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 to simulate a realistic corporate network segment.

Network Infrastructure

- **Domain Name:** `TAROT.fool`
- **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
Fors1	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

2. Attack Methodology and Results

2.1 LLMNR/NBT-NS Poisoning

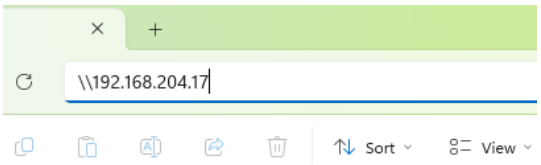
Description

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

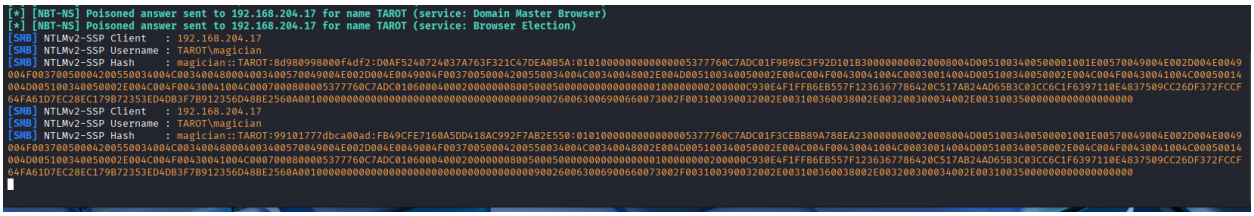
- Trigger: User attempted to browse \\<non-existent share>



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

Evidence

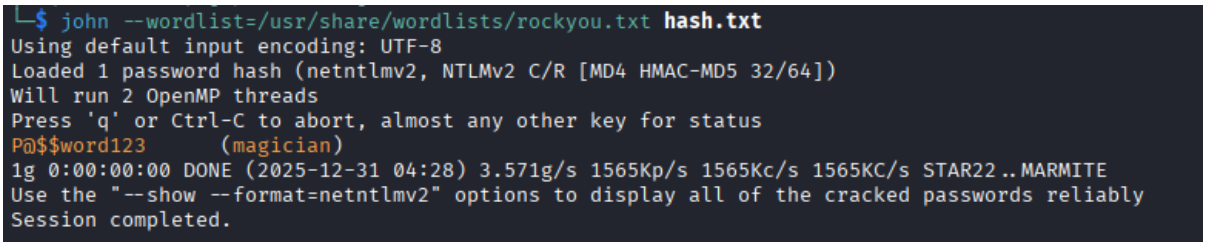
- Successfully intercepted NTLMv2 challenge-response authentication
- Example captured credential:



- Confirmed NTLMv2 format and integrity

Impact

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



- 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