Pentera™

Penetration Test

Detailed Report

May. 25, 2025 | Pentest Monedero XIGA

Pentera™ automated penetration test report summarizes the vulnerabilities, exploit achievements and remediation action items recommended in your network based on the latest ethical hacking pentesting techniques

pronet

PENTERA

Pentesting

ECC1695784032

Pronet
Pentester
C. Caturegli 219B Col. Olivares

Table Of Contents

Detailed Report

Appendix

Executive Summary

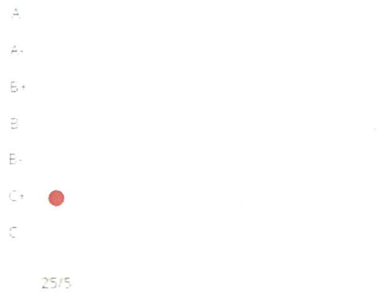
✓ Completed successfully

Cyber Resilience Score & Settings

Resilience Score
C+

Test Name:	**Pentest Monedero XIGA**
Description:	Penetration test de IPs de Monedero XIGA
Type:	**Penetration Testing (Black Box)**
Time & Duration:	May 23 2025 23:44 - May 24 2025 20:10, 20:25
Included IP Range(s):	**10.255.248.110, 10.255.248.14, 10....** 15 Ranges
Action Approval Score:	112 / 112 - 100%
User Input:	**8 - Network Rescan(s)**

Resilience Score Over Last 1 Tasks



Resilience Score Card

Critical Assets	[illegible]	
Credentials and Account Takeover	Gained access to 11 accounts (1 of them privileged): 10 Domain user(s) and 1 Local administrator user(s)	Critical
Sniffing	Sniffed 44 credentials and performed 81 relay attacks	High
Password Strength	Cracked 29 out of 36 passwords: 5 strong, 1 easy and 23 trivial	High
Lateral Movement	Performed lateral movement to 2 Windows Server(s)	Medium
Accessible Data	Gained access to 2 Hosts (with complete access)	Critical
Host Takeover	Pentera was able to 'take over'[1] 2 out of 15 hosts (13%): 2 Windows Server(s)	Critical
AV/EDR Bypass	Bypassed AV/EDR and opened remote command sessions on 2 host(s)	Medium

112 Total Action Approvals

● 112 Approved (100%) ● 0 Not Approved (0%)

17767 Total Actions

● 14610 Successful (83%) 3157 No-results (17%)

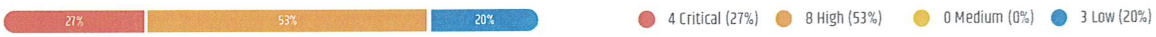
[1] Gain complete access to a host's hardware, software and files

Host Findings

17 Discovered Hosts

Pentera identified 17 live hosts across 2 device categories, 4 were affected by critical vulnerabilities

Vulnerability Severity Distribution

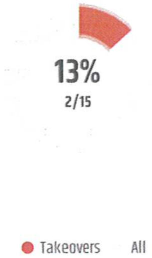


Windows Workstation	Windows Server	Windows	Linux	Mac Workstation	Network Devices	Other
0	14	0	3	0	0	0

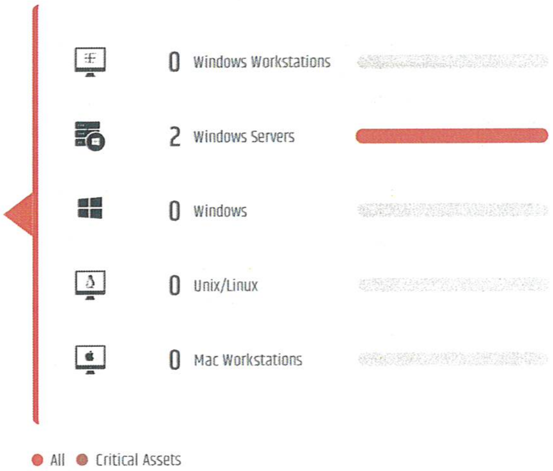
13% Host Takeover[1]

Out of 15 live hosts, Pentera took over 2 hosts

Takeover Percentage



Takeover Distribution



Live Hosts Table

(Listing 15 of 15 hosts).

Host	OS Version	Takeover	Details
SRV-XIGA-DB.gasmartcorp.local	Win2012R2 (D) Server	▲	Logged on user(s): User: kpimentel Domain/ Workgroup: GASMARTCORP.LOCAL
SRV-XIGA-APP.gasmartcorp.local	Win2008R2 (D) Server		Domain/Workgroup: GASMARTCORP.LOCAL
SRV-NAS.gasmartcorp.local	Win2012R2 (D) Server		Domain/Workgroup: GASMARTCORP.LOCAL
SRV-MOVIL.gasmartcorp.local	Win2019 (D) Server	▲	Logged on user(s): User: masteradmin Domain Workgroup: GASMARTCORP.LOCAL

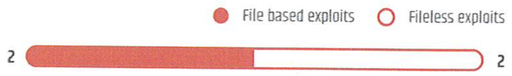
SRV-SAP-DB.gasmartcorp.local	Win2012R2 (D) Server	Domain/Workgroup: GASMARTCORP.LOCAL
SRV-SAP-APP.gasmartcorp.local	Win2012R2 (D) Server	Domain/Workgroup: GASMARTCORP.LOCAL
SRV-TRESSN-DB.gasmartcorp.local	Win2012R2 (D) Server	Domain/Workgroup: GASMARTCORP.LOCAL
SRV-TRESSN-APP.gasmartcorp.local	Win2012R2 (D) Server	Domain/Workgroup: GASMARTCORP.LOCAL
SRV-SERVICIOS.gasmartcorp.local	Win2019 (D) Server	Domain/Workgroup: GASMARTCORP.LOCAL
SRV-NWEB.gasmartcorp.local	Win2012R2 (D) Server	Domain/Workgroup: GASMARTCORP.LOCAL
SRV-XIGA-APP-QA.gasmartcorp.local	Win2012R2 (D) Server	Domain/Workgroup: GASMARTCORP.LOCAL
SRV-XIGA-DB-QA.gasmartcorp.local	Win2012R2 (D) Server	Domain/Workgroup: GASMARTCORP.LOCAL
SRV-XIGA-DB-DEV.gasmartcorp.local	Win2012R2 (D) Server	Domain/Workgroup: GASMARTCORP.LOCAL
SRV-XIGA-APP-DEV.gasmartcorp.local	Win2012R2 (D) Server	Domain/Workgroup: GASMARTCORP.LOCAL
SRV-AD-01.gasmartcorp.local	Win2012R2 (D) Server	Domain/Workgroup: GASMARTCORP.LOCAL
SRV-PCCOUNTER.gasmartcorp.local	Win2012R2 (D) Server	Domain/Workgroup: GASMARTCORP.LOCAL
10.255.243.3 00:09:0F:09:00:02 Fortinet	Linux	

4 Antivirus/EDR Bypass Events

Bypassed 1 AV/EDR vendors and opened remote command session on 2 hosts

Bypass Events Distribution Per Vendor

4 Unknown / No AV/EDR Installed

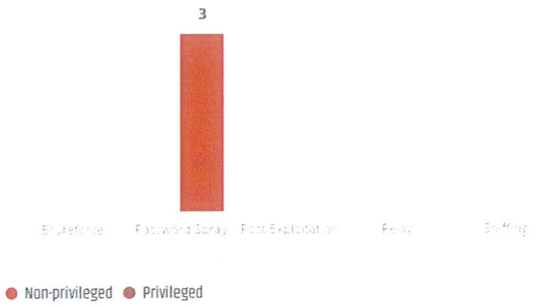


Credentials & Passwords

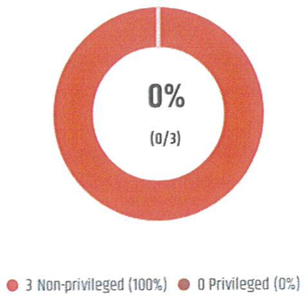
3 Compromised Accounts[1]

Pentera 'obtained access' to 3 accounts out of 3 using 1 techniques

Obtaining Techniques



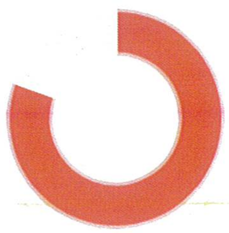
Privileged Account Distribution



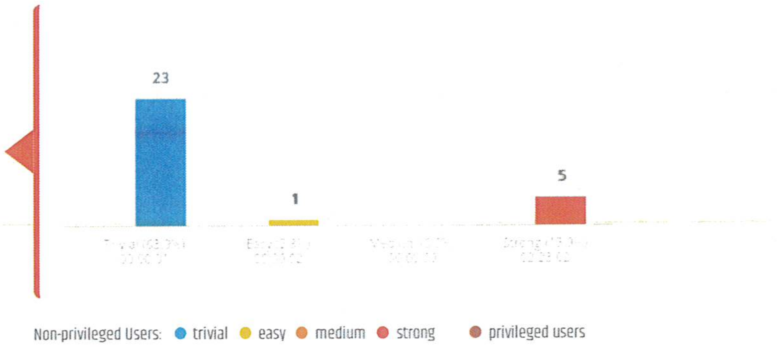
29 Passwords Cracked

50% of your passwords were cracked in under 30 minutes, a total of 29 accounts were cracked by Pentera in 20 hours.

Cracking Success Rate



Cracking Difficulty



Compromised Accounts Table

(Listing 3 of 3 items).

Username	Account Type	Privileged	Compromised By	Cleartext Password Obtained	Host / Domain Name
masteradmin	Local User Account	No	Password spraying	No	10.255.239.14
masteradmin	Local User Account	No	Password spraying	No	10.255.248.14
vortiz	Domain User Account	No	Password spraying	Yes	GASMARTCORP

Detailed Report

173 Vulnerabilities

66	27	34	46
Critical	High	Medium	Low

Pentera identified a total of 173 vulnerability occurrences across 4 severity levels

Listing 18 of 18 items.

SMB message signing is disabled

#1 Remediation Priority [1]

1.0 Severity

11 occurrences

An attacker could abuse the unsigned SMB servers to relay NTLM challenges from other hosts and gain shell access.

10.255.248.4
10.255.248.75
10.255.248.76
10.255.248.5
10.255.248.110
10.255.248.14
10.255.248.111
10.255.248.52
10.255.248.22
10.255.239.9
10.255.248.108

SMB server on endpoint does not validate clients

#2 Remediation Priority [1]

5.8 Severity

1 occurrences

GASMARTCORP.LOCAL

Host can be forced to authenticate by a rogue server

#3 Remediation Priority [1]

4.7 Severity

19 occurrences

In cases where the DNS server fails in name resolution queries, the LLMNR, NetBIOS-NS and mDNS services attempt to resolve them. Since those are a broadcast protocols, anyone can respond to the query. An attacker may refer the request to a machine in his control using a man-in-the-middle attack, And obtain sensitive data such as username and password hash.

MSSQLSERVER
GASMARTCORP.LOCAL
QOPAITXHWBGXZNO
FTPSERVER
workgroup

BlueKeep (CVE-2019-0708)

#4 Remediation Priority [1]

9.8 Severity

1 occurrences

An attacker might look for vulnerable operating systems in the organizational network. By exploiting this vulnerability the attacker could crash the target (Denial of Service) or get a high privileged shell (with SYSTEM access) on a host with no need for authentication at all, getting the attacker a foothold in the organization's network.

10.255.248.52

[1] Remediation priority recommendations factor in the number of hosts affected by a vulnerability, the number and severity of achievements caused by it, and whether the vulnerability provided access to your Critical Assets as configured in Pentera.

#5 Remediation Priority [1]

5.5 Severity

EPP/EDR allowed writing malicious payload to disk

22 occurrences

An attacker may write a malware to disk for persistence on compromised hosts. A malware written to disk is one step before successful malware infection. Such a malware can perform various actions desired by the attacker, such as information collection, file encryption, or backdoor communication.

10.255.248.14 10.255.248.110

#6 Remediation Priority [1]

8.8 Severity

AV did not block malicious payload

38 occurrences

An attacker may inject a malware in order to run commands and control the host in various ways. An updated and fully capable AV/EDR security layout is required to ensure the safety of the network.

10.255.248.14 10.255.248.110

#7 Remediation Priority [1]

8.3 Severity

Cleartext credentials stored in the memory

1 occurrences

After a user logs on, a variety of credentials are generated and stored in the Local Security Authority Subsystem Service (LSASS) process in memory. An attacker with administrative access to a host can extract clear text credentials from the host's memory and proceed his attack into the organizational network. With these credentials he could possibly access different services and assets in the domain and steal or manipulate sensitive information.

10.255.248.110

#8 Remediation Priority [1]

8.1 Severity

NTLM hashed credentials stored in the memory

1 occurrences

After a user logs on, a variety of credentials are generated and stored in the Local Security Authority Subsystem Service (LSASS) process in memory. This is meant to facilitate single sign-on (SSO), ensuring a user isn't prompted to input credentials each time resource access is requested. The credential data may include Kerberos tickets, NTLM password hashes, LM password hashes, and even clear-text passwords (WDigest and SSP authentication protocols). An attacker with administrative access to a host can extract NTLM hashed credentials from the memory and use them to connect to hosts using an attacked called pass-the-hash, and possibly take-over those hosts.

10.255.248.2

[1] Remediation priority recommendations factor in the number of hosts affected by a vulnerability, the number and severity of achievements caused by it, and whether the vulnerability provided access to your Critical Assets, as configured in Pentera.

#9 Remediation Priority [1]

7.9 Severity

Password can easily be cracked

22 occurrences

Many password cracking tools rely on dictionary rulesets, so it is important to avoid common passwords (such as Aa123456 or P@ssw0rd) and regular, unmodified dictionary terms. Inserting intentional, idiosyncratic misspellings or using acronyms is the recommended best practice. You can enhance Pentera's cracking abilities by uploading a custom wordlist to Pentera's Custom Dictionary and retest to uncover passwords that could be predicted or guessed by attackers who invest in social engineering techniques and are familiar with their targets.

```
administrator                          esepulveda                             soledad
admin                                  andres                                 2
javiera                                m                                      ignacia
moportus                               user                                   cuentas
administrador                          pls                                    invitado
usuario                                kassandra                              monica
de
```

#10 Remediation Priority [1]

8.6 Severity

Using empty password(s)

1 occurrences

Succeeded in cracking the password using an empty password

```
guest
```

#11 Remediation Priority [1]

8.8 Severity

KDC Bamboozling (CVE-2021-42287)

2 occurrences

The CVE-2021-42287 refers to Active Directory Domain Services Elevation of Privilege Vulnerability. By exploiting this vulnerability the attacker can obtain a service ticket for any user on the domain including domain admins.

```
10.255.248.2                           GASMARTCORP.LOCAL
```

#12 Remediation Priority [1]

6.9 Severity

Password can be cracked using low GPU effort

1 occurrences

Many password cracking tools rely on dictionary rulesets, so it is important to avoid common passwords (such as Aa123456 or P@ssw0rd) and regular, unmodified dictionary terms. Inserting intentional, idiosyncratic misspellings or using acronyms is the recommended best practice. You can enhance Pentera's cracking abilities by uploading a custom wordlist to Pentera's Custom Dictionary and retest to uncover passwords that could be predicted or guessed by attackers who invest in social engineering techniques and are familiar with their targets.

```
vortiz
```

[1] Remediation priority recommendations factor in the number of hosts affected by a vulnerability, the number and severity of achievements caused by it, and whether the vulnerability provided access to your Critical Assets, as configured in Pentera

#13 Remediation Priority [1]

4.9 Severity

Password can be cracked using high GPU effort

5 occurrences

Many password cracking tools rely on dictionary rulesets, so it is important to avoid common passwords (such as Aa123456 or P@ssw0rd) and regular, unmodified dictionary terms. Inserting intentional, idiosyncratic misspellings or using acronyms is the recommended best practice. You can enhance Pentera's cracking abilities by uploading a custom wordlist to Pentera's Custom Dictionary and retest to uncover passwords that could be predicted or guessed by attackers who invest in social engineering techniques and are familiar with their targets.

```
areyes
ahuerta
kpimentel
gmunoz
miguel.pacheco
```

#14 Remediation Priority [1]

5.3 Severity

The web application has a directory listing which is inappropriately exposed, yielding potentially sensitive information to attackers.

3 occurrences

The web application has a directory listing which is inappropriately exposed, disclosing potentially sensitive information to attackers. The specific risks and consequences vary depending on which files are listed and accessible.

```
10.255.248.52
```

#15 Remediation Priority [1]

2.3 Severity

Discovered closed ports on the host

14 occurrences

Discovered closed port on the host (reachable without firewalling).

```
10.255.248.4
10.255.248.75
10.255.248.76
10.255.248.5
10.255.248.110
10.255.248.14
10.255.248.111
10.255.248.52
10.255.248.22
10.255.239.9
10.255.248.108
```

#16 Remediation Priority [1]

3.3 Severity

Host uses NTLMv1 authentication

10 occurrences

An attacker might grab the NTLMv1 hash and crack it easily, NTLMv2 is more complex to crack.

```
10.255.248.4
10.255.248.75
10.255.248.76
10.255.248.5
10.255.248.110
10.255.248.14
10.255.248.111
10.255.248.52
10.255.248.22
10.255.239.9
10.255.248.108
```

[1] Remediation priority recommendations factor in the number of hosts affected by a vulnerability, the number and severity of achievements caused by it, and whether the vulnerability provided access to your Critical Assets as configured in Pentera.

#17

Remediation Priority [1]

0.0

Severity

Host supports SMBv1 protocol

10 occurrences

An attacker might abuse many security flaws in the protocol to take over the host. Microsoft has advised to completely stop the use of Server Message Block 1.0.

```
10.255.248.4
10.255.248.75
10.255.248.76
10.255.248.5
10.255.248.110
10.255.248.14
10.255.248.111
10.255.248.52
10.255.248.22
10.255.239.9
10.255.248.108
```

#18

Remediation Priority [1]

2.0

Severity

Printer Spooler service is available

11 occurrences

An attacker may use valid credentials in order to authenticate to the target machine Printer Spooler service, and attempt to initiate a reverse-authentication from the targeted machine account back to the attacker machine.

```
10.255.248.4
10.255.248.75
10.255.248.76
10.255.248.5
10.255.248.110
10.255.248.14
10.255.248.111
10.255.248.52
10.255.248.22
10.255.239.9
10.255.248.108
```

[1] Remediation priority recommendations factor in the number of hosts affected by a vulnerability, the number and severity of achievements caused by it, and whether the vulnerability provided access to your Critical Assets as configured in Pentera.

497 Achievements

45	245	106	101
Critical	High	Medium	Low

Pentera accomplished 497 achievements in total. Every achievement represents a discrete successful action performed by Pentera.

(Listing 35 of 35 items)

Severity	Details
10 Severity	**(1) Completed ransomware attack kill chain on the host** Pentera was able to execute an end-to-end attack of the selected ransomware family without being blocked.
9.4 Severity	**(2) Gathered valuable information from host** An attacker might find sensitive information and credentials on the host that might help in further attacks
9.2 Severity	**(1) Encrypted files on the host** Attackers may encrypt files, data, cloud storage objects, and online backups on local and remote drives to disrupt operations and interrupt system availability. In ransomware attacks, a unique decryption key is offered in exchange for a ransom payment.
9.1 Severity	**(1) Opened a remote access session on the host** An attacker can remotely execute arbitrary code on a host in the network, might steal or manipulate sensitive data, cause a denial of service and possibly extend his attack over the network.
9.0 Severity	**(10) Validated domain credentials** An attacker may abuse the domain credentials to login to hosts and gather information about the users and possibly take-over the host and escalate his attack.
8.0 Severity	**(23) Cracked user hash using CPU** An attacker might capture user password hashes during his attack, then try and crack them using various hash cracking tools. The purpose will be to gather as many user credentials as possible to escalate his attack, take-over hosts in the network and possibly learn the password policy of the organization.
7.9 Severity	**(1) Emulated deletion of shadow copies** Adversaries may turn off system recovery services or delete volume shadow copies to compound the effects of data encrypted for impact.
7.5 Severity	**(6) Cracked user hash using GPU** An attacker might capture user password hashes during his attack, then try and crack them using various hash cracking tools. The purpose will be to gather as many user credentials as possible to escalate his attack, take-over hosts in the network and possibly learn the password policy of the organization.
7.2 Severity	**(1) Enumerated files on the host** Attackers may enumerate files and directories on hosts, local system sources, or network shares to find files of interest and sensitive data to exfiltrate. File and directory discovery can be performed in an automated manner or using a command and scripting Interpreter, such as cmd.
7.2 Severity	**(82) Executed code remotely on the host**
7.1 Severity	**(10) Found a user with privileged RCE capabilities** An attacker might use gathered credentials from breached hosts to move laterally across the network.

Severity	Details
5.8 Severity	**(1) Grabbed screen capture from remote host** Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations.
5.7 Severity	**(1) Injected .NET assembly to remote process** Adversaries may inject their payloads to remote processes to gain stealthiness.
5.5 Severity	**(1) Captured credentials over MSSQL**
5.5 Severity	**(2) Captured credentials over FTP**
5.5 Severity	**(8) Captured credentials over HTTP** An attacker may steal credentials by sniffing unencrypted HTTP traffic and use them to access hosts or services in the network, which may lead to sensitive data theft or manipulation, and possibly to a complete take-over of the hosts or services.
5.5 Severity	**(52) Captured credentials over SMB** An attacker may steal credentials by impersonating hosts and tricking users to authenticate with him over SMB, and use them in order to access hosts or services in the network, which may lead to sensitive data theft or manipulation and possibly to a complete take-over of the hosts or services.
5.4 Severity	**(81) Performed a relay attack over SMB** An attacker may abuse the Relay attack vector to authenticate to another host without obtaining the cleartext credentials.
5.3 Severity	**(3) Discovered directory listing** An attacker can use an exposed directory listing to obtain the complete index of all the resources located inside the directory.
5.1 Severity	**(2) Executed remote WMI query** The WMI remote interface allows querying many aspects of the operating system.
5.0 Severity	**(1) Found access point to another broadcast domain** An attacker might use this host to proceed the attack towards another network.
3.5 Severity	**(1) Validated local credentials** An attacker may abuse the local credentials to login to hosts and gather information about the users and possibly take-over the host and escalate his attack.
3.4 Severity	**(18) Uploaded malware to host via LOLBAS** An attacker can execute arbitrary malicious code on a host to extract sensitive data, manipulate the system, or use it to further advance the attack.
3.4 Severity	**(4) Uploaded malware to host** An attacker can execute arbitrary malicious code on a host to extract sensitive data, manipulate the system, or use it to further advance the attack.

Severity	Details
3.3 Severity	**(82) Opened remote control channel on the host**
3.0 Severity	**(1) Infiltrated .SCF file** An attacker may create a malicious file on a remote share or host which will cause other users viewing it to authenticate with him over SMB so he can steal their credentials.
2.0 Severity	**(12) Accessed shares using domain credentials** An attacker with valid domain credentials may access shared folders and steal sensitive information from them.
2.0 Severity	**(11) Authenticated with machine's printer service using validated credentials** An attacker may use valid credentials in order to authenticate to the target machine Printer Spooler service, and attempt to initiate a reverse-authentication from the targeted machine account back to the attacker machine.
1.2 Severity	**(34) Payload established connection with Pentera's C2 server** An attacker may establish a connection to a remote malicious payload on a victim's machine in order to control the payload remotely. This allows an attacker to receive information from the payload and instruct it with additional commands. The connection method could be either Bind (the attacker connects to the remote payload) or Reverse (the remote payload connects to the attacker).
1.1 Severity	**(1) Created mutex object on the host** Programs use mutex (mutual exclusion) objects as a locking mechanism to serialize access to a resource on the system. Malware might use a mutex to avoid reinfecting the host or coordinate multithreaded activity. Malware might dynamically generate mutex names in an attempt to evade detection.
1.0 Severity	**(1) Generated Encryption key** Adversaries may generate a random key for encrypting files.
1.0 Severity	**(30) Enumerated web services anonymously** An attacker may enumerate exposed web services and look for confidential data, vulnerable inputs or crack web authentication pages.
1.0 Severity	**(9) IIS Windows Server Default Page**
1.0 Severity	**(2) IIS-7 Default Page**
0.0 Severity	**(1) Found credentials for out of range host(s)** An attacker may steal credentials and use them to login into other hosts, which may lead to sensitive data theft or manipulation and possibly to a complete take-over of the hosts.

MITRE ATT&CK Matrix for Enterprise - Heat Map (1 of 2)

MITRE | ATT&CK

Total Patterns

22753

Most Common Technique

Discovery / File and Directory Discovery

Reconnaissance

- Active Scanning T1595 ^ 🟥
  - Scanning IP Blocks T1595.001 🟦
  - Vulnerability Scanning T1595.002 🟥
- Gather Victim Network Information T1590 ^ 🟦
  - DNS T1590.002 🟦
- Network Service Discovery T1046 🟦

Initial Access

- Exploit Public-Facing Application T1190 🟦
- Valid Accounts T1078 🟧

Execution

- Exploitation for Client Execution T1203 🟦
- System Services T1569 ^ 🟥
  - Service Execution T1569.002 🟥
- Windows Management Instrumentation T1047 🟧
- System Binary Proxy Execution T1218 ^ 🟦
  - Rundll32 T1218.011 🟦
- Native API T1106 🟦
- Command and Scripting Interpreter T1059 ^ 🟥
  - PowerShell T1059.001 🟥
- Screen Capture T1113 🟥

Persistence

Privilege Escalation

- Access Token Manipulation T1134 ^ 🟦
  - Make and Impersonate Token T1134.003 🟦
- Create or Modify System Process T1543 ^ 🟥
  - Windows Service T1543.003 🟥

Defense Evasion

- Indicator Removal T1070 ^ 🟥
  - File Deletion T1070.004 🟦
- Process Injection T1055 ^ 🟥
  - Asynchronous Procedure Call T1055.004 🟦
  - Portable Executable Injection T1055.002 🟥
- Trusted Developer Utilities Proxy Execution T1127 ^ 🟥
  - MSBuild T1127.001 🟥
- System Binary Proxy Execution T1218 🟥
- Software Deployment Tools T1072 🟦
- Obfuscated Files or Information T1027 ^ 🟦
  - Indicator Removal from

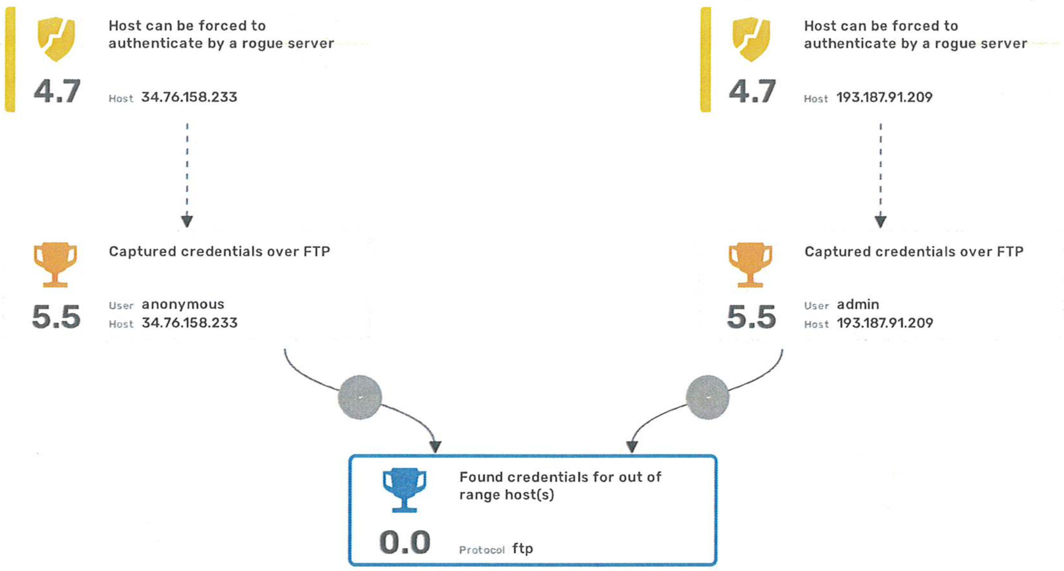
MITRE ATT&CK Matrix for Enterprise - Heat Map (2 of 2)

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Network Sniffing T1040 🟧	Remote System Discovery T1018 🟦	Exploitation of Remote Services T1210 🟧	Data from Local System T1005 🟥	Ingress Tool Transfer T1105 🟥	Exfiltration Over Alternative... T1048 ^ 🟥	Resource Hijacking T1496 🟦
Steal Web Session Cookie T1539 🟦	System Information Discovery T1082 🟦	Remote Services T1021 ^ 🟧	Data from Network Shared Drive T1039 🟦	Application Layer Protocol T1071 ^ 🟥	Exfiltration Over Unencrypted Non... T1048.003 🟥	Service Stop T1489 🟦
Brute Force T1110 ^ 🟥	Network Service Discovery T1046 🟥	Remote Desktop Protocol T1021.001 🟦	Screen Capture T1113 🟦	Web Protocols T1071.001 🟥		System Shutdown/Reboot T1529 🟦
Password Guessing T1110.001 🟥	Network Sniffing T1040 🟧	SMB/Windows Admin Shares T1021.002 🟨	Remote Services T1021 ^ 🟦	File Transfer Protocols T1071.002 🟥		Inhibit System Recovery T1490 🟥
Adversary-in-the-Middle T1557 ^ 🟥	Network Share Discovery T1135 🟦	Distributed Component Objec... T1021.003 🟧	Remote Desktop Protocol T1021.001 🟦	Non-Application Layer Protocol T1095 🟥		Data Encrypted for Impact T1486 🟥
LLMNR/NBT-NS Poisoning and SM... T1557.001 🟥	Cloud Service Discovery T1526 🟦	Taint Shared Content T1080 🟨		Proxy T1090 ^ 🟦		
Forced Authentication T1187 🟨	File and Directory Discovery T1083 🟧	Use Alternate Authentication... T1550 ^ 🟦		Internal Proxy T1090.001 🟦		
OS Credential Dumping T1003 ⌄ 🟥	System Owner/User Discovery T1033 🟦	Pass the Hash T1550.002 🟦				
Credentials from Password Stores T1555 ^ 🟥	Permission Groups Discovery T1069 ⌄ 🟦					
Credentials from Web Browsers T1555.003 🟥	Gather Victim Identity Information T1589 ⌄ 🟦					
Unsecured Credentials T1552 ⌄ 🟥	Software Discovery T1518 ⌄ 🟦					
Steal or Forge Kerberos Tickets T1558 🟥	Query Registry T1012 🟦					

Appendix

Select Attack Vector(s)

0.0 Found credentials for out of range host(s)



Host can be forced to authenticate by a rogue server
4.7
Host 34.76.158.233

Host can be forced to authenticate by a rogue server
4.7
Host 193.187.91.209

Captured credentials over FTP
5.5
User anonymous
Host 34.76.158.233

Captured credentials over FTP
5.5
User admin
Host 193.187.91.209

Found credentials for out of range host(s)
0.0
Protocol ftp

Summary

Found 2 ftp passwords

Parameters

Protocol: ftp **Host:** 193.187.91.209, User **Host:** 34.76.158.233, User

Details

Time: May 24, 2025 13:22

Insight

An attacker may steal credentials and use them to login into other hosts, which may lead to sensitive data theft or manipulation and possibly to a complete take-over of the hosts.

1.0 Enumerated web services anonymously

Summary

Found 1 page(s) of the web service,Generated 1 screen shot(s),Found 1 comment(s) in HTML source,Found Web Server information

Parameters

Host: 10.255.248.22 **Port:** 443

Details

Time: May 23, 2025 23:48
MITRE Technique(s): Network Service Discovery (T1046) ,File and Directory Discovery (T1083)

Insight

An attacker may enumerate exposed web services and look for confidential data, vulnerable inputs or crack web authentication pages.

1.0 IIS Windows Server Default Page

Parameters

Host: https **Vulnerable URL:** https **Curl Command:** curl -X 'GET' -d '' -H 'Accept

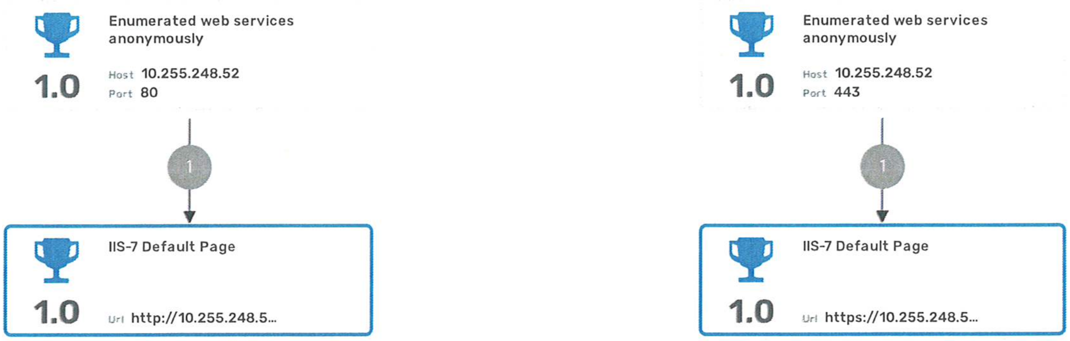
Details

Time: May 23, 2025 23:57

MITRE Technique(s): Network Service Discovery (T1046)

*Use Pentera web interface to view all items

1.0 IIS-7 Default Page


Enumerated web services anonymously
1.0
Host 10.255.248.52
Port 80
1
IIS-7 Default Page
1.0
Url http://10.255.248.5...
Enumerated web services anonymously
1.0
Host 10.255.248.52
Port 443
1
IIS-7 Default Page
1.0
Url https://10.255.248.5...

Parameters

Host: http **Vulnerable URL:** http **Curl Command:** curl -X 'GET' -d '' -H 'Accept

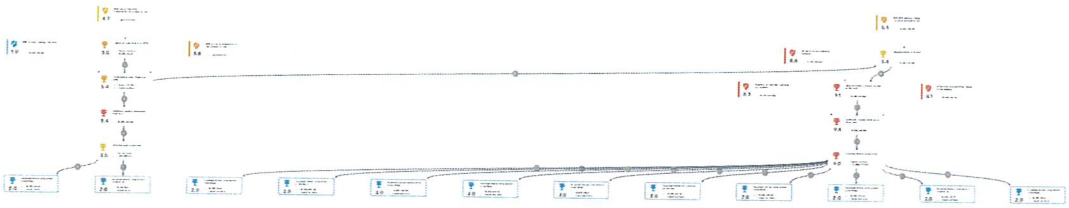
Details

Time: May 24, 2025 00:03

MITRE Technique(s): Network Service Discovery (T1046)

*Use Pentera web interface to view all items

2.0 Accessed shares using domain credentials



Summary

(Summary excludes IPC$ results),User masteradmin has 4 readWrite access shares)

Parameters

Host: 10.255.248.14 **User name:** masteradmin **User ntlm hash:** ****

Details

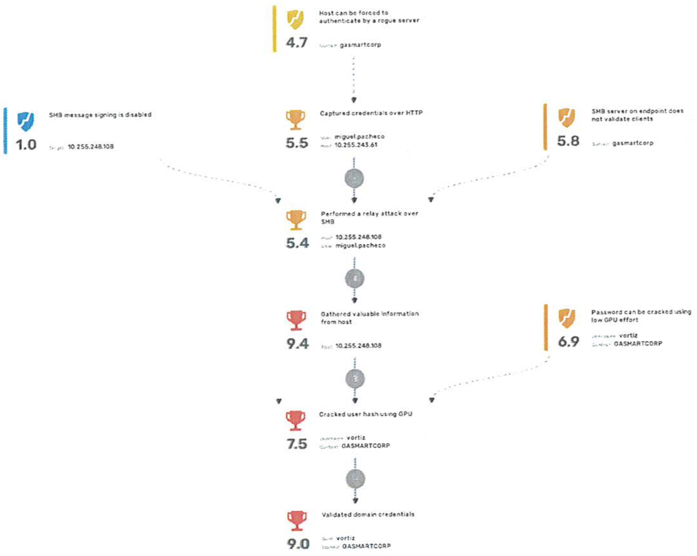
Time: May 24, 2025 10:52
Domain: GASMARTCORP.LOCAL
IPv4: 10.255.248.14
OS: Win2019 (D)
MITRE Technique(s): Network Share Discovery (T1135)

Insight

An attacker with valid domain credentials may access shared folders and steal sensitive information from them.

*Use Pentera web interface to view all items

2.0 Authenticated with machine's printer service using validated credentials


Host can be forced to authenticate by a rogue server
4.7
gasmartcorp
SMB message signing is disabled
1.0
10.255.248.108
Captured credentials over HTTP
5.5
miguel.pacheco
10.255.243.61
SMB server on endpoint does not validate clients
5.8
gasmartcorp
Performed a relay attack over SMB
5.4
10.255.248.108
miguel.pacheco
Gathered valuable information from host
9.4
10.255.248.108
Password can be cracked using low GPU effort
6.9
vortiz
GASMARTCORP
Cracked user hash using GPU
7.5
vortiz
GASMARTCORP
Validated domain credentials
9.0
vortiz
GASMARTCORP

Parameters

User: vortiz **Password:** **** **Domain:** gasmartcorp

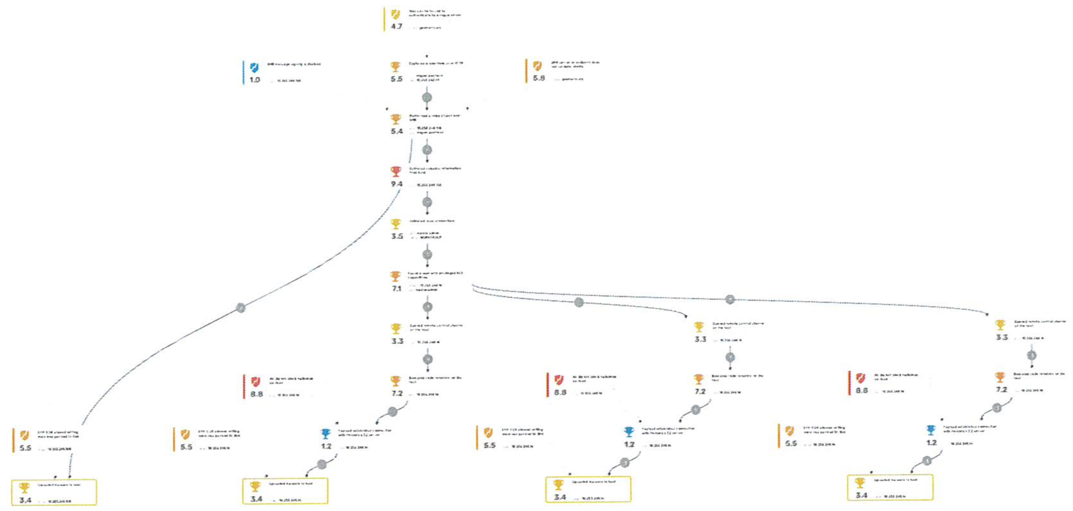
Details

Time: May 24, 2025 12:18
Domain: GASMARTCORP.LOCAL
IPv4: 10.255.248.108
OS: Win2012R2 (D)
MITRE Technique(s): Forced Authentication (T1187)

Insight

An attacker may use valid credentials in order to authenticate to the target machine Printer Spooler service, and attempt to initiate a reverse-authentication from the targeted machine account back to the attacker machine.

3.4 Uploaded malware to host



Parameters

Host: 10.255.248.110 **User:** GASMARTCORP\miguel.pacheco

Details

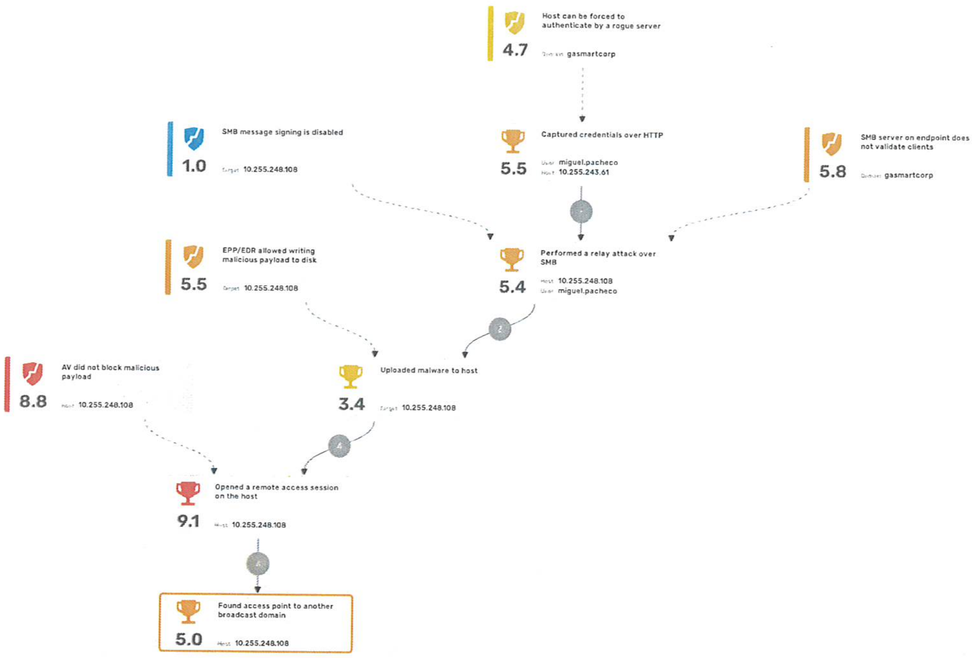
Time: May 24, 2025 10:51
Domain: GASMARTCORP.LOCAL
IPv4: 10.255.248.110
OS: Win2012R2 (D)
MITRE Technique(s): Ingress Tool Transfer (T1105) ,System Services (T1569) ,Service Execution (T1569.002)

Insight

An attacker can execute arbitrary malicious code on a host to extract sensitive data, manipulate the system, or use it to further advance the attack.

*Use Pentera web interface to view all items

5.0 Found access point to another broadcast domain


Host can be forced to authenticate by a rogue server
4.7
Domain gasmartcorp
SMB message signing is disabled
1.0
Target 10.255.248.108
Captured credentials over HTTP
5.5
User miguel.pacheco
Host 10.255.243.61
SMB server on endpoint does not validate clients
5.8
Domain gasmartcorp
EPP/EDR allowed writing malicious payload to disk
5.5
Target 10.255.248.108
Performed a relay attack over SMB
5.4
Host 10.255.248.108
User miguel.pacheco
2
AV did not block malicious payload
8.8
Host 10.255.248.108
Uploaded malware to host
3.4
Target 10.255.248.108
4
Opened a remote access session on the host
9.1
Host 10.255.248.108
Found access point to another broadcast domain
5.0
Host 10.255.248.108

Parameters

Host: 10.255.248.110

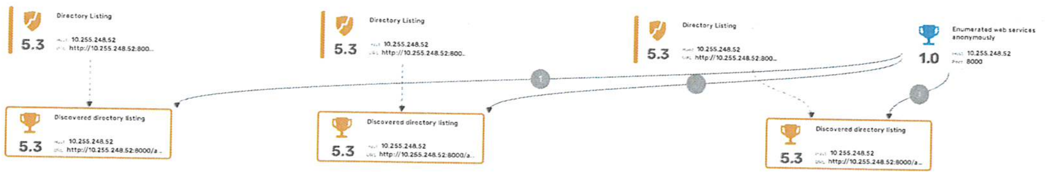
Details

Time: May 24, 2025 10:52
Domain: GASMARTCORP.LOCAL
IPv4: 10.255.248.110
OS: Win2012R2 (D)
MITRE Technique(s): Credentials from Password Stores (T1555) ,Credentials from Web Browsers (T1555.003) ,Unsecured Credentials (T1552) ,Credentials In Files (T1552.001) ,Credentials in Registry (T1552.002)

Insight

An attacker might use this host to proceed the attack towards another network.

5.3 Discovered directory listing


Directory Listing
5.3
10.255.248.52
http://10.255.248.52:800...
Directory Listing
5.3
10.255.248.52
http://10.255.248.52:800...
Directory Listing
5.3
10.255.248.52
http://10.255.248.52:800...
Enumerated web services anonymously
1.0
10.255.248.52
8000
Discovered directory listing
5.3
10.255.248.52
http://10.255.248.52:8000/a...
Discovered directory listing
5.3
10.255.248.52
http://10.255.248.52:8000/a...
Discovered directory listing
5.3
10.255.248.52
http://10.255.248.52:8000/a...

Parameters

Host: 10.255.248.2 **Port:** 8000 **URL:** http

Details

Time: May 24, 2025 00:15
MITRE Technique(s): Exploitation of Remote Services (T1210) ,Active Scanning (T1595) ,Vulnerability Scanning (T1595.002)
CWE: CWE-548
OWASP: A01:2021 - Broken Access Control

Insight

An attacker can use an exposed directory listing to obtain the complete index of all the resources located inside the directory.

5.5 Captured credentials over MSSQL

Parameters

Host: 189.132.86.136

Details

Time: May 24, 2025 06:37

Results

User: sa

Type of Creds: Cleartext

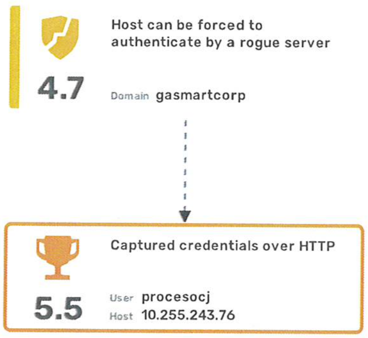
Credentials: ****

User: sa

Type of Creds: Cleartext

!Use Pentera web interface to view all items

5.5 Captured credentials over HTTP


4.7
Host can be forced to authenticate by a rogue server
Domain gasmartcorp
5.5
Captured credentials over HTTP
User procesocj
Host 10.255.243.76

Parameters

Domain: gasmartcorp

Details

Time: May 24, 2025 01:43

Insight

An attacker may steal credentials by sniffing unencrypted HTTP traffic and use them to access hosts or services in the network, which may lead to sensitive data theft or manipulation, and possibly to a complete take-over of the hosts or services.

Results

Host: 10.255.243.47
User: procesocj
Type of Creds: ntlmv2
Context: Domain
Requested Path: wpad/wpad.dat

5.5 Captured credentials over SMB

Details

Time: May 24, 2025 02:19

Insight

An attacker may steal credentials by impersonating hosts and tricking users to authenticate with him over SMB, and use them in order to access hosts or services in the network, which may lead to sensitive data theft or manipulation and possibly to a complete take-over of the hosts or services.

Results

Host: 186.10.135.102
User: administrator
Type of Creds: ntlmv2
Context: Local
Credentials: ****

*Use Pentera web interface to view all items

5.5 Captured credentials over MSSQL

Parameters

Host: 189.132.86.136

Details

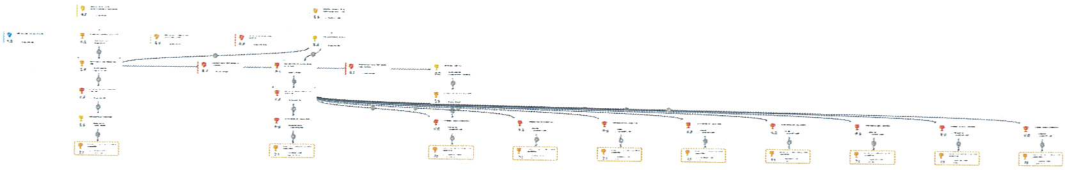
Time: May 24, 2025 06:
37

Results

User: sa
Type of Creds: Cleartext
Credentials: ****
User: sa
Type of Creds: Cleartext

*Use Pentera web interface to view all items

7.1 Found a user with privileged RCE capabilities



Summary

User has high privileges on 1 host

Parameters

Context: 10.255.248.14 **User:** masteradmin **ntlm:** ****

Details

Time: May 24, 2025 10:52
MITRE Technique(s): Windows Management Instrumentation (T1047) ,Valid Accounts (T1078)

Insight

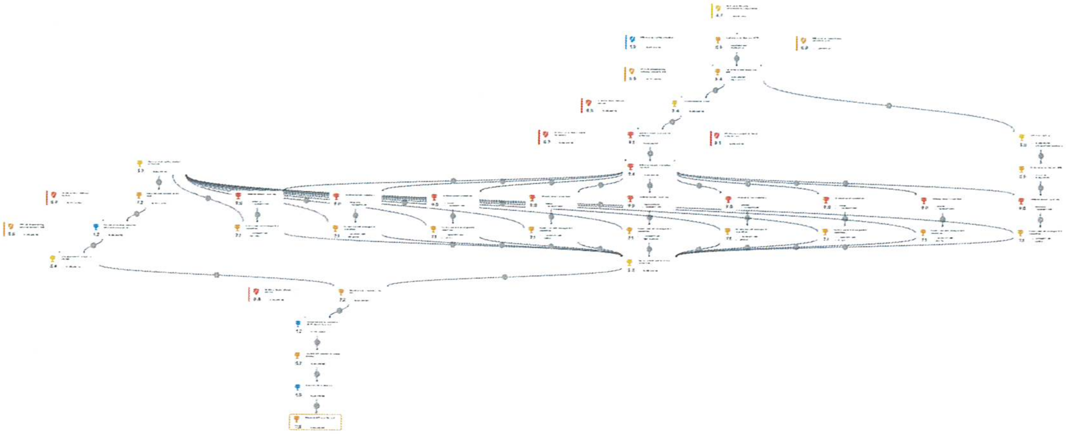
An attacker might use gathered credentials from breached hosts to move laterally across the network.

Results

Hosts:
10.255.248.14 (WMI)

*Use Pentera web interface to view all items

7.2 Enumerated files on the host



Parameters

Ransomware Family: Conti **Host:** 10.255.248.108 **Enumerated directory:** C

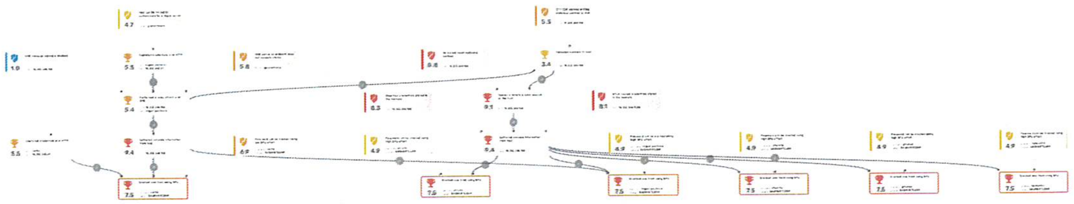
Details

Time: May 24, 2025 12:07
Domain: GASMARTCORP.LOCAL
IPv4: 10.255.248.108
OS: Win2012R2 (D)
MITRE Technique(s): File and Directory Discovery (T1083) ,Data from Local System (T1005)

Insight

Attackers may enumerate files and directories on hosts, local system sources, or network shares to find files of interest and sensitive data to exfiltrate. File and directory discovery can be performed in an automated manner or using a command and scripting Interpreter, such as cmd.

7.5 Cracked user hash using GPU



Parameters

Username: vortiz **Context:** GASMARTCORP **Hash:** ****

Details

Time: May 24, 2025 11:25
MITRE Technique(s): Brute Force (T1110) ,Password Guessing (T1110.001)

Insight

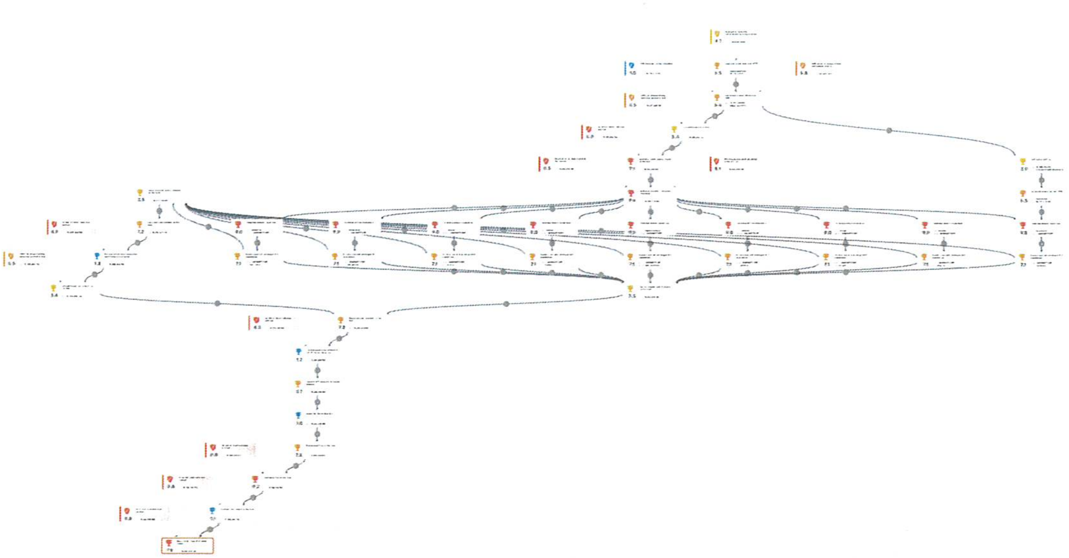
An attacker might capture user password hashes during his attack, then try and crack them using various hash cracking tools. The purpose will be to gather as many user credentials as possible to escalate his attack, take-over hosts in the network and possibly learn the password policy of the organization.

Results

Cracked password: ****
Hash type: NTLMv2
Cracking engine: GPU
Cracking duration: 00:00:02.239

¹Use Pentera web interface to view all items

7.9 Emulated deletion of shadow copies



Parameters

Ransomware Family: Conti **Host:** 10.255.248.108 **Command:** vssadmin.exe delete shadows /all /quiet /?

Details

Time: May 24, 2025 12:07
Domain: GASMARTCORP.LOCAL
IPv4: 10.255.248.108
OS: Win2012R2 (D)
MITRE Technique(s): Inhibit System Recovery (T1490) ,Data from Local System (T1005)

Insight

Adversaries may turn off system recovery services or delete volume shadow copies to compound the effects of data encrypted for impact.

¹Use Pentera web interface to view all items

8.0 Cracked user hash using CPU

Parameters

Username: administrator **Context:** 186.10.135.102 **Hash:** ****

Details

Time: May 24, 2025 02:19
MITRE Technique(s): Brute Force (T1110) ,Password Guessing (T1110.001)

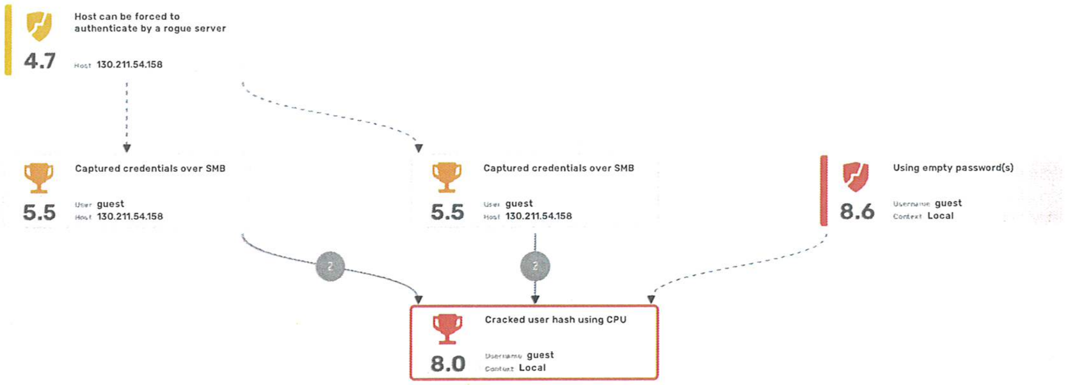
Insight

An attacker might capture user password hashes during his attack, then try and crack them using various hash cracking tools. The purpose will be to gather as many user credentials as possible to escalate his attack, take-over hosts in the network and possibly learn the password policy of the organization.

Results

Cracked password: ****
Hash type: NTLMv2
Cracking engine: CPU
Cracking duration: 00:00:01.649

8.0 Cracked user hash using CPU



Parameters

Username: guest **Context:** 130.211.54.158 **Hash:** ****

Details

Time: May 24, 2025 03:
07

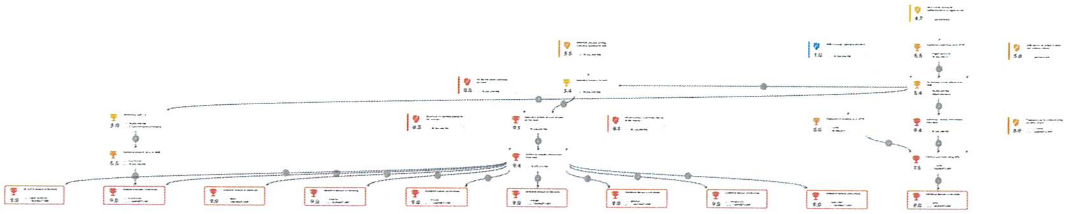
Insight

An attacker might capture user password hashes during his attack, then try and crack them using various hash cracking tools. The purpose will be to gather as many user credentials as possible to escalate his attack, take-over hosts in the network and possibly learn the password policy of the organization.

Results

Cracked password: ****
Hash type: NTLMv2
Cracking engine: CPU
Cracking duration: 00:00:00.743

9.0 Validated domain credentials



Parameters

User: miguel.pacheco **Domain:** GASMARTCORP **ntlm:** ****

Details

Time: May 24, 2025 10:55

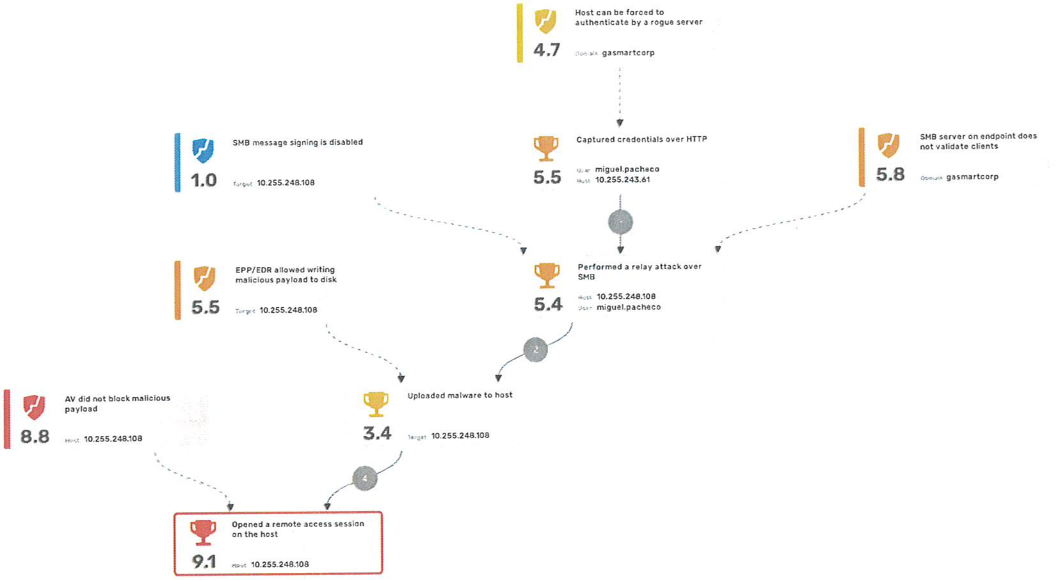
Insight

An attacker may abuse the domain credentials to login to hosts and gather information about the users and possibly take-over the host and escalate his attack.

Results

Host: 10.255.248.2
Protocol: Kerberos
Port: 88

9.1 Opened a remote access session on the host


Host can be forced to authenticate by a rogue server
4.7
Domain gasmartcorp
SMB message signing is disabled
1.0
Target 10.255.248.108
Captured credentials over HTTP
5.5
User miguel.pacheco
Host 10.255.243.61
SMB server on endpoint does not validate clients
5.8
Domain gasmartcorp
EPP/EDR allowed writing malicious payload to disk
5.5
Target 10.255.248.108
Performed a relay attack over SMB
5.4
Host 10.255.248.108
User miguel.pacheco
2
AV did not block malicious payload
8.8
Host 10.255.248.108
Uploaded malware to host
3.4
Target 10.255.248.108
4
Opened a remote access session on the host
9.1
Host 10.255.248.108

Parameters

Domain: GASMARTCORP **Host:** 10.255.248.108

Details

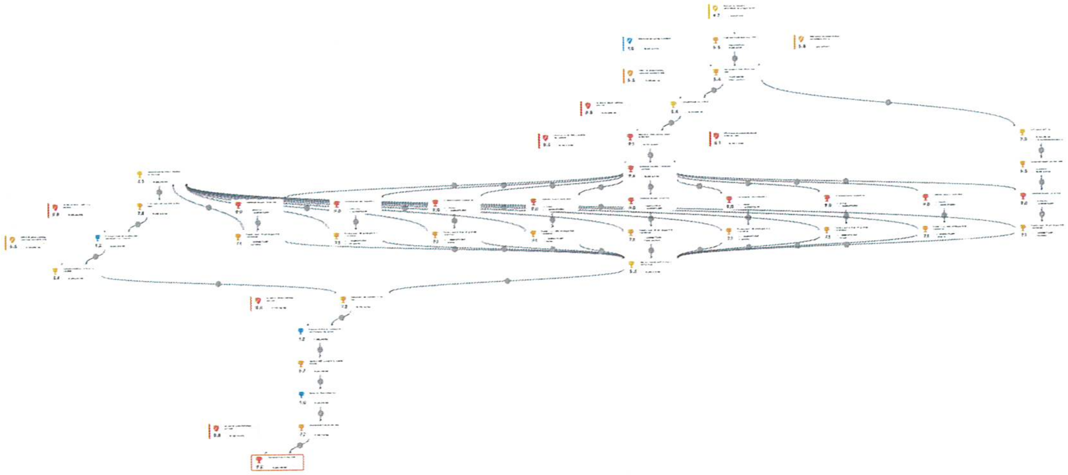
Time: May 24, 2025 10:52
Domain: GASMARTCORP.LOCAL
IPv4: 10.255.248.108
OS: Win2012R2 (D)
MITRE Technique(s): Credentials from Password Stores (T1555) ,Credentials from Web Browsers (T1555.003) ,Unsecured Credentials (T1552) ,Credentials In Files (T1552.001) ,Credentials in Registry (T1552.002)

Insight

An attacker can remotely execute arbitrary code on a host in the network, might steal or manipulate sensitive data, cause a denial of service and possibly extend his attack over the network.

*Use Pentera web interface to view all items

9.2 Encrypted files on the host



Parameters

Ransomware Family: Conti **Host:** 10.255.248.108 **Encryption Mode:** Fast **Encryption Algorithm:** Salsa20
Encrypted Directory: C

Details

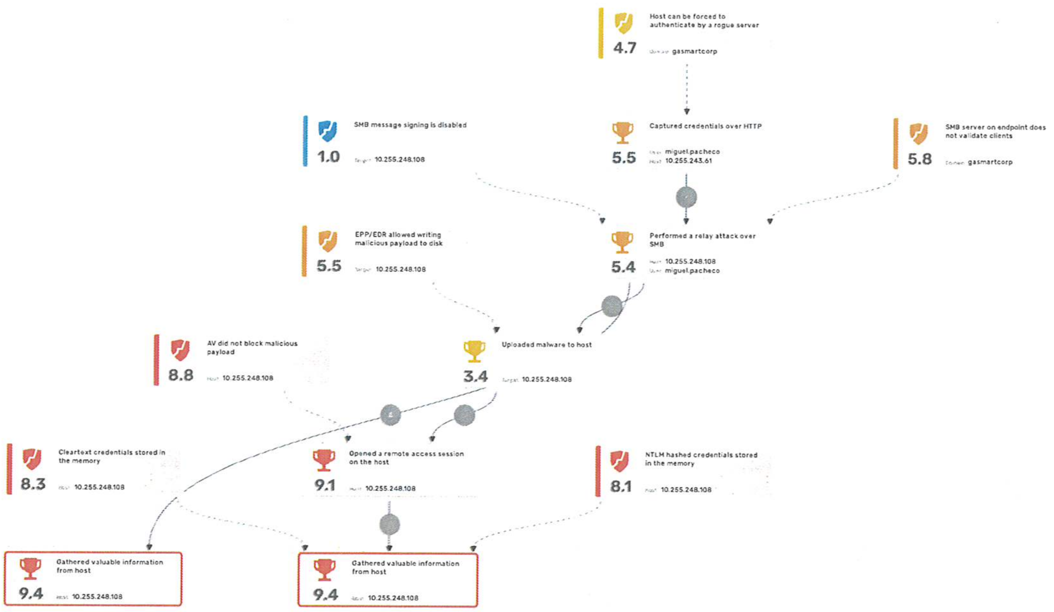
Time: May 24, 2025 12:07
Domain: GASMARTCORP.LOCAL
IPv4: 10.255.248.108
OS: Win2012R2 (D)
MITRE Technique(s): Data Encrypted for Impact (T1486)

Insight

Attackers may encrypt files, data, cloud storage objects, and online backups on local and remote drives to disrupt operations and interrupt system availability. In ransomware attacks, a unique decryption key is offered in exchange for a ransom payment.

[1]Use Pentera web interface to view all items

9.4 Gathered valuable information from host


4.7
Host can be forced to authenticate by a rogue server
Domain gasmartcorp
1.0
SMB message signing is disabled
Target 10.255.248.108
5.5
Captured credentials over HTTP
User miguel.pacheco
Host 10.255.243.61
5.8
SMB server on endpoint does not validate clients
Domain gasmartcorp
5.5
EPP/EDR allowed writing malicious payload to disk
Target 10.255.248.108
5.4
Performed a relay attack over SMB
Host 10.255.248.108
User miguel.pacheco
8.8
AV did not block malicious payload
Host 10.255.248.108
3.4
Uploaded malware to host
Target 10.255.248.108
8.3
Cleartext credentials stored in the memory
Host 10.255.248.108
9.1
Opened a remote access session on the host
Host 10.255.248.108
8.1
NTLM hashed credentials stored in the memory
Host 10.255.248.108
9.4
Gathered valuable information from host
Host 10.255.248.108
9.4
Gathered valuable information from host
Host 10.255.248.108

Summary

Extracted 105 browser credential(s)

Parameters

Domain: GASMARTCORP **User:** miguel.pacheco **Host:** 10.255.248.108

Details

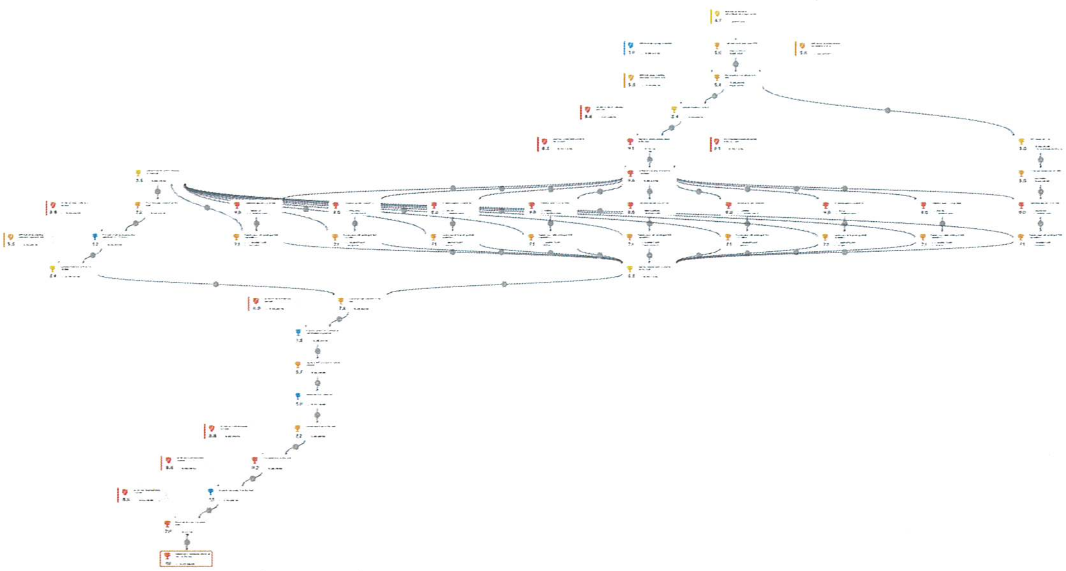
Time: May 24, 2025 10:51
Domain: GASMARTCORP.LOCAL
IPv4: 10.255.248.108
OS: Win2012R2 (D)

Insight

An attacker might find sensitive information and credentials on the host that might help in further attacks

*Use Pentera web interface to view all items

10 Completed ransomware attack kill chain on the host



Parameters

Ransomware Family: Conti

Host: 10.255.248.108

Details

Time: May 24, 2025 12:07
Domain: GASMARTCORP.LOCAL
IPv4: 10.255.248.108
OS: Win2012R2 (D)
MITRE Technique(s): Process Injection (T1055) ,Portable Executable Injection (T1055.002)

Insight

Pentera was able to execute an end-to-end attack of the selected ransomware family without being blocked.

*Use Pentera web interface to view all items

Testing Scenario Details

Group	Type	Details
Info	Name	Pentest Monedero XIGA
	Description	Penetration test de IPs de Monedero XIGA
	Type	Penetration Testing (Black Box)
	Scheduling	No schedule
	Created By	pronet
Summary	Pentera Version	v5.8.1
	Completion Status	✓ Completed successfully
	Time & Duration	May 23 2025 23:44 - May 24 2025 20:10, 20:25
	Action Approval Score	112 / 112 , 100%
Ranges	Include IP Range(s)	10.255.248.52 10.255.248.14 10.255.248.110 10.255.248.2 10.255.248.75 10.255.248.76 10.255.248.4 10.255.248.5 10.255.248.9 10.255.248.108
Intensity	Maximum Duration	00d:20h:01m
	Spoofing Duration	00d:20h:01m
	Perform Automatic Rescan	00d:02h:00m
	Stealthiness Level	(4) Normal discovery, common Windows & Linux services enumeration (default)
Exploitation Settings	Basic	Allow Exploits - Require Approval for Exploits Allow DHCP Man In the Middle Attacks (Always requires approval) Allow Out of IP Range Spoofing Allow Services Bruteforce - Require Approval Allow Web application Enumeration and Attacks - Allow Web Application Bruteforce (always requires approval)
	Advanced	Allow Automatic Active Directory Account Creation, Relay Attacks Allow Automatic Credentials Dump Relay Attacks Allow Automatic 'Printer Bug' Relay Attacks Allow Automatic Active Directory Controller(s) Identification And Queries Allow out of range discovery of Azure Cloud Virtual Machines

Group	Type	Details
Notifications		soporte@pronet.mx

Include IP Range(s)

(Listing 15 of 15 items).

10.255.248.75

10.255.248.14

10.255.248.5

10.255.248.2

10.255.248.4

10.255.248.108

10.255.248.76

10.255.248.110

10.255.248.22

10.255.248.53

10.255.248.52

10.255.248.10

CONFIDENTIAL AND PROPRIETY INFORMATION

Pentera provides the Pentera™ service and report "As Is", without any warranty of any kind. Pentera makes no warranty that the information contained in this report is complete or error - free.

pronet

CEH

PENTERA

PENTERA

Remediation Wiki Articles

Sorted by **Remediation Priority**

Remediation articles are offered for select vulnerabilities to help you understand the underlying causes, the recommended steps for fixing the issues, and how to re-test with Pentera and validate that your remediation steps were successful.

Please refer to the Vulnerabilities Section in your report for the complete list and recommended remediation priority. The vulnerabilities covered by these articles may not represent the complete list as shown in your report.

SMB Message Signing

Insight

The SMB protocol, initially designed for file and share access, is now used as a main communication protocol in Windows. Many different named pipes implement the SMB protocol and allow, among other services, remote code execution.

Using the SMB protocol, a user in the domain can authenticate himself and use the services exposed by the other Windows servers and workstations within the domain.

SMB message signing is a cryptographic method of encrypting the network packets sent by the client, in order to authenticate them and their origin. This feature was introduced in Windows 2000, and later was added into older versions of Windows too.

The first version of SMB, called appropriately SMB1 uses MD5 hashing as the crypto method. Later, as part of the improvements done in SMB2, the crypto method was switched to the HMAC SHA-256 hashing algorithm.

By default, only the DC is configured with SMB signing, and all workstations and servers are configured to support, but not enforce, signing.

Impact

The SMB messages can be used by malicious users in two ways:

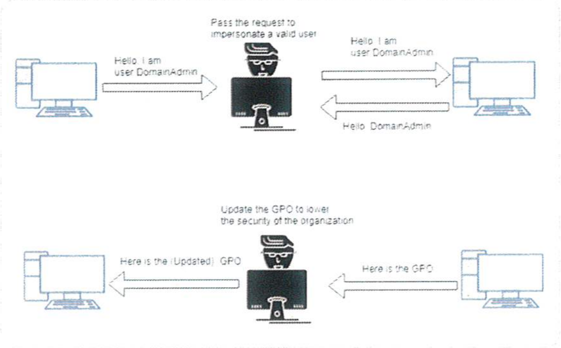
1. Man-In-The-Middle (MITM) attack:

   A malicious attacker can poison the network and make a victim send an SMB request to his computer. Then, that attacker will redirect that request to a target Windows machine.

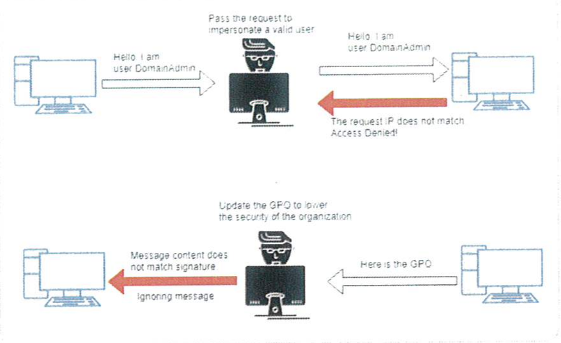
   Once the redirection is complete, the attacker uses the victims' authentication as if it were his own, and can exploit the messages to run malicious code on the target machine.
2. Updating an organization's settings such as GPO:

   Since the SMB protocol is used to send commands and updates, for example, the organizational group policy, a malicious attacker can hijack the message, and update it as he wishes to lower the security settings of the organization

Both these attacks can be mitigated by enabling SMB Signing, thus preventing anyone from tampering with the messages and redirecting them.


Pass the request to impersonate a valid user
Hello. I am user DomainAdmin
Hello. I am user DomainAdmin
Hello. DomainAdmin
Update the GPO to lower the security of the organization
Here is the (Updated) GPO
Here is the GPO

When SMB signing is disabled


Pass the request to impersonate a valid user
Hello I am user DomainAdmin
Hello I am user DomainAdmin
The request IP does not match Access Denied!
Update the GPO to lower the security of the organization
Message content does not match signature
Ignoring message
Here is the GPO

When SMB signing is enabled

Recommendations

Enabling SMB Signing is done by editing the OS registry value. However, it is strongly recommended to configure them by using group policies instead of changing the values directly since group policies can be configured differently and might override the local changes.

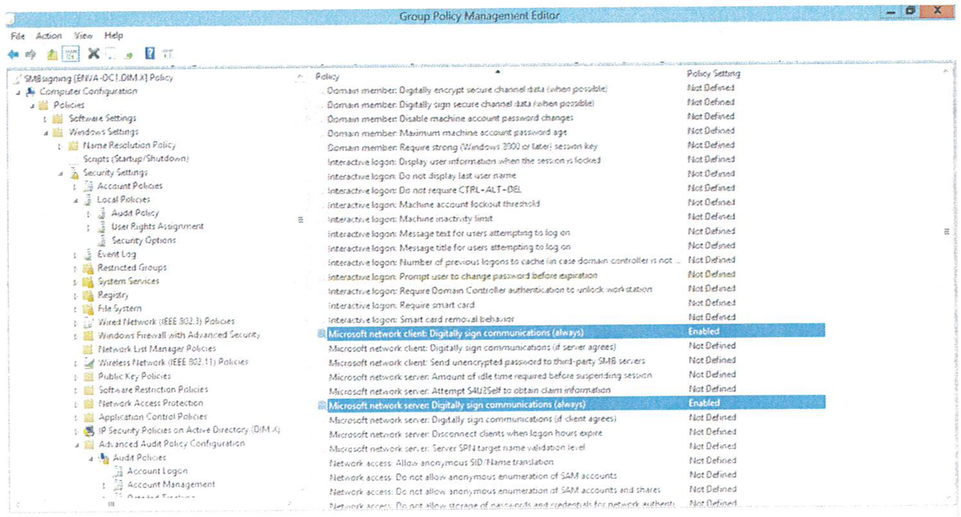
It is important to note that SMB Signing has 3, not 2, settings:

- **Enabled** - This option will not prevent malicious activity since the attacker can request the machine to switch to unsigned communication.
- **Disabled**
- **Required** - This is the recommended setting. It forces the OS to communicate strictly through signed messaging.

Enabled SMB Signing means that the machine is capable of communicating using Signed SMB messaging, but it allows for unsigned communication as well. If SMB Signing is set to be enabled, the machine will prefer to use signed communication, but will fall back to the unsigned version upon request.

Technical Enforcement

Enabling SMB signing can be done by using the GPO. In order to enable and enforce SMB signing, enable the option: **Digitally sign communication**(**always**) of the client and the server:



```
SMBsigning [ENVA-DC1.DIM.X] Policy
  Computer Configuration
    Policies
      Software Settings
      Windows Settings
        Name Resolution Policy
        Scripts (Startup/Shutdown)
        Security Settings
          Account Policies
          Local Policies
            Audit Policy
            User Rights Assignment
            Security Options
          Event Log
          Restricted Groups
          System Services
          Registry
          File System
          Wired Network (IEEE 802.3) Policies
          Windows Firewall with Advanced Security
          Network List Manager Policies
          Wireless Network (IEEE 802.11) Policies
          Public Key Policies
          Software Restriction Policies
          Network Access Protection
          Application Control Policies
          IP Security Policies on Active Directory (DIM.X)
          Advanced Audit Policy Configuration
            Audit Policies
              Account Logon
              Account Management
```

Policy	Policy Setting
Domain member: Digitally encrypt secure channel data (when possible)	Not Defined
Domain member: Digitally sign secure channel data (when possible)	Not Defined
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) session key	Not Defined
Interactive logon: Display user information when the session is locked	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case domain controller is not ...	Not Defined
Interactive logon: Prompt user to change password before expiration	Not Defined
Interactive logon: Require Domain Controller authentication to unlock workstation	Not Defined
Interactive logon: Require smart card	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Not Defined
Microsoft network client: Send unencrypted password to third-party SMB servers	Not Defined
Microsoft network server: Amount of idle time required before suspending session	Not Defined
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Not Defined
Microsoft network server: Disconnect clients when logon hours expire	Not Defined
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Not Defined
Network access: Do not allow storage of passwords and credentials for network authenti...	Not Defined

How to use Pentera for validation

You can run a quick test with Pentera to identify machines that are vulnerable to the exploit or validate that the vulnerability does not exist in your environment. If the vulnerability was previously found in your network, you can use Pentera to validate that your remediation efforts were successful and the issue has been fixed.

1. Create a template with the range of IPs you want to scan.
2. After the initial scan, Pentera will scan for machines with disabled SMB signing.
3. You can view the results in the Vulnerabilities tab. If the vulnerability "**SMB Message Signing disabled**" is shown, there are hosts in need of remediation.

References and Resources

- https://blogs.technet.microsoft.com/josebda/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2/

DISCLAIMER

Pentera® provides remediation recommendations based on the latest research conducted by the Pentera® research team. The information is provided "as is" for informational purposes only. Pentera® does not assume any responsibility and expressly disclaims any liability for any use of or inability to use the Remediation Wiki articles or any material contained in them, or from any action or decision taken as a result of using them.

The Remediation Wiki offers links to other sites. Pentera® is not responsible for the content of any linked site or any link in a linked site and does not endorse or approve the linked sites.

Name Resolution Protocols (LLMNR/NBNS/mDNS)

MITRE

LLMNR/NBT-NS Poisoning and Relay (T1171)

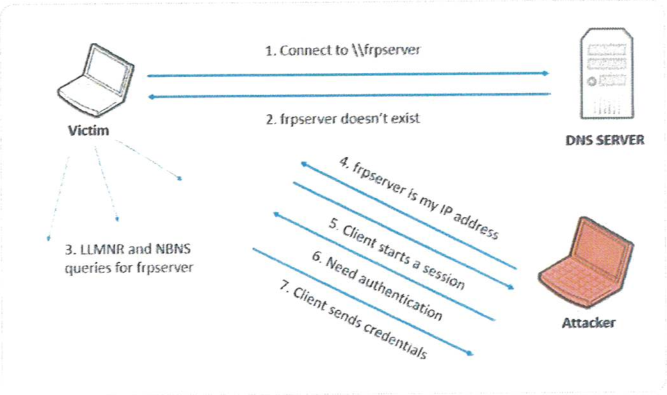
Insight

LLMNR (Link-Local Multicast Name Resolution), NBNS (Netbios Name Service) and mDNS (Multicast Domain Name Service) are Microsoft Windows protocols which serve as alternate methods of Name Resolution. If a machine tries to resolve a particular host, but DNS resolution fails, the machine will then attempt to ask all other machines on the local network for the correct address via LLMNR, NBNS or mDNS. Since this operation is performed using broadcast or multicast queries with no means of validation, it is susceptible to malicious answers distributed by an attacker, effectively poisoning the network.

Impact

An attacker can listen on a network for these LLMNR (UDP/5355) or NBNS (UDP/137) broadcasts and respond to them, pretending that the location of the requested host is at the attacker's machine.

Let's look at an example in the diagram below:


1. Connect to \\frpserver
2. frpserver doesn't exist
Victim
DNS SERVER
3. LLMNR and NBNS queries for frpserver
4. frpserver is my IP address
5. Client starts a session
6. Need authentication
7. Client sends credentials
Attacker

1. The victim machine wants to go the print server at \\ftpserver, but mistakenly types in \\frpserver
2. The DNS server responds to the victim that no dns record was found
3. The victim turn to the network and asks by using LLMNR or NBNS if there is anyone knows the location of \\pntserver
4. The attacker responds to the victim that \\pntserver is his own IP address
5. The victim believes the attacker and starts a session with him
6. The attacker asks the victim to authenticate
7. The client sends its credentials (NTLMv1 / NTLMv2)
8. The attacker can now crack the hash to discover the password

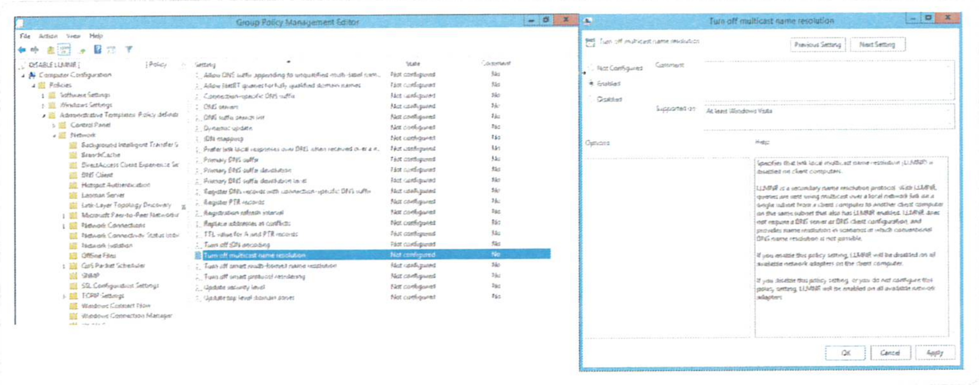
Recommendations

Disable the protocols: mDNS, LLMNR, and NBNS.

Disable mDNS

There is a `mDNSResponder.exe` process that belongs to the `Bonjour Service` in Windows, which is Apple's "Zero Configuration Networking" application, typically installed automatically by iTunes, Skype and others. It can be disabled by using GPO.

Disable LLMNR via GPO



Setting	State	Comment
Allow DNS suffix appending to unqualified multi-label nam...	Not configured	No
Allow NetBT queries for fully qualified domain names	Not configured	No
Connection-specific DNS suffix	Not configured	No
DNS servers	Not configured	No
DNS suffix search list	Not configured	No
Dynamic update	Not configured	No
IDN mapping	Not configured	No
Prefer link local responses over DNS when received over a n...	Not configured	No
Primary DNS suffix	Not configured	No
Primary DNS suffix devolution	Not configured	No
Primary DNS suffix devolution level	Not configured	No
Register DNS records with connection-specific DNS suffix	Not configured	No
Register PTR records	Not configured	No
Registration refresh interval	Not configured	No
Replace addresses in conflicts	Not configured	No
TTL value for A and PTR records	Not configured	No
Turn off IDN encoding	Not configured	No
Turn off multicast name resolution	Not configured	No
Turn off smart multi-homed name resolution	Not configured	No
Turn off smart protocol reordering	Not configured	No
Update security level	Not configured	No
Update top level domain zones	Not configured	No

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Vista

Specifies that link local multicast name resolution (LLMNR) is disabled on client computers.

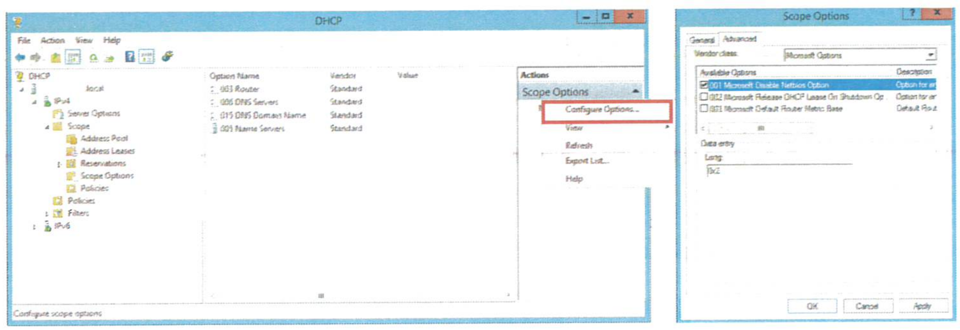
LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in scenarios in which conventional DNS name resolution is not possible.

If you enable this policy setting, LLMNR will be disabled on all available network adapters on the client computer.

If you disable this policy setting, or you do not configure this policy setting, LLMNR will be enabled on all available network adapters.

1. Create a new GPO record for all computers in the environment.
2. Navigate to **Local Computer Policy / Computer Configuration / Administrative Templates / Network / DNS Client**.
3. Set **Turn Off Multicast Name Resolution** to **Enabled**.

Disable NBNS in a DHCP environment



Option Name	Vendor	Value
003 Router	Standard	
006 DNS Servers	Standard	
015 DNS Domain Name	Standard	
005 Name Servers	Standard	

Vendor class: Microsoft Options

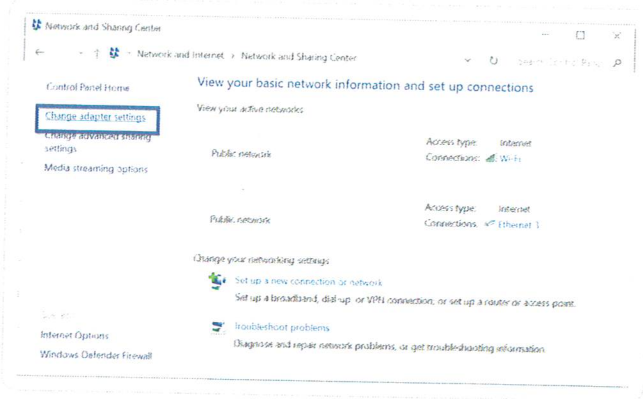
Available Options	Description
☑ 001 Microsoft Disable Netbios Option	Option for en
☐ 002 Microsoft Release DHCP Lease On Shutdown Op	Option for en
☐ 003 Microsoft Default Router Metric Base	Default Rout

Data entry
Long:
0x2

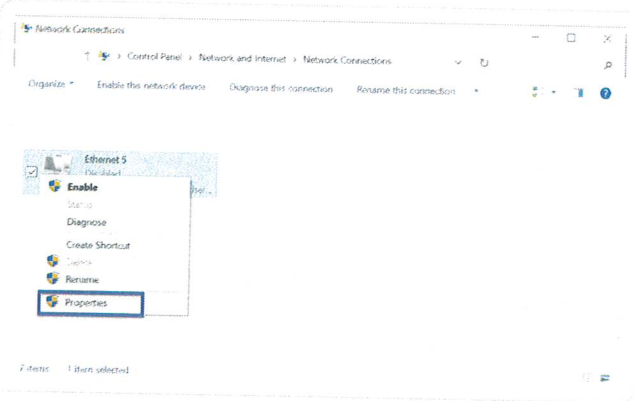
1. Go to DHCP Management
2. Go to "scope options" for the network you are changing
3. Right click and Configure Options
4. Select Advanced tab and change "Vendor class" to "Microsoft Options"
5. In the "Available Options" frame, select and check the box "001 Microsoft Disable Netbios Option"
6. In the "Data Entry" frame, change the data entry to 0x2
7. Click "OK". The new settings will take affect when the clients renew their addresses.

Disable NBNS on a single host

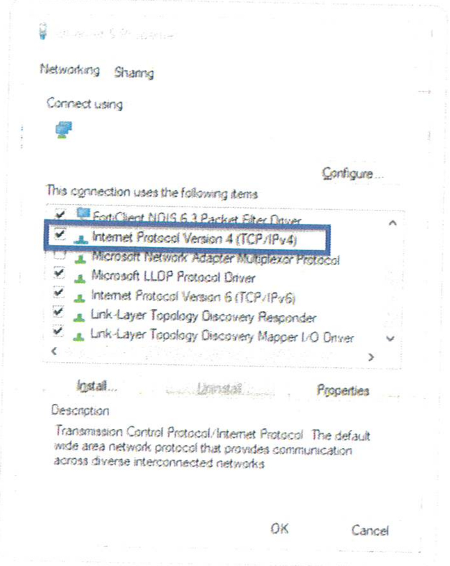
1. Open the **Control Panel** > **Network and Sharing Center**.
2. Select **Change adapter settings**.


Network and Sharing Center
Network and Internet > Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
View your basic network information and set up connections
View your active networks
Public network
Access type: Internet
Connections: Wi-Fi
Public network
Access type: Internet
Connections: Ethernet 1
Change your networking settings
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
Internet Options
Windows Defender Firewall

3. The list of local area (LAN) connections will be shown. Right-click a **LAN** and select **Properties**.

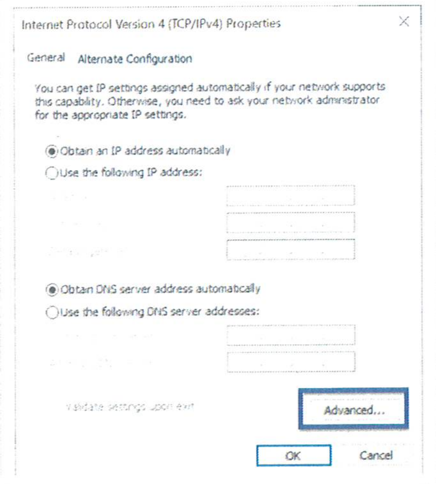


4. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.


Ethernet 5 Properties
Networking
Sharing
Connect using
Configure...
This connection uses the following items
FortiClient NDIS 6.3 Packet Filter Driver
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Link-Layer Topology Discovery Responder
Link-Layer Topology Discovery Mapper I/O Driver
Install...
Uninstall
Properties
Description
OK
Cancel

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5. Select **Advanced**.

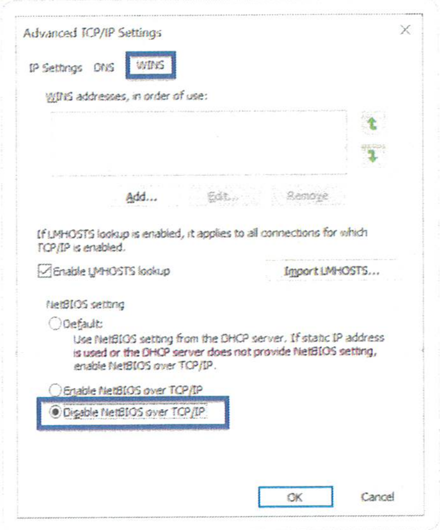


You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

6. Navigate to the **WINS** (Windows Internet Name Service) tab, and enable the option to **Disable NetBIOS over TCP/IP**. Click **OK** to save your changes.



If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

NetBIOS setting

○ Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

● Disable NetBIOS over TCP/IP

Technical Enforcement

Name Resolution Processes

When a name needs to be resolved, a computer running Windows Vista and further, that is using both IPv6 and IPv4 (the default configuration) will do the following:

1. Perform normal DNS resolution by combining the name with the primary DNS suffix of the computer and sending a DNS Name Query Request message to its DNS server. Windows performs additional DNS queries as needed based on name devolution or additional search suffixes that have been configured.
2. If DNS name resolution is not successful, send up to two sets of multicast LLMNR Name Query Request messages over both IPv6 and IPv4.
3. If LLMNR name resolution is not successful and NBNS is enabled, broadcast up to three NBNS Name Query Request messages.

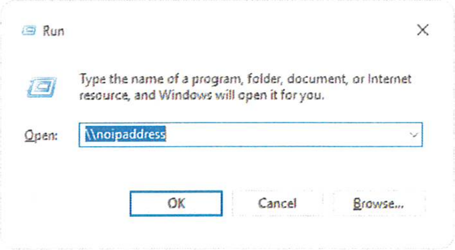
If the name being resolved has a DNS suffix such as [dot]domain[dot]com or [dot]local, LLMNR and NBNS are not used.

Notice that LLMNR is used regardless of whether the host has been configured to use a DNS server. This allows a computer running Windows to resolve the computer names of neighboring LLMNR hosts that do not have corresponding address records stored in DNS.

How to use Pentera for validation

Create an Advanced Penetration Testing Scenario and ensure that spoofing is enabled and that your IP address is within range.

Run the task. From your host machine, make queries that you know will have no IP address -



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: \\noipaddress

If no **sniffing** achievement appears, you have validated that you have successfully disabled LLMNR and NBNS.

Keep in mind that if you only disable one of the protocols, the other continues to put your network at risk.

Tips & Best Practices

- It is best in general to prevent inter-VLAN communication. By limiting communication between hosts on the same network, you greatly reduce the success of most local network attacks.
- Add DNS records for all hosts in your network to eliminate the need for NBNS.

References and Resources

- More about NBNS by Microsoft - NetBIOS Over TCP/IP

DISCLAIMER

Pentera® provides remediation recommendations based on the latest research conducted by the Pentera® research team. The information is provided "as is" for informational purposes only. Pentera® does not assume any responsibility and expressly disclaims any liability for any use of or inability to use the Remediation Wiki articles or any material contained in them, or from any action or decision taken as a result of using them.

The Remediation Wiki offers links to other sites. Pentera® is not responsible for the content of any linked site or any link in a linked site and does not endorse or approve the linked sites.

BlueKeep - (CVE-2019-0708)

Insight

CVE-2019-0708 is a critical vulnerability, also known as **BlueKeep**, that affects the Remote Desktop Service protocols (RDP) on Windows systems that predate Windows 7 and Windows Server 2008. The CVE-2019-0708 vulnerability allows an unauthenticated attacker under the default configuration to crash remote systems (thereby causing a Denial Of Service attack). Also, this vulnerability enables an attacker to remotely execute high privileged code on any vulnerable system.

Remote Desktop Protocol

The Remote Desktop Services in Windows environments allow users to access resources and software on a remote Windows endpoint, and interact it using a graphical interface, similar to the desktop that is running locally on the endpoint. The protocol is a Client-Server protocol, in which the remote target is the server, and the user is the client. RDP is a multi-channel protocol, which allows it to carry different types of data in separated, encrypted, virtual channels. For example, one channel can be used to transfer input from keyboard and another to transfer sound to and from the remote endpoint. Developers can also create custom channel extensions in order to transfer more types of data.

Denial Of Service

Before the authentication phase of RDP, the client and the server negotiate information in order to prepare the session. A part of this information, which is sent by the client, is a list of virtual channels to be opened for the session. For example, if the client wishes to share clipboard data with the remote host, it will request the server to connect to the clipboard channel for the session. It was discovered that one channel, called "MS_T120" is a static channel, connected by the service itself, and always binds to channel number 31. This is an internal channel intended to be used only by services, while clients have no legitimate reason to connect to this channel.

If a client, or in our case, an attacker, attempts to connect to that certain channel during the negotiation phase, another reference will be created for the same channel. Thus, the channels table will contain 2 entries which point to the same channel. Later, an attacker can send a crafted packet to that channel, which will request it to be closed (And the channel object will be freed by the operating system).

Once RDP disconnected, the service will attempt to close the channel using its own reference. However, since the channel was already closed by the attacker, the system will fail while trying to free a freed object.

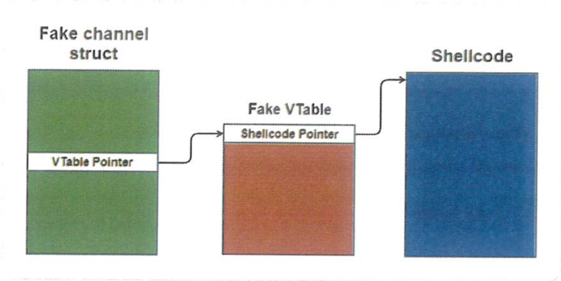
Since RDP's code is executed in the kernel space, a crash in the code results in a crash to the whole syste, and the end user will experience a blue screen. This type of vulnerability is known as the **Use After Free** (UAF).

Remote Code Execution (RCE)

It turns out that when the service references the MS_T120 channel, it executes a list of functions that are stored in table pointed by the channel's struct. Using that, the attacker needs the following to execute code:

1. Create a new channel struct in the same location of the one that was freed
2. In that channel struct, there will be a link to a table
3. Create the table with an entry that points to a shell code address
4. Plant the shell code in that specific address
5. Trigger disconnection from the RDP, and the service will execute the shell code

The following diagram describes the desired result (*taken from MalwareTech blog, link in the section below*):

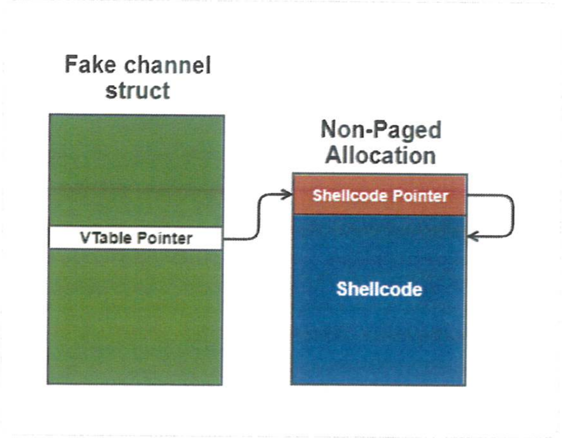


The above plan entails a few challenges:

1. The attacker needs write access to the location of the older channel struct
2. Every piece needs to be planted in the correct address (which is also unknown)
3. The shell code needs to be allocated in a space where code execution is possible

Channel structs, like the one that was freed, are allocated in a region called the Non-paged Pool. The attacker needs to gain write access to that region so he can allocate a new channel struct in place of the older one. Such write access can be achieved by sending data messages to other channels, which store those message in the same region. Most channels read and deallocate messages as they arrive (which is bad for the attacker), however, one certain channel is found to never read message thus leaving them allocated in the space. Write access to random address in the pool is not enough, since the attackers need to write to the same location of the old struct (which is also unknown). A solution would be to send many messages in the same size of the older channel (which is fixed) to increase the likelihood of one allocation to be place in the right location.

As for the shell code location, since there is no **Data Execution Prevention (DEP)** in the **Non-paged Pool** on Windows 7 or older versions, an attacker could write the shell code anywhere. Therefore the diagram can be refined so (*taken from MalwareTech blog*):



The last challenge that is left for the attacker is to determine the **VTable Pointer address** (which is the location of the shell code). If the struct points to a wrong address, the shell code won't be triggered (and the system will probably crash). Since the attacker knows where the pool starts (as there is a fixed address for every operating system) and since the operating system usually refrains from allocating anything in that pool, the attacker could pick an address deep into the pool (say 500MB after the pool starts) which will probably be unallocated and therefore available for the shell code. Then, the attacker can spray many copies of the shell code so that the chosen address will likely contain the shell code. As a result, the VTable Pointer will be set as the attacker's chosen address and the shell code will probably be triggered.

Impact

An unauthenticated attacker could crash remote endpoints (Denial of Service) and potentially execute arbitrary high privilege code on them. Affected Windows versions are:

Windows XP

- Windows Server 2003
- Windows Vista
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

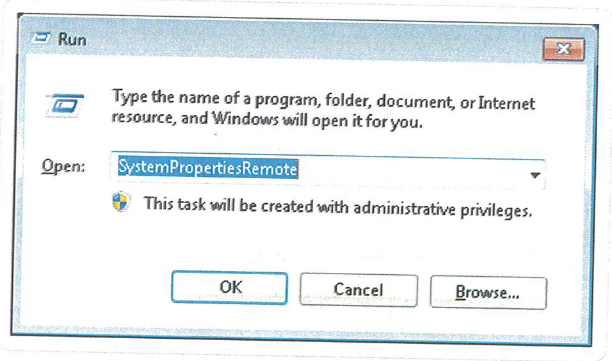
Recommendations

1. Install Microsoft's patch on vulnerable systems.
2. Enable Network Level Authentication (NLA) which forces users to authenticate prior communicating with the remote desktop service.
3. On endpoints which don't require the remote desktop capability, it should be disabled.
4. Where possible, block communication to the remote desktop service (TCP on port 3389) using a firewall.
5. Monitor interactions with the service, both on the network level (using network monitoring tools in the environment) and on the endpoint level (using the Event Viewer on Windows).

Technical Enforcement

Enable Network Level Authentication (NLA)

1. In order to enable NLA for a specific system, press WinKey + R, then type **SystemPropertiesRemote**

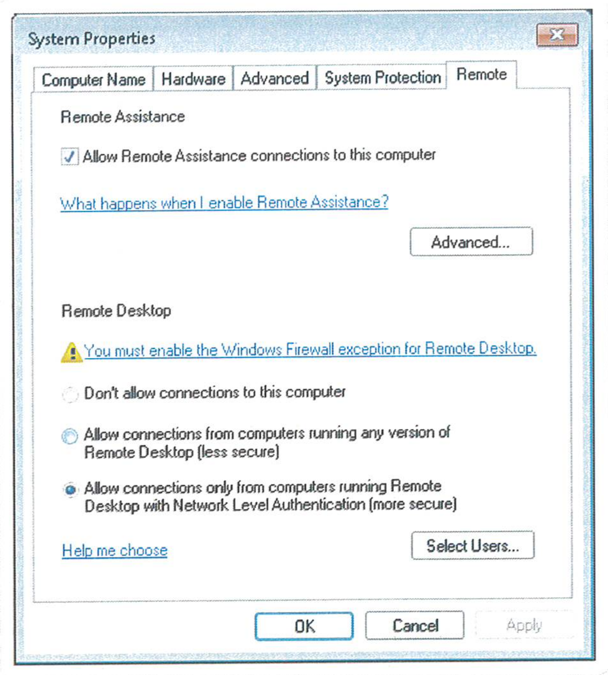


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: SystemPropertiesRemote

This task will be created with administrative privileges.

2. In the opened window, make sure to choose "**Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)**"



System Properties

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

⚠ You must enable the Windows Firewall exception for Remote Desktop.

○ Don't allow connections to this computer

○ Allow connections from computers running any version of Remote Desktop (less secure)

● Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Help me choose

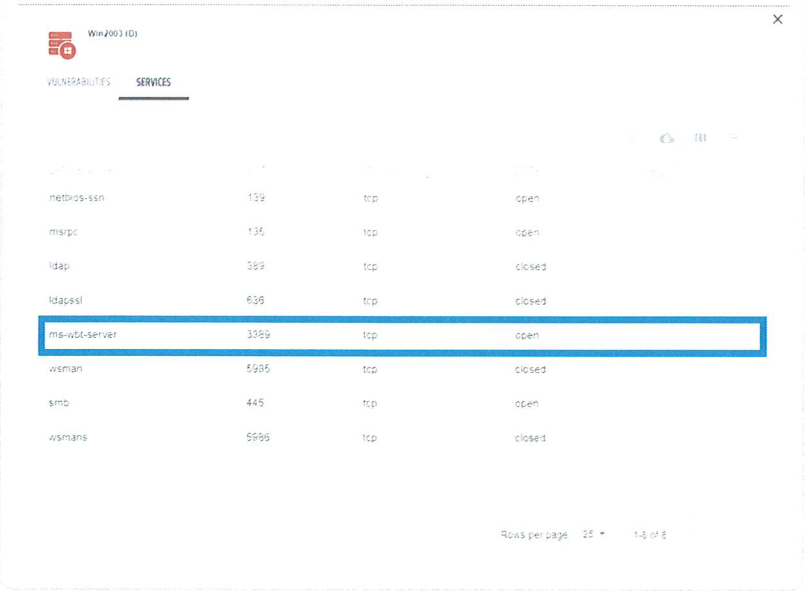
3. To enable NLA using Group Policy, edit the Group Policy and apple the setting called "**Require user authentication for remote connections by using Network Level Authentication**" which is located under **Computer Configuration\Policies \Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security**. Applying this setting takes precedence over the setting in the Remote tab (from the previous steps)

More information can be found at https://social.technet.microsoft.com/wiki/contents/articles/5490.configure-network-level-authentication-for-remote-desktop-services-connections.aspx

How to use Pentera for validation

- Create a new "Advance Penetration Testing" or "Vulnerability Assessment" template with IP addresses of the Windows machines you want to test remediation on.
- Navigate to the **Host** section from the top menu.
- Click on the desired target host and then click on **Services**. Check if Pentera can access port 3389 over TCP on the target machines.

If the port is inaccessible due to firewall protection, consider changing Pentera's network position or enabling temporary access from the Pentera machine.

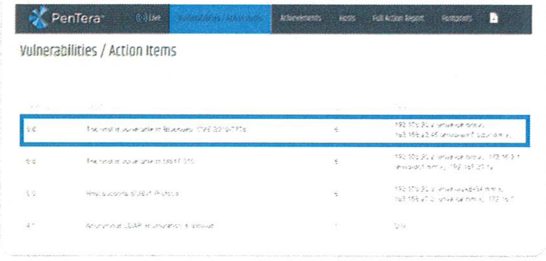


netbios-ssn	139	tcp	open
msrpc	135	tcp	open
ldap	389	tcp	closed
ldapssl	636	tcp	closed
ms-wbt-server	3389	tcp	open
wsman	5985	tcp	closed
smb	445	tcp	open
wsmans	5986	tcp	closed

Rows per page 25 ▾ 1-8 of 8

- To view all vulnerable hosts, check the **Vulnerabilities** tab for a vulnerability entitled: **The host is vulnerable to BlueKeep (CVE-2019-0708)** (severity of 9.8). If so, the host is vulnerable.

  Selet the vulnerability from the list to view the hosts listed under the relevant column.



Vulnerabilities / Action Items

9.8	The host is vulnerable to BlueKeep (CVE-2019-0708)	6	[illegible]
9.8	The host is vulnerable to MS17-010	6	[illegible]
5.9	Host supports SSLv3 Protocol	6	[illegible]
[illegible]	Anonymous LDAP enumeration is allowed	1	N/A

Tips & Best Practices

Although the Remote Desktop service is a very useful and powerful Windows feature, it poses a risk to endpoint since attackers tend to leverage it for malicious intentions. It is highly recommended to follow the other mitigation steps listed here since they might protect endpoint from future vulnerabilities that will affect this service.

References and Resources

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
- https://www.microsoft.com/security/blog/2019/08/08/protect-against-bluekeep/
- https://social.technet.microsoft.com/wiki/contents/articles/5490.configure-network-level-authentication-for-remote-desktop-services-connections.aspx
- https://www.malwaretech.com/2019/05/analysis-of-cve-2019-0708-bluekeep.html
- https://www.malwaretech.com/2019/09/bluekeep-a-journey-from-dos-to-rce-cve-2019-0708.html

DISCLAIMER

Pentera® provides remediation recommendations based on the latest research conducted by the Pentera® research team. The information is provided "as is" for informational purposes only. Pentera® does not assume any responsibility and expressly disclaims any liability for any use of or inability to use the Remediation Wiki articles or any material contained in them, or from any action or decision taken as a result of using them.

The Remediation Wiki offers links to other sites. Pentera® is not responsible for the content of any linked site or any link in a linked site and does not endorse or approve the linked sites.

Cached Credentials

MITRE

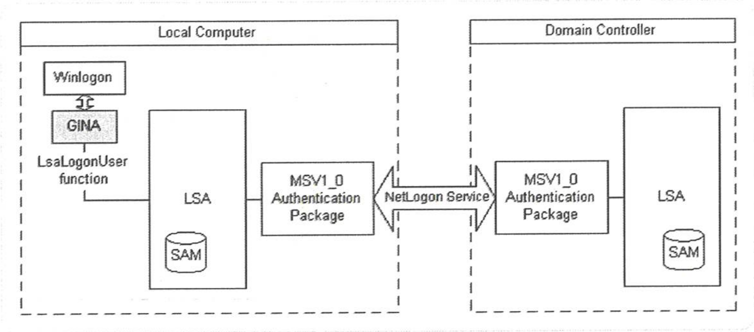
Credential Dumping (T1003)

Insight

Microsoft Windows uses several authentication protocols for multiple purposes. The following protocols are particularly meaningful in the information security world, due to the way they save passwords in the operating system.

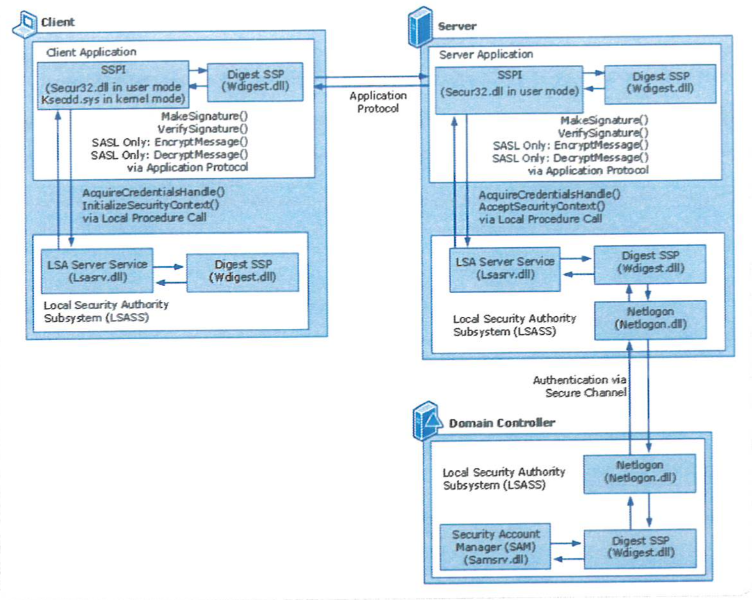
- **CredSSP -** The Credential Security Support Provider protocol (CredSSP) is a Security Support Provider that lets an application delegate the User's Credentials from the Client to the Target Server for Remote Authentication.

  The client is authenticated over an encrypted channel by using the Simple and Protected Negotiate (SPNEGO) protocol with either Microsoft Kerberos or Microsoft NTLM.
- **MSV -** An authentication package for local machine logons. The LSA calls the MSV1_0 Authentication Package to process Logon Data for the Winlogon Logon Process. It also supports Domain Logons. MSV1_0 processes the Domain Logons using Pass-Through Authentication.



MSV1_0 processes the Domain Logons using Pass-Through Authentication

- **WDigest -** The Digest Authentication is a protocol that is used for different Authentication Exchanges (for example; LDAP and HTTP). This protocol is similar to NTLM as it uses challenge/response protocols in order establish authentication between the server and the client. The client's challenge/response key is encrypted by the user's password. The server receives the client's encrypted response and compares it based on the associated user's AD credentials. After this authentication flow, communication between the client and the server commences.

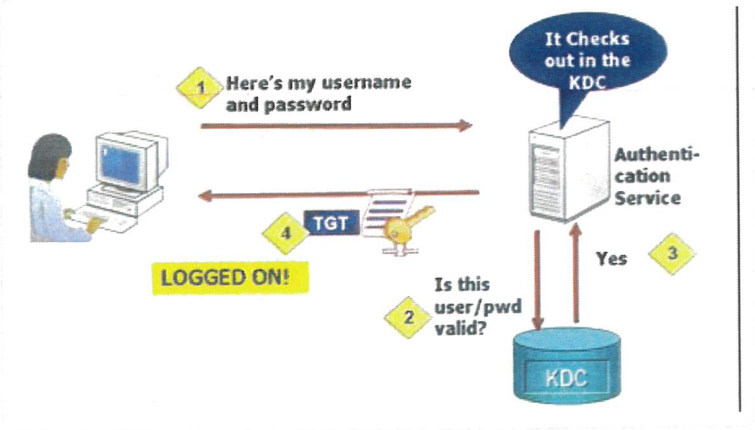


In depth diagram of the WDigest authentication flow

- **Kerberos -** Kerberos is a network authentication protocol that is based on using a ticketing system to allow computers that are communicating over a non-secure network to establish trust in a secure manner.

The Kerberos protocol relays on third-party verification and has several advantages over NTLM:

- **Speed** - The Kerberos authentication method is much faster as the ticket that is received from the client already includes all the necessary information from the client which making it faster than the challenge/response authentication of NTLM.
- **Mutual Authentication** - In contrast to NTLM, Kerberos supports mutual authentication, meaning, that both the server and the client have to authenticate each other.



Kerberos supports mutual authentication

Exploitation

After the user Logs-On, a variety of credentials are generated and stored in the Local Security Authority Subsystem Service process-in memory (LSASS). This is meant to facilitate Single Sign-On (SSO) ensuring that a user is not prompted each time resource-access is requested. The credential data may include Kerberos tickets, NTLM password hashes, LM password hashes (if the password is less than 15 characters, depending on Windows OS version and patch level), and even clear-text passwords (to support WDigest and SSP authentication among others). While you can prevent a Windows computer from creating the LM hash in the local computer SAM database (and the AD database), this does not prevent the system from generating the LM hash in-memory.

Known tools and techniques

While many tools perform quite a few methods of these actions, the most common tool and perhaps the best one is Mimikatz, made by Benjamin Delpy. Since Mimikatz is an open source tool, different variations of it have surfaced, and it is easily modified to bypass Antivirus software and in some cases even detection systems.

Mimikatz and all equivalent tools require **Administrative or System Access**, and sometimes require **Debug Mode** in order to extract the needed information from different protocols.

Impact

An attacker with Administrative Access to a host can extract cleartext credentials from the host's memory and proceed the attack further into the organizational network.

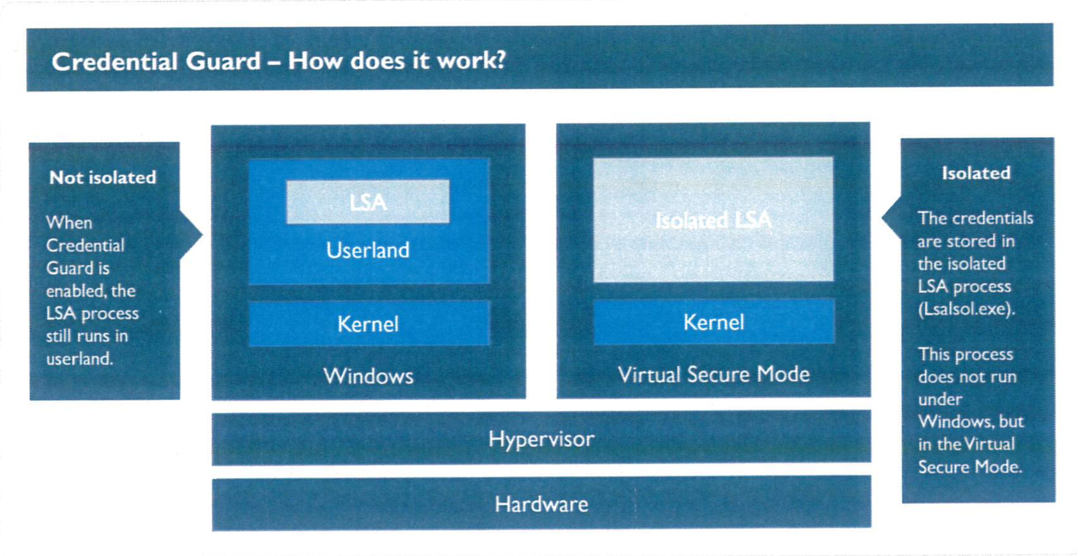
Armed with cleartext credentials, an attacker can access different services and assets in the domain and steal or manipulate sensitive information.

Recommendations

Windows 10 and Windows 2016

In Windows 10 and Windows 2016, Microsoft introduced a security feature called "**Windows Defender Credential Guard**" or LSA protection. It uses a virtualization feature of modern CPUs in order provide a separate memory space which is isolated from the normal Operating System (at the hardware level).

With the Credential Guard enabled, the LSASS process which contains the sensitive authentication data splits into 2 processes, one runs in the normal OS and another runs in the Isolated Designated Virtual area. Consequently , the Mimikatz attack on the LSA would be unsuccessful since it would not be able to access the isolated LSA process.



Credential Guard – How does it work?

Not isolated

When Credential Guard is enabled, the LSA process still runs in userland.

Isolated

The credentials are stored in the isolated LSA process (Lsalsol.exe).

This process does not run under Windows, but in the Virtual Secure Mode.

With Credential Guard enabled, the LSASS process is split into 2 processes

Earlier versions of Windows (prior to Windows 10 and Windows 2016)

When using an OS that predates Windows 10 or Windows Server 2016, the following steps can be applied to increase protection. It is recommended that you disable several settings in the organizational Group Policy:

1. Disable `SeDebugPrivilege` for local administrators on every Host. This step is necessary since this Windows feature enables easy escalation of privileges over a process using the Windows API for a malicious attack.

You can do that by setting GPO from: **Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment > Debug Program > Enable**.

2. Disable WDigest usage by editing the following Registry entry: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest` - Set both *Negotiate* and *UseLogonCredential* to **0**.
3. It is recommended that you enable LSA protection. This can be done by creating the Registry Key *RunAsPPL* and setting the value to **1** in the following Registry location: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA`.
4. It is recommended that you limit the number of cached logins that the system saves. By default the system saves the last **10** password hashes.

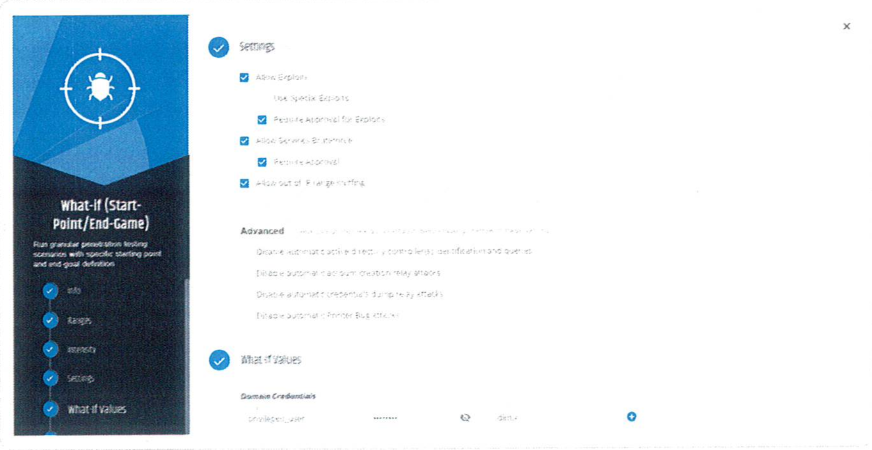
   We recommend setting it to **0** using the following path: **Computer Configuration > Windows Settings > Local Policy -> Security Options > Interactive Logon: Number of previous logons to cache > 0**.

   > WARNING
   > In the event that the connection with the Domain Controller is lost, the user will not be able to login to the host.

How to use Pentera for validation

You can run a quick test with Pentera to identify machines that are vulnerable to the exploit or validate that the vulnerability does not exist in your environment. If the vulnerability was previously found in your network, you can use Pentera to validate that your remediation efforts were successful and the issue has been fixed.

Create a What-if Testing Scenario and set the range to cover hosts you suspect to have vulnerable operating systems. Provide crednetials for a high-privileged user that will enable the system to take over the hosts. Set the template to use no special exploits, as seen in the following screenshot:


What-If (Start-Point/End-Game)
Run granular penetration testing scenarios with specific starting point and end goal definition
Info
Ranges
Intensity
Settings
What If Values
×

Settings

☑ Allow Exploits

Use Specific Exploits

☑ Require Approval for Exploits

☑ Allow Services Bruteforce

☑ Require Approval

☑ Allow out of IP range sniffing

Advanced

Disable automatic active directory controller(s) identification and queries

Disable automatic account creation relay attacks

Disable automatic credentials dump relay attacks

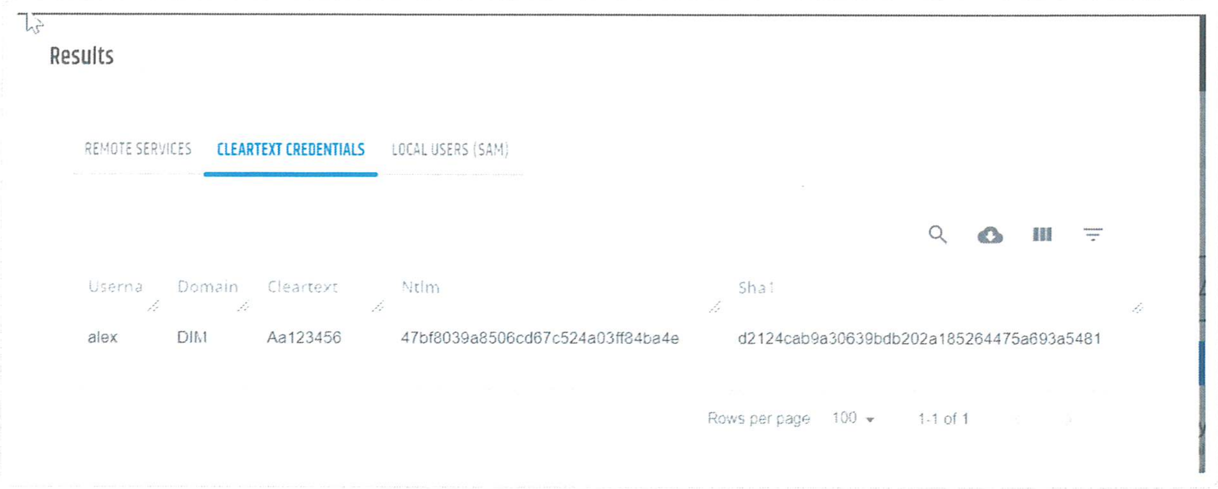
Disable automatic Printer Bug attacks

What If Values

Domain Credentials

privileged_user •••••••• [illegible]

Run the test and wait for a 9.4 Achievement on one of the hosts that you previously logged on to. Check if you gathered any domain credentials (with or without cleartext).



Results

Userna	Domain	Cleartext	Ntlm	Sha1
alex	DIM	Aa123456	47bf8039a8506cd67c524a03ff84ba4e	d2124cab9a30639bdb202a185264475a693a5481

Example of cached credentials extracted from a host by Pentera

References and Resources

- https://docs.microsoft.com/en-us/windows/desktop/secauthn/credential-security-support-provider
- https://docs.microsoft.com/en-us/windows/desktop/secauthn/msv1-0-authentication-package
- https://adsecurity.org/?page_id=1821
- https://blog.nviso.be/2018/01/09/windows-credential-guard-mimikatz/
- https://support.microsoft.com/en-us/help/131065/how-to-obtain-a-handle-to-any-process-with-sedebugprivilege
- https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements
- https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection
- https://www.itprotoday.com/security/comparing-windows-kerberos-and-ntlm-authentication-protocols
- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778868(v=ws.10)
- https://www.jimwilbur.com/2017/10/wdigest-clear-text-passwords/
- https://www.varonis.com/blog/kerberos-authentication-explained/

DISCLAIMER

Pentera® provides remediation recommendations based on the latest research conducted by the Pentera® research team. The information is provided "as is" for informational purposes only. Pentera® does not assume any responsibility and expressly disclaims any liability for any use of or inability to use the Remediation Wiki articles or any material contained in them, or from any action or decision taken as a result of using them.

The Remediation Wiki offers links to other sites. Pentera® is not responsible for the content of any linked site or any link in a linked site and does not endorse or approve the linked sites.

Password Policy Recommendations

MITRE

Brute Force (T1110)

Insight

Many data breaches are attributed to human factors, and weak passwords are among the most salient causes. Weak passwords can be easily cracked using advanced cracking tools, enabling attackers to gain access to the organizational infrastructure and later continue further exploitation.

Many weak passwords are based on simple words, which are very easy for hackers to crack and use to gain entry to critical enterprise services. In 2018, passwords were still the most commonly used authentication method and "Password1" was still the most common password. Shockingly, "Password1" meets most organizational password policies (at least 8 characters, a mix of uppercase and lowercase letters and a number), yet it can easily be cracked in mere seconds.

Impact

You can have the best cyber defenses, but if your keys are trivial they pose a low barrier. If easily cracked, credentials provide an easy entry point for attackers into the organization.

Credential sniffing is a common attack technique enabling attackers to access the user hash, as shown below.

Achievement Details

Name

[illegible]

Parameters

Domain: BANSHEE

Results

[illegible]

Attackers can then use off-the-shelf password cracking tools and leverage strong GPU processing power to speed-up cracking time. Passwords that are not strong enough will enable attackers to gain access to cleartext passwords within seconds (for trivial passwords) or a few hours (when less trivial).

The ability of hackers to crack passwords have come a long way in the last couple of years. Easy access to computing power and large-scale GPUs have completely changed the landscape, enabling hackers to crack passwords and gain easy entry into organizations.

Once attackers have access to valid user credentials, they can leverage their achievement to progress the attack - the impact will depend on the user's privileges. Focus on securing higher-privilege users first, as they can provide attackers with more significant progress in exploiting the organization.

Recommendations

Maintain a Strong Password Policy

Maintaining and enforcing a stronger password policy is paramount.

The standard Microsoft password policy, which requires at least 8 characters, a mix of upper- and lowercase letters and a number, is no longer sufficient to block attackers from cracking passwords. For more information about Microsoft's Windows/AD recommended password policy, see password complexity requirements.

It is recommended that organizations update their password policy and enforcement with the following specifications:

1. Minimum password length: It is recommended to increase minimum characters to 10 characters (12 or above for privileged users).
2. Require at least 1 special character.
3. Require at least 1 of each: uppercase letter, lowercase letter and a digit.
4. Dictionary check: Validate that the password is not based on a simple dictionary word. If it is, it practically reduces the effective complexity of the password to 3-5 characters.

Additional Recommendations

- Educate your users, with a focus on privileged users, on the impact of using weak passwords and how easy it is to crack them.
- Consider using multi-factor authentication (MFA) with a focus on privileged users and strengthened authentication processes based on the risk or type of operation.
- Consider changing the organization's policy to enforce a password change every 90 days. Educate your users and enforce the use of longer and stronger passwords.

  Forcing employees to implement frequent password changes drives them to use easy to crack and predictable password patterns, such as changing "Password1" to "Password2".
- Consider applying a password filter to enforce more complex rules and regexes.

  See Strong- Password Enforcement and Passfilt.dll for instructions for using Microsoft's implementation of a password filter.

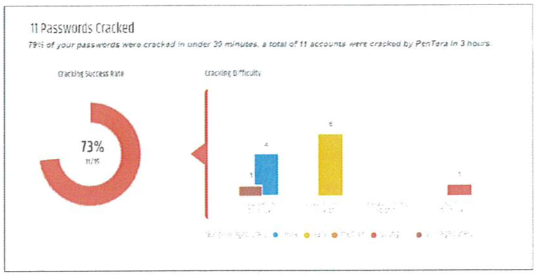
  An example for an open source password filter can be found at https://github.com/ryanries/PassFiltEx.

Technical Enforcement

Run Pentera with sniffing enabled and give the testing run enough time to sniff NTLM hash credentials and at least 6 hours to run through Pentera's 4-tiered password cracking engine. The results will provide a good indication of how effective the password policy is.

At the end of the testing run, the detailed report will provide detailed findings of the password strength evaluation. The **Passwords Cracked** section shows the total number of accounts Pentera was able to crack, how many of them belong to privileged accounts, and graphs the distribution of passwords by their strength and resilience to cracking.

Password complexity is ranked on a 4-tier scale: trivial, easy, medium, and strong, as determined by the type of Password Cracking Engine required to obtain the password.



11 Passwords Cracked

79% of your passwords were cracked in under 30 minutes, a total of 11 accounts were cracked by PenTera in 3 hours.

Tips & Best Practices

Here are 5 suggestions that both corporations and individuals should implement to ensure their password security:

#1 Don't use common dictionary words.

Examples: Password1, Football01.

This includes using simple digit-to-letter substitutions - as those are easily cracked by dictionary attack tools.

For example: Pa$$word1, F00tball01.

#2 Don't use sequential letters or numbers in your password.

Example: 123456, abcdef.

A password like Ab123456 is practically a 3 character password.

#3 Don't use your name or username as part of the password and/or other personal data that can be easily obtained via social networks (i.e. your kids' or pets' names).

#4 Do use a higher number of characters with a mix of upper/lower case letters, numbers and special characters.

Password length is key for a strong password. Consider using passphrases that have a higher number of characters, yet are easier to remember. Add special characters to the mix to make your password even stronger.

Example: ILikeMarsBars!!

#5 Do try to keep the password unpredictable. Introduce deliberate typos or insert a random number or special character in the middle of the password.

Example: ILike4FourNumbers!, Ihave2Twokidz.

DISCLAIMER

Pentera® provides remediation recommendations based on the latest research conducted by the Pentera® research team. The information is provided "as is" for informational purposes only. Pentera® does not assume any responsibility and expressly disclaims any liability for any use of or inability to use the Remediation Wiki articles or any material contained in them, or from any action or decision taken as a result of using them.

The Remediation Wiki offers links to other sites. Pentera® is not responsible for the content of any linked site or any link in a linked site and does not endorse or approve the linked sites.

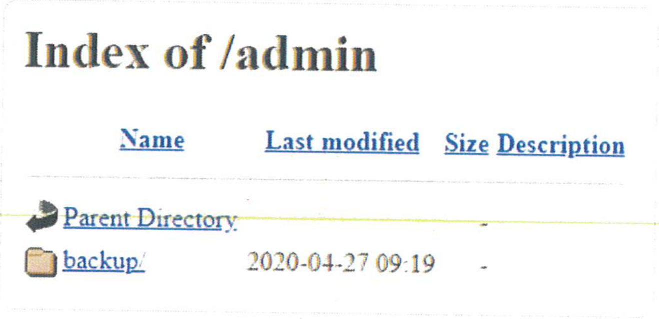
Directory Listing Attack

Insight

Web servers can be configured to automatically list the contents of directories that do not have an index page present. This can allow attackers to quickly identify the resources at a given path and enable them to proceed directly to analyzing and attacking those resources. In particular, a directory listing vulnerability increases the exposure of sensitive files, which were not intended to be accessible to users, such as temporary and hidden files, crash dumps, and configuration files.

Impact

Usually, a directory listing vulnerability provides access to unintended locations that developers did not anticipate, such as backup and debug folders. These data types have the potential to expose data that can allow attackers to compromise the web application, or even the entire server.



Index of /admin

Name	Last modified	Size	Description
Parent Directory		-	
backup/	2020-04-27 09:19	-	

Recommendations

As a security best practice, it is recommended to disable directory listing. You can disable directory listing by creating an empty index file in the relevant directory. This may be `index.php`, `index.html`, or any other extension your web server is configured to parse.

Technical Enforcement

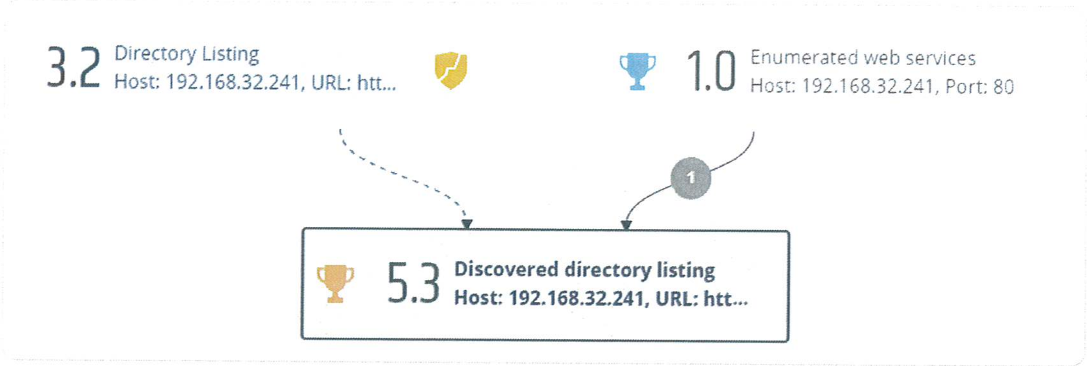
Follow industry best practices to disable the directory listing vulnerability. The following website contains sample configurations for disabling the directory listing vulnerability on most common web servers: https://www.netsparker.com/blog/web-security/disable-directory-listing-web-servers/.

You can use Pentera's newly developed web engines to detect directory listing vulnerabilities and their locations, which can help you optimize maintenance and prevention.

How to use Pentera for validation

Directory listing vulnerabilities are automatically detected on any web service covered by the scope of a Pentera test. No further action is required by the Pentera operator.

The screenshot below shows the vulnerability as detected by Pentera.


3.2 Directory Listing
Host: 192.168.32.241, URL: htt...
1.0 Enumerated web services
Host: 192.168.32.241, Port: 80
1
5.3 Discovered directory listing
Host: 192.168.32.241, URL: htt...

Tips & Best Practices

Run Pentera routinely whenever any code changes are introduced into your web applications to make sure all defenses are in working order.

Reference & Recommended Resources

- https://cwe.mitre.org/data/definitions/548.html
- https://www.netsparker.com/blog/web-security/disable-directory-listing-web-servers/

DISCLAIMER

Pentera® provides remediation recommendations based on the latest research conducted by the Pentera® research team. The information is provided "as is" for informational purposes only. Pentera® does not assume any responsibility and expressly disclaims any liability for any use of or inability to use the Remediation Wiki articles or any material contained in them, or from any action or decision taken as a result of using them.

The Remediation Wiki offers links to other sites. Pentera® is not responsible for the content of any linked site or any link in a linked site and does not endorse or approve the linked sites.

Net-NTLMv1/v2

Insight

NTLM, or NThashes, are a suite of Microsoft security protocols intended to provide authentication, integrity, and confidentiality to users. They are stored in the Security Account Manager (SAM) database and in the domain controller's `NTDS.dit` database. Here's what an NTLM hash looks like:

```
aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42
                       LM              :           NT
```

Starting with Windows Vista and Windows Server 2008, only the NT hash is stored by default.

Net-NTLMv1

In this protocol, the server authenticates the client by sending an 8-byte random number, the challenge. The client performs an operation involving the challenge and a secret shared between client and server, specifically one of the two password hashes described above. The client returns the 24-byte result of the computation. In fact, in NTLMv1 the computations are usually made using both hashes and both 24-byte results are sent. The server verifies that the client has computed the correct result, and from this infers possession of the secret, and hence the authenticity of the client.

Example for Net-NTLMv1:

```
admin::kNS:338d08f8e26de93300000000000000000000000000000000:9526fb8c23a90751cdd619b6cea564
742e1e4bf33006ba41:cb8086049ec4736c
```

Algorithm:

```
C = 8-byte server challenge, random
K1 | K2 | K3 = LM-Hash|NT-Hash|5-bytes-0
response = DES(K1,C) | DES(K2,C) | DES(K3,C)
```

Net-NTLMv2

This protocol enhances security by adding cliente challenge to the server. This way, the server must receive as part of the response the client challenge. The second response sent by NTLMv2 uses a variable length client challenge which includes (1) the current time inNT Timeformat, (2) an 8-byte random value , (3) the domain name and (4) some standard format stuff. The response must include a copy of this client challenge, and is therefore variable length.

Both client and server challenge with the NT hash of the user's password and other identifying information. The exact formula is to begin with the NT Hash, which is stored in the SAM or AD, and continue to hash in, using HMAC-MD5, the username and domain name.

Example for Net-NTLMv2:

```
admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c783031000000
0000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030
```

Algorithm:

```
SC = 8-byte server challenge, random
CC = 8-byte client challenge, random
CC* = (X, time, CC2, domain name)
v2-Hash = HMAC-MD5(NT-Hash, user name, domain name)
LMv2 = HMAC-MD5(v2-Hash, SC, CC)
NTv2 = HMAC-MD5(v2-Hash, SC, CC*)
response = LMv2 | CC | NTv2 | CC*
```

Impact

NTLM

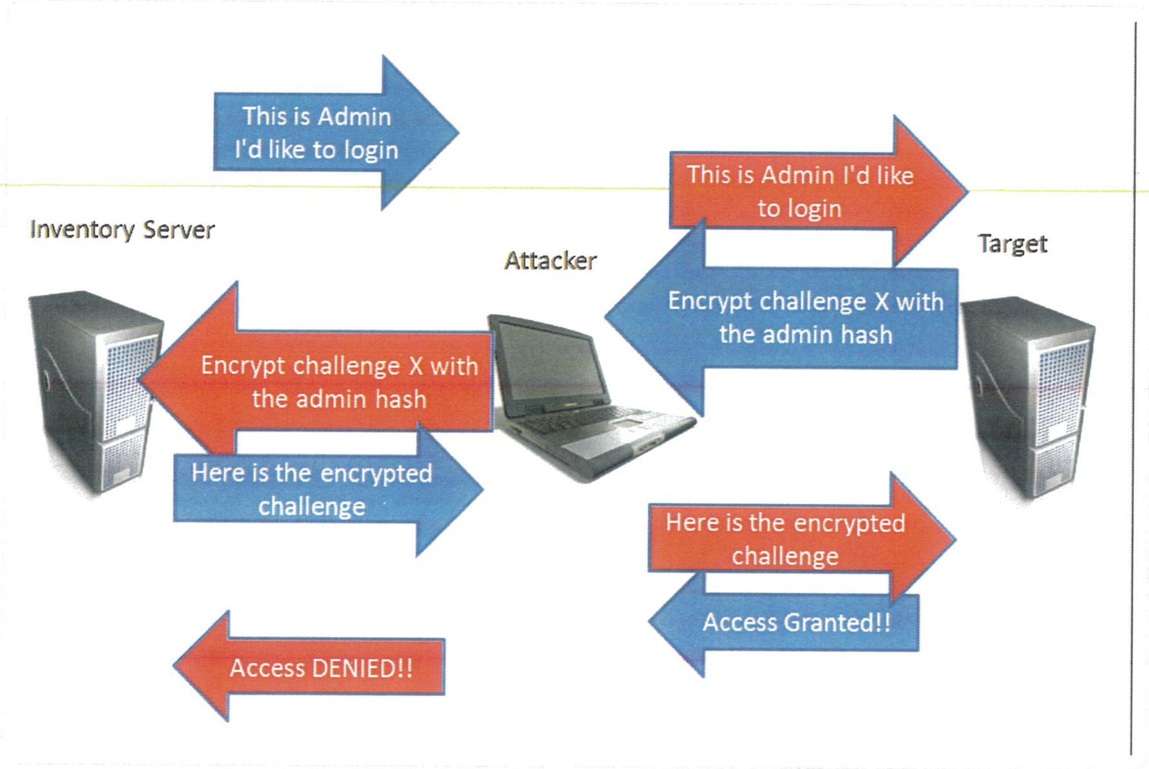
Those can be obtained by dumping the SAM database, or using tools like Mimikatz, and can be used in Pass-The-Hashin under a minute attacks or cracked to get clear-text passwords.

Net-NTLMv1/v2

With Net-NTLMv1 an attacker can send their own challenge, making the cracking relatively easy. A Net-NTLMv1 hash can be cracked in under a minute with free tools that are readily available on the internet and using ready-to-use rainbow tables.

You can get both Net-NTLMv1/v2 hashes when using tools like Responder or Inveigh. While neither type is vulnerable to Pass-The-Hash attacks, they can be used for relay attacks:

- An attacker sitting between the client and a service or a server can intercept their communication, relay the authentication request and use the granted access.
- The Net-NTLM cannot be used back on the same machine (reflective attack), but it is still usable to relay the hash to another machine. Also, it can be relayed "as-is", without the need to crack it.
- With tools like Responder and a relay tool, it can be used to automatically intercept connections and relay authentication hashes.


This is Admin I'd like to login
This is Admin I'd like to login
Inventory Server
Attacker
Target
Encrypt challenge X with the admin hash
Encrypt challenge X with the admin hash
Here is the encrypted challenge
Here is the encrypted challenge
Access Granted!!
Access DENIED!!

Attacking using Net-NTLM hashes

Recommendations

It is recommended to use Kerberos, or at the very least, the Net-NTLMv2 protocol, while the continued use of NTLM or NTLMv1, puts your systems at risk.

If there's a need to support older machines that cannot use NTLMv2:

- Isolate devices that cannot use NTLMv2 as much as possible using a Virtual LAN (VLAN).

- Closely monitor devices that cannot use NTLMv2 but require Interet access for indications of compromise.

It is also improtant to enable SMB signing to prevent relay attacks.

Technical Enforcement

To use a Group Policy Object (GPO) to force Windows to use NTLMv2:

1. Open the Group Policy Management Console.
2. Select the GPO to which you wish to add the setting, or create a new one.
3. Find "Network Security: LAN Manager authentication level", which is located in Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options.
4. Set the LAN Manager authentication level to NTLMv2 response only/refuse LM and NTLM.

To make sure you are on NTLMv2:

- Enable Logon Success Auditing on the domain controller, and then look for **Success Auditing Event 4624**, which contains information about the NTLM version.

  You will receive event logs that resemble the following:

```
Sample Event ID: 4624
Source: Microsoft-Windows-Security-Auditing
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
Description:
An account was successfully logged on.

Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Type: 3

New Logon:
Security ID: ANONYMOUS LOGON
Account Name: ANONYMOUS LOGON
Account Domain: NT AUTHORITY
Logon ID: 0xa2226a
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0x0
Process Name: -

Network Information:
Workstation Name: Workstation1
Source Network Address: <IP address>
Source Port: 49194

Detailed Authentication Information:
Logon Process: NtLmSsp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): NTLM V1
Key Length: 128
```

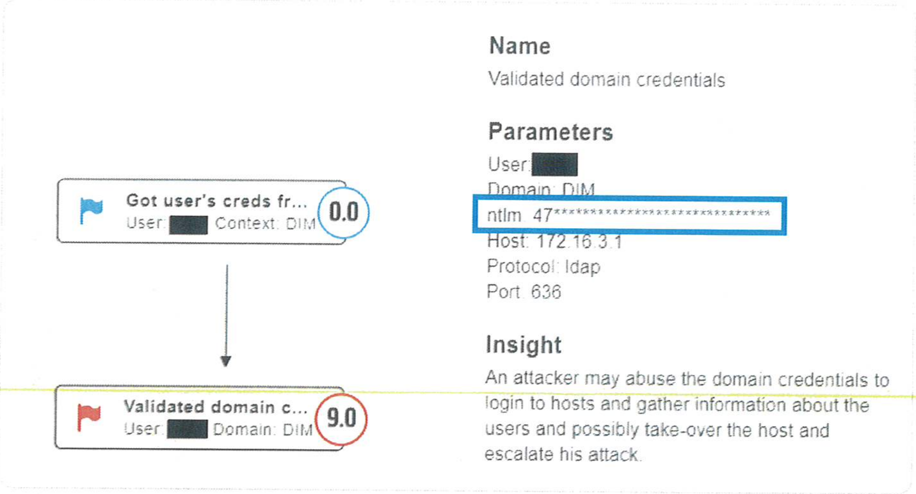
How to use Pentera for validation

You can run a test with Pentera to identify whether your network is vulnerable to pass-the-hash attacks. If the vulnerability was previously found in your network, you can use Pentera to validate that your remediation efforts were successful and the issue has been fixed.

After starting a task, go into User Input and input an NTLM hash. You can use the following Python script to get an NTLM hash:

```
import hashlib,binascii
hash = hashlib.new('md4', "password".encode('utf-16le')).digest()
print binascii.hexlify(hash)
```

If a pass-the-hash attack was performed by Pentera, an achievement with the input will be seen.



Got user's creds fr...
User: [redacted] Context: DIM
0.0

Validated domain c...
User: [redacted] Domain: DIM
9.0

Name

Validated domain credentials

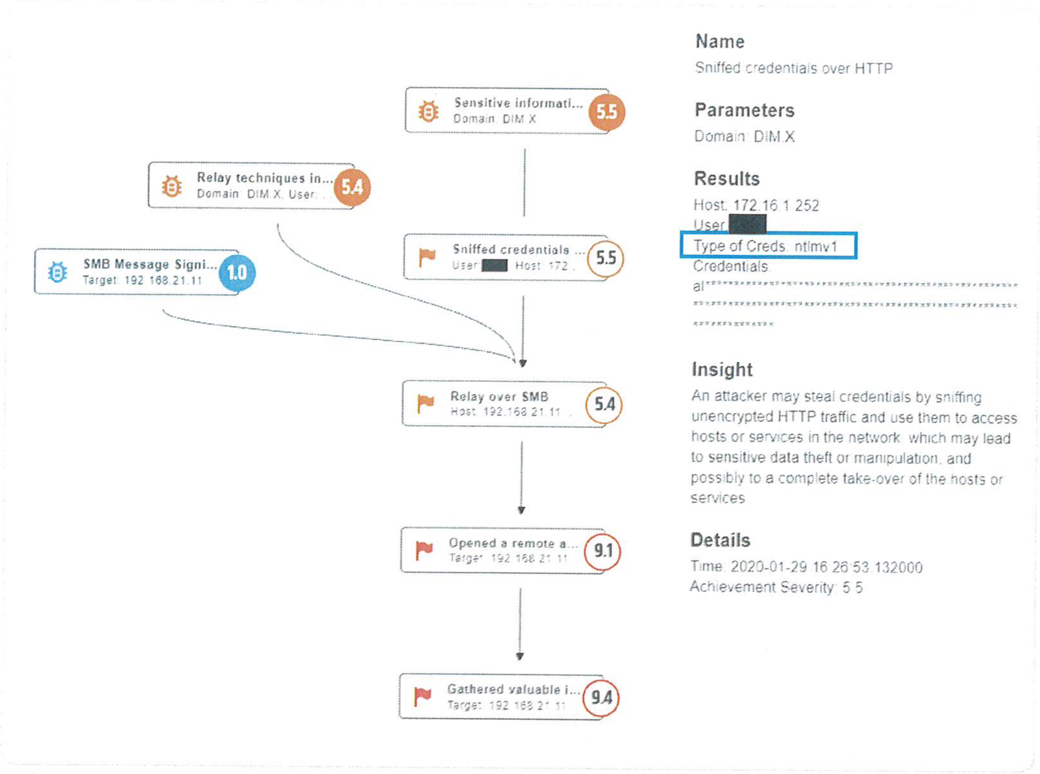
Parameters

User: [redacted]
Domain: DIM
ntlm: 47******************************
Host: 172.16.3.1
Protocol: ldap
Port: 636

Insight

An attacker may abuse the domain credentials to login to hosts and gather information about the users and possibly take-over the host and escalate his attack.

A sample achievement showing results obtained by a pass-the-hash attack


Sensitive informati... Domain: DIM.X 5.5
Relay techniques in... Domain: DIM.X. User: . 5.4
SMB Message Signi... Target: 192.168.21.11 1.0
Sniffed credentials ... User [redacted] Host: 172 . 5.5
Relay over SMB Host: 192.168.21.11 . 5.4
Opened a remote a... Target: 192.168.21.11 9.1
Gathered valuable i... Target: 192.168.21.11 9.4

Name
Sniffed credentials over HTTP

Parameters
Domain: DIM.X

Results
Host: 172.16.1.252
User [redacted]
Type of Creds: ntlmv1
Credentials
al**
****
****

Insight
An attacker may steal credentials by sniffing unencrypted HTTP traffic and use them to access hosts or services in the network, which may lead to sensitive data theft or manipulation, and possibly to a complete take-over of the hosts or services

Details
Time: 2020-01-29 16:26:53.132000
Achievement Severity: 5.5

Example of an attack map showing that Pentera performed relay over NTLMv1

NTLM sniffing with Kerberos:

If after setting Kerberos, Pentera can still find NTML hashes, this is a clear indication that Kerberos was set incorrectly. Reconfigure the policy and retest your network with Pentera.

References and Resources

- About NTLMv1: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-nlmp/464551a8-9fc4-428e-b3d3-bc5bfb2e73a5
- About NTLMv2: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-nlmp/5e550938-91d4-459f-b67d-75d70009e3f3
- NTLMv2 configuration guide: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain
- Guide for identifying which protocl is in use: https://support.microsoft.com/en-ca/help/4090105/how-to-audit-domain-controller-use-of-ntlmv1-and-ntlmv2
- Guide for setting up Kerberos: https://docs.oracle.com/cd/E23941_01/E26092/html/kerberos-auth.html

DISCLAIMER
Pentera® provides remediation recommendations based on the latest research conducted by the Pentera® research team. The information is provided "as is" for informational purposes only. Pentera® does not assume any responsibility and expressly disclaims any liability for any use of or inability to use the Remediation Wiki articles or any material contained in them, or from any action or decision taken as a result of using them.

The Remediation Wiki offers links to other sites. Pentera® is not responsible for the content of any linked site or any link in a linked site and does not endorse or approve the linked sites.

Printer Spooler Service

Insight

The Print Spooler Service software interface controls the order in which documents are printed. It uses the Windows Print System Remote Protocol (MS-RPRN), and is enabled by default on all Windows systems.

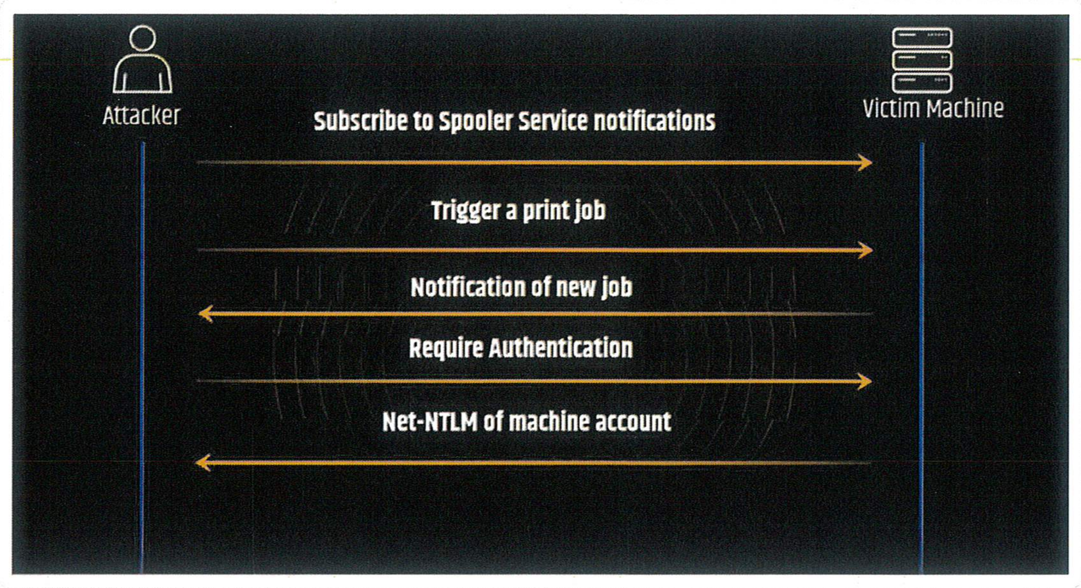
One of the protocol's APIs is `RpcRemoteFindFirstPrinterChangeNotification(Ex)`, which implements both a print client and a print server. Consequently, any Windows machine that has a Printer Spooler Service running can also act as a print server.

The implication is that any client that is a domain user can subscribe to the print server's notifications to learn when new print jobs are created, and any client, regardless of whether it is a member of the domain, can create a new print job.

Using these two features, any client with valid domain credentials can subscribe to notifications from the Spooler Service, and immediately create a new print job, triggering the notification.

The notification is sent to the client, who can ask for Net-NTLM authentication, which the server will deliver using the machine account user.

Attackers can use this vulnerability for NTLM relay attacks and to leverage their position in the organization.



Impact

An attacker with a valid domain credentials can force any Windows machine with the spooler service running to initiate a connection via SMB. Utilizing the Relay technique, an attacker can take advantage of this connection and use that machine's user against any other machine in the network.

This attack can be used against a Domain Controller, an Exchange, or any other host within the domain.

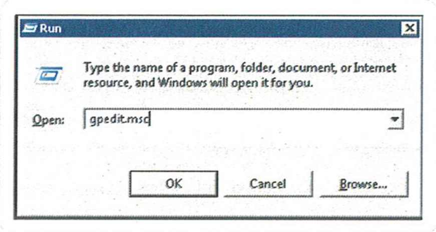
Recommendations

There is no way to prevent the Printer Spooler from implementing the Print Server API. The easiest and best way to prevent this type of attack is to simply disable the service.

If you do not need the Spooler Service server in your organization, we recommend to disable client connections in order to prevent attackers from triggering authentications.

How to disable client connections to the Spooler Service:

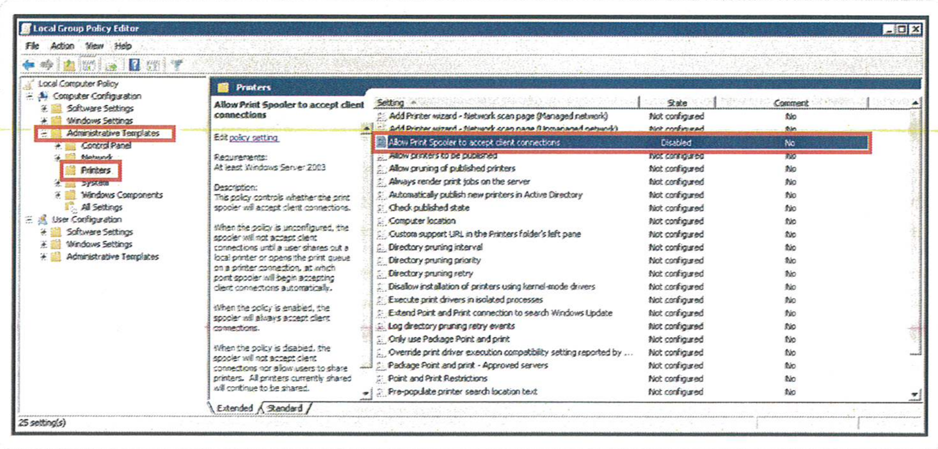
1. Open the Local Group Policy Editor: Go to **Start** → Open **Run** and type `gpedit.msc`.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: gpedit.msc

2. Under **Administrative Templates → Printers**, set the configuration **Allow Print Spooler to accept client connections** to **Disabled**.



Allow Print Spooler to accept client connections

Edit policy setting

Requirements:
At least Windows Server 2003

Description:
This policy controls whether the print spooler will accept client connections.

When the policy is unconfigured, the spooler will not accept client connections until a user shares out a local printer or opens the print queue on a printer connection, at which point spooler will begin accepting client connections automatically.

When the policy is enabled, the spooler will always accept client connections.

When the policy is disabled, the spooler will not accept client connections nor allow users to share printers. All printers currently shared will continue to be shared.

Setting	State	Comment
Add Printer wizard - Network scan page (Managed network)	Not configured	No
Add Printer wizard - Network scan page (Unmanaged network)	Not configured	No
Allow Print Spooler to accept client connections	Disabled	No
Allow printers to be published	Not configured	No
Allow pruning of published printers	Not configured	No
Always render print jobs on the server	Not configured	No
Automatically publish new printers in Active Directory	Not configured	No
Check published state	Not configured	No
Computer location	Not configured	No
Custom support URL in the Printers folder's left pane	Not configured	No
Directory pruning interval	Not configured	No
Directory pruning priority	Not configured	No
Directory pruning retry	Not configured	No
Disallow installation of printers using kernel-mode drivers	Not configured	No
Execute print drivers in isolated processes	Not configured	No
Extend Point and Print connection to search Windows Update	Not configured	No
Log directory pruning retry events	Not configured	No
Only use Package Point and print	Not configured	No
Override print driver execution compatibility setting reported by ...	Not configured	No
Package Point and print - Approved servers	Not configured	No
Point and Print Restrictions	Not configured	No
Pre-populate printer search location text	Not configured	No

3. If you are in an Active Directory environment, we recommend enforcing this policy for all hosts in the domain.

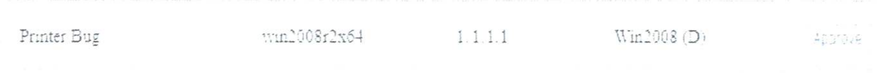
   However, if this is not an option, it is advisable to manually lower the permissions of the privileged machine users, such as those of the Exchange and Domain Controller.

How to use Pentera for validation

You can run a quick test with Pentera to identify machines that are vulnerable to the exploit or validate that the vulnerability does not exist in your environment. If the vulnerability was previously found in your network, you can use Pentera to validate that your remediation efforts were successful and the issue has been fixed.

Create a new What-if Testing Scenario and provide credentials for a low privileges domain user and configure it to require approvals. Run the test.

If an approval for **Printer Bug** appears, it is an indication that the Spooler Service is open on the host. Approving this action will initiate the Printer Bug action, which checks the Spooler Service exploit.



Printer Bug	win2008r2x64	1.1.1.1	Win2008 (D)	Approve

References and Resources

- Print System Remote Protocol by Microsoft
- Print Spooler Service by Microsoft

DISCLAIMER
Pentera® provides remediation recommendations based on the latest research conducted by the Pentera® research team. The information is provided "as is" for informational purposes only. Pentera® does not assume any responsibility and expressly disclaims any liability for any use of or inability to use the Remediation Wiki articles or any material contained in them, or from any action or decision taken as a result of using them.

The Remediation Wiki offers links to other sites. Pentera® is not responsible for the content of any linked site or any link in a linked site and does not endorse or approve the linked sites.