1. Lab Title & Source

Poisoned Credentials - CyberDefenders

---

2. Objective

State what you were trying to learn or prove.
Example:

> Analyze captured network traffic to identify suspicious activity, extract IOCs, and simulate SOC alert triage.

---

3. Tools & Technologies Used

List all tools (include versions if possible).

- **Wireshark** – For PCAP analysis, protocol filtering, and extracting artifacts.
- **LLMNR/NBT-NS Analysis Filters** – To identify poisoning attempts.
- **SMB Protocol Analysis** – To detect authentication attempts and credential capture.
- **MITRE ATT&CK Framework** – To classify and document adversary TTPs.

Scenario Summary

> Investigate a suspected case of credential theft through network traffic analysis. Identify the attacker's machine, victims, method of compromise, and credentials captured, while mapping activity to the MITRE ATT&CK framework.

---

5. Methodology / Steps Taken

1. **Loaded the provided PCAP** into Wireshark for packet analysis.
2. **Applied filters** for `llmnr` and `nbns` to identify suspicious name resolution requests.

3. Detected a **mistyped hostname query** (`fileshaare`) coming from victim IP `192.168.232.162`.

4. Identified a **rogue responder** (`192.168.232.215`) answering with a forged response.

5. **Correlated network activity** to find a second victim (`192.168.232.176`) receiving the same rogue responses.

6. Filtered for `smb` traffic to **inspect authentication attempts** following the poisoning.

7. Extracted **compromised username** (`janesmith`) and **compromised host** (`ACCOUNTINGPC`) from SMB session data.

8. Mapped the activity to **MITRE ATT&CK** techniques:

    a. **T1557.001** – LLMNR/NBT-NS Poisoning

    b. **T1078** – Valid Accounts

    c. **T1210** – Exploitation of Remote Services

9. Documented all **IOCs** (attacker IP, victim IPs, compromised account, poisoned hostname) for reporting.

---

6. Findings & IOCs

- **Mistyped Query Detected**
  The victim machine (192.168.232.162) issued a query for "`fileshaare`" (incorrect spelling), which triggered the attack opportunity.

- **Rogue Machine Identified**
  The malicious responder, not a legitimate DNS, was located at **192.168.232.215**, answering the poisoned query.

- **Additional Victim Found**
  A second victim machine that also received poisoned responses was identified: **192.168.232.176**.

- **Compromised User Credentials**
  An SMB session included the username **janesmith**, indicating account

compromise.

- **Compromised Hostname**
 The attacker accessed the machine with the hostname **ACCOUNTINGPC** via SMB.

---

7. Skills Demonstrated

- **PCAP & Protocol Analysis** – Filtering and analyzing LLMNR, NBT-NS, and SMB traffic.
- **Rogue Host Identification** – Pinpointing attacker IPs and distinguishing them from legitimate network devices.
- **Credential Harvesting Detection** – Extracting compromised usernames and related hostnames from authentication traffic.
- **Incident Scoping** – Identifying multiple affected hosts and assessing the breadth of compromise.
- **Threat Intelligence Mapping** – Aligning observed behavior with MITRE ATT&CK techniques (T1557.001, T1078, T1210).
- **Forensic Reporting** – Documenting the investigative process and key findings in a structured manner for escalation.