Cybersecurity Daily Dairy

Day 18: Penetration Testing & Information Gathering

Date: July 7, 2025

Topics Covered:

- Overview of Penetration Testing tools
- Introduction to Wappalyzer and WebCheck for web fingerprinting
- Subdomain enumeration using theHarvester, Dmitry, and Subfinder
- Deep reconnaissance using shell scripting and OSINT tools
- Assignment on subdomain and email enumeration

Tools and Concepts:

1. Wappalyzer

A browser extension that identifies technologies used on websites, such as CMS platforms, JavaScript frameworks, analytics tools, and more.

2. WebCheck

An online scanner that provides detailed reports about a website's tech stack, HTTP headers, and security misconfigurations.

3. HTTrack

Used for mirroring websites. Can also help in passive discovery of site structure or hidden subdirectories.

Subdomain Enumeration Techniques:

theHarvester

A reconnaissance tool that collects subdomains, emails, and other open-source information from public databases.

Dmitry

A deep information gathering tool that collects domain-related data such as whois info, subdomains, email addresses, open ports, and more.

Shell Scripting for Recon

Shell scripts can be used to automate reconnaissance steps like subdomain enumeration, whois lookup, DNS record fetching, and more.

Subfinder & Assetfinder

Popular subdomain enumeration tools used in bug bounty programs to discover domain infrastructure.

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 and data engine
dig	DNS record lookup
amass	Comprehensive subdomain enumeration
shodan	Internet-connected devices search engine
nslookup	DNS querying

Web Threats and Architecture Concepts:

- robots.txt file restricts search engine bots from indexing specific pages or directories
- SSL/TLS provides encryption and security to website communications via HTTPS
- POST method is preferred for transmitting sensitive data, while GET is used for simpler URL-based requests
- MITM attacks can intercept communication between two parties
- Network threats include VOIP abuse, ARP poisoning, and traffic sniffing via tools like Ettercap or Bettercap
- Business logic flaws can allow attackers to manipulate application workflows, such as altering prices