Hack the Box Challenge: Sense Walkthrough

Hello friends!! Today we are going to solve another CTF challenge “**Sense**” which is available online for those who want to increase their skill in penetration testing and black box testing. sense is retried vulnerable lab presented by **Hack the Box** for making online penetration practices according to your experience level, they have collection of vulnerable labs as challenges from beginners to Expert level. We are going to start a new series of hack the box beginning with **Sense** craft which is designed for beginners.

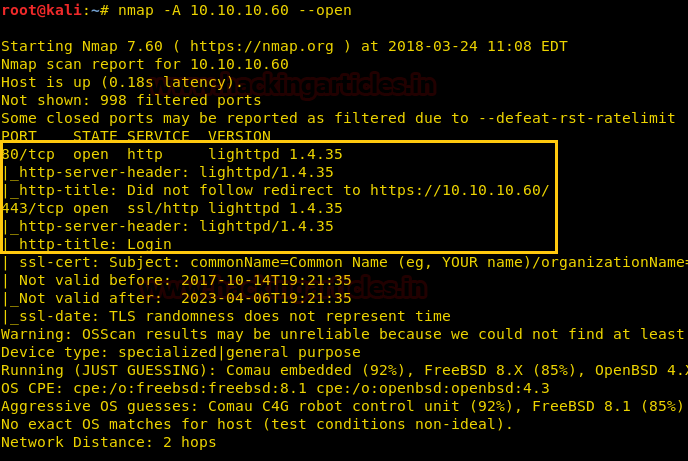
**Level:**Intermediate

**Task:** find **user.txt** and **root.txt** file in victim’s machine.

Since these labs are online available therefore they have static IP and IP of sense is **10.10.10.60** so let’s begin with nmap port enumeration.

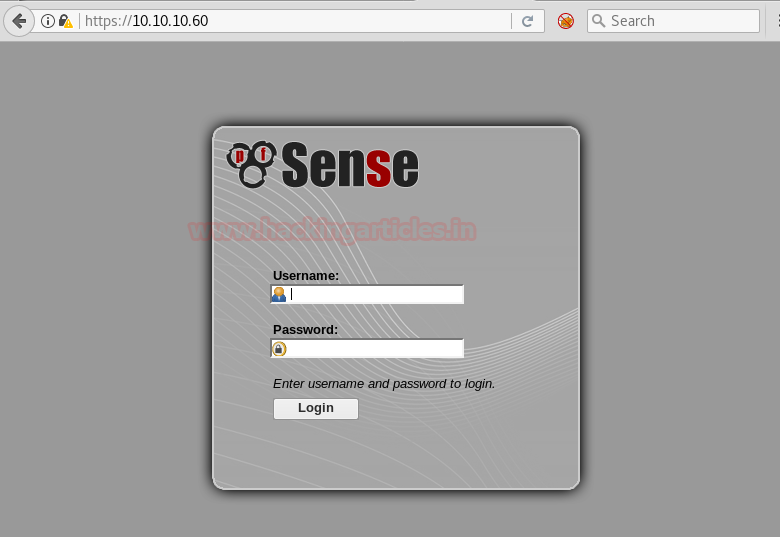


|  |  |
| --- | --- |
| 1 | nmap -A 10.10.10.60 --open |

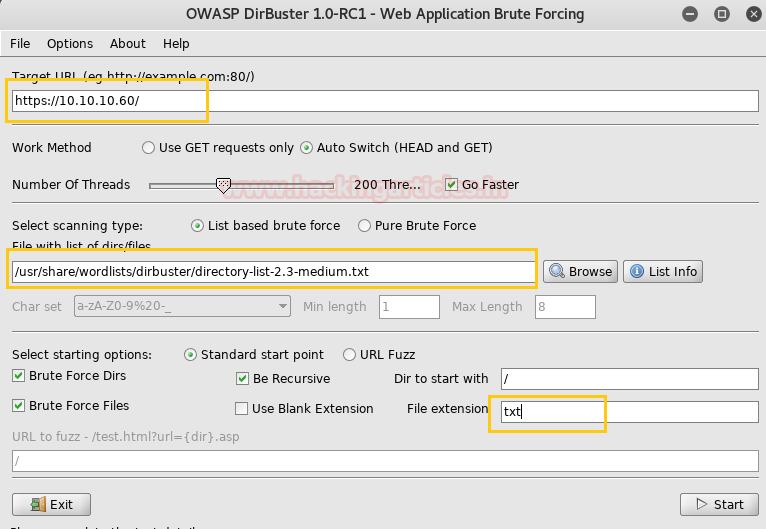


From given below image, you can observe we found port 80, 443 are open in victim’s network.

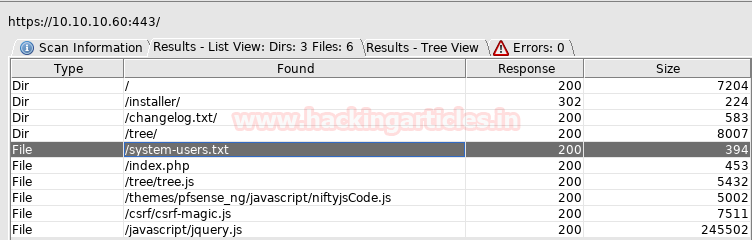
Knowing port 80 is open in victim’s network we preferred to explore his IP in browser but didn’t get any remarkable clue on its PF Sense Login Portal for next step.



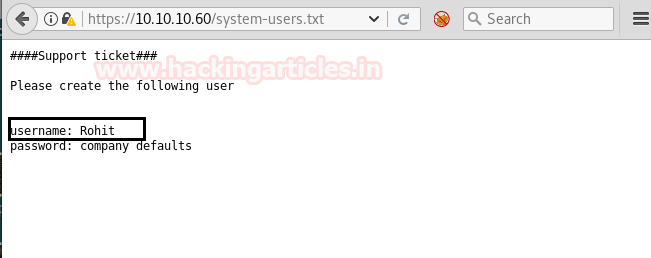
Now we have this Login Portal using **DirBuster** **Tool**. As you can see we have given Target IP https://10.10.10.60/ in the Target URL option. And we have given the path of the directory we want to enumerate which is **/usr/share/wordlists/disbuster/directory-list-2-3-medium.txt** .  In **File Extension** option we have given the format of the file which is txt . Then Click on start for **BruteForcing**.



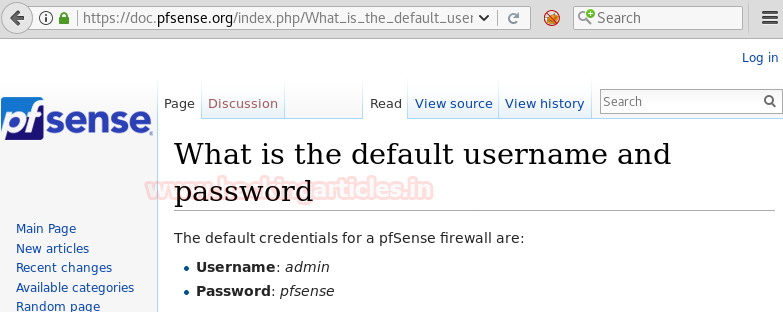
After going through all the directories and file’s we came up with a conclusion that **system-users.txt**has the clue for our next step.



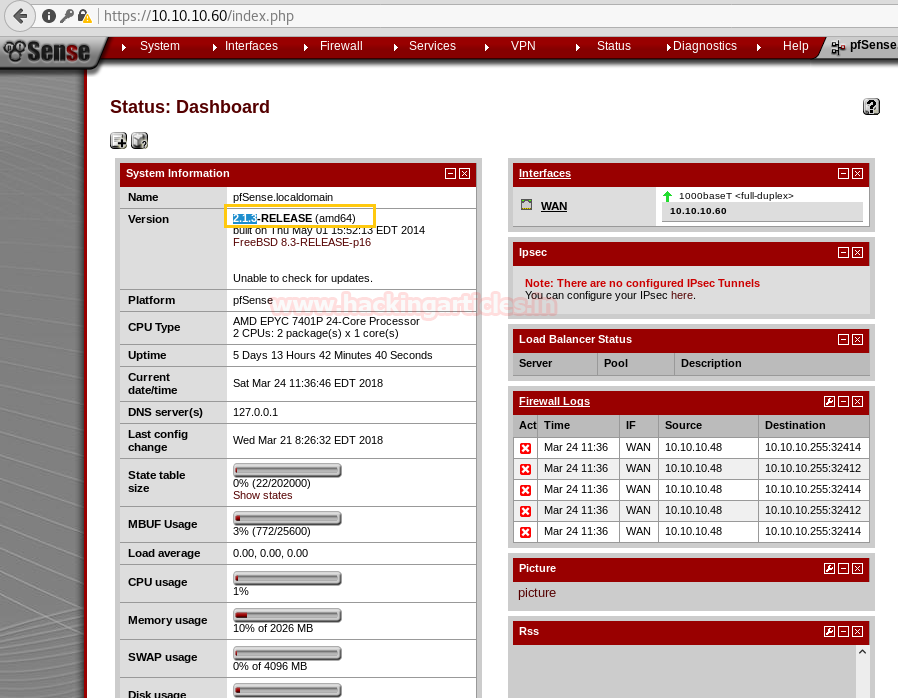
Now we have simply accessed the file using the browser by giving an input of **https://10.10.10.60/system-users.txt ,**what we saw was a Username and Password which can be used to accessed Sense Login portal. But giving these inputs didn’t actually log us in.



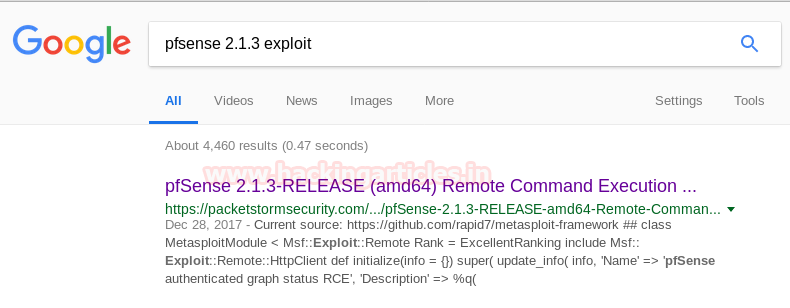
This made us curious, then we decided to take a little help from google. We searched for the default username and password for **PFSENSE.**The result we got can be seen in image below.



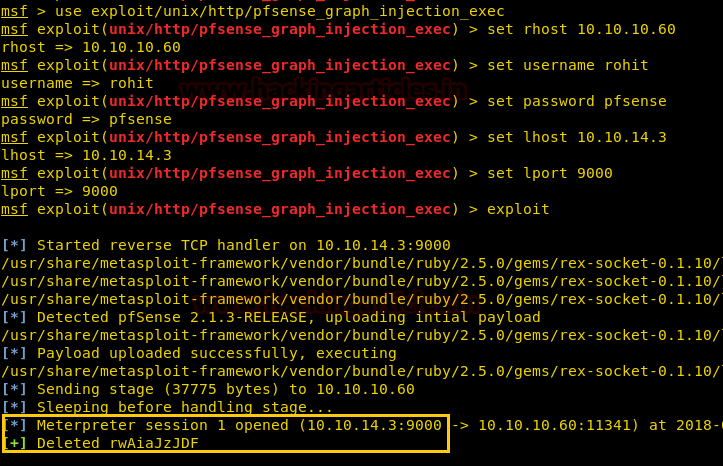
Than we have given username as rohit and password as pfsense. Where r is in small letter these credentials have successfully logged us into the pfsense portal.



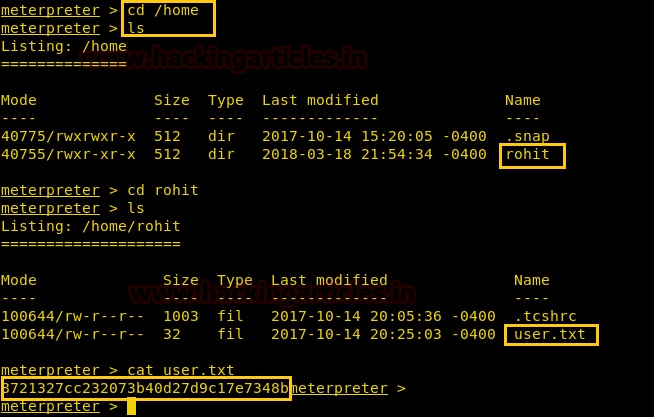
We figured out that we should try searching for the pfsense version which is 2.1.3 on google. And as usual it came out to be an Remote Command Execution Exploit.



Once we are assured of the username and password, we have used metasploit exploit and got the meterpreter as you can see below.



Once we have got the meterpreter. We have used command **cd /home**to check what kind of directories are on home. Than we check inside the **rohit** directory using **command ls /home/rohit**, here we found out the user.txt file and used **cat user.txt** to read the file content which contains our first **FLAG!!**



After getting our first **FLAG.**We have used shell command and whoami command which has displayed the current user which is root, then after getting into root directory we have used ls command which gave us the root.txt file. Whose content we would like to see by using the **cat root.txt** command. **Finally we found our final FLAG!!**



**Author**: Ashray Gupta is a Researcher and Technical Writer at Hacking Articles**.**He is a certified ethical hacker, web penetration tester and a researcher in nanotechnology. Contact [**Here**](https://www.linkedin.com/in/ashray-gupta-b77221b6/)