### **Cybersecurity 401**

**Module 9 - Pentesting**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **Lab 42 - Pentest Practice 1 of 2**

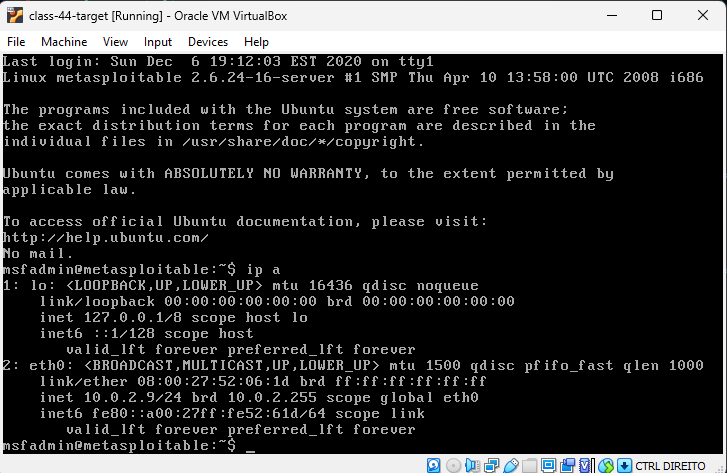
## 

## 

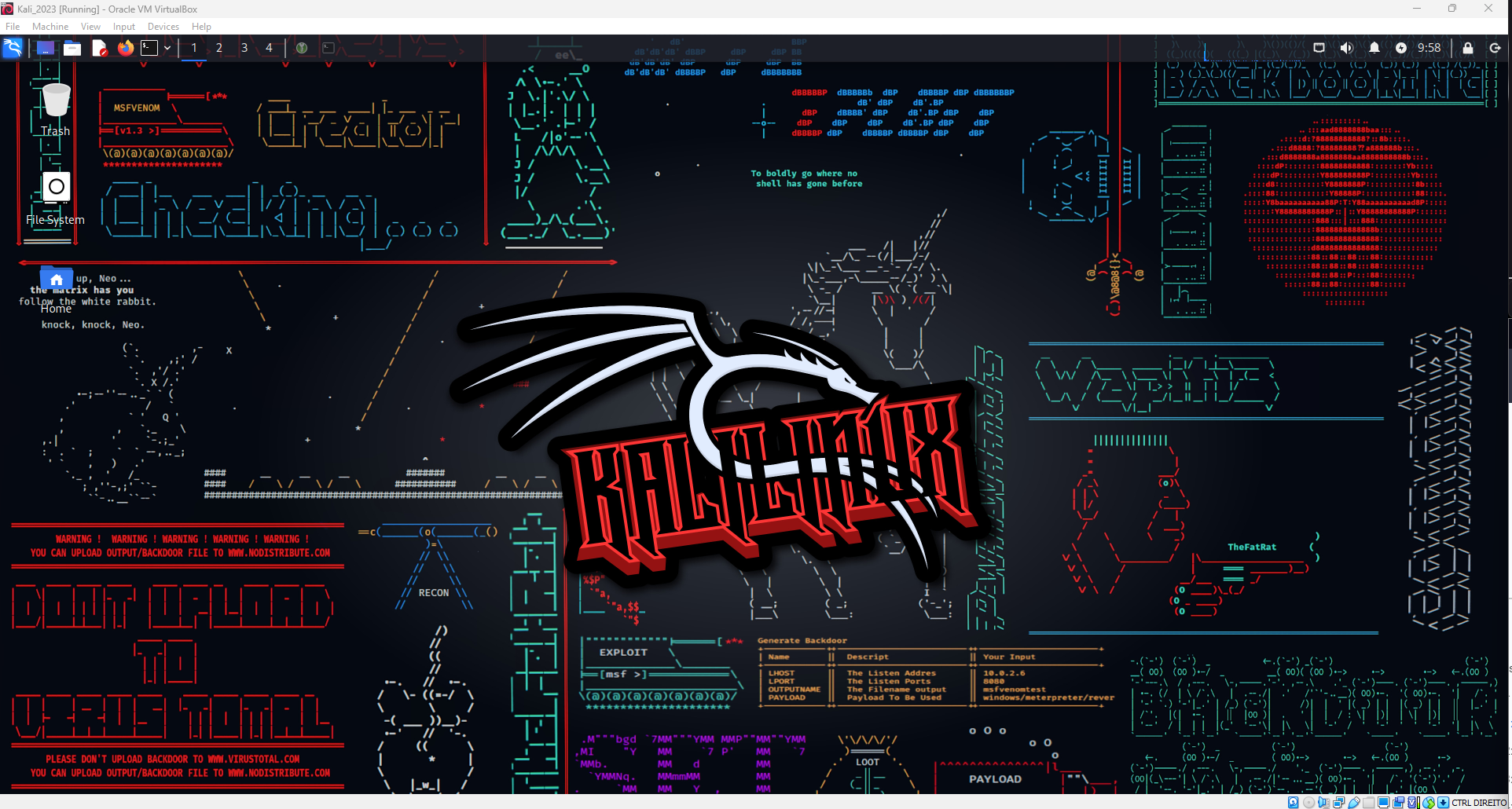
**| Rodrigo Brasil 01/2024 |**

### **Part 1: Staging**

**First, import the class-44-target.ova into Virtualbox. Assign it to NAT Network alongside your Kali Linux VM.**

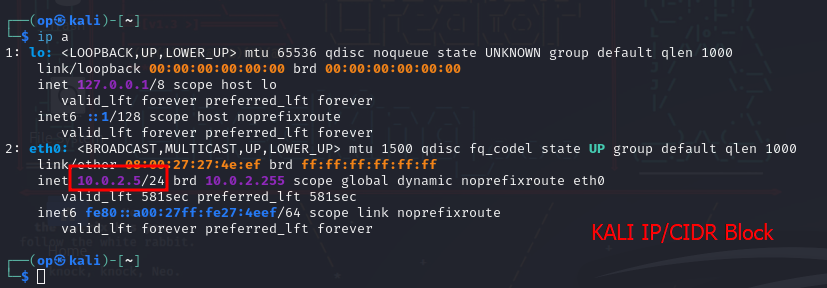
****

**Next, import a Kali VM into Virtualbox. Load all pentest scripts into this VM. Assign it to a NAT Network alongside your target box. You may opt to use your own existing Kali Linux instead, if you prefer.**

****

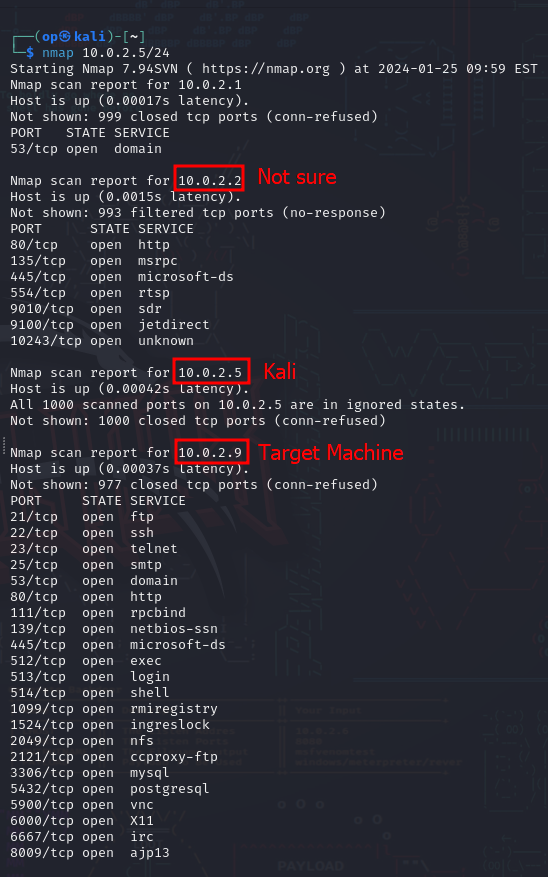
### **Part 2: Enumeration**

**Now that you have imported the target system to Virtualbox, first determine its IP address using an enumeration tool of your choice.**

****

****

Using the command nmap with the kali VM ip and adding the CIDRblock it will enumerate the ip’s on the same network has kali

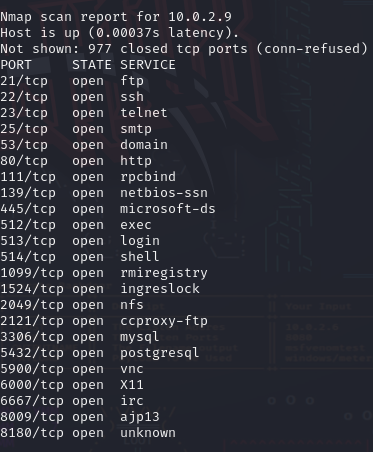
****

The results show **3 IP’s** one being the kali VM and 2 others

by looking at the open ports we can assume that the ip with the most open ports (**10.0.2.9**) is our target machine.

**After identifying the target system’s IP, you’ll need to get an idea of its vulnerabilities by using techniques such as:**

* **Port scanning**

****

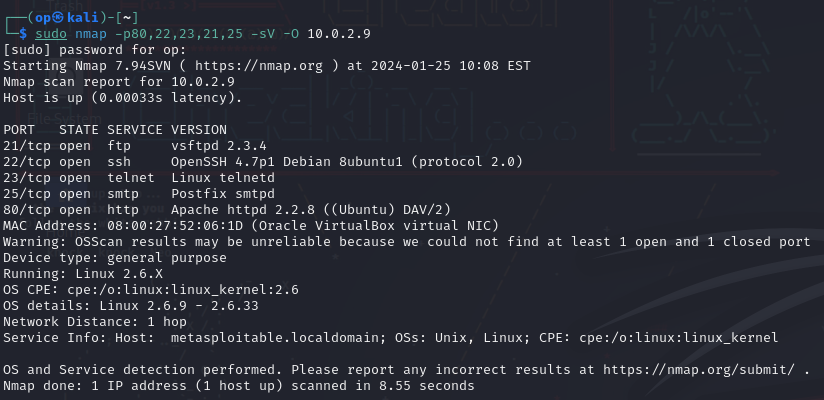
Having now the knowledge of these open ports and the IP

****

Using the tool nmap with the flags:

-p to specify the ports 80, 22, 23, 21, 25

-sV to enumerate the services running on the specified ports and -O to enumerate what OS is the target running, we will perform the scan.

****

Results from the scan

From these results it is possible to see what services and versions of them are running on the specified ports and the OS which is linux with the kernel version 2.6.

with this information we can scan for vulnerabilities

* **Vulnerability scanning**

****

Using the tool nmap with the same flags has before but adding a new one --script

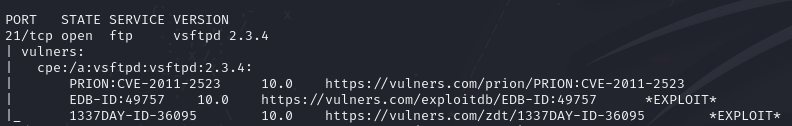
There are 3 scripts we can use to search for exploits:

* **vuln**
* **vulners**
* **vulnscan**

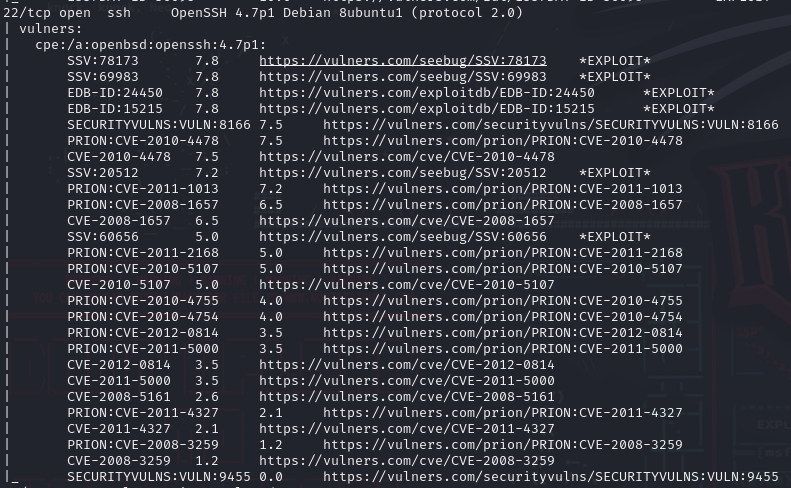
For this case it was used **vulners**

using the flag -- script we will specify the script **vulners** to search for known vulnerabilities for the services versions gathered

because we specified the ports it will give only the vulnerabilities for the services running on those ports rather then all of them



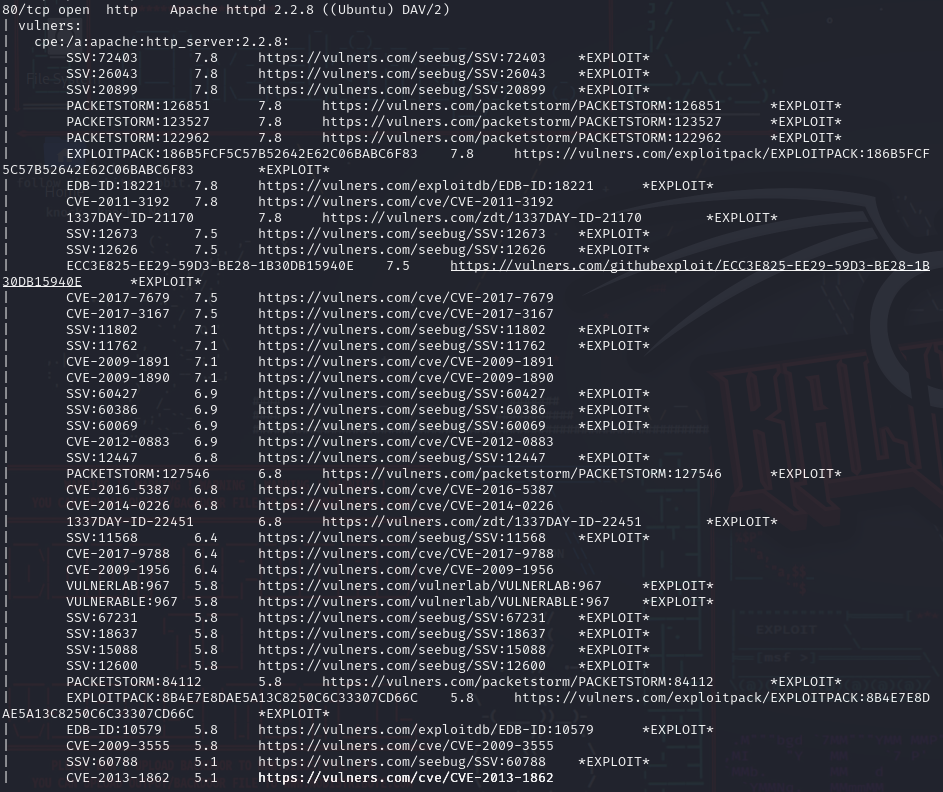
Starting with the port 21 with the service ftp version vsftpd 2.3.4

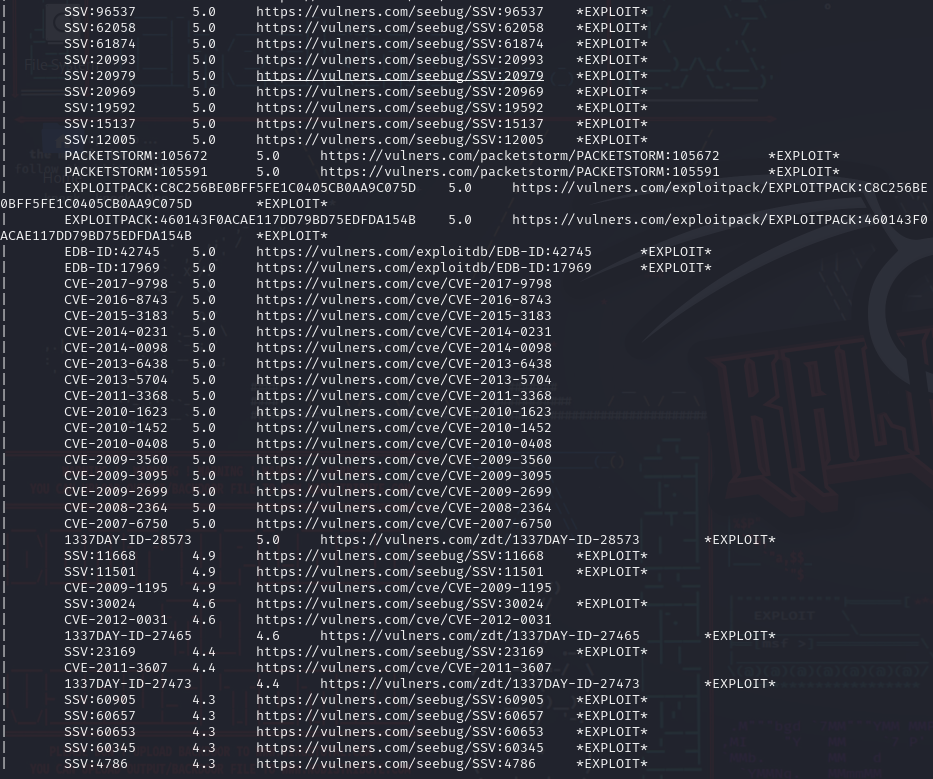


at port 22 with the service ssh version openssh 4.71p



Port 23 and 25 no vulnerabilities were found



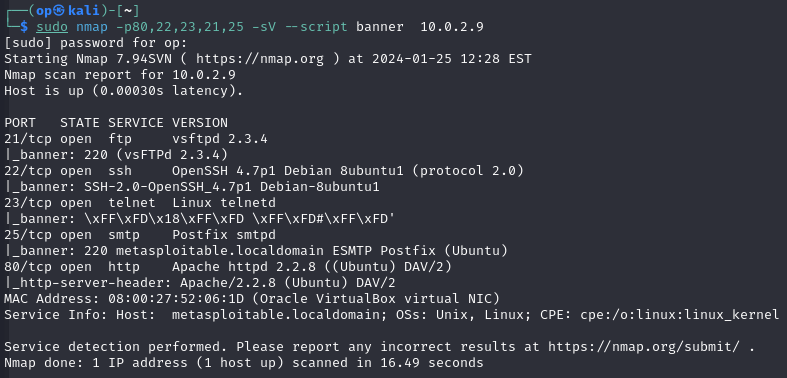




Port 80 were found alot

* **Banner grabbing/service fingerprinting**

****

****

**Based on your findings, determine how you will exploit the target’s weaknesses and gain access. Be sure to document the information you uncovered about the target.**

### 

### **Part 3: Exploitation**

**It appears this PC has quite a few vulnerabilities; in this stage, you will be performing attack techniques against the target in order to gain access. Techniques you may consider include:**

* **Brute force authentication**

****

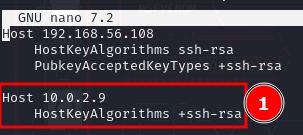
Firstly tried to simply login without any user



but had this error



To fix it had to go to kali´s ssh config file



And add the host that i'm trying to login and its key algorithm



Trying to login again asked for a password with the user from my machine

which is not what i want and i don't know what users are available on the other machine

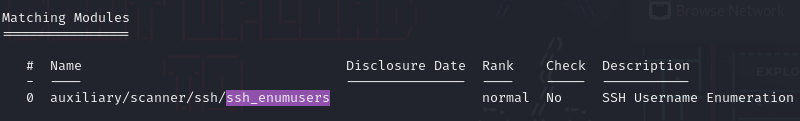
so i'm going to enumerate the ssh users available using an auxiliary ssh scanner from metasploit

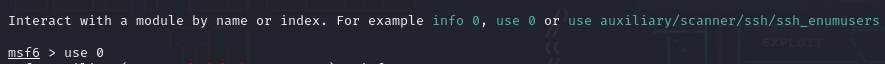


Launching metasploit with “**msfconsole**”



using search to search for the ssh\_enumusers scanner module



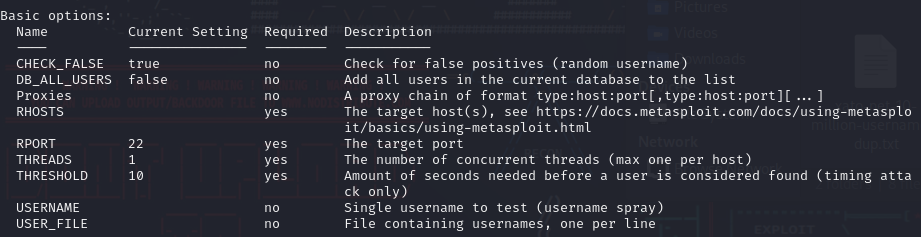


Using the tip given by metasploit to use the module with “use 0”



selected the module

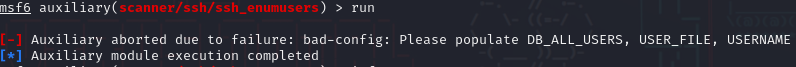




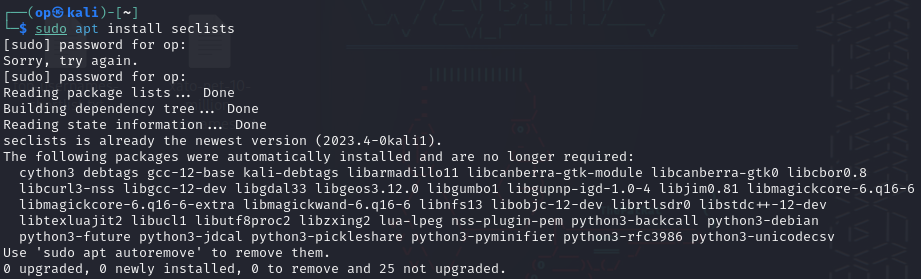
Typing info to show how to use this module



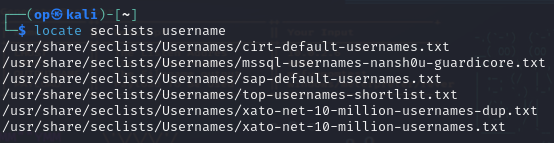
Gave it the target machine IP has the RHOST



Even tho the module info said that only the RHOST is necessary it still gave an bad config error asking for a user list, username or a database

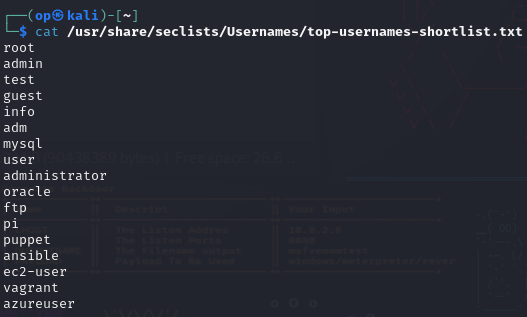


so ended up downloading and using seclists



using the locate command for usernames lists on seclists, it showed 6 username lists





i chose top usernames shortlist because it is a very small list and has some basic usernames that might be detected my the enum module



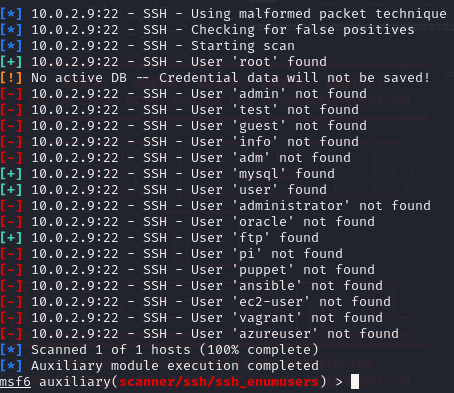
Jumping back to metasploit, set the USER\_FILE option with the username list



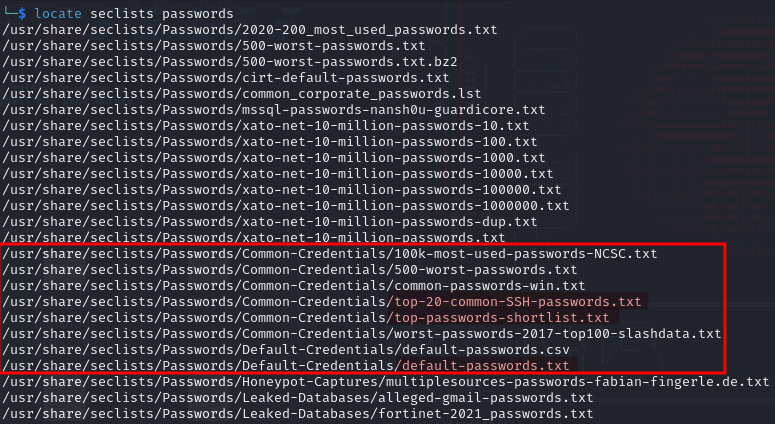
And set verbose to true



ran the module



Now with the results from the enum module im going to try to brute force the password from the users that it found starting with the user “user”



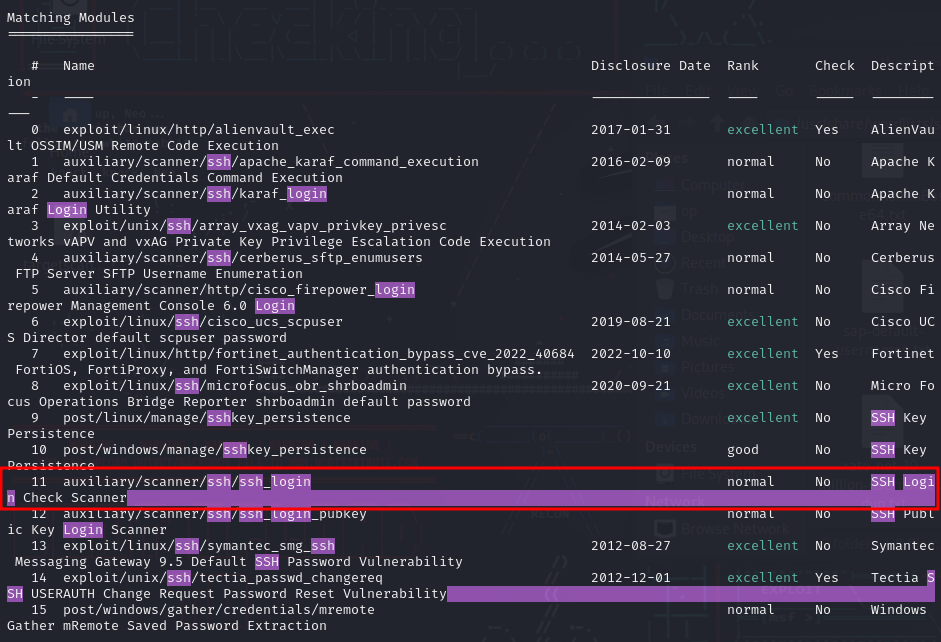




Tried to use hydra to brute force the password but was always getting an error related to the key algorithms so jumped back to metasploit



Using search to search for the ssh login scanner module



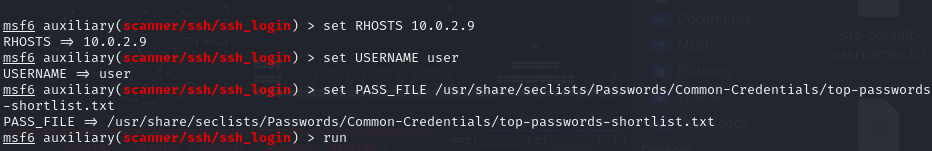


use the module with “use 11”





Typing info to show how to use this module

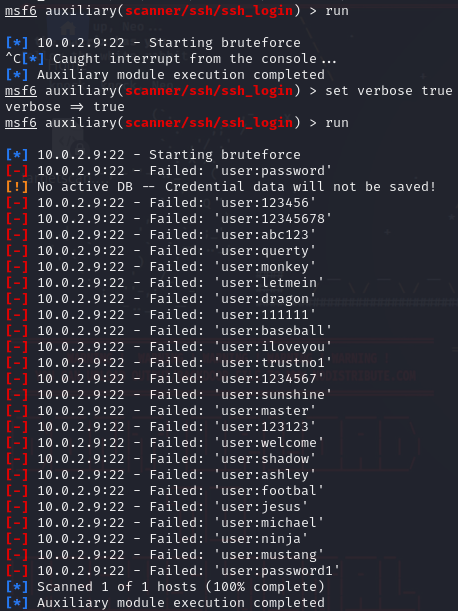


Set the RHOSTS to the target IP 10.0.2.9

Set the username as “user”

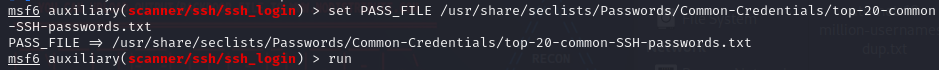
Set the PASS\_FILE to the password list to **top-passwords-shortlist.txt**

and run the module



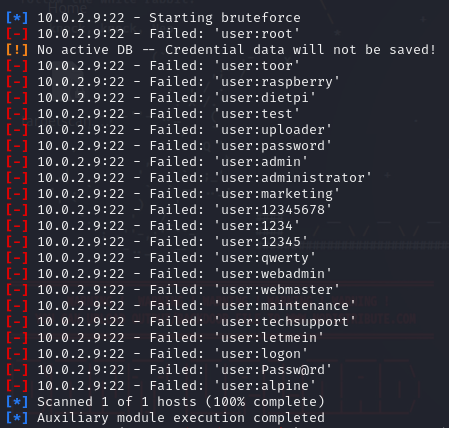
Forgot to enable verbose mode so stopped the module with ctrl + c

set verbose mode to true and ran it again

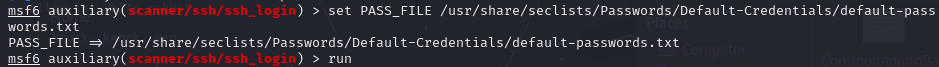


after it finished the brute force wasn't successful so changed the password list to **top-20-common-ssh-passwords.txt**

and ran the module again

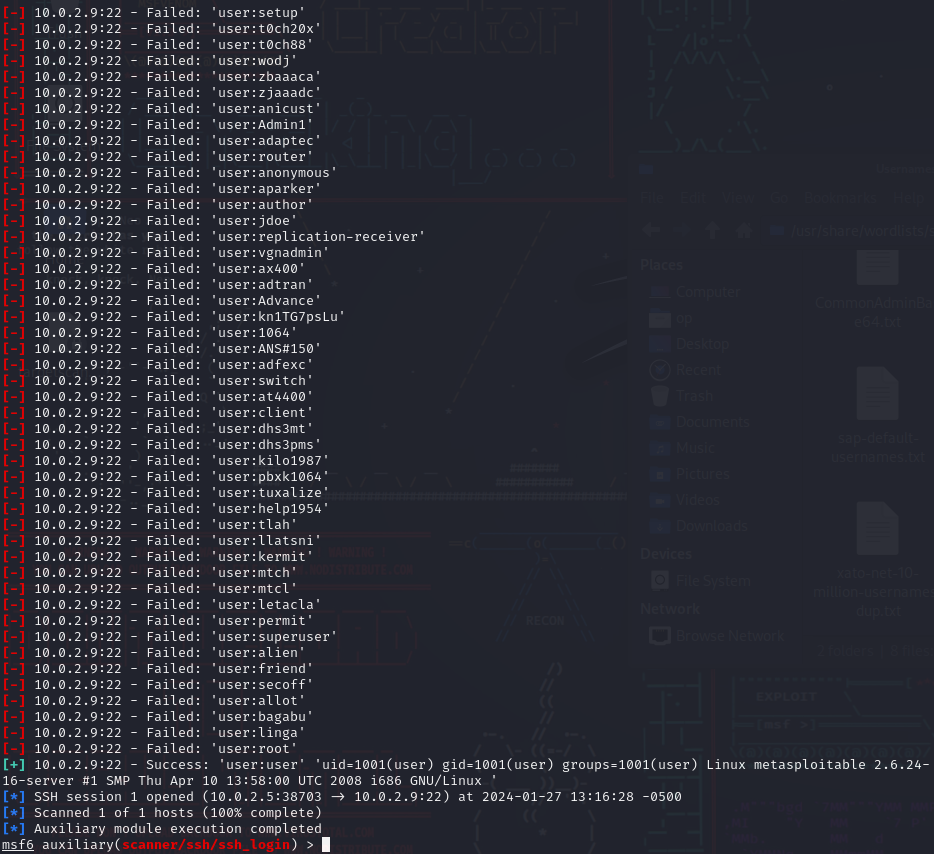


Second time wasn't it



So decided to change the password list again to **default-passwords.txt**

This list is bigger than the other two so it took a little bit longer



but the third time’s the charm



finally got a match

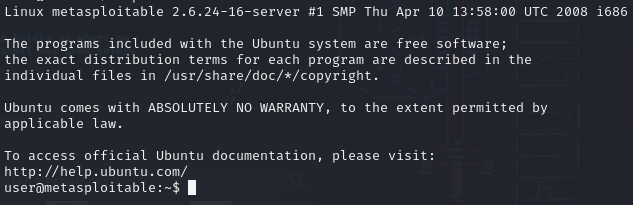
The “user” password was “**user**”…



Attempt to login with the “**user**” onto the target



Using the found password “**user**”



Successfully logged into the target



has “**user**”

* **Shell connectivity**
* **Privilege escalation**

**It is important to carefully document your attacks, as you’ll need to craft a detailed report for this lab.**

### 

### **Part 4: Reporting**

**Document your findings in the OSCP-OS-XXXXX-Lab-Report\_Template3.2.docx file, removing any irrelevant templated example data. Upload this file to your Google Drive and link to it in your submission.**

**An effective report should be well-organized, free of typos/formatting issues, technically accurate, comprehensive, and generally valuable to a decision maker or stakeholder.**