

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.

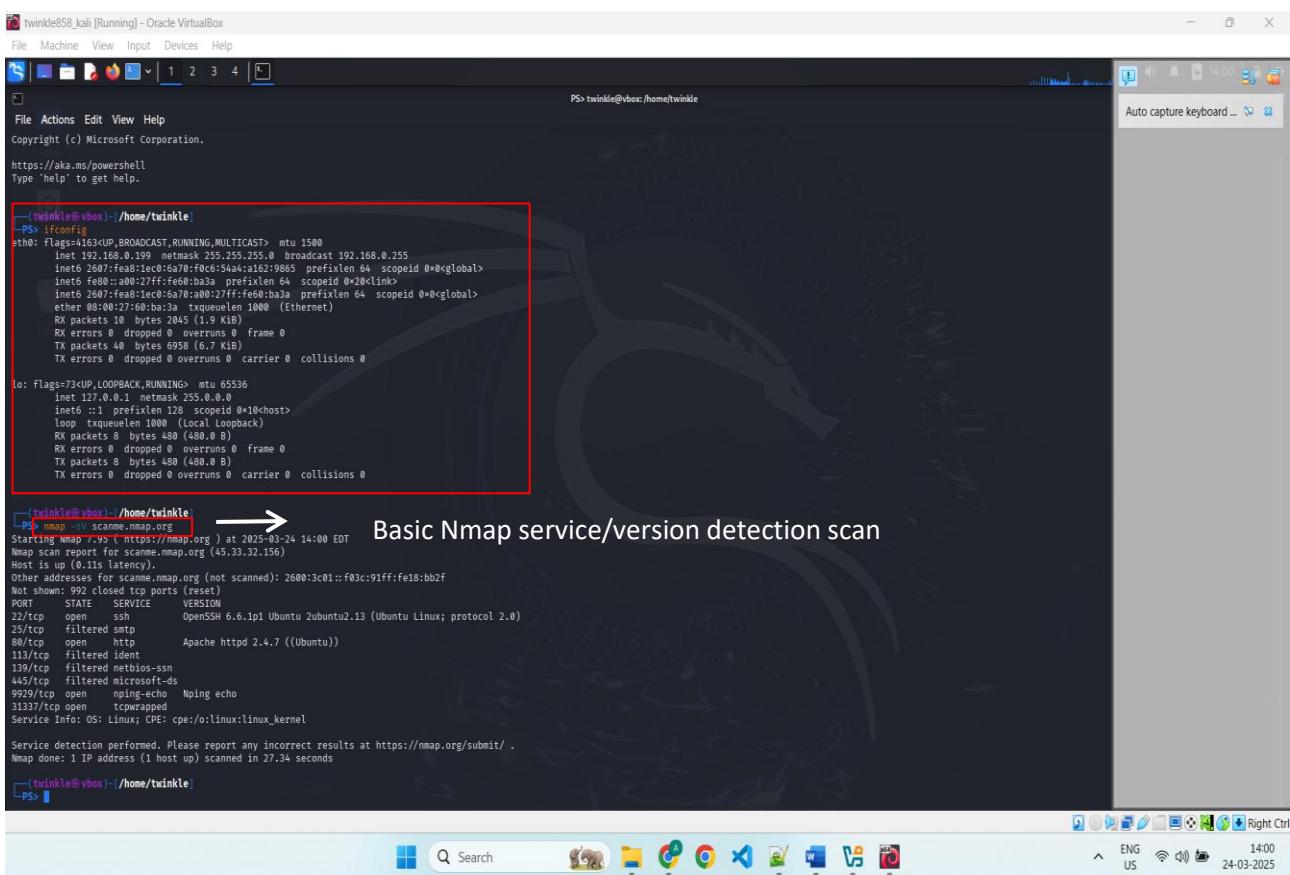
Resources

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 By scanning a target system, security analysts may identify outdated services, misconfigured systems, or open ports that shouldn't be exposed.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



twinkle@twinkle:~\$ ifconfig
File Machine View Input Devices Help
Copyright (c) Microsoft Corporation.
https://aka.ms/powershell
Type 'help' to get help.
twinkle@twinkle:~\$
twinkle@twinkle:~\$ ls
twinkle@twinkle:~\$ cd /home/twinkle
twinkle@twinkle:/home/twinkle\$ ps -a
twinkle@twinkle:/home/twinkle\$ nmap -sC -sV scanme.nmap.org
Starting Nmap 7.93 (https://nmap.org) at 2023-03-24 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): 2600:3c:01::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 open filtered ident
443/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
9939/tcp open ping-echo Nping echo
31337/tcp open tcptrapped
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
twinkle@twinkle:~\$ ps -a
twinkle@twinkle:~\$

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

```

twinkle858 kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
PS> twinkle@vbox: /home/twinkle
PS> nmap -A scanme.nmap.org
Starting Nmap 7.90 ( https://nmap.org ) at 2023-03-24 14:12 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.000s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::fe3c: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)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:bd:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a8:b2 (RSA)
|_  256 96:02:0b:5e:57:94:3c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
25/tcp    open  smt     smt
35/tcp    open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
_|_http-title: Go ahead and ScanMe!
|_http-server-type: Apache/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
9937/tcp  open  tcpwrapped
Device type: general-purpose-router
Running: Linux 5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1723/tcp)
HOP RTT     ADDRESS
1  2.05 ms  192.168.0.1
2  16.40 ms  209.148.233.226
3  20.27 ms  24.156.151.29
4  17.81 ms  209.148.233.226
5  ...  6
6  26.30 ms  zeyo-akamai.trel.yyr1.ca.zip.zzyo.com (208.184.12.175)
7  27.48 ms  ae2.r02.yt001.icn.netrach.akamai.com (23.283.140.40)
8  55.69 ms  ae7.701.ord01.icn.netrach.akamai.com (23.32.63.110)
9  98.34 ms  ae16.r02.sj001.icn.netrach.akamai.com (23.193.113.29)
10 99.04 ms  ae2.r12.sj001.icn.netrach.akamai.com (23.207.232.41)
11 98.34 ms  ae22.gw1.scz1.netrach.akamai.com (23.203.158.53)
12 100.00 ms  ...
13 100.00 ms  ...
14 100.00 ms  ...
15 100.00 ms  ...
16 97.54 ms  scanme.nmap.org (45.33.32.156)

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 24.11 seconds

```

Nmap aggressive scan showing open ports and detected services.

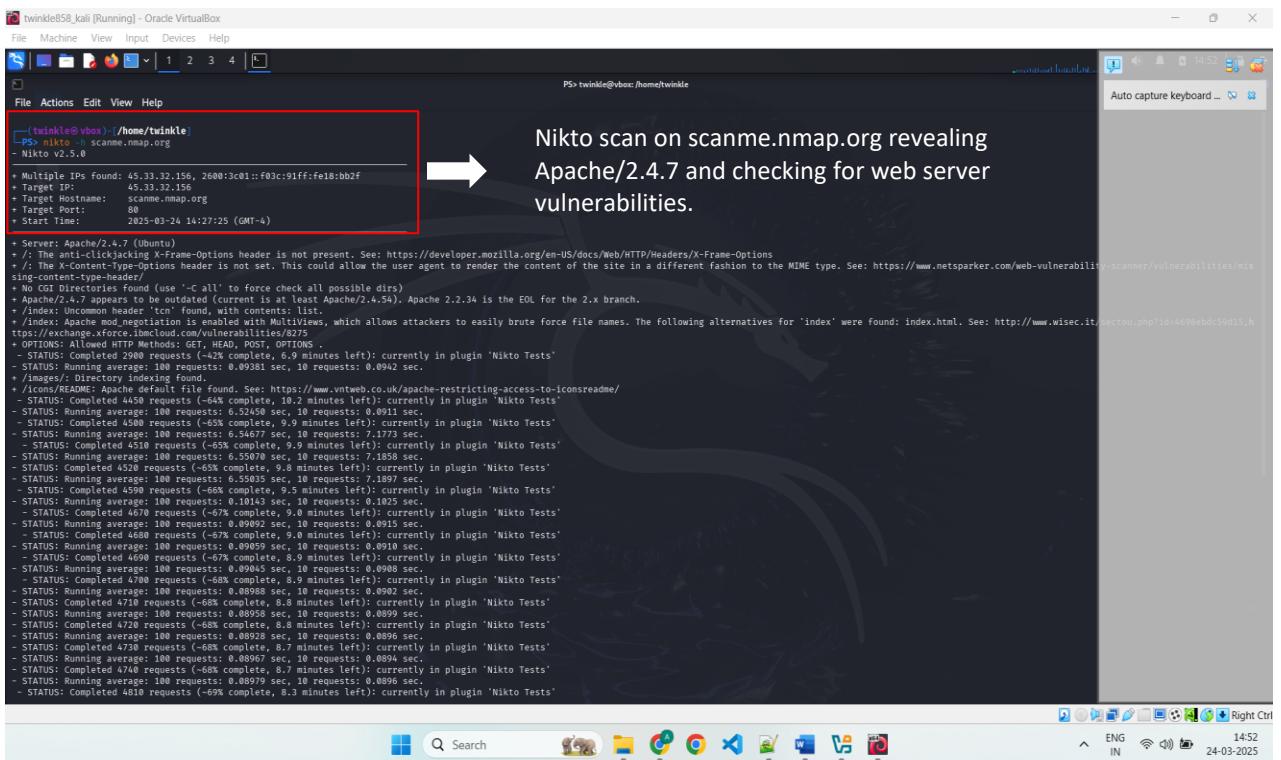
- **SSH Host Keys:** Four fingerprint types (DSA, RSA, ECDSA, ED25519) are shown, verifying it's a real SSH service. These are useful for confirming authenticity but can be outdated.
- **HTTP Title:** The web server displays the message: "Go ahead and ScanMe!" which confirms the site is meant for testing.
- **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 on scanme.nmap.org revealing Apache/2.4.7 and checking for web server vulnerabilities.

Nikto scan showing Apache version and missing headers

```
(twinkle@vbox)-[~/home/twinkle]
File Actions Edit View Help
└─PS> nikto -h scanme.nmap.org
- Nikto v2.5.0

+ Multiple IPs found: 45.33.32.156, 2600:3c01::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 Content-Security-Policy 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/misconfig-content-security-policy/
+ 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 2.2.24 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcm' found with contents: list
+ /index: Apache mod_negotiation is enabled, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/seccomp.php?id=469&e0d559d15.htm
+ /index: Apache mod_expires is enabled, which allows attackers to easily brute force file names, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/seccomp.php?id=469&e0d559d15.htm
+ 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: 0.0938 sec, 10 requests: 0.0942 sec.
+ /images/: Directory index file 'index.html' found
+ /index: README file 'README.html' 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: 0.62458 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: 0.63467 sec, 10 requests: 0.0911 sec.
- STATUS: Completed 4550 requests (-65% complete, 9.8 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.65507 sec, 10 requests: 0.0912 sec.
- STATUS: Completed 4520 requests (-65% complete, 9.8 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.65503 sec, 10 requests: 0.0917 sec.
- STATUS: Completed 4500 requests (-65% complete, 9.8 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.65503 sec, 10 requests: 0.0925 sec.
- STATUS: Completed 4670 requests (-67% complete, 9.0 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.6909 sec, 10 requests: 0.0915 sec.
- STATUS: Completed 4680 requests (-67% complete, 9.0 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.69095 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: 0.69095 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: 0.6899 sec, 10 requests: 0.0902 sec.
- STATUS: Completed 4710 requests (-68% complete, 8.8 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.68998 sec, 10 requests: 0.0909 sec.
- STATUS: Completed 4720 requests (-68% complete, 8.8 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.68928 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: 0.68928 sec, 10 requests: 0.0896 sec.
- STATUS: Completed 4740 requests (-68% complete, 8.7 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.68979 sec, 10 requests: 0.0896 sec.
- STATUS: Completed 4810 requests (-69% complete, 8.3 minutes left): currently in plugin 'Nikto Tests'
```

twinkle858_kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

PS> twinkle@vbox:~/home/twinkle

```
File Actions Edit View Help
STATUS: Running average: 100 requests: 6.55835 sec, 10 requests: 7.1897 sec.
- STATUS: Completed 4590 requests (~6% complete, 9.5 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 10.101 sec, 10 requests: 10.725 sec.
- STATUS: Completed 4574 requests (~67% complete, ~0.9 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09992 sec, 10 requests: 0.0915 sec.
- STATUS: Completed 4688 requests (~67% complete, 9.0 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09859 sec, 10 requests: 0.0910 sec.
- STATUS: Completed 4596 requests (~67% complete, 9.0 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09445 sec, 10 requests: 0.0908 sec.
- STATUS: Completed 4709 requests (~68% complete, 8.9 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09888 sec, 10 requests: 0.0902 sec.
- STATUS: Completed 4719 requests (~68% complete, 8.8 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09886 sec, 10 requests: 0.0903 sec.
- STATUS: Completed 4729 requests (~68% complete, 8.8 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09528 sec, 10 requests: 0.0896 sec.
- STATUS: Completed 4739 requests (~68% complete, 8.7 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09867 sec, 10 requests: 0.0894 sec.
- STATUS: Completed 4749 requests (~68% complete, 8.7 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09855 sec, 10 requests: 0.0893 sec.
- STATUS: Completed 4810 requests (~9% complete, 8.3 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09803 sec, 10 requests: 0.0891 sec.
- STATUS: Completed 4950 requests (~7% complete, 7.7 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.08882 sec, 10 requests: 0.0890 sec.
- STATUS: Completed 5079 requests (~7% complete, 7.6 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.08860 sec, 10 requests: 0.0875 sec.
- STATUS: Completed 5079 requests (~73% complete, 7.1 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.08845 sec, 10 requests: 0.0887 sec.
- STATUS: Completed 5089 requests (~73% complete, 7.0 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.08837 sec, 10 requests: 0.0885 sec.
- STATUS: Completed 5780 requests (~83% complete, 4.1 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09122 sec, 10 requests: 0.0915 sec.
- STATUS: Completed 6870 requests (~87% complete, 3.0 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09772 sec, 10 requests: 0.0981 sec.
- STATUS: Completed 7260 requests (~90% complete, 2.8 minutes left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09000 sec, 10 requests: 0.0907 sec.
- STATUS: Completed 6950 requests (~100% complete, 1 seconds left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.08884 sec, 10 requests: 0.0889 sec.
- STATUS: Completed 6950 requests (~100% complete, 1 seconds left); currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.08848 sec, 10 requests: 0.0895 sec.
- STATUS: Completed 7150 requests; currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.08887 sec, 10 requests: 0.0891 sec.
- STATUS: Completed 7260 requests; currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.08661 sec, 10 requests: 0.0867 sec.
- STATUS: Completed 7260 requests; currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.09302 sec, 10 requests: 0.0933 sec.
+ 8051 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2025-03-24 14:51:03 (GMT-4) (1418 seconds)

+ 1 host(s) tested
```

twinkle@vbox:~/home/twinkle

PS>

Nikto completed over 8051 test requests in this scan, which indicates an extensive assessment of web vulnerabilities

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 `scamme.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@twinkie:~$ 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 [111 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 [10.6 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@twinkie:~$ sudo apt install lynis -y
Installing:
lynis

Installing dependencies:
menu

Suggested packages:
apt-listbugs debsums tripwire samhain 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 https://kali.download/kali kali-rolling/main amd64 lynis all 3.1.4-1 [273 kB]
Get:2 https://kali.download/kali kali-rolling/main amd64 menu amd64 2.1.51 [355 kB]
Fetched 629 kB in 1s (758 kB/s)
Selecting previously unselected package lynis.
(Reading database ... 40038 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 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 triggers for menu (2024.4.0) ...
Processing triggers for menu (2.1.51) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
Processing triggers for menu (2.1.51) ...
```

- 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

```

twinkle@twinkle:~/Documents$ ./lynis audit system
[ Lynis 3.1.4 ]

Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2024, CISOFy - https://ciscofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

[*] Initializing program
- Detecting OS ... [ DONE ]
- Checking profiles ... [ DONE ]

Program version: 3.1.4
Operating system: Linux
Operating system name: Kali Linux
Operating system release: Kali Linux release
Kernel version: 5.11.2
Hardware platform: x86_64
Hostname: vbox

Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins

Auditor: [Not Specified]
Language: en
Test category: all
Test group: all
- Program update status ... [ NO UPDATE ]

[*] System tools
- Scanning available tools...
- Checking system binaries...

[*] Plugins (phase 1)
Note: plugins have more extensive tests and may take several minutes to complete

```

15:06
24-03-2025

Auto capture keyboard ...

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

```

twinkle@twinkle:~/Documents$ ./lynis audit system
[ Lynis 3.1.4 ]

* Article: Antivirus for Linux: is it really needed? https://linux-audit.com/malware/antivirus-for-linux-really-needed/
* Article: Monitoring Linux Systems For Rootkits: https://linux-audit.com/monitoring-linux-systems-for-rootkits/
* Website: https://ciscofy.com/lynis/controls/HUN-72307

Follow-up:
- Show details of a test (Lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://ciscofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

Lynis security scan details:
Hardening Index : 61 [ ###### ]
Tests performed : 276
Plugins enabled : 1

Components:
- Firewall [V]
- Malware scanner [V]

Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

Lynis modules:
- Compliance status [ ]
- Security audit [V]
- Vulnerability scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat

Lynis 3.1.4

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2024, CISOFy - https://ciscofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

twinkle@twinkle:~/Documents$ ./lynis audit system
[ Lynis 3.1.4 ]

```

15:10
24-03-2025

Auto capture keyboard ...

-
- **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.

```
twinkle@twinkie:~$ msfconsole
[*] Enhance Lync audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)
[-] twinkle@twinkie:~$ msfconsole
[-] msf6 > search apache
[!] metasploit v6.4.44-dev
+ --=[ 2486 exploits - 1281 auxiliary - 393 post
+ --=[ 1663 payloads - 49 encoders - 13 nops
+ --=[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search apache
Matching Modules
#  Name
0  exploit/multi/http/apache_api_default_token_rce
1  exploit/linux/http/atutor_filemanager_traversal
2  exploit/multi/http/apache_activemq_upload_jsp
3  exploit/multi/http/apache_universal
4    \ target: Linux
5    \ target: Windows
6  auxiliary/scanner/http/apache_userdir_enum
7  exploit/multi/http/apache_normalize_path_rce
8
9    \ target: Unix Command (In-Memory)
10 auxiliary/scanner/http/apache_normalize_path
```

```

twinkle858 kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
msf6 > search apache
Matching Modules
# Name
0 exploit/multi/http/apache_sparkle_api_default_token_rce
1 exploit/linux/http/stotor_filenamemanager_traversal
2 exploit/multi/http/apache_activemq_upload.jsp
3   \ target: Java Universal
4   \ target: Linux
5   \ target: Windows
6 auxiliary/scanner/http/apache_userdir_enum
7 exploit/multi/http/apache_normalize_path_rce
8   \ target: Automatic (Dropper)
9   \ target: Unix Command (In-Memory)
10 auxiliary/scanner/http/apache_normalize_path
11   \ action: CHECK_RCE
12   \ action: CHECK_TRAVERSAL
13   \ action: READ_FILE
14 exploit/windows/http/apache_activemq_upload
15 auxiliary/scanner/http/apache_activemq_traversal
16 auxiliary/scanner/http/apache_activemq_source_disclosure
17 exploit/multi/misc/apache_activemq_rce_cve_2023_46604
18   \ target: Windows
19   \ target: Linux
20   \ target: Windows
21 exploit/linux/http/apache_airflow_dag_rce
22 auxiliary/scanner/http/axis_login
23 auxiliary/scanner/http/axis_local_file_inclusion
24 auxiliary/dos/http/apache_commons_fileupload_dos
25 exploit/multi/http/apache_commons_textshell
26   \ target: Java (In-Memory)
27   \ target: Windows EXE Dropper
28   \ target: Windows Command
29   \ target: Unix Command
30   \ target: Windows Dropper
31 exploit/linux/http/apache_continuum_cmd_exec
32 exploit/linux/http/apache_couchdb_cmd_exec
33   \ target: Automatic
34   \ target: Apache CouchDB version 1.x
35   \ target: Apache CouchDB version 2.x
36 exploit/multi/http/apache_couchdb_erlang_rce
37   \ target: Unix Command
38   \ target: Linux Dropper
39   \ target: Windows Command
40   \ target: Windows Dropper
41   \ target: PowerShell Stager
42 exploit/linux/http/apache_druid_js_rce
43   \ target: Linux (dropper)

Disclosure Date Rank Check Description
2020-11-07 excellent Yes APISDN Admin API default access token RCE
2016-03-01 excellent Yes Autot 2.2.1 Directory Traversal / Remote Code Execution
2016-06-01 excellent No ActiveMQ web shaii upload
2021-05-10 normal No mod_userdir* User Enumeration
2021-05-10 excellent Yes Apache 2.4.49/2.4.58 Traversal RCE
2021-05-10 normal No Apache 2.4.49/2.4.58 Traversal RCE scanner
2021-05-10 normal No Check for RCE (if mod.cgi is enabled).
2021-05-10 normal No Check for vulnerability.
2021-05-10 normal No Read file on the remote server.
2015-08-19 excellent Yes Apache ActiveMQ 5.x-5.11.1 Directory Traversal Shell Upload
2016-02-06 normal No Apache ActiveMQ Directory Traversal
2016-02-06 normal No Apache ActiveMQ File Inclusion Disclosure
2023-10-27 excellent Yes Apache ActiveMQ Unauthenticated Remote Code Execution
2020-07-14 excellent Yes Apache Airflow 1.10.10 - Example DAG Remote Code Execution
2020-07-14 normal No Apache Axis2 Brute Force Utility
2020-07-14 normal No Apache Axis2 v1.4.1 Local File Inclusion
2020-07-14 normal No Apache Commons Fileupload and Apache Tomcat DoS
2022-10-13 excellent Yes Apache Commons Text RCE
2016-04-06 excellent Yes Apache Continuum Arbitrary Command Execution
2016-04-06 excellent Yes Apache CouchDB Arbitrary Command Execution
2022-01-21 excellent Yes Apache Couchdb Erlang RCE
2021-01-21 excellent Yes Apache Druid 0.20.0 Remote Command Execution
2012-07-04 excellent Yes Kconfig 3.x Chained Remote Code Execution
2008-04-04 excellent No RedHat Piraha Virtual Server Package passed.php3 Arbitrary Command Execution
2008-04-04 excellent Yes SPiP connect Parameter PmP injection
2008-06-06 excellent No SpandAssassin spand Remote Command Execution
2022-03-31 manual Yes Spring Framework Class property RCE (Spring4Shell)
2012-05-17 excellent Yes Symantec Web Gateway 5.0.2.8 rfile File Inclusion Vulnerability
2012-05-17 normal No Tomcat Administration Tool Default Access
2012-05-17 normal No Tomcat Application Manager Login Utility
2012-05-17 excellent Yes Tomcat RCE via JSP Upload Bypass
2000-01-09 normal No Tomcat UTF-8 Directory Traversal Vulnerability
2000-01-09 excellent Yes Trend Micro Web Security (Virtual Appliance) Remote Code Execution
2000-01-09 normal No TrendMicro Data Loss Prevention 5.5 Directory Traversal
2003-06-07 excellent Yes VMware Aria Operations for Networks (VRealize Network Insight) pre-authenticated RCE
2021-03-02 excellent Yes VMware View Planner Unauthenticated Log File Upload RCE
2009-01-09 normal No WANGKONGBAO CNS-1000 and 1100 UTM Directory Traversal
2017-05-03 normal No Windows Gather Apache Tomcat Enumeration
2018-10-09 average Yes WordPress PHPMailer Host Header Command Injection
2017-05-03 excellent Yes BlueImp's jQuery (Arbitrary) File Upload
2011-07-03 normal No

Interact with a module by name or index. For example info 318, use 318 or use exploit/unix/webapp/query_file_upload
After interacting with a module you can manually set a TARGET with set TARGET <target>
msf6 > search vsftpd
Matching Modules
# Name
0 auxiliary/dos/ftp_vsftpd_232
1 exploit/unix/ftp_vsftpd_234_backdoor 2011-07-03 normal Yes vsFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp_vsftpd_234_backdoor 2011-07-03 excellent No vsFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp_vsftpd_234_backdoor
msf6 > 
```

Metasploit search reveals the `vsftpd_2.3.4_backdoor` exploit, which enables remote shell access by triggering a hidden backdoor in the vulnerable FTP service

```

twinkle858 kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
msf6 > search vsftpd
Matching Modules
# Name
0 auxiliary/dos/ftp_vsftpd_232
1 exploit/unix/ftp_vsftpd_234_backdoor 2011-07-03 normal Yes vsFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp_vsftpd_234_backdoor 2011-07-03 excellent No vsFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp_vsftpd_234_backdoor
msf6 > 
```

Metasploit module info for `vsftpd_234_backdoor`

The screenshot shows a terminal window titled 'twinkie858_kali [Running] - Oracle VirtualBox'. The command 'msf6 > info 1' is run, displaying information about the 'vsftpd_2.3.4_backdoor' module. A red box highlights the module details: Name: VSFTPD v2.3.4 Backdoor Command Execution, Module: exploit/unix/ftp/vsftpd_234_backdoor, Platform: Unix, Arch: cmd, Privilege: root, License: Metasploit Framework License (BSD), Rank: Excellent, Disclosed: 2011-07-03. An arrow points from this highlighted text to the right, leading to a detailed description of the module.

Metasploit module info for vsftpd_2.3.4_backdoor, a high-risk vulnerability that allows remote command execution via a hidden backdoor in the FTP service

```

Interact with a module by name or index. For example info 1, use ! or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > info 1
      Name: VSFTPD v2.3.4 Backdoor Command Execution
      Module: exploit/unix/ftp/vsftpd_234_backdoor
      Platform: Unix
      Arch: cmd
      Privilege: root
      License: Metasploit Framework License (BSD)
      Rank: Excellent
      Disclosed: 2011-07-03

      Provided by:
      hdm <@hdm.io>
      MC <mcm@metasploit.com>

      Available targets:
      Id  Name
      --  --
      => 0  Automatic

      Check supported:
      No

      Basic options:
      Name   Current Setting  Required  Description
      RHOSTS  yes            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
      RPORT   21             yes       The target port (TCP)

      Payload information:
      Space: 2000
      Avoid: <characters

      Description:
      This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.

      References:
      OSVDB (7373)
      https://pastebin.com/AetTqSS5
      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

      view the full module info with the info -d command.
msf6 > 

```

- **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.