Day 18: Penetration Testing & Information Gathering (July 7, 2025)

Topics Covered:

- Penetration Testing tools overview.
- Wappalyzer and WebCheck for web fingerprinting.
- Subdomain enumeration (theHarvester, Dmitry, Subfinder).
- Deep reconnaissance with shell scripting and OSINT tools.
- Assignment on subdomain and email enumeration.

Tools and Concepts:

1. **Wappalyzer:** Browser extension to identify website technologies.
2. **WebCheck:** Online scanner for website tech stack, HTTP headers, security.
3. **HTTrack:** Mirrors websites for passive discovery.

Subdomain Enumeration Techniques:

- **theHarvester:** Collects subdomains, emails from public databases.
- **Dmitry:** Deep info gathering (whois, subdomains, emails, open ports).
- **Shell Scripting:** Automates recon tasks.
- **Subfinder & Assetfinder:** Popular subdomain discovery tools.

Common Information Gathering Tools:

Tool	Purpose
dmitry	Deep info gathering
theHarvester	Subdomain and email harvesting
recon-ng	Reconnaissance framework
wappalyzer	Technology fingerprinting
subfinder	Subdomain discovery
assetfinder	Asset discovery
whatweb	Web fingerprinting
whois	Domain registration details
censys.io	Internet-wide scan engine
dig	DNS record lookup
amass	Comprehensive subdomain enumeration
shodan	Internet-connected devices search