

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.

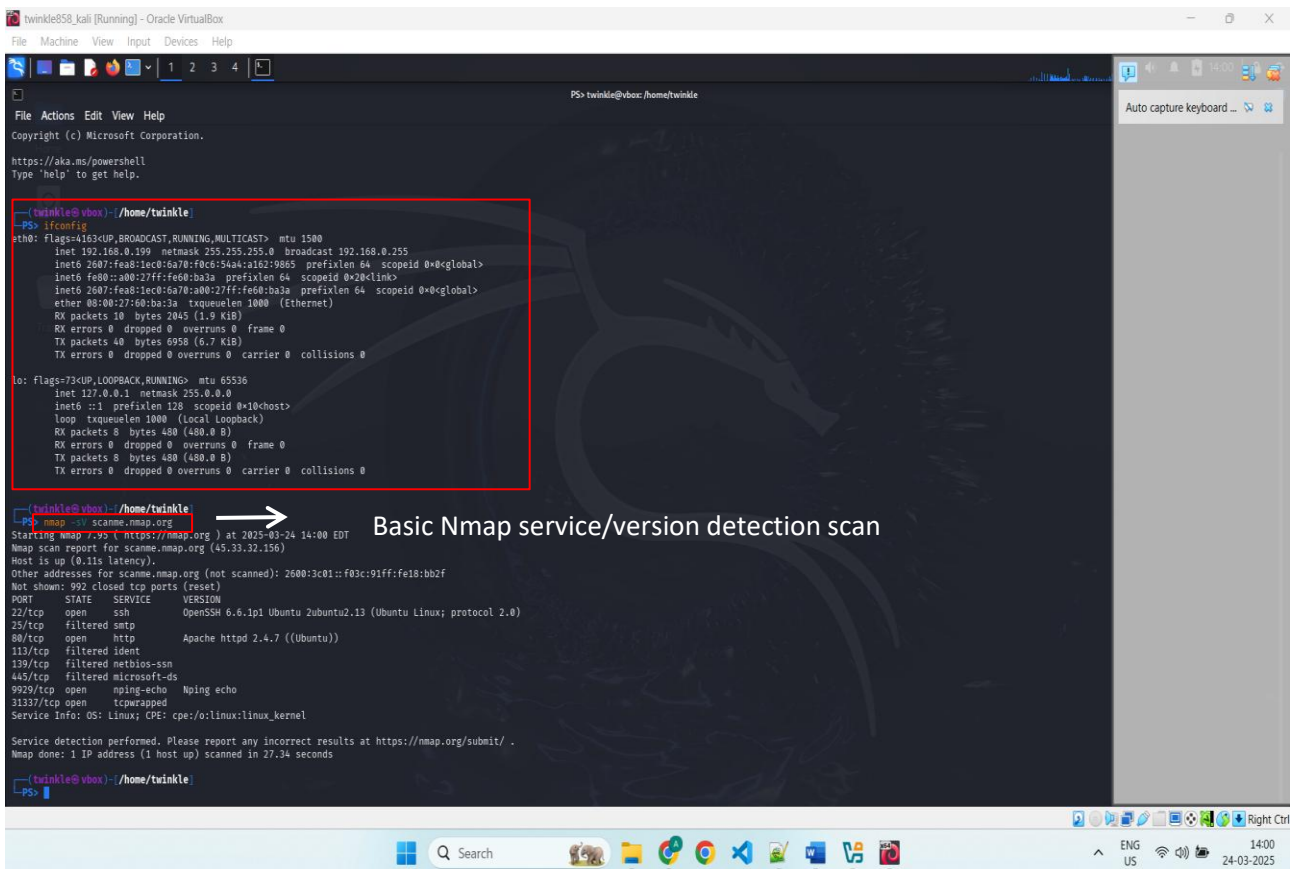
Resources

- 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 By scanning a target system, security analysts may identify outdated services, misconfigured systems, or open ports that shouldn't be exposed.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.



The screenshot shows a Kali Linux terminal window with the following content:

```
twinkle@kali:~/home/twinkle$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.199 netmask 255.255.0.0 broadcast 192.168.0.255
    inet6 2007:feab:1ec0:6a70:f0c5:5404:2162:9805 prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fe60:baja prefixlen 64 scopeid 0<link>
    inet6 2607:feab:1ec0:6a70:a00:27ff:fe60:baja prefixlen 64 scopeid 0<global>
    ether 08:00:27:60:ba:3a txqueuelen 1000 (Ethernet)
    RX packets 10 bytes 2045 (1.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40 bytes 6958 (6.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

twinkle@kali:~/home/twinkle$ nmap -v -sT https://nmap.org
Starting Nmap 7.95 (https://nmap.org) at 2025-03-24 14:00 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
113/tcp   filtered ident
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9929/tcp   open  nping-echo Nping echo
31337/tcp  open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

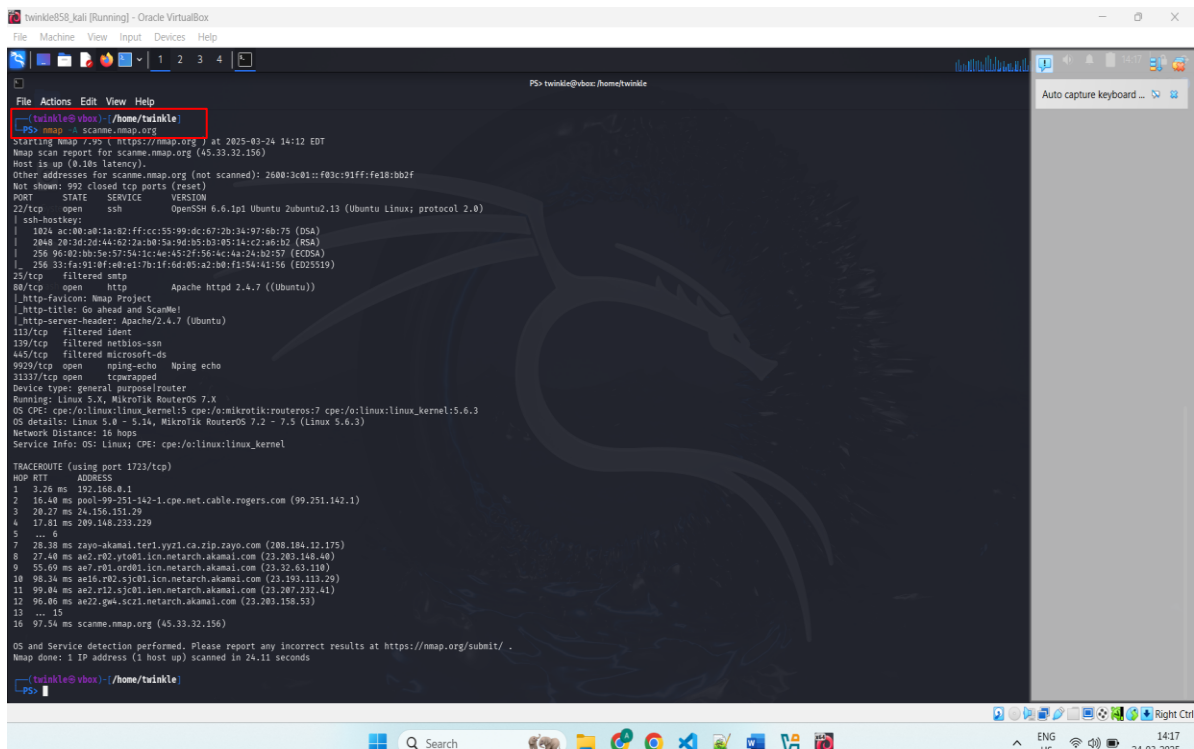
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 27.34 seconds
```

An arrow points from the terminal output to the text "Basic Nmap service/version detection scan".

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]

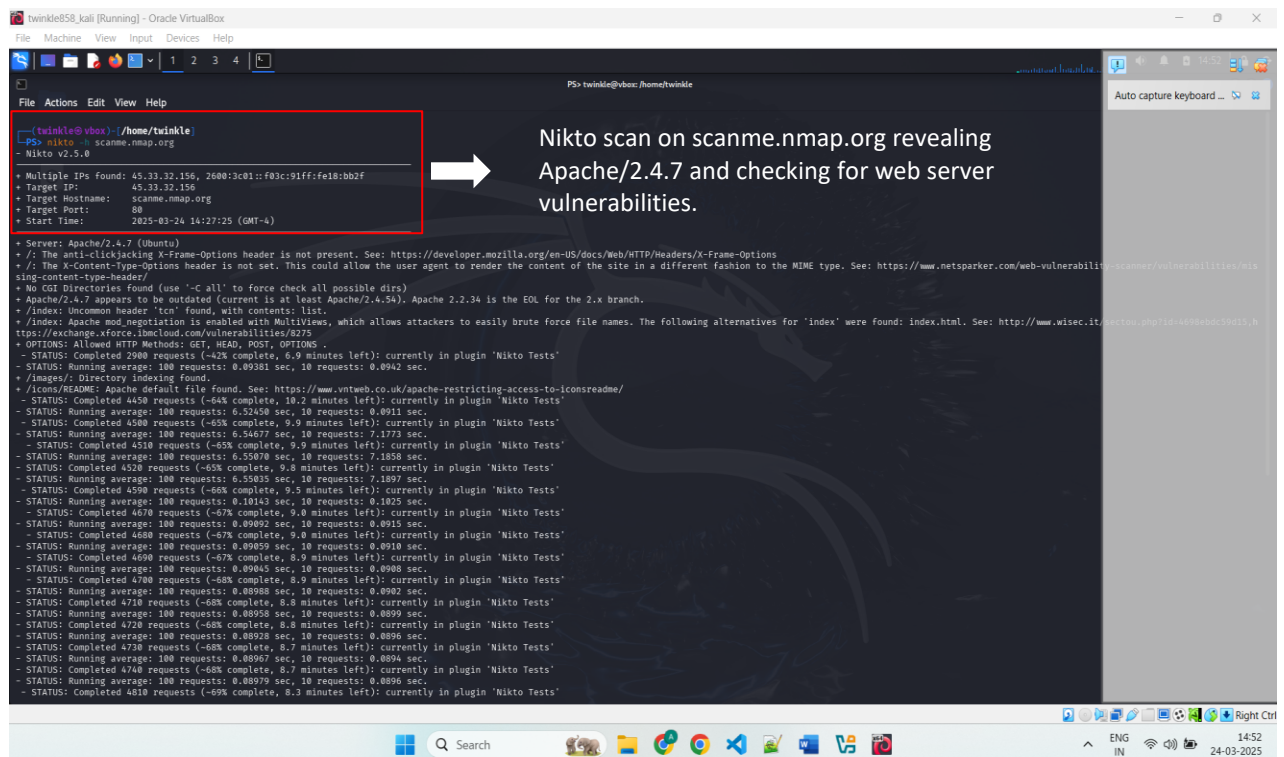
✓ Output #2 – Web Vulnerability Assessment using Nikto

- **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



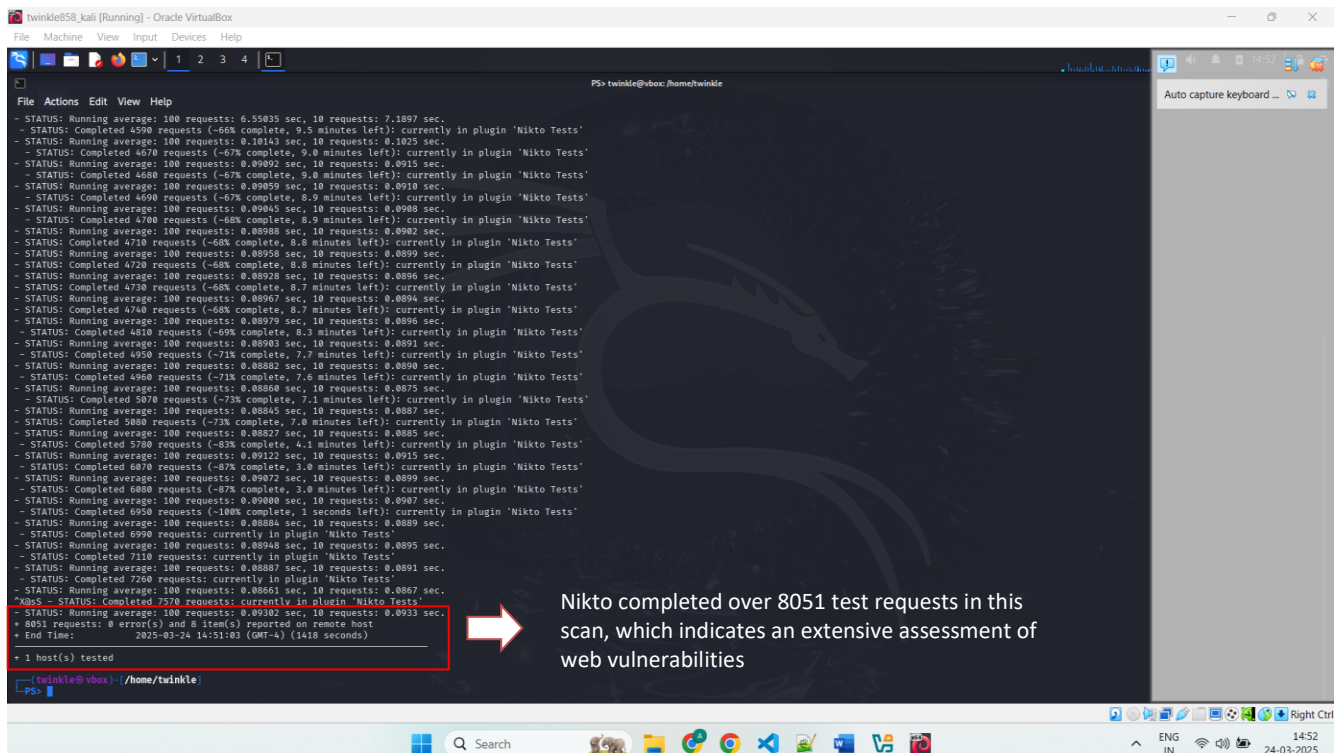
```
twinkle850kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

PS: twinkle@vbox:/home/twinkle
twinkle@vbox:~/home/twinkle
PS: nikto -h scanme.nmap.org
Nikto v2.5.8

+ Multiple IPs found: 45.33.32.156, 2600:3c11::f03c:91ff:fe18:bb2f
+ Target IP: 45.33.32.156
+ Target Hostname: scanme.nmap.org
+ Target Port: 80
+ Start Time: 2025-03-24 14:27:25 (GMT+4)

+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.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.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=46998bdc30015,h
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS.
- STATUS: Completed 2900 requests (~42% complete, 6.9 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09381 sec, 10 requests: 0.0942 sec.
+ /images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
- STATUS: Completed 4450 requests (~64% complete, 10.2 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.52450 sec, 10 requests: 0.0911 sec.
- STATUS: Completed 4500 requests (~65% complete, 9.9 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.54677 sec, 10 requests: 7.1773 sec.
- STATUS: Completed 4510 requests (~65% complete, 9.9 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.55070 sec, 10 requests: 7.1858 sec.
- STATUS: Completed 4520 requests (~65% complete, 9.8 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.55033 sec, 10 requests: 7.1897 sec.
- STATUS: Completed 4590 requests (~68% complete, 9.5 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.10143 sec, 10 requests: 0.1025 sec.
- STATUS: Completed 4670 requests (~67% complete, 9.0 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09059 sec, 10 requests: 0.0910 sec.
- STATUS: Completed 4690 requests (~67% complete, 8.9 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09092 sec, 10 requests: 0.0905 sec.
- STATUS: Completed 4698 requests (~67% complete, 8.9 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09045 sec, 10 requests: 0.0908 sec.
- STATUS: Completed 4700 requests (~68% complete, 8.9 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.08958 sec, 10 requests: 0.0899 sec.
- STATUS: Completed 4720 requests (~68% complete, 8.8 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.08928 sec, 10 requests: 0.0896 sec.
- STATUS: Completed 4730 requests (~68% complete, 8.7 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.08967 sec, 10 requests: 0.0894 sec.
- STATUS: Completed 4740 requests (~68% complete, 8.7 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.08970 sec, 10 requests: 0.0896 sec.
- STATUS: Completed 4810 requests (~69% complete, 8.3 minutes left): currently in plugin 'Nikto Tests'
```

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

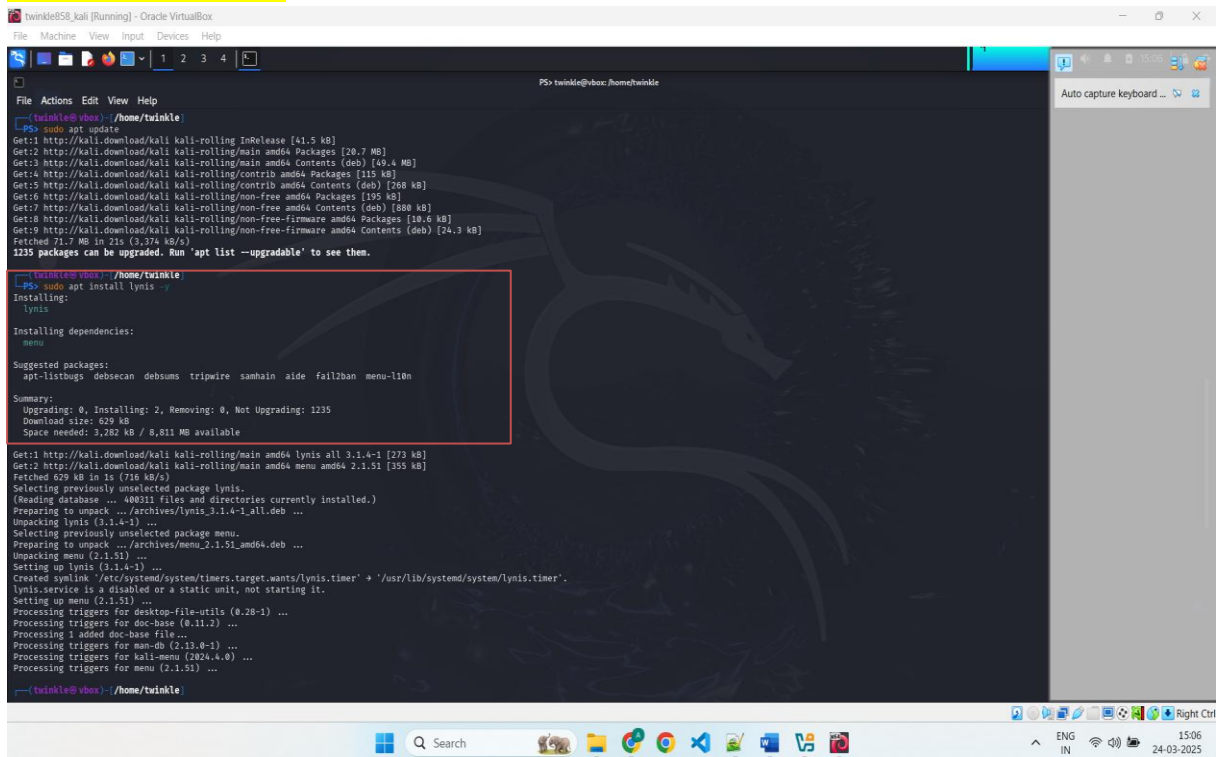
- The Nikto scan successfully identified potential vulnerabilities on the target web server scanme.nmap.org, which is running Apache 2.4.7. Although this server is meant for testing, in a real-world scenario, outdated software, default directories, and missing headers would pose serious security risks.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



```
twinkle@kali: /home/twinkle
PS> twinkle@kali: /home/twinkle

twinkle@kali: /home/twinkle
PS> sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.7 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.4 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [268 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [195 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [888 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [18.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [24.3 kB]
Fetched 71.7 MB in 21s (3,374 kB/s)
1235 packages can be upgraded. Run 'apt list --upgradable' to see them.

twinkle@kali: /home/twinkle
PS> sudo apt install lynis -y
Installing:
lynis

Installing dependencies:
menu

Suggested packages:
apt-listbugs debsecan debsums tripwire sanhain aide fail2ban menu-l10n

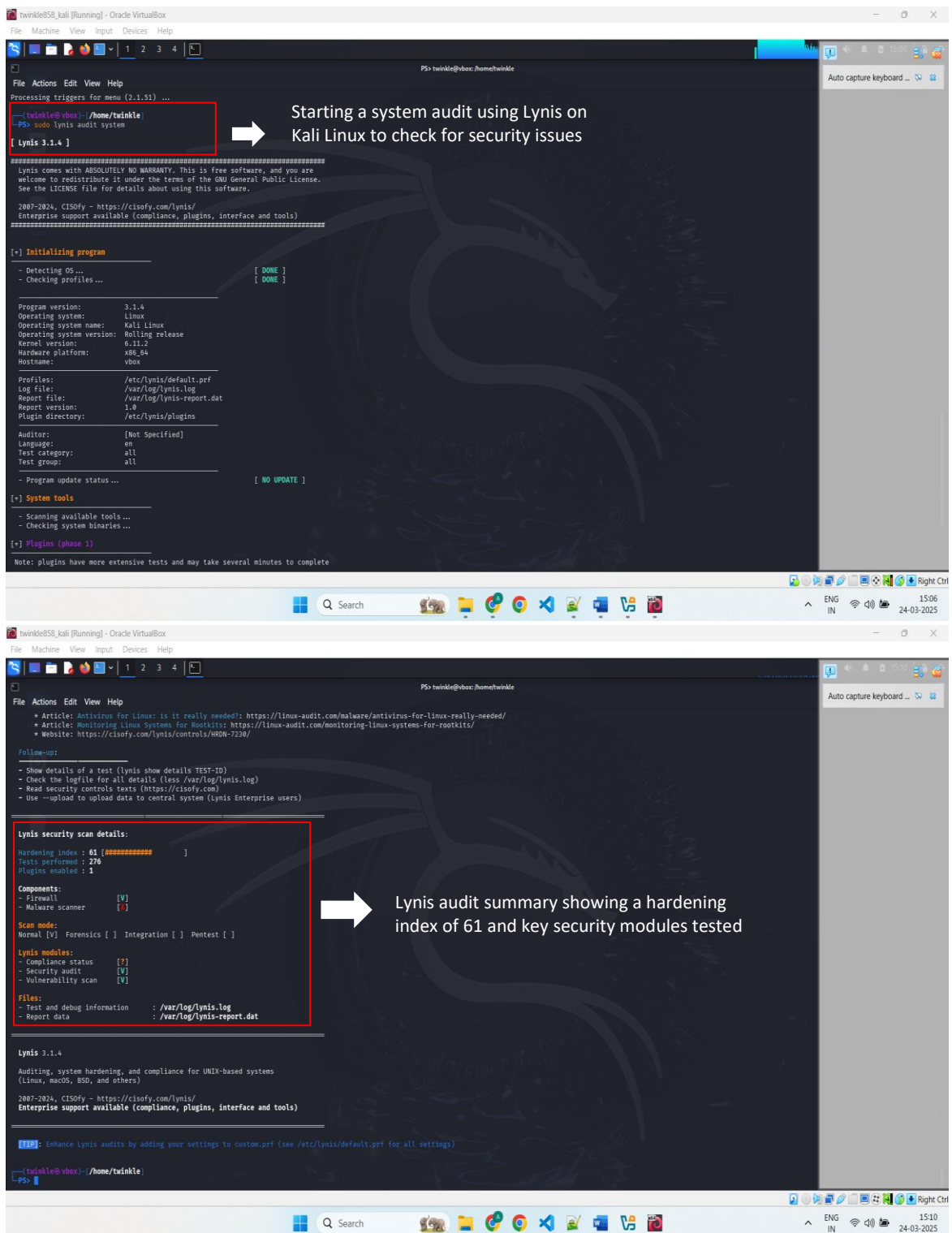
Summary:
Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1235
Download size: 629 kB
Space needed: 3,282 kB / 8,811 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 lynis all 3.1.4-1 [273 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 menu amd64 2.1.51 [355 kB]
Fetched 629 kB in 1s (716 kB/s)
Selecting previously unselected package lynis.
(Reading database ... 40831 files and directories currently installed.)
Preparing to unpack .../archives/lynis_3.1.4-1_all.deb ...
Unpacking lynis (3.1.4-1) ...
Selecting previously unselected package menu.
Preparing to unpack .../archives/menu_2.1.51_amd64.deb ...
Unpacking menu (2.1.51) ...
Setting up lynis (3.1.4-1) ...
Created symlink '/etc/systemd/system/timers.target.wants/lynis.timer' → '/usr/lib/systemd/system/lynis.timer'.
lynis.service is a disabled or a static unit, not starting it.
Setting up menu (2.1.51) ...
Processing triggers for desktop-file-utils (0.28-1) ...
Processing triggers for doc-base (0.11.2) ...
Processing 1 added doc-base file...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
Processing triggers for menu (2.1.51) ...

twinkle@kali: /home/twinkle
```

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

sudo lynis audit system



-
- **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.prp 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.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the following commands and output:

```
P$ twinkle@vbox: /home/twinkle  
  
[Tip]: Enhance Lynis audits by adding your settings to custom.prfl (see /etc/lynis/default.prfl for all settings)  
  
---(twinkle@vbox)-:/home/twinkle/  
P$ cd console  
Metasploit tip: Metasploit can be configured at startup, see msfconsole  
--help to learn more  
  
=====
```

A red box highlights the command `--help to learn more`.

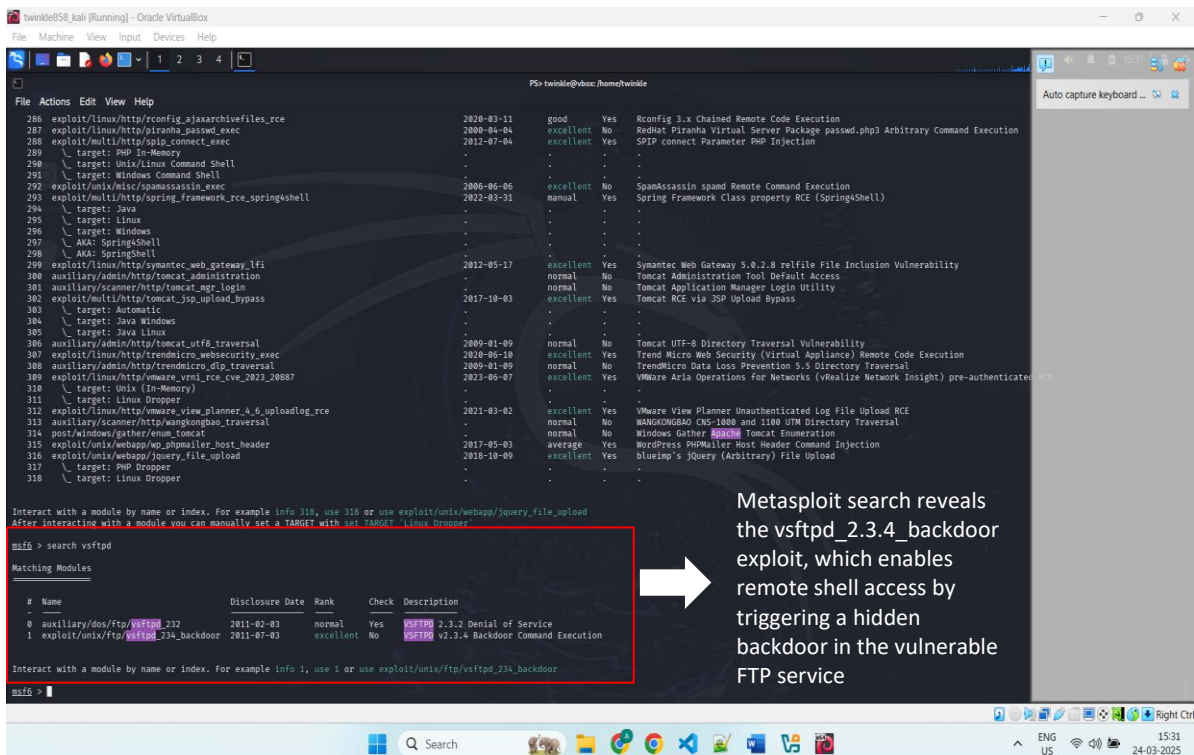
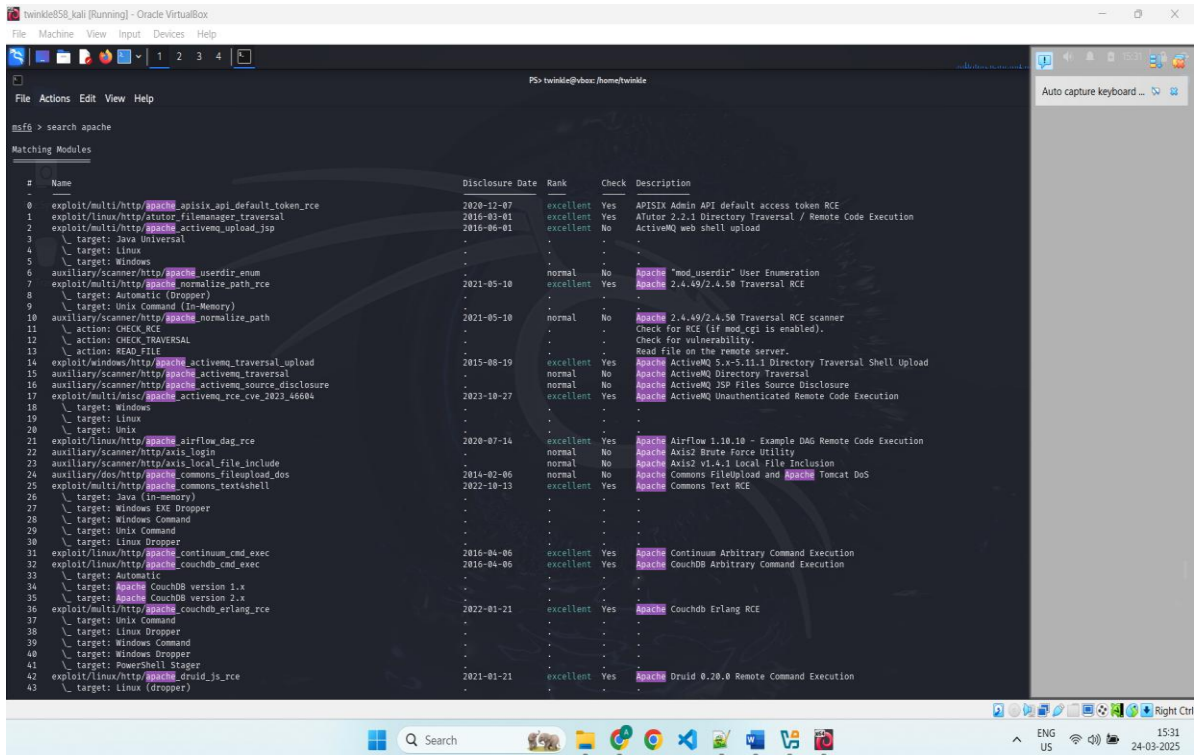
The terminal continues with the installation progress bar and version information:

```
+-----+  
+- [ metasploit v6.4.44-dev ]  
+- -- [ 2486 exploits - 1281 auxiliary - 393 post ]  
+- -- [ 1463 payloads - 49 encoders - 13 nops ]  
+- -- [ 0 evasion ]  
+-----+
```

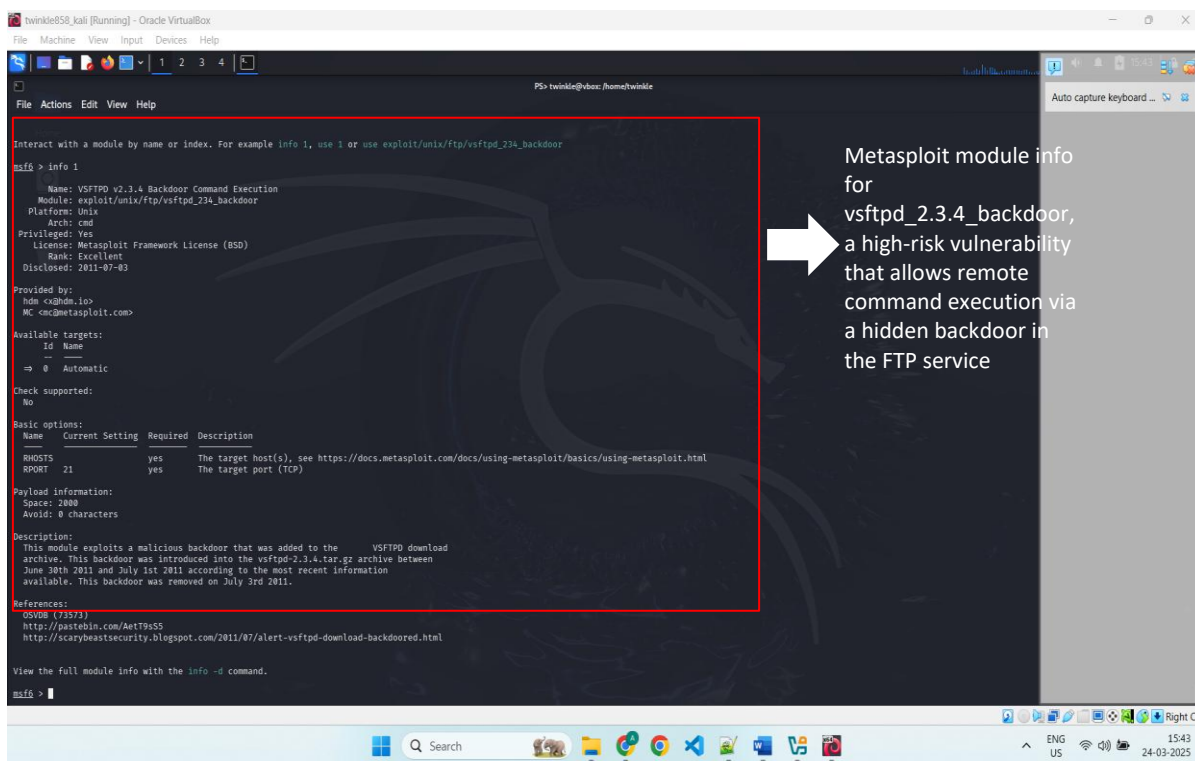
Below the progress bar, it says "Metasploit Documentation: https://docs.metasploit.com/".

Next, the user runs `msf6 > search apache`, which returns a list of modules matching the search criteria:

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/apache_apixix_api_default_token_rce	2020-12-07	excellent	Yes	APISIX Admin API default access token RCE
1	exploit/linux/http/atutor_filemanager_traversal	2016-03-01	excellent	Yes	Atutor 2.2.1 Directory Traversal / Remote Code Execution
2	exploit/multi/http/apache_activemq_upload_jsp	2016-06-01	excellent	No	ActiveMQ web shell upload
3	\ target: Java Universal	-	-	-	-
4	\ target: Linux	-	-	-	-
5	\ target: Windows	-	-	-	-
6	auxiliary/scanner/http/apache_userdir_enmm	-	normal	No	Apache "mod_userdir" User Enumeration
7	exploit/multi/http/apache_normalize_path_rce	2021-05-10	excellent	Yes	Apache 2.4.49/2.4.50 Traversal RCE
8	\ target: Automatic (Dropper)	-	-	-	-
9	\ target: Unix Command (fd-memory)	-	-	-	-
10	auxiliary/scanner/http/apache_normalize_path	2021-05-10	normal	No	Apache 2.4.49/2.4.50 Traversal RCE scanner



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.