Conestoga College	
Course	**INFO8965: Computer and Network Security**
Activity	**Vulnerability Assessment**
Student Name	**Twinkle Akhilesh Mishra**
Date performed	**24-March-2025**

Objectives

- Develop skills in vulnerability assessment using Kali Linux tools.

Resources

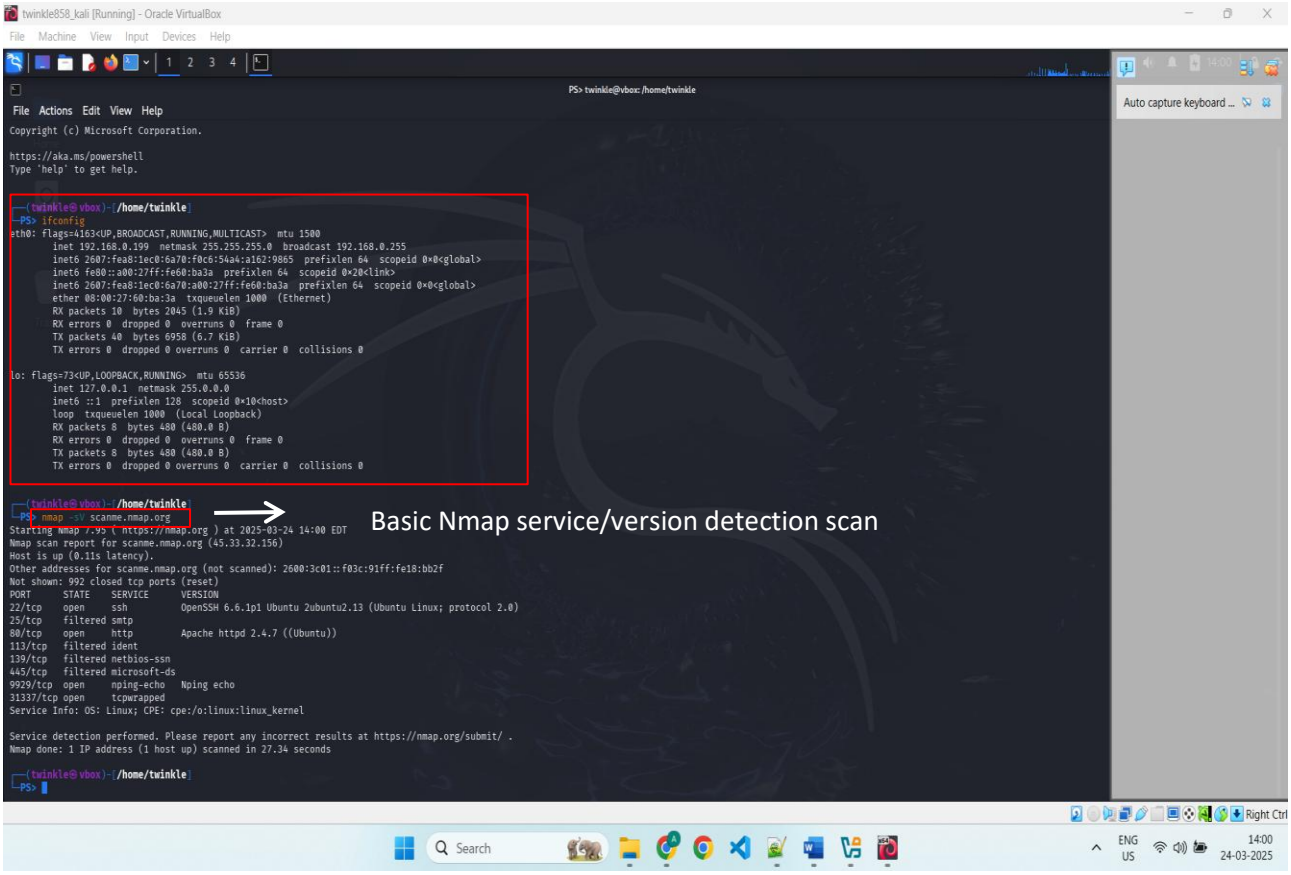
- Hardware: PC/Laptop
  - Software: `nmap, nikto, lynis, Metasploit (Pre-installed tools in Kali Linux)`

(A) Network Scanning with Nmap [3 marks]

✓ Output #1 – Network Scanning and Port Detection using Nmap

- When you scan a network, you look for active devices, open ports, and services that are working on it.It is an important part of vulnerability review because it helps find places where attackers might break in. By scanning a target system, security analysts may identify outdated services, misconfigured systems, or open ports that shouldn't be exposed.
  - Open the command terminal and identify the IP address of your local machine by typing: **Ifconfig**
  - Chosen `scanme.nmap.org` as a target for your scan.

- The IP address of the local Kali Linux machine is **192.168.0.199** (assigned to interface eth0). This confirms the system is properly connected to a network, which is a required step before running external scans.

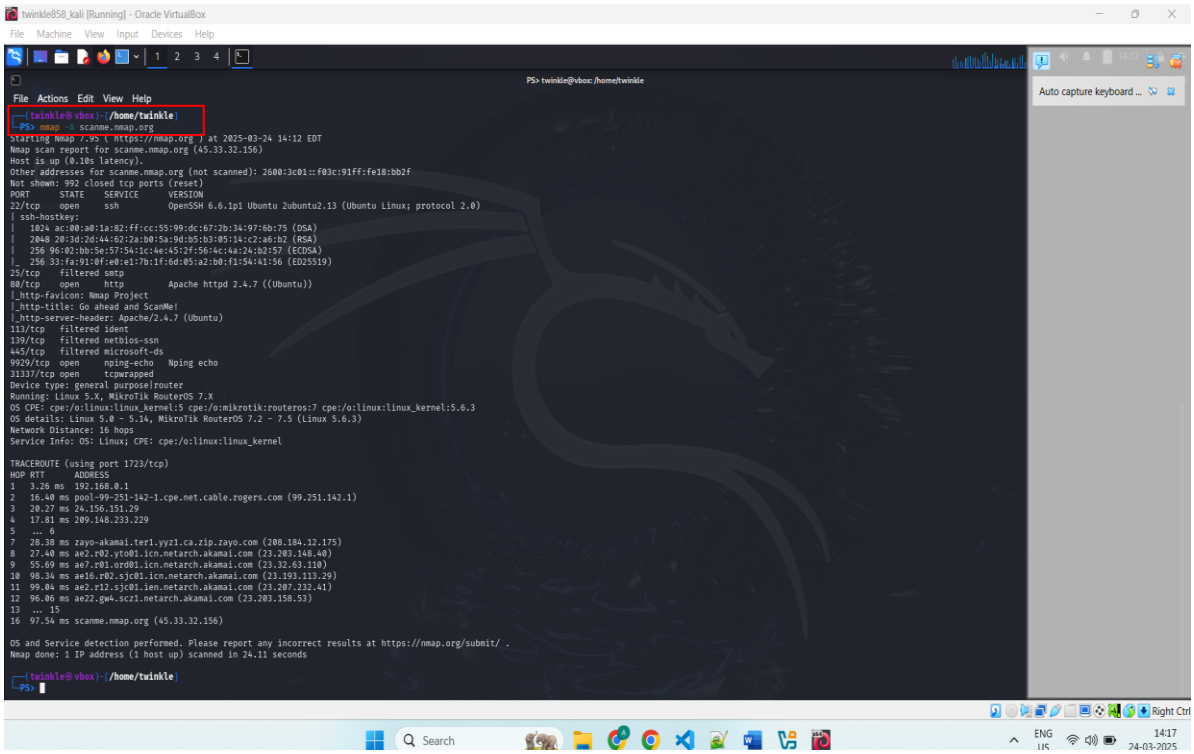


Port	State	Service	Version
22	open	ssh	OpenSSH 6.6.1p1 (Ubuntu 2ubuntu2.13)
80	open	http	Apache httpd 2.4.7 (Ubuntu)
9929	open	nping-echo	Nping echo
31337	open	tcpwrapped	Possibly protected or filtered service

- **Basic network scans** (Output#1 : part A):
  - The basic Nmap scan revealed several open ports including **SSH (22)**, **HTTP (80)**, **Nping Echo (9929)**, and a **tcpwrapped service (31337)**.
  - These ports show that the server is actively hosting services, with Apache web server and SSH access exposed to the internet. While SSH and HTTP are common, the Apache version (2.4.7) is outdated and could have known exploits.
  - Ports like 9929 and 31337 are unusual and could indicate either testing services or protected services hidden behind security wrappers. This information is valuable for identifying potential entry points during a vulnerability assessment.

- **Aggressive network scans** (Output#1 : part B):
  - In this part of the lab, I performed an aggressive scan on the target scanme.nmap.org using the command:
  - **nmap -A scanme.nmap.org**
  - This scan provides more detailed information, including OS detection, service versions, script results, and traceroute.
  - The use of tcpwrapped suggests some services may be protected by access controls or hidden behind filtering mechanisms.

Port	State	Service	Version
22	open	SSH	OpenSSH 6.6.1p1 (Ubuntu)
80	open	HTTP	Apache httpd 2.4.7 (Ubuntu)
9929	open	nping-echo	Nping Echo
31337	open	tcpwrapped	Protected/obscured service



Nmap aggressive scan showing open ports and detected services.

- **SSH Host Keys**: Four fingerprint types (DSA, RSA, ECDSA, ED25519) are shown, verifying it's a real SSH service. These are useful for confirming authenticity but can be outdated.
- **HTTP Title**: The web server displays the message: “Go ahead and ScanMe!” which confirms the site is meant for testing.
- **Device Type**: General-purpose router
- **Operating System**: Detected as **Linux 5.X**, more specifically **MikroTik RouterOS 7.X**, which runs on Linux kernel 5.6.3.
- **Traceroute**: Shows the path of 16 hops between my Kali Linux machine and the scanme.nmap.org server.
- **Potential Vulnerabilities Suggested:**

a. **Apache/2.4.7 (Ubuntu)** is outdated and may contain multiple vulnerabilities depending on configuration (e.g., denial of service, directory traversal).

b. **OpenSSH 6.6.1p1** is also an older version — depending on its configuration, it may allow insecure algorithms or suffer from legacy protocol issues.

c. **Port 31337 (tcpwrapped)** is often associated with hidden or protected services. It could indicate a hardened service, or possibly even a decoy or backdoor service for testing.

d. **No SSL/TLS detected on web server**, meaning all HTTP traffic is likely in plain text, making it vulnerable to sniffing or man-in-the-middle attacks.

Conclusion:

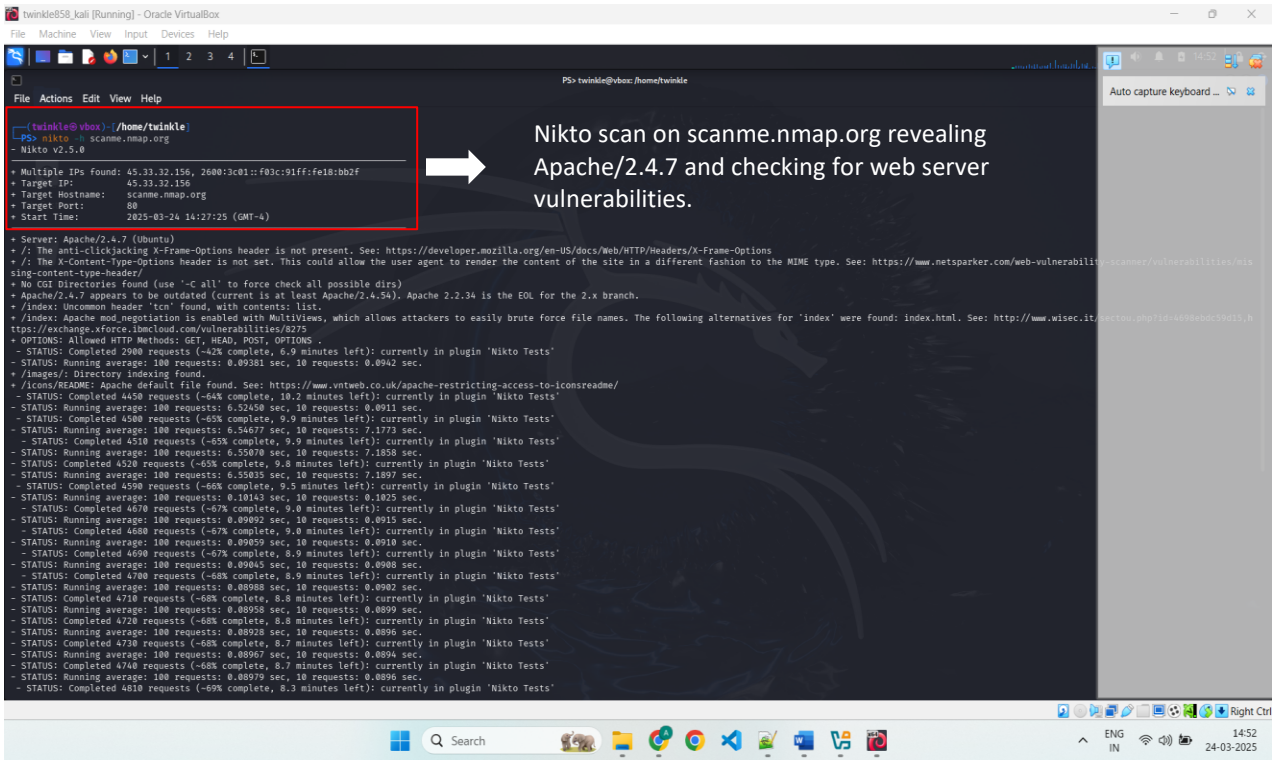
The aggressive Nmap scan provides a better picture of the target system’s security posture. The outdated Apache and OpenSSH versions should be reviewed for known CVEs. Port 31337’s presence suggests the server may have additional services intentionally obscured. Overall, this scan helps identify which services and versions may need further testing with tools like Nikto or Metasploit.

(B) Web vulnerability assessment using Nikto [3 marks]

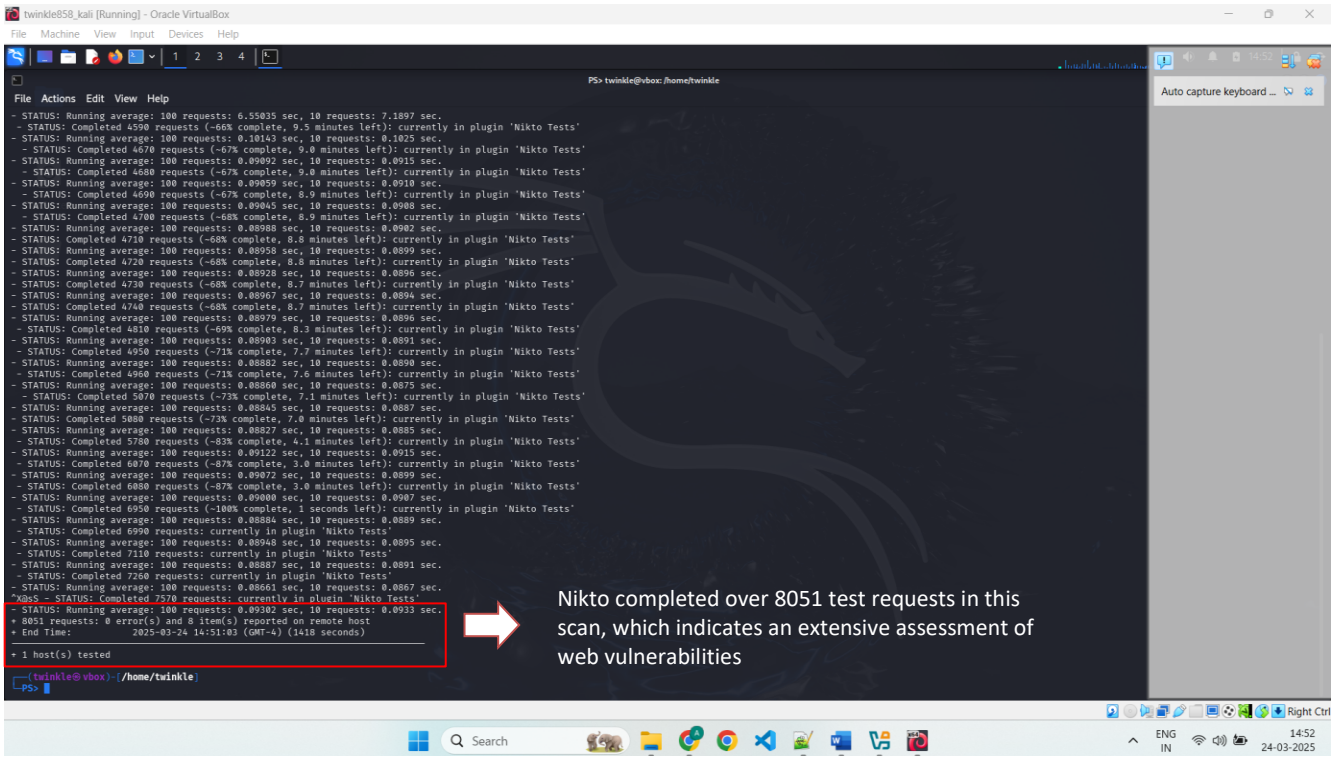
✓ **Output #2 – Web Vulnerability Assessment using Nikto**

- **Nikto** is an open-source web server vulnerability detector. It scans a website for out-of-date software, malicious files, unsecured headers, and typical configuration errors. It's particularly handy in ethical hacking because it instantly identifies potential security flaws in publicly accessible web servers.

- **Scanning for Web Vulnerabilities**:
  - Using Nikto to identify any web-based vulnerabilities:
    nikto -h scanme.nmap.org



Nikto scan showing Apache version and missing headers



Vulnerability / Warning	Explanation	Suggested Fix
Apache default files found (/icons/README)	Default files can give attackers clues about the web server and its directory structure.	Remove or restrict access to default/test directories.
Outdated Apache version (2.4.7)	Older versions may be affected by multiple known CVEs (bugs, exploits).	Update to the latest Apache release and apply patches.
Missing security headers (e.g., X-Frame-Options, Content-Security-Policy)	Without proper headers, the site is vulnerable to clickjacking, MIME sniffing, etc.	Configure Apache to include recommended HTTP security headers.
Web root may expose sensitive files or structure	Overly permissive directory access can lead to exposure of sensitive files.	Use .htaccess rules or server config to deny directory listing.

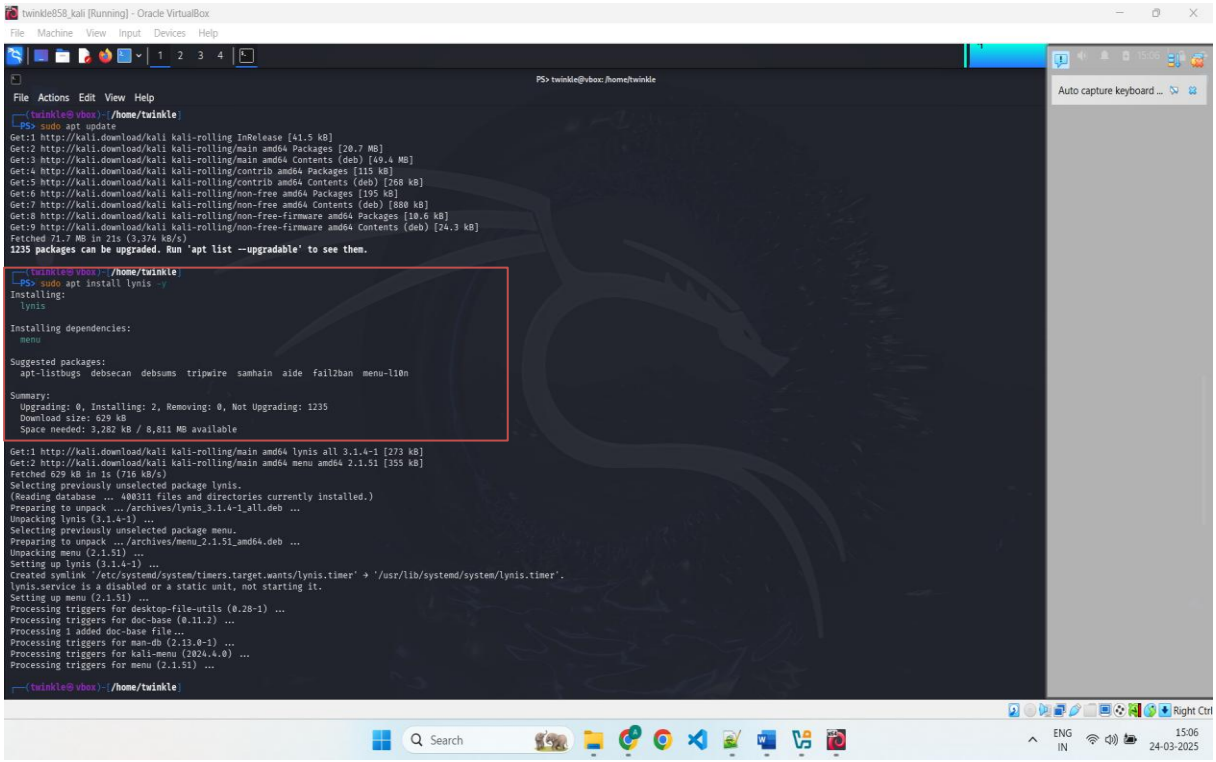
- **Conclusion**
  - The Nikto scan successfully identified potential vulnerabilities on the target web server scanme.nmap.org, which is running Apache 2.4.7. Although this server is meant for testing, in a real-world scenario, outdated software, default directories, and missing headers would pose serious security risks. These findings show the value of using Nikto in routine vulnerability assessments.

(C) System Vulnerability Analysis with Lynis [2 marks]

✓ Output #3 – System Hardening Assessment using Lynis

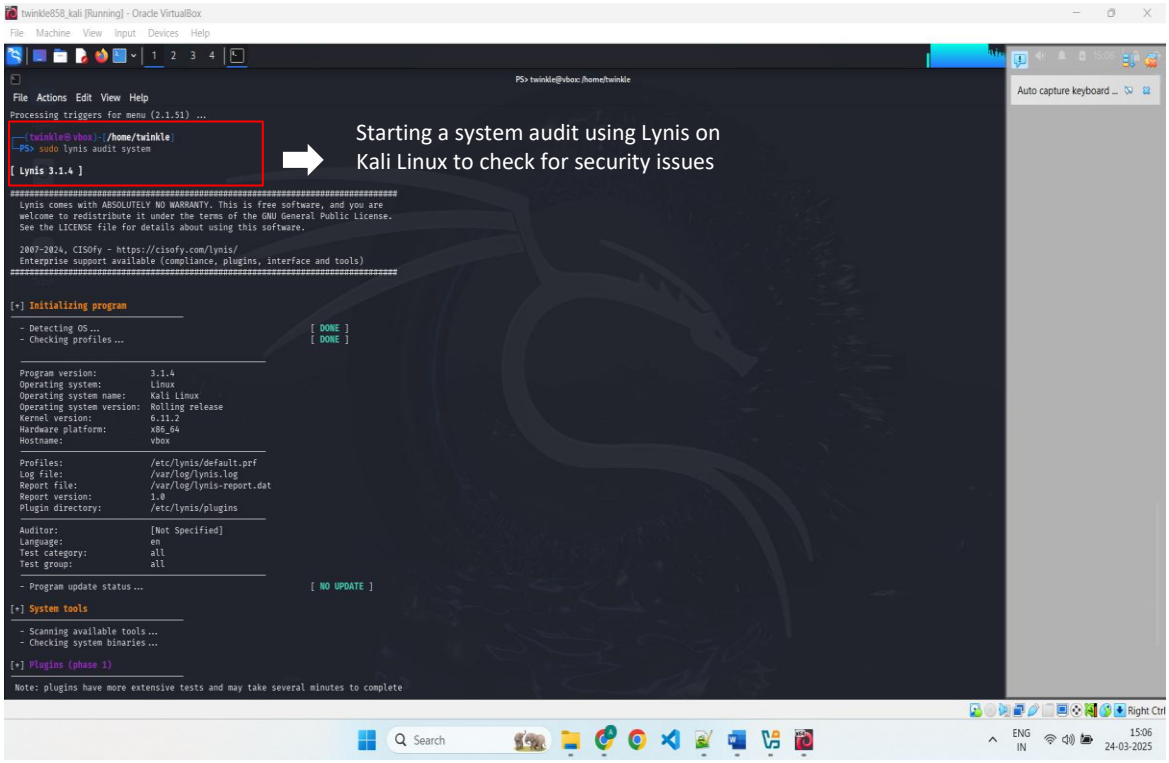
- Lynis is a security auditing and hardening tool for Unix-based systems that I have been using on Kali Linux.It checks system-level scans to check for vulnerabilities, weak configurations, and missing security practices. It's often used by system administrators and penetration testers to assess how secure a Linux machine is and to get suggestions for improving it.
- Step 1: Install Lynis

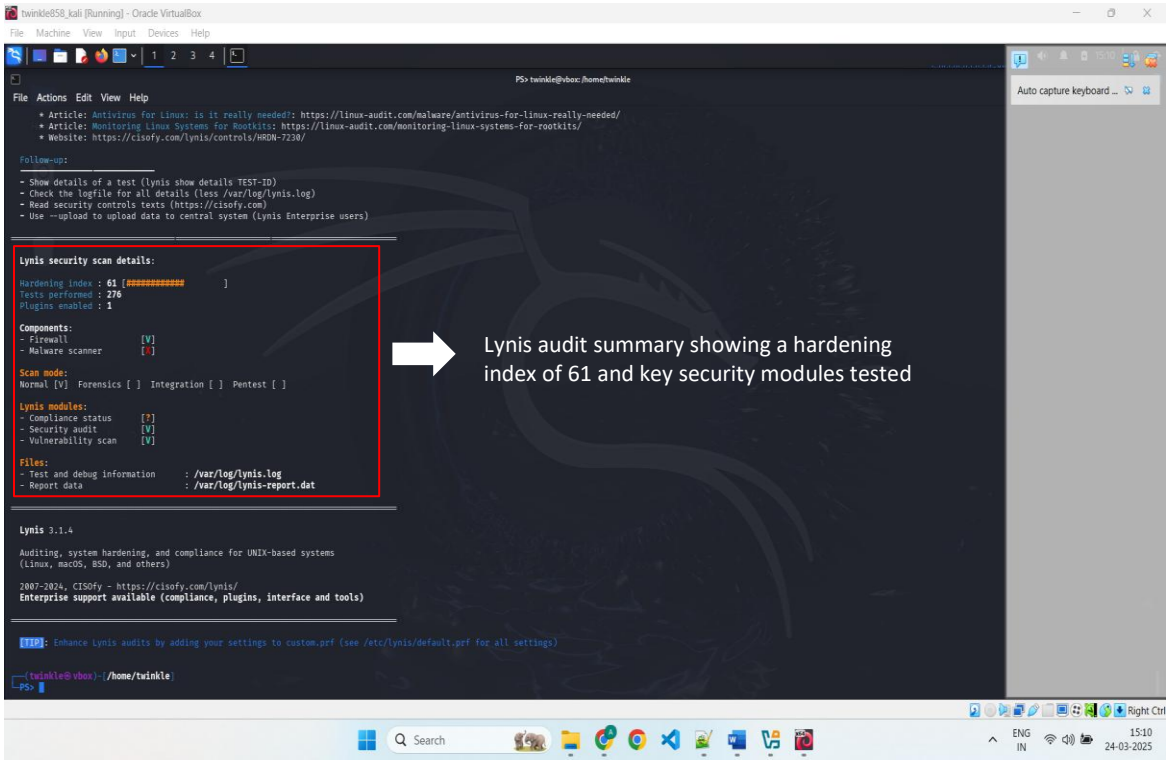
  sudo apt install lynis -y



- Step 2: Run a Lynis scan to assess Kali Linux system.

  sudo lynis audit system


Starting a system audit using Lynis on
Kali Linux to check for security issues


Lynis audit summary showing a hardening
index of 61 and key security modules tested

- **Scan Findings:**
  - **Hardening Index:** 61 (out of 100)
    A moderate score – suggests several areas of improvement.
  - **Tests Performed:** 276
  - **Plugins Enabled:** 1 (basic modules used)
  - **Modules Checked:**
    - Firewall
    - Security Audit
    - Vulnerability Scan
    - Malware Scanner (Not enabled)

Finding	What It Means	Suggested Action
Hardening score below 70	System has security gaps	Review full log and apply suggestions
Malware scanner not enabled	Could miss malicious binaries or changes	Enable malware scanning in Lynis settings
Configuration file not customized	Using default auditing profile	Edit /etc/lynis/default.prf for custom scans
No forensic or pentest mode	Only basic system checks performed	Run Lynis in other modes for deeper audits

- **Conclusion:**
  - The Lynis audit provided a useful overview of system security. With a hardening index of **61**, the system is not critically insecure but has room for improvement. Enabling malware scanning, configuring a stronger password policy, and customizing scan profiles would help increase the score. Lynis is a valuable tool for maintaining good security posture on Linux machines.

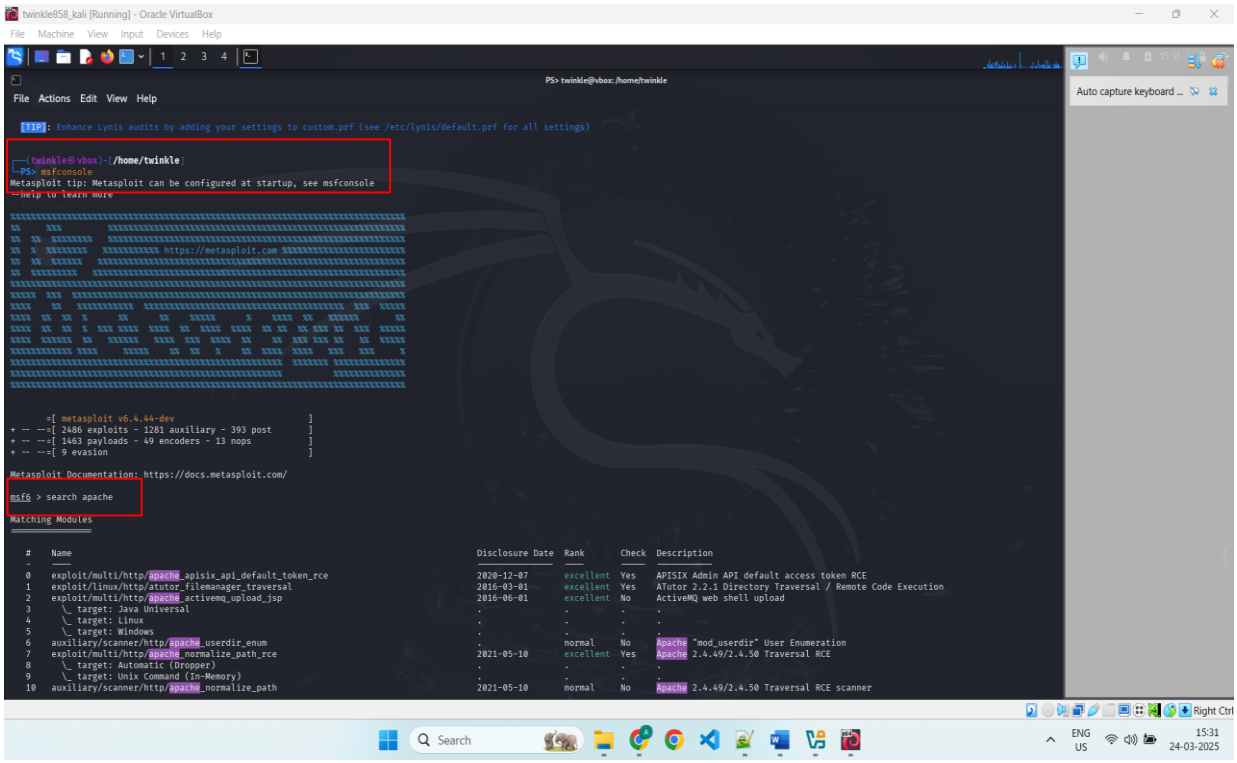
(D) Exploitation and Vulnerability Verification with Metasploit [2 marks]

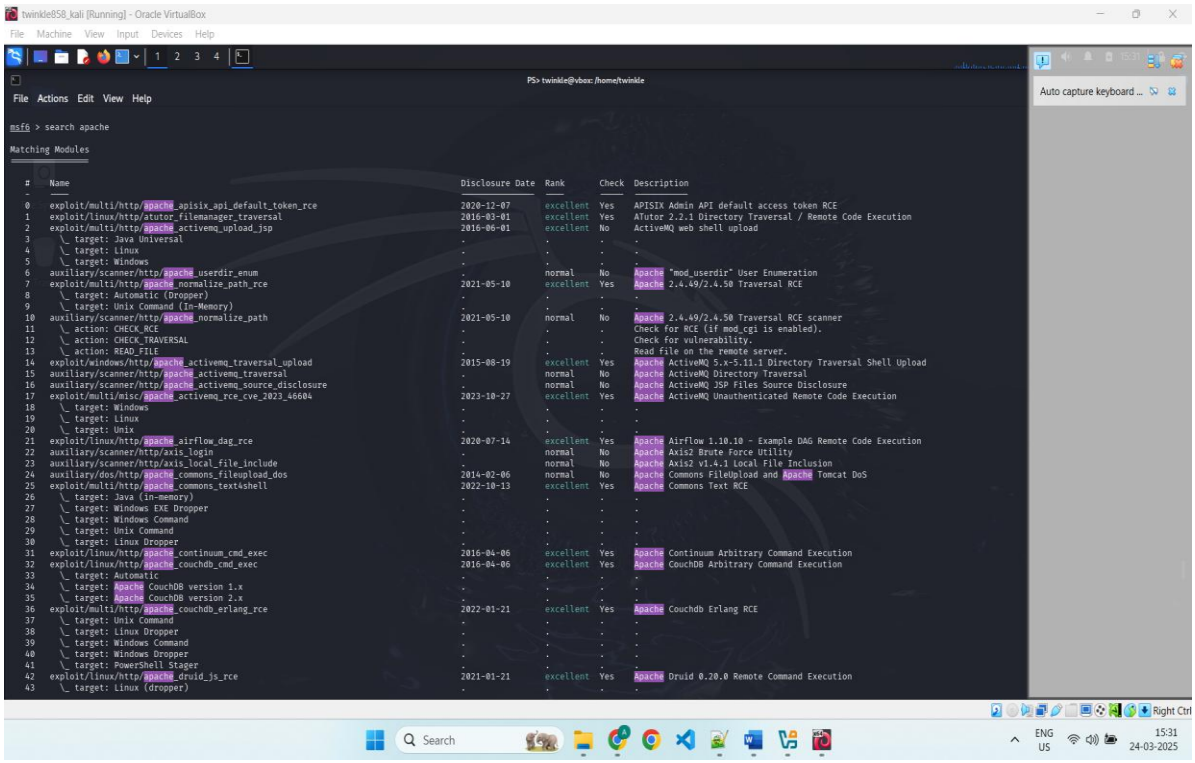
✓ Output #4 – Vulnerability Discovery and Analysis Using Metasploit

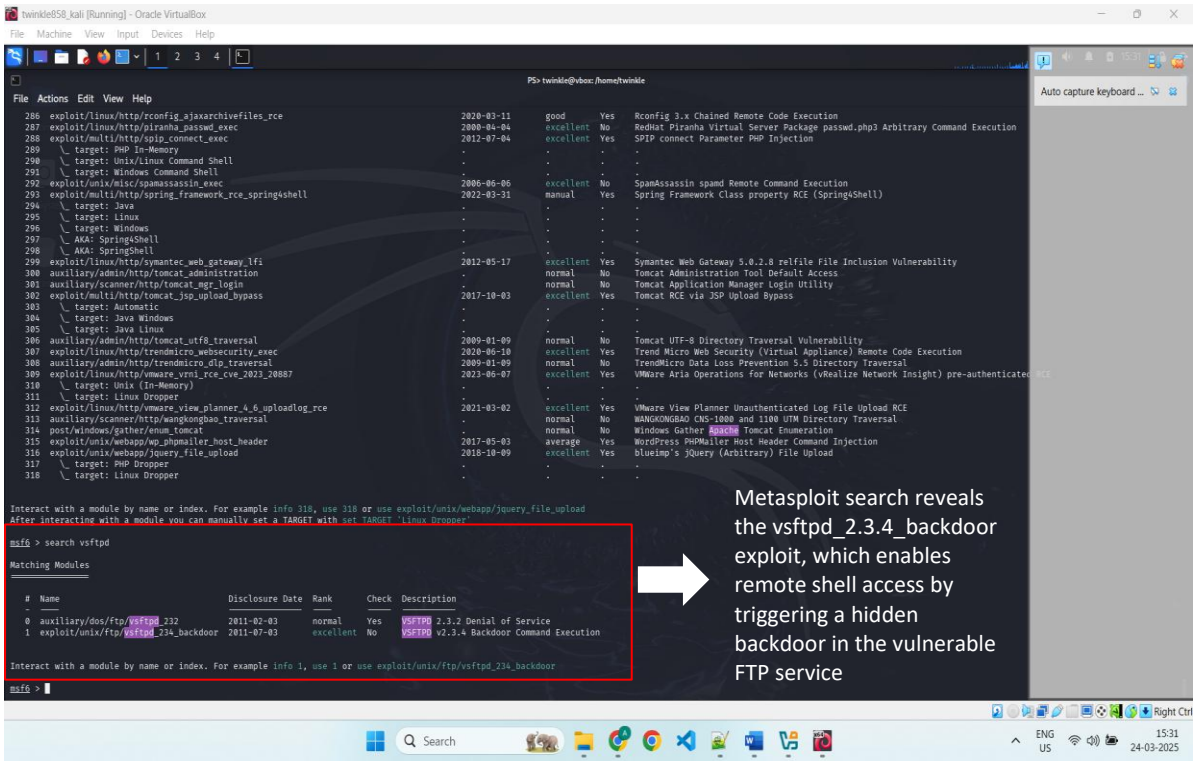
- Metasploit is basically a penetration testing framework that identifies, verifies, and exploits known system vulnerabilities. It contains a large database of exploits and tools that security experts use to simulate real-world assaults. Metasploit can assist confirm whether open ports and services discovered using tools like Nmap actually are susceptible.

- **Step 1:** Start Metasploit to search for a vulnerability related to one of the services found in your previous scans:

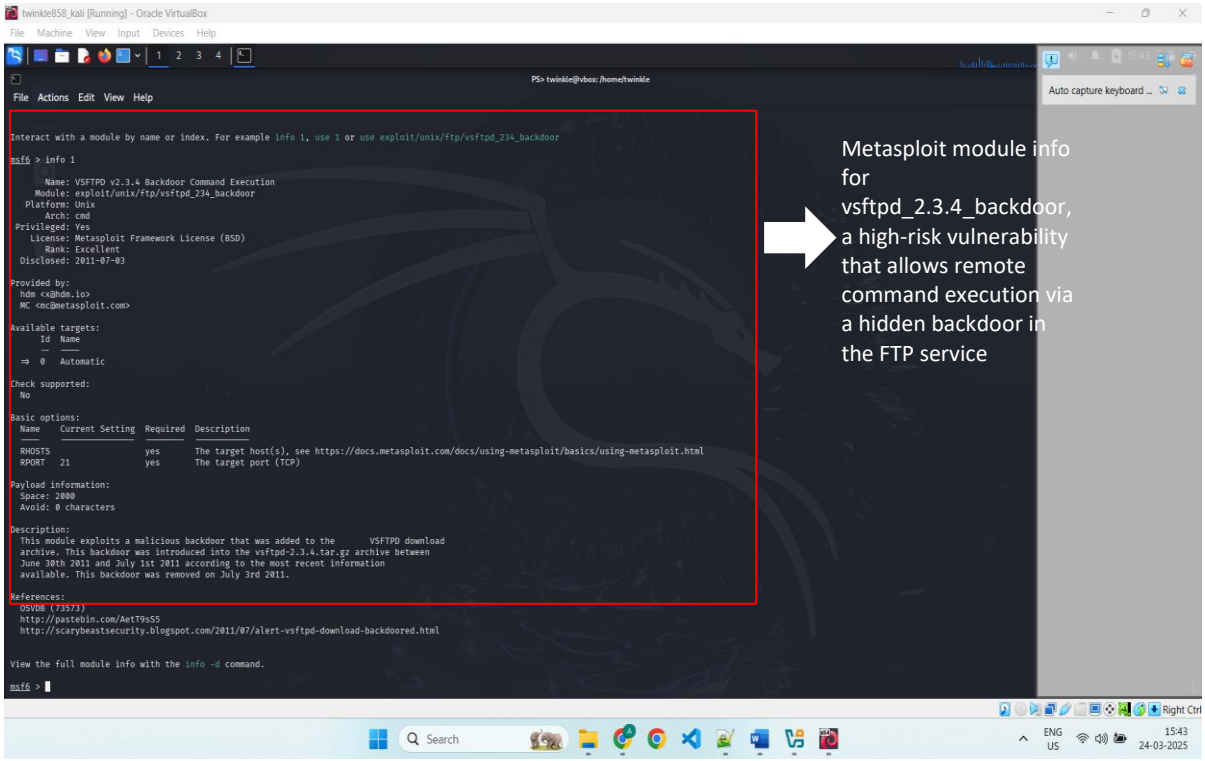
  msfconsole.







Metasploit module info for vsftpd_234_backdoor



- **Explanation of the Exploit:**
  - In Metasploit, I searched for vulnerabilities related to **vsftpd**, an FTP server used on many Unix-based systems. I found a module named exploit/unix/ftp/vsftpd_234_backdoor. This module takes advantage of a **malicious backdoor** that was injected into the vsftpd 2.3.4 source archive between **June 30th and July 1st, 2011**.
  - According to the official module info, when a client connects to a vulnerable server and uses a username containing :), the backdoor activates and opens a shell on port **6200**, giving the attacker **remote command access**.

Field	Details
Exploit Name	vsftpd_234_backdoor
Disclosed	July 3, 2011
Platform	Unix
Privilege	Yes (root shell possible)
Payload Space	2000 bytes
References	OSVDB, Pastebin, scarybeastsecurity.blogspot.com
Check Support	No

- **Chosen Exploit Module:**
  - **Name:** exploit/unix/ftp/vsftpd_234_backdoor
  - **Rank:** Excellent
  - **Vulnerability:** Backdoor in vsftpd version 2.3.4
  - **Type:** Remote Command Execution

- **Conclusion:**
  - Metasploit makes it easy to search, study, and potentially exploit known security issues. In this example, I found and reviewed a real-world backdoor in vsftpd 2.3.4. While it didn't directly apply to the earlier scans of scanme.nmap.org, it demonstrates how dangerous outdated software can be and how tools like Metasploit can help in vulnerability validation.