

WEEK 3 – THEORETICAL KNOWLEDGE

Advanced Reconnaissance & OSINT

What is Recon?

Reconnaissance is the process of gathering target information to plan attack paths. Attackers use both **passive** and **active** methods.

Type	Example Tools	MITRE	Description
Passive Recon	Shodan, WHOIS, Google Dorking	T1593	No direct interaction with target
Active Recon	Nmap, Banner Grabbing	T1046	Directly scanning the target

Key points:

- Identify open ports, services, employee emails, and tech stack.
- Build target attack surface.
- Map subdomains → find weak entry.

Case Study Example:

Equifax breach attackers used subdomain scanning and outdated Apache Struts discovery through OSINT.

Initial Access Techniques

Attackers first enter a network using social engineering or service exploitation.

Technique	Tools	MITRE	Target Weakness
Speare Phishing	Gophish, Evilginx2	T1566.001	Human trust
Credential Attacks	Hydra, Password Spraying	T1110	Weak passwords
Exploit Remote Apps	Metasploit	T1190	Unpatched systems

Goal: Gain a foothold into the network.

Exploitation & Vulnerability Research

Lifecycle:

1. Scan for vulnerabilities
2. Match exploit
3. Execute payload
4. Establish access

Area	Tools	Example Vulnerability
Web Exploit	OWASP ZAP, Burp Suite	SQLi, XSS
Binary Exploit	GDB, radare2	Buffer Overflow
Kernel Exploit	Exploit-DB, Metasploit	Priv Esc

Key MITRE:

T1190 (Exploit Public Facing Application)

T1068 (Privilege Escalation)

Example:

CVE-2021-3156 Sudo heap overflow gave root access.

Lateral Movement & Persistence

Goal	Method	Tool	MITRE
Move inside network	Pass-the-Hash, PsExec	Impacket	T1021
Maintain control	Registry keys, Scheduled Tasks	schtasks.exe	T1053

Evasion Techniques

Attackers hide attacks from AV, EDR, and monitoring systems.

Evasion Type	Example	Tool	MITRE
AV Bypass	Encoded payloads	msfvenom	T1027
Network Masking	Tor Proxychains	proxychains	T1090
Masquerading	Rename malicious processes	LOLBins	T1036

Objective: Remain undetected as long as possible.