# CEH v13 Module 2: Footprinting and Reconnaissance

## Practice Questions & Scenario-Based Mastery

### Question 1

A penetration tester wants to find all PDF documents on a target's website that might contain the word 'restricted'. Which Google search operator combination is the most effective for this task?

* A) site:target.com filetype:pdf "restricted"
* B) inurl:target.com ext:pdf +restricted
* C) link:target.com pdf restricted
* D) target.com intitle:pdf restricted

Correct Answer: A) site:target.com filetype:pdf "restricted"

Rationale: The 'site:' operator restricts results to a specific domain, while 'filetype:' filters by extension and quotes ensure the exact keyword is found.

### Question 2

During the reconnaissance phase, you are using 'theHarvester'. Which of the following best describes the primary purpose of this tool in a CEH engagement?

* A) To perform a vulnerability scan on a web application.
* B) To gather subdomains, email addresses, and hostnames from public sources.
* C) To crack password hashes extracted from a database.
* D) To perform an active port scan on a target network.

Correct Answer: B) To gather subdomains, email addresses, and hostnames from public sources.

Rationale: theHarvester automates OSINT gathering by querying search engines, PGP key servers, and social networks like LinkedIn.

### Question 3

You need to identify the mail server for a target organization to prepare for a phishing simulation. Which DNS record type should you query?

* A) A record
* B) MX record
* C) NS record
* D) PTR record

Correct Answer: B) MX record

Rationale: The MX (Mail Exchange) record identifies the mail servers responsible for receiving email for a domain.

### Question 4

An ethical hacker attempts to run the command 'dig axfr @https://www.google.com/search?q=ns1.target.com target.com'. What is the hacker trying to perform?

* A) A reverse DNS lookup for the entire subnet.
* B) A DNS Zone Transfer.
* C) A denial-of-service attack on the DNS server.
* D) A query for the Start of Authority (SOA) record only.

Correct Answer: B) A DNS Zone Transfer.

Rationale: 'axfr' is the keyword used in DNS queries to request a full zone transfer, which reveals all records in a domain if the server is misconfigured.

### Question 5

Which tool is best described as a 'search engine for internet-connected devices' and can be used to find vulnerable industrial control systems or webcams?

* A) Maltego
* B) Shodan
* C) Recon-ng
* D) Whois

Correct Answer: B) Shodan

Rationale: Shodan crawls the internet to index banners and metadata from devices like routers, servers, and IoT gadgets.

### Question 6

Which of the following activities is considered 'Passive Footprinting'?

* A) Running a traceroute to the target's web server.
* B) Searching for an employee's profile on a professional social network.
* C) Attempting a DNS zone transfer from the target's name server.
* D) Using Nmap to check for open ports on the target's firewall.

Correct Answer: B) Searching for an employee's profile on a professional social network.

Rationale: Passive footprinting involves gathering info without directly interacting with the target's systems or network.

### Question 7

A hacker uses the tool 'FOCA' during an assessment. What is the primary output expected from this tool?

* A) A list of open ports and services.
* B) Metadata from publicly available documents (PDFs, Office files).
* C) A visual map of a target's internal network topology.
* D) A brute-force attack against an FTP server.

Correct Answer: B) Metadata from publicly available documents (PDFs, Office files).

Rationale: FOCA extracts metadata like usernames, software versions, and server paths from exposed files.

### Question 8

When performing a reverse DNS lookup, you are translating an IP address into a hostname. Which record is being queried?

* A) CNAME
* B) PTR
* C) SOA
* D) TXT

Correct Answer: B) PTR

Rationale: The Pointer (PTR) record resides in the reverse lookup zone and maps an IP address back to its hostname.

### Question 9

Which OSINT tool allows an investigator to visualize relationships between domains, IP addresses, and people in a graph-based interface?

* A) Sherlock
* B) Maltego
* C) theHarvester
* D) Netcraft

Correct Answer: B) Maltego

Rationale: Maltego uses 'transforms' to discover data and then displays them in a visual graph to show connections.

### Question 10

An attacker wants to find directories on a server that are allowing directory listing. Which Google Dork should they use?

* A) intitle:"index of"
* B) inurl:admin
* C) site:\*.com
* D) filetype:txt

Correct Answer: A) intitle:"index of"

Rationale: Web servers that allow directory listing often have 'Index of' in the title of the resulting page.

### Question 11

How does the 'traceroute' command determine the path to a destination?

* A) It sends a single packet with a very high TTL.
* B) It sends a sequence of packets with increasing Time-to-Live (TTL) values.
* C) It queries the DNS server for the path.
* D) It uses a specialized 'Path' protocol.

Correct Answer: B) It sends a sequence of packets with increasing Time-to-Live (TTL) values.

Rationale: Each router decrements the TTL; when it hits zero, it sends an ICMP 'Time Exceeded' message back, allowing the sender to map the hop.

### Question 12

You retrieve the Start of Authority (SOA) record for a domain. Which field in this record is incremented every time a change is made to the zone file?

* A) Refresh rate
* B) Serial number
* C) TTL (Time to Live)
* D) Retry interval

Correct Answer: B) Serial number

Rationale: The serial number is used by secondary servers to determine if their copy of the zone is out of date; it must be incremented after every change.

### Question 13

Which of the following is the most effective countermeasure against unauthorized DNS zone transfers?

* A) Hiding the primary DNS server's IP address.
* B) Configuring the DNS server to only allow zone transfers to specific IP addresses.
* C) Using a WAF to block DNS traffic.
* D) Disabling the DNS server entirely.

Correct Answer: B) Configuring the DNS server to only allow zone transfers to specific IP addresses.

Rationale: Restricting AXFR requests to trusted secondary servers ensures unauthorized users cannot download the zone database.

### Question 14

A penetration tester uses 'HTTrack' during the footprinting phase. What is the intended outcome of using this tool?

* A) To perform a vulnerability scan on SSL/TLS.
* B) To mirror the entire website onto a local machine for offline analysis.
* C) To find hidden administrative portals via brute force.
* D) To intercept and modify traffic.

Correct Answer: B) To mirror the entire website onto a local machine for offline analysis.

Rationale: Mirroring allows the tester to search through scripts and comments without alerting the live server.

### Question 15

A hacker has a username for a target and wants to see if that same username is used across multiple social media platforms. Which tool is best suited for this OSINT task?

* A) theHarvester
* B) Sherlock
* C) Photon
* D) Maltego

Correct Answer: B) Sherlock

Rationale: Sherlock is specifically designed to hunt for usernames across hundreds of social media platforms simultaneously.

### Question 16

A DNS 'CNAME' record is discovered for 'https://www.google.com/search?q=ftp.target.com' pointing to 'https://www.google.com/search?q=server-01.hosting-provider.com'. What does this tell the hacker?

* A) The organization's FTP server is actually being hosted by a third party.
* B) The FTP server is using a non-standard port.
* C) The FTP server is currently down.
* D) The FTP server is vulnerable to an exploit.

Correct Answer: A) The organization's FTP server is actually being hosted by a third party.

Rationale: A CNAME (Canonical Name) is an alias. Seeing it point to an external domain reveals the actual infrastructure provider.

### Question 17

Which reconnaissance framework is written in Python and uses a modular structure similar to Metasploit?

* A) Wifite
* B) Recon-ng
* C) Social Engineer Toolkit (SET)
* D) SQLmap

Correct Answer: B) Recon-ng

Rationale: Recon-ng is a powerful OSINT framework that organizes modules into categories like 'Recon' and 'Discovery'.

### Question 18

What is the primary difference between 'Competitive Intelligence' and 'Ethical Hacking Footprinting'?

* A) Competitive intelligence is illegal.
* B) Competitive intelligence focuses on business strategy, while footprinting focuses on security vulnerabilities.
* C) Footprinting is always active.
* D) There is no difference.

Correct Answer: B) Competitive intelligence focuses on business strategy, while footprinting focuses on security vulnerabilities.

Rationale: Both use OSINT, but the intent and the specific type of information sought (market vs. technical weakness) are different.

### Question 19

A hacker visits a target's homepage and uses the 'Wappalyzer' browser extension. What is the hacker trying to identify?

* A) The browser history of employees.
* B) The technology stack used by the website (PHP, jQuery, Apache).
* C) The physical location of the data center.
* D) Whether the website is vulnerable to XSS.

Correct Answer: B) The technology stack used by the website.

Rationale: Wappalyzer identifies software and frameworks by looking for specific code signatures and headers.

### Question 20

An organization wants to prevent hackers from seeing the personal name and contact info of the domain registrant. What should they implement?

* A) DNSSEC
* B) WHOIS Privacy (Privacy Shield)
* C) A reverse proxy server.
* D) A firewall with Deep Packet Inspection.

Correct Answer: B) WHOIS Privacy (Privacy Shield)

Rationale: Privacy services replace the owner's personal contact info with the contact info of a proxy service in public records.