalBlue or WannaCry exploits a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol. This vulnerability is denoted by entry CVE-2017-0144 in the Common Vulnerabilities and Exposures (CVE) catalog. The vulnerability exists because the SMB version 1 (SMBv1) server in various versions of Microsoft Windows accepts specially crafted packets from remote attackers, allowing them to execute arbitrary code on the target computer.

The analyst was able to confirm the existence of this vulnerability through a Metasploit module designed to look for the presence of the EternalBlue attack that could compromise the confidentiality and integrity of communication by allowing a remote session between the vulnerable system and the attaker. The analyst was unable to demonstrate the process necessary to fully exploit this vulnerability within the timeframe of this engagement. The results of the provided scans indicate the patch has not been installed per Microsoft’s security bulletin MS17-010.

TraceSecurity recommends following the Microsoft issued security bulletin MS17-010, which details the flaw and announced that patches had been released for all Windows versions that were currently supported at that time, these being Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, and Windows Server 2016, as well as Windows Vista. The WannaCry ransomware attack uses the EternalBlue vulnerability to spread itself.

TraceSecurity inherently recommends ensuring that all Microsoft patches are tested and implemented on all related systems and services to ensure new vulnerabilities are patched in a timely manner.

Figure 35: Table - EternalBlue or WannaCRY Vulnerability Found on Multiple Hosts:

|  |  |
| --- | --- |
| 172.16.0.31 | 172.16.6.191 |

Figure 36: EternalBlue or WannaCRY Vulnerability Found on 172.16.6.191:

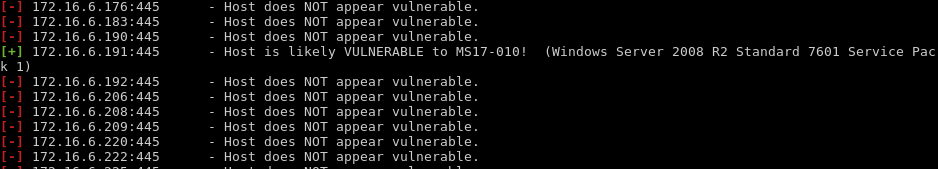


Figure 37: Failed Attempt to Start a Remote Session through MS17\_010 Exploit on 172.16.0.31

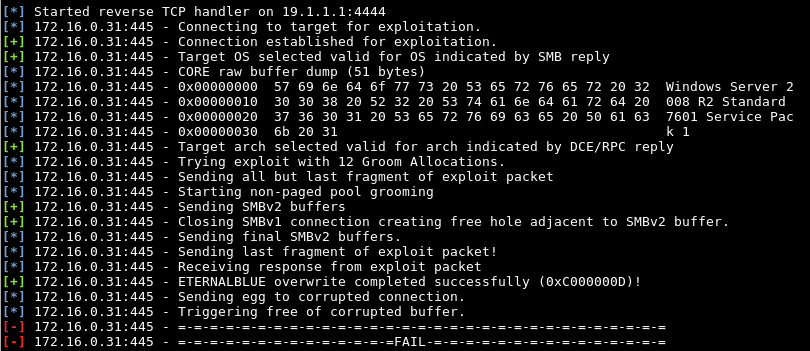
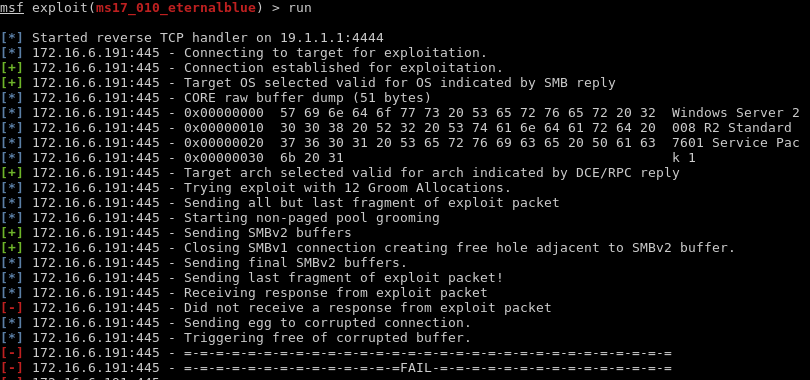


Figure 38: Failed Attempt to Start a Remote Session through MS17\_010 Exploit on 172.16.6.191



## Plaintext protocols in use – medium risk

One or more systems were found to be using plain-text protocols such as Telnet or HTTP. These protocols passes login credentials in plaintext, which can easily be captured by attackers to enumerate logins to penetrate the perimeter of an organization's network. Once authenticated to one Telnet session or access a web application interface over http, it is possible that other devices could accept the authentication level of the breached connection and allow deeper penetration once the credentials are captured.

The analyst discovered one or more systems using the Telnet and/or http protocols. Although the login attempts were unsuccessful, they prove the concept of possible login attempts from malicious parties. With more time, an attacker could sniff or act as a “Man In The Middle" (MITM) to capture usernames and passwords of legitimate logins.

TraceSecurity recommends replacing Telnet and http with encrypted protocols for devices that require authentication or transmit sensitive information. If insecure protocols cannot be disabled, TraceSecurity recommends limiting the accessibility of the devices with an ACL or blocking all port activity within the organization’s network with routing rules within the scheme of the organization’s network rules.

Figure 39: Plaintext Protocol Found on http://172.16.5.30 that Accepts Login Credentials:

Although the analyst was unable to successfully login to the specified device, the login screen passes the credentials in plain-text that would allow an attacker to sniff out the correct credentials during a MITM (Man In The Middle) attack.

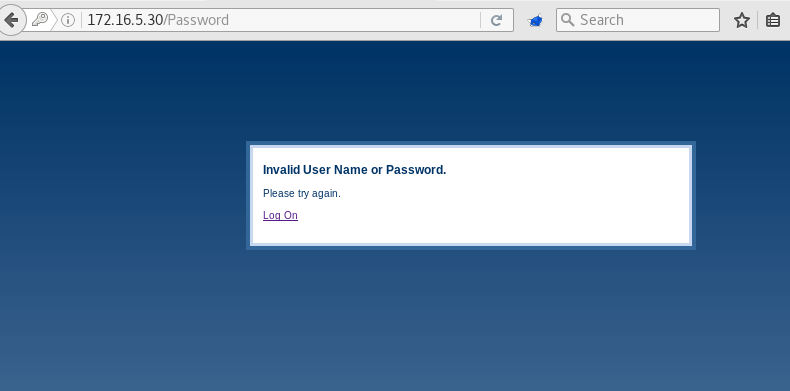


Figure 40: Plaintext Protocol Found on http://172.16.8.71 that Accepts Login Credentials:

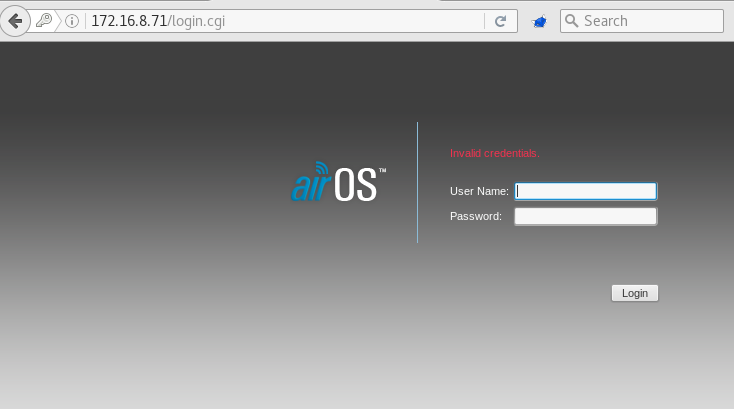
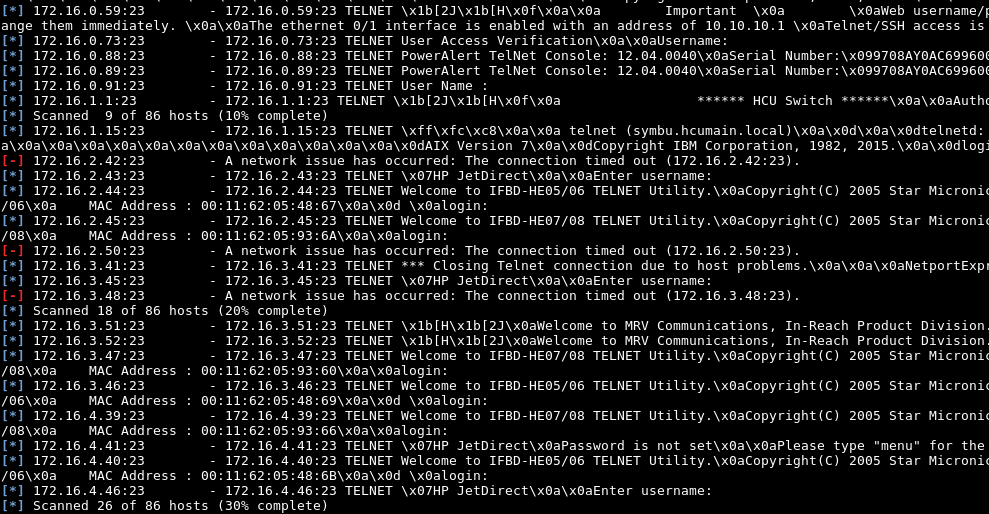


Figure 41: Table - Telnet Version Scan on Multiple Devices with TCP Port 23 Open:

The figure below shows the analyst’s successful login with anonymous credentials to a device with telnet enabled. The following devices were also found to have telnet enabled and should have the described recommendation applied:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.0.11  172.16.0.16  172.16.0.15  172.16.0.59  172.16.0.73  172.16.0.88  172.16.0.89  172.16.0.91  172.16.1.1  172.16.1.15  172.16.2.42  172.16.2.43  172.16.2.44  172.16.2.45  172.16.2.50  172.16.3.41  172.16.3.45  172.16.3.48  172.16.3.51  172.16.3.52  192.168.101.68  10.20.36.10 | 172.16.3.47  172.16.3.46  172.16.4.39  172.16.4.41  172.16.4.40  172.16.4.46  172.16.4.54  172.16.4.52  172.16.4.53  172.16.4.55  172.16.4.80  172.16.5.28  172.16.5.30  172.16.5.46  172.16.5.69  172.16.5.70  172.16.5.72  172.16.5.76  172.16.5.75  172.16.6.39  192.168.101.91  192.168.201.9 | 172.16.6.41  172.16.6.42  172.16.6.45  172.16.6.46  172.16.6.49  172.16.6.48  172.16.6.54  172.16.6.53  172.16.6.56  172.16.6.57  172.16.6.59  172.16.7.76  172.16.7.75  172.16.7.77  172.16.7.79  172.16.7.82  172.16.7.84  172.16.7.85  172.16.7.88  172.16.8.40  192.168.101.92 | 172.16.8.41  172.16.8.42  172.16.8.43  172.16.8.44  172.16.9.1  172.16.9.74  172.16.9.78  172.16.9.83  172.16.9.82  172.16.9.81  172.16.9.75  10.10.10.1  10.10.10.3  10.10.10.6  10.10.10.9  192.168.101.12  192.168.101.64  192.168.101.66  192.168.101.65  192.168.101.67  10.20.36.1 |

Figure 42: Telnet Version Scan on Multiple Devices with TCP Port 23 Open:



## MS SQL Server DR-Dos Amplification – Medium Risk

The analyst identified a host that has MS SQL Server installed and prone to reflected DRDoS vulnerability. The MS SQL Server Resolution Service allows a client to interrogate a server hosting a SQL Server installation and to receive back detailed information about the SQL Server instances available on the server. The client sends a one-byte request to the server, and the server responds with a variable-length message containing instance names, versions, and other connection details.

The vulnerability is probable due to a series of Nmap scans and MSSql Ping responses from the identified devices.

Successful exploitation will allow remote attackers to cause Distributed Reflection Denial of Service (DRDoS) conditions against remote hosts.

TraceSecurity recommends restricting access to MS Sql servers to any unauthorized traffic.

Figure 43: Table - DRDoS Amplification probable on Multiple Devices:

The following devices were found to be vulnerable to this attack method by the analyst during the testing phase of the engagement:

|  |  |  |
| --- | --- | --- |
| 172.16.0.22 | 172.16.0.31 | 172.16.0.36 |

Figure 44: Example of Nmap Script Results Showing Possible Vulnerabilities:

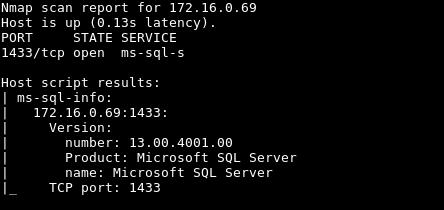
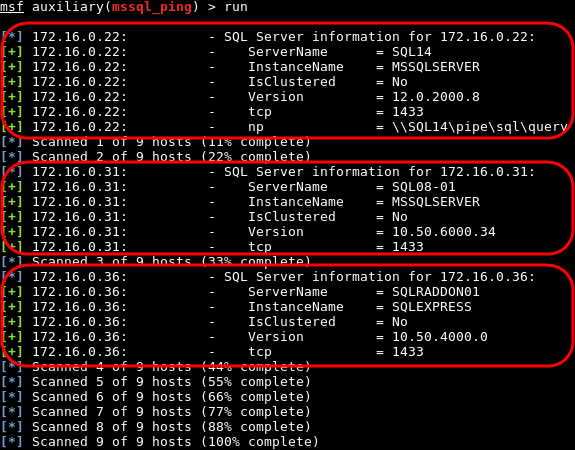


Figure 45: Metasploit Results Confirming the Potential for DRDoS Amplification on 3 devices:



## Anonymous Domain User Enumeration – Medium Risk

By default, Windows allows anonymous users to perform enumeration of the SAM account or user names as well as network shares. When left changed, an unauthorized user could anonymously list account names and shared resources; thereby, using the information to attempt authentication attacks and conduct skillfully planned social-engineering attacks.

During the penetration test the analyst was able to retrieve usernames with anonymous credentials from Windows server located at XXXXX. Using common tools the analyst was able to send randomized account requests without authentication to the system and gather SAM user names and network resources or shares.

TraceSecurity recommends the organization evaluate the best practices published by Microsoft that encourages the Anonymous Logon Policy to be Enabled, with the credit union’s network and system connectivity scheme to prevent unauthorized users from listing account names and network shares. The policy is located at: \Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.

***Figure 26: Domain Users Enumerated from XXXXX with Anonymous Access:***

## CBC Ciphers Detected over ssh – Low Risk

One or more systems were found using CBC cipher algorithms over SSH. CBC ciphers can allow an attacker to recover up to 32 bits of plaintext from an arbitrary block of ciphertext from an SSH connection. A successful attack exploits the encrypted length field and the wait state that arises in OpenSSH providing the length checks pass. The MAC error reveals the amount of data expected in the packet, and, through this, the content of the length field. This leaks information about the target ciphertext block so that the attacker can generate a shortened, random cipher that will reveal up to 32 bits of the encrypted cipher.

The analyst identified the presence of CBC ciphers by running Nmap scripts against a list of devices with TCP Port 22 open. The subsequent screen capture is a sample of the results. All 66 devices scanned with TCP Port 22 open contained CBC ciphers available.

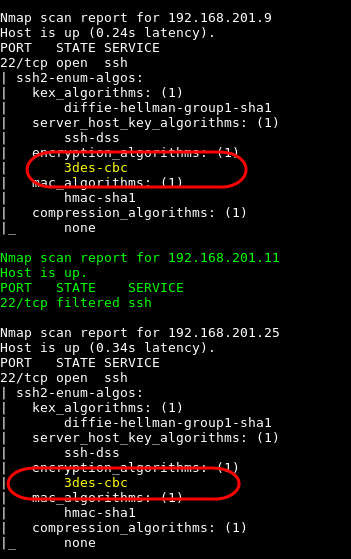
TraceSecurity recommends updating all necessary SSH protocols with AES CTR mode and arcfour ciphers as they are not vulnerable to CBC attack. These may be preferentially selected by placing the following directive in sshd\_config and ssh\_config: Ciphers aes128-ctr,aes256-ctr ,arcfour256 ,arcfour ,aes128-cbc ,aes256-cbc. OpenSSH has addressed the CBC vulnerabilities in version 7.5 and 7.5p1 and later.

Figure 55: Table - Nmap Scans Revealing the use of CBC Ciphers on Multiple Hosts:

The following figure demonstrates the presence of CBC ciphers on the designated host. The following list of devices also contained CBC ciphers and should be have the described changes made to reduce the risk of exploitation minimized or eliminated:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.0.1  172.16.0.2  172.16.0.11  172.16.0.16  172.16.0.15  172.16.0.18  172.16.0.37  172.16.0.42  172.16.0.59  172.16.0.61  172.16.0.73  172.16.0.87  172.16.0.102  172.16.0.104  172.16.0.107  172.16.0.109  172.16.0.112  172.16.0.113  172.16.0.115  172.16.0.114  172.16.0.119  172.16.0.118  172.16.0.117  172.16.0.232  172.16.0.233 | 172.16.3.19  172.16.3.51  172.16.3.52  172.16.4.1  172.16.4.10  172.16.4.9  172.16.4.54  172.16.4.52  172.16.4.53  172.16.4.55  172.16.5.1  172.16.5.8  172.16.5.9  172.16.5.28  172.16.6.1  172.16.6.4  172.16.6.5  172.16.6.6  172.16.6.8  172.16.6.7  172.16.6.9  172.16.6.11  172.16.6.10  172.16.6.39  172.16.6.113 | 172.16.7.1  172.16.1.1  172.16.7.7  172.16.8.10  172.16.8.17  172.16.9.1  10.10.10.1  10.10.10.3  10.10.10.2  10.10.10.4  10.10.10.6  10.10.10.5  10.10.10.8  10.10.10.9  172.16.1.7  172.16.1.11  172.16.1.15  172.16.1.31  172.16.1.37  172.16.2.1  172.16.2.9  172.16.2.19  172.16.3.2  172.16.3.9  172.16.3.15 | 172.16.1.3  172.16.1.9  172.16.1.8  172.16.8.1  172.16.8.9  10.0.0.105  192.168.101.1  192.168.101.11  192.168.101.16  192.168.101.17  192.168.101.18  192.168.101.26  192.168.101.28  192.168.101.61  192.168.101.77  192.168.101.91  192.168.101.92  192.168.205.1  10.20.36.1  10.20.36.2  10.20.36.10  10.20.36.9  192.168.201.9  192.168.201.25 |

Figure 56: Nmap Scan Example revealing the use of CBC Ciphers on Multiple Hosts:



## Weak and Insecure Ciphers – Low risk

One or more systems were found using TLS ciphers with key sizes less than 128 bits, and cipher algorithms with insufficient key sizes. Degraded ciphers and algorithms could be broken by a malicious user. When an SSL (Secure-Socket Layer) connection is made between two computers, a session key is negotiated. Through this negotiation, the client sends an unencrypted "Hello" packet, which contains a list of supported cipher suites. Through a man-in-the-middle (MITM) attack, an attacker could intercept this list and modify it to include only weak ciphers. The server would then be forced to accept a degraded cipher. An attacker could then capture the encrypted data and attempt to crack the ciphers.

In addition, one device allows SSLv3 that is prone to information disclosure vulnerability attacks. Successful exploitation will allow a man-in-the-middle (MITM) attacker to gain access to the plain-text data stream.

The analyst discovered multiple external-facing hosts currently configured to use vulnerable TLS (Transport Layer Security) ciphers. TLS ciphers allow traffic between a client and a web server to be passed over the public Internet through a secure channel. In addition, the analyst discovered an SSLv3 vulnerability, known as POODLE, on host an external host. This vulnerability allows an attacker to control a network by using a MITM session to hijack valuable information that would otherwise be encrypted.

TraceSecurity recommends requiring strong ciphers that have at least 128 bits of key space and strong algorithms, such as SHA256. If this hinders end user functions, TraceSecurity recommends that Information Technology personnel perform a review of the security settings of these hosts.

TraceSecurity also recommends disabling SSLv3 entirely and replacing it with a minimum of TLSv1, then rejecting any clients requiring SSLv3 to prevent them from downgrading the installed TLSv1. If the organization requires legacy client support, then TraceSecurity recommends enabling TLS\_FALLBACK\_SCSV cipher suite value as a patch to OpenSSL that prevents downgrading from TLS1.2 to 1.1 or 1.0 by a potential attacker.

Figure 46: Table - Insecure Protocols Detected on Multiple Hosts with SSLv2 Accepted:

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Connections Accepted** | **Affected Hosts/Services** | | |
| SSLv2 Accepted: | 172.16.0.1:443  172.16.0.14:443  172.16.0.24:443  172.16.0.31:443  172.16.0.33:443 | 172.16.0.45:443  172.16.0.49:443  172.16.0.120:443  172.16.0.238:443  172.16.0.240:443 | 172.16.0.249:443  172.16.6.191:443  172.16.7.1:443  192.168.101.30:443  192.168.201.27:443 |

Figure 47: Table - Insecure Protocols Detected on Multiple Hosts with SSLv3 Accepted:

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Connections Accepted** | **Affected Hosts/Services** | | |
| SSLv3 Accepted: | 10.0.0.104:443  10.0.0.106:443  10.0.0.146:443  172.16.0.14:443  172.16.0.24:443  172.16.0.28:443  172.16.0.31:443  172.16.0.33:443  172.16.0.45:443  172.16.0.49:443  172.16.0.78:443  172.16.0.79:443  172.16.0.104:443  172.16.0.109:443  172.16.0.114:443  172.16.0.120:443  172.16.0.212:443  172.16.0.213:443  172.16.0.238:443  172.16.0.240:443  172.16.0.249:443  172.16.1.7:443 | 172.16.1.8:443  172.16.2.19:443  172.16.2.42:443  172.16.2.43:443  172.16.2.50:443  172.16.3.15:443  172.16.3.19:443  172.16.3.45:443  172.16.3.48:443  172.16.4.1:443  172.16.4.14:443  172.16.4.46:443  172.16.5.21:8443  172.16.5.46:443  172.16.5.49:443  172.16.5.75:443  172.16.6.41:443  172.16.6.42:443  172.16.6.49:443  172.16.6.50:443  172.16.6.54:443  172.16.6.56:443 | 172.16.6.57:443  172.16.6.59:443  172.16.7.7:443  172.16.7.30:8443  172.16.7.75:443  172.16.7.76:443  172.16.7.77:443  172.16.7.79:443  172.16.7.82:443  172.16.7.84:443  192.168.101.18:443  192.168.101.26:443  192.168.101.28:443  192.168.101.30:443  192.168.101.42:443  192.168.101.64:443  192.168.101.66:443  192.168.101.68:443  192.168.101.91:443  192.168.101.162:443  192.168.201.9:443  192.168.201.27:443  192.168.205.1:443 |

Figure 48: Table - Insecure Protocols Detected on Multiple Hosts with TLSv1.0 Accepted:

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Connections Accepted** | **Affected Hosts/Services** | | |
| TLSv1.0 Accepted: | 10.0.0.181:443  10.0.0.182:443  10.0.0.183:443  10.0.9.100:443  10.20.36.2:443  10.20.36.9:443  172.16.0.1:443  172.16.0.11:443  172.16.0.14:443  172.16.0.24:443  172.16.0.28:443  172.16.0.30:443  172.16.0.31:443  172.16.0.32:443  172.16.0.33:443  172.16.0.34:443  172.16.0.35:443  172.16.0.45:443  172.16.0.49:443  172.16.0.59:443  172.16.0.60:443  172.16.0.63:443  172.16.0.66:443  172.16.0.76:443  172.16.0.78:443  172.16.0.79:443  172.16.0.82:443  172.16.0.87:443  172.16.0.102:443  172.16.0.104:443  172.16.0.107:443  172.16.0.109:443  172.16.0.112:443  172.16.0.113:443  172.16.0.114:443  172.16.0.115:443  172.16.0.117:443  172.16.0.118:443  172.16.0.120:443  172.16.0.121:443  172.16.0.212:443  172.16.0.213:443  172.16.0.231:8443  172.16.0.232:443  172.16.0.234:443  172.16.0.235:443  172.16.0.238:443  172.16.0.240:443  172.16.0.244:443  172.16.0.248:443 | 172.16.1.7:443  172.16.1.8:443  172.16.1.9:443  172.16.1.10:443  172.16.1.12:443  172.16.1.35:443  172.16.2.1:443  172.16.2.17:443  172.16.2.19:443  172.16.2.42:443  172.16.2.43:443  172.16.2.50:443  172.16.2.54:443  172.16.3.2:443  172.16.3.15:443  172.16.3.17:443  172.16.3.19:443  172.16.3.45:443  172.16.3.48:443  172.16.4.1:443  172.16.4.9:443  172.16.4.14:443  172.16.4.17:443  172.16.4.41:443  172.16.4.46:443  172.16.4.80:443  172.16.5.1:443  172.16.5.8:443  172.16.5.9:443  172.16.5.21:443  172.16.5.21:8443  172.16.5.22:443  172.16.5.46:443  172.16.5.49:443  172.16.5.62:443  172.16.5.66:443  172.16.5.68:443  172.16.5.75:443  172.16.5.76:443  172.16.5.111:443  172.16.6.1:443  172.16.6.7:443  172.16.6.11:443  172.16.6.18:443  172.16.6.19:443  172.16.6.41:443  172.16.6.42:443  172.16.6.43:443  172.16.6.44:443  172.16.6.49:443 | 172.16.6.60:443  172.16.6.191:443  172.16.7.1:443  172.16.7.7:443  172.16.7.30:443  172.16.7.30:8443  172.16.7.31:443  172.16.7.32:443  172.16.7.75:443  172.16.7.76:443  172.16.7.77:443  172.16.7.79:443  172.16.7.82:443  172.16.7.83:443  172.16.7.84:443  192.168.101.18:443  192.168.101.26:443  192.168.101.28:443  192.168.101.30:443  192.168.101.38:443  192.168.101.42:443  192.168.101.50:443  192.168.101.61:443  192.168.101.63:443  192.168.101.64:443  192.168.101.66:443  192.168.101.67:443  192.168.101.68:443  192.168.101.77:443  192.168.101.102:443  192.168.101.108:443  192.168.101.118:443  192.168.101.122:443  192.168.101.128:443  192.168.101.129:443  192.168.101.134:443  192.168.101.135:443  192.168.101.136:443  192.168.101.162:443  192.168.101.165:443  192.168.101.168:443  192.168.101.182:443  192.168.101.185:443  192.168.101.188:443  192.168.101.194:443  192.168.101.210:443  192.168.201.9:443  192.168.201.25:443  192.168.201.27:443  192.168.205.1:443 |
| 10.0.0.104:443  10.0.0.106:443  10.0.0.114:443  10.0.0.130:443  10.0.0.131:443  10.0.0.132:443  10.0.0.138:443  10.0.0.139:443  10.0.0.146:443  10.0.0.161:443  10.0.0.162:443  10.0.0.163:443  172.16.0.249:443  172.16.1.1:443  172.16.6.57:443  172.16.6.59:443  172.16.6.50:443  172.16.6.54:443  172.16.6.56:443 |

Figure 49: Table - Insecure Protocols Detected on Multiple Hosts with TLSv1.1 Accepted:

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Connections Accepted** | **Affected Hosts/Services** | | |
| TLSv1.1 Accepted: | 10.0.0.104:443  10.0.0.106:443  10.0.0.114:443  10.0.0.146:443  10.0.0.161:443  10.0.0.162:443  10.0.0.163:443  10.0.0.171:443  10.0.0.172:443  10.0.0.173:443  10.0.0.181:443  10.0.0.182:443  10.0.0.183:443  10.20.36.2:443  10.20.36.9:443  172.16.0.1:443  172.16.0.11:443  172.16.0.15:443  172.16.0.16:443  172.16.0.28:443  172.16.0.30:443  172.16.0.32:443  172.16.0.35:443  172.16.0.60:443  172.16.0.63:443  172.16.0.66:443  172.16.0.76:443  172.16.0.78:443  172.16.0.79:443  172.16.0.82:443  172.16.0.86:443  172.16.0.87:443  172.16.0.99:443  172.16.0.102:443  172.16.0.107:443  172.16.0.112:443  172.16.0.113:443 | 172.16.0.114:443  172.16.0.118:443  172.16.0.121:443  172.16.0.231:8443  172.16.0.234:443  172.16.0.235:443  172.16.0.244:443  172.16.0.248:443  172.16.1.1:443  172.16.1.9:443  172.16.1.10:443  172.16.1.12:443  172.16.1.15:443  172.16.1.35:443  172.16.2.1:443  172.16.2.17:443  172.16.2.54:443  172.16.3.2:443  172.16.3.17:443  172.16.4.1:443  172.16.4.17:443  172.16.4.19:443  172.16.4.80:443  172.16.5.1:443  172.16.5.19:443  172.16.5.21:443  172.16.5.21:8443  172.16.5.62:443  172.16.5.66:443  172.16.5.68:443  172.16.5.76:443  172.16.5.111:443  172.16.6.1:443  172.16.6.11:443  172.16.6.18:443  172.16.6.19:443  172.16.6.43:443 | 172.16.6.44:443  172.16.6.60:443  172.16.7.1:443  172.16.7.7:443  172.16.7.30:443  172.16.7.30:8443  172.16.7.31:443  172.16.7.32:443  172.16.7.83:443  192.168.101.1:443  192.168.101.16:443  192.168.101.17:443  192.168.101.38:443  192.168.101.50:443  192.168.101.63:443  192.168.101.67:443  192.168.101.77:443  192.168.101.102:443  192.168.101.108:443  192.168.101.118:443  192.168.101.122:443  192.168.101.128:443  192.168.101.129:443  192.168.101.134:443  192.168.101.135:443  192.168.101.136:443  192.168.101.165:443  192.168.101.168:443  192.168.101.182:443  192.168.101.185:443  192.168.101.188:443  192.168.101.194:443  192.168.101.210:443  192.168.201.25:443  192.168.205.1:443 |

Figure 50: Table - Weak & Insecure Protocols Detected on Multiple Hosts with TLSv1.1 Accepted <128bit:

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Connections Accepted** | **Affected Hosts/Services** | | |
| TLSv1.1 Accepted with  <128 Bit Ciphers: | 10.0.0.104:443  10.0.0.106:443  10.0.0.114:443  10.0.0.146:443  10.0.0.162:443  10.0.0.171:443  10.0.0.172:443  10.0.0.173:443  10.0.0.182:443  10.20.36.9:443  172.16.0.1:443  172.16.0.11:443  172.16.0.15:443  172.16.0.16:443  172.16.0.28:443  172.16.0.30:443  172.16.0.32:443  172.16.0.35:443  172.16.0.66:443  172.16.0.78:443  172.16.0.79:443  172.16.0.86:443  172.16.0.99:443  172.16.0.113:443  172.16.0.114:443  172.16.0.118:443  172.16.0.231:8443 | 172.16.0.234:443  172.16.0.235:443  172.16.0.248:443  172.16.1.1:443  172.16.1.15:443  172.16.2.1:443  172.16.2.54:443  172.16.3.2:443  172.16.4.1:443  172.16.4.19:443  172.16.4.80:443  172.16.5.1:443  172.16.5.19:443  172.16.5.21:8443  172.16.5.66:443  172.16.5.68:443  172.16.5.76:443  172.16.5.111:443  172.16.6.1:443  172.16.6.19:443  172.16.6.43:443  172.16.6.44:443  172.16.6.60:443  172.16.7.1:443  172.16.7.7:443  172.16.7.30:8443  172.16.7.31:443 | 172.16.7.32:443  172.16.7.83:443  192.168.101.1:443  192.168.101.16:443  192.168.101.17:443  192.168.101.50:443  192.168.101.63:443  192.168.101.67:443  192.168.101.77:443  192.168.101.102:443  192.168.101.108:443  192.168.101.118:443  192.168.101.122:443  192.168.101.128:443  192.168.101.129:443  192.168.101.134:443  192.168.101.135:443  192.168.101.136:443  192.168.101.165:443  192.168.101.168:443  192.168.101.182:443  192.168.101.185:443  192.168.101.188:443  192.168.101.194:443  192.168.101.210:443  192.168.201.25:443  192.168.205.1:443 |

Figure 51: Table - Weak & Insecure Protocols Detected on Multiple Hosts with TLSv1.1 Accepted ADH/RC4/AECDH:

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Connections Accepted** | **Affected Hosts/Services** | | |
| TLSv1.1 Accepted with ADH,  AECDH, or RC4 Ciphers: | 10.0.0.104:443  10.0.0.106:443  10.0.0.146:443  10.0.0.162:443  10.0.0.182:443  10.20.36.9:443  172.16.0.1:443  172.16.0.11:443  172.16.0.28:443  172.16.0.30:443  172.16.0.66:443  172.16.0.78:443 | 172.16.0.79:443  172.16.0.113:443  172.16.0.114:443  172.16.0.118:443  172.16.0.248:443  172.16.1.1:443  172.16.2.1:443  172.16.3.2:443  172.16.4.1:443  172.16.4.80:443  172.16.5.1:443  172.16.5.76:443 | 172.16.6.1:443  172.16.6.19:443  172.16.6.60:443  172.16.7.1:443  172.16.7.7:443  192.168.101.1:443  192.168.101.16:443  192.168.101.17:443  192.168.101.77:443  192.168.201.25:443  192.168.205.1:443 |

Figure 52: Table - Weak & Insecure Protocols Detected on Multiple Hosts with TLSv1.2 Accepted <128bit:

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Connections Accepted** | **Affected Hosts/Services** | | |
| TLSv1.2 Accepted with  <128 Bit Ciphers: | 10.0.0.104:443  10.0.0.106:443  10.0.0.114:443  10.0.0.130:443  10.0.0.131:443  10.0.0.132:443  10.0.0.138:443  10.0.0.139:443  10.0.0.146:443  10.0.0.162:443  10.0.0.171:443  10.0.0.172:443  10.0.0.173:443  10.0.0.182:443  10.0.9.100:443  10.20.36.9:443  172.16.0.1:443  172.16.0.11:443  172.16.0.15:443  172.16.0.16:443  172.16.0.28:443  172.16.0.32:443  172.16.0.35:443  172.16.0.66:443  172.16.0.78:443  172.16.0.79:443  172.16.0.86:443  172.16.0.99:443  172.16.0.113:443 | 172.16.0.114:443  172.16.0.118:443  172.16.0.231:8443  172.16.0.234:443  172.16.0.235:443  172.16.0.248:443  172.16.1.1:443  172.16.1.15:443  172.16.2.1:443  172.16.2.54:443  172.16.3.2:443  172.16.4.1:443  172.16.4.19:443  172.16.4.80:443  172.16.5.1:443  172.16.5.19:443  172.16.5.66:443  172.16.5.68:443  172.16.5.76:443  172.16.5.111:443  172.16.6.1:443  172.16.6.19:443  172.16.6.35:443  172.16.6.43:443  172.16.6.44:443  172.16.6.60:443  172.16.6.191:443  172.16.7.1:443  172.16.7.7:443 | 172.16.7.31:443  172.16.7.32:443  172.16.7.83:443  192.168.101.1:443  192.168.101.16:443  192.168.101.17:443  192.168.101.50:443  192.168.101.63:443  192.168.101.67:443  192.168.101.77:443  192.168.101.102:443  192.168.101.108:443  192.168.101.118:443  192.168.101.122:443  192.168.101.128:443  192.168.101.129:443  192.168.101.134:443  192.168.101.135:443  192.168.101.136:443  192.168.101.165:443  192.168.101.168:443  192.168.101.182:443  192.168.101.185:443  192.168.101.188:443  192.168.101.194:443  192.168.101.210:443  192.168.201.25:443  192.168.201.27:443  192.168.205.1:443 |

Figure 53: Table - Weak & Insecure Protocols Detected on Multiple Hosts with TLSv1.2 Accepted ADH/RC4/AECDH:

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Connections Accepted** | **Affected Hosts/Services** | | |
| TLSv1.2 Accepted with ADH,  AECDH, or RC4 Ciphers: | 10.0.0.104:443  10.0.0.106:443  10.0.0.130:443  10.0.0.131:443  10.0.0.132:443  10.0.0.138:443  10.0.0.139:443  10.0.0.146:443  10.0.0.162:443  10.0.0.182:443  10.0.9.100:443  10.20.36.9:443  172.16.0.1:443  172.16.0.11:443 | 172.16.0.28:443  172.16.0.66:443  172.16.0.78:443  172.16.0.79:443  172.16.0.113:443  172.16.0.114:443  172.16.0.118:443  172.16.0.248:443  172.16.1.1:443  172.16.2.1:443  172.16.3.2:443  172.16.4.1:443  172.16.4.80:443  172.16.5.1:443 | 172.16.5.76:443  172.16.6.1:443  172.16.6.19:443  172.16.6.60:443  172.16.6.191:443  172.16.7.1:443  172.16.7.7:443  192.168.101.1:443  192.168.101.16:443  192.168.101.17:443  192.168.101.77:443  192.168.201.25:443  192.168.201.27:443  192.168.205.1:443 |

Figure 54: Table - Insecure Session Renegotiation Supported on Multiple Hosts:

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Checks** | **Affected Hosts/Services** | | |
| Insecure Session  Renegotiation Supported: | 172.16.0.115:443  172.16.0.117:443  172.16.2.42:443  172.16.2.50:443  172.16.3.15:443  172.16.4.9:443  172.16.4.14:443  172.16.4.41:443  172.16.5.8:443 | 172.16.5.9:443  172.16.5.46:443  172.16.5.49:443  172.16.6.7:443  172.16.6.41:443  172.16.6.42:443  172.16.6.49:443  172.16.6.50:443  172.16.6.54:443 | 172.16.7.76:443  172.16.7.77:443  192.168.101.11:443  192.168.101.42:443  192.168.101.61:443  192.168.101.66:443  192.168.101.68:443  192.168.101.162:443  192.168.201.9:443 |

Post-Exploitation evidence

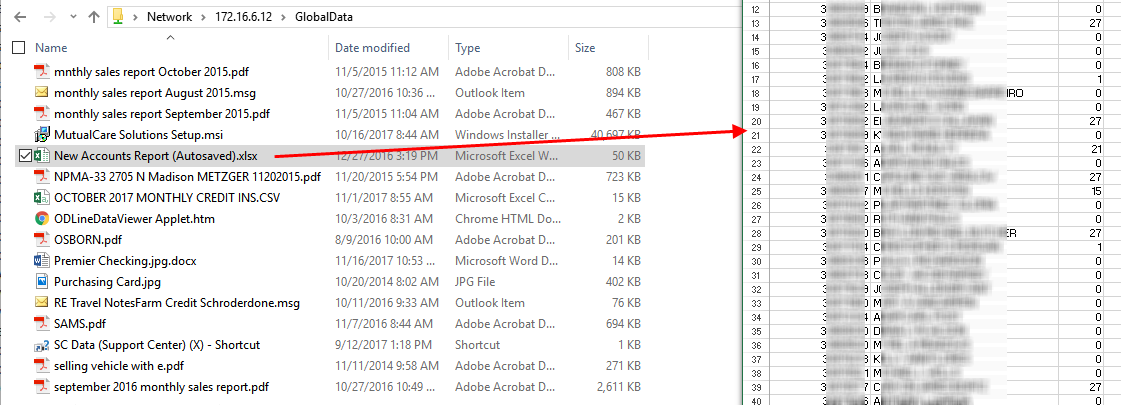
Adding users to the Domain Admins group grants the users full access rights to Active Directory and other systems that use Windows authentication. If an attacker adds a user to Domain Admins it can result in the access or deletion of critical organizational units, domain controller shutdown and other business continuity issues. To ensure it’s important to continuously monitor all changes made to the Domain Admins group and be able to quickly mitigate those changes.

The analyst demonstrated 3 individual penetration techniques within the LLMNR Poisoning Attack and the Weak Password Attack that granted the analyst enough access to the credit union’s systems to create rogue accounts with Domain Admin privileges in order to further exploit the credit union’s systems. The 8 hour penetration testing took place in blocks of time that spanned 3 calendar days. On each day, the analyst continued to utilize rogue accounts to capture sensitive documents and compromising data without interference.

TraceSecurity recommends enabling domain policies that record changes to security access groups or implementing an application or service to monitor and report changes to the domain to prevent unauthorized accounts from going unchecked for extended periods of time.

The following figures demonstrate the files and information accessed by the analyst with newly created Domain Admin account access.

Figure 57: Account Numbers Located on 172.16.6.12 by Accessing Shares with Compromised Credentials:



# APPENDIX

## Additional test results and findings

The Appendix section of this report is reserved to demonstrate some of the actions performed during the Internal Penetration Test. Many of the screenshots below may include unsuccessful attacks against a resource, results from many Network Mapping activities, and additional scanning for potential vulnerabilities or exploits attempts.

***Figure 67: Lockout Tries set to “0” on Devices Located at 172.16.1.35:***

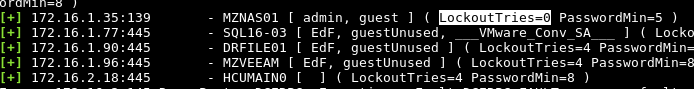


Figure 68: Default Login Attempted on http://172.16.0.212:

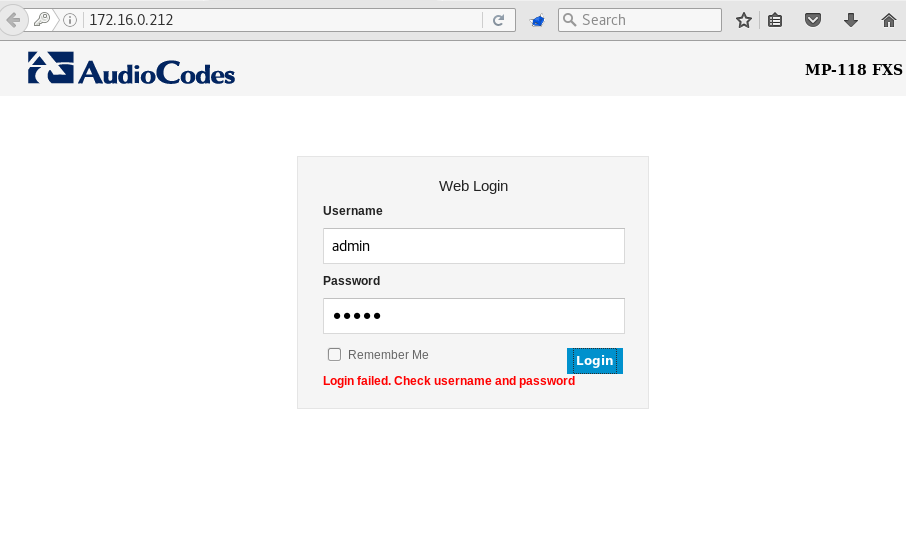


Figure 69: Default Login Attempted on https://172.16.0.213:

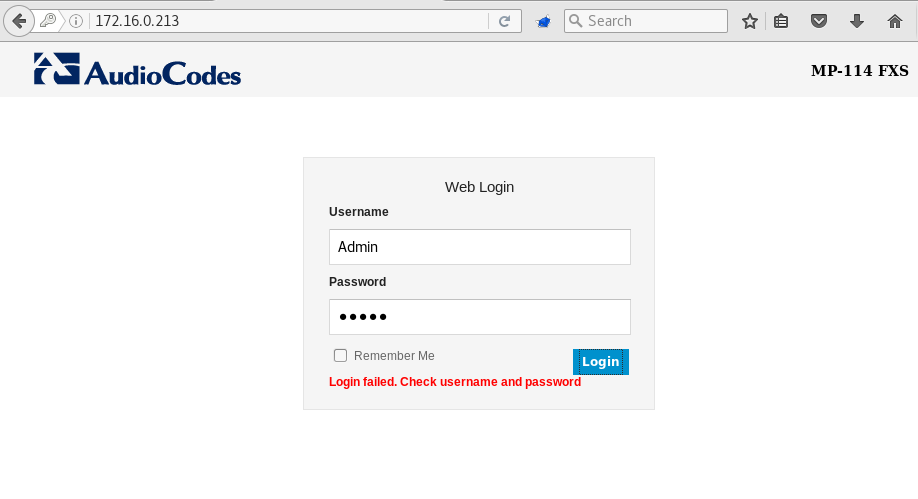


Figure 70: Password Attack on Enumerated Accounts (anonymously) on 172.16.2.18:

The analyst used a common “Username as Password” attack to locate weak passwords associated with extracted usernames from an anonymous LDAP lookup.

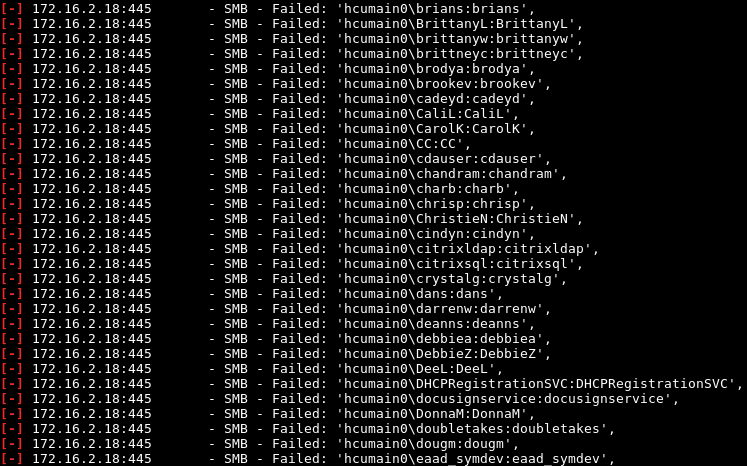


Figure 71: Default Login Attempt on https://172.16.5.75:

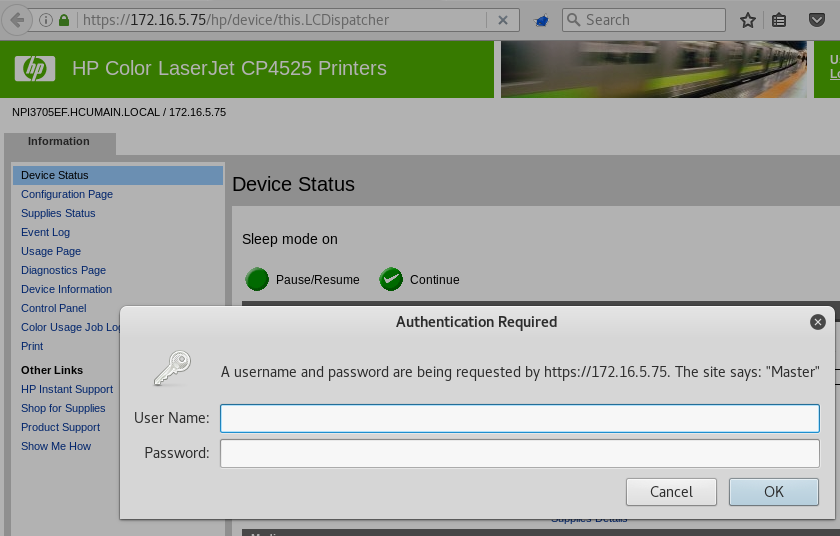


Figure 72: Default Login Attempt on https://172.16.7.83:

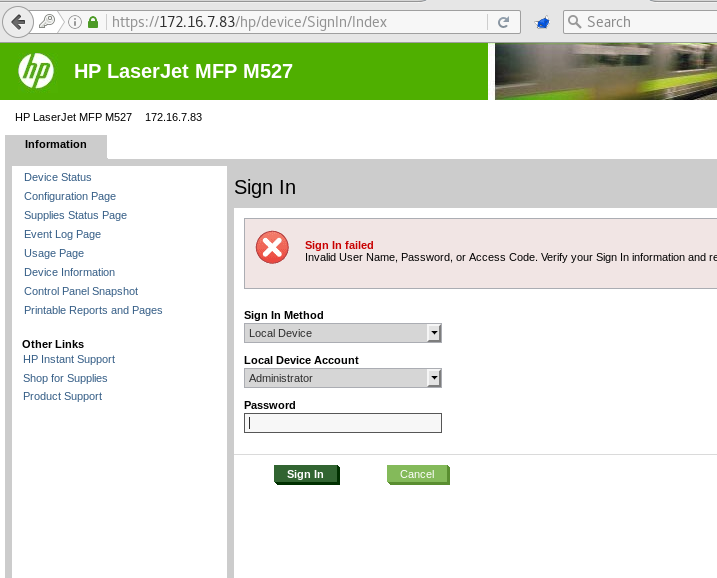


Figure 73: Meterpreter Session Attempt with Compromised Credentials:

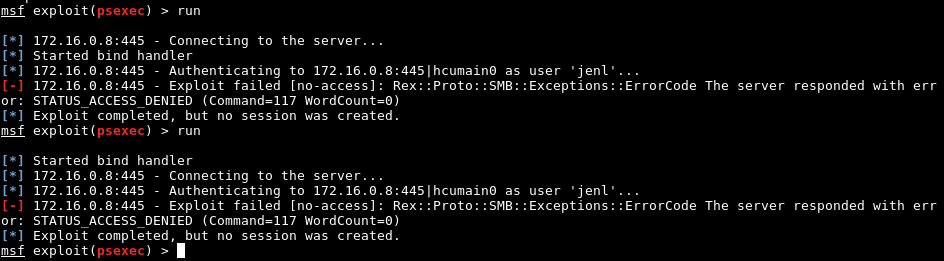


Figure 74: Default Login Attempt at https://172.16.3.15:

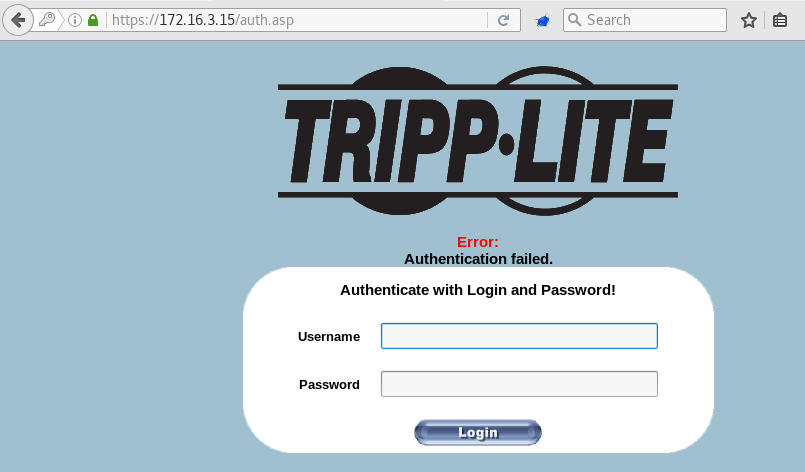


Figure 75: Default Login Attempt at https://172.16.5.22:

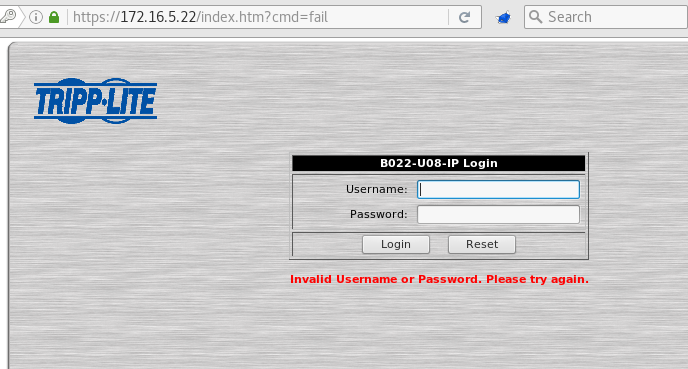


Figure 76: Default Login Attempt at http://172.16.8.71:

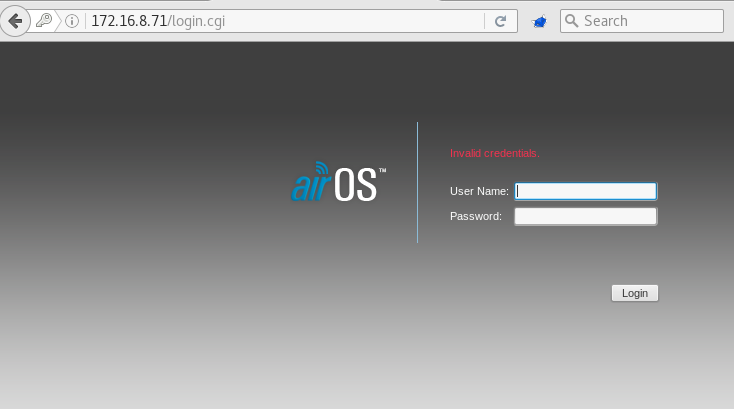


Figure 77: Remote Desktop Login Attempt with Compromised Credentials:

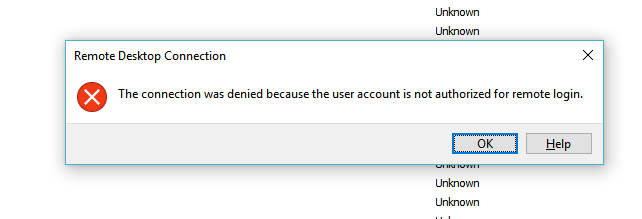


Figure 78: Remote Desktop Login Attempt with Compromised Credentials on 192.168.201.26:

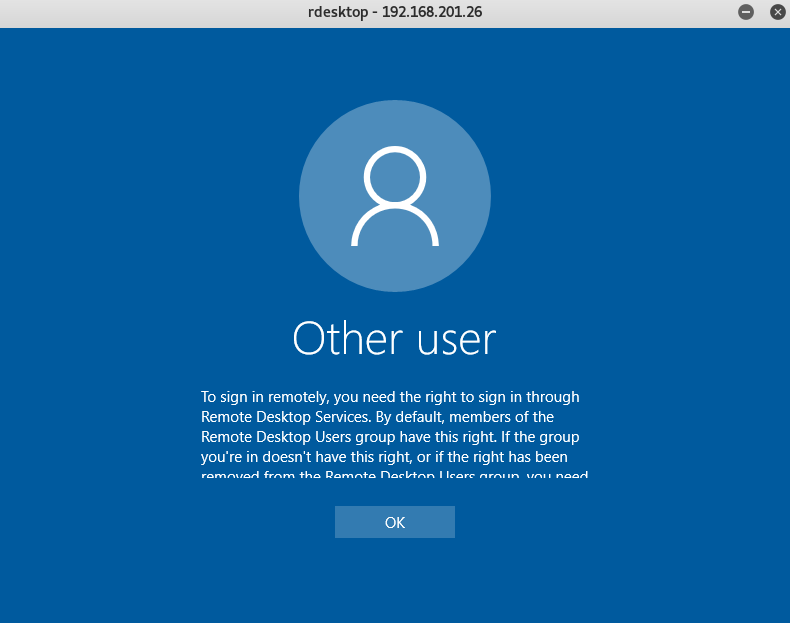


Figure 79: VNC None-Auth Vulnerability Check on Devices with TCP Port 5900 Open:



Figure 80: Table - Full List of Live Devices Found in the Subnets Beginning With “10.”:

|  |  |  |  |
| --- | --- | --- | --- |
| 10.10.10.1  10.10.10.3  10.10.10.2  10.10.10.4  10.10.10.6  10.10.10.5  10.10.10.8  10.10.10.9 | 10.0.0.11  10.0.0.12  10.0.0.105  10.0.0.106  10.0.0.104  10.0.0.114  10.0.0.130  10.0.0.132  10.0.0.131  10.0.0.138  10.0.0.142  10.0.0.139 | 10.0.0.144  10.0.0.143  10.0.0.146  10.0.0.161  10.0.0.162  10.0.0.163  10.0.0.172  10.0.0.171  10.0.0.173  10.0.0.182  10.0.0.181  10.0.0.183 | 10.0.9.100  10.20.36.1  10.20.36.2  10.20.36.10  10.20.36.9 |

Figure 81: Table - Full List of Live Devices Found in the 172.16.0.0/24 Subnet:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.0.1  172.16.0.2  172.16.0.7  172.16.0.8  172.16.0.9  172.16.0.11  172.16.0.16  172.16.0.15  172.16.0.14  172.16.0.18  172.16.0.17  172.16.0.19  172.16.0.21  172.16.0.23  172.16.0.22  172.16.0.24  172.16.0.27  172.16.0.28  172.16.0.30  172.16.0.31  172.16.0.32  172.16.0.33  172.16.0.34  172.16.0.35  172.16.0.36  172.16.0.37  172.16.0.38 | 172.16.0.42  172.16.0.40  172.16.0.45  172.16.0.46  172.16.0.47  172.16.0.48  172.16.0.49  172.16.0.50  172.16.0.60  172.16.0.59  172.16.0.61  172.16.0.63  172.16.0.67  172.16.0.66  172.16.0.64  172.16.0.65  172.16.0.68  172.16.0.69  172.16.0.70  172.16.0.73  172.16.0.76  172.16.0.75  172.16.0.78  172.16.0.79  172.16.0.82  172.16.0.84 | 172.16.0.87  172.16.0.86  172.16.0.85  172.16.0.88  172.16.0.89  172.16.0.91  172.16.0.96  172.16.0.98  172.16.0.97  172.16.0.102  172.16.0.99  172.16.0.100  172.16.0.104  172.16.0.106  172.16.0.105  172.16.0.107  172.16.0.109  172.16.0.112  172.16.0.110  172.16.0.113  172.16.0.115  172.16.0.114  172.16.0.119  172.16.0.118  172.16.0.117  172.16.0.121 | 172.16.0.120  172.16.0.122  172.16.0.123  172.16.0.173  172.16.0.175  172.16.0.174  172.16.0.172  172.16.0.212  172.16.0.214  172.16.0.213  172.16.0.219  172.16.0.232  172.16.0.233  172.16.0.231  172.16.0.238  172.16.0.240  172.16.0.239  172.16.0.241  172.16.0.242  172.16.0.244  172.16.0.245  172.16.0.248  172.16.0.247  172.16.0.249  172.16.0.235  172.16.0.234 |

Figure 82: Table - Full List of Live Devices Found in the 172.16.1.0/24 Subnet:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.1.1  172.16.1.3  172.16.1.9  172.16.1.8  172.16.1.7 | 172.16.1.10  172.16.1.11  172.16.1.12  172.16.1.15  172.16.1.18 | 172.16.1.28  172.16.1.31  172.16.1.35  172.16.1.37  172.16.1.77 | 172.16.1.90  172.16.1.96  172.16.1.172  172.16.1.173  172.16.1.174  172.16.1.175 |

Figure 83: Table - Full List of Live Devices Found in the 192.168.101.0/24 & 192.168.205.0/24 Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| 192.168.101.1  192.168.101.12  192.168.101.11  192.168.101.16  192.168.101.17  192.168.101.18  192.168.101.19  192.168.101.26  192.168.101.27  192.168.101.30  192.168.101.28  192.168.101.34  192.168.101.38  192.168.101.42  192.168.101.50  192.168.101.60  192.168.101.61  192.168.101.63  192.168.101.64  192.168.101.66  192.168.101.65  192.168.101.67  192.168.101.68  192.168.101.75  192.168.101.77  192.168.101.91  192.168.101.92  192.168.101.101  192.168.101.102  192.168.101.104  192.168.101.105  192.168.101.107  192.168.101.108  192.168.101.109  192.168.101.106  192.168.101.110  192.168.101.112  192.168.101.114  192.168.101.115  192.168.101.113  192.168.101.117  192.168.101.118  192.168.101.116  192.168.101.103  192.168.101.119  192.168.101.120  192.168.101.124  192.168.101.121 | 192.168.101.122  192.168.101.126  192.168.101.127  192.168.101.125  192.168.101.129  192.168.101.130  192.168.101.128  192.168.101.131  192.168.101.134  192.168.101.137  192.168.101.1  192.168.101.101  192.168.101.102  192.168.101.103  192.168.101.104  192.168.101.105  192.168.101.106  192.168.101.107  192.168.101.108  192.168.101.109  192.168.101.11  192.168.101.110  192.168.101.112  192.168.101.113  192.168.101.114  192.168.101.115  192.168.101.116  192.168.101.117  192.168.101.118  192.168.101.119  192.168.101.12  192.168.101.120  192.168.101.121  192.168.101.122  192.168.101.124  192.168.101.125  192.168.101.126  192.168.101.127  192.168.101.128  192.168.101.129  192.168.101.130  192.168.101.131  192.168.101.133  192.168.101.134  192.168.101.135  192.168.101.136  192.168.101.137  192.168.101.138 | 192.168.101.139  192.168.101.140  192.168.101.141  192.168.101.143  192.168.101.144  192.168.101.145  192.168.101.146  192.168.101.147  192.168.101.148  192.168.101.149  192.168.101.150  192.168.101.151  192.168.101.152  192.168.101.153  192.168.101.154  192.168.101.155  192.168.101.156  192.168.101.157  192.168.101.158  192.168.101.159  192.168.101.16  192.168.101.160  192.168.101.161  192.168.101.162  192.168.101.163  192.168.101.164  192.168.101.165  192.168.101.167  192.168.101.168  192.168.101.169  192.168.101.17  192.168.101.170  192.168.101.171  192.168.101.172  192.168.101.173  192.168.101.174  192.168.101.175  192.168.101.176  192.168.101.177  192.168.101.178  192.168.101.179  192.168.101.18  192.168.101.180  192.168.101.181  192.168.101.182  192.168.101.183  192.168.101.184  192.168.101.185 | 192.168.101.187  192.168.101.188  192.168.101.189  192.168.101.19  192.168.101.190  192.168.101.191  192.168.101.192  192.168.101.193  192.168.101.194  192.168.101.196  192.168.101.197  192.168.101.198  192.168.101.203  192.168.101.206  192.168.101.207  192.168.101.210  192.168.101.213  192.168.101.26  192.168.101.27  192.168.101.28  192.168.101.30  192.168.101.34  192.168.101.38  192.168.101.42  192.168.101.50  192.168.101.60  192.168.101.61  192.168.101.63  192.168.101.64  192.168.101.65  192.168.101.66  192.168.101.67  192.168.101.68  192.168.101.75  192.168.101.77  192.168.101.91  192.168.101.92  192.168.201.11  192.168.201.25  192.168.201.26  192.168.201.27  192.168.201.28  192.168.201.9  192.168.205.1  192.168.205.106  192.168.205.107  192.168.205.3 |

Figure 84: Table - Full List of Live Devices Found in the 172.16.2.0/24 Subnet:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.2.1  172.16.2.9  172.16.2.12  172.16.2.17  172.16.2.18 | 172.16.2.19  172.16.2.15  172.16.2.42  172.16.2.43  172.16.2.44  172.16.2.45 | 172.16.2.50  172.16.2.54  172.16.2.111  172.16.2.133  172.16.2.137  172.16.2.145 | 172.16.2.149  172.16.2.147  172.16.2.153  172.16.2.174  172.16.2.175  172.16.2.13 |

Figure 85: Table - Full List of Live Devices Found in the 172.16.5.0/24 Subnet:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.5.1  172.16.5.8  172.16.5.10  172.16.5.9  172.16.5.17  172.16.5.18  172.16.5.20  172.16.5.19  172.16.5.21  172.16.5.22  172.16.5.28  172.16.5.30  172.16.5.29 | 172.16.5.43  172.16.5.46  172.16.5.49  172.16.5.62  172.16.5.66  172.16.5.68  172.16.5.69  172.16.5.71  172.16.5.70  172.16.5.72  172.16.5.76  172.16.5.75 | 172.16.5.84  172.16.5.104  172.16.5.111  172.16.5.121  172.16.5.122  172.16.5.142  172.16.5.144  172.16.5.145  172.16.5.147  172.16.5.146  172.16.5.148  172.16.5.149  172.16.5.150 | 172.16.5.151  172.16.5.152  172.16.5.155  172.16.5.160  172.16.5.163  172.16.5.162  172.16.5.166  172.16.5.171  172.16.5.173  172.16.5.175  172.16.5.174  172.16.5.176  172.16.5.32 |

Figure 86: Table - Full List of Live Devices Found in the 172.16.6.0/24 Subnet:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.6.1  172.16.6.4  172.16.6.5  172.16.6.6  172.16.6.8  172.16.6.7  172.16.6.9  172.16.6.11  172.16.6.10  172.16.6.12  172.16.6.13  172.16.6.15  172.16.6.17  172.16.6.18  172.16.6.19  172.16.6.20  172.16.6.22  172.16.6.35  172.16.6.39  172.16.6.41  172.16.6.42  172.16.6.43  172.16.6.44  172.16.6.45  172.16.6.46  172.16.6.49 | 172.16.6.48  172.16.6.50  172.16.6.54  172.16.6.53  172.16.6.55  172.16.6.56  172.16.6.57  172.16.6.59  172.16.6.60  172.16.6.113  172.16.6.140  172.16.6.143  172.16.6.142  172.16.6.141  172.16.6.144  172.16.6.146  172.16.6.145  172.16.6.147  172.16.6.149  172.16.6.148  172.16.6.150  172.16.6.151  172.16.6.152  172.16.6.153  172.16.6.155  172.16.6.156 | 172.16.6.154  172.16.6.158  172.16.6.159  172.16.6.160  172.16.6.162  172.16.6.161  172.16.6.166  172.16.6.164  172.16.6.163  172.16.6.165  172.16.6.167  172.16.6.168  172.16.6.170  172.16.6.173  172.16.6.171  172.16.6.174  172.16.6.176  172.16.6.179  172.16.6.177  172.16.6.178  172.16.6.184  172.16.6.183  172.16.6.182  172.16.6.185  172.16.6.186  172.16.6.190 | 172.16.6.191  172.16.6.189  172.16.6.192  172.16.6.195  172.16.6.196  172.16.6.199  172.16.6.202  172.16.6.203  172.16.6.206  172.16.6.204  172.16.6.205  172.16.6.208  172.16.6.209  172.16.6.207  172.16.6.220  172.16.6.222  172.16.6.225  172.16.6.226  172.16.6.227  172.16.6.228  172.16.6.229  172.16.6.231  172.16.6.232  172.16.6.245  172.16.6.246  172.16.6.247 |

Figure 87: Table - Full List of Live Devices Found in the 172.16.7.0/24 Subnet:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.7.1  172.16.7.30  172.16.7.31  172.16.7.32  172.16.7.76  172.16.7.75  172.16.7.78  172.16.7.77  172.16.7.79  172.16.7.82  172.16.7.84  172.16.7.83  172.16.7.85 | 172.16.7.88  172.16.7.101  172.16.7.102  172.16.7.103  172.16.7.105  172.16.7.108  172.16.7.107  172.16.7.109  172.16.7.112  172.16.7.110  172.16.7.115  172.16.7.114  172.16.7.130 | 172.16.7.131  172.16.7.132  172.16.7.136  172.16.7.134  172.16.7.133  172.16.7.135  172.16.7.138  172.16.7.139  172.16.7.141  172.16.7.144  172.16.7.7  172.16.7.152 | 172.16.7.151  172.16.7.150  172.16.7.155  172.16.7.157  172.16.7.156  172.16.7.158  172.16.7.160  172.16.7.163  172.16.7.161  172.16.7.177  172.16.7.179  172.16.7.183  172.16.7.178 |

Figure 88: Table - Full List of Live Devices Found in the 172.16.8.0/24 Subnet:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.8.1  172.16.8.9  172.16.8.10  172.16.8.12  172.16.8.17  172.16.8.16 | 172.16.8.18  172.16.8.19  172.16.8.20  172.16.8.40  172.16.8.41  172.16.8.42 | 172.16.8.43  172.16.8.44  172.16.8.71  172.16.8.85  172.16.8.102  172.16.8.141  172.16.8.144 | 172.16.8.143  172.16.8.145  172.16.8.148  172.16.8.149  172.16.8.147  172.16.8.175 |

Figure 89: Table - Full List of Live Devices Found in the 172.16.9.0/24 Subnet:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.9.1  172.16.9.16  172.16.9.18  172.16.9.19  172.16.9.20  172.16.9.21  172.16.9.22  172.16.9.23  172.16.9.33  172.16.9.32  172.16.9.34 | 172.16.9.74  172.16.9.78  172.16.9.83  172.16.9.82  172.16.9.81  172.16.9.85  172.16.9.87  172.16.9.88  172.16.9.89  172.16.9.100  172.16.9.102 | 172.16.9.101  172.16.9.103  172.16.9.105  172.16.9.104  172.16.9.106  172.16.9.107  172.16.9.109  172.16.9.112  172.16.9.111  172.16.9.113  172.16.9.117 | 172.16.9.118  172.16.9.120  172.16.9.121  172.16.9.122  172.16.9.123  172.16.9.125  172.16.9.126  172.16.9.176  172.16.9.75  172.16.9.86 |

Figure 90: Table - Full List of Live Devices Found in the 172.16.3.0/24 Subnet:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.3.2  172.16.3.9  172.16.3.12  172.16.3.14  172.16.3.15  172.16.3.17 | 172.16.3.18  172.16.3.19  172.16.3.41  172.16.3.45  172.16.3.44  172.16.3.48 | 172.16.3.51  172.16.3.52  172.16.3.131  172.16.3.134  172.16.3.143  172.16.3.145 | 172.16.3.142  172.16.3.144  172.16.3.149  172.16.3.175  172.16.3.47  172.16.3.46 |

Figure 91: Table - Full List of Live Devices Found in the 172.16.4.0/24 Subnet:

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.4.1  172.16.4.10  172.16.4.9  172.16.4.12  172.16.4.13  172.16.4.14  172.16.4.16  172.16.4.17 | 172.16.4.18  172.16.4.19  172.16.4.39  172.16.4.41  172.16.4.40  172.16.4.46  172.16.4.54  172.16.4.52 | 172.16.4.53  172.16.4.55  172.16.4.80  172.16.4.84  172.16.4.142  172.16.4.141  172.16.4.144  172.16.4.146 | 172.16.4.147  172.16.4.145  172.16.4.149  172.16.4.150  172.16.4.151  172.16.4.154  172.16.4.175 |