Internal Network Penetration Test

TECHNICAL REPORT

Sample Client

May 29, 2024

whiterookcyber.com.au

Copyright

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. White Rook Cyber 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:	Demo Consultant
Title:	Consultant
Office:	(844) 866-2732
Email:	support@whiterook.com.au

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 system 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 Penetration Test (14)		
IPv6 DNS Spoofing	📶	Critical
Link-Local Multicast Name Resolution (LLMNR) Spoofing	📶	Critical
Microsoft Windows RCE (BlueKeep)	📶	Critical
NetBIOS Name Service (NBNS) Spoofing	📶	Critical
Outdated Microsoft Windows Systems	📶	Critical
SMBv1 Enabled	📶	High
Weak Active Directory Account Password Policy	📶	High
Anonymous FTP Enabled	📶	Medium
Insecure Protocol - FTP	📶	Medium
Insecure Protocol - Telnet	📶	Medium
SMB NULL Session Authentication	📶	Medium
SMB Signing Not Required	📶	Medium
LDAP Permits Anonymous Bind Access	📶	Low
Egress Filtering Deficiencies	📶	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), White Rook Cyber recommends that Sample Client visit the specific URLs provided within the table below. Furthermore, White Rook Cyber has also elaborated on how these TTPs were used during the penetration test in this report's Penetration Test Narrative section.

White Rook Cyber recommends Sample 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
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Remote System Discovery	Discovery	T1018
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Active Scanning: Scanning IP Blocks	Reconnaissance	T1595.001
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Network Service Discovery	Discovery	T1046
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Brute Force: Password Guessing	Credential-access	T1110.001
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Network Service Discovery	Discovery	T1046
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Network Service Discovery	Discovery	T1046
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Network Service Discovery	Discovery	T1046
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Gather Victim Host Information: Software	Reconnaissance	T1592.002
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	System Information Discovery	Discovery	T1082
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	System Owner/User Discovery	Discovery	T1033
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Brute Force: Password Spraying	Credential-access	T1110.003
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Brute Force: Password Guessing	Credential-access	T1110.001
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Brute Force: Password Guessing	Credential-access	T1110.001
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Brute Force: Password Guessing	Credential-access	T1110.001
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Brute Force: Password Guessing	Credential-access	T1110.001
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay	Credential-access	T1557.001
Mon, Jun 12, 2023 @ 10:21:05 AM CDT	Brute Force: Password Cracking	Credential-access	T1110.002

Internal Network Penetration Test

Engagement Scope of Work

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

IP ADDRESSES & RANGES			
[redacted]/24	[redacted]/24	[redacted]/24	[redacted]/24
[redacted]/24	[redacted]/24	[redacted]/24	[redacted]/24
[redacted]/24	[redacted]/24	[redacted]/24	[redacted]/24
[redacted]/23	[redacted]/23	[redacted]/23	

Agent Information

To perform this assessment, White Rook Cyber 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 Customer D Agent
Private IP Address	[redacted]
Subnet Mask	[redacted] (/16)
DNS Server	[redacted]
Default Gateway	[redacted]

Task Performed

To assess the targets listed above fully, White Rook Cyber 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

White Rook Cyber and Sample Client agreed to the following rules of engagements:

ACTIVITY	DEFINITION	PERMISSION
Exploitation	White Rook Cyber consultants will cautiously execute exploitation techniques to gain access to sensitive data and/or systems.	

Post Exploitation	If exploitation is successful, White Rook Cyber will attempt to escalate privileges within the environment to gain further access to systems and/or data.	

The following activities were either disabled or reduced as part of the penetration testing engagement to comply with the scope requirements:

ACTIVITY	CONFIGURED SETTING	RECOMMENDED

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 fifteen (15) IP addresses/ranges that were provided as part of the scope, White Rook Cyber was able to identify a total of two hundred and seventy-six (276) systems to be active within the targeted environment.

MITRE ATT&CK®	
Name	Active Scanning: Scanning IP Blocks
Tactic	Reconnaissance
TTP ID	T1595.001
Note	White Rook Cyber also performed a port scan against two hundred and seventy-six (276) 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 two hundred and seventy-six (276) addresses/ranges that were scanned, White Rook Cyber found one thousand and seventeen (1,017) 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
Undetected	238
Windows 10.0 Build 19041 x64	16
Windows 10.0 Build 18362 x64	12
Windows 10.0 Build 17763 x64	3

Windows Server 2016 Standard 14393 x64	2
Unix	1
Windows Server 2012 R2 Standard 9600 x64	1
Windows 7 Professional 7601 Service Pack 1 x64	1
VxWorks	1
Windows 5.1	1

PORT/PROTOCOL	COUNT
80/tcp	218
22/tcp	104
23/tcp	89
443/tcp	69
5060/tcp	46
445/tcp	41
135/tcp	39
9100/tcp	37
631/tcp	37
515/tcp	37

The first step in the enumeration phase was the discovery of systems on the local subnet.

MITRE | ATT&CK®	
Name	Remote System Discovery
Tactic	Discovery
TTP ID	T1018
Note	White Rook Cyber performed an arp-scan across the local network subnet to determine which systems are on the local subnet ([redacted]/16). This is also an essential task as these systems would be targets for man-in-the-middle attacks since they are on the same subnet. To facilitate this task, White Rook Cyber used a tool known as *arp-scan*.

The following results demonstrate that two hundred and ninety-one (291) systems exist on the same local subnet:

```
Interface: eth0, type: EN10MB, MAC: e4:5f:01:00:c3:54, IPv4: [redacted]
Starting arp-scan 1.10.0 with 65536 hosts (https://github.com/royhills/arp-scan)
[redacted]      40:a8:f0:dd:68:00       Hewlett Packard
[redacted]      a0:b3:cc:1b:06:00       Hewlett Packard
[redacted]      40:a8:f0:e0:06:00       Hewlett Packard
[redacted]      10:1f:74:a2:af:20       Hewlett Packard
[redacted]      3c:2a:f4:b8:66:01       Brother Industries, LTD.
[redacted]      ec:9a:74:b7:ff:c0       Hewlett Packard
[redacted]      e8:39:35:7f:fa:20       Hewlett Packard
[redacted]      40:a8:f0:d8:89:00       Hewlett Packard
[redacted]      f0:92:1c:3c:80:00       Hewlett Packard
```

```
[redacted]      d4:c9:ef:c3:41:80       Hewlett Packard
[redacted]      d4:c9:ef:c3:11:40       Hewlett Packard
[redacted]      10:1f:74:a2:ef:e0       Hewlett Packard
[redacted]      74:46:a0:08:b8:a0       Hewlett Packard
[redacted]      1c:98:ec:8f:d7:80       Hewlett Packard Enterprise
[redacted]      ec:eb:b8:78:ad:c0       Hewlett Packard Enterprise
[redacted]      3c:4a:92:a6:9f:00       Hewlett Packard
[redacted]      10:4f:58:64:0f:00       Aruba, a Hewlett Packard Enterprise Company
[redacted]      10:4f:58:68:a3:00       Aruba, a Hewlett Packard Enterprise Company
[redacted]      b8:d4:e7:8e:32:80       Aruba, a Hewlett Packard Enterprise Company

----- SNIPPED -----

The remainder of this output has been snipped for reporting purposes.
```

While White Rook Cyber identified these systems via arp-scan on the local subnet, it was noted that these systems were not in-scope as part of this penetration test, but could potentially have exploits or vulnerabilities present. As a result, the systems identified above are only shown for informational purposes.

White Rook Cyber identified one (1) Microsoft SQL (MSSQL) Service present within the tested environment. While this discovery does not indicate any significant issues were found, MSSQL 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 server, at which point an attacker can begin to run SQL commands or execute system level commands.

MITRE ATT&CK®	
Name	Brute Force: Password Guessing
Tactic	Credential-access
TTP ID	T1110.001
Note	White Rook Cyber performed an enumeration to identify information about Microsoft SQL servers found within the discovery phase.

The following information was discovered from the Microsoft SQL servers:

White Rook Cyber identified one (1) MySQL service 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.

MITRE ATT&CK®	
Name	Network Service Discovery
Tactic	Discovery
TTP ID	T1046
Note	White Rook Cyber performed an enumeration to identify information about the MySQL services found during the discovery phase.

The following information was enumerated from the MySQL service(s) found during this assessment:

```
[*] [redacted]:3306      - [redacted]:3306 is running MySQL, but responds with an error: \x04Host '[redacted]' is not allo
wed to connect to this MySQL server
```

Next, White Rook Cyber identified thirteen (13) systems that exposed port 3389/tcp, which hosts the Remote Desktop Protocol (RDP) service and began enumerating information from the opened services. In particular, White Rook Cyber attempted to identify whether or not the targets were vulnerable to common vulnerabilities that could be exploited to achieve remote code execution or denial-of-service (DoS).

Thirteen (13) systems were scanned using the cve_2019_0708_bluekeep module to identify potential RDP vulnerabilities. Scan results identified one (1) vulnerable system. The following results were obtained from this scan:

```
[*] file:/root/pentest/102172/discovery/port_scans/open_ports/tcp/3389.txt:3389 - Scanned  9 of 13 hosts (69% complete)
[+] [redacted]:3389      - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[*] file:/root/pentest/102172/discovery/port_scans/open_ports/tcp/3389.txt:3389 - Scanned 10 of 13 hosts (76% complete)
[*] file:/root/pentest/102172/discovery/port_scans/open_ports/tcp/3389.txt:3389 - Scanned 10 of 13 hosts (76% complete)
[*] file:/root/pentest/102172/discovery/port_scans/open_ports/tcp/3389.txt:3389 - Scanned 10 of 13 hosts (76% complete)
[*] file:/root/pentest/102172/discovery/port_scans/open_ports/tcp/3389.txt:3389 - Scanned 10 of 13 hosts (76% complete)
[*] file:/root/pentest/102172/discovery/port_scans/open_ports/tcp/3389.txt:3389 - Scanned 11 of 13 hosts (84% complete)
[*] file:/root/pentest/102172/discovery/port_scans/open_ports/tcp/3389.txt:3389 - Scanned 12 of 13 hosts (92% complete)
[*] file:/root/pentest/102172/discovery/port_scans/open_ports/tcp/3389.txt:3389 - Scanned 12 of 13 hosts (92% complete)
[*] file:/root/pentest/102172/discovery/port_scans/open_ports/tcp/3389.txt:3389 - Scanned 12 of 13 hosts (92% complete)
[*] file:/root/pentest/102172/discovery/port_scans/open_ports/tcp/3389.txt:3389 - Scanned 13 of 13 hosts (100% complete)
```

White Rook Cyber identified one (1) PostgreSQL service present within the tested environment. While this discovery does not indicate any significant issues were found, PostgreSQL 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.

MITRE | ATT&CK	
Name	Network Service Discovery
Tactic	Discovery
TTP ID	T1046
Note	White Rook Cyber performed an enumeration to identify information about the PostgreSQL services found during the discovery phase.

The following information was enumerated from the PostgreSQL service(s) found during this assessment:

```
[*] [redacted]:5432 Postgres - Version Unknown (Pre-Auth)
```

Testing of FTP services identified ten (10) systems to accept anonymous FTP authentication credentials. Anonymous login credentials would allow 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 [redacted]
Host is up, received user-set (0.0037s latency).
Scanned at 2023-06-11 01:45:56 UTC for 0s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 63
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| total 1
| -r--r--r--   1 root     printer   4096 Sep 28  2001 CFG-PAGE.TXT
|_----------   1 root     printer      0 Sep 28  2001 Sleep-----------
```

While analyzing one of the FTP services at [redacted], White Rook Cyber was able to enumerate the directory structure. The results of the directory structure listing are below:

```
./
./help
./info
./prnlog
./stat
./syslog
```

MITRE | ATT&CK	
Name	Network Service Discovery
Tactic	Discovery
TTP ID	T1046
Note	White Rook Cyber continued testing against these services by attempting to enumerate the files stored on the affected FTP servers. To facilitate this process, White Rook Cyber leveraged the *lftp* tool, which can significantly expedite the time it takes to enumerate FTP services.

Based on the results of the reviewed FTP services, no sensitive information was identified.

White Rook Cyber identified eighty-nine (89) 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:

```
[+] [redacted]:23          - [redacted]:23 TELNET \x1b[2J\x1b[ -- snipped --
[+] [redacted]:23          - [redacted]:23 TELNET \x1b[2J\x1b[ -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET \x1b[2J\x1b -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET \x1b[2J\x1b -- snipped --
[+] [redacted]:23          - [redacted]:23 TELNET \x1b[2J\x1b[ -- snipped --
[+] [redacted]:23          - [redacted]:23 TELNET \x1b[2J\x1b[ -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET Sorry, the  -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET Sorry, the  -- snipped --
[+] [redacted]:23          - [redacted]:23 TELNET Sorry, the m -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET \x1b[2J\x1b -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET \x1b[2J\x1b -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET \x1b[2J\x1b -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET \x1b[2J\x1b -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET \x1b[2J\x1b -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET \x1b[2J\x1b -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET Sorry, the  -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET Sorry, the  -- snipped --
[+] [redacted]:23          - [redacted]:23 TELNET Sorry, the m -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET \x1b[2J\x1b -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET \x1b[2J\x1b -- snipped --
[+] [redacted]:23         - [redacted]:23 TELNET \x1b[2J\x1b -- snipped --

----- SNIPPED -----

The remainder of this output has been snipped for reporting purposes.
```

Next, White Rook Cyber identified forty-one (41) systems that exposed port 445/tcp, which is for the Server Message Block (SMB) service. This service was targeted for the 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 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 *relays* them to another system, pivoting off that authenticated session to perform additional attacks, such as remote command execution.

Testing identified four (4) of the forty-one (41) systems with port 445/tcp opened that did not require SMB signing, therefore being vulnerable to SMB relay attacks. The following sample output from CrackMapExec identified this weakness:

```
[redacted]:(signing:False)
[redacted]:(signing:False)
[redacted]:(signing:False)
[redacted]:(signing:False)
```

MITRE | ATT&CK®

Name	System Information Discovery
Tactic	Discovery
TTP ID	T1082
Note	Additionally, scans were conducted across these systems to identify information about the operating systems, including operating system versions, service pack versions, domain membership, etc.

As part of this operating system identification process, White Rook Cyber identified thirty-eight (38) operating systems. It's important to note that the tools and techniques used to gather information about operating system versions are not always 100% accurate. While White Rook Cyber makes several attempts to confirm the accurate operating systems through additional methods, it should be noted that some results may require additional validation from a system administrator. The following output demonstrates some of the results obtained:

```
SMB         [redacted]     445    [obfuscated-dns]  [*] Windows 10.0 Build 19041 x64 (name: [obfuscated-dns]) (domain:[obf
uscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]     445    [obfuscated-dns]  [*] Windows Server 2016 Standard 14393 x64 (name: [obfuscated-dns]) (d
omain:[obfuscated-domain].local) (signing:True) (SMBv1:True)
SMB         [redacted]     445    [obfuscated-dns]  [*] Windows 10.0 Build 18362 x64 (name: [obfuscated-dns]) (domain:[obf
uscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]     445    [obfuscated-dns]  [*] Windows 10.0 Build 18362 x64 (name: [obfuscated-dns]) (domain:[obf
uscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]     445    [obfuscated-dns]  [*] Windows 10.0 Build 19041 x64 (name: [obfuscated-dns]) (domain:[obf
uscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]     445    [obfuscated-dns]  [*] Windows 10.0 Build 19041 x64 (name: [obfuscated-dns]) (domain:[obf
uscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]      445    [obfuscated-dns]  [*] Windows 10.0 Build 19041 x64 (name: [obfuscated-dns]) (domain:[ob
fuscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]     445    [obfuscated-dns]  [*] Windows 10.0 Build 19041 x64 (name: [obfuscated-dns]) (domain:[obf
uscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]       445    [obfuscated-dns]  [*] Windows 10.0 Build 18362 x64 (name: [obfuscated-dns]) (domain:[o
bfuscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]     445    [obfuscated-dns]  [*] Windows Server 2012 R2 Standard 9600 x64 (name: [obfuscated-dns])
(domain:[obfuscated-domain].local) (signing:True) (SMBv1:True)
SMB         [redacted]     445    [obfuscated-dns]  [*] Windows 10.0 Build 19041 x64 (name: [obfuscated-dns]) (domain:[obf
uscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]     445    [obfuscated-dns]  [*] Unix (name: [obfuscated-dns]) (domain:%H) (SMBv1:True)
SMB         [redacted]     445    [obfuscated-dns]  [*] Windows 10.0 Build 17763 x64 (name: [obfuscated-dns]) (domain[obfu
scated-domain]) (SMBv1:False)
SMB         [redacted]     445    [obfuscated-dns]  [*] Windows 10.0 Build 18362 x64 (name: [obfuscated-dns]) (domain:[obf
uscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]      445    [obfuscated-dns]  [*] Windows 10.0 Build 19041 x64 (name: [obfuscated-dns]) (domain:[ob
fuscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]     445    [obfuscated-dns]  [*] VxWorks (name:) (domain:) (SMBv1:True)
SMB         [redacted]      445    [obfuscated-dns]  [*] Windows 10.0 Build 18362 x64 (name: [obfuscated-dns]) (domain:[ob
fuscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]     445    [obfuscated-dns]  [*] Windows 10.0 Build 17763 x64 (name: [obfuscated-dns]) (domain:[obf
uscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]      445    [obfuscated-dns]  [*] Windows 10.0 Build 18362 x64 (name: [obfuscated-dns]) (domain:[ob
fuscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]      445    [obfuscated-dns]  [*] Windows 10.0 Build 18362 x64 (name: [obfuscated-dns]) (domain:[ob
fuscated-domain].local) (signing:True) (SMBv1:False)
SMB         [redacted]     445    [obfuscated-dns]  [*] Windows 10.0 Build 19041 x64 (name: [obfuscated-dns]) (domain:[obf
uscated-domain].local) (signing:True) (SMBv1:False)
```

```
----- SNIPPED -----

The remainder of this output has been snipped for reporting purposes.
```

White Rook Cyber also identified one (1) system that used an outdated operating system. Outdated operating systems 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:

```
SMB         [redacted]      445    [obfuscated-dns]  [*] Windows 7 Professional 7601 Service Pack 1 x64 (name:[obfuscated-
dns]) (domain:[obfucsated-domain]) (signing:True) (SMBv1:True)
```

MITRE | ATT&CK®

Name	Gather Victim Host Information: Software
Tactic	Reconnaissance
TTP ID	T1592.002
Note	Next, in an attempt to identify some common security vulnerabilities in outdated operating systems, White Rook Cyber leveraged the Metasploit Framework to perform specific checks to determine whether or not 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.

Thirty-five (35) systems were scanned using the auxiliary/scanner/smb/smb_ms17_010 module to identify potential SMB vulnerabilities. This module attempts to discover systems that contain a common vulnerability named EternalBlue. When successfully 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 the enumeration of local administrator password hashes, the enumeration of Active Directory infrastructure 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:

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

----- SNIPPED -----

The remainder of this output has been snipped for reporting purposes.
```

White Rook Cyber then ran a custom script to check if any systems allowed for SMB NULL session authentication (i.e. without a username or password). SMB NULL sessions can allow attackers with network access to identify and possibly retrieve files that may exist on an SMB (445/tcp) server. If permissions allow for write access, an attacker could also attempt to use this to store malicious code. The results showed that one (1) system accepted SMB NULL session authentication:

```
[redacted]
```

The below sample evidence shows some of the results of this attack:

```
[[redacted]]
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC
        MEMORY_CARD     Disk      FLASH MEMORY PHOTO
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------

------------------------------------------------------------
```

White Rook Cyber then tried to take advantage of SMB NULL session authentication in order to enumerate the SMB shares available on the affected system. The aim of this process was to identify any accessible shares containing potentially sensitive company data as well as shares configured with WRITE access. However, no accessible shares were identified.

Additionally, an enumeration of SMB services was performed in an attempt to identify whether 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:

```
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jun 11 01:50:46 2023

 =========================================( Target Information )=========================================

Target ........... [redacted]
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on [redacted] )============================


[E] Can't find workgroup/domain



 ================================( Nbtstat Information for [redacted] )================================

Looking up status of [redacted]

----- SNIPPED -----

The remainder of this output has been snipped for reporting purposes.
```

No valuable information, such as domain/local user accounts and password policies, was obtained as part of this enumeration process.

Next, White Rook Cyber's objective was to perform a password attack against the Active Directory environment. However, White Rook Cyber needed to gather a list of potential domain user accounts to perform this process. White Rook Cyber used the Kerbrute tool to assist with this process. Kerbrute is a tool that can be used to enumerate domain user accounts by interacting with Kerberos. Based on the response from a ticket-granting ticket (TGT) request to the key distribution center (KDC) server, Kerbrute is able to deduce whether or not the domain user account provided was valid or not.

White Rook Cyber used naming schemes for four different naming conventions: 1) first initial last name, 2) first name last initial, 3) first name dot last initial (e.g. First.Last), and 4) first name. A combination of common first and last names was used as part of this process, as well as publicly available resources.

The following domain was observed as part of the initial host discovery scans performed at the beginning of the assessment:

- [obfuscated-domain].local

MITRE ATT&CK®	
Name	System Owner/User Discovery
Tactic	Discovery
TTP ID	T1033
Note	White Rook Cyber targeted the following domain controller(s) as part of this Kerberos user enumeration attack: [redacted] ([obfuscated-dns])

During this process, White Rook Cyber discovered fifty-nine (59) valid domain user accounts for one (1) domain. The following usernames were observed:

```
[obfuscated-domain].local
----

[obfuscated username]
admin
[obfuscated username]
[obfuscated username]
[obfuscated username]
[obfuscated username]
[obfuscated username]
[obfuscated username]
[obfuscated username]
[obfuscated username]

 --- snipped (max 10 of 59) shown ---
```

During the enumeration phase of the test, White Rook Cyber identified a total of fifty-nine (59) usernames using multiple tools, such as kerbrute and enum4linux, to target for a password attack.

During this password attack, White Rook Cyber identified zero (0) successful login attempts and fifty-nine (59) failed login attempts. The complete evidence of this login attack can be found within the supporting evidence. The following is a short snippet of the password attack results:

```
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\admin:S[obfuscated] STATUS_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
```

```
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE
SMB         [redacted]     445    BO-BDC2          [-] [obfuscated-domain].local\[obfuscated username]:S[obfuscated] STATU
S_LOGON_FAILURE

----- SNIPPED -----

The remainder of this output has been snipped for reporting purposes.
```

During testing, White Rook Cyber identified one (1) system that was vulnerable to the RCE exploit called Bluekeep (CVE-2019-0708). However, the identified operating system for one (1) host is likely to crash during exploitation. Because of this, White Rook Cyber did not attempt exploitation of this system.

MITRE ATT&CK	
Name	Brute Force: Password Guessing
Tactic	Credential-access
TTP ID	T1110.001
Note	White Rook Cyber also reviewed a list of one (1) Microsoft SQL (MSSQL) server 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 significant issues, including remote command execution. No servers were found to contain weak or default credentials at the time of testing. The following code snippet shows sample output results of this scan:

```
[-] [redacted]:1433       - [redacted]:1433 - LOGIN FAILED: WORKSTATION\sa:password (Incorrect: )
[-] [redacted]:1433       - [redacted]:1433 - LOGIN FAILED: WORKSTATION\sa:sa (Incorrect: )
[-] [redacted]:1433       - [redacted]:1433 - LOGIN FAILED: WORKSTATION\sa: (Incorrect: )
```

	MITRE | ATT&CK®
Name	Brute Force: Password Guessing
Tactic	Credential-access
TTP ID	T1110.001
Note	White Rook Cyber also reviewed a list of one (1) MySQL server and conducted a limited password attack to determine if any weak or default credentials could be discovered.

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

```
[-] [redacted]:3306      - [redacted]:3306 - Unsupported target version of MySQL detected. Skipping.
```

	MITRE | ATT&CK®
Name	Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay
Tactic	Credential-access
TTP ID	T1557.001
Note	As part of the exploitation phase, White Rook Cyber continued to perform DNS poisoning attacks via NBNS, LLMNR and mDNS.

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. Similarly, multicast DNS (mDNS) can be used within small networks to resolve a DNS name when no local DNS server exists. This is done via IP multicast query messages to the hosts on the local subnet. The problem with this configuration is that it is possible to respond to these broadcast/multicast 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.

White Rook Cyber 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 assigning all IPv6 clients with an IP address and DNS configurations that route traffic through the attacker's system.

While White Rook Cyber was successful with capturing NBNS/LLMNR/mDNS broadcast packets across the local subnet, it was not possible to capture any credentials at the time of testing. This is primarily due to the lack of systems and/or services successfully authenticating to the penetration testing VM during these attacks. An example of these successful NBNS/LLMNR/mDNS poisoning attempts is shown below:

```
2023-06-11 02:10:27,806 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name [obfuscated-dns]
2023-06-11 02:10:27,808 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name [obfuscated-dns]
2023-06-11 02:10:28,256 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name [obfuscated-dns]
2023-06-11 02:10:28,263 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name [obfuscated-dns]
2023-06-11 02:10:28,298 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name [obfuscated-dns]
2023-06-11 02:10:28,304 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name [obfuscated-dns]
2023-06-11 02:11:27,338 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name wpad
2023-06-11 02:11:27,341 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name wpad
2023-06-11 02:11:27,345 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name wpad
```

```
2023-06-11 02:11:39,445 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name wpad
2023-06-11 02:11:39,446 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name wpad
2023-06-11 02:11:39,448 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name wpad
2023-06-11 02:11:43,594 - [*] [NBT-NS] Poisoned answer sent to [redacted] for name WORKGROUP (service: Local Master Browse
r)
2023-06-11 02:11:57,738 - [*] [NBT-NS] Poisoned answer sent to [redacted] for name [obfuscated-dns] (service: Local Master
Browser)
2023-06-11 02:21:36,735 - [*] [LLMNR]  Poisoned answer sent to fe80::b111:2fcc:8d38:3faa for name wpad
2023-06-11 02:21:36,739 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name wpad
2023-06-11 02:21:36,739 - [*] [LLMNR]  Poisoned answer sent to fe80::b111:2fcc:8d38:3faa for name wpad
2023-06-11 02:22:05,567 - [*] [LLMNR]  Poisoned answer sent to fe80::b111:2fcc:8d38:3faa for name [obfuscated-dns]
2023-06-11 02:22:05,568 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name [obfuscated-dns]
2023-06-11 02:22:06,553 - [*] [NBT-NS] Poisoned answer sent to [redacted] for name [obfuscated-dns] (service: Local Master
Browser)
2023-06-11 02:22:06,555 - [*] [NBT-NS] Poisoned answer sent to [redacted] for name WORKGROUP (service: Local Master Browse
r)

----- SNIPPED -----

The remainder of this output has been snipped for reporting purposes.
```

When attempting to perform IPv6 attacks, White Rook Cyber successfully assigned IPv6 addresses with the attacking system set as the default DNS server. An example of this can be found below:

```
Starting mitm6 using the following configuration:
Primary adapter: eth0 [e4:5f:01:00:c3:54]
IPv4 address: [redacted]
IPv6 address: fe80::e65f:1ff:fe00:c354
Warning: Not filtering on any domain, mitm6 will reply to all DNS queries.
Unless this is what you want, specify at least one domain with -d
IPv6 address fe80::2187:1 is now assigned to mac=00:07:32:7b:32:65 host= ipv4=
IPv6 address fe80::2187:2 is now assigned to mac=f0:2a:2b:51:fb:3e host=[obfuscated-dns]. ipv4=
IPv6 address fe80::2187:3 is now assigned to mac=48:b0:2d:10:89:f0 host=[obfuscated-dns]. ipv4=
IPv6 address fe80::2187:4 is now assigned to mac=78:e7:d1:a1:ee:1d host= ipv4=
IPv6 address fe80::2187:6 is now assigned to mac=bc:4a:56:02:16:31 host=router4478AE. ipv4=
IPv6 address fe80::2187:7 is now assigned to mac=00:07:32:7b:32:65 host= ipv4=
IPv6 address fe80::2187:8 is now assigned to mac=00:1e:67:59:ed:a5 host=[obfuscated-dns].[obfuscated-domain].local. ipv4=
Sent spoofed reply for wpad.[obfuscated-domain].local. to fe80::2187:8
IPv6 address fe80::2187:10 is now assigned to mac=00:9c:02:c1:27:2f host=[obfuscated-dns]. ipv4=
Sent spoofed reply for ctldl.windowsupdate.com. to fe80::be4a:56ff:fe02:1631
Sent spoofed reply for ctldl.windowsupdate.com. to fe80::be4a:56ff:fe02:1631
IPv6 address fe80::2187:11 is now assigned to mac=38:ca:84:ce:84:43 host=[obfuscated-dns]had. ipv4=
IPv6 address fe80::2187:12 is now assigned to mac=00:25:90:65:ad:d4 host=[obfuscated-dns].[obfuscated-domain].local. ipv4=
IPv6 address fe80::2187:14 is now assigned to mac=00:25:90:69:e2:de host=[obfuscated-dns].[obfuscated-domain].local. ipv4=
Sent spoofed reply for isatap.[obfuscated-domain].local. to fe80::2187:14

----- SNIPPED -----

The remainder of this output has been snipped for reporting purposes.
```

At the time of testing, White Rook Cyber was successful with capturing password hashes via NTLM relaying attacks. The following output is a snippet of the NTLM relay log results:

```
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation



[*] HTTPD(80): Client requested path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?0f2e7c3ffb5c870b
[*] HTTPD(80): Client requested path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?359566c305181112
[*] HTTPD(80): Client requested path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?7beacdcbe3866ca0
[*] HTTPD(80): Client requested path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?f1b044029ccc57f5
[*] HTTPD(80): Client requested path: /wpad.dat
[*] HTTPD(80): Client requested path: /wpad.dat
[*] HTTPD(80): Client requested path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?123951b7d891ea05
[*] HTTPD(80): Client requested path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?3842b29457a5042b
[*] HTTPD(80): Client requested path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?0e863877f2bb2c72
[*] HTTPD(80): Client requested path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?bac14001ed8b8d1e
[*] HTTPD(80): Client requested path: /wpad.dat
[*] HTTPD(80): Client requested path: /wpad.dat
[*] HTTPD(80): Client requested path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?5dcd6cace05af320
[*] HTTPD(80): Client requested path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5499967f4a1ff7dd
[-] HTTPD(80): Exception in HTTP request handler: [Errno 104] Connection reset by peer
[-] HTTPD(80): Exception in HTTP request handler: [Errno 104] Connection reset by peer
[-] HTTPD(80): Exception in HTTP request handler: [Errno 104] Connection reset by peer
[-] HTTPD(80): Exception in HTTP request handler: [Errno 104] Connection reset by peer

----- SNIPPED -----

The remainder of this output has been snipped for reporting purposes.
```

While conducting DNS poisoning and NTLM Relay attacks, it was possible to obtain one (1) new password hash. These hashes were queued into a password recovery process in an attempt to identify the cleartext password. An example of up to five (5) captured hashes can be found below:

```
[obfuscated username]::[obfuscated-domain]:56c4e1b16ae0e5cb:7b3f70dea98fbd0a96d380e1213cd515:01010000000...[partially-obfu
scated]
```

White Rook Cyber attempted to obtain the plaintext password for the acquired hash by leveraging the HashCat password cracking tool and a list of common passwords to try. During this attack, one (1) plaintext password was uncovered:

```
[obfuscated-domain].local\[obfuscated username]:[obfuscated]
```

In order to verify the obtained plaintext domain account password, White Rook Cyber used the credentials to try and authenticate to the domain controller at [redacted]. The results of this attack showed that the password was valid:

```
SMB         [redacted]     445    [obfuscated-dns]          [+] [obfuscated-domain].local\[obfuscated username]:[obfuscate
d]
```

The captured Net-NTLM hashes were relayed to the targeted system(s). This attack resulted in the SAM database containing the hashed passwords for local users being dumped from one (1) host:

```
10.10.9.164_samhashes.sam
```

White Rook Cyber used all previously obtained local account password hashes and domain account credentials to try and authenticate to all discovered hosts that had the SMB service (port 445/tcp) available. The aim of this attack, which leveraged the pass-the-hash technique, was to check if these credentials provided local Administrator privileges on any hosts. White Rook Cyber leveraged these credentials to successfully authenticate to thirty-six (36) hosts. Moreover, the credentials provided local administrator privileges on two (2) of those systems. See the breakdown of results below:

```
--------------------------------------------------------------------------------
[COMPROMISED HOSTS]
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]          Privileges obtained: regular user
- IP: [redacted]          Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]           Privileges obtained: regular user
- IP: [redacted]          Privileges obtained: regular user
- IP: [redacted]          Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
- IP: [redacted]         Privileges obtained: regular user
--- snipped (showing 20 out of 29) ---
[SAMPLE EVIDENCE]
--------------------------------------------------------------------------------
SMB         [redacted]     445    [obfuscated-dns]      [+] [obfuscated-domain]\administrator:[partially-obfuscated]16022
(Pwn3d!)
SMB         [redacted]     445    [obfuscated-dns]      [+] [obfuscated-domain].local\[obfuscated username]:[obfuscated]
(Pwn3d!)
SMB         [redacted]     445    [obfuscated-dns]      [+] \[obfuscated username]:[partially-obfuscated]1720a
SMB         [redacted]      445    [obfuscated-dns]      [+] [obfuscated-dns]\admin:[partially-obfuscated]de875
--------------------------------------------------------------------------------
```

White Rook Cyber then leveraged the credentials for the compromised account(s) to run the impacket-secretsdump tool against the two (2) systems where the compromised account(s) had local admin privileges. This attack aimed to obtain password hashes and/or plaintext passwords from the SAM database and from memory. The below sample evidence shows some of the credentials that were obtained during this attack:

```
PlainText (1)
---
[obfuscated-domain].local\[obfuscated username]:[obfuscated]

NTLM (7)
---
admin:1005:aad3b435b51404eeaad3b435b51404ee:082dcc95a1292874ff[obfuscated]
administrator:500:aad3b435b51404eeaad3b435b51404ee:aa1d5e70dd2[obfuscated]
[obfuscated username]:1007:aad3b435b51404eeaad3b435b51404ee:f051feb0dd37[obfuscated]
---snipped---

NTLM Domain Computer (1)
---
[obfuscated-domain]\[obfuscated computer name]$:aad3b435b51404eeaad3b435b51404ee:2bbe4435a267574[obfuscated]

MSCache (10)
---
[obfuscated username]:aac0b7405e9ec166[obfuscated]
[obfuscated username]:2c6325984ed579c662[obfuscated]
[obfuscated username]:32d1b7d75bd0c1f5c0a[obfuscated]
---snipped---
```

White Rook Cyber attempted to obtain the plaintext password for the acquired hash(es) by leveraging the HashCat password cracking tool and a list of common passwords to try. However, this attack failed.

In order to verify the obtained plaintext domain account password, White Rook Cyber used the credentials to try and authenticate to the domain controller at [redacted]. The results of this attack showed that the password was valid and even provided White Rook Cyber with local admin rights on the domain controller:

```
SMB         [redacted]     445    BO-PDC2          [+] [obfuscated-domain].local\[obfuscated username]:[obfuscated] (Pwn3
d!)
```

Next, White Rook Cyber used the CME tool together with the [obfuscated-domain].local\[obfuscated username] credentials in order to obtain the password policy for the [obfuscated-domain].local domain from the domain controller at [redacted]:

```
Minimum password length:  8
Password history length:  6
Maximum password age:  355 days 3 minutes

Password Complexity Flags:  000001
    Domain Refuse Password Change:  0
    Domain Password Store Cleartext:  0
    Domain Password Lockout Admins:  0
    Domain Password No Clear Change:  0
    Domain Password No Anon Change:  0
    Domain Password Complex:  1

Minimum password age:  1 day 4 minutes
Reset Account Lockout Counter:  10 minutes
Locked Account Duration:  10 minutes
Account Lockout Threshold:  5
Forced Log off Time:  Not Set
```

The results showed that the [obfuscated-domain].local domain was configured with the following weak password policy setting(s):

```
Reset Account Lockout Counter: 10
Locked Account Duration: 10
```

In order to obtain more information on the [obfuscated-domain].local domain, White Rook Cyber used the password for the [obfuscated-domain].local\[obfuscated username] account to enumerate LDAP using the Bloodhound-Python tool. A total of four hundred and thirty-four (434) computers, three hundred and forty-six (346) users and one hundred and one (101) groups were identified on the domain in this manner. The results also showed that the domain was configured with fourteen (14) domain admin accounts. The below sample evidence shows some of the active directory information that was gathered:

```
[computers]
--snipped--
[obfuscated-dns]
[obfuscated-dns]
[obfuscated-dns]
[obfuscated-dns]
[obfuscated-dns]
--snipped--

[domain admins]
--snipped--
[obfuscated user account]
[obfuscated user account]
[obfuscated user account]
[obfuscated user account]
[obfuscated user account]
--snipped--

[groups]
--snipped--
password boss users
vpn
duo mfa
enterprise key admins
system managed accounts group
--snipped--

[users]
--snipped--
NT AUTHORITY
[obfuscated user account]
[obfuscated user account]
[obfuscated user account]
[obfuscated user account]
--snipped--
```

The active directory information that had previously been obtained via LDAP enumeration, showed that the [obfuscated-domain].local[obfuscated username] account was part of the domain admins group. This meant that White Rook Cyber had now fully compromised the [obfuscated-domain].local domain.

Next, White Rook Cyber attempted to perform an attack known as Kerberoasting. This attack takes advantage of the Kerberos protocol and can be performed for any valid domain user account, regardless of privileges. When an active directory user logs in, they receive a Ticket Granting Ticket (TGT) from the Kerberos key distribution center. If the authenticated user then requests a specific resource in the domain, their TGT is used to request a Ticket Granting Service (TGS) token for that resource. Part of this TGS is encrypted with the NTLM hash of the service account for the requested resource. If an attacker obtains a TGS, they can try and crack it and obtain the user's password via brute-force methods or lists of common passwords. Obtaining a TGS requires knowledge of the existing service principal names (SPNs) that Windows uses to identify which service accounts are being used to encrypt TGS tokens.

White Rook Cyber used the credentials for the [obfuscated-domain].local\[obfuscated username] account together with the impacket-GetUserSPNs tool in an attempt to obtain the SPNs configured on the domain and use those to obtain TGS tokens.

The below results show that two (2) unique SPNS were obtained:

```
ServicePrincipalName                              Name           MemberOf
----------------------------------------------    -------------  ---------------------------------------------------------
MSSQLSvc/[obfuscated-dns].[obfuscated-domain].local:SQLEXPRESS       Administrator  CN=SophosAdministrator,CN=Users,DC=[ob
fuscated-domain],DC=local
MSSQLSvc/[obfuscated-domain]School.[obfuscated-domain].local:SQLAVG  setup          CN=Administration,OU=Administrative,DC
=[obfuscated-domain],DC=local
```

The SPNS were then used to retrieve two (2) unique TGS tokens:

```
$krb5tgs$23$*Administrator$[obfuscated-domain].local$[obfuscated-domain].local/Administrator*$[obfuscated]
$krb5tgs$23$*setup$[obfuscated-domain].local$[obfuscated-domain].local/setup*$[obfuscated]
```

White Rook Cyber attempted to obtain the plaintext password for the acquired hashes by leveraging the HashCat password cracking tool and a list of common passwords to try. During this attack, one (1) plaintext password was uncovered:

```
[obfuscated-domain].local\setup:[obfuscated]
```

In order to verify the obtained plaintext domain account password, White Rook Cyber used the credentials to try and authenticate to the domain controller at [redacted]. The results of this attack showed that the password was valid and even provided White Rook Cyber with local admin rights on the domain controller:

```
SMB         [redacted]     445    BO-PDC2          [+] [obfuscated-domain].local\setup:[obfuscated] (Pwn3d!)
```

Next, White Rook Cyber used the obtained domain admin credentials in order to enumerate the SMB shares available on the compromised system(s). The aim of this process was to identify any accessible shares containing potentially sensitive company data. At the time of testing, sensitive data was discovered, including email information, tax information, financial information, credentials, passports. The below evidence shows some of the sensitive information that was observed:

```
[credentials]
\\[redacted]\administration\[obfuscated name]\Passwords\Amazon userid-password.doc          A    26112  Tue Jul  9 14:02:5
0 2013
\\[redacted]\administration\[obfuscated name]\Passwords\Pitney Bowes userid-password.doc      A    22016  Mon Jul 22 16:3
1:35 2019
\\[redacted]\administration\[obfuscated name]\Passwords\School Speciality userid-password.doc      A    27136  Tue Jul 28
21:15:56 2020
\\[redacted]\administration\[obfuscated name]\Passwords\USPS userid-password.doc            A    27136  Wed Sep  2 17:29:4
8 2020
\\[redacted]\administration\[obfuscated name]]\Passwords\Amazon userid-password.doc          A    26112  Tue Jul  9 14:02:
50 2013
--snipped--

[email information]
\\[redacted]\gdrive\Scans\Physical Forms\HS Girls\Samson, Amber 2021-4-28 email re-date.pdf      A   236174  Fri Jul 31 0
```

```
1:20:04 2020
\\[redacted]\gdrive\Scans\Physical Forms\HS Girls\EXPIRED 2019-20 Sports Physicals\Hentges, Kadence 2019-10-31 Email.pdf
A   125779  Thu Oct 31 22:15:26 2019
\\[redacted]\administration\[obfuscated name]\JOBS e-mail.doc                     A    24064  Mon Jan 28 19:40:24 2008
\\[redacted]\administration\[obfuscated name]\Board member Info\Email info for board members.docx      A    12578  Fri Feb
4 16:38:11 2022
\\[redacted]\administration\[obfuscated name]\Church Bulletins\Email addresses for church bulletins.docx      A    12268
Fri Jan 14 21:17:29 2022
--snipped--

[financial information]
\\[redacted]\administration\[obfuscated name]\Lodge of the Four Seasons - Credit Auth Form for Don Jeffries.pdf      A
84105  Fri Mar 23 21:30:00 2018
\\[redacted]\administration\[obfuscated name]\Paint the Town Paid Invoice.docx      A    68616  Fri Aug  3 15:40:29 2018
\\[redacted]\administration\[obfuscated name]\Credit Card - 2008-2009.xls         A    16384  Fri Jun 26 18:24:44 2009
\\[redacted]\administration\[obfuscated name]\Credit Card - 2009-2010.xls         A    52736  Thu Jul 15 22:08:04 2010
\\[redacted]\administration\[obfuscated name]\D & K Invoice Worksheet.xls         A    29696  Tue Jan 14 14:25:38 2020
--snipped--

[passports]
\\[redacted]\teachers\[obfuscated name]\Paragraph Passport 6.docx           A    14090  Mon Aug 10 17:25:15 2015
\\[redacted]\teachers\[obfuscated name]\Paragraph Passport 7.docx           A    14257  Mon Aug 10 17:24:35 2015
\\[redacted]\teachers\[obfuscated name]\Paragraph Passport.docx             A    14260  Mon Aug 10 17:24:24 2015
\\[redacted]\teachers\[obfuscated name]\[obfuscated name]backup\passport facts about applying.docx      A    20016  Wed Ma
y 13 19:57:17 2015
\\[redacted]\teachers\[obfuscated name]\Personal\Scotland\[obfuscated name] - Passport.jpg         A   999885  Wed May 18
17:54:22 2022
--snipped--

[tax information]
\\[redacted]\administration\Angie's Folder\Tax exemption form for Dell.pdf      A    50387  Mon Dec 13 18:28:41 2021
\\[redacted]\administration\[obfuscated name]\Home Depot Tax Exempt Request.doc      A    24576  Tue Feb 21 15:03:34 2012
\\[redacted]\administration\[obfuscated name]\Cole County Tax Dist.xls            A    14336  Mon Aug  9 17:26:22 2010
\\[redacted]\administration\Angie's Folder\Miscellaneous\Dell tax.pdf                        A    47810  Wed Dec 15 14:37:
59 2021
\\[redacted]\administration\Angie's Folder\Miscellaneous\Dollar general tax exempt form.pdf      A    71971  Wed Mar  2 2
0:45:34 2022
--snipped--
```

Next, White Rook Cyber enumerated web services in the environment with the aim of obtaining sensitive information by exploiting default credentials, security vulnerabilities or misconfigurations.

Testing showed that fourteen (14) web instances allowed unauthenticated address book access. This made it possible to extract user information that could be used to enumerate Active Directory usernames. The affected services were:

```
http://[redacted] - Konica Minolta
http://[redacted] - Konica Minolta
http://[redacted] - Konica Minolta
http://[redacted] - Konica Minolta
http://[redacted] - Konica Minolta
http://[redacted] - Konica Minolta
http://[redacted] - Konica Minolta
http://[redacted] - Konica Minolta
http://[redacted] - Konica Minolta
http://[redacted] - Konica Minolta
http://[redacted] - Konica Minolta
http://[redacted] - Konica Minolta
http://[redacted] - Konica Minolta
http://[redacted] - Konica Minolta
```

The sample output below shows (some of the) obtained user information:

```
[obfuscated name]
[obfuscated name]
[obfuscated name]
[obfuscated name]
```

```
[obfuscated name]
[obfuscated name]
[obfuscated name]
[obfuscated name]
[obfuscated name]
[obfuscated name]
--snipped--
```

The address book information could have been used for username guessing. However, this attack was not performed since a full list of domain user accounts had already been obtained via LDAP enumeration.

The following table contains all the accounts for which plaintext credentials were obtained during post-exploitation:

Domain or source IP	User	Domain Administrator	Weak Password
[obfuscated-domain].local	[obfuscated user account]	No	Yes
[obfuscated-domain].local	[obfuscated user account]	Yes	No
[obfuscated-domain].local	[obfuscated user account]	Yes	Yes

The accounts mentioned in the table above should be considered compromised and should have their passwords changed as soon as possible as they could pose a significant threat to the organization's overall environment depending on the account permissions and the security controls implemented.

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, White Rook Cyber 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 IPv6 over IPv4, 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 - 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.

Affected Nodes

TEN (10) NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
[redacted]	[obfuscated]	Windows Server 2012 R2 Standard 9600 x64
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		VxWorks
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected

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.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/

Evidence

```
IPv6 address fe80::2187:1 is now assigned to mac=00:07:32:7b:32:65 host= ipv4=
IPv6 address fe80::2187:2 is now assigned to mac=f0:2a:2b:51:fb:3e host=[obfuscated dns]. ipv4=
IPv6 address fe80::2187:3 is now assigned to mac=48:b0:2d:10:89:f0 host=[obfuscated dns]. ipv4=
IPv6 address fe80::2187:4 is now assigned to mac=78:e7:d1:a1:ee:1d host= ipv4=
IPv6 address fe80::2187:6 is now assigned to mac=bc:4a:56:02:16:31 host=[obfuscated dns]. ipv4=
IPv6 address fe80::2187:7 is now assigned to mac=00:07:32:7b:32:65 host= ipv4=
IPv6 address fe80::2187:8 is now assigned to mac=00:1e:67:59:ed:a5 host=[obfuscated dns].[obfuscated domain].loca
l. ipv4=
Sent spoofed reply for wpad.[obfuscated domain].local. to fe80::2187:8
IPv6 address fe80::2187:10 is now assigned to mac=00:9c:02:c1:27:2f host=[obfuscated dns]. ipv4=
Sent spoofed reply for ctldl.windowsupdate.com. to fe80::be4a:56ff:fe02:1631
Sent spoofed reply for ctldl.windowsupdate.com. to fe80::be4a:56ff:fe02:1631
IPv6 address fe80::2187:11 is now assigned to mac=38:ca:84:ce:84:43 host=[obfuscated dns]. ipv4=
IPv6 address fe80::2187:12 is now assigned to mac=00:25:90:65:ad:d4 host=[obfuscated dns].[obfuscated domain].loca
l. ipv4=
IPv6 address fe80::2187:14 is now assigned to mac=00:25:90:69:e2:de host=[obfuscated dns].[obfuscated domain].loca
l. ipv4=
Sent spoofed reply for isatap.[obfuscated domain].local. to fe80::2187:14
IPv6 address fe80::2187:15 is now assigned to mac=00:07:32:7b:32:65 host= ipv4=
Sent spoofed reply for wpad.[obfuscated domain].local. to fe80::2187:12
IPv6 address fe80::2187:16 is now assigned to mac=d0:8e:79:f5:72:2e host=[obfuscated dns]. ipv4=
Sent spoofed reply for teredo.ipv6.microsoft.com. to fe80::2187:14
Sent spoofed reply for dns.msftncsi.com. to fe80::2187:14
IPv6 address fe80::8662:1 is now assigned to mac=00:9c:02:c1:27:2f host=BOAC-[obfuscated dns]. ipv4=

--snipped--
```

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 checks 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 host's file, the system then sends a DNS query to its configured DNS server(s) to attempt to retrieve 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-resolution.aspx

Evidence

```
2023-06-11 02:10:27,806 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name [obfuscated dns]
2023-06-11 02:10:27,808 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name [obfuscated dns]
2023-06-11 02:10:28,256 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name [obfuscated dns]
2023-06-11 02:10:28,263 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name [obfuscated dns]
2023-06-11 02:10:28,298 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name [obfuscated dns]
2023-06-11 02:10:28,304 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name [obfuscated dns]
2023-06-11 02:11:27,338 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name wpad
2023-06-11 02:11:27,341 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name wpad
2023-06-11 02:11:27,345 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name wpad
2023-06-11 02:11:39,445 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name wpad
2023-06-11 02:11:39,446 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name wpad
2023-06-11 02:11:39,448 - [*] [LLMNR]  Poisoned answer sent to fe80::2187:14 for name wpad
2023-06-11 02:21:36,735 - [*] [LLMNR]  Poisoned answer sent to fe80::b111:2fcc:8d38:3faa for name wpad
2023-06-11 02:21:36,739 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name wpad
2023-06-11 02:21:36,739 - [*] [LLMNR]  Poisoned answer sent to fe80::b111:2fcc:8d38:3faa for name wpad
2023-06-11 02:22:05,567 - [*] [LLMNR]  Poisoned answer sent to fe80::b111:2fcc:8d38:3faa for name [obfuscated dns]
2023-06-11 02:22:05,568 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name [obfuscated dns]
2023-06-11 02:22:07,666 - [*] [LLMNR]  Poisoned answer sent to fe80::[redacted] for name [obfuscated dns]
2023-06-11 02:22:07,671 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name [obfuscated dns]
2023-06-11 02:22:08,139 - [*] [LLMNR]  Poisoned answer sent to fe80::[redacted] for name [obfuscated dns]
2023-06-11 02:22:08,139 - [*] [LLMNR]  Poisoned answer sent to [redacted] for name [obfuscated dns]

--snipped--
```

CRITICAL

Microsoft Windows RCE (BlueKeep)

Observation

During testing, systems were identified that are vulnerable to CVE-2019-0708 (BlueKeep), which is a vulnerability that exists in Microsoft Windows systems. This vulnerability is extremely valuable to an attacker due to the availability of tools and code that could take advantage of this weakness. Successful exploitation of this vulnerability typically results in full access to the exploited system(s).

Security Impact

By exploiting the BlueKeep vulnerability, an attacker could gain full control over the affected system. This typically leads to additional attacks within the organization, including extraction of cleartext passwords and hashes, along with lateral movement within the network. Since exploitation of this vulnerability does not require privilege escalation on the affected system, an attacker would typically have as much access as they need on the compromised system to start enumerating the system.

Affected Nodes

ONE (1) NODE AFFECTED

IP Address	Host Name	Operating System
[redacted]	[obfuscated]	Windows 5.1

Recommendation

It is recommended to apply security updates on the affected system. Furthermore, the organization should evaluate its patch management program to determine the reason for the lack of security updates. As this vulnerability is a commonly exploited vulnerability and could result in significant access, it should be remediated immediately.

Reproduction Steps

Using a tool such as Metasploit, use the following module:

```
exploit/windows/rdp/cve_2019_0708_bluekeep_rce
```

Provide the necessary IP address information about the source and target, and type "exploit" to launch the exploit. It should be noted that exploitation of this issue could potentially cause an impact on the availability of the remote system.

References

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

Evidence

```
[+] [redacted]:3389      - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120
channel.
```

CRITICAL

NetBIOS Name Service (NBNS) Spoofing

Observation

NetBIOS Name Service (NBNS) 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 checks 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 NBNS broadcast packet on the local network to seek assistance from other systems.

Security Impact

Since the NBNS 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.

Affected Nodes

THREE (3) NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
[redacted]		Undetected
[redacted]	[obfuscated]	Unix
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64

Recommendation

The following are some strategies for preventing the use of NBNS in a Windows environment or reducing the impact of NBNS Spoofing attacks:

- Configure the UseDnsOnlyForNameResolutions registry key in order to prevent systems from using NBNS queries (http://technet.microsoft.com/en-us/library/cc775874(v=ws.10).aspx). Set the registry DWORD to 1.
- Disable the NetBIOS service for all Windows hosts in the internal network. This can be done via DHCP options, network adapter settings, or a registry key.

Reproduction Steps

On a system configured with NBNS, 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://markgamache.blogspot.com/2013/01/ntlm-challenge-response-is-100-broken.html
- http://support.microsoft.com/kb/313314
- http://develnet.blogspot.com/2006/10/disabling-netbios-over-tcpip-via.html
- http://technet.microsoft.com/en-us/library/cc775874(v=ws.10).aspx

Evidence

```
2023-06-11 02:11:43,594 - [*] [NBT-NS] Poisoned answer sent to [redacted] for name WORKGROUP (service: Local Master Browser)
2023-06-11 02:11:57,738 - [*] [NBT-NS] Poisoned answer sent to [redacted] for name [obfuscated dns] (service: Local Master Browser)
2023-06-11 02:22:06,553 - [*] [NBT-NS] Poisoned answer sent to [redacted] for name [obfuscated dns] (service: Local Master Browser)
2023-06-11 02:22:06,555 - [*] [NBT-NS] Poisoned answer sent to [redacted] for name WORKGROUP (service: Local Master Browser)
2023-06-11 02:41:04,676 - [*] [NBT-NS] Poisoned answer sent to [redacted] for name WPAD (service: Workstation/Redirector)
2023-06-11 02:41:04,677 - [*] [NBT-NS] Poisoned answer sent to [redacted] for name WPAD (service: Workstation/Redirector)
2023-06-11 02:41:04,681 - [*] [NBT-NS] Poisoned answer sent to [redacted] for name WPAD (service: Workstation/Redirector)
```

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.

Affected Nodes

ONE (1) NODE AFFECTED

IP Address	Host Name	Operating System
[redacted]	[obfuscated]	Windows 7 Professional 7601 Service Pack 1 x64

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

```
SMB         [redacted]      445    BORH-SHEILA-NEW  [*] Windows 7 Professional 7601 Service Pack 1 x64 (name:[obfu
scated dns]) (domain:[obfuscated domain].local) (signing:True) (SMBv1:True)
                "os": "Windows 7 Professional 7601 Service Pack 1",
```

HIGH

SMBv1 Enabled

Observation

Server Message Block (or SMB) is a communication protocol used in Windows operating systems to communicate with each other over a network. SMB serves an important part in an Active Directory environment as it provides file sharing, printer sharing, and network browsing to machines in the environment. It also allows for processes to communicate with each other using a concept called named pipes, and this is what's known as inter-process communication.

Security Impact

SMBv1 has been depreciated by Microsoft since 2013. Due to this, SMBv1 has become outdated and contains multiple exploits/vulnerabilities that can allow remote control execution on the target machine using this protocol.

Affected Nodes

SEVEN (7) NODES AFFECTED

IP Address	Host Name	Operating System
[redacted]	[obfuscated]	Windows Server 2012 R2 Standard 9600 x64
[redacted]	[obfuscated]	Windows 7 Professional 7601 Service Pack 1 x64
[redacted]	[obfuscated]	Windows Server 2016 Standard 14393 x64
[redacted]	[obfuscated]	Windows Server 2016 Standard 14393 x64
[redacted]	[obfuscated]	Windows 5.1
[redacted]	[obfuscated]	Unix
[redacted]		VxWorks

Recommendation

To stay protected from exploits that target vulnerabilities in this protocol, it's recommended to disable SMBv1 in favor of SMBv2/v3.

Microsoft has published documentation on their site about disabling SMBv1, as well as upgrading to SMBv2/v3 in just a few commands.

- **Disabling SMBv1:** https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server#how-to-remove-smbv1-via-powershell
- **Enabling SMBv2/v3:** https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server#how-to-remove-smbv1-via-powershell

Reproduction Steps

The **CrackMapExec** tool can be utilized to check whether or not a host has SMBv1 enabled. To do so the following command can be used:

```
crackmapexec smb <ip>
```

This will scan the IP and return a result similar to this:

```
SMB         [redacted]     445    SRV    [*] Windows Server 2012 R2 Standard 9600 x64 (name:SRV) (domain:domain.lo
cal) (SMBv1:True)
```

The **(SMBv1:True)** part of the response is what indicates whether or not SMBv1 is in use. In this case you can see it shows that this host has SMBv1 enabled since the value is set to **True**.

References

- **WannaCry:** What is WANNACRY/WANACRYPTOR? (cisa.gov)
- **Petya:** Petya Destructive Malware Variant Spreading via Stolen Credentials and EternalBlue Exploit | Mandiant
- **Bad Rabbit**: Bad Rabbit, Software S0606 | MITRE ATT&CKÂ®

Evidence

```
SMB         [redacted]     445    [obfuscated dns]          [*] Windows Server 2016 Standard 14393 x64 (name:[obfu
scated dns]) (domain:[obfuscated domain].local) (signing:True) (SMBv1:True)
SMB         [redacted]     445    [obfuscated dns]               [*] Unix (name:[obfuscated dns]) (domain:[obfusca
ted domain]) (signing:False) (SMBv1:True)
SMB         [redacted]     445    [obfuscated dns]    [*] Windows Server 2012 R2 Standard 9600 x64 (name:[obfuscat
ed dns]) (domain:[obfuscated domain].local) (signing:True) (SMBv1:True)
SMB         [redacted]      445    [obfuscated dns]  [*] Windows 7 Professional 7601 Service Pack 1 x64 (name:[obf
uscated dns]) (domain:[obfuscated domain].local) (signing:True) (SMBv1:True)
SMB         [redacted]     445    [obfuscated dns]          [*] Windows Server 2016 Standard 14393 x64 (name:[obfu
scated dns]) (domain:[obfuscated domain].local) (signing:True) (SMBv1:True)
SMB         [redacted]     445    NONE             [*] VxWorks (name:) (domain:) (signing:False) (SMBv1:True)
```

HIGH

Weak Active Directory Account Password Policy

Observation

An Active Directory Domain Password Policy is extremely critical as it is the security settings that many domain user accounts will use when having their accounts configured. These policies include lockout thresholds, lockout durations, minimum characters required, password complexity requirements, and more. During post-exploitation, it was discovered that the password policy configured does not meet security best practices.

Security Impact

A weak password policy can be disastrous for a company in that it allows attackers to exploit the weaknesses of domain user accounts. For example, the lack of a strict account lockout threshold allows malicious attackers to perform numerous login attempts to domain user accounts prior to being locked out. Here are some of the security impacts that can be associated with domain password policies:

- **Minimum password length:** An attacker can take advantage of this by trying weak passwords that exist in the dictionary, such as Apple, Car, Dog, etc. By increasing the minimum password length, an attacker's chances of successfully guessing and/or even cracking (through password cracking techniques) a password is much lower.
- **Lockout threshold:** If the lockout threshold value is too low, an attacker can perform numerous login attempts to the user accounts before locking out an account, which then depends on the lockout duration for unlocking the domain user account.
- **Lockout duration (minutes):** If the account does not remain locked out for a long period of time, then attackers can continuously perform login attempts every X amount of minutes that the account gets unlocked. A small number increases the chances of a successful attack as the disruption to user accounts will be minimum.
- **Lockout observation window (minutes):** By default, Microsoft Windows sets this to 30. This setting indicates how many times someone can perform a login attempt before it subtracts from the lockout threshold. For example, if this setting is set to 30, then this means an attacker can perform one login attempt per 30 minutes, and the lockout threshold will never exceed the value of 1 because the observation window *resets* the counter every 30 minutes.

Recommendation

Use the references to reconfigure your domain's password policy to adhere to security best practices.

Reproduction Steps

Using the Microsoft Windows command line interface (CLI), use the following command to query the domain's password policy:

```
net accounts "domain" /domain
```

References

- https://blog.devolutions.net/2018/02/top-10-password-policies-and-best-practices-for-system-administrators
- https://www.microsoft.com/en-us/microsoft-365/blog/2018/03/05/azure-ad-and-adfs-best-practices-defending-against-password-spray-attacks/

Evidence

The results showed that the [obfuscated domain].local domain was configured with the following weak password policy setting(s):

```
Reset Account Lockout Counter: 10
Locked Account Duration: 10
```

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 anyone to log in 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.

Affected Nodes

TEN (10) NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected

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, connect to the affected FTP server(s) using "anonymous/anonymous" (username and password).

Evidence

```
Nmap scan report for [redacted]
Host is up, received user-set (0.0037s latency).
Scanned at 2023-06-11 01:45:56 UTC for 0s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 63
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| total 1
| -r--r--r--   1 root     printer   4096 Sep 28  2001 CFG-PAGE.TXT
|_----------   1 root     printer      0 Sep 28  2001 Sleep-----------
```

```
Nmap scan report for [redacted]
Host is up, received arp-response (0.00043s latency).
Scanned at 2023-06-11 01:45:52 UTC for 3s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 64
| 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
MAC Address: 00:26:73:7D:59:8A (Ricoh Company)
```

```
Nmap scan report for [redacted]
Host is up, received arp-response (0.00089s latency).
Scanned at 2023-06-11 01:45:52 UTC for 1s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 64
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| total 1
| -r--r--r--   1 root     printer   4096 Sep 28  2001 CFG-PAGE.TXT
|_----------   1 root     printer      0 Sep 28  2001 Sleep-----------
MAC Address: 30:05:5C:84:49:CA (Brother industries)
```

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.

Affected Nodes

ELEVEN (11) NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected

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 [redacted]
Host is up, received user-set (0.0054s latency).
Scanned at 2023-06-10 18:03:37 UTC for 3496s
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE   REASON
21/tcp   open  ftp       syn-ack ttl 63
```

```
Nmap scan report for [redacted]
Host is up, received arp-response (0.0010s latency).
Scanned at 2023-06-10 13:49:56 UTC for 9s
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE   REASON
21/tcp   open  ftp       syn-ack ttl 64
MAC Address: 30:05:5C:84:44:46 (Brother industries)
```

```
Nmap scan report for [redacted]
Host is up, received user-set (0.0032s latency).
Scanned at 2023-06-10 18:03:37 UTC for 2666s
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE   REASON
21/tcp   open  ftp       syn-ack ttl 63
```

```
Nmap scan report for [redacted]
Host is up, received arp-response (0.0010s latency).
Scanned at 2023-06-10 13:49:56 UTC for 9s
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE   REASON
21/tcp   open  ftp       syn-ack ttl 64
MAC Address: 30:05:5C:84:49:CA (Brother industries)
```

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.

Affected Nodes

EIGHTY-NINE (89) NODES AFFECTED

IP Address	Host Name	Operating System
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]	[obfuscated]	Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected

[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected

[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		Undetected
[redacted]		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 [redacted]
Host is up, received user-set (0.00037s latency).
Scanned at 2023-06-10 16:17:45 UTC for 24s
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE REASON
23/tcp open  telnet  syn-ack ttl 64
```

```
Nmap scan report for [redacted]
Host is up, received user-set (0.00053s latency).
Scanned at 2023-06-10 21:39:56 UTC for 30s
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE REASON
23/tcp open  telnet  syn-ack ttl 64
```

```
Nmap scan report for [redacted]
Host is up, received user-set (0.00088s latency).
Scanned at 2023-06-10 17:37:38 UTC for 29s
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE REASON
23/tcp open  telnet  syn-ack ttl 64
```

```
Nmap scan report for [redacted]
Host is up, received user-set (0.0029s latency).
Scanned at 2023-06-11 01:45:59 UTC for 0s

PORT   STATE SERVICE REASON
23/tcp open  telnet  syn-ack ttl 64
| telnet-encryption:
|_  Telnet server does not support encryption
```

MEDIUM

SMB NULL Session Authentication

Observation

A Server Message Block protocol (SMB) service allows SMB NULL Session Authentication (i.e. without a username or password). SMB NULL sessions allow anyone to log in to SMB shares to browse the files that have been remotely uploaded.

Security Impact

The issue with SMB NULL sessions is that any individual, including an attacker, could gain remote access to the SMB share and observe the contents. If the NULL session also provides write access, an attacker may also be able to leverage this insecure configuration in order to store/transmit malicious code.

The exposure of files stored on affected SMB shares 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.

Affected Nodes

ONE (1) NODE AFFECTED		
IP Address	**Host Name**	**Operating System**
[redacted]		VxWorks

Recommendation

If the SMB 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 SMB NULL session authentication and implementing authentication that leverages a complex password.

Reproduction Steps

Connect to the affected SMB server(s) using a blank username and a blank password. For the built-in Unix utility smbclient, the syntax is shown below:

```
smbclient -L <IP> --no-pass
```

If the operation succeeds without any errors and smbclient prints information about the configured shares and/or workgroups, the SMB server is affected.
The same checks can also be performed using dedicated scripts that are part of the Metasploit framework or the Nmap portscanning tool.

Evidence

```
[[redacted]]
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC
        MEMORY_CARD     Disk      FLASH MEMORY PHOTO
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
------------------------------------------------------------
```

MEDIUM

SMB Signing Not Required

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 required 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. Furthermore, 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.

Affected Nodes

FOUR (4) NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
[redacted]	[obfuscated]	Windows 10.0 Build 17763 x64
[redacted]	[obfuscated]	Unix
[redacted]		VxWorks
[redacted]	[obfuscated]	Windows 5.1

Recommendation

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

Reproduction Steps

Leverage 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

```
SMB         [redacted]     445    [obfuscated dns]               [*] Unix (name:[obfuscated dns]) (domain:[obfusca
ted domain]) (signing:False) (SMBv1:True)
SMB         [redacted]     445    [obfuscated dns]   [*] Windows 10.0 Build 17763 x64 (name:[obfuscated dns]) (dom
ain:[obfuscated domain]) (signing:False) (SMBv1:False)
SMB         [redacted]     445    NONE             [*] VxWorks (name:) (domain:) (signing:False) (SMBv1:True)
SMB         [redacted]     445    [obfuscated dns]      [*] Windows 5.1 (name:[obfuscated dns]) (domain:[obfuscate
d domain].local) (signing:False) (SMBv1:True)
[redacted]:(signing:False)
[redacted]:(signing:False)
```

LOW

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.

Affected Nodes

TWO (2) NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
[redacted]	[obfuscated]	Windows Server 2016 Standard 14393 x64
[redacted]	[obfuscated]	Windows Server 2016 Standard 14393 x64

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 "ldap-rootdse" 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-rootdse
```

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 [redacted]
Host is up, received arp-response (0.00016s latency).
Scanned at 2023-06-11 01:46:03 UTC for 0s

PORT    STATE SERVICE REASON
389/tcp open  ldap    syn-ack ttl 128
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       currentTime: 20230611014603.0Z
|       subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=[obfuscated domain],DC=local
|       dsServiceName: CN=NTDS Settings,CN=[obfuscated dns],CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Conf
iguration,DC=[obfuscated domain],DC=local
|       namingContexts: DC=[obfuscated domain],DC=local
|       namingContexts: CN=Configuration,DC=[obfuscated domain],DC=local
|       namingContexts: CN=Schema,CN=Configuration,DC=[obfuscated domain],DC=local
|       namingContexts: DC=DomainDnsZones,DC=[obfuscated domain],DC=local
|       namingContexts: DC=ForestDnsZones,DC=[obfuscated domain],DC=local
|       defaultNamingContext: DC=[obfuscated domain],DC=local
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=[obfuscated domain],DC=local
|       configurationNamingContext: CN=Configuration,DC=[obfuscated domain],DC=local
|       rootDomainNamingContext: DC=[obfuscated domain],DC=local

--snipped--
```

INFORMATIONAL Egress Filtering Deficiencies

Observation

An egress filtering check was performed as part of the internal network penetration test. This check aims to determine if the internal environment allows excessive access to the public Internet, which could increase the risk of data exfiltration. This check was not performed against a specific in-scope target, but on the public Internet in general to evaluate this risk.

During this check, it was possible to identify access to an excessive number of ports residing on the public Internet. This particular check targeted scanme.nmap.org, which is designed for organizations to check whether or not they have access to servers on the public Internet.

Security Impact

Allowing end-users 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 ([external-ip])
Host is up (0.048s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (reset)
PORT      STATE    SERVICE
19/tcp    filtered chargen
22/tcp    open     ssh
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite
```

```
Read data files from: /usr/bin/../share/nmap
# Nmap done at Sun Jun 11 01:44:07 2023 -- 1 IP address (1 host up) scanned in 2.13 seconds
```

Appendix A: Host Discovery (Operating Systems)

Internal Network Penetration Test

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
[redacted]	[obfuscated]	Windows Server 2012 R2 Standard 9600 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 17763 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 17763 x64	
[redacted]	[obfuscated]	Unix	
[redacted]	[obfuscated]	Windows Server 2016 Standard 14393 x64	
[redacted]	[obfuscated]	Windows Server 2016 Standard 14393 x64	
[redacted]		VxWorks	
[redacted]	[obfuscated]	Windows 10.0 Build 17763 x64	
[redacted]	[obfuscated]	Windows 7 Professional 7601 Service Pack 1 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 18362 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 18362 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 18362 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 18362 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 18362 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	

[redacted]	[obfuscated]	Windows 10.0 Build 18362 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 18362 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 18362 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 18362 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 19041 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 18362 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 18362 x64	
[redacted]	[obfuscated]	Windows 10.0 Build 18362 x64	
[redacted]	[obfuscated]	Windows 5.1	

Appendix B: Identified Nodes Without Ports

During testing, all identified systems were found to have at least one (1) open port. As a result, no table will be displayed in this section.

Appendix C: Host Discovery (Opened Ports)

Internal Network Penetration Test

IP Address	DNS Name	Port (Limited to 1000)	Protocol
[redacted]	[obfuscated]	22	tcp
[redacted]	[obfuscated]	80	tcp
[redacted]	[obfuscated]	23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		23	tcp

[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		443	tcp
[redacted]		80	tcp
[redacted]		9100	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		80	tcp

[redacted]		22	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		9100	tcp
[redacted]		21	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		139	tcp
[redacted]		514	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		7443	tcp
[redacted]		8080	tcp
[redacted]	[obfuscated]	49155	tcp
[redacted]	[obfuscated]	49154	tcp
[redacted]	[obfuscated]	49153	tcp
[redacted]	[obfuscated]	49152	tcp
[redacted]	[obfuscated]	8443	tcp
[redacted]	[obfuscated]	8088	tcp
[redacted]	[obfuscated]	3389	tcp
[redacted]	[obfuscated]	1521	tcp
[redacted]	[obfuscated]	1099	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	443	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	80	tcp

[redacted]	[obfuscated]	49156	tcp
[redacted]	[obfuscated]	49175	tcp
[redacted]		22	tcp
[redacted]		5900	tcp
[redacted]		443	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]	[obfuscated]	5357	tcp
[redacted]	[obfuscated]	3389	tcp
[redacted]	[obfuscated]	1521	tcp
[redacted]	[obfuscated]	1099	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	443	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	80	tcp
[redacted]	[obfuscated]	8443	tcp
[redacted]	[obfuscated]	8088	tcp
[redacted]	[obfuscated]	80	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	3389	tcp
[redacted]	[obfuscated]	8009	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	443	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		5900	tcp
[redacted]		443	tcp
[redacted]		3128	tcp
[redacted]		8090	tcp
[redacted]		8443	tcp
[redacted]		53	tcp

[redacted]		25	tcp
[redacted]		22	tcp
[redacted]		443	tcp
[redacted]		1025	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		9100	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		9100	tcp
[redacted]		631	tcp
[redacted]		50001	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		80	tcp
[redacted]		427	tcp
[redacted]		9100	tcp
[redacted]		80	tcp
[redacted]		427	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		50001	tcp
[redacted]		9100	tcp
[redacted]		21	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		515	tcp

[redacted]		631	tcp
[redacted]		9100	tcp
[redacted]		8080	tcp
[redacted]		9100	tcp
[redacted]		515	tcp
[redacted]		443	tcp
[redacted]		427	tcp
[redacted]		80	tcp
[redacted]		50001	tcp
[redacted]		631	tcp
[redacted]		631	tcp
[redacted]		515	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		21	tcp
[redacted]		9100	tcp
[redacted]		443	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		8080	tcp
[redacted]		9100	tcp
[redacted]		515	tcp
[redacted]		443	tcp
[redacted]		80	tcp
[redacted]		9100	tcp
[redacted]		631	tcp
[redacted]		80	tcp
[redacted]		21	tcp
[redacted]		23	tcp
[redacted]		443	tcp
[redacted]		515	tcp

[redacted]		631	tcp
[redacted]		9100	tcp
[redacted]		50001	tcp
[redacted]		80	tcp
[redacted]		427	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		9100	tcp
[redacted]		50001	tcp
[redacted]		9100	tcp
[redacted]		631	tcp
[redacted]		515	tcp
[redacted]		443	tcp
[redacted]		427	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		50001	tcp
[redacted]		9100	tcp
[redacted]		631	tcp
[redacted]		515	tcp
[redacted]		443	tcp
[redacted]		427	tcp
[redacted]		50001	tcp
[redacted]		80	tcp
[redacted]		427	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		9100	tcp
[redacted]	[obfuscated]	8080	tcp
[redacted]	[obfuscated]	22	tcp
[redacted]	[obfuscated]	80	tcp

[redacted]	[obfuscated]	139	tcp
[redacted]	[obfuscated]	443	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	1310	tcp
[redacted]	[obfuscated]	3128	tcp
[redacted]	[obfuscated]	8000	tcp
[redacted]	[obfuscated]	8001	tcp
[redacted]		50001	tcp
[redacted]		9100	tcp
[redacted]		631	tcp
[redacted]		515	tcp
[redacted]		443	tcp
[redacted]		427	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		50001	tcp
[redacted]		9100	tcp
[redacted]		631	tcp
[redacted]		515	tcp
[redacted]		443	tcp
[redacted]		427	tcp
[redacted]		50001	tcp
[redacted]		9100	tcp
[redacted]		631	tcp
[redacted]		515	tcp
[redacted]		443	tcp
[redacted]		427	tcp
[redacted]		80	tcp
[redacted]		9100	tcp
[redacted]		631	tcp
[redacted]		50001	tcp
[redacted]		515	tcp
[redacted]		443	tcp

[redacted]		427	tcp
[redacted]		80	tcp
[redacted]		9100	tcp
[redacted]		80	tcp
[redacted]		427	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		50001	tcp
[redacted]		8290	tcp
[redacted]		9100	tcp
[redacted]		7	tcp
[redacted]		80	tcp
[redacted]		515	tcp
[redacted]		8080	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		5900	tcp
[redacted]		22	tcp
[redacted]		50001	tcp
[redacted]		443	tcp
[redacted]		427	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		9100	tcp
[redacted]		80	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	593	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	636	tcp
[redacted]	[obfuscated]	88	tcp
[redacted]	[obfuscated]	80	tcp
[redacted]	[obfuscated]	53	tcp

[redacted]	[obfuscated]	3269	tcp
[redacted]	[obfuscated]	3268	tcp
[redacted]	[obfuscated]	3389	tcp
[redacted]	[obfuscated]	464	tcp
[redacted]	[obfuscated]	389	tcp
[redacted]	[obfuscated]	636	tcp
[redacted]	[obfuscated]	8090	tcp
[redacted]	[obfuscated]	8080	tcp
[redacted]	[obfuscated]	5432	tcp
[redacted]	[obfuscated]	5357	tcp
[redacted]	[obfuscated]	3389	tcp
[redacted]	[obfuscated]	3269	tcp
[redacted]	[obfuscated]	3268	tcp
[redacted]	[obfuscated]	1102	tcp
[redacted]	[obfuscated]	1089	tcp
[redacted]	[obfuscated]	1068	tcp
[redacted]	[obfuscated]	1034	tcp
[redacted]	[obfuscated]	593	tcp
[redacted]	[obfuscated]	464	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	443	tcp
[redacted]	[obfuscated]	389	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	88	tcp
[redacted]	[obfuscated]	80	tcp
[redacted]	[obfuscated]	53	tcp
[redacted]		9111	tcp
[redacted]		9290	tcp
[redacted]		9101	tcp
[redacted]		9102	tcp
[redacted]		9110	tcp
[redacted]		9220	tcp
[redacted]		80	tcp

[redacted]		139	tcp
[redacted]		443	tcp
[redacted]		445	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		6839	tcp
[redacted]		7435	tcp
[redacted]		8080	tcp
[redacted]		9100	tcp
[redacted]	[obfuscated]	3389	tcp
[redacted]	[obfuscated]	2179	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]		631	tcp
[redacted]		9100	tcp
[redacted]		21	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		7627	tcp
[redacted]		3306	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		111	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		111	tcp
[redacted]		80	tcp
[redacted]		9009	tcp
[redacted]		111	tcp
[redacted]		80	tcp

[redacted]		9009	tcp
[redacted]		111	tcp
[redacted]		9100	tcp
[redacted]		8080	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		8080	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		4343	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		111	tcp
[redacted]		443	tcp
[redacted]		2049	tcp
[redacted]		4001	tcp
[redacted]		9081	tcp
[redacted]		4003	tcp
[redacted]		9090	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	1433	tcp
[redacted]	[obfuscated]	49153	tcp
[redacted]	[obfuscated]	49154	tcp
[redacted]	[obfuscated]	49152	tcp
[redacted]	[obfuscated]	5357	tcp
[redacted]	[obfuscated]	3389	tcp
[redacted]		4000	tcp

[redacted]		8080	tcp
[redacted]		8002	tcp
[redacted]		8001	tcp
[redacted]		9009	tcp
[redacted]		80	tcp
[redacted]		111	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		111	tcp
[redacted]		9009	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		111	tcp
[redacted]		111	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		111	tcp
[redacted]		8080	tcp
[redacted]		4343	tcp
[redacted]		443	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		111	tcp
[redacted]		9100	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		631	tcp

[redacted]		8080	tcp
[redacted]		4001	tcp
[redacted]		9081	tcp
[redacted]		9090	tcp
[redacted]		443	tcp
[redacted]		2049	tcp
[redacted]		4003	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		111	tcp
[redacted]		80	tcp
[redacted]		111	tcp
[redacted]		9009	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]		9009	tcp
[redacted]		111	tcp
[redacted]		80	tcp
[redacted]		9009	tcp
[redacted]		111	tcp
[redacted]		80	tcp
[redacted]		111	tcp
[redacted]		80	tcp
[redacted]		9009	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	9001	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	808	tcp
[redacted]		111	tcp
[redacted]		80	tcp
[redacted]		9009	tcp
[redacted]		9009	tcp
[redacted]		80	tcp

[redacted]		111	tcp
[redacted]		80	tcp
[redacted]		9009	tcp
[redacted]		111	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	5357	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]		9009	tcp
[redacted]		80	tcp
[redacted]		111	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		111	tcp
[redacted]		9009	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	139	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	808	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]	[obfuscated]	135	tcp

[redacted]	[obfuscated]	445	tcp
[redacted]		443	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	808	tcp
[redacted]	[obfuscated]	9001	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]		515	tcp
[redacted]		80	tcp
[redacted]		631	tcp
[redacted]		443	tcp
[redacted]		9500	tcp
[redacted]		9100	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]	[obfuscated]	139	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		1443	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	808	tcp
[redacted]		111	tcp
[redacted]		9009	tcp
[redacted]		80	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	808	tcp
[redacted]	[obfuscated]	139	tcp
[redacted]	[obfuscated]	5357	tcp
[redacted]	[obfuscated]	135	tcp

[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	808	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		443	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]	[obfuscated]	445	tcp

[redacted]	[obfuscated]	135	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		445	tcp
[redacted]		808	tcp
[redacted]		135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]		50001	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		9100	tcp
[redacted]		427	tcp
[redacted]		808	tcp
[redacted]		445	tcp
[redacted]		135	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	3389	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]		9009	tcp
[redacted]		111	tcp
[redacted]		80	tcp
[redacted]	[obfuscated]	445	tcp

[redacted]	[obfuscated]	135	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]		8088	tcp
[redacted]		80	tcp
[redacted]		554	tcp
[redacted]		5060	tcp
[redacted]		443	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		5900	tcp
[redacted]		8080	tcp
[redacted]		443	tcp
[redacted]		4343	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	3389	tcp
[redacted]	[obfuscated]	80	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	3389	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]		443	tcp
[redacted]		5060	tcp
[redacted]		5061	tcp
[redacted]		80	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	3389	tcp
[redacted]		80	tcp

[redacted]		5061	tcp
[redacted]		5060	tcp
[redacted]		443	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		443	tcp
[redacted]		5900	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	80	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		9100	tcp
[redacted]		21	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		443	tcp
[redacted]		3007	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	445	tcp
[redacted]	[obfuscated]	3389	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]	[obfuscated]	3389	tcp
[redacted]	[obfuscated]	135	tcp
[redacted]	[obfuscated]	139	tcp

[redacted]	[obfuscated]	445	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		5060	tcp
[redacted]		5060	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		554	tcp
[redacted]		80	tcp
[redacted]		8080	tcp
[redacted]		5357	tcp
[redacted]		1935	tcp

[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp

[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		1025	tcp
[redacted]		22	tcp
[redacted]		25	tcp
[redacted]		53	tcp
[redacted]		443	tcp
[redacted]		3128	tcp
[redacted]		8090	tcp
[redacted]		8443	tcp
[redacted]		49152	tcp
[redacted]		49156	tcp
[redacted]		62078	tcp
[redacted]		49152	tcp
[redacted]		49154	tcp
[redacted]		62078	tcp
[redacted]		135	tcp
[redacted]		139	tcp
[redacted]		445	tcp
[redacted]		49152	tcp

[redacted]		49153	tcp
[redacted]		62078	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp

[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		8090	tcp
[redacted]		8443	tcp
[redacted]		443	tcp
[redacted]		53	tcp
[redacted]		25	tcp
[redacted]		22	tcp
[redacted]		1025	tcp
[redacted]		3128	tcp
[redacted]		49154	tcp
[redacted]		49152	tcp
[redacted]		62078	tcp
[redacted]		8080	tcp
[redacted]		21	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		81	tcp

[redacted]		82	tcp
[redacted]		83	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		9100	tcp
[redacted]		515	tcp
[redacted]		9100	tcp
[redacted]		631	tcp
[redacted]		443	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		21	tcp
[redacted]		62078	tcp
[redacted]		21	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		9100	tcp
[redacted]		631	tcp
[redacted]		631	tcp
[redacted]		21	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		9100	tcp
[redacted]		49154	tcp
[redacted]		49152	tcp
[redacted]		62078	tcp
[redacted]		8080	tcp
[redacted]		80	tcp

[redacted]		443	tcp
[redacted]		515	tcp
[redacted]		631	tcp
[redacted]		9100	tcp
[redacted]		62078	tcp
[redacted]		49152	tcp
[redacted]		49153	tcp
[redacted]		49152	tcp
[redacted]		62078	tcp
[redacted]		49152	tcp
[redacted]		49154	tcp
[redacted]		22	tcp
[redacted]		4343	tcp
[redacted]		443	tcp
[redacted]		80	tcp
[redacted]		49153	tcp
[redacted]		4343	tcp
[redacted]		443	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		4343	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		443	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		4343	tcp
[redacted]		443	tcp
[redacted]		443	tcp
[redacted]		80	tcp
[redacted]		9100	tcp
[redacted]		8080	tcp
[redacted]		631	tcp

[redacted]		62078	tcp
[redacted]		49153	tcp
[redacted]		49152	tcp
[redacted]		62078	tcp
[redacted]		49152	tcp
[redacted]		49152	tcp
[redacted]		49154	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		4343	tcp
[redacted]		443	tcp
[redacted]		49154	tcp
[redacted]		49152	tcp
[redacted]		4343	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		443	tcp
[redacted]		4343	tcp
[redacted]		9100	tcp
[redacted]		631	tcp
[redacted]		515	tcp
[redacted]		23	tcp
[redacted]		443	tcp
[redacted]		80	tcp
[redacted]		21	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		23	tcp

[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		22	tcp

[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		25	tcp
[redacted]		53	tcp
[redacted]		443	tcp
[redacted]		1025	tcp
[redacted]		3128	tcp
[redacted]		8090	tcp
[redacted]		8443	tcp
[redacted]		3689	tcp
[redacted]		7100	tcp
[redacted]		62078	tcp
[redacted]		5000	tcp
[redacted]		7000	tcp
[redacted]		631	tcp
[redacted]		515	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp

[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		80	tcp
[redacted]		80	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		22	tcp
[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		22	tcp

[redacted]		23	tcp
[redacted]		80	tcp
[redacted]		80	tcp