Introduction to Linux & Privilege Escalation

Mentoring program

/* WHERE THERE IS A SHELL, THERE IS A WAY */

TABLE OF CONTENTS

Part 1 : Introduction to Linux

/* WHERE THERE IS A SHELL, THERE IS A WAY */

TABLE OF CONTENTS

Part 2 : Linux PrivEsc

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Part 1

Introduction to Linux

/* WHERE THERE IS A SHELL, THERE IS A WAY */

01.
Basic commands

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Basic commands

Command	Description
pwd	Print working (current) directory
ls	List directory contents
cd	Change the working directory
mkdir	Make (create) directories
cat/less	Print file contents

/* WHERE THERE IS A SHELL, THERE IS A WAY */

02.
Search and filter

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Search and filter

01 find

Search for files in a directory hierarchy.

```
$ find directories... -opt1 expr ... -optN expr
```

02 grep

Filter lines matching a pattern.

```
$ grep [OPTIONS] pattern files...
```

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Search and filter

01 Example (find)

Look for all files in “dirs” directory that are of type regular file (f), and that are named exactly “flag.txt”.

```
$ find dirs/ -type f -name flag.txt
```

02 Example (grep)

Print all lines in “dump.txt” that contain “flag”.

```
$ grep flag dump.txt
```

/* WHERE THERE IS A SHELL, THERE IS A WAY */

03.
Binary files

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Binary files

01 file

Determine file type.

```
$ file filename
```

02 strings

Print strings of printable characters in files.

```
$ strings filename
```

03 xxd

Make a hexdump of a file.

```
$ xxd filename
```

Make a file out of a hexdump file.

```
$ xxd -r hexdump
```

/* WHERE THERE IS A SHELL, THERE IS A WAY */

04.
Miscellaneous

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Miscellaneous

01 man

Browse reference manuals for commands.

```
$ man command
```

02 exiftool

Read file metadata.

```
$ exiftool filename
```

03 base64

Encode file in base64.

```
$ base64 filename
```

Decode file from base64.

```
$ base64 -d b64file
```

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Part 2

Linux PrivEsc

/* WHERE THERE IS A SHELL, THERE IS A WAY */

01.
Basic methodology

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Basic methodology

01 Check sudo

Check commands you can execute with sudo:

```
$ sudo -l
```

02 Check processes

Check running processes:

```
$ ps -aef
```

03 Check unusual files

Check for any unusual files in these directories:

- /home/$*USER*/
- /tmp/
- /var/tmp/
- /var/backups/
- /root/

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Basic methodology

04 Enumerate users

```
$ cat /etc/passwd
```

05 Cron jobs

Look for any vulnerable scripts being executed as cron jobs in:

- /etc/crontab (file)
- /etc/cron.d/
- /etc/cron.daily/
- /etc/cron.*/

/* WHERE THERE IS A SHELL, THERE IS A WAY */

02.
sudo

/* WHERE THERE IS A SHELL, THERE IS A WAY */

sudo

01 What is sudo?

sudo is used to execute a command as another user, based on the configured sudo policies.

02 Check sudo

List the allowed commands for the invoking user:

```
$ sudo -l
```

03 Execute with sudo

```
$ sudo -u user command
```

04 GTFOBins

Find out how to exploit sudo misconfigurations on gtfobins.github.io

/* WHERE THERE IS A SHELL, THERE IS A WAY */

03.
Other techniques

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Other techniques

01 Path manipulation

Linux Privilege Escalation Using PATH Variable

02 SUID

Linux Privilege Escalation using SUID Binaries

03 LD_PRELOAD

Linux Privilege Escalation using LD_Preload

04 Everything

- HackTricks
- Payload All The Things

/* WHERE THERE IS A SHELL, THERE IS A WAY */

Resources

01 Books

- Practical guide to Linux commands

02 Practice

- picoCTF
- OverTheWire Bandit
- Root Me
- TryHackMe

03 Youtube

- What is CTF?
- The Secret step-by-step Guide to learn Hacking
- How to Learn Hacking with CTFs
- John Hammond
- IppSec

/* WHERE THERE IS A SHELL, THERE IS A WAY */

THANK YOU

Any questions?

/* WHERE THERE IS A SHELL, THERE IS A WAY */