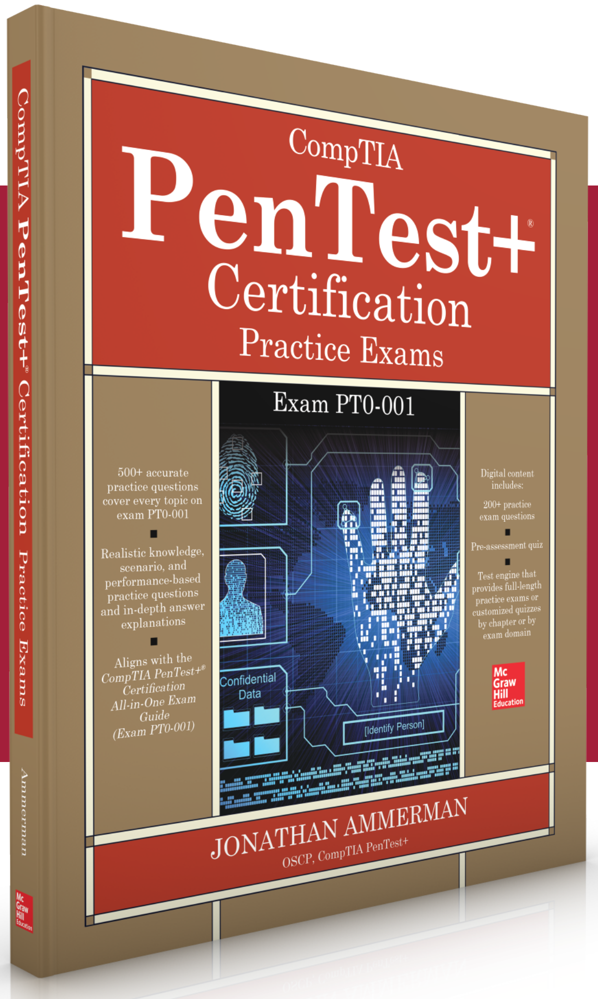
McGraw Hill

CompTIA

PenTest+® Certification

PRACTICE EXAMS

EXAMS PT0-001


CompTIA PenTest+® Certification Practice Exams
Ammerman
CompTIA
PenTest+®
Certification
Practice Exams
Exam PT0-001
500+ accurate practice questions cover every topic on exam PT0-001
Realistic knowledge, scenario, and performance-based practice questions and in-depth answer explanations
Aligns with the CompTIA PenTest+® Certification All-in-One Exam Guide (Exam PT0-001)
Confidential Data
[Identify Person]
Digital content includes:
200+ practice exam questions
Pre-assessment quiz
Test engine that provides full-length practice exams or customized quizzes by chapter or by exam domain
Mc Graw Hill Education
JONATHAN AMMERMAN
OSCP, CompTIA PenTest+

Sample Chapter

CHAPTER 2:

Getting to Know Your Targets

LEARN MORE

BUY NOW

Because learning changes everything.®

CHAPTER 2

Getting to Know Your Targets

This chapter includes questions on the following topics:

- Information gathering in a given scenario using appropriate techniques
- A comparison of various tools and their use cases

Following the pre-engagement meetings, the definition of the scope and rules of engagement, and the signing of contracts, a penetration tester is free to begin the next phase of an assessment: information gathering. It is generally accepted that there are two types of information gathering: passive and active. Passive information gathering consists of any collection of intelligence by means that are effectively invisible to the target in question; active information gathering will be discussed in Chapters 3 and 4.

By its most basic definition, passive information gathering is the collection of information from publicly available sources; this could mean queries in any given search engine, harvesting information from public DNS servers, or searching for the target organization's networks with tools such as Shodan or theharvester. To define it more precisely, passive information gathering is any collection of intelligence that may be useful in a penetration test without directly connecting or identifying oneself to the target of the penetration test. Although it is not terribly common to find a quick path to an exploitable process or service via passive information gathering, the data collected is still of importance to the overall penetration test; organizations often are unaware of just how wide their digital footprint is and will be amazed at the information you can find without them being aware. The questions in this chapter focus on basic information gathering principles and on the tools commonly used to do so.

McGraw Hill

CompTIA PenTest+® Certification

PRACTICE EXAMS

EXAMS PT0-001

Q QUESTIONS

1. Censys was created at the University of Michigan by the team of researchers who also developed what wide-scale Internet-scanning tool?
   - **A.** Nmap
   - **B.** Zmap
   - **C.** Nikto
   - **D.** Dirbuster

2. Domain registration information returned on a WHOIS search does *not* include which of the following?
   - **A.** Domain administrator e-mail
   - **B.** Domain administrator fax
   - **C.** Domain administrator organization
   - **D.** Domain administrator GPS coordinates

3. Open-source intelligence (OSINT) collection frameworks are used to effectively manage sources of collected information. Which of the following best describes open-source intelligence?
   - **A.** Company documentation labeled “Confidential” on an internal company storage share requiring authentication
   - **B.** Press release drafts found on an undocumented web page inside a company’s intranet
   - **C.** Any information or data obtained via publicly available sources that is used to aid or drive decision-making processes
   - **D.** Information gained by source code analysis of free and open-source software (FOSS)

4. In the following recon-ng output, what command is being invoked that is used to configure module parameters when called with a specific option and value?

```
[recon-ng][default][bing_linkedin_cache] > __________
__________ module options

Usage: __________ <option> <value>

  Name        Current Value  Required  Description
  ----------  -------------  --------  -----------
  LIMIT       0              yes       limit total number of pages per api
                                       request (0 = unlimited)
  SOURCE      default        yes       source of input (see 'show info' for
                                       details)
  SUBDOMAINS                 no        subdomain(s) to search on LinkedIn:
                                       www, ca, uk, etc
```

   - **A.** `use`
   - **B.** `set`
   - **C.** `load`
   - **D.** `show`

5. Which method of collecting open-source intelligence consists of the collection of published documents, such as Microsoft Office or PDF files, and parsing the information hidden within to reveal usernames, e-mail addresses, or other sensitive data?

   A. Metadata analysis

   B. File scraping

   C. File mining

   D. File excavation

6. Which of the following search engines is *not* used by FOCA when searching for documents?

   A. Bing

   B. Google

   C. Yahoo

   D. DuckDuckGo

7. What is the process by which large data sets are analyzed to reveal patterns or hidden anomalies?

   A. Passive information gathering

   B. Footprinting

   C. Active information gathering

   D. Data mining

8. In the following command, which flag is responsible for saving output to both XML and HTML files?

```
theharvester -d example.com -b google -f foo -v -n
```

   A. `-v`

   B. `-f`

   C. `-n`

   D. `-b`

9. Which of the following is an external resource or API that may be installed in Maltego to expand its capabilities?

   A. Shift

   B. Transform

   C. Modifier

   D. Tweak

10. Which static web page is focused on information gathering, providing web links and resources that can be used during the reconnaissance process, and can greatly aid penetration testers in the data-mining process?

A. Maltego

B. OSINT Framework

C. Shodan

D. Censys

11. Which of the following is an open-source, Python-based tool that runs strictly from the standard user command line and includes both passive and active options for intelligence collection (numerous command-line switches enable or disable functionality such as limiting queries to a specific search engine or running searches for identified IP addresses and hostnames in Shodan)?

A. recon-ng

B. Shodan

C. theharvester

D. Maltego

12. Which technique is used during passive reconnaissance to map a user-defined hostname to the IP address or addresses with which it is associated?

A. DNS zone transfer

B. Reverse DNS lookup

C. Investigation

D. Forward DNS lookup

13. While footprinting an organization for a penetration test, you discover that a service it relies on uses FTP across port 14147 for data transfers. How could you refine a Shodan search to only reveal FTP servers on that port?

A. `FTP port 14147`

B. `FTP:14147`

C. `FTP port:14147`

D. `FTP;port 14147`

14. Which free and GNU-licensed tool written for the Windows operating system family gathers information by scraping metadata from Microsoft Office documents, which can include usernames, e-mail addresses, and real names?

A. Maltego

B. FOCA

C. recon-ng

D. theharvester

15. Which of the following data sources is *not* a valid option in theharvester?

- **A.** Google
- **B.** LinkedIn
- **C.** Facebook
- **D.** Twitter

16. Which recon-ng command can be used to identify available modules for intelligence collection?

- **A.** `show workspaces`
- **B.** `show modules`
- **C.** `use modules`
- **D.** `set modules`

17. In a penetration test, it often occurs that a great deal of information pertinent to attacking target systems and goals is provided to the penetration tester. Which of the following are often provided by the target organization? (Choose two.)

- **A.** IP addresses
- **B.** Live usernames
- **C.** Domain names
- **D.** Administrator passwords for the Exchange and Active Directory servers

18. Which feature in Shodan is a collection of documentation that may be useful for developers who want to integrate Shodan searching into tools or applications they have developed or are currently developing?

- **A.** Reports
- **B.** Developer Integrations
- **C.** REST API
- **D.** Explore

19. What is the process of assessing a target to collect preliminary knowledge about systems, software, networks, or people without directly engaging the target or its assets?

- **A.** Reconnaissance
- **B.** Passive information gathering
- **C.** Web searching
- **D.** Active information gathering

20. When used as part of a search through theharvester, what will be the effect of the `-n` flag?

- **A.** A DNS brute-force search will be conducted for the domain name provided.
- **B.** Identified hosts will be cross-referenced with the Shodan database.
- **C.** A simple declaration of the domain or company name for which to conduct the search.
- **D.** A reverse DNS query will be run for all discovered ranges.

QUICK ANSWER KEY

1. B
2. D
3. C
4. B
5. A
6. C
7. D
8. B
9. B
10. B
11. C
12. D
13. C
14. B
15. C
16. B
17. A, C
18. C
19. B
20. D

IN-DEPTH ANSWERS A

1. Censys was created at the University of Michigan by the team of researchers who also developed what wide-scale Internet-scanning tool?

   A. Nmap

   B. Zmap

   C. Nikto

   D. Dirbuster

   ☑ **B**. The developers of Censys are also responsible for the development of Zmap, a wide-scale Internet port scanner.

   ☒ **A**, **C**, and **D** are incorrect. Nmap was originally written by Gordon Lyon and is now found at its github repository (https://github.com/nmap/nmap), where public users can submit code and contribute to its further development. Nikto is developed by Chris Sullo and David Lodge; more information may be found at the developers' website (https://cirt.net/nikto2), and the tool itself may be found at its github repository (https://github.com/sullo/nikto). Dirbuster was originally developed as part of the OWASP Dirbuster project, which is now inactive. Fortunately, the functionality of Dirbuster has been absorbed by the OWASP ZAP (Zed Attack Proxy) team, which has functionally forked Dirbuster into an extension for the ZAP project. Because these tools were all developed by a different team from the one responsible for Censys, these answers are incorrect.

2. Domain registration information returned on a WHOIS search does *not* include which of the following?

   A. Domain administrator e-mail

   B. Domain administrator fax

   C. Domain administrator organization

   D. Domain administrator GPS coordinates

   ☑ **D**. Although WHOIS domain registration information can be quite detailed, the most one can expect to find concerning geographic location is a physical address. GPS coordinates are not found in a WHOIS query, making this the correct answer. Additionally, note that this information may all ultimately be protected by a WHOIS guard service; for numerous reasons, web administrators may have issues with broadcasting their names, e-mail addresses, and home addresses across the Internet. To account for this, domain registrars will often front their own information in WHOIS information for a domain, with a simple e-mail address to contact in the case of abuse or misuse of a domain they have registered on behalf of a client. This allows action to be taken if a site with privatized WHOIS data is serving malware, engaged in copyright infringement, or other situations where there is a legal or ethical duty to shut down a site or require its alteration.

   ☒ **A**, **B**, and **C** are incorrect. E-mail addresses, fax numbers, and organizational names for the domain administrator are all commonly found in WHOIS domain registry entries.

3. Open-source intelligence (OSINT) collection frameworks are used to effectively manage sources of collected information. Which of the following best describes open-source intelligence?

A. Company documentation labeled “Confidential” on an internal company storage share requiring authentication

B. Press release drafts found on an undocumented web page inside a company’s intranet

C. Any information or data obtained via publicly available sources that is used to aid or drive decision-making processes

D. Information gained by source code analysis of free and open-source software (FOSS)

☑ **C.** Open-source intelligence is any information or data obtained via publicly available sources that is used to aid or drive decision-making processes.

☒ **A**, **B**, and **D** are incorrect. **A** and **B** are incorrect because documentation labeled “Confidential” on network shared storage requiring authentication and websites locked behind a company intranet are clearly meant to share knowledge with individuals within the organization with a need to know the information. As such, they are examples of information that would not be discoverable via open-source collection methods. **D** is incorrect because the use of the term “open source” in this case is a red herring, referring to its relevance to software rather than information gathering. Be wary for such misleading answers during the exam.

4. In the following recon-ng output, what command is being invoked that is used to configure module parameters when called with a specific option and value?

```
[recon-ng][default][bing_linkedin_cache] > __________
__________ module options

Usage: __________ <option> <value>

  Name        Current Value  Required  Description
  ----------  -------------  --------  -----------
  LIMIT       0              yes       limit total number of pages per api
                                       request (0 = unlimited)
  SOURCE      default        yes       source of input (see 'show info' for
                                       details)
  SUBDOMAINS                 no        subdomain(s) to search on LinkedIn:
                                       www, ca, uk, etc
```

A. `use`

B. `set`

C. `load`

D. `show`

☑ **B.** In both Metasploit and recon-ng, the `set` command is used to configure module options.

☒ **A**, **C**, and **D** are incorrect. The `use` and `load` options are identical in function: they load a given module for use in recon-ng, but do not set module options. The `show` command is used to display various pieces of information about the framework.

5. Which method of collecting open-source intelligence consists of the collection of published documents, such as Microsoft Office or PDF files, and parsing the information hidden within to reveal usernames, e-mail addresses, or other sensitive data?

A. Metadata analysis

B. File scraping

C. File mining

D. File excavation

☑ **A**. Metadata analysis is the term for collecting open-source intelligence by parsing published documents for information hidden within to reveal usernames, e-mail addresses, or other sensitive data.

☒ **B**, **C**, and **D** are incorrect. File scraping, file mining, and file excavation are all meaningless phrases meant to sound like information security terminology, without having a specific meaning within that context. Be wary of answers in this vein during the exam.

6. Which of the following search engines is *not* used by FOCA when searching for documents?

A. Bing

B. Google

C. Yahoo

D. DuckDuckGo

☑ **C**. Yahoo is not used by FOCA when it searches for documents, making this the correct answer.

☒ **A**, **B**, and **D** are incorrect. Bing, Google, and DuckDuckGo are all used by FOCA when it searches for documents.

7. What is the process by which large data sets are analyzed to reveal patterns or hidden anomalies?

A. Passive information gathering

B. Footprinting

C. Active information gathering

D. Data mining

☑ **D**. Data mining is the process by which large data sets are analyzed to reveal patterns or hidden anomalies.

☒ **A**, **B**, and **C** are incorrect. **A** and **C** are incorrect because passive and active information gathering are methods of intelligence *collection,* not analysis. **B** is incorrect because footprinting is the process of conducting reconnaissance against computers and information systems during a penetration test with the aim of finding the most efficient methods of attack that will meet the goals of the assessment.

8. In the following command, which flag is responsible for saving output to both XML and HTML files?

```
theharvester -d example.com -b google -f foo -v -n
```

A. `-v`

B. `-f`

C. `-n`

D. `-b`

☑ **B.** The `-f` flag in theharvester will dump output into both an HTML and XML document (in this case, to foo.xml and foo.html).

☒ **A**, **C**, and **D** are incorrect. The `-v`, `-n`, and `-b` flags, respectively, verify a hostname via DNS resolution, perform a reverse DNS query on the IP ranges discovered to be in use, and allow the user to define the data source (such as Google, Bing, or LinkedIn).

9. Which of the following is an external resource or API that may be installed in Maltego to expand its capabilities?

A. Shift

B. Transform

C. Modifier

D. Tweak

☑ **B.** An external resource or API that may be installed in Maltego to expand its capabilities is called a transform.

☒ **A**, **C**, and **D** are incorrect. Although related definitionally, the terms "shift," "modifier," and "tweak" are not relevant to Maltego.

10. Which static web page is focused on information gathering, providing web links and resources that can be used during the reconnaissance process, and can greatly aid penetration testers in the data-mining process?

A. Maltego

B. OSINT Framework

C. Shodan

D. Censys

☑ **B.** The OSINT Framework is a static web page is focused on information gathering, providing web links and resources that can be used during the reconnaissance process and can greatly aid penetration testers in the data mining process.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because Maltego is an OSINT collection application that is known for its ability to build and illustrate connections between various data points. **C** and **D** are incorrect because Shodan and Censys are Internet of Things (IoT) search engines that excel at finding open services on the Internet. It is also worth noting that as search engines, definitionally neither Shodan nor Censys can be static pages.

11. Which of the following is an open-source, Python-based tool that runs strictly from the standard user command line and includes both passive and active options for intelligence collection (numerous command-line switches enable or disable functionality such as limiting queries to a specific search engine or running searches for identified IP addresses and hostnames in Shodan)?

A. recon-ng

B. Shodan

C. theharvester

D. Maltego

☑ **C.** The tool theharvester is best described by the question.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because while recon-ng is written in Python, it is a framework designed solely for web-based open-source intelligence collection. It is typically run from within its own pseudo-shell environment (although there is support for bash and other shell-based, command-line tasks being executed via recon-cli, a component distributed with the core recon-ng packages). **B** is incorrect because Shodan is a web application and generally is not run from the command line, barring the use of Shodan's API. In addition, Shodan is explicitly mentioned in the question, making it far less likely to be the correct choice. **D** is incorrect because Maltego is a Java-based application with a graphical user interface and is best known for its excellent illustration of data point connections. Note that while Maltego *may* be run from the command line for some functions, the strengths of its graphical interface make it the primary means of access for many penetration testers. In addition, Maltego is proprietary software. Since the question explicitly asks for an open-source tool, the certification candidate can safely rule this answer out.

12. Which technique is used during passive reconnaissance to map a user-defined hostname to the IP address or addresses with which it is associated?

A. DNS zone transfer

B. Reverse DNS lookup

C. Investigation

D. Forward DNS lookup

☑ **D**. A forward DNS lookup queries the name server for a domain or hostname, for which the DNS server will then provide the associated IP address; this function is present at the heart of the Internet, as the use of human-readable terms such as "google.com" in web browsers would fail without it. Put another way, in the absence of a service such as DNS, we would be required to use machine-readable logical addresses alone (that is, IP addresses) to do nearly anything across a network.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because a DNS zone transfer is a type of DNS transaction wherein a DNS database is replicated to the requesting system. DNS zone transfers can be of great benefit to penetration testers if internal corporate name servers permit them; knowledge of the entirety of an organization's IP space and hostnames can be of immense value in identifying potential targets during a penetration test. **B** is incorrect because a reverse DNS lookup takes a user-provided IP address and then queries a name server for the host(s) or domain(s) with which that address is associated. **C** is incorrect because "investigation" is not a term with an explicit definition in the lexicon of penetration testing.

13. While footprinting an organization for a penetration test, you discover that a service it relies on uses FTP across port 14147 for data transfers. How could you refine a Shodan search to only reveal FTP servers on that port?

A. `FTP port 14147`

B. `FTP:14147`

C. `FTP port:14147`

D. `FTP;port 14147`

☑ **C**. Search and filter terms in Shodan must be provided in the format *search_string filter:value*. In the example given, `FTP port:14147` will search for FTP connections available on the open Internet and then filter all but those running on port 14147 from the search results.

☒ **A**, **B**, and **D** are incorrect because search and filter terms in Shodan must be provided in the format *search_string filter:value*.

14. Which free and GNU-licensed tool written for the Windows operating system family gathers information by scraping metadata from Microsoft Office documents, which can include usernames, e-mail addresses, and real names?

A. Maltego

B. FOCA

C. recon-ng

D. theharvester

☑ **B**. FOCA is a free, GNU-licensed tool that gathers information by scraping metadata from Microsoft Office documents, which can include usernames, e-mail addresses, and real names. Note that while FOCA can be run in Linux and Unix variants using WINE (a compatibility layer or interface that allows Windows applications to run on *nix operating systems), the question specifically mentions that the tool was written *for* Windows, rather than stating that it *only* runs in Windows.

☒ **A**, **C**, and **D** are incorrect. **A** and **C** are incorrect because while Maltego and recon-ng are capable of scraping metadata from files with the use of transforms or modules, neither of these tools was written specifically for the Windows operating system family. **D** is incorrect because theharvester is limited to what can be pulled directly from a website; scraping the contents of files stored on a website is beyond its capabilities. In addition, theharvester is like Maltego and recon-ng in that it was not written specifically for the Windows operating system.

15. Which of the following data sources is *not* a valid option in theharvester?

A. Google

B. LinkedIn

C. Facebook

D. Twitter

☑ **C**. Although theharvester can query many data sources, Facebook is not one of them, which makes C the correct answer. Pay careful attention to questions that are stated with a negating term such as "is not" or "are not."

☒ **A**, **B**, and **D** are incorrect. Google, LinkedIn, and Twitter are all valid data sources for theharvester, making these incorrect choices for this question.

16. Which recon-ng command can be used to identify available modules for intelligence collection?

A. `show workspaces`

B. `show modules`

C. `use modules`

D. `set modules`

☑ **B**. The command `show modules` will list all available modules for use in recon-ng.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because the command `show workspaces` will output a list of all workspaces that have been added to the recon-ng database. **C** is incorrect because the command `use modules` will return an error since there is no module named "modules." **D** is incorrect because `set modules` will display usage guidelines for the "set" command, along with a list of module options that may be configured.

17. In a penetration test, it often occurs that a great deal of information pertinent to attacking target systems and goals is provided to the penetration tester. Which of the following are often provided by the target organization? (Choose two.)

A. IP addresses

B. Live usernames

C. Domain names

D. Administrator passwords for the Exchange and Active Directory servers

☑ **A** and **C**. IP addresses and domain names are typically provided by a target organization in the statement of work prior to an engagement; this is in fact necessary, at minimum, to establish the scope for the penetration test. From this sparse information, further data may be obtained and used via open-source intelligence collection to greatly enhance the success rate of a penetration test.

☒ **B** and **D** are incorrect. Live usernames and administrator passwords are secrets that should be discovered by a penetration tester during an engagement, if they are discovered at all. The obvious exception here is a white box penetration test, wherein valid authentication credentials may be part of the starting information provided to a penetration tester.

18. Which feature in Shodan is a collection of documentation that may be useful for developers who want to integrate Shodan searching into tools or applications they have developed or are currently developing?

A. Reports

B. Developer Integrations

C. REST API

D. Explore

☑ **C.** The REST API section is a collection of documentation on the Shodan API; this component is useful for developers who might want to integrate Shodan searching into tools or applications they have developed or are currently developing.

☒ **A**, **B**, and **D** are incorrect. **A** is incorrect because the Reports feature of Shodan transforms the relevant output of a given query into a readily understood, easy-to-digest infographic. It identifies the countries in which search hits occur as well as vulnerabilities and informational items relevant to those systems, which can provide an excellent snapshot of an organization's security posture. **B** is incorrect because the Developer Integrations section of shodan.io is simply a collection of links to documentation on tools, applications, and other resources that have integrated the Shodan API. Examples include the Metasploit framework, recon-ng, and Maltego. **D** is incorrect because the Explore function of Shodan is a means of seeing search queries made by other users; the value here lies in the ability of the wisdom of the crowd to reveal search terms or approaches that a user might not have considered previously.

19. What is the process of assessing a target to collect preliminary knowledge about systems, software, networks, or people without directly engaging the target or its assets?

A. Reconnaissance

B. Passive information gathering

C. Web searching

D. Active information gathering

☑ **B.** Passive information gathering is the process of assessing a target to collect preliminary knowledge about systems, software, networks, or people without directly engaging the target or its assets.

☒ **A**, **C**, and **D** are incorrect. **A** is incorrect because reconnaissance is a broader term that can describe both passive *and* active information-gathering efforts. **C** is incorrect because web searching is just one specific activity which is performed while passive information gathering. **D** is incorrect because active information gathering is the process of collecting information about target systems, software, networks, or people in a manner which requires direct engagement with the target or its assets.

20. When used as part of a search through theharvester, what will be the effect of the `-n` flag?

A. A DNS brute-force search will be conducted for the domain name provided.

B. Identified hosts will be cross-referenced with the Shodan database.

C. A simple declaration of the domain or company name for which to conduct the search.

D. A reverse DNS query will be run for all discovered ranges.

☑ **D**. The `-n` flag in theharvester will result in a reverse DNS query being run for all discovered ranges.

☒ **A**, **B**, and **C** are incorrect. **A** is incorrect because a DNS brute-force search is the result of the `-c` flag. **B** is incorrect because a cross-reference with the Shodan database is the result of the `-h` flag. **C** is incorrect because a declaration of the domain or company name for which to conduct the search is expected after the `-d` flag.