Unit - 3

① Google to mine sensitive information

→ Using key terms with operators

Operater	Description
Filetype	Type of file filetype : xls
inurl	Only search this url inurl : bla
link	Search within link link : ...
intitle	Search within title .

② WHOIS

Tools to query info. an organization entered when registering its domain.

→ Can use domain name or IP.

③ Exploring domain ownership

→ Finding details of who owns the domain

↳ Part of social engineering.

→ Internet Assigned Numbers Authority (IANA)

④ Passive Information Gathering Attacks

ⓐ Dumpster Diving: Info. in the address's garbage bin.

ⓑ Wardriving: Finding & marking location and status of wireless networks.

ⓒ Wardialing: Scanning all phone numbers to check for connected modems with vulnerabilities.
↳ Tools:
- i) Tone Loc
- ii) THC Scan
- iii) Demon Dialer

⑤ ICMP (Ping) (Internet Control Message Protocol)

→ Part of TCP/IP protocol suite
→ Designed to aid network diagnostics and sending error messages.
→ ICMP is sent for only 1 fragment.
→ No priority.
→ Can't reply with ICMP.

→ Ping is a type of ICMP to verify connectivity.

Type	Code	Function
0/8	N/A	Echo req/res.
3	0-15	Dest. unreachable
4	0	Source quench
5	0-3	Redirect
11	0-1	time exceeded
12	0	Parameter fault
13/14	0	Time stamp req/res
17/18	0	Subnet mask req/res.

⑥ ~~Enumeration~~ Port Scanning Tools

i) Nmap
ii) Superscan
iii) THC-A map
iv) Look@LAN
v) Net Scan Tools

⑦ TCP & UDP Port Scanning

→ TCP is a connection oriented protocol.
→ TCP can return many different types of responses to a scanning program.

→ UDP does not have flags or issue responses to scanning.
→ UDP ~~Can~~ Scans can get ICMP port unreachable or no response if ICMP is blocked.

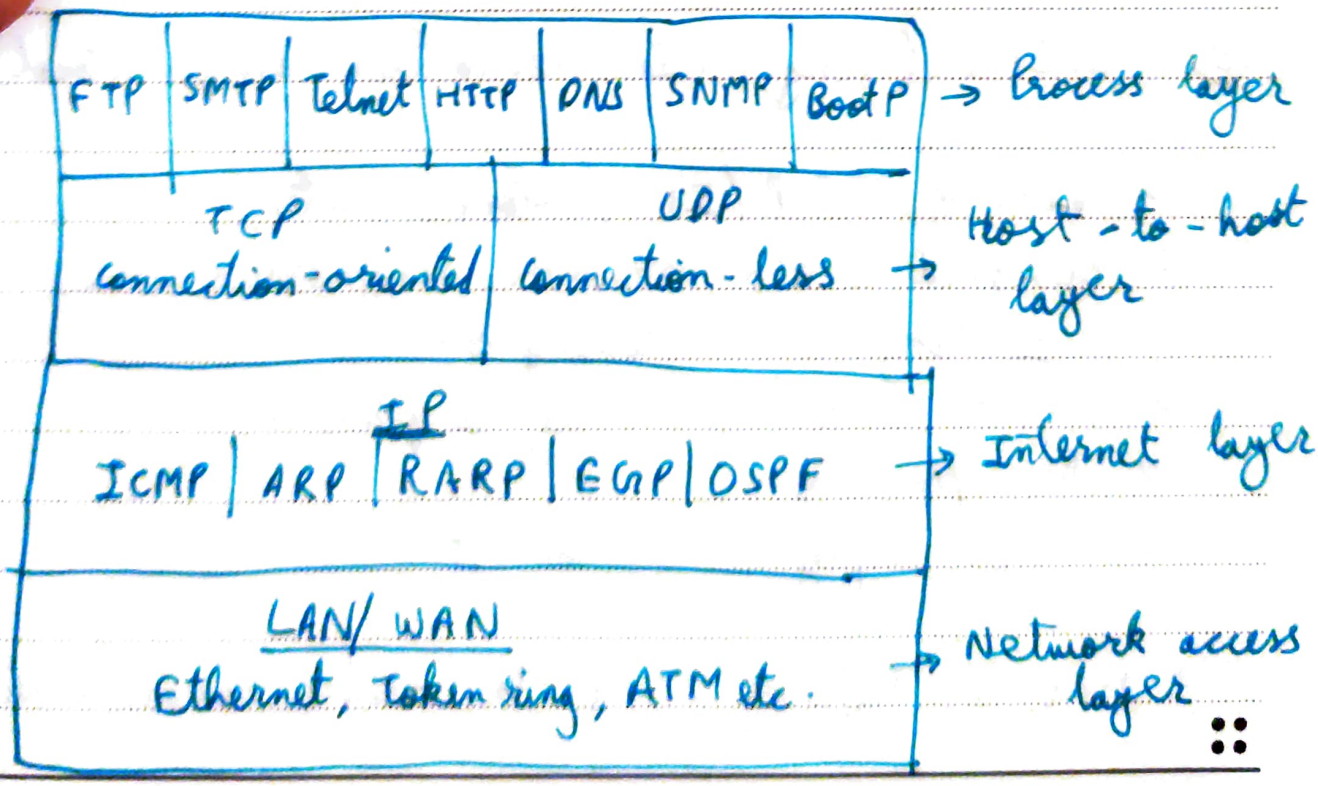
~~Scan~~ Scan name	Details
TCP full connect Scan	Most reliable but most detectable and is logged. open → SYN/ACK closed → RST/ACK
TCP SYN Scan	Half-open. Most IDS now detect it. open → SYN/ACK closed → RST/ACK
TCP FIN Scan	Closed → RST ~~/ACK~~ Usually works with Unix only.
TCP NULL Scan	~~Attempts to determine Access control list~~ No flags set. closed → RST

TCP ACK Scan	Attempts to determine Access Control List or identifies stateless inspection Can determine filtered ports.
TCP XMAS Scan	FIN, URG, PSH are ~~or~~ toggled. Closed → RST

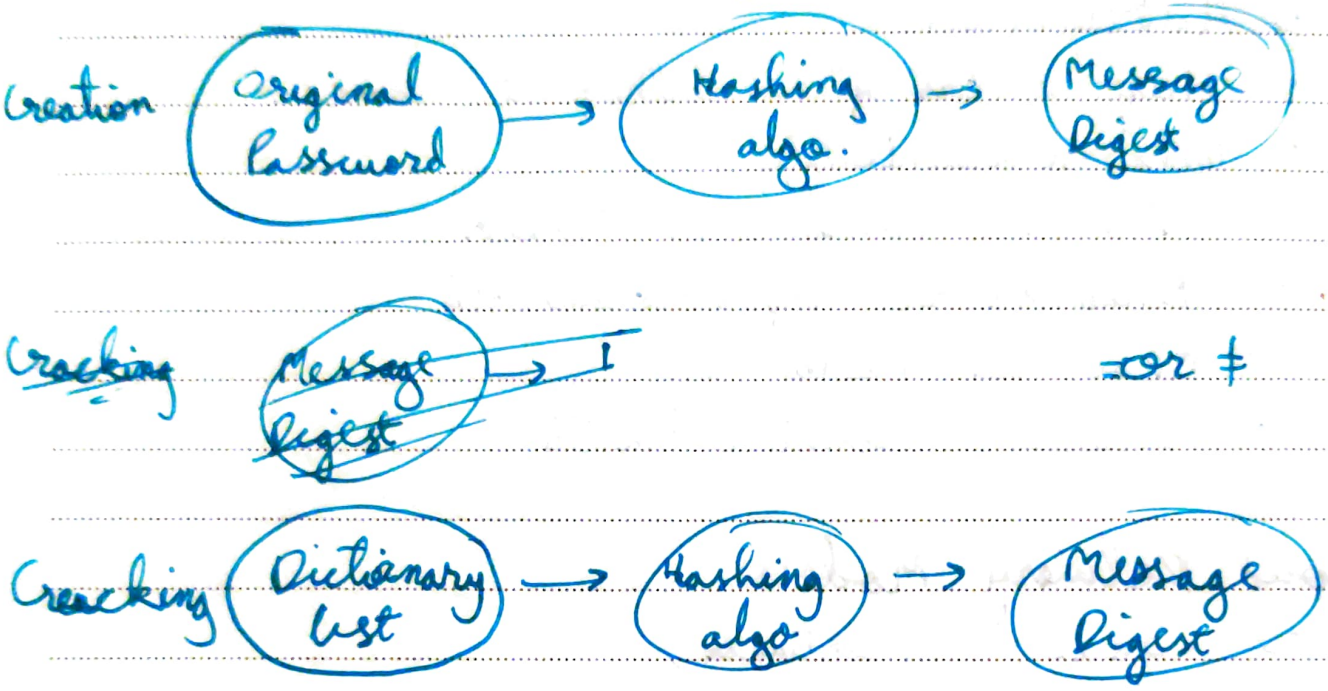
⑧ Detecting Live Systems

i) Wardriving : Looking for open wireless access points.
ii) ICMP (ping) : Ping is used to detect live systems.
iii) Port scanning: & Detect open ports.
iv) OS fingerprinting : Determining OS of another system.

⑨ TCP/IP protocol Stack



(11) Password Cracking Process



(12) Steps in Passive Information Gathering

- Scrutinizing key employees
- Dumpster diving
- Analysing web page coding
- Exploiting website authentication methods
- Mining for job ads & analysing financial data
- Using google to mine sensitive info.
- Exploring domain ownership.

(13) Reduce effectiveness of Enumerating Systems

i) Turn off SNMP. If not possible, block port 161 at network choke points & upgrade to SNMP v3.
Implement ACL filtering to allow only specific stations or subnets to read/write.

ii) → Higher end switches (FOR routers)
→ Dynamic ARP inspection
→ Anti Sniffing
→ Promiscuous mode detection
→ Improved routing protocols
→ Signatures added to IDS.

iii) For windows,
→ Block ports
→ Disable unnecessary services
→ Use the restrict anonymous setting