Mostafa.khademi@rocketmail.com

STEPS TO HACKING

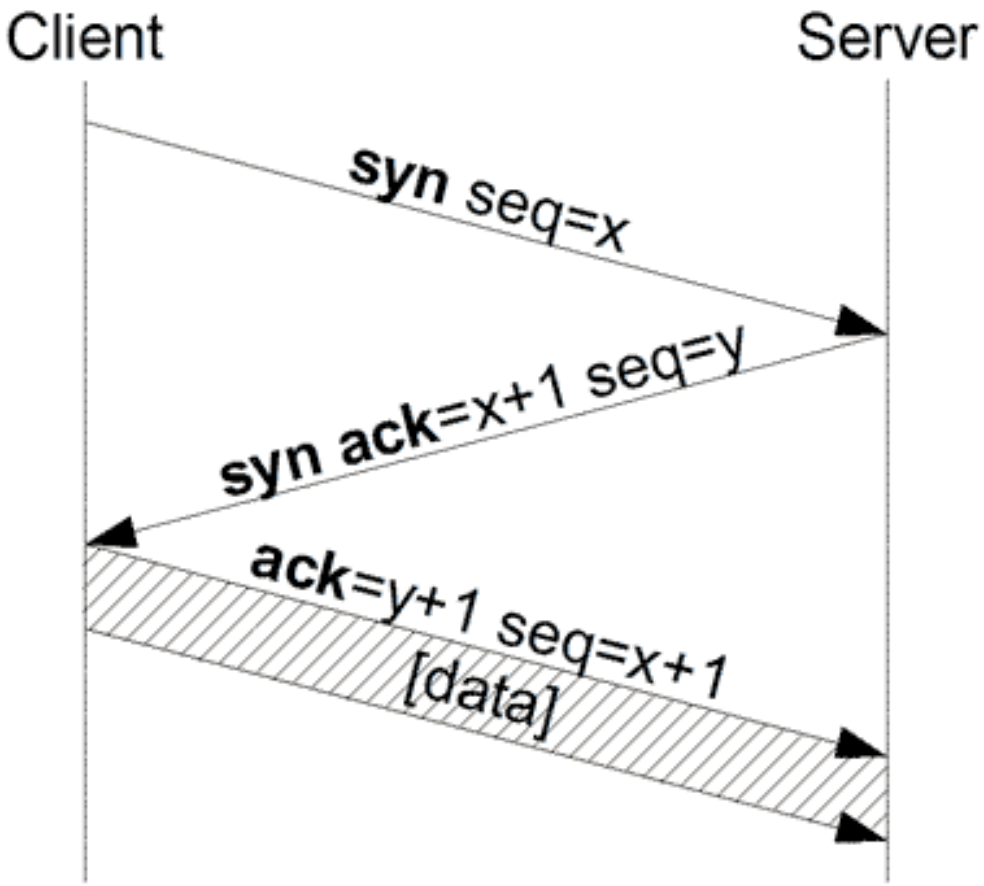
5 Steps to Hack

- 1) Information Gathering (nslookup,ping,…)
- 2) Scanning (nmap,nessus,OpenVAS,…)
- 3) Gaining Access (Exploits,…)
- 4) Maintaining Access (Privilege Escalations)
- 5) Clearing Tracks

Scanning

- 1) Network Scanning
- 2) Port Scanning
- 3) vulnerability Scanning

3 Way Handshake



Network Scanning With Nmap

- Find up host on an range IP:

  nmap –sn 192.168.56.0/24

  nmap –sn 192.168.56.1-100

- Save data in graphical form

If you want to save your data graphically Should use –oA and choose a name

Port Scan

- *Nmap –sT target IP*
- *Nmap -sS target IP*
- *Nmap –sN target IP*
- *Nmap –sX target IP*

Search for some port:

Nmap –p port-number IP-address

Search for a port without ping:

Nmap –p port-number –Pn Ipaddress

Search for version:

Nmap –p port-number –sV Ip-address

Search for operating system:

Nmap –O IP-address