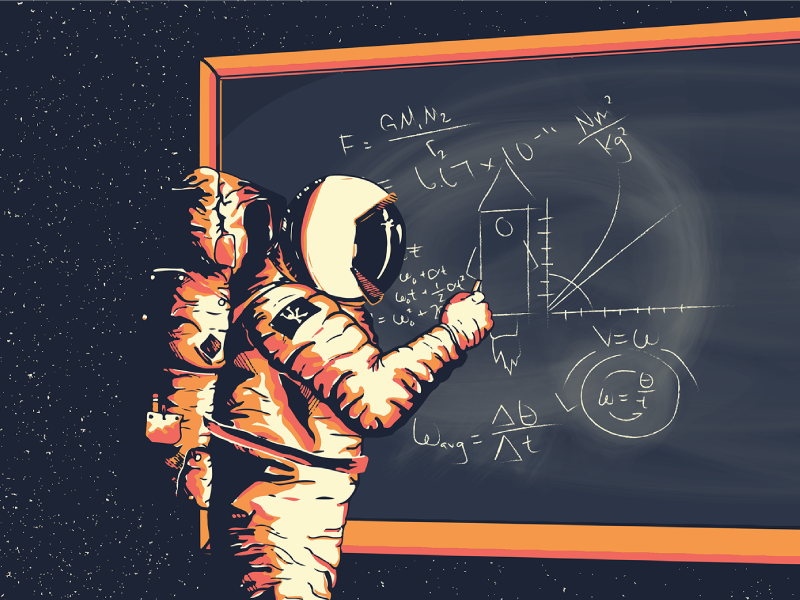
**Vulnversity Walkthrough**

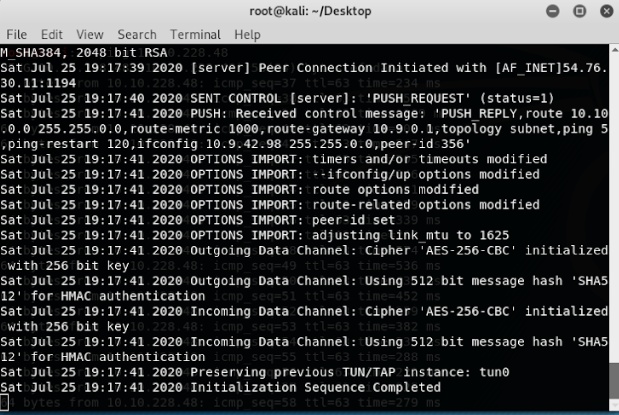
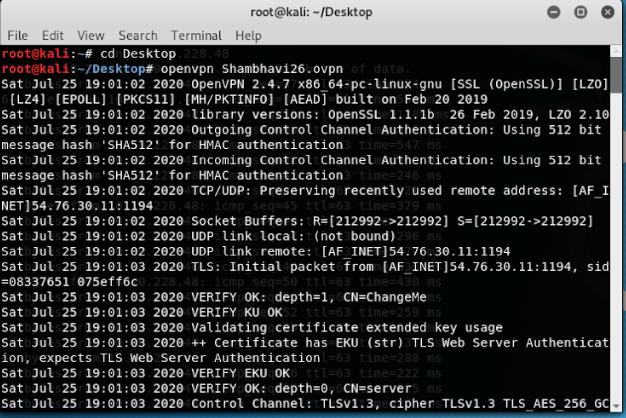


**Vulnversity covers the following tasks:**

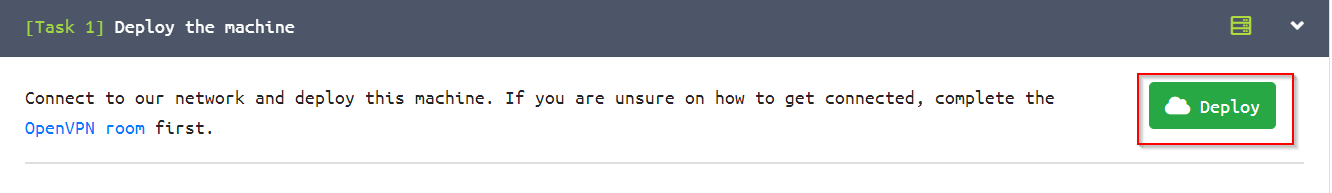
1. **Task1: *Deploy the machine***
2. **Task2: *Reconnaissance***
3. **Task3: *Locating directories using GoBuster***
4. **Task4: *Compromise the webserver***
5. **Task5: *Privilege Escalation***

**Task1: Deploy the machine**

**Before deploying the machine make sure your openvpn is connected .**

****

**When it shows Initialization Sequence Completed that means vpn is connected successfully .**

**Now click on Deploy to deploy the machine.**

**Task 2: Reconnaissance**

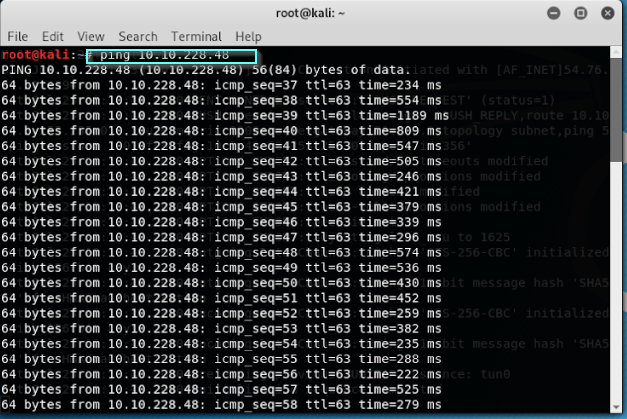
**Reconnaissance is a pentest phase where the tester performs information gathering. Tools such as nmap, gobuster, dirbuster, Maltago, Sparta, e.t.c are used to gather all the available information of a machine. This information can be an open port, range of IP address, potential vulnerability and user information.**

**Gather information about this machine using a network scanning tool called nmap.**

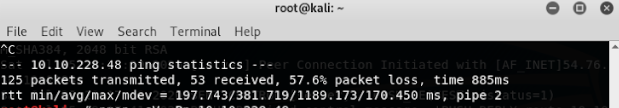
**nmap is an free, open-source and powerful tool used to discover hosts and services on a computer network. In our example, we are using nmap to scan this machine to identify all services that are running on a particular port. nmap has many capabilities, below is a table summarising some of the functionality it provides.**

|  |  |
| --- | --- |
| **nmap flag** | **Description** |
| **-sV** | **Attempts to determine the version of the services running** |
| **-p <x> or -p-** | **Port scan for port <x> or scan all ports** |
| **-Pn** | **Disable host discovery and just scan for open ports** |
| **-A** | **Enables OS and version detection, executes in-build scripts for further enumeration** |
| **-sC** | **Scan with the default nmap scripts** |
| **-v** | **Verbose mode** |
| **-sU** | **UDP port scan** |
| **-sS** | **TCP SYN port scan** |

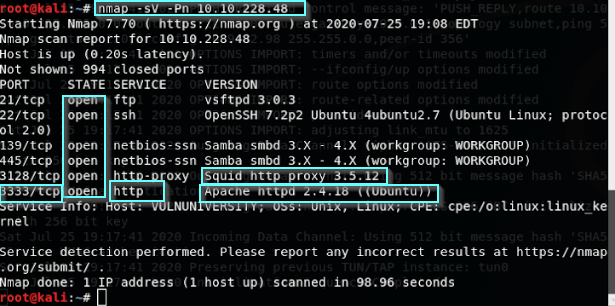
**First use ping command along with the IP address of the target machine to send ICMP Packets to the target machine and get the response from it .**

****

**Press ctrl+C to exit this command .**

****

**Now scan the box using the command : nmap -sV <machines ip>**

****

**Now from this we will be able to answer all the questions .**

|  |  |
| --- | --- |
|  | **Question: Scan the box, how many ports are open?**  **Solution: From the above snapshot its clear there are 6 ports are open.**  **Question: What version of the squid proxy is running on the machine?**  **Solution: 3.5.12**  **Question: How many ports will nmap scan if the flag -p-400 was used?**  **Solution: 400**  **Question: Using the nmap flag -n what will it not resolve?**  **Solution: DNS**  **Question: What is the most likely operating system this machine is running?**  **Solution: Ubuntu**  **Question: What port is the web server running on?**  **Solution: 3333(We will look for the port with http service ).**  **NOTE:**  **Its important to ensure you are always doing your reconnaissance thoroughly before progressing. Knowing all open services (which can all be points of exploitation) is very important, don't forget that ports on a higher range might be open so always scan ports after 1000 (even if you leave scanning in the background)**  **Task 3: Locating directories using GoBuster**  **Here we can also use dirbuster , dirb in place of gobuster.**  **GoBuster is a tool used to brute-force URIs (directories and files), DNS subdomains and virtual host names. For this machine, we will focus on using it to brute-force directories.**  **To get started, you will need a wordlist for GoBuster /dirbuster/dirb (which will be used to quickly go through the wordlist to identify if there is a public directory available. If you are using**[**Kali Linux**](https://tryhackme.com/room/kali)**you can find many wordlists under /usr/share/wordlists.**  **Command for gobuster : gobuster dir -u http://<ip>:3333 -w <word list location>**  **Explanation on the flag:**   * **-u: target URL** * **-w: wordlists**     **If we wish to use dirb use this command:**      **The hidden directory is called ‘internal’ where we can upload a file to perform a potential exploitation.**  **Question: What is the directory that has an upload form page?**  **Solution: /internal/**  **Task 4: Compromise the webserver**  **Now you have found a form to upload files, we can leverage this to upload and execute our payload that will lead to compromising the web server.**  **First open the form page on the browser by using**  **Ip address:portnumber/internal/**    **This is the upload form page which will be displayed. Now in order to check which extension is not allowed first download php-reverse-shell-1.0.tar.gz and then extract that file .**    **Now upload the .php file on the form page and it will show extension not allowed.**      **Question. Try upload a few file types to the server, what common extension seems to be blocked?**  **Solution: .php**  **To identify which extensions are not blocked, we're going to fuzz the upload form. To do this, we're doing to use BurpSuite.**  **Now upload .php file and start the burpsuite and use foxy proxy and turn on burp and click on submit button on the upload form page so that we can intercept the request on burp .**  **Now right click on request and send it to intruder . Inside the positions make changes in filename as shown in the blue box by adding $ and clearing $ .**    **Now move to payloads and add payload options as shown in the below blue box.**    **Now start the attack and check for the lengths. Check the response of the extension with different length.**  **Now check for its response by clicking on it. And check the whole html code at the last it will show success i.e this extension is allowed.**    **Now convert.php file into .phtml file and change the port number(between 1000 to 9000) and mention the ip address of the file to the ip address of tun0 (use ifconfig and find the ip address of openvpn and use that).**  **Now submit that file into upload form page and it will show success.**    **Question: Run this attack, what extension is allowed?**  **Solution: .phtml**  **We're now going to listen to incoming connections using netcat. Run the following command: nc -lvnp 1234(or the port no which you have specified in the .phtml file)**  **Upload your shell and navigate to http://<ip>:3333/internal/uploads/php-reverse-shell.phtml - This will execute your payload You should see a connection on your netcat session.**    **In order to find the name of the user who manages the web server use the command cat /etc/passwd**  **In order to find the user flag use the following commands :**  **Cd /home**  **ls**  **cd /bill**  **ls**  **This will give the user flag:** **8bd7992fbe8a6ad22a63361004cfcedb**    **Task 5: Privilege Escalation**  **Now you have compromised this machine, we are going to escalate our privileges and become the superuser (root).**  **In Linux, SUID (set owner userId upon execution) is a special type of file permission given to a file. SUID gives temporary permissions to a user to run the program/file with the permission of the file owner (rather than the user who runs it).**  **For example, the binary file to change your password has the SUID bit set on it (/usr/bin/passwd). This is because to change your password, it will need to write to the shadowers file that you do not have access to, root does, so it has root privileges to make the right changes.**  https://i.imgur.com/ZhaNR2p.jpg  **In order to search for all the suid files use the below command in the red box:**    **And the file which stands out is /systemctl/**    **Now in order to become a root and find the final flag type the following commands in the below red box :** |
|  |  |