Experiment-7

Analyze and Exploit the Root System of CMROS

Date: 04-10-24

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

- 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 attacting 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 kalilinux browser and search cmros ip address
- Give a rightclick → 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 which is 'test'.

→ # ssh test@192.168.232.128 (cmos ip address) -p 13652

- It ask for the password, type the password as "test" it wont appear.
- Next use ls command.
- Use whoami to find the user.
- To know the suspicious file redirect to Desktop and use ls command.
- Now goto windows system, open browser and download WinSCP.
- It shows a login dialog box under the new state if there any other login delete them giving right click.
- Set the file protocol as SCP give hostname & cmos ip address, portnumber 13652, username & password as "test" → click on save → click on login → click on continue.

OUTPUT

- It shows goto Desktop and check the files present int 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 is 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. Nouse use ls command.

→# cd Desktop, →/Desktop# pwd, →/Desktop# cd..,
→# pwd, →# cd .., →# ls, →# cd Desktop,
→ #ls, → #cd home, →# cd.., →# cd.., →#ls,
→# cd home, →# cd desktop, →# ls, →# cd test,
→# ls, →/home/test # cd Desktop, →/home/test/Desktop#
→#/home/test/Desktop# cat s3cr3t.txt,

type command.

→ nano s3cr3t.txt, click ctrl x, ctrl Y,
it opens file and write anything in

type filename, next use command cat s3cr3t.tx
it displays the file content.