<https://tryhackme.com/room/anonymous>

Try to get the two flags!  Root the machine and prove your understanding of the fundamentals! This is a virtual machine meant for beginners. Acquiring both flags will require some basic knowledge of Linux and privilege escalation methods.

--------------------------------------------------------------------

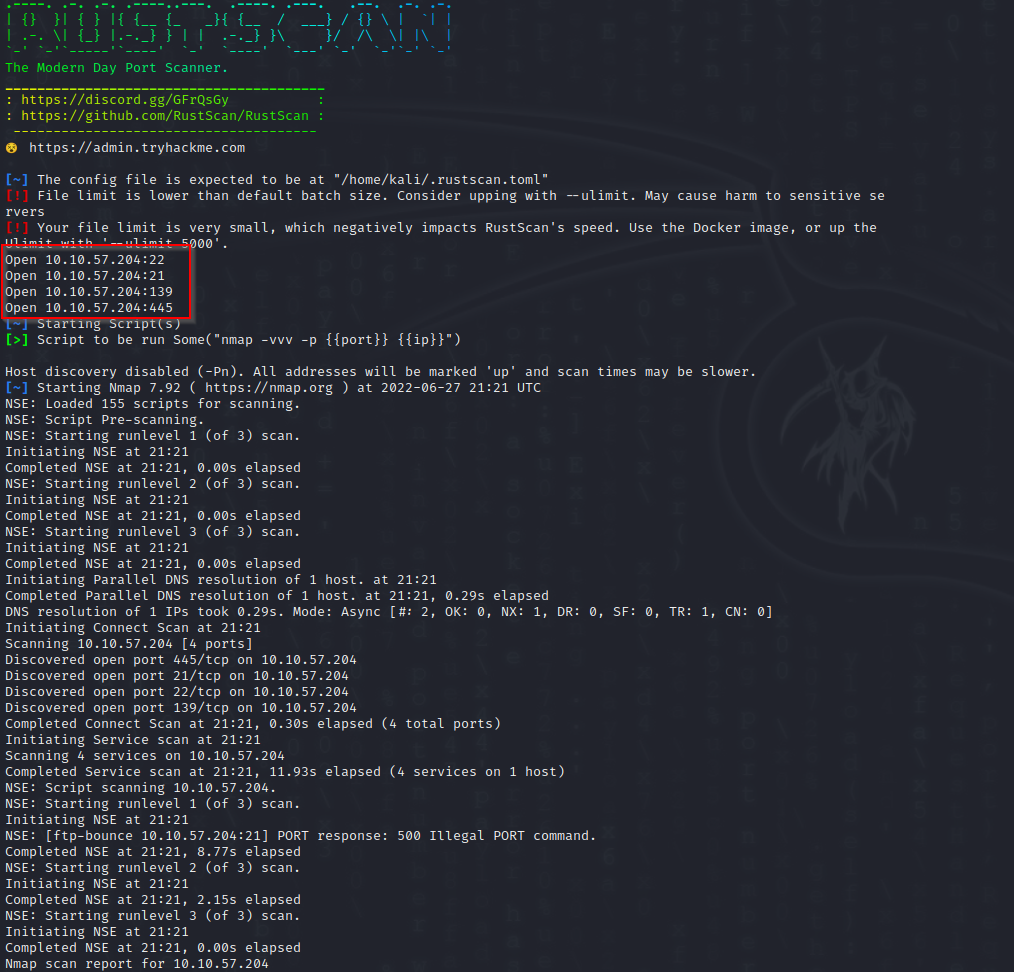
*For more information on Linux, check out*[Learn Linux](https://tryhackme.com/room/zthlinux)

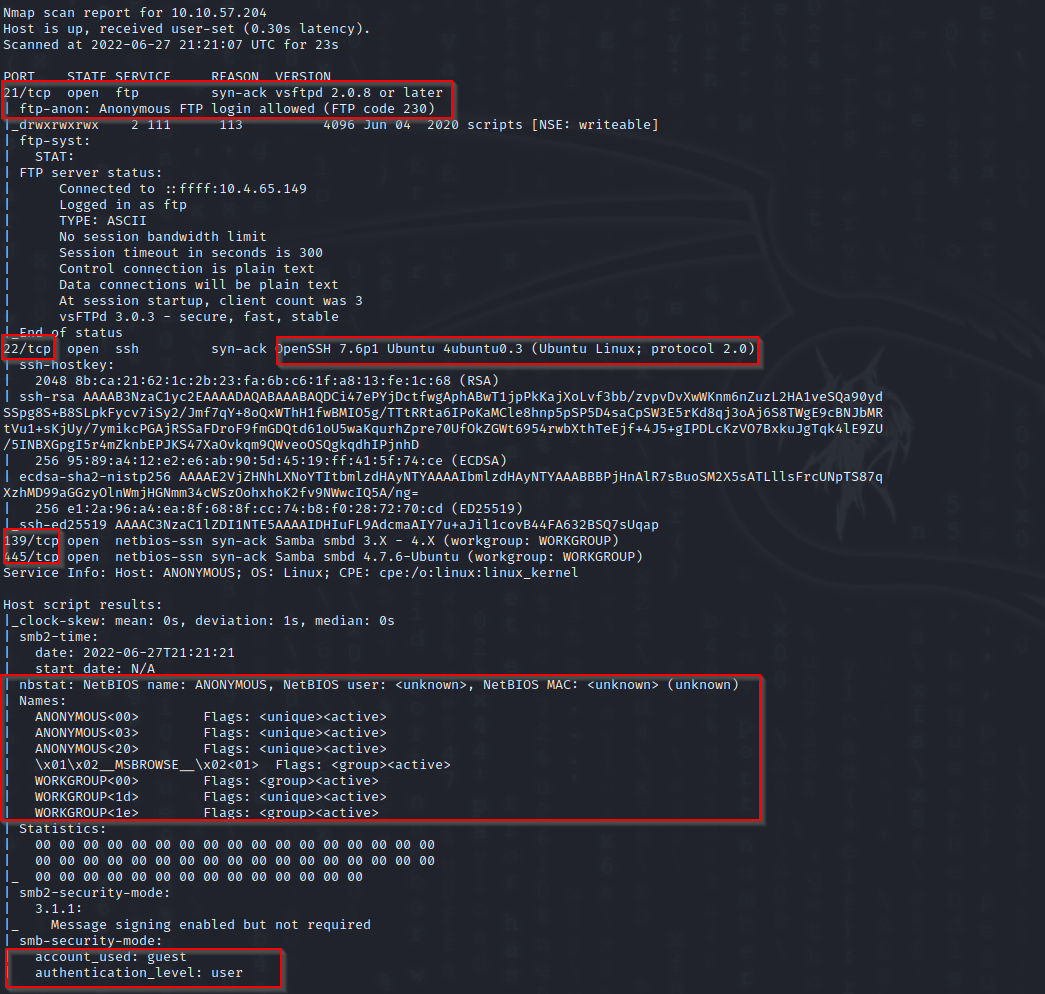
**Enumeration**

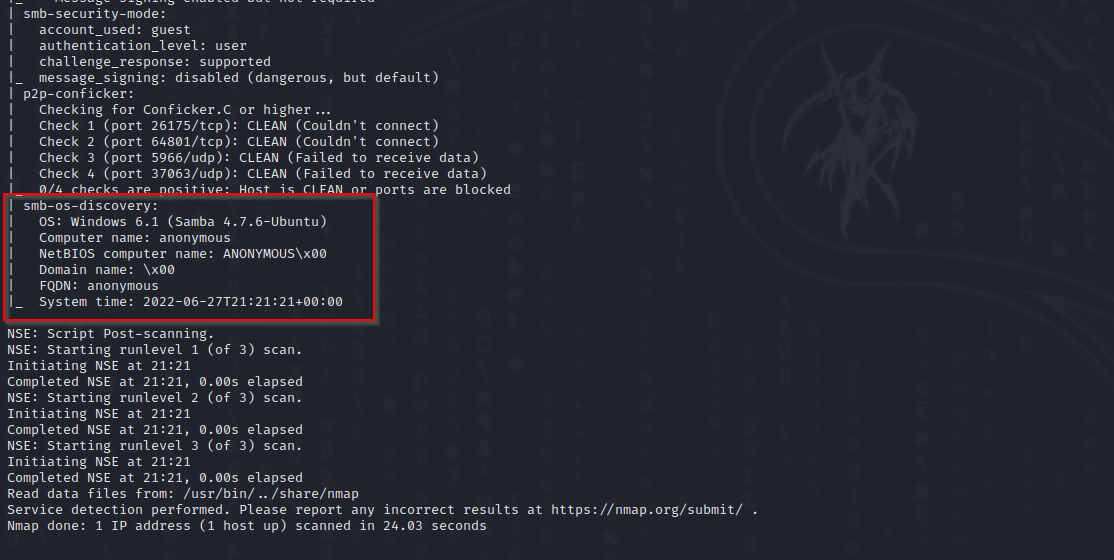
We were provided with only and IP address of the system.

Using our system we started a port scan

rustscan -a $ip -- -A -sV -sC -T4 -Pn | tee TotalRustscan.log







The server has 4 open ports

**Port 21**

Ftp service, running VSFTPD 2.0.8

Anonymous FTP logon us available

**Port 22**

SSH. Open SSH 7.6p1

Nmap suggest a linux based OS

**Port 139 and 445**

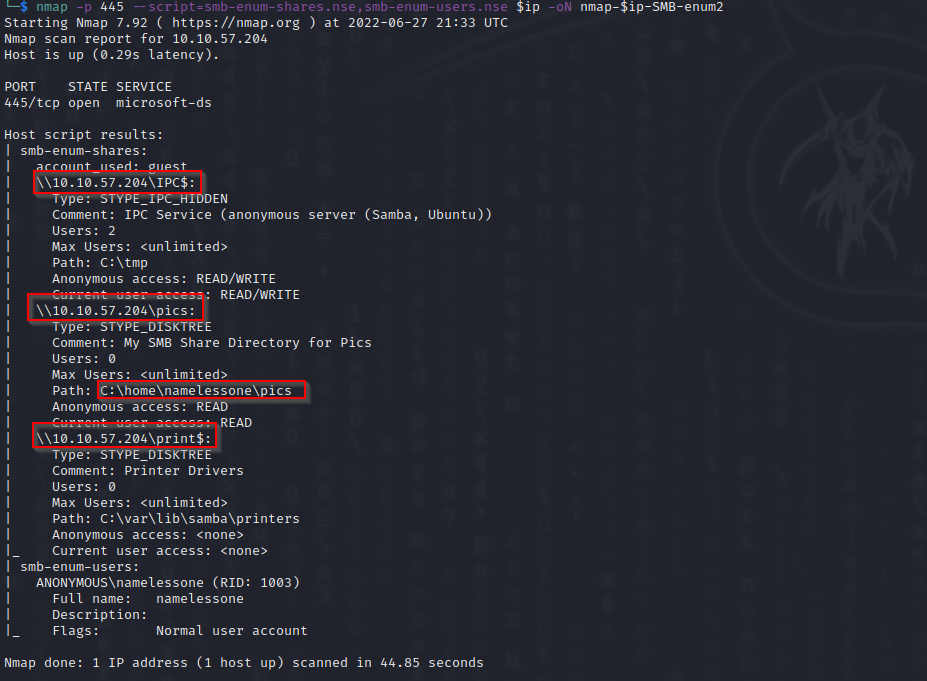
SMB service

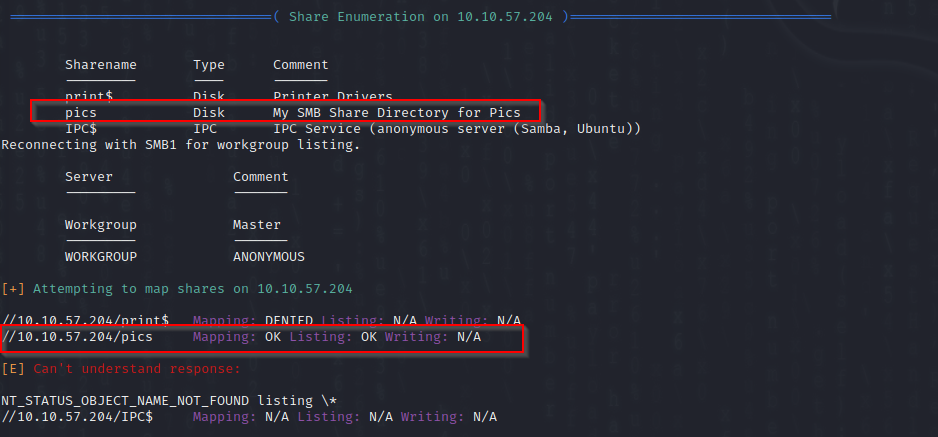
Anonymous guest user log on allowed

**SMB Enumeration**

We used two tools

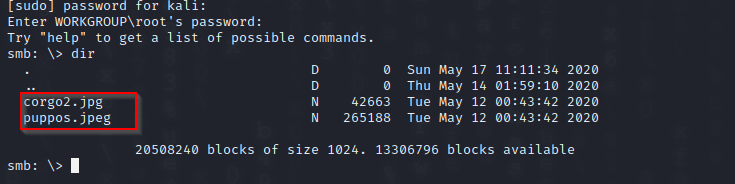
Nmap and Enum4Linux





There is a number of shares

However the “pics” share are of interest



There are two pictures

corgo2.jpg

puppos.jpeg

We downloaded both



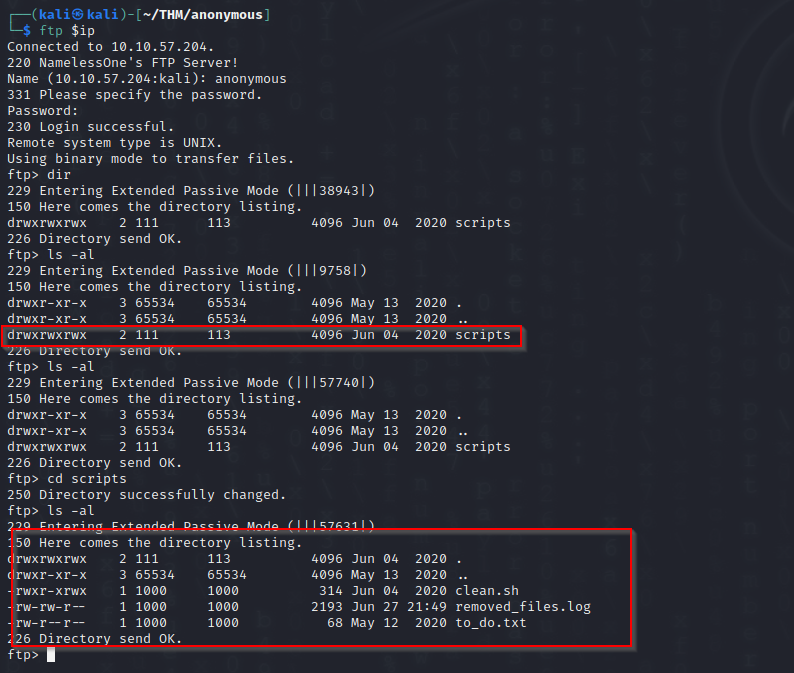


Both files seems to have hidden content within



However we need a password to extract the data

**FTP Enumeration**



We logged on anonymously

Inside the script directory there are 3 files

Note the directory itself has all the RWX permissions

After downloading the files it seems the clean.sh runs regularly

The output gets logged on the .log file

We edited the sh file, uploaded the modified version

Shortly after the log file was modified



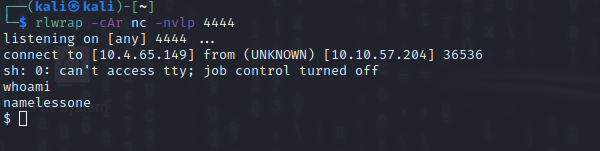


Next we will try a basic reverse shell

We add the line to the scrip and upload it



Then start a listener and wait

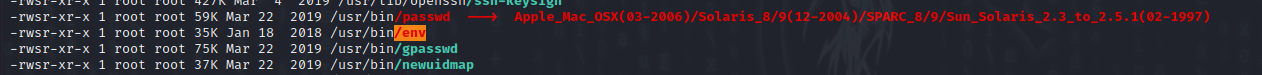


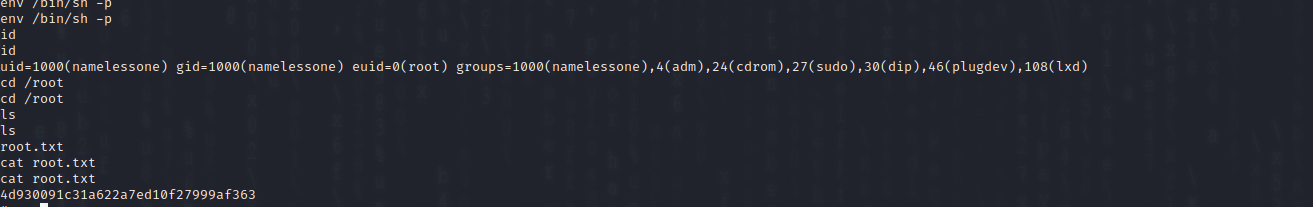
**Privilege Escalation**

Upload linpeas



Linpeased showed the env command can be exploited for SUID permissions





**Summary**

We found 4 ports open

Two of the services, SMB and FTP allowed for anonymous log on.

Using SMB, 2 images were able to be download

The FTP server hosted and open scrip

The directory and the script had read and write permissions

The script was modified and used to create and reverse shell, getting access to the system.

Further user privilege escalation was gained using the env command.

Root privileged was gained using this

**Security Suggestion**

Use a firewall to block and restrict access to these services.

Disable anonymous log on to both the SMB and the FTP service.

Removed the script from the FTP folder

Change the permissions of the FTP folder to read only

The script permission need to be change to not allow writing.

The system env command need updating.