NTLM Relay Attack - Lab Investigation Report

Investigator: Natasha

Date: April 11, 2025

Lab Title: NTLM Relay Attack and Post-Event Forensics

1. Objective

The objective of this lab was to understand and execute a simulated NTLM relay attack in a controlled environment. Following the attack, forensic investigation techniques were applied to identify the attack vector, determine the details of the logon session, and extract indicators of compromise from Windows event logs.

2. Lab Environment

- Host System: Windows (IP: 192.168.1.12)
- Attacker System: Kali Linux VM running on VirtualBox (IP: 192.168.1.13)
- Tools Used:
  - Responder
  - Impacket-ntlmrelayx
  - EVTXtract + Grep
  - Custom Bash scripts for log filtering

3. Attack Execution Summary

Step 1: Network Configuration

- Configured VirtualBox network to Bridged Adapter mode.
- Enabled promiscuous mode for VM.
- Verified bi-directional ping between host and VM.

Step 2: Running Responder

- Started Responder on Kali VM:

```
  sudo responder -I eth0
```

- Responder began poisoning LLMNR and mDNS traffic on the local network.

Step 3: NTLM Relay with Impacket

- Launched NTLM relay listener:

```
  impacket-ntlmrelayx -tf targets.txt -smb2support
```

- Responder captured authentication requests and relayed them to the target via NTLM relay.

4. Forensic Analysis

Log Collection

- Extracted Windows Event Logs in `.evtx` format.

- Converted to text using `EVTXtract`.

Key Logon Event Identified

- Event ID: 4624 (Successful Logon)

- Target User Name: arthur.kyle

- Logon Type: 3 (Network Logon)

- Logon ID: 0x0000000000651ad0

- Time of Logon (UTC): 2024-07-31 04:55:16.240589

- Source IP: Identified from IPAddress field

Share Accessed

- The malicious tool accessed the IPC$ share using relayed credentials.

5. Indicators of Compromise (IOCs)

- Suspicious logon with Type 3 from unexpected IP

- Use of SYSTEM account to launch `services.exe`

- Access to IPC$ share shortly after logon

6. Conclusion

This lab successfully demonstrated an NTLM relay attack against a Windows host. By using Responder and impacket's ntlmrelayx tool, credentials were intercepted and reused to authenticate to a remote share. The post-attack forensic analysis highlighted how such attacks can be detected via Event ID 4624, LogonType, LogonID, and network-related fields like IpAddress and IpPort.

7. Recommendations

- Disable LLMNR and NetBIOS on the network

- Enforce SMB signing

- Use Kerberos over NTLM whenever possible

- Monitor Event ID 4624 for anomalous network logon activity