**DAY-7**

**SCANNING**

Scanning is the second phase of ethical hacking

Network scanning is a phase where the ethical hacker needs to gather the network into such as:

🡪Number of devices that are live on network

🡪To find the open and closed ports on the network

🡪To find the services and their versions

🡪To find operating system of devices

🡪To find the banner details of the devices

🡪To find the firewalls and bypass them

🡪To use a VPN and to be anonymous

These are basic techniques of scanning and there are 10 other advanced scanning techniques

To scan, nmap can be used to find above options

To find number of devices in a network use pingsweep technique that is to ping a range of ip addressess

Tools like angry ip scanner and advanced ip scanner can be used

Angry ip scanner:

Blue 🡪 online

Green 🡪 open ports

Red 🡪 offline

Range of port numbers: 0-65535

**Sitereport.netcraft.com** we can find other details