Dipak Bhateja 11901377 **Roll no:- 42**

CA-3 Open Source Technologies

Objective of the Project :-

The objective of network devices security testing is to identify and mitigate potential vulnerabilities in the network devices that can be exploited by attackers. By conducting vulnerability assessments, penetration testing, and configuration audits, network administrators can identify and remediate security weaknesses before they can be exploited by attackers. The use of network traffic analysis tools, network intrusion detection and prevention systems, and password cracking tools can also help in detecting and preventing unauthorized access to the network devices.

The objective of physical security testing is to evaluate the effectiveness of physical security measures in protecting the network devices from physical attacks or unauthorized access. By conducting physical security assessments, physical access control tests, and surveillance camera testing, network administrators can identify potential vulnerabilities in the physical security of the network devices and take appropriate measures to address them. The testing of alarm systems, response procedures, and social engineering awareness training and policies can also help in improving the overall physical security posture of the network devices.

Description of the project :-

In this project we refer to the techniques, tools, and methodologies that a network administrator can use to perform testing on network devices security and physical security.

For network devices security testing, the objective is to identify potential vulnerabilities in the network devices and take appropriate measures to mitigate them. This can be achieved by conducting vulnerability assessments, penetration testing, configuration audits, network traffic analysis, network intrusion detection and prevention, password cracking, and social engineering testing.

For physical security testing, the objective is to evaluate the effectiveness of physical security measures in protecting the network devices from physical attacks or unauthorized access. This can be achieved by conducting physical security

assessments, physical access control testing, surveillance camera testing, alarm system and response procedure testing, and social engineering testing.

In both cases, open-source software can be used to perform the testing, such as Nmap, OpenVAS, Metasploit, Wireshark, Snort, John the Ripper, and Social Engineer Toolkit for network devices security testing, and OpenCV, Motion, Zoneminder, Fingerprint GUI, Firefly, and Social Engineer Toolkit for physical security testing.

Scope of the Project :-

- Defining the testing objectives and goals for network devices security and physical security.
- Identifying the network devices and physical security measures that will be tested.
- Conducting vulnerability assessments, penetration testing, configuration audits, network traffic analysis, network intrusion detection and prevention, password cracking, physical access control testing, surveillance camera testing, alarm system and response procedure testing, and social engineering testing.
- Analyzing the results of the tests to identify vulnerabilities and areas for improvement.
- Developing and implementing mitigation strategies to address the identified vulnerabilities and improve the overall security posture of the network devices and physical security measures.
- Continuously monitoring and updating the security measures to maintain a secure network environment.
- Documenting the testing process, results, and mitigation strategies for future reference and compliance purposes

Target System Description :-

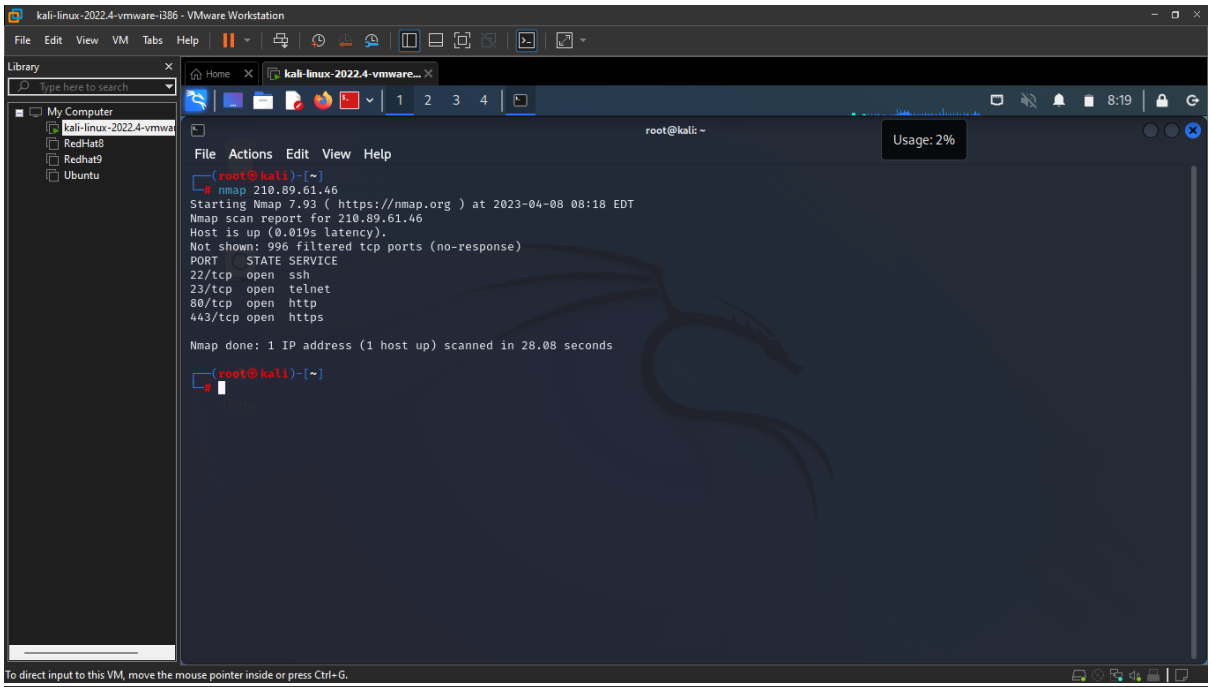
Network Devices: The project could focus on testing the security of various network devices such as routers, switches, firewalls, load balancers, and servers. The devices may include both wired and wireless devices, and they may be located on-premises, in a data center, or in the cloud.

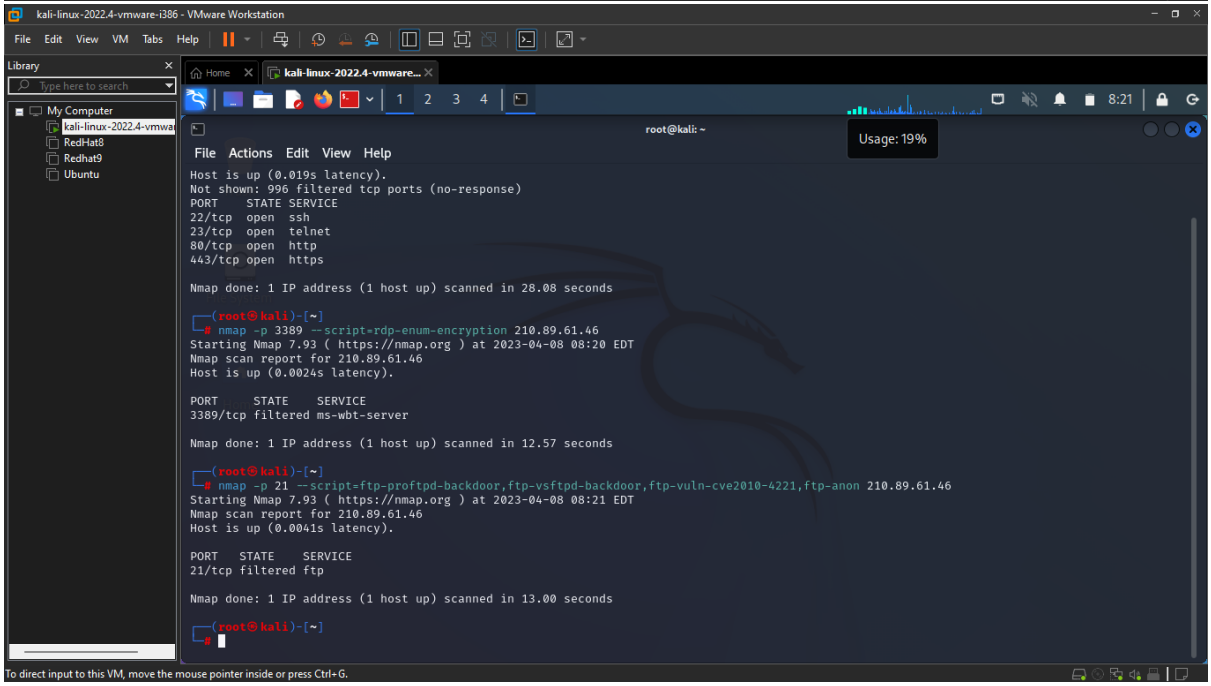
Physical Security Measures: The project could focus on testing the physical security measures that are in place to protect the network devices. This may include testing the effectiveness of access control mechanisms such as key cards, biometric scanners, and security cameras, as well as testing the response procedures in case of physical security incidents.

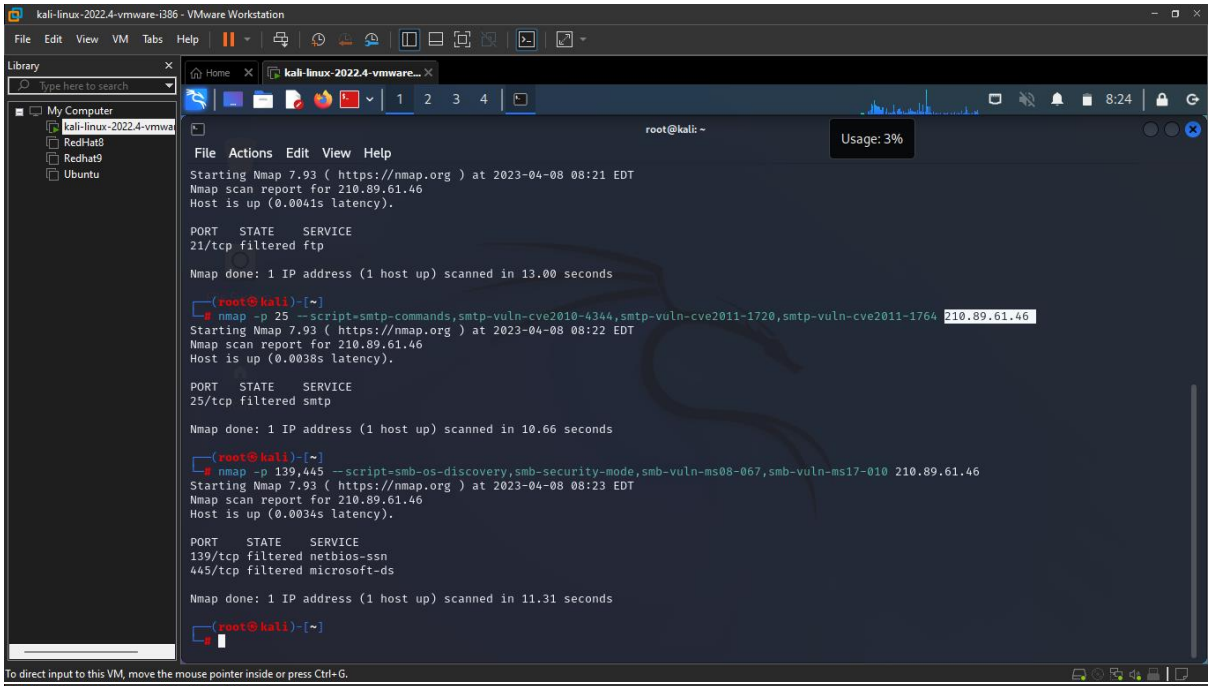
Analysis Report:-

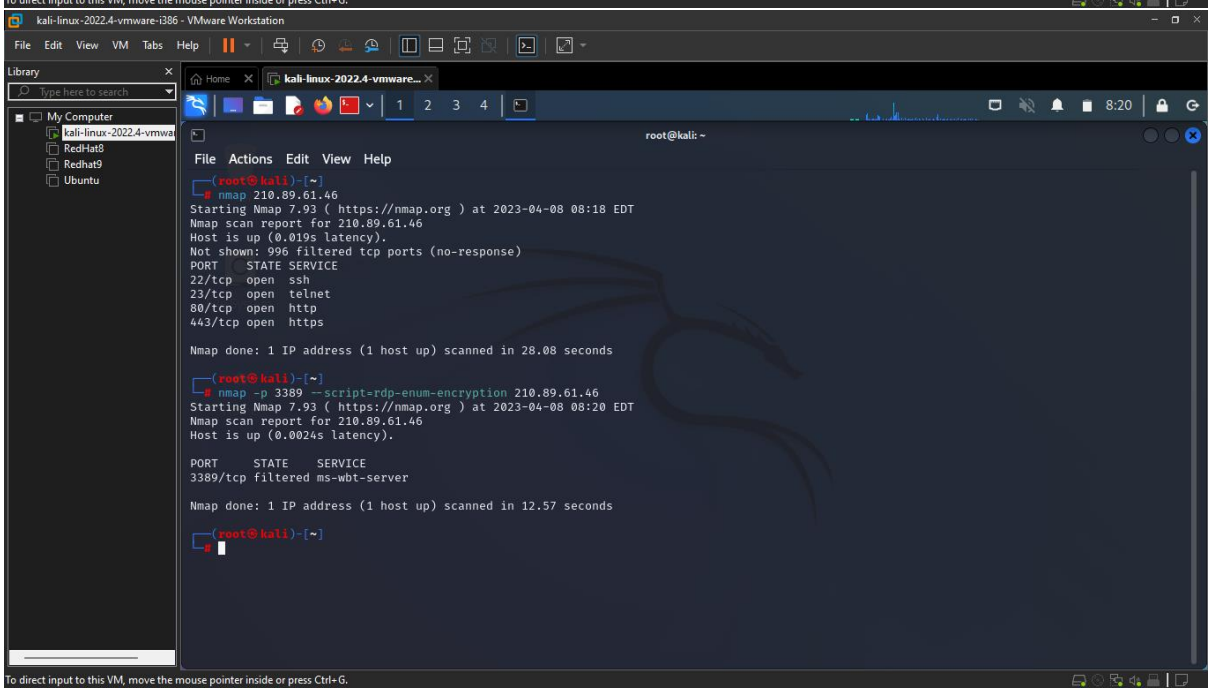
- **System Snapshots and Full analysis report**

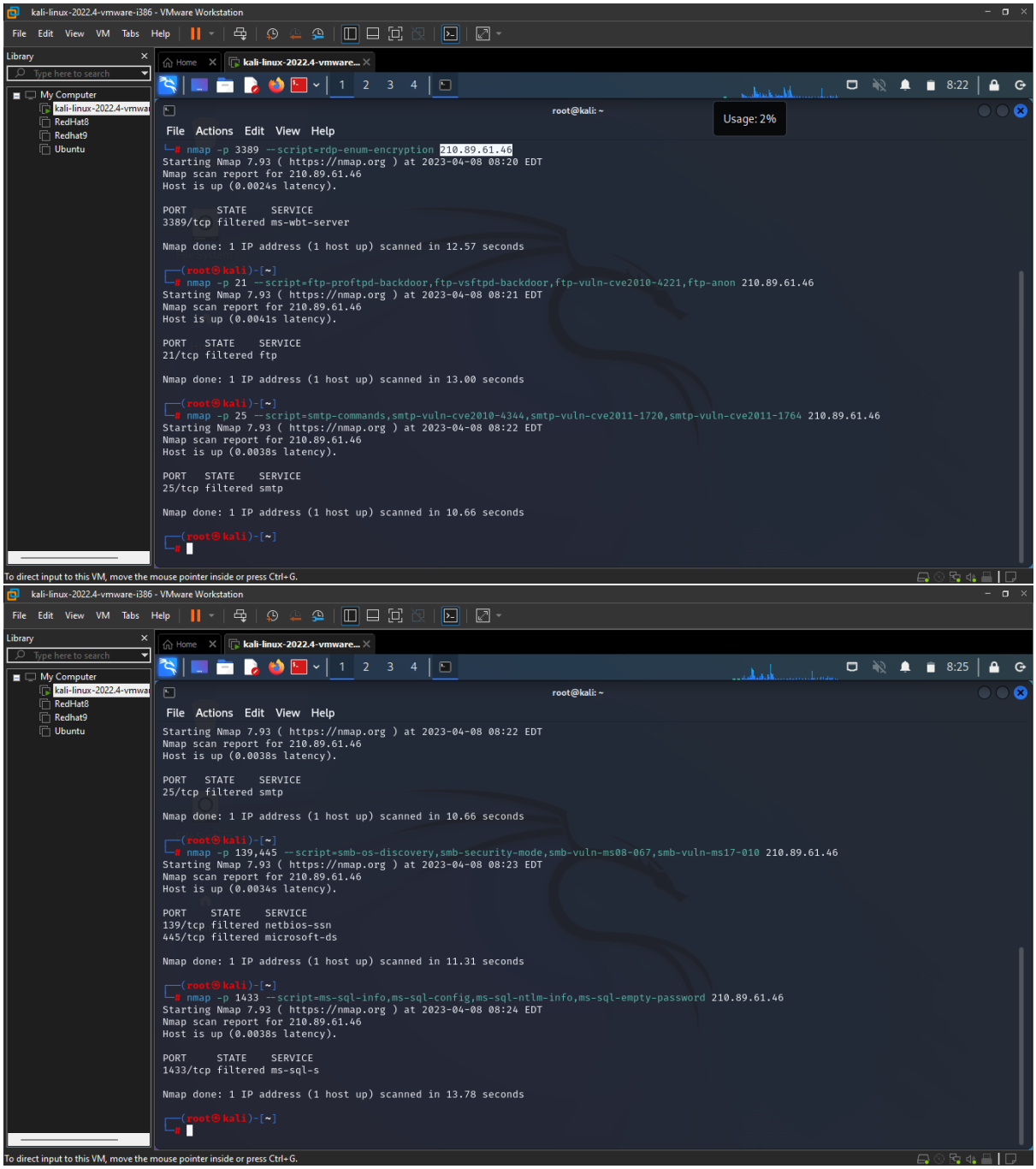
NMAP





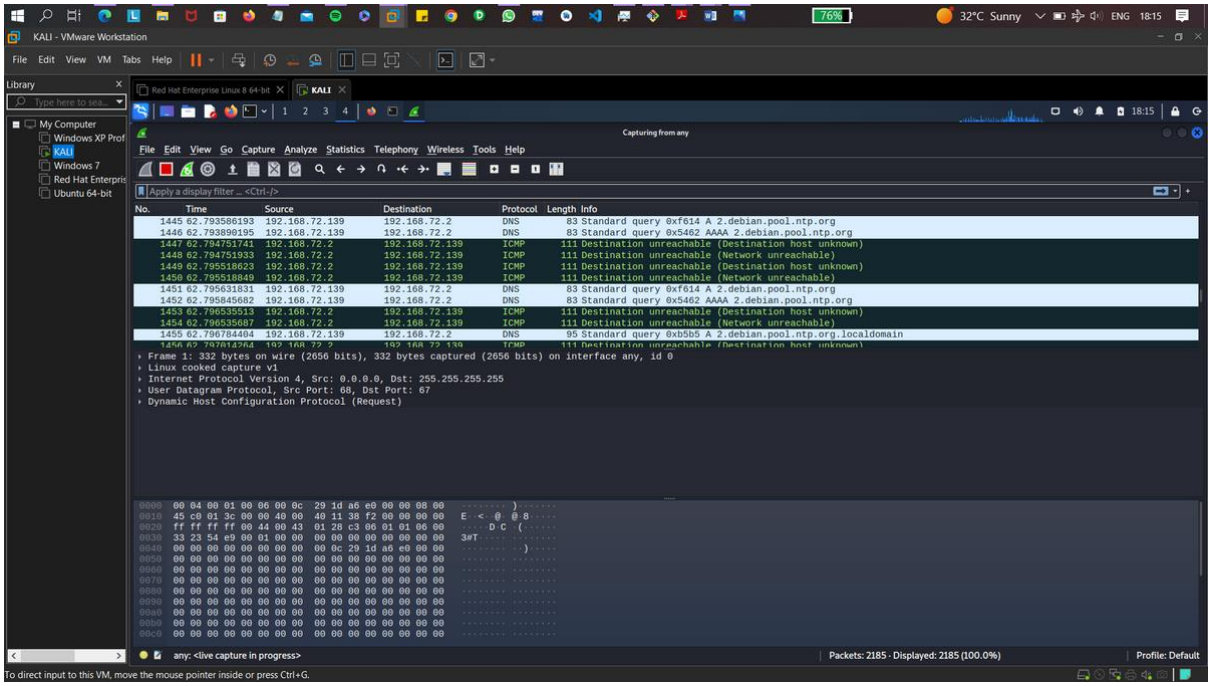

kali-linux-2022.4-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2022.4-vmwa
RedHat8
Redhat9
Ubuntu
Home
kali-linux-2022.4-vmware...
1 2 3 4
8:24
root@kali: ~
Usage: 3%
File Actions Edit View Help
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:21 EDT
Nmap scan report for 210.89.61.46
Host is up (0.0041s latency).
PORT STATE SERVICE
21/tcp filtered ftp
Nmap done: 1 IP address (1 host up) scanned in 13.00 seconds
(root㉿kali)-[~]
nmap -p 25 --script=smtp-commands,smtp-vuln-cve2010-4344,smtp-vuln-cve2011-1720,smtp-vuln-cve2011-1764 210.89.61.46
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:22 EDT
Nmap scan report for 210.89.61.46
Host is up (0.0038s latency).
PORT STATE SERVICE
25/tcp filtered smtp
Nmap done: 1 IP address (1 host up) scanned in 10.66 seconds
(root㉿kali)-[~]
nmap -p 139,445 --script=smb-os-discovery,smb-security-mode,smb-vuln-ms08-067,smb-vuln-ms17-010 210.89.61.46
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:23 EDT
Nmap scan report for 210.89.61.46
Host is up (0.0034s latency).
PORT STATE SERVICE
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 11.31 seconds
(root㉿kali)-[~]
#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali-linux-2022.4-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2022.4-vmwa
RedHat8
Redhat9
Ubuntu
Home
kali-linux-2022.4-vmware...
1 2 3 4
8:20
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
nmap 210.89.61.46
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:18 EDT
Nmap scan report for 210.89.61.46
Host is up (0.019s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet
80/tcp open http
443/tcp open https
Nmap done: 1 IP address (1 host up) scanned in 28.08 seconds
(root㉿kali)-[~]
nmap -p 3389 --script=rdp-enum-encryption 210.89.61.46
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:20 EDT
Nmap scan report for 210.89.61.46
Host is up (0.0024s latency).
PORT STATE SERVICE
3389/tcp filtered ms-wbt-server
Nmap done: 1 IP address (1 host up) scanned in 12.57 seconds
(root㉿kali)-[~]
#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali-linux-2022.4-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2022.4-vmwa
RedHat8
Redhat9
Ubuntu
Home
kali-linux-2022.4-vmware...
1 2 3 4
8:22
root@kali: ~
Usage: 2%
File Actions Edit View Help
└─# nmap -p 3389 --script=rdp-enum-encryption 210.89.61.46
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:20 EDT
Nmap scan report for 210.89.61.46
Host is up (0.0024s latency).
PORT STATE SERVICE
3389/tcp filtered ms-wbt-server
Nmap done: 1 IP address (1 host up) scanned in 12.57 seconds
┌──(root㉿kali)-[~]
└─# nmap -p 21 --script=ftp-proftpd-backdoor,ftp-vsftpd-backdoor,ftp-vuln-cve2010-4221,ftp-anon 210.89.61.46
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:21 EDT
Nmap scan report for 210.89.61.46
Host is up (0.0041s latency).
PORT STATE SERVICE
21/tcp filtered ftp
Nmap done: 1 IP address (1 host up) scanned in 13.00 seconds
┌──(root㉿kali)-[~]
└─# nmap -p 25 --script=smtp-commands,smtp-vuln-cve2010-4344,smtp-vuln-cve2011-1720,smtp-vuln-cve2011-1764 210.89.61.46
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:22 EDT
Nmap scan report for 210.89.61.46
Host is up (0.0038s latency).
PORT STATE SERVICE
25/tcp filtered smtp
Nmap done: 1 IP address (1 host up) scanned in 10.66 seconds
┌──(root㉿kali)-[~]
└─#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

kali-linux-2022.4-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2022.4-vmwa
RedHat8
Redhat9
Ubuntu
Home
kali-linux-2022.4-vmware...
1 2 3 4
8:25
root@kali: ~
File Actions Edit View Help
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:22 EDT
Nmap scan report for 210.89.61.46
Host is up (0.0038s latency).
PORT STATE SERVICE
25/tcp filtered smtp
Nmap done: 1 IP address (1 host up) scanned in 10.66 seconds
┌──(root㉿kali)-[~]
└─# nmap -p 139,445 --script=smb-os-discovery,smb-security-mode,smb-vuln-ms08-067,smb-vuln-ms17-010 210.89.61.46
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:23 EDT
Nmap scan report for 210.89.61.46
Host is up (0.0034s latency).
PORT STATE SERVICE
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 11.31 seconds
┌──(root㉿kali)-[~]
└─# nmap -p 1433 --script=ms-sql-info,ms-sql-config,ms-sql-ntlm-info,ms-sql-empty-password 210.89.61.46
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:24 EDT
Nmap scan report for 210.89.61.46
Host is up (0.0038s latency).
PORT STATE SERVICE
1433/tcp filtered ms-sql-s
Nmap done: 1 IP address (1 host up) scanned in 13.78 seconds
┌──(root㉿kali)-[~]
└─#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Wireshark:-



B)

Physical security testing: To perform physical security testing, as a network administrator, some of the techniques, tools, and methodologies that can be followed are:

Conducting physical security assessments to identify potential vulnerabilities in the physical security of the network devices.

Conducting physical access control tests to determine if access controls like key cards or biometric authentication are effective.

Testing the effectiveness of physical security policies and procedures like visitor management and employee access control.

Performing surveillance camera testing to ensure that surveillance cameras are working properly and are capturing the necessary footage.

Testing the effectiveness of alarm systems and response procedures.

Conducting social engineering tests to determine the effectiveness of physical security awareness training and policies.

Some open-source software that can be used to perform physical security testing are:

OpenCV: an open-source computer vision library that can be used to develop video surveillance applications.

Motion: an open-source software that can turn a webcam or camera into a motion detector.

Zoneminder: an open-source video surveillance system.

Fingerprint GUI: an open-source biometric authentication software for Linux.

Firefly: an open-source access control system.

The Social-Engineer Toolkit: a social engineering testing tool.

Github Repository Link:-

https://github.com/BhatejaDipak/CA3-Open-Source.git

References :-

- https://www.wireshark.org/docs/
- Nmap

• https://wiki.wireshark.org/Hyper_Text_Transfer_Protocolrk.org

• https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/

• https://www.kali.org/tools/wireshark/