TRYHACKME CTF

Gaming Server

Step 1: Reconnaissance

Perform Nmap Scan : ***sudo nmap -sC -sV -T4 10.10.180.249***

We Got port 22 and 80 Open, Since ssh(22) Requires credentials or Public Key, We try to inspect the Website in Port 80.

In the Website we got a username **john** while analyzing the source code of the webpage and while surfing through the website we got the **/uploads** folder which contains a word list and text file.

While Performing the Directory Enumeration using the gobuster tool.

***gobuster dir -u http://10.10.180.249 -w /usr/share/wordlists/rockyou.txt***

I got /secret directory in the result of the scan.

When analyzing the http://***10.10.180.249***/secret we got ssh public key.

Step 2: Gaining Access

While connecting all the files obtained in the Information Gathering phase we can try to access ssh with username john and public key of the user.

We need to find the password from the public key so that we can use the ssh2john module.

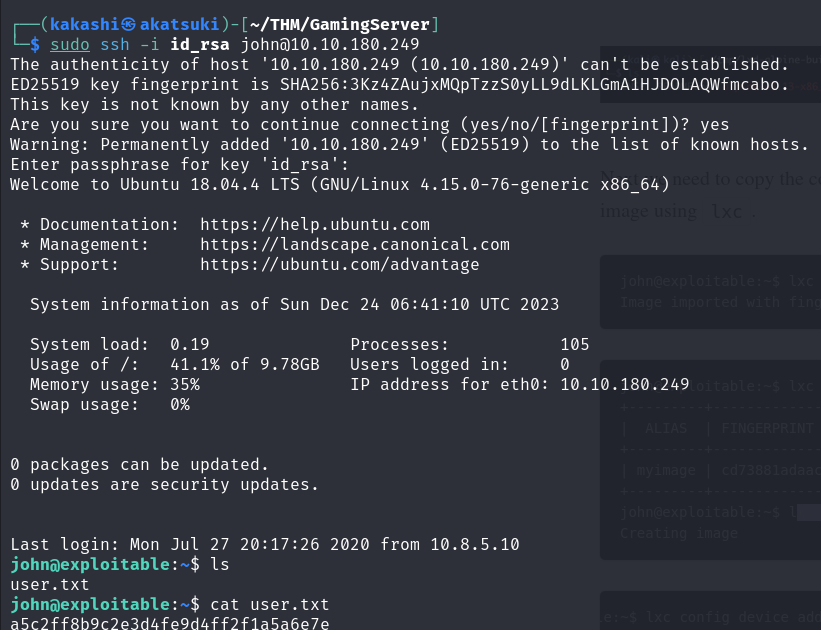
***ssh2john id\_rsa > hash.txt***

***john –wordlist=wordlist.txt hash.txt***

Here the wordlist.txt is what we obtained from the /uploads directory and id\_rsa is the secret key obtained from the /secret directory.

We got the password **letmein**  
  
Try Login with the obtained credentials:

***sudo ssh -i id\_rsa john@10.10.180.249***

**

We got the user.txt next we to find root.txt for that we need to escalate the privileges to root.

Since sudo -l is not available we need to find another way to check for possible priv escalation.



We got lxd, We can use that to escalate our privileges.

I found this website and followed the steps to gain root shell.

[Lxd Privilege Escalation - Hacking Articles](https://www.hackingarticles.in/lxd-privilege-escalation/)

