**Scanning**

Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network.

Scanning methodology:

* Hackers and Pen-testers check for Live systems.
* Check for open ports
* Banner Grabbing: is the method for obtaining information regarding the targeted system on a network and services running on its open ports.
* Scan for vulnerability

Practical:

1. <https://hackertarget.com/nmap-online-port-scanner/>
2. <https://tools.tracemyip.org/search--isp/gtpl+broadband+pvt>
3. <https://observatory.mozilla.org/>
4. https://www.qualys.com/community-edition/#/freescan
5. Shodan.io (google chrome extension)
6. Advance IP scanner
7. Advance Port scanner
8. The dude
9. Angry IP scanner

Nmap:

#Nmap 172.16.216.1

#nmap –sn 172.16.125.0/16

#nmap –iL Desktop/ip.txt

#nmap –p 0-500 172.16.216.1

To scan 0 to 500 port

#nmap –p- 172.16.216.1

To scan all port

ALL

Nmap -T4 –v –A –Pn –f ipaddress

T4-Aggressive speed scan

-v=verbose

-A=os detection

-Pn=Portscan only

-f =scan small fragmentation

Nikto –host scanme.nmap.org