TRAINING DAY 18 REPORT

Understand Footprinting

Today, I learn some important concepts

OSINT Framework

The **OSINT Framework** is usually presented as an interactive web-based directory. It organizes tools and services by categories, such as:

- **Social Media**
- **People Search Engines**
- **Domain Names**
- **Public Records**
- **Geolocation Tools**
- **Dark Web Tools**
- **Email Addresses**
- **Metadata Extraction**

Each category branches into subcategories, linking to external tools or platforms that can be used for investigations.

theHarvester is a **command-line tool** used to **gather information about email addresses, subdomains, hosts, virtual hosts, open ports, and banners** from public sources like search engines and the Shodan API. It's widely used in **penetration testing** and **reconnaissance** phases.

Introduction to Shodan

Shodan (Sentient Hyper-Optimized Data Access Network) is a powerful **search engine for internet-connected devices**. Unlike Google, which indexes websites, **Shodan indexes exposed devices and services**—like webcams, routers, servers, industrial control systems, smart TVs, and more.

Network Footprinting

Network footprinting is the **first step in cyber reconnaissance**. The goal is to **gather information about a target's network** — such as IP addresses, subnets, domains, services, and technologies — **without actively alerting the target**.

Key Objectives of Network Footprinting

1. Identify domain names and associated IP addresses
2. Discover subdomains and hidden services
3. Map network ranges (IP blocks, subnets)
4. Determine open ports and running services
5. Identify operating systems and software versions
6. Collect DNS records (A, MX, NS, TXT, SPF)
7. Uncover email servers and naming conventions
8. Detect presence of firewalls or IDS/IPS
9. Gather information about third-party services (CDNs, hosting)
10. Discover publicly exposed assets and endpoints
11. Extract SSL certificate details (e.g., via crt.sh)
12. Assess physical/geographic location of servers
13. Identify vulnerabilities tied to discovered services
14. Gather metadata from public documents or websites
15. Build a list of potential targets for social engineering

Tools Used in Network Footprinting

Passive Tools

1. **WHOIS** – Get registrar info and netblocks
2. **Shodan / Censys** – Find exposed services
3. **theHarvester** – Collect emails, subdomains
4. **crt.sh / Certspotter** – Discover SSL certs with hidden subdomains
5. **Recon-ng / Spiderfoot** – Automate passive OSINT
6. **Google Dorks** – Search exposed files/services

Active Tools (Used in Controlled/Authorized Environments)

1. **Nmap** – Port and service discovery
2. **Netcat** – Banner grabbing
3. **Traceroute** – Map network paths
4. **NSLookup / Dig** – Resolve DNS records
5. **SNMPwalk** – Query SNMP-enabled devices
6. **Ping Sweeps** – Identify live hosts