

Experiment-7

Analyze and Exploit the Root System of CMROS

Date: 8/11/24

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

Step 1:

Open CMROS in VM-ware

Step 2:

Copy the IP address of CMROS and press any key.

Step 3:

Open the Kali Linux and power on the machine.

step4: Open terminal and enter 'ifconfig'

step5:

Open nmap and pasti the CMROS IP address as the target and scan.

step6:

In the Terminal of Kali Linux, enter nmap -p - 65535 -T4 -A -V 192.168.232.151

step7:

Open firefox in Kali and enter IP address. The right click select view page source. we get username and password as text.

step8:

open cmros and login

step9:

Then power off cmros and power on again.

↳ in kali give

ssh @ 192.168.232.151 -p 13652

give password.

test@vulnos: ~

step10:

> \$ ls

use whoami to find the user

> ~ \$ whoami

To know suspicious file

> \$ cd desktop

redirect Desktop

> /Desktop \$ ls

Cap.pcapng s3cr3t.txt

Step 4: Open terminal and enter 'ifconfig'

Step 5:

Open nmap and pasti -the CMROS IP address as the target and scan.

Step 6:

In the Terminal of Kali Linux, enter nmap -p - -65535 -T4 -A -V 192.168.232.151

Step 7:

Open firefox in Kali and enter IP address. Then right click Select view page source. we get username and password as text.

Step 8:

open cmros and login

Step 9:

Then power off cmros and power on again.

↳ in kali give

ssh@192.168.232.151 -p 13652

give password.

test@vuln0s: ~

Step 10:

> \$ ls

> w \$ whoami

> \$ cd desktop

> /Desktop \$ ls

Cap.pcapng \$3cr3t.txt

use whoami to find the user
To know suspicious file

redirect Desktop

Step 11: Go to WinSCP file protocol : sftp

Host name as IP address.

Port number : 13652

Step 12: open Kali Linux , search wireshark tool
open wireshark tool.

open cap.pcapng file in the wireshark from desktop folder.

Step 13: click any tcp filter and then right click →
click follow → TCP stream.

It display user Credentials.

Step 14:

Now copy and open cmos using Credentials we got

Now use ls

0: # ls

># cd Desktop

># ls

>cd home

>cd ..

>cd Desktop

>cd test

># ls → cap.pcapng s3cr3t.txt

>cat s3cr3t.txt

>37cedde2e98a22a53f12e53094e1fe268

>#

Don't do this