Day 2:

1) Information gathering or recon:

1) Active recon -> Gathering information being in touch.

2) Passive recon -> Gathering information through Internet.

2) Google dorking:

To optimize the search result.

Ex: site:tesla.com.

inurl:login site:tesla.com.

site:tesla.com filetype:pdf.

3) OSINT -> open source intelligence.

- theHarvester (tool)

4) Website Information.

-> whatweb (tool)

Extension called wappalyzer.

-> Whois lookup.

-> Finding IP

Sublist3r -> tool in Kali linux.

→ dirsearch for scanning.

→ Nmap (Network mapper) to scan

Ex:

root@kali:~# nmap -sn 192.168.128.