**Day2\_Summary**

Information Gathering and Reconissance:

1.Active Scanning

2.Passive Scanning

3.Google Dorking(Passive Scanning) – GHDB

(insite: , inurl: , filetype: , intext: )

arp-scan -To scan all the devices that are connected to

your network)

4. OSINT -passive scanning

profil3r

5. Website Information

-Website Technologies

-Finding IP

-whoislookup

-To find subdomains

hunter.io - to get email address of the employees in that network

Wappalyzer -To get all the softwares that helped in building that website.

Scanning: scanning for vulnerabilities

-looking for files and folder in that website: dirbuster and dirb

-Nmap(Network mapper): To scan