Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Footprinting

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Chapter Outline

- Definition, Purpose, and Process
- Terminology, Attacks, and Tools
- Useful Websites and Social Engineering Methods

Definition, Purpose, and Process

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

What is Footprinting

- **Footprinting is the first step in the ethical hacking process. It consists of passively and actively gaining information about the target.**
- **Types of information:**
  - **IP address ranges**
  - **Namespaces**
  - **Employee information**
  - **Phone numbers**
  - **Facility information**
  - **Job information**

Purpose of Footprinting

- During the footprinting process the attacker wants to gain useful information that will help facilitate future attacks.
- This step should be done carefully and methodically. Imprecision can attract the targets attention.
- Attackers can spend a bulk of their time just gathering and verifying information.

Footprinting Process

- **Footprinting usually has the following steps:**
  - **Collecting public information about the target**
    - **Host and network information**
  - **Determining the operating system(s) used in the environment.**
  - **Issue queries like DNS, network and organizational queries.**
  - **Search for known or potential vulnerabilities that exist in the target infrastructure.**

Terminology, Attacks, and Tools

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Footprinting Terminology

- **Open source and passive information gathering**
  - **The least aggressive approach to gathering information. Attackers use publicly available sources like newspapers, websites, social media, etc.**
- **Active information gathering**
  - **The attacker uses methods like social engineering to gain information about the target.**
- **Pseudonymous footprining**
  - **The attacker disguises themselves as someone else to gain information on the target.**
- **Internet footprinting**
  - **The attacker gains information on the target using the internet.**

Footprinting Attacks

- **Social engineering**
  - **The ability target information from the target through direct communication.**
- **Network and system attacks**
  - **Used to gather information on the system environment, configuration, and operating systems.**
- **Information leakage**
  - **Private information is accidentally revealed.**
- **Privacy Loss**
  - **An unauthorized user gains access to private data**
- **Revenue Loss**
  - **A breach or loss of data results in financial loss.**

Footprinting Tools

- **Search engines**
  - **Search engines can be used to gain a ton of information on the target. This can be information that they thought was hidden or simply forgot about. Types of firewalls, intranet portals, login pages, employee data, etc.**
- **Google hacking**
  - **Advanced operators can be used with a google search in order to get more specific results.**
- **Netcraft**
  - **A suite of tools that obtains web server version, address, subnet data, operating systems, and subdomain data.**

Footprinting Tools

- **Link extractor**
  - **A tool that extracts internal and external URLs for a location.**
- **Restricted websites**
  - **Websites that are not intended for public consumption. May be a page that isn't publicized and require login credentials.**
- **Geography**
  - **Knowing the target's physical location can aid in dumpster diving, social engineering, etc.**
  - **Google Earth, Google Maps, and webcams can help identify the geography.**

Useful Websites and Social Engineering Methods

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Useful Websites

- **Echosec**
  - www.echosec.net
  - **Allows users to search social media post by location.**
- **Maltego**
  - www.paterva.com
  - **Retrieves information form social media websites and shows the relationship between them.**
- **Job sites**
  - **Under required skills one can determine operating systems, system infrastructure, etc.**
- **Financial sites**
  - **Sties like Yahoo Finance can provide company data that isn't publicized elsewhere.**

Social Engineering Methods

- **Eavesdropping**
  - Listening in on private conversations of others or reading written correspondence.
- **Phishing**
  - A fictious message meant to look like it was sent from a legitimate source. It is used to entice the target to provide information or open a link/ attachment.
- **Shoulder surfing**
  - Observing a target while they operate a device to obtain passwords, account numbers, or other data.
- **Dumpster diving**
  - Going through the targets trash to find personal information.