02-Footprinting / Reconnaissance

Victim Data: no direct interaction

Scope & Contract:

Scope: Site & company: expsec.us
You may phish any email account ending in @expsec.us
You may phish any social media accounts that match found credentials

Rules: do not send any files to anyone. If you need a website other than the site owned by your instructor use http://certifiedhacker.com/ a real website with no instructions (from ec council)

Advanced: Build a data file of users names/ accounts/ possible passwords / password file
Use file offered in class if you want to submit to 1@vmlt.com with a subject line of RECON.

Attacker Data: Kali/ Parrot

Objective

Extract information about the target organization WITHOUT DIRECT INTERACTION OR SCANNING.
Document all the data collected for later use.

Employee details, partner details, weblinks, web technologies, patents, trademarks
List email addresses, possible passwords, tools they use to support business.
Domains, sub-domains, network blocks, network topologies, trusted routers, firewalls, IP addresses of the reachable systems, the Whois record, DNS records.

Overview of Reconnaissance

Footprinting can be categorized into passive footprinting and active footprinting:

Passive: Involves gathering information without direct interaction. This is useful when there is a requirement that the information-gathering activities are not to be detected by the target.

Active: Involves gathering information with direct interaction.

LAB Activities: Footprinting & Reconnaissance

1. Perform reconnaissance through search engines

1.2. video search engines

1.3. FTP search engines

1.4. IoT search engines

2. Perform reconnaissance through web services

2.1. Find the company’s domains and sub-domains using Netcraft

2.2. Gather personal information using PeekYou online people search service

2.3. Gather an email list using theHarvester*

2.4. Gather information using deep and dark web searching

2.5. Determine target OS through passive reconnaissance

3. Perform reconnaissance through social networking sites

3.1. Gather employees’ information from LinkedIn using theHarvester*

3.2. Gather personal information from various social networking sites using Sherlock

3.3. Gather information using Followerwonk

4. Perform website reconnaissance

4.1. Gather information about a target website using ping command line utility

4.2. Gather information about a target website using Website Informer

4.3. Extract a company’s data using Web Data Extractor

4.4. Mirror the target website using HTTrack Web Site Copier

4.5. Gather a wordlist from the target website using CeWL

5. Perform email reconnaissance

5.1. Gather information about a target by tracing emails using eMailTrackerPro

6. Perform Whois reconnaissance*

6.1. Perform Whois lookup using DomainTools

7. Perform DNS reconnaissance*

7.1. Gather DNS information using nslookup command line utility and online tool

7.2. Perform reverse DNS lookup using reverse IP domain check and DNSRecon

8. Perform network reconnaissance

8.1. Locate the network range

8.2. Perform network tracerouting in Windows and Linux Machines

9. Perform reconnaissance using various tools

9.1. Recon-ng

9.2. Maltego

*Indicates capture