--Recon—

-- Outline

* What is Recon?
* Type of Recon
* Methodology for Recon
* Detalis about DNS Recon
* Bash Scripts for DNS recon

-What is Recon??
--Recon is the process of gathering information about a target (such as a network, system, or organization) to gain a better understanding of its vulnerabilities, architecture, and potential points of entry.
--It is a critical phase in the process of identifying and assessing potential security risks.
--It helps security professionals and ethical hackers gather intelligence about a target before attempting to exploit any vulnerabilities.

-There are 2 types
Passive recon: This involves information without directly interacting with the target. It relies on publicly available sources like search engines, social media, WHOIS records, and public databases.

Active Recon: This involves actively probing and interacting with the target. It may include activities like part scanning,DNS enumeration, and network sniffing.

-Importance of Recon for WPB
knowledge is power / Information is power

Ethical Hacking Phases:
Recon > Scanning > Gaining Access > Maintaining Access > Clearing Track

Methadology for Recon:
01. Dig domain information as soon as possible
02. Collect PID or PII, name, email, locaion etc
03. Port Scanning,Service identification, OS fingerprinting
04. Path or hidden directory exposing
05. Vulnerability Scanning

Note down the information and Prioritizing the information

https://mxtoolbox.com/networkTools.aspx
https://mxtoolbox.com/
https://whois.domaintools.com/
https://viewdns.info/

ping www.abc.xyz
nmap -sV -sC -A <ip>
nmap -p- <ip>
dircearch -u www.abc.xyz -r 3
nuclei -u www.abc.xyz/search?q=text -t /home/kali/nuclei-templates/http/cves