Footprinting & Reconnaissance

Footprinting

- Process of **collecting as much information as possible about a target network**
- Attacker **gathers publicly available sensitive information**

Know Security Posture | Reduce Focus Area | Identify Vulnerabilities | Draw Network Map

Objectives

Collect Network Information | Collect System Information | Collect Organization's Information

Methodology

- Footprinting through Search Engines
- Footprinting using Advanced Hacking Techniques
- Footprinting through Social Networking Sites
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering

Google Hacking Techniques

Query String | Vulnerable Targets | Google Operators

Advanced Search Operators

- [cache:]
- [link:]
- [related:]
- [info:]
- [site:]
- [allintitle:]
- [intitle:]
- [allintitle:]
- [inurl:]

Social Engineering on Social Networking Sites

- Gather **Sensitive Information**
- Create **Fake** Profile
- Post **Personal** Information
- **Tracking** Groups & **Trick to Reveal Information**

Website Footprinting

- **Monitoring** & **analyzing** the target organization's website
- Use of **Burp Suite, Zaproxy, Paros Proxy, Website Informer, Firebug** etc.
- Examining **HTML source**
- Examining **cookies**

Competitive Intelligence Gathering

- Process of **identifying**, **gathering**, **analyzing**, **verifying** & using information
- **Non-interfering** & **subtle in nature**
- **Sources**
  - Company websites & ads
  - Press release & annual reports
  - Trade journals, conferences & newspaper
  - Patent & trademarks
  - Analyst & regulatory reports
  - Customer & vendor interviews
  - Social engineering employees
  - Agent, distributors and suppliers

WHOIS Lookup

Maintained by **Regional Internet Registries** & contain the personal information of **domain owners**

- **WHOIS query return**:
  - Domain name details
  - Contact details of domain owner
  - Domain name server
  - When domain has been created etc.

DNS Information

- **Determine key hosts in the network** to perform social engineering attacks
- Provides information about **location** & **type of servers**

Locate the Network Range

- Assists to create a **map of the target**
- **Range of IP addresses** using **ARIN** tool

Social Engineering

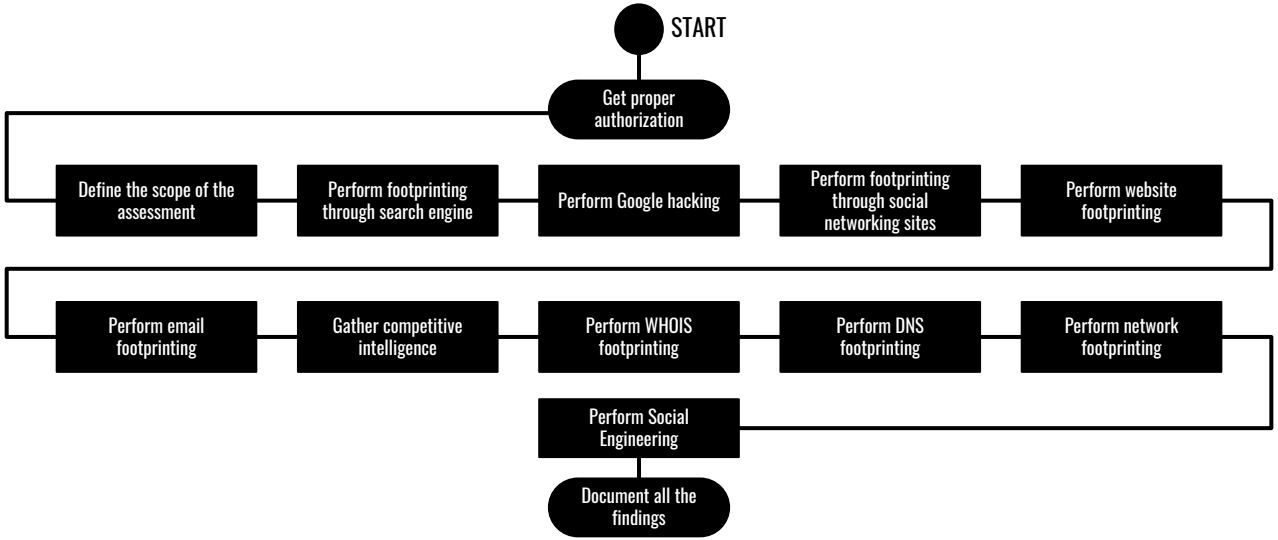
- Exploiting human behavior to **extract confidential information**
- **People are unaware** of their valuable information
- **Information gathers like:**
  - Credit card details & social security number
  - Usernames & passwords
  - Operating systems & software versions
  - Network layout information
  - IP addresses & names of server
- **Techniques:**
  - Eavesdropping
    - Unauthorized listening of conversation
    - Interception of any form of communication
  - Shoulder surfing
    - Attacker secretly observes the target
  - Dumpster diving
    - Looking for treasure in someone else's trash
  - Impersonation on social networking sites

Footprinting Countermeasures

- **Restrict the employees** to access from organization's network
- **Configure web servers** to avoid information leakage
- Educate employee to **use pseudonyms**
- Do not **reveal critical information**
- **Limit the amount of information** that are publishing
- Use of **footprinting techniques**
- **Prevent caching** of the web page
- Use **anonymous registration services**
- Enforce **security policies**
- **Restrict zone transfer** to authorized servers
- **Disable directory listing** in web servers
- Educate about **social engineering tricks & risks**
- Privacy services on **WHOIS lookup database**
- Avoid **domain-level cross-linking**
- **Encrypt** & **password protect sensitive information**

Footprinting Pen Testing

- Used to **determine organization's publicly available information**
- Gathering information from **internet & publicly accessible sources**
- **Helps** organizations to:
  - **Prevent information leakage**
  - **Prevent social engineering attempts**
  - **Prevent DNS record retrieval**



THE END