Task1: (ASN Task)

Aim:
To find whether a domain is shared by hosting provider or acquired by itself and to fetch unique subdomains from the target domain.

Tools to use:
1) Ping.
2) whois.
3) asnlookup.com.
4) shodan.io

Target domain: samsung.com

Note: Add screenshot after each and ever step
Answer:

Task2: (Certificate Transparency Task)

Aim:
To find a domain is logged under crt.sh, paste who is the certificate authority and to find a unique subdomains by using both GUI and Command line method

Tools to use:
1) crt.sh
2) crt.sh automation

Target domain: airtel.com

Note: Add screenshot after each and every step
Answer:

Task3: (DNS Enum Task)

Aim:
To find a IPv4 address, anythirdparty services integrated, whom owns DNS, What mail servers used in the target domain

Tools to use:
1) dig
2) MX Toolbox

Target domain: uber.com

Note: Add screenshot after each and every step
Answer:

Task4: (Subdomain Enum)

Aim:
To find a subdomains from different type of tools and paste it' as image and categorize the subdomains via LLM (Chatgpt)

Tools to use:
1) Subfinder
2) https://subdomainfinder.c99.nl/
3) Amass
4)sublister
5) puredns
6) virustotal
7)cencys
8) shodan
9) chaosdiscovery

Target domain: uber.com

Note: Add screenshot after each and every step
Answer:

Task5: (Filtering duplicate Subdomain)

Aim:
To filter duplicate subdomains from the list of txt file, by combining them and sorting it out (Use any one method)

Tools to use: (Any one)
1) Manual method
2) One liner
3) bash scripting
4) LLM

Target domain: uber.com

Note: Add screenshot after each and every step
Answer:

Task6: (NMAP Scan)

Aim:
To Find open ports and exploiting the open ports via NMAP Script Engine
Tools to use: (Any one)
1) NMAP
2) Zenmap

Target domain: nasa.gov and their subdomains

Note: Try To use all the commands teached in the Video
Answer:

Task7: (Filtering Live subdomains)

Aim:
To Filter live subdomains from filtered duplicate subdomains via HTTPX and view the 200 and 403 status code via Eyewitness
Tools to use:

3) HTTPX
4) Eyewitness

Note: Add screenshot after each and every step
Target domain: nasa.gov filtered duplicate subdomains
Answer:

Task 8: Nuclei Automation

Aim:
Use **Nuclei** to scan a target for known vulnerabilities using pre-defined and custom templates. The goal is to identify real vulnerabilities and understand how Nuclei fits into a recon workflow.
Tools to use: (Any one)

5) Nuclei

Note: Add screenshot after each and every step
Target domain: nasa.gov live Domains

Task 9: Manual Recon

Aim:
Use **Manual recon to Find any sensitive endpoints to exploit vulnerability**

Tools to use:

6) Manual recon, inspect element, viewpage source, analzye.js files

Note: Add screenshot after each and every step
Target domain: nasa.gov live Domains

Task 10: Gathering URL

Aim:
Try To get As much a url from the below mentioned tools

Tools to use:
Gau, waybackurls,WayBackupFinder,back-me-up,katana,jsfinder,mantra,SecretFinder,gospider, paramspider,Arjun

Note: Add screenshot after each and every step
Target domain: nasa.gov

Task 11: Exploiting URL

Aim:
Try To exploit XSS, SQL, OPen redirect and sensitive info disclosure

Tools to use:
Uro, grep, grep.sh automater, secretfinder, sqlmap, kxss, dalfox, qsreplace

Note: Add screenshot after each and every step
Target domain: nasa.gov

Task 12: Fuzzing

Aim:
Try To FUZZ using different tools and find sensitive info disclosure

Tools to use:
Dirserach, gobuster, FFUF

Note: Add screenshot after each and every step
Target domain: nasa.gov

Task 13: Using Extensions

Aim:
Try To Use all the Extensions below and have a hands on practical

Tools to use:
Bulk url opener, screen recorder for POC, security header test, cookie editor link grabber, shodan, urban vpn (IP rotate), wappalayzer, hunter, foxy proxy dot git, find something, D3coder

Note: Add screenshot after each and every step
Target domain: nasa.gov

Task 14: WAF identification

Aim:
Try to Find WAF behind the websites

Tools to use:
WAfwoof, subfinder, httpx, dirserach

Note: Add screenshot after each and every step
Target domain: nasa.gov

Task 15: Shodan Recon

Aim:
Try to Use all different types of queries and practise

Tools to use:
shodan

Note: Add screenshot after each and every step
Target domain: nasa.gov

Task 16: Github Recon

Aim:
Try to Use all different types of queries and practise

Tools to use:
Github, Githgrabber, trufflehog

Note: Add screenshot after each and every step
Target domain: nasa.gov

Task 17: Google Dorks Recon

Aim:
Try to Use all different types of queries and practise

Tools to use:
Google, bigbounty recon, faisal dorks automation

Note: Add screenshot after each and every step
Target domain: nasa.gov

Task 18: One Liner Automation

Aim:
Try to Use all different types of queries and practise

Tools to use:
One liner script, boltnew

Note: Add screenshot after each and every step

Target domain: nasa.gov

Task 19: WP-Recon

Aim:
Use Manual method and also automation, inorder to find vulnerable plugins and themes and Wp version

Tools to use:
AJAK Automation Tool, WP-Scan

Note: Add screenshot after each and every step
Target domain: nasa.gov