

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.

step 4: Open terminal and enter 'ifconfig'

step 5:

Open nmap and paste 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. The 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@vulnos: /

step 10:

> \$ ls

> ~ \$ whoami

> \$ cd desktop

> / Desktop \$ ls

cap.pcapng s3cr3t.txt

use whoami to find the user
To know suspicious file
redirect Desktop

step 4: Open terminal and enter 'ifconfig'

step 5:

Open nmap and paste 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. The 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 @ vulnos : /

step 10:

> \$ ls

> ~ \$ whoami

> \$ cd desktop

> / Desktop \$ ls

Cap.pcapng s3cr.txt

use whoami to find the user

To know suspicious file

redirect Desktop

step 11: Go to WINSCP file protocol : scp
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 top filter and then right click →
click follow → TCP stream.

It display user Credentials.

step 14:

now copy and open cmr02 using Credentials we
got
now use ls

OS: # ls

> # cd Desktop

> # ls

> cd home

> cd ..

> cd Desktop

> cd test

> # ls → cap.pcapng s3cr3t.txt

> cat s3cr3t.txt

> 37cedde2e98a22a53f12e57094e1tede268

> #

[Handwritten signature]