PosioningCreeeedentials

Category: Network Forensics
Difficulty: Easy
Date Completed: 2025-04-29

🔍 Summary

This lab demonstrates an internal network attack leveraging NBNS and LLMNR poisoning to capture or relay Net-NTLMv2 hashes from victim machines. The attacker exploited user typos to respond to name resolution requests with rogue IPs, then initiated SMB protocol negotiations to steal authentication credentials. The analyst's goal was to trace the poisoning attempts, identify the rogue IP, compromised user, and affected systems.

🔄 Timeline of Events

- **20:27:45** — Victim (192.168.232.162) queries `FILESHAARE<20>` via NBNS (typo)
- **20:27:45** — Attacker (192.168.232.215) responds with a forged address
- **20:30:40** — Victim (192.168.232.176) queries `CYBERCACTUS<1B>`, triggering another NBNS poisoning attempt
- **20:30:40** — Legitimate system (192.168.232.148) responds, but conflict occurs
- **20:30:45** — Victim queries non-existent `PRINETR<20>`
- **20:30:45** — Attacker responds via mDNS and starts communication
- **20:33:09** — Attacker begins SMB negotiation with victim (192.168.232.176)
- **20:33:09** — NTLM authentication handshake occurs; victim sends credentials for `janesmith`
- **20:33:09** — Attacker gains unauthorized access to target system: `ACCOUNTINGPC`

🔧 Technical Walkthrough

- **Tools Used**: Wireshark
- **Artifacts Found**:
  - NBNS queries for mistyped resources (e.g., `FILESHAARE`, `PRINETR`)
  - mDNS/NBNS spoofing by 192.168.232.215
  - NTLMSSP authentication revealing compromised user
  - SMB Session Setup attempts showing hostname accessed
- **IOCs**:

- Attacker IP: `192.168.232.215`
- Compromised User: `janesmith`
- Targeted Host: `ACCOUNTINGPC`

🧹 MITRE Mapping

- **Credential Access**: T1557.001 - Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning
- **Collection**: T1039 - Data from Network Shared Drive

🤔 Lessons Learned

- **What surprised me?** How exploitable these legacy protocols are and that they still exist in modern networks. I now understand why LLMNR/NBT-NS are dangerous despite being local.
- **What would I do differently?** I would trace all victim responses quicker by grouping by poisoned response targets.
- **Which new tool or concept did I master?** Learned how to trace NTLMSSP authentication flows in SMB to reveal usernames and hostnames.

🧠 Thought Process for Each Question

Q1:

In the context of the incident described in the scenario, the attacker initiated their actions by taking advantage of benign network traffic from legitimate machines. Can you identify the specific mistyped query made by the machine with the IP address 192.168.232.162?

Filtered:

```
ip.addr == 192.168.232.162
```

This shows:

51	74.355657	192.168.232.215	192.168.232.162	NBNS	104	Name query response NB 192.168.232.215
52	74.356170	192.168.232.162	224.0.0.252	LLMNR	70	Standard query 0xaeb2 A fileshaare
53	74.356581	192.168.232.162	224.0.0.252	LLMNR	70	Standard query 0x2ead AAAA fileshaare
54	74.359127	192.168.232.215	192.168.232.162	MDNS	98	Standard query response 0x0000 AAAA fe80::c0a9:714f:8ea7:3313
55	74.360087	192.168.232.215	192.168.232.162	LLMNR	96	Standard query response 0xaeb2 A fileshaare A 192.168.232.215
56	74.364501	192.168.232.215	192.168.232.162	LLMNR	108	Standard query response 0x2ead AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
57	74.367825	192.168.232.162	192.168.232.148	TCP	66	51878 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

This confirms that the victim mistyped `fileshare` as `fileshaare`, and `192.168.232.215` (attacker) pretended to be that host.

Q2:

We are investigating a network security incident. To conduct a thorough investigation, we need to determine the IP address of the rogue machine. What is the IP address of the machine acting as the rogue entity?

As mentioned above, `192.168.232.215` is the rogue machine — it answered spoofed NBNS/LLMNR queries.

Q3:

As part of our investigation, identifying all affected machines is essential. What is the IP address of the second machine that received poisoned responses from the rogue machine?

Filter:

```
ip.addr == 192.168.232.215 and (udp.port == 5355 or udp.port == 137)
```

ip.addr == 192.168.232.215 and (udp.port == 5355 or udp.port == 137)

No.	Time	Source	Destination	Protocol	Length	Info
51	74.355657	192.168.232.215	192.168.232.162	NBNS	104	Name query response NB 192.168.232.215
55	74.360087	192.168.232.215	192.168.232.162	LLMNR	96	Standard query response 0xaeb2 A fileshaare A 192.168.232.215
56	74.364501	192.168.232.215	192.168.232.162	LLMNR	108	Standard query response 0x2ead AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
71	74.409394	192.168.232.215	192.168.232.162	LLMNR	96	Standard query response 0x61e8 A fileshaare A 192.168.232.215
72	74.413998	192.168.232.215	192.168.232.162	LLMNR	108	Standard query response 0x9b15 AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
79	74.422420	192.168.232.215	192.168.232.162	LLMNR	96	Standard query response 0xb281 A fileshaare A 192.168.232.215
80	74.426719	192.168.232.215	192.168.232.162	LLMNR	108	Standard query response 0x6108 AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
87	74.441497	192.168.232.215	192.168.232.162	LLMNR	96	Standard query response 0xc4a3 A fileshaare A 192.168.232.215
88	74.445950	192.168.232.215	192.168.232.162	LLMNR	108	Standard query response 0x1ce7 AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
145	249.286604	192.168.232.215	192.168.232.176	NBNS	104	Name query response NB 192.168.232.215
146	249.286609	192.168.232.176	192.168.232.215	NBNS	104	Registration response, Name is in conflict NB 192.168.232.148
152	250.280521	192.168.232.215	192.168.232.176	NBNS	104	Name query response NB 192.168.232.215
153	250.280526	192.168.232.176	192.168.232.215	NBNS	104	Registration response, Name is in conflict NB 192.168.232.148
157	251.281828	192.168.232.215	192.168.232.176	NBNS	104	Name query response NB 192.168.232.215
158	251.281834	192.168.232.176	192.168.232.215	NBNS	104	Registration response, Name is in conflict NB 192.168.232.148
161	252.282406	192.168.232.215	192.168.232.176	NBNS	104	Name query response NB 192.168.232.215
167	254.178176	192.168.232.215	192.168.232.176	NBNS	104	Name query response NB 192.168.232.215
171	254.182306	192.168.232.215	192.168.232.176	LLMNR	90	Standard query response 0x4a65 A prinetr A 192.168.232.215
172	254.186728	192.168.232.215	192.168.232.176	LLMNR	102	Standard query response 0x5ae5 AAAA prinetr AAAA fe80::c0a9:714f:8ea7:3313
187	254.233162	192.168.232.215	192.168.232.176	LLMNR	90	Standard query response 0x3188 A prinetr A 192.168.232.215
188	254.237206	192.168.232.215	192.168.232.176	LLMNR	102	Standard query response 0x567d AAAA prinetr AAAA fe80::c0a9:714f:8ea7:3313
195	254.247641	192.168.232.215	192.168.232.176	LLMNR	90	Standard query response 0x02c2 A prinetr A 192.168.232.215
196	254.251873	192.168.232.215	192.168.232.176	LLMNR	102	Standard query response 0xb232 AAAA prinetr AAAA fe80::c0a9:714f:8ea7:3313
203	254.260139	192.168.232.215	192.168.232.176	LLMNR	90	Standard query response 0x85e5 A prinetr A 192.168.232.215
204	254.262949	192.168.232.215	192.168.232.176	LLMNR	102	Standard query response 0xd22d AAAA prinetr AAAA fe80::c0a9:714f:8ea7:3313

Or more directly:

```
nbns.addr == 192.168.232.215
```

nbns.addr == 192.168.232.215

No.	Time	Source	Destination	Protocol	Length	Info
51	2023-10-21 20:27:45.449772	192.168.232.215	192.168.232.162	NBNS	104	Name query response NB 192.168.232.215
145	2023-10-21 20:30:40.380719	192.168.232.215	192.168.232.176	NBNS	104	Name query response NB 192.168.232.215
152	2023-10-21 20:30:41.374636	192.168.232.215	192.168.232.176	NBNS	104	Name query response NB 192.168.232.215
157	2023-10-21 20:30:42.375943	192.168.232.215	192.168.232.176	NBNS	104	Name query response NB 192.168.232.215
161	2023-10-21 20:30:43.376521	192.168.232.215	192.168.232.176	NBNS	104	Name query response NB 192.168.232.215
167	2023-10-21 20:30:45.272291	192.168.232.215	192.168.232.176	NBNS	104	Name query response NB 192.168.232.215

Answer: **192.168.232.176**

From what I'm seeing:

- NBNS is first to ask who is `FILESHAARE`
- Rogue answers
- Victim falls back to LLMNR
- A and AAAA queries are now used from LLMNR, like a two-stage authentication

For example, `192.168.232.176` queried `CYBERCACTUS<1B>`. There is a conflict detected with `192.168.232.148`.

So the legit answers fail, only the rogue can answer eventually.

Victim falls back to LLMNR after NBNS fails to return valid results.

Bonus: What is `<1B>`?

Code	Meaning	Use Case
`<20>`	File Server Service	Used to access `\\HOST\share`
`<1B>`	Domain Master Browser	Lets clients locate the domain controller (PDC)
`<1E>`	Browser Service Elections	Used during "Master Browser" elections and announcements

If multiple `<1B>` responses appear, it's a strong sign of NetBIOS poisoning or name spoofing.

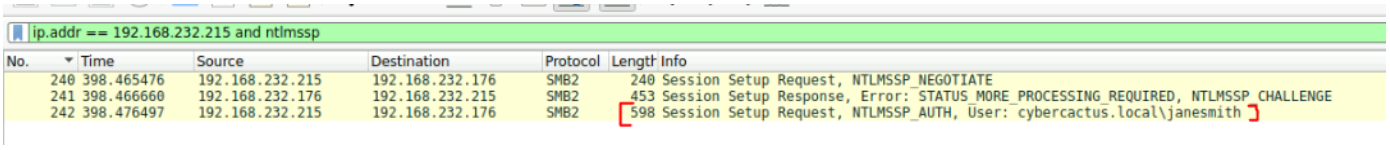
Q4:

We suspect that user accounts may have been compromised. To assess this, we must determine the username associated with the compromised account. What is the username of the account that the attacker compromised?

Best approach:

```
ip.addr == 192.168.232.215 and ntlmssp
```

Because NTLMSSP reveals credentials during SMB authentication.



Here's the NTLM handshake:

- `192.168.232.215` requests resource from `192.168.232.176`
- `192.168.232.176` responds with a challenge

```
Security Blob [truncated]: a182013f3082013ba003…
▾ GSS-API Generic Security Service Application Program Interface
  ▾ Simple Protected Negotiation
    ▾ negTokenTarg
        negResult: accept-incomplete (1)
        supportedMech: 1.3.6.1.4.1.311.2.2.10 (NTLMSSP - Microsoft NTLM Security Support Provider)
        responseToken [truncated]: 4e544c4d5353500002000000160016003800000358289e2c8eb5e4b7c037617000000000000…
      ▾ NTLM Secure Service Provider
          NTLMSSP identifier: NTLMSSP
          NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
        ▸ Target Name: CYBERCACTUS
        ▸ Negotiate Flags: 0xe2898235, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negotiate Version, N
          NTLM Server Challenge: c8eb5e4b7c037617
          Reserved: 0000000000000000
        ▸ Target Info
        ▸ Version 10.0 (Build 19041); NTLM Current Revision 15
```

Then:

240	398.465476	192.168.232.215	192.168.232.176	SMB2	240 Session Setup Request, NTLMSSP_NEGOTIATE
241	398.466660	192.168.232.176	192.168.232.215	SMB2	453 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
242	398.476497	192.168.232.215	192.168.232.176	SMB2	598 Session Setup Request, NTLMSSP_AUTH, User: cybercactus.local\janesmith
250	398.591702	192.168.232.176	192.168.232.215	SMB2	139 Session Setup Response
251	398.603950	192.168.232.215	192.168.232.176	SMB2	230 Encrypted SMB3
252	398.605390	192.168.232.176	192.168.232.215	SMB2	190 Encrypted SMB3
257	398.618720	192.168.232.215	192.168.232.176	SMB2	178 Encrypted SMB3
258	398.619076	192.168.232.176	192.168.232.215	SMB2	178 Encrypted SMB3

Attacker responds with the username **janesmith**.

You'll also see:

- `STATUS_MORE_PROCESSING_REQUIRED`: indicates NTLM is in progress
- Encrypted SMB data following successful authentication

Answer: `janesmith`

Q5:

As part of our investigation, we aim to understand the extent of the attacker's activities. What is the hostname of the machine that the attacker accessed via SMB?

Again:

```
ip.addr == 192.168.232.215 and ntlmssp
```

Check the target info for hostname:

No.	Time	Source	Destination	Protocol	Length	Info
240	398.465476	192.168.232.215	192.168.232.176	SMB2	240	Session Setup Request, NTLMSSP_NEGOTIATE
241	398.466660	192.168.232.176	192.168.232.215	SMB2	453	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
242	398.476497	192.168.232.215	192.168.232.176	SMB2	598	Session Setup Request, NTLMSSP_AUTH, User: cybercactus.local\janesmith

```
Reserved: 0000000000000000
▾ Target Info
    Length: 210
    Maxlen: 210
    Offset: 78
  ▸ Attribute: NetBIOS domain name: CYBERCACTUS
  ▾ Attribute: NetBIOS computer name: ACCOUNTINGPC
      Target Info Item Type: NetBIOS computer name (0x0001)
      Target Info Item Length: 24
      NetBIOS Computer Name: ACCOUNTINGPC
  ▸ Attribute: DNS domain name: cybercactus.local
  ▸ Attribute: DNS computer name: AccountingPC.cybercactus.local
  ▸ Attribute: DNS tree name: cybercactus.local
  ▸ Attribute: Timestamp
  ▸ Attribute: End of list
▾ Version 10.0 (Build 19041); NTLM Current Revision 15
    Major Version: 10
```

Answer: `ACCOUNTINGPC`