Study Guide

Certified Ethical Hacking: Reconnaisssance/Footprinting

# Checklist of Exam Objectives: Areas to Study

## Breakdown footprinting and reconnaissance to gain primary information about a potential target

### Review footprinting concepts

### Detail the footprinting methodology

### Demonstrate footprinting through search engines

### Demonstrate footprinting through web services

### Demonstrate footprinting through social networking sites

### Demonstrate website footprinting

### Demonstrate email footprinting

### Demonstrate WHOIS footprinting

### Demonstrate DNS footprinting (nslookup)

### Demonstrate network footprinting

### Demonstrate footprinting through social engineering

### Compare footprinting tools

### Examine footprinting countermeasures

# Exam Essentials: What you need to know

#### Golden Keys:

#### Goals of Reconnaissance

#### Attacker can collect the following information −

#### Domain name

#### IP Addresses

#### Namespaces

#### Employee information

#### Phone numbers

#### E-mails

* Know how to look for news, press releases, blogs, and newsgroup entries from a corporation.
* Gather information on a target company and data about its network and system security using all accessible public resources.
* To locate personnel of the target company, use Yahoo! People Search or other Internet search engines.
* Understand how to use DNS to look up specific record information. Know how to query a DNS server for record information, such as hosts and IP addresses, using DNSstuff, NSlookup, or Sam Spade.
* Learn how to use Whois to find for personal or business information. Know how to get registrar and corporate contact information using the ARIN, LACNIC, RIPE NCC, APNIC, and Whois databases.
* Know how to locate the external and internal domain names of a target company.
* You should be able to find the domain information for a firm using Whois. The exam also requires knowledge of the ARIN database.
* Understand where a target company's web server and other network infrastructure equipment are physically located. To gain a graphical depiction of the route to a target company's network, use various tools. You can use these tools to physically find the servers.
* Understand how to track email sent or received by a company. You should be able to monitor an email sent to a target organization and gather extra information to utilize in an attack using email tracking services.
* Recognize the distinction between human-based and computer-based social engineering attacks. To launch an attack, human-based social engineering involves nontechnical tactics, whereas computer-based social engineering employs a computer.
* Human-based social engineering techniques include impersonation, posing as a key user, the third-person method, posing as technical support, shoulder surfing, and dumpster diving.
* Computer-based social-engineering approaches include email attachments, bogus websites, pop-up windows, and reverse social engineering.
* Recognize the significance of employee training. Preventing social-engineering attacks requires training staff on the indicators of social engineering and the company's security policy.

# Important Terminology

* Spider – to download a duplicate version of a targeted website
* Active reconnaissance – direct interaction with a target system/network
* Passive reconnaissance – gather intel with no direct interaction with target
* WayBackMachine – a website where you can visit websites based on dates
* Social Engineering – hacking humans by getting them to do things they normally wouldn’t do based on an emotion

#### Domain Name Intel

Use http://www.whois.com/whois website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry, name server, owner's contact information, and more

#### Finding IP Address

* Ping various DNS name records
  + A – AAAA
  + MX
  + SOA
  + TXT
  + CNAME
  + SPF

#### Finding IP Address Ranges

You can obtain a range of IP addresses assigned to a particular company using American Registry for Internet Numbers (ARIN)

#### Social Engineering

#### The manipulation of a person to induce them to do something they should not do

#### 

#### History of the Website

Using the WayBackMachine at <https://www.archive.org>

#### NetCraft

Blueprint a comprehensive list of information about the technologies and information about target website.

#### HTTrack

CLI version or Web Interface version to spider a targeted website

#### Email header

Show servers and where the location of those servers are. Headers can provide: Names, Addresses (IP, email), Mail servers, Time stamps, Authentication and more

#### IP Address Management

* ARIN - North America
* APNIC - Asia Pacific
* RIPE - Europe, Middle East
* LACNIC - Latin America
* AfriNIC – Africa

#### Nslookup

Performs DNS queries

#### Network Footprinting

IP address range can be obtained from regional registrar (e.g: ARIN for America, RIPE for Europe, etc)

#### OSRFramework

Uses open source intelligence to get information about target.

#### Recon-ng

A web-based open-source reconnaissance tool used to extract information from a target organization and its personnel.

#### theHarvester

An OSINT tool; Useful for gathering information like:

* Emails
* Subdomains
* Hosts
* Employee names
* Open ports

#### Sublist3r

Enumerates subdomains using many several engines such as Google, Yahoo, Bing, Baidu and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS

#### Maltego

OSINT tool, you can extract a broad type of information through the network, technologies and personnel(email, phone number, twitter).

#### Shodan

A search engine that crawlers to traverse your entire site, directly into the channel behind the Internet, various types of port equipment including IoT devices.

# Self-Assessment Questions: Test your Understanding

1. What type of device would you use the web service Shodan for?
   1. IoT
   2. Mobile
   3. Web servers
   4. Cloud storage servers
2. What information-gathering tool will give you information regarding the operating system

of a web server?

* 1. NSlookup
  2. DNSlookup
  3. tracert
  4. Netcraft

1. What tool is a good source of information for employee’s names and addresses?
   1. Tracert
   2. WHOIS
   3. Netcraft
   4. Traceroute
2. Dumpster diving can be considered which type of social-engineering attack
   1. Human-based
   2. Computer-based
   3. Physical based
   4. Paper based
3. What is the best way to prevent a social-engineering attack?
   1. Install/upgrade a firewall to prevent scanning
   2. Review IDS logs
   3. Training for employees
   4. Hire more helpdesk support staff
4. Nslookup can be used to gather which intel?
   1. DNS server location
   2. Hostnames and IP addresses
   3. WHOIS intel
   4. Name server and Operating systems
5. How does traceroute work?
   1. It uses a protocol that will is rejected by the gateway to determine the location of said router
   2. It sends a specially crafted IP packet to a router to locate the number of hops from the sender to the destination network
   3. It uses an ICMP destination-unreachable message to learn the name of a router and OS
   4. It uses the TTL value in an ICMP message to determine the number of hops from the sender to the router
6. Which are the four regional Internet registries?
   1. APNIC, LACNIC, ARIN, RIPE NCC
   2. APNIC, MOSTNIC, ARIN, RIPE NCC
   3. APNIC, PICNIC, NANIC, RIPE NCC
   4. APNIC, PICNIC, NANIC, ARIN
7. Which of the following is a tool for performing passive reconnaissance?
   1. Ping sweep
   2. Host scanning
   3. Traceroute
   4. WHOIS search
8. What is the next immediate step to be performed after reconnaissance?
   1. Enumeration
   2. Scanning
   3. System hijacking
   4. SQL Injection
9. What is the goal of reconnaissance?
   1. To find a target
   2. To map out the target network
   3. To scan the network for vulnerabilities
   4. To gather data on a target without being detected

# Answers to Self-Assessment Questions:

1. A - IoT
2. D – Netcraft
3. C – WHOIS
4. A – Human based
5. C – Training for employees
6. B – Hostname and IP addresses
7. D – Uses a TTL and an ICMP message to determine the number of hops
8. A- APNIC, LACNIC, ARIN, RIPE NCC
9. D- WHOIS
10. B- Scanning
11. To gather data on a target without being detected