

***Task 1 - Get Connected***

Ready? Let's get going!

No answer needed

***Task 2 - Understanding NFS***

Answer the questions below

What does NFS stand for?

Network File System

What process allows an NFS client to interact with a remote directory as though it was a physical device?

Mounting

What does NFS use to represent files and directories on the server?

file handle

What protocol does NFS use to communicate between the server and client?

RPC

What two pieces of user data does the NFS server take as parameters for controlling user permissions? Format: parameter 1 / parameter 2

user id / group id

Can a Windows NFS server share files with a Linux client? (Y/N)

Y

Can a Linux NFS server share files with a MacOS client? (Y/N)

Y

What is the latest version of NFS? [released in 2016, but is still up to date as of 2020] This will require external research.

4.2

Run an nmap scan of your choice.

How many ports are open on the target machine?

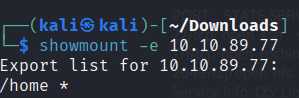
7

Which port contains the service we're looking to enumerate?

2049

Now, use /usr/sbin/showmount -e [IP] to list the NFS shares, what is the name of the visible share?

/home

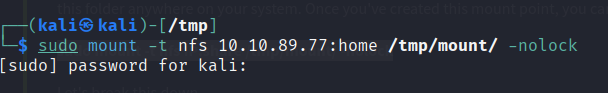


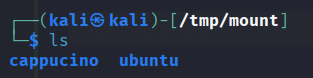
Time to mount the share to our local machine!

First, use "mkdir /tmp/mount" to create a directory on your machine to mount the share to. This is in the /tmp directory- so be aware that it will be removed on restart.

Then, use the mount command we broke down earlier to mount the NFS share to your local machine. Change directory to where you mounted the share- what is the name of the folder inside?

Cappucino



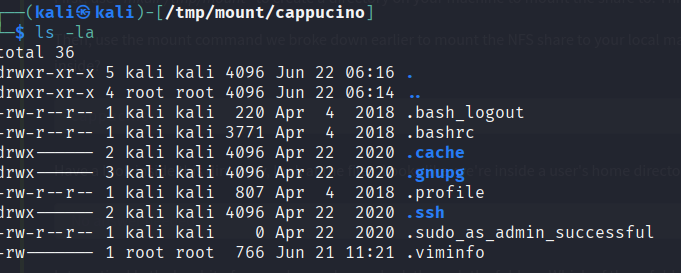


Have a look inside this directory, look at the files. Looks like we're inside a user's home directory...

No answer needed

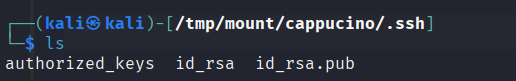
Interesting! Let's do a bit of research now, have a look through the folders. Which of these folders could contain keys that would give us remote access to the server?

.ssh

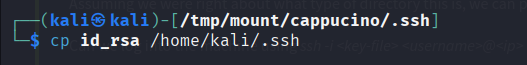


Which of these keys is most useful to us?

id\_rsa



Copy this file to a different location your local machine, and change the permissions to "600" using "chmod 600 [file]".

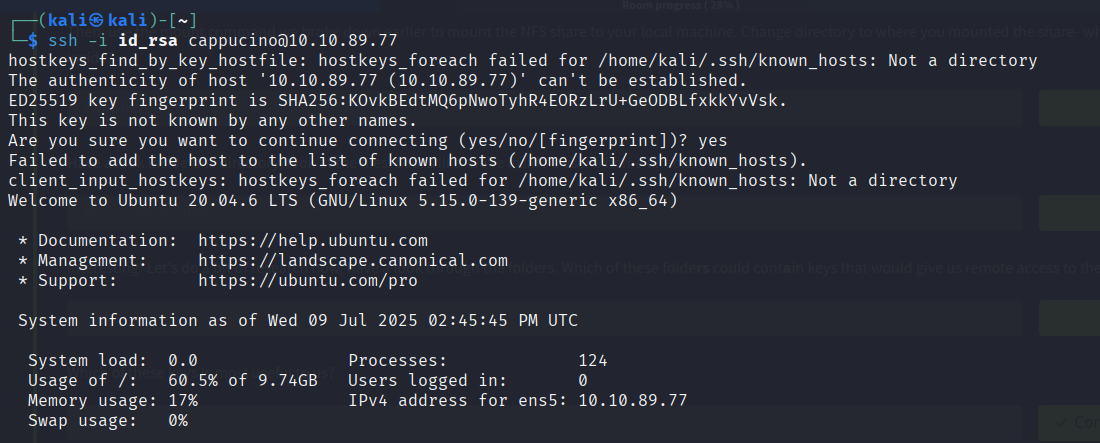




Assuming we were right about what type of directory this is, we can pretty easily work out the name of the user this key corresponds to.

Can we log into the machine using ssh -i <key-file> <username>@<ip> ? (Y/N)

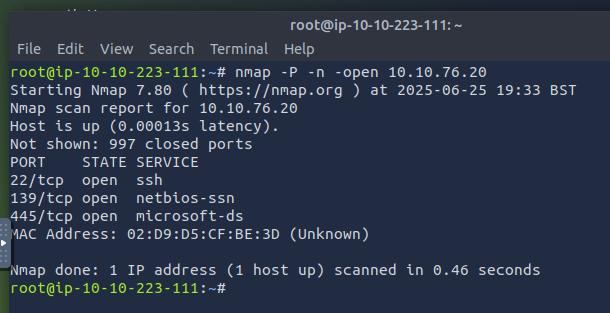
Y



***Task 3 - Enumerating SMB***

***Conduct an nmap scan of your choosing, How many ports are open?***

3



***What ports is SMB running on? Provide the ports in ascending order.***

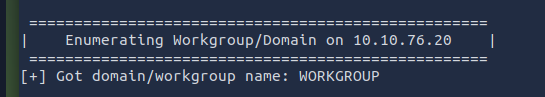
139-445

***Let's get started with Enum4Linux, conduct a full basic enumeration. For starters,***

***what is the workgroup name?***

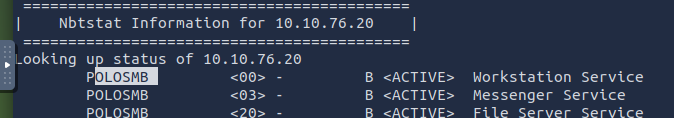
Workgroup





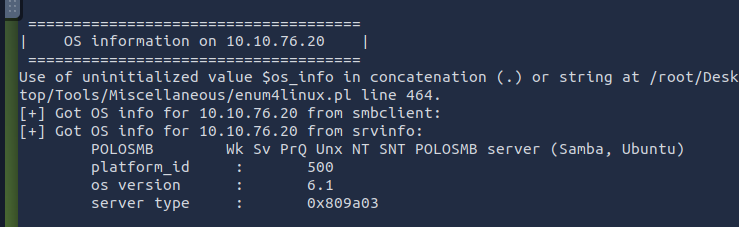
***What comes up as the name of the machine?***

POLOSMB



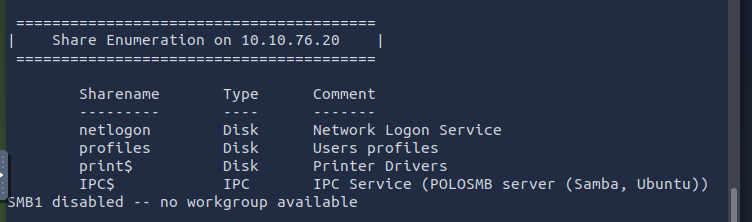
***What operating system version is running?***

6.1



***What share sticks out as something we might want to investigate?***

Profiles



***Task 4 - Exploiting NFS***

***Answer the questions below***

***First, change directory to the mount point on your machine, where the NFS share should still be mounted, and then into the user's home directory.***

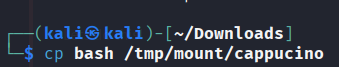
***No answer needed***

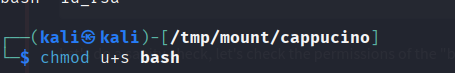
***Download the bash executable to your Downloads directory. Then use "cp ~/Downloads/bash ." to copy the bash executable to the NFS share. The copied bash shell must be owned by a root user, you can set this using "sudo chown root bash"***

***No answer needed***

***Now, we're going to add the SUID bit permission to the bash executable we just copied to the share using "sudo chmod +[permission] bash". What letter do we use to set the SUID bit set using chmod?***

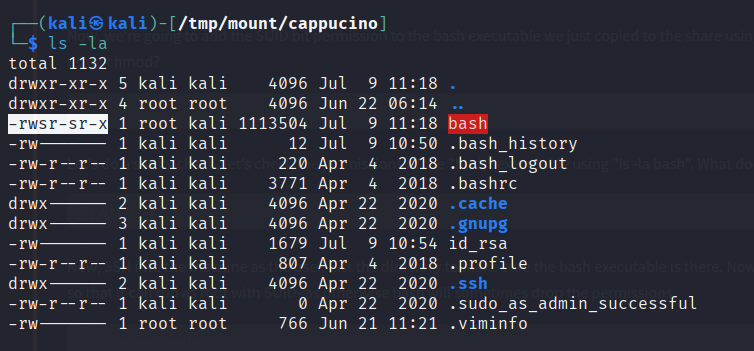
***S***





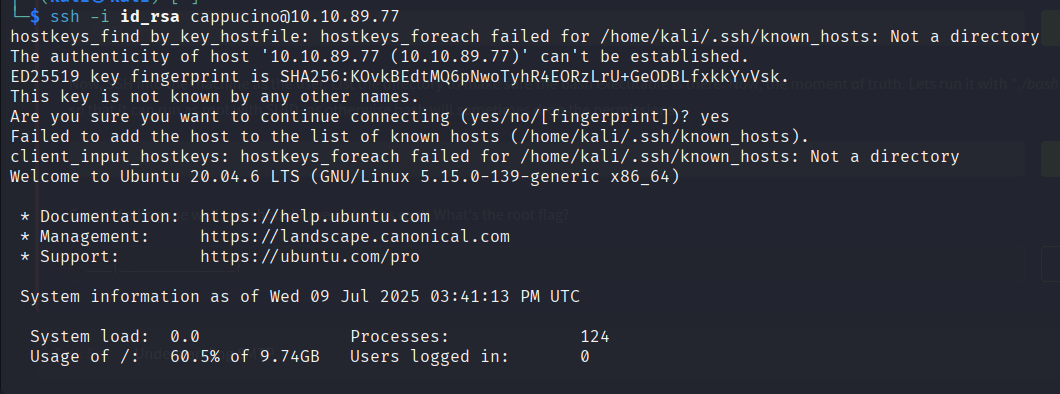
***Let's do a sanity check, let's check the permissions of the "bash" executable using "ls -la bash". What does the permission set look like? Make sure that it ends with -sr-x.***

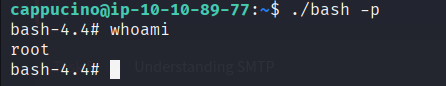
***-rwsr-sr-x***

******

***Now, SSH into the machine as the user. List the directory to make sure the bash executable is there. Now, the moment of truth. Lets run it with "./bash -p". The -p persists the permissions, so that it can run as root with SUID- as otherwise bash will sometimes drop the permissions.***

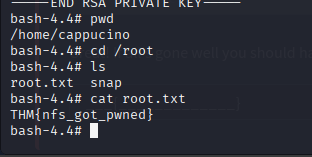
***No answer needed***

******

******

***Great! If all's gone well you should have a shell as root! What's the root flag?***

***THM{nfs\_got\_pwned}***



***Task 5 - Understanding SMTP***

***What does SMTP stand for?***

***Simple Mail Transfer Protocol***

***What does SMTP handle the sending of? (answer in plural)***

***emails***

***What is the first step in the SMTP process?***

***SMTP handshake***

***What is the default SMTP port?***

***25***

***Where does the SMTP server send the email if the recipient's server is not available?***

***smtp queue***

***On what server does the Email ultimately end up on?***

***POP/IMAP***

***Can a Linux machine run an SMTP server? (Y/N)***

***Y***

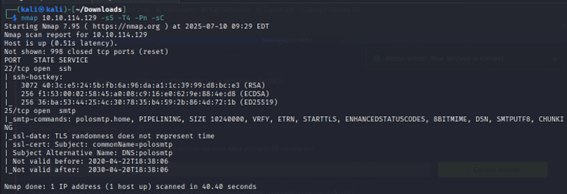
***Can a Windows machine run an SMTP server? (Y/N)***

***Y***

***Task 6 - Enumerating SMTP***

***First, lets run a port scan against the target machine, same as last time. What port is SMTP running on?***

***25***

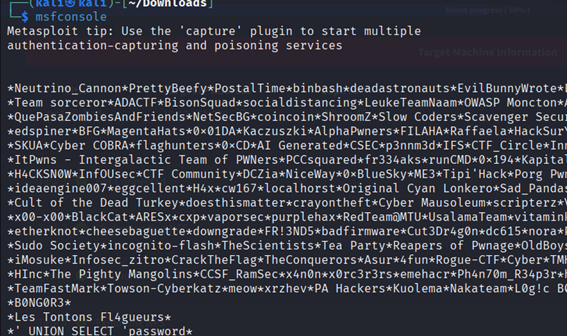


***Okay, now we know what port we should be targeting, let's start up Metasploit. What command do we use to do this?***

***If you would like some more help or practice using Metasploit, TryHackMe has a module on Metasploit that you can check out here:***

***https://tryhackme.com/module/metasploit***

***msfconsole***

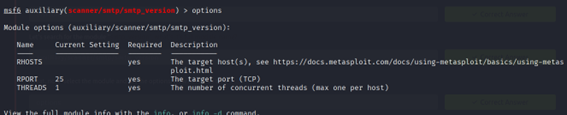


***Let's search for the module "smtp\_version", what's it's full module name?***

***auxiliary/scanner/smtp/smtp\_version***

***Great, now- select the module and list the options. How do we do this?***

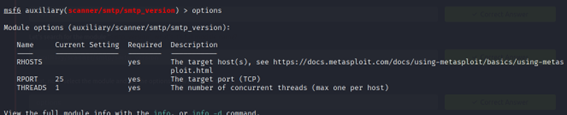
***Options***





***Have a look through the options, does everything seem correct? What is the option we need to set?***

***RHOSTS***



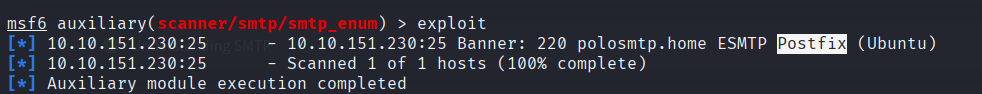
***Set that to the correct value for your target machine. Then run the exploit. What's the system mail name?***

***polosmtp.home***



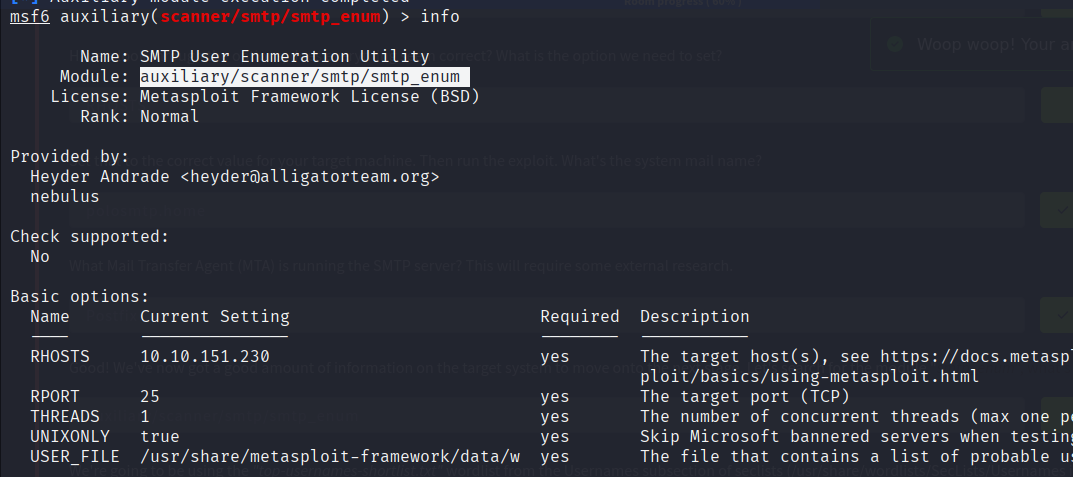
***What Mail Transfer Agent (MTA) is running the SMTP server? This will require some external research.***

***Postfix***



***Good! We've now got a good amount of information on the target system to move onto the next stage. Let's search for the module "smtp\_enum", what's it's full module name?***

***auxiliary/scanner/smtp/smtp\_enum***

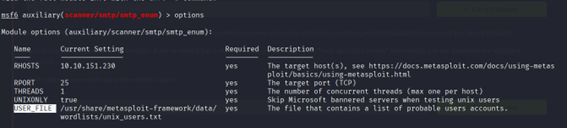
******

***We're going to be using the "top-usernames-shortlist.txt" wordlist from the Usernames subsection of seclists (/usr/share/wordlists/SecLists/Usernames if you have it installed).***

***Seclists is an amazing collection of wordlists. If you're running Kali or Parrot you can install seclists with: "sudo apt install seclists" Alternatively, you can download the repository from here.***

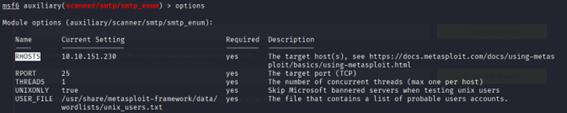
***What option do we need to set to the wordlist's path?***

***USER\_FILE***



***Once we've set this option, what is the other essential paramater we need to set?***

***RHOSTS***



***Now, run the exploit, this may take a few minutes, so grab a cup of tea, coffee, water. Keep yourself hydrated!***

***No answer needed***

***Okay! Now that's finished, what username is returned?***

***Administrator***

