CHAPTER 2

Reconnaissance: Information Gathering for the Ethical Hacker

This chapter includes questions from the following topics:

- Define active and passive footprinting
- Identify methods and procedures in information gathering
- Understand the use of social networking, search engines, and Google hacking in information gathering
- Understand the use of whois, ARIN, and nslookup in information gathering
- Describe DNS record types

Criminology (the study of the nature, causes, control, and prevention of criminal behavior) is a fascinating subject, and although we're concentrating on the virtual world in this book, it's amazing how much footprinting is done in the *physical* criminal world as well. Most of us have already heard a million times the standard things we're supposed to do to make our homes less desirable as a target for the bad guys. Things such as keeping the house well lit, installing timers on lights and TVs to make the house appear "lived in" all the time, and installing a good alarm system are so common in these discussions that we tend to nod off in boredom when a security expert starts talking about them. But did you know most common burglars prefer to work during the daytime, when it's most likely you're not at home at all? Did you know most don't give a rip about your alarm system because they plan on being inside for eight to ten minutes or less? And did you further know that most timer systems for lights don't change a thing in the bad guy's mind because there's usually *sound* associated with people being home?

For the sake of example, take an imaginary ride with me around my subdivision, and we'll try thinking like a criminal footprinting a neighborhood for targets. Maybe we'll start by just driving around the neighborhood to ascertain who the nosy neighbors are and what houses make the most promising opportunities. This house on our right is in a cul-de-sac and provides more privacy and less police patrol traffic than those on the main drag. Oh, what about that house over there? Yeah, it looks like the yard hasn't been mowed for a while, so maybe they aren't home—or they just don't pay as close attention to home details as the other homeowners do. The owners of that two-story over there have a dog, so we'll probably avoid that one. But look just there: that house has a giant box leaning against the garbage can for the brand-new 82-inch QLED TV the owner just purchased. We should probably write this address down for a closer look later. And the house across the pond there with the sliding glass door? It definitely has potential.

As fascinating as footprinting a building might seem, were you aware that *you*, as a person, could be footprinted in the physical world as well? According to several studies on the matter, criminals are good at sensing weakness based just on *the way you walk*. In one such study, 47 inmates at a maximum-security prison were surveyed, and the findings showed that social predators are very good at picking victims based on their gait, posture, and stride. The study provided the inmates with a film of 12 people (eight women and four men, some of whom had been attacked before) walking down a street and asked them to rate each person as a potential victim. The ratings were then compared against each person's actual history. Surprisingly (or maybe not so surprisingly), the people who the criminals picked as likely victims were usually the same ones who had been victimized in the past. Inmates described the men and women they saw as targets as “walking like an easy target... slow, with short strides.” What distinguished the likely victims from the rest of the pedestrians? Things such as posture, body language, pace, length of stride, and awareness of their environment. Nonverbal communication works wonderfully well, and a person’s level of self-confidence can be identified just by the style of walk. Walk with your head down at a slow or unorganized, meandering pace, and you’re screaming to the world you lack self-confidence. Walk fast, fluidly, and with a purpose, and you’re less likely to be a target.

I could go on and on here (I really like this subject and could chat about it forever), but this book is about the virtual world, and I’m prepping you to be an ethical hacker, not a policeman working a beat. This chapter is also all about reconnaissance and footprinting—in the virtual world—and is all about the methods and tools used to gather information about your targets before you even try to attack them.

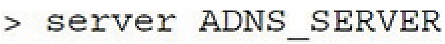
STUDY TIPS There will be plenty of questions from this particular segment of hacking, mainly because it’s so important to gather good intelligence before starting an attack. Sure, you can sometimes get lucky and strike quickly, but often, putting in the work during footprinting reaps the biggest rewards.

What will be the biggest area of focus you’ll see on your actual exam? A couple of versions ago, it was all things DNS, but now it's much more varied. You are just as likely to see questions on active versus passive reconnaissance as you are Google hacking, OS fingerprinting, and DNS subtleties. EC-Council has definitely broadened the horizons when it comes to recon and footprinting questions so, while I hate to say memorize everything, memorize everything.

Tips on the tricky questions here are the same as you'll hear me say in every other chapter—they're nit-picky, in-the-weeds, specific-knowledge questions designed to trip you up. Know your e-mail headers and DNS records, of course, but you'll also see questions on specific tools and how they act. And by all means start practicing your Google hacking right now—you'll definitely need it since most Google hacking questions will require you to know exact syntax.

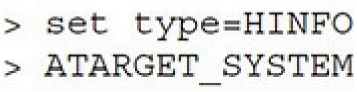
1. You are attempting to find out the operating system and CPU type of systems in your target organization. The DNS server you want to use for lookup is named ADNS_Server, and the target machine you want the information on is ATARGET_SYSTEM. Which of the following nslookup command series is the best choice for discovering this information? (The output of the commands is redacted.)

A.



```
> server ADNS_SERVER
```

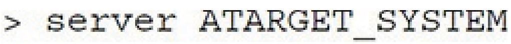
…



```
> set type=HINFO
> ATARGET_SYSTEM
```

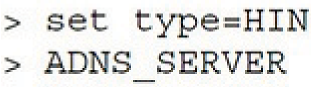
…

B.



```
> server ATARGET_SYSTEM
```

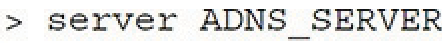
…



```
> set type=HINFO
> ADNS_SERVER
```

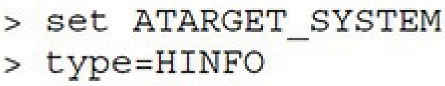
…

C.



```
 > server ADNS_SERVER
```

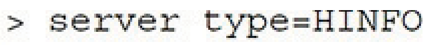
…



```
> set ATARGET_SYSTEM
> type=HINFO
```

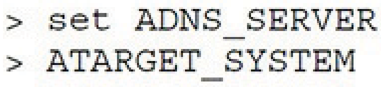
…

D.



```
> server type=HINFO
```

…



```
> set ADNS_SERVER
> ATARGET_SYSTEM
```

…

2. A pen test team member sends an e-mail to an address that she knows is not valid inside an organization. Which of the following is the best explanation for why she took this action?

A. To possibly gather information about internal hosts used in the organization’s e-mail system

B. To start a denial-of-service attack

C. To determine an e-mail administrator’s contact information

D. To gather information about how e-mail systems deal with invalidly addressed messages

3. From the partial e-mail header provided, which of the following represents the true originator of the e-mail message?

Return-path: <SOMEONE@anybiz.com>
Delivery-date: Tue, 12 Mar 2019 00:31:13 +0200
Received: from mailexchanger.anotherbiz.com([220.15.10.254])
by mailserver.anotherbiz.com running ExIM with esmtp
id xxxxxx-xxxxxx-xxx; Tue, 12 Mar 2019 01:39:23

```
+0200
Received: from mailserver.anybiz.com
([158.190.50.254] helo=mailserver.anybiz.com)
by mailexchanger.anotherbiz.com with esmtp id
xxxxxx-xxxxxx-xx
for USERJOE@anotherbiz.com; Tue, 12 Mar
2019 01:39:23 +0200
Received: from SOMEONEComputer
[217.88.53.154] (helo=[SOMEONEcomputer])
by mailserver.anybiz.com with esmtpa (Exim
x.xx)
(envelope-from <SOMEONE@anybiz.com) id
xxxxx-xxxxxx-xxxx
for USERJOE@anotherbiz.com; Mon, 11 Mar
2019 20:36:08 -0100
Message-ID: <xxxxxxxx.xxxxxxxx@anybiz.com>
Date: Mon, 11 Mar 2019 20:36:01 -0100
X-Mailer: Mail Client
From: SOMEONE Name
<SOMEONE@anybiz.com>
To: USERJOE Name
<USERJOE@anotherbiz.com>
Subject: Something to consider
...
```

A. 220.15.10.254

B. 158.190.50.254

C. 217.88.53.154

D. The e-mail header does not show this information.

4. You are looking for pages with the terms *CEH* and *V10* in their title. Which Google hack is the appropriate one?

A. inurl:CEHinurl:V10

B. allintitle:CEH V10

C. intitle:CEHinurl:V10

D. allinurl:CEH V10

5. You are on a Cisco router and want to identify the path a packet travels to a specific IP. Which of the following is the best command choice for this?

A. ping

B. ifconfig

C. tracert

D. traceroute

6. Which of the following activities are *not* considered passive footprinting? (Choose two.)

A. Dumpster diving

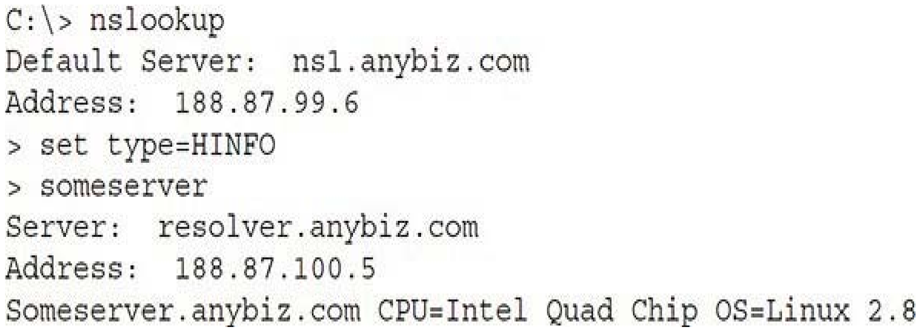
B. Reviewing financial sites for company information

C. Clicking links within the company's public website

D. Calling the company's help desk line

C. Employing passive sniffing

7. Examine the following command sequence:



```
C:\> nslookup
Default Server:  ns1.anybiz.com
Address:  188.87.99.6
> set type=HINFO
> someserver
Server:  resolver.anybiz.com
Address:  188.87.100.5
Someserver.anybiz.com CPU=Intel Quad Chip OS=Linux 2.8
```

Which of the following statements best describes the intent of the command sequence?

A. The operator is enumerating a system named someserver.

B. The operator is attempting DNS poisoning.

C. The operator is attempting a zone transfer.

D. The operator is attempting to find a name server.

8. An organization has a DNS server located in the DMZ and other DNS servers located on the intranet. What is this implementation commonly called?

A. Dynamic DNS

B. DNSSEC

C. Split DNS

D. Auto DNS

9. You are setting up DNS for your enterprise. Server A is both a web server and an FTP server. You want to advertise both services for this machine as name references your customers can use. Which DNS record type would you use to accomplish this?

   A. NS

   B. SOA

   C. MX

   D. PTR

   E. CNAME

10. A company has a public-facing web application. Its internal intranet-facing servers are separated and protected by a firewall. Which of the following choices would be helpful in protecting against unwanted enumeration?

    A. Allowing zone transfers to ANY

    B. Ensuring there are no A records for internal hosts on the public-facing name server

    C. Changing the preference number on all MX records to zero

    D. Not allowing any DNS query to the public-facing name server

11. An ethical hacker searches for IP ranges owned by the client, reads news articles, observes when bank

employees arrive and leave from work, searches the client’s job postings, and visits the client’s dumpster. Which of the following is a true statement?

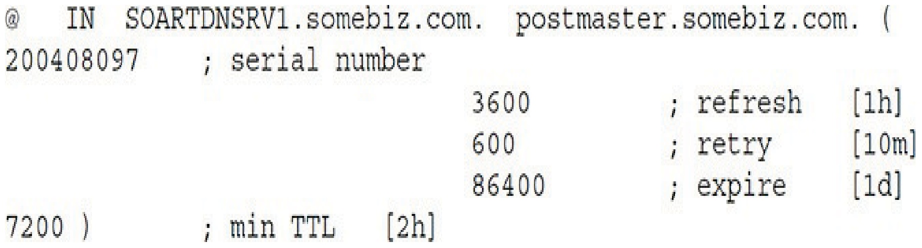
A. All of the actions are active footprinting.

B. All of the actions are passive footprinting.

C. The ethical hacker is in the system attack phase.

D. The ethical hacker is acting as a black-hat attacker.

12. Examine the following SOA record:



```
@   IN  SOARTDNSRV1.somebiz.com.  postmaster.somebiz.com. (
200408097    ; serial number
                               3600          ; refresh   [1h]
                               600           ; retry     [10m]
                               86400         ; expire    [1d]
7200 )        ; min TTL   [2h]
```

If a secondary server in the enterprise is unable to check in for a zone update within an hour, what happens to the zone copy on the secondary?

A. The zone copy is dumped.

B. The zone copy is unchanged.

C. The serial number of the zone copy is decremented.

D. The serial number of the zone copy is incremented.

13. Which protocol and port number combination is used by default for DNS zone transfers?

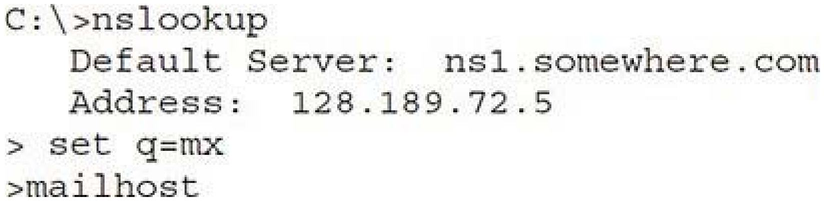
A. UDP 53

B. UDP 161

C. TCP 53

D. TCP 22

14. Examine the following command-line entry:



```
C:\>nslookup
   Default Server:  ns1.somewhere.com
   Address:  128.189.72.5
> set q=mx
>mailhost
```

Which statements are true regarding this command sequence? (Choose two.)

A. Nslookup is in noninteractive mode.

B. Nslookup is in interactive mode.

C. The output will show all mail servers in the zone somewhere.com.

D. The output will show all name servers in the zone somewhere.com.

15. Joe accesses the company website, www.anybusi.com, from his home computer and is presented with a defaced site containing disturbing images. He calls the IT department to report the website hack and is told they do not see any problem with the site—no files have been changed, and when accessed from their terminals (inside the company), the site appears normally. Joe connects over VPN into the company website and notices the site appears normally. Which of the following might explain the issue?

- **A.** DNS poisoning
- **B.** Route poisoning
- **C.** SQL injection
- **D.** ARP poisoning

16. One way to mitigate against DNS poisoning is to restrict or limit the amount of time records can stay in cache before they're updated. Which DNS record type allows you to set this restriction?

- **A.** NS
- **B.** PTR
- **C.** MX
- **D.** CNAME
- **E.** SOA

17. Which of the following may be a security concern for an organization?

- **A.** The internal network uses private IP addresses registered to an Active Directory–integrated DNS server.
- **B.** An external DNS server is Active Directory

integrated.

C. All external name resolution requests are accomplished by an ISP.

D. None of the above.

18. Which of the following is a good footprinting tool for discovering information on a publicly traded company's founding, history, and financial status?

A. SpiderFoot

B. EDGAR Database

C. Sam Spade

D. Pipl.com

19. What method does traceroute use to map routes traveled by a packet?

A. By carrying a hello packet in the payload, forcing the host to respond

B. By using DNS queries at each hop

C. By manipulating the Time-To-Live (TTL) parameter

D. By using ICMP Type 5, Code 0 packets

20. Brad is auditing an organization and is asked to provide suggestions on improving DNS security. Which of the following would be valid options to recommend? (Choose all that apply.)

A. Implementing a split-horizon operation

B. Restricting zone transfers

C. Obfuscating DNS by using the same server for other applications and functions

D. Blocking all access to the server on port 53

21. A zone file consists of which records? (Choose all that apply.)

A. PTR

B. MX

C. SN

D. SOA

E. DNS

F. A

G. AX

22. Within the OSRFramework, which tool verifies if a username/profile exists in up to 306 different platforms?

A. domainfy.py

B. mailfy.py

C. searchfy.py

D. usufy.py

23. A colleague enters the following into a Google search string:

```
intitle:intranet inurl:intranet
```

```
intext:"finance"
```

Which of the following statements is most correct concerning this attempt?

A. The search engine will not respond with any result because you cannot combine Google hacks in one line.

B. The search engine will respond with all pages having the word *intranet* in their title and *finance* in the URL.

C. The search engine will respond with all pages having the word *intranet* in the title and in the URL.

D. The search engine will respond with only those pages having the word *intranet* in the title and URL and with *finance* in the text.

24. Amanda works as senior security analyst and overhears a colleague discussing confidential corporate information being posted on an external website. When questioned on it, he claims about a month ago he tried random URLs on the company's website and found confidential information. Amanda visits the same URLs but finds nothing. Where can Amanda go to see past versions and pages of a website?

A. Search.com

B. Google cache

C. Pasthash.com

D. Archive.org

25. Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?

A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.

B. CSIRT provides a computer security surveillance service to supply the government with important intelligence information on individuals traveling abroad.

C. CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multinational corporations.

D. CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.

26. Your client's business is headquartered in Japan. Which regional registry would be the best place to look for footprinting information?

A. APNIC

B. RIPE

C. ASIANIC

D. ARIN

E. LACNIC

QUICK ANSWER KEY

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

20. A, B

21. A, B, D, F

22. D

23. D

24. D

25. A

26. A

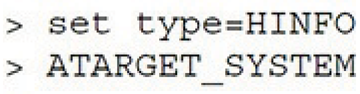
ANSWERS A

1. You are attempting to find out the operating system and CPU type of systems in your target organization. The DNS server you want to use for lookup is named ADNS_Server, and the target machine you want the information on is ATARGET_SYSTEM. Which of the following nslookup command series is the best choice for discovering this information? (The output of the commands is redacted.)

A.

```
> server ADNS_SERVER
```

…



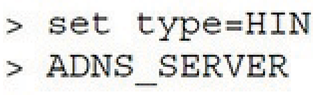
```
> set type=HINFO
> ATARGET_SYSTEM
```

…

B.

```
> server ATARGET_SYSTEM
```

…



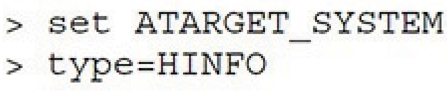
```
> set type=HINFO
> ADNS_SERVER
```

…

C.

```
 > server ADNS_SERVER
```

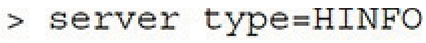
…



```
> set ATARGET_SYSTEM
> type=HINFO
```

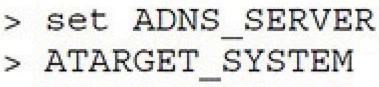
…

D.



```
> server type=HINFO
```

…



```
> set ADNS_SERVER
> ATARGET_SYSTEM
```

…

☑ **A.** This question gets you on two fronts. One regards knowledge on HINFO, and the other is nslookup use. First, the DNS record HINFO (per RFC 1035) is a resource type that identifies values for CPU type and operating system. Are you absolutely required to include an HINFO record for each host in your network? No, not at all. Should you? I'm sure there's some reason, somewhere and sometime, that adding HINFO makes sense, but I certainly can't think of one. In other words, this is a great record type to remember for your exam, but your chances of seeing it in use in the real world rank somewhere between seeing Lobster on the menu at McDonald's and catching a Leprechaun riding a unicorn through your backyard.

Nslookup syntax is the second portion of this question, and you'll definitely need to know it. The syntax for the tool is fairly simple:

```
nslookup [-options] {hostname | [-server]}
```

The command can be run as a single instance, providing information based on the options you choose, or you can run it in interactive mode, where the command runs as a tool, awaiting input from you. For example, on a Microsoft Windows machine, if you simply type **nslookup** at the prompt, you'll see a display showing your default DNS server and its associated IP address. From there, nslookup sits patiently, waiting for you to ask whatever you want (as an aside, this is known as *interactive mode*). Typing a question mark shows all the options and switches you have available.

☒ **B, C,** and **D** are incorrect because the syntax does not match.

2. A pen test team member sends an e-mail to an address that she knows is not valid inside an organization. Which of the following is the best explanation for why she took this action?

A. To possibly gather information about internal hosts used in the organization's e-mail system

B. To start a denial-of-service attack

C. To determine an e-mail administrator's contact information

D. To gather information about how e-mail systems deal with invalidly addressed messages

☑ **A.** The thought process behind this is a lot like banner grabbing or any of a hundred different forced-error situations in hacking: lots of information can be gleaned from responses to an error situation. A bogus internal address has the potential to provide more information about the internal servers used in the organization, including IP addresses and other pertinent details.

☒ **B** is incorrect because a bogus e-mail doesn't necessarily indicate the beginning of a DoS attack.

☒ **C** is incorrect because the e-mail administrator's contact information is not sent on invalid e-mail responses.

☒ **D** is incorrect because the pen tester would already know how systems deal with bogus e-mail addresses—what she wouldn't know is what servers inside this particular organization carry out those steps.

3. From the partial e-mail header provided, which of the following represents the true originator of the e-mail message?

Return-path: <SOMEONE@anybiz.com>

```
Delivery-date: Tue, 12 Mar 2019 00:31:13 +0200
Received: from
mailexchanger.anotherbiz.com([220.15.10.254])
by mailserver.anotherbiz.com running ExIM
with esmtp
id xxxxxx-xxxxxx-xxx; Tue, 12 Mar 2019 01:39:23
+0200
Received: from mailserver.anybiz.com
([158.190.50.254] helo=mailserver.anybiz.com)
by mailexchanger.anotherbiz.com with esmtp id
xxxxxx-xxxxxx-xx
for USERJOE@anotherbiz.com; Tue, 12 Mar
2019 01:39:23 +0200
Received: from SOMEONEComputer
[217.88.53.154] (helo=[SOMEONEcomputer])
by mailserver.anybiz.com with esmtpa (Exim
x.xx)
(envelope-from <SOMEONE@anybiz.com) id
xxxxx-xxxxxx-xxxx
for USERJOE@anotherbiz.com; Mon, 11 Mar
2019 20:36:08 -0100
Message-ID: <xxxxxxxx.xxxxxxxx@anybiz.com>
Date: Mon, 11 Mar 2019 20:36:01 -0100
X-Mailer: Mail Client
From: SOMEONE Name
<SOMEONE@anybiz.com>
To: USERJOE Name
```

```
<USERJOE@anotherbiz.com>
Subject: Something to consider
...
```

A. 220.15.10.254

B. 158.190.50.254

C. 217.88.53.154

D. The e-mail header does not show this information.

☑ **C.** E-mail headers are packed with information showing the entire route the message has taken, and I can guarantee you'll see at least one question on your exam about them. You'll most likely be asked to identify the true originator—the machine (person) who sent the e-mail in the first place (even though in the real world with proxies and whatnot to hide behind, it may be impossible). This is clearly shown in line 9: Received: from SOMEONEComputer [217.88.53.154] (helo= [SOMEONEcomputer]). But don't just study and rely on that one section. Watch the entire trek the message takes and make note of the IPs along the way.

☒ **A** and **B** are incorrect because these IPs do not represent the true originator of the message. They show e-mail servers that are passing/handling the message.

☒ **D** is incorrect because the e-mail header definitely shows the true originator.

4. You are looking for pages with the terms *CEH* and *V10* in their title. Which Google hack is the appropriate one?

A. inurl:CEHinurl:V10

B. allintitle:CEH V10

C. intitle:CEHinurl:V10

D. allinurl:CEH V10

☑ **B.** The Google search operator allintitle searches for pages that contain the string, or strings, you specify. It also allows for the combination of strings in the title, so you can search for more than one term within the title of a page.

☒ **A** is incorrect because the operator inurl looks only in the URL of the site, not the page title. In this example, the search might bring you to a page like this: http://anyplace.com/apache_Version/pdfs.html.

☒ **C** is incorrect because the inurl operator isn't looking in the page title. Yes, you can combine operators, but these two just won't get this job done.

☒ **D** is incorrect because allinurl does not look at page titles; it's concerned only with the URL itself. As with the title searches, this allinurl operator allows you to combine search strings.

5. You are on a Cisco router and want to identify the path a packet travels to a specific IP. Which of the following is the best command choice for this?

A. ping

B. ifconfig

C. tracert

D. traceroute

☑ **D.** You probably knew, right up front, this was a traceroute question, but the kicker comes when deciding *which* traceroute command to use. Traceroute, of course, uses ICMP packets and the TTL (Time-To-Live) value to map out a path between originator and destination. The first packet sent uses a TTL of 1, to show the first hop. The next packet sets it to 2, and so on, and so on, until the destination is found. Each ICMP response provides information on the current hop (unless ICMP is being filtered). On a Windows machine, you'd use the command *tracert*. On Linux (and Cisco for that matter), you'd use *traceroute*.

☒ **A** is incorrect because the ping command simply tests for connectivity and to see if the system is "live." ICMP Echo Request packets are sent to the destination, and ICMP Echo Reply packets are returned with information on the system. Of course, ICMP is often filtered at the host (or firewall) level, so a negative ping response doesn't necessarily mean the system is down.

☒ **B** is incorrect because the ifconfig command is used in Linux systems to display information about the system's network interfaces. Ifconfig allows for configuring, controlling, and querying TCP/IP network interface parameters—for example, setting the IP address and subnet mask (netmask) on a NIC.

☒ **C** is incorrect because the tracert command will work on a Windows system, but not on a Cisco device.

6. Which of the following activities are *not* considered passive footprinting? (Choose two.)

A. Dumpster diving

B. Reviewing financial sites for company information

C. Clicking links within the company's public website

D. Calling the company's help desk line

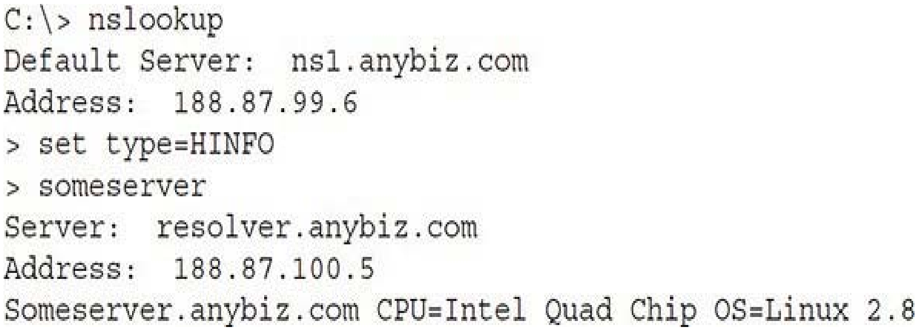
E. Employing passive sniffing

☑ **D, E.** This one may be a little tricky, but only because we live and work in the real world and this is an exam question. EC-Council has several questionable takes on things regarding real-world application and what they say you should remember for your exam, and this is one of those examples. Just remember ECC wants you to know active and passive footprinting can be defined by two things: what you touch and how much discovery risk you put yourself in. Social engineering in and of itself is not all passive or active in nature. In the case of dumpster diving, it's also considered passive (despite the real-world risk of discovery and the action you have to take to pull it off) according to ECC.

However, pick up a phone and call someone inside the company or talk to people in the parking lot, and you've exposed yourself to discovery and are now practicing active footprinting. As far as “passive” sniffing goes, sniffing isn’t a footprinting action at all. The term “passive sniffing” concerns the act of simply plugging in and watching what comes by, without any packet interjection or other action required on your part.

☒ **A, B,** and **C** are incorrect because these are all examples of passive reconnaissance. Other examples might include checking out DNS records (DNS is publicly available and, per ECC, you can passively footprint an organization by using freely available DNS records) and checking job listings for the company.

7. Examine the following command sequence:



```
C:\> nslookup
Default Server:  ns1.anybiz.com
Address:  188.87.99.6
> set type=HINFO
> someserver
Server:  resolver.anybiz.com
Address:  188.87.100.5
Someserver.anybiz.com CPU=Intel Quad Chip OS=Linux 2.8
```

Which of the following statements best describes the intent of the command sequence?

A. The operator is enumerating a system named someserver.

B. The operator is attempting DNS poisoning.

C. The operator is attempting a zone transfer.

D. The operator is attempting to find a name server.

☑ **A.** The HINFO record type is one of those really great ideas that was designed to make life easier on everyone yet turned out to be a horrible idea. Defined in RFC 1035, Host Information (HINFO) DNS records were originally intended to provide the type of computer and operating system a host uses (back in the day, you could also put things like room numbers and other descriptions in the record). However, to avoid publicly advertising that information (for obvious reasons), this record type simply is not used much anymore. And if you find one on a public-facing machine, it's a sure sign of incompetence on the part of the server administrators. In this example, the type is set to HINFO, and a machine name—someserver—is provided. The attacker can use the information contained in the record as an enumeration source.

☒ **B** is incorrect because DNS poisoning is not carried out this way. In this command sequence, the operator is asking for information, not pushing up false entries to a name server.

☒ **C** is incorrect because this is not how nslookup is used to perform a zone transfer. To do that, you would use the **set type=any** command and then **ls -d anybiz.com**. You’ll more than likely see that on your exam, too.

☒ **D** is incorrect because checking for name servers in the domain would require the **set type=NS** command.

8. An organization has a DNS server located in the DMZ and other DNS servers located on the intranet. What is this implementation commonly called?

A. Dynamic DNS

B. DNSSEC

C. Split DNS

D. Auto DNS

☑ **C.** The idea behind split DNS is pretty simple: create two zones for the same domain, with one just for the internal network while the other is used by any external networks. Internal hosts are directed to the internal domain name server. Separating the domain servers greatly restricts the footprinting an attacker can perform from the outside.

☒ **A** is incorrect because dynamic DNS doesn’t work this way. In “regular” DNS, a name is tied to a static IP address; however, for any number of reasons, a hosted device may need to change its IP address often. In dynamic DNS, a service provider uses a program that runs on the system, contacting the DNS service each time the IP address changes and subsequently updating the DNS database to reflect the change in IP address. That way, even though a domain name’s IP address changes, users don’t have to do anything out of the ordinary to continue service—the dynamic DNS service will ensure they’re pointed in the right direction.

☒ **B** is incorrect because Domain Name System Security Extensions (DNSSEC) is a suite of IETF specifications for securing certain kinds of information provided by DNS. Dan Kaminsky made DNS vulnerabilities widely known back around 2010, and most service providers roll this out to ensure that DNS results are cryptographically protected. It’s designed to provide origin authentication of DNS data and data integrity.

☒ **D** is incorrect because this term simply doesn’t exist. It’s here purely as a distractor.

9. You are setting up DNS for your enterprise. Server A is both a web server and an FTP server. You want to advertise both services for this machine as name references your customers can use. Which DNS record type would you use to accomplish this?

A. NS

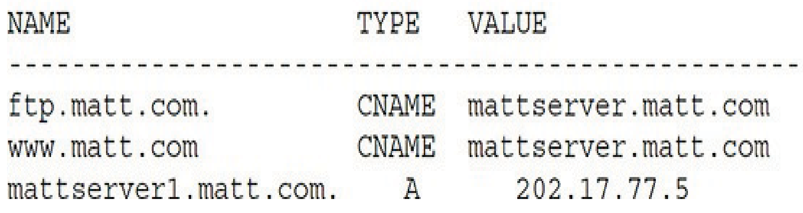
B. SOA

C. MX

D. PTR

E. CNAME

☑ **E.** We all know—or should know by now—that a hostname can be mapped to an IP using an A record within DNS. CNAME records provide for aliases within the zone on that name. For instance, your server might be named mattserver1.matt.com. A sample DNS zone entry to provide HTTP and FTP access might look like this:



```
NAME                  TYPE   VALUE
--------------------------------------------------
ftp.matt.com.         CNAME  mattserver.matt.com
www.matt.com          CNAME  mattserver.matt.com
mattserver1.matt.com.    A      202.17.77.5
```

☒ **A** is incorrect because a Name Server (NS) record shows the name servers within your zone. These servers are the ones that respond to your client’s requests for name resolution.

☒ **B** is incorrect because the Start of Authority (SOA) entry identifies the primary name server for the zone. The SOA record contains the hostname of the server responsible for all DNS records within the namespace, as well as the basic properties of the domain.

☒ **C** is incorrect because the Mail Exchange (MX) record identifies the e-mail servers within your domain.

☒ **D** is incorrect because a Pointer (PTR) record works the opposite to an A record. The pointer maps an IP address to a hostname and is generally used for reverse lookups.

10. A company has a public-facing web application. Its internal intranet-facing servers are separated and protected by a firewall. Which of the following choices would be helpful in protecting against unwanted enumeration?

A. Allowing zone transfers to ANY

B. Ensuring there are no A records for internal hosts on the public-facing name server

C. Changing the preference number on all MX records to zero

D. Not allowing any DNS query to the public-facing name server

☑ **B.** If your company has a publicly facing website, it follows that a name server somewhere has to answer lookups in order for your customers to find the site. That name server, however, does not need to provide lookup information to internal machines. Of the choices provided, as silly as it seems to point out, ensuring there are no A records (those used to map hostnames to an IP address) on the external name server is a good start.

☒ **A** is incorrect because allowing a zone transfer to anyone asking for it is just plain dumb. It may or may not help an attacker enumerate your internal network (maybe you don't have anything in there to worry about), but it's just a horrendously bad idea.

☒ **C** is incorrect because changing the preference number on an MX record doesn't have a thing to do with enumeration. The preference number (a lower number means first used) determines only which server handles e-mail first.

☒ **D** is incorrect because if your customers can't query for the IP associated with the hostname, how are they supposed to find your website?

11. An ethical hacker searches for IP ranges owned by the client, reads news articles, observes when bank employees arrive and leave from work, searches the client's job postings, and visits the client's dumpster. Which of the following is a true statement?

A. All of the actions are active footprinting.

B. All of the actions are passive footprinting.

C. The ethical hacker is in the system attack phase.

D. The ethical hacker is acting as a black-hat attacker.

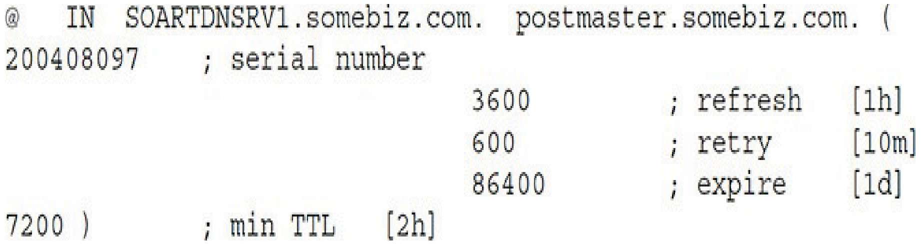
☑ **B.** I know, I know—I can hear you professional test takers screaming at me already: "Any answer that starts with 'all' can be eliminated!" And, normally, I'd agree with you, but it's precisely why I added it here. Each and every example in this question happens to be an example of passive footprinting.

☒ **A** is incorrect because none of these actions are active footprinting. An *active footprinting* effort is one that requires the attacker to touch the device, network, or resource, whereas *passive footprinting* refers to measures to collect information from publicly accessible sources.

☒ **C** is incorrect because the attacker is in the reconnaissance phase.

☒ **D** is incorrect because there is no indication which “hat” the attacker is acting as, although as an ethical hacker, it should be as a white hat.

12. Examine the following SOA record:



```
@   IN  SOARTDNSRV1.somebiz.com.  postmaster.somebiz.com. (
200408097    ; serial number
                               3600         ; refresh   [1h]
                               600          ; retry     [10m]
                               86400        ; expire    [1d]
7200 )       ; min TTL   [2h]
```

If a secondary server in the enterprise is unable to check in for a zone update within an hour, what happens to the zone copy on the secondary?

A. The zone copy is dumped.

B. The zone copy is unchanged.

C. The serial number of the zone copy is decremented.

D. The serial number of the zone copy is incremented.

☑ **B.** You will definitely see questions about the SOA record. In this question, the key portion you're looking for is the TTL (Time-To-Live) value at the bottom, which is currently two hours (7200 seconds). This sets the time a secondary server has to verify its records are good. If it can't check in, this TTL for zone records will expire, and they'll all be dumped. Considering, though, this TTL is set to two hours and the question states it has been only one hour since update, the zone copy on the secondary will remain unchanged.

☒ **A** is incorrect because the secondary is still well within its window for verifying the zone copy it holds. It dumps the records only when TTL is exceeded.

☒ **C** is incorrect because, first, serial numbers are never decremented; they're always incremented. Second, the serial number of the zone copy is changed only when a connection to the primary occurs and a copy is updated.

☒ **D** is incorrect because while serial numbers are incremented on changes (the secondary copies the number from the primary's copy when transferring records), the serial number of the zone copy is changed only when a connection to the primary occurs and a copy is updated. That has not occurred here.

13. Which protocol and port number combination is used by default for DNS zone transfers?

A. UDP 53

B. UDP 161

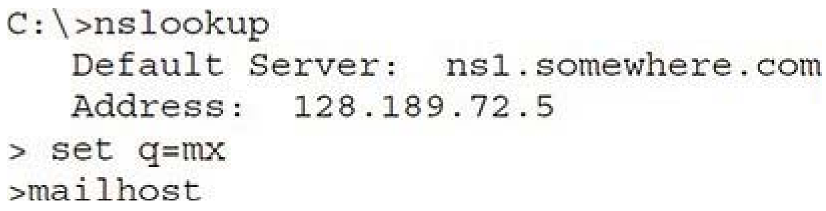
C. TCP 53

D. TCP 22

☑ **C.** TCP 53 is the default protocol and port number for zone transfers. DNS actually uses both TCP and UDP to get its job done, and if you think about what it's doing, they make sense in particular circumstances. A name resolution request and reply? Small and quick, so use port 53 on UDP. A zone transfer, which could potentially be large and requires some insurance it all gets there? Port 53 on TCP is the answer.

☒ **A, B,** and **D** are incorrect because they do not represent the default port and protocol combination for a zone transfer.

14. Examine the following command-line entry:



```
C:\>nslookup
   Default Server:  ns1.somewhere.com
   Address:  128.189.72.5
> set q=mx
>mailhost
```

Which statements are true regarding this command sequence? (Choose two.)

A. Nslookup is in noninteractive mode.

B. Nslookup is in interactive mode.

C. The output will show all mail servers in the zone somewhere.com.

D. The output will show all name servers in the zone somewhere.com.

☑ **B, C.** Nslookup runs in one of two modes—interactive and noninteractive. Noninteractive mode is simply the use of the command followed by an output. For example, **nslookup www.google.com** will return the IP address your server can find for Google. Interactive mode is started by simply typing **nslookup** and pressing ENTER. Your default server name will display, along with its IP address, and a caret (>) will await entry of your next command. In this scenario, we've entered interactive mode and set the type to MX, which we all know means "Please provide me with all the mail exchange servers you know about."

☒ **A** is incorrect because we are definitely in interactive mode.

☒ **D** is incorrect because type was set to MX, not NS.

15. Joe accesses the company website, www.anybusi.com, from his home computer and is presented with a defaced site containing disturbing images. He calls the IT department to report the website hack and is told they do not see any problem with the site—no files have been changed, and when accessed from their terminals (inside the company), the site appears normally. Joe connects over VPN into the company website and notices the site appears normally. Which of the following might explain the issue?

A. DNS poisoning

B. Route poisoning

C. SQL injection

D. ARP poisoning

☑ **A.** DNS poisoning makes the most sense here. In many cases (such as mine right here in my own work-from-home office), a VPN connection back to the company forces you to use the company DNS instead of your local resolution. In this example, Joe's connection from home uses a different DNS server for lookups than that of the business network. It's entirely possible someone has changed the cache entries in his local server to point to a different IP than the one hosting the real website—one that the hackers have set up to provide the defaced version. The fact the web files haven't changed and it seems to be displaying just fine from inside the network also bears this out. If it turns out Joe's DNS modification is the only one in place, there is a strong likelihood that Joe is being specifically targeted for exploitation—something Joe should take very seriously. Lastly, the HOSTS and LMHOSTS files can also play a big role in this kind of scenario—however, if an attacker already has that kind of access to Joe's computer, he has bigger problems than the corporate website.

☒ **B** is incorrect because route poisoning has nothing to do with this. Route poisoning is used in distance vector routing protocols to prevent route loops in routing tables.

☒ **C** is incorrect because although SQL injection is, indeed, a hacking attack, it's not relevant here. The fact the website files remain intact and unchanged prove that access to the site through an SQL weakness isn’t what occurred here.

☒ **D** is incorrect because ARP poisoning is relevant inside a particular subnet, not outside it (granted, you can have ARP forwarded by a router configured to do so, but it simply isn’t the case for this question). ARP poisoning will redirect a request from one machine to another inside the same subnet and has little to do with the scenario described here.

16. One way to mitigate against DNS poisoning is to restrict or limit the amount of time records can stay in cache before they’re updated. Which DNS record type allows you to set this restriction?

A. NS

B. PTR

C. MX

D. CNAME

E. SOA

☑ **E.** The SOA record holds all sorts of information, and when it comes to DNS poisoning, the TTL is of primary interest. The shorter the TTL, the less time records are held in cache. While it won't prevent DNS poisoning altogether, it can limit the problems a successful cache poisoning attack causes.

☒ **A** is incorrect because an NS record shows the name servers found in the domain.

☒ **B** is incorrect because a PTR record provides for reverse lookup capability—an IP-address-to-hostname mapping.

☒ **C** is incorrect because an MX record shows the mail exchange servers in the zone.

☒ **D** is incorrect because a CNAME record is used to provide alias entries for your zone (usually for multiple services or sites on one IP address).

17. Which of the following may be a security concern for an organization?

A. The internal network uses private IP addresses registered to an Active Directory–integrated DNS server.

B. An external DNS server is Active Directory integrated.

C. All external name resolution requests are accomplished by an ISP.

D. None of the above.

☑ **B.** If you have a Windows Active Directory (AD) network, having AD-integrated DNS servers has some great advantages. For example (and directly from Microsoft, I might add), "with directory-integrated storage, dynamic updates to DNS are conducted based upon a multimaster update model. In this model, any authoritative DNS server, such as a domain controller running a DNS server, is designated as a primary source for the zone. Because the master copy of the zone is maintained in the Active Directory database, which is fully replicated to all domain controllers, the zone can be updated by the DNS servers operating at any domain controller for the domain." Zones are also replicated and synchronized to new domain controllers automatically whenever a new one is added to an Active Directory domain, and directory replication is faster and more efficient than standard DNS replication. But having an Active Directory server facing externally is a horrible idea.

☒ **A** is incorrect because having AD-integrated DNS servers inside your network, with all private IP addresses, is just fine. Actually, it's a pretty good idea if you think about it for a bit.

☒ **C** is incorrect because having an external ISP answer all name resolution requests for your public-facing servers isn't a bad idea at all. Even if the ISP's DNS is subject to attack, nothing is there but the public-facing hosts anyway.

☒ **D** is incorrect because there is a correct answer provided.

18. Which of the following is a good footprinting tool for discovering information on a publicly traded company's founding, history, and financial status?

A. SpiderFoot

B. EDGAR Database

C. Sam Spade

D. Pipl.com

☑ **B.** The EDGAR Database —https://www.sec.gov/edgar.shtml —holds various competitive intelligence information on businesses and is an old favorite of EC-Council. Per the website, "All companies, foreign and domestic, are required to file registration statements, periodic reports, and other forms electronically through EDGAR. Anyone can access and download this information for free. Here you'll find links to a complete list of filings available through EDGAR and instructions for searching the EDGAR database." Finally, one more note on EDGAR and the SEC: They have purview only over publicly traded companies. Privately held companies are not regulated or obligated to put information in EDGAR. Additionally, even publicly traded companies might not provide information about privately owned subsidiaries, so be careful and diligent.

☒ **A** is incorrect because SpiderFoot is a free, open source, domain footprinting tool. According to the site, "it will scrape the websites on that domain, as well as search Google, Netcraft, Whois and DNS to build up information."

☒ **C** is incorrect because Sam Spade is a DNS footprinting tool.

☒ **D** is incorrect because pipl.com is a site used for "people search." For footprinting, pipl.com can use so-called "deep web searching" for loads of information you can use. The following is from the site: "Also known as 'invisible web,' the term 'deep web' refers to a vast repository of underlying content, such as documents in online databases that general-purpose web crawlers cannot reach. The deep web content is estimated at 500 times that of the surface web, yet has remained mostly untapped due to the limitations of traditional search engines.”

19. What method does traceroute use to map routes traveled by a packet?

A. By carrying a hello packet in the payload, forcing the host to respond

B. By using DNS queries at each hop

C. By manipulating the Time-To-Live (TTL) parameter

D. By using ICMP Type 5, Code 0 packets

☑ **C.** Traceroute (at least on Windows machines) tracks a packet across the Internet by incrementing the TTL on each packet it sends by one after each hop is hit and returns, ensuring the response comes back explicitly from that hop and returns its name and IP address. This provides route path and transit times. It accomplishes this by using ICMP ECHO packets to report information on each “hop” (router) from the source to destination. As an aside, Linux machines use a series of UDP packets by default to carry out the same function in traceroute.

☒ **A** is incorrect because ICMP simply doesn’t work that way. A hello packet is generally used between clients and servers as a check-in/health mechanism, not a route-tracing method.

☒ **B** is incorrect because a DNS lookup at each hop is pointless and does you no good. DNS isn’t for route tracing; it’s for matching hostnames and IP addresses.

☒ **D** is incorrect because an ICMP Type 5, Code 0 packet is all about message redirection and not about a ping request (Type 8).

20. Brad is auditing an organization and is asked to provide suggestions on improving DNS security. Which of the following would be valid options to recommend? (Choose all that apply.)

A. Implementing a split-horizon operation

B. Restricting zone transfers

C. Obfuscating DNS by using the same server for other applications and functions

D. Blocking all access to the server on port 53

☑ **A, B.** Split-horizon DNS (also known as split-view or split DNS) is a method of providing different answers to DNS queries based on the source address of the DNS request. It can be accomplished with hardware or software solutions and provides one more step of separation between you and the bad guys. Restricting zone transfers to only those systems you desire to have them is always a good idea. If you leave it open for anyone to grab, you're just asking for trouble. DNSSEC should also be included, but isn't an option listed.

☒ **C** is incorrect because you generally should not put DNS services on a machine performing other tasks or applications. Does it happen in the real world? Sure it does, and just like it's not too far-fetched to find a stray Windows 2000 machine in any given organization's network, it's probably more common than we'd like to guess.

☒ **D** is incorrect because restricting all port 53 access to the server means it's not acting as a DNS server anymore: no one can query for name lookups, and no zone transfers are going to happen. I guess in some weird way the DNS side of it is *really* secure, but its functionality has dropped to nothing.

21. A zone file consists of which records? (Choose all that apply.)

A. PTR

B. MX

C. SN

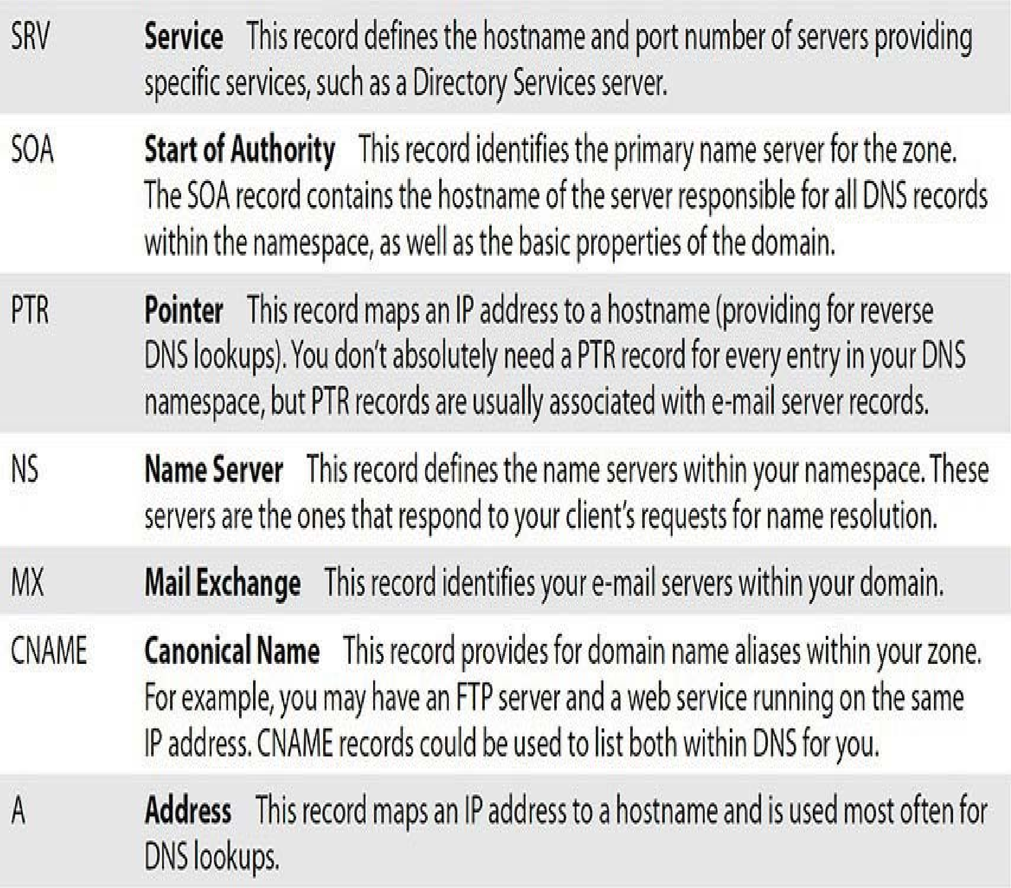
D. SOA

E. DNS

F. A

G. AX

☑ **A, B, D, F.** A zone file contains a list of all the resource records in the namespace zone. Valid resource records are as follows:



SRV	**Service** This record defines the hostname and port number of servers providing specific services, such as a Directory Services server.
SOA	**Start of Authority** This record identifies the primary name server for the zone. The SOA record contains the hostname of the server responsible for all DNS records within the namespace, as well as the basic properties of the domain.
PTR	**Pointer** This record maps an IP address to a hostname (providing for reverse DNS lookups). You don't absolutely need a PTR record for every entry in your DNS namespace, but PTR records are usually associated with e-mail server records.
NS	**Name Server** This record defines the name servers within your namespace. These servers are the ones that respond to your client's requests for name resolution.
MX	**Mail Exchange** This record identifies your e-mail servers within your domain.
CNAME	**Canonical Name** This record provides for domain name aliases within your zone. For example, you may have an FTP server and a web service running on the same IP address. CNAME records could be used to list both within DNS for you.
A	**Address** This record maps an IP address to a hostname and is used most often for DNS lookups.

☒ **C, E,** and **G** are incorrect because they are not valid DNS resource records.

22. Within the OSRFramework, which tool verifies if a username/profile exists in up to 306 different platforms?

A. domainfy.py

B. mailfy.py

C. searchfy.py

D. usufy.py

☑ **D.** The OSRFramework

(https://github.com/i3visio/osrframework) is an open source research framework in Python that helps you in the task of user profiling by making use of different open source intelligence (OSINT) tools. The framework design itself is reminiscent of the Metasploit framework. It also has a web-based GUI that does the work for you if you like to work without the command line. In other words, it's a set of libraries used to perform OSINT tasks, helping you gather more, and more accurate, data using multiple applications in one easy-to-use package. Usufy.py is but one of the tools in the framework, and it verifies if a username/profile exists in up to 306 different platforms.

☒ **A** is incorrect because this tool verifies the existence of a given domain (per the site, in up to 1567 different registries).

☒ **B** is incorrect because this tool checks if a username (e-mail) has been registered in *e-mail* providers.

☒ **C** is incorrect because this tool looks for *profiles* using *full names and other info* in up to seven platforms. As an aside, ECC words this differently by saying the tool queries the

OSRFramework platform itself.

23. A colleague enters the following into a Google search string:

```
intitle:intranet inurl:intranet
intext:"finance"
```

Which of the following statements is most correct concerning this attempt?

A. The search engine will not respond with any result because you cannot combine Google hacks in one line.

B. The search engine will respond with all pages having the word *intranet* in their title and *finance* in the URL.

C. The search engine will respond with all pages having the word *intranet* in the title and in the URL.

D. The search engine will respond with only those pages having the word *intranet* in the title and URL and with *finance* in the text.

☑ **D.** This is a great Google hack that's listed on several websites providing Google hacking examples. Think about what you're looking for here—an internal page (*intranet* in title and URL) possibly containing finance data. Don't you think that would be valuable? This example shows the beauty of combining Google hacks to really burrow down to what you want to grab. Granted, an intranet being available from the Internet, indexed by Google and open enough for you to touch it, is unlikely, but these are questions concerning syntax, not reality.

☒ **A** is incorrect because Google hack operators *can* be combined. In fact, once you get used to them, you'll spend more time combining them to narrow the focus of an attack than launching them one by one.

☒ **B** is incorrect because the operator does not say to look for *finance* in the URL. It specifically states that should be looked for in the text of the page.

☒ **C** is incorrect because there is more to the operation string than just *intranet* in the URL and title. Don't just skim over the **intext:"finance"** operator—it makes Answer D more correct.

24. Amanda works as senior security analyst and overhears a colleague discussing confidential corporate information being posted on an external website. When questioned on it, he claims about a month ago he tried random URLs on the company's website and found confidential information. Amanda visits the same URLs but finds nothing. Where can Amanda go to see past versions and pages of a website?

A. Search.com

B. Google cache

C. Pasthash.com

D. Archive.org

☑ **D.** The Internet Archive (http://archive.org) is a nonprofit organization "dedicated to build an Internet library. Its purposes include offering permanent access for researchers, historians, scholars, people with disabilities, and the general public to historical collections that exist in digital format." The good-old Wayback Machine has been used for a long time to pull up old copies of websites, for good and maybe not-so-good purposes. Archive.org includes "snapshots of the World Wide Web," which are archived copies of pages taken at various points in time dating back to 1996. As an additional note, Archive.org is only going to pull and store pages that were linked, shared, or commonly available, so don't assume every page ever put up by anyone anywhere will always be available.

- ☒ **A** is incorrect because Search.com is simply another search engine at your disposal. It does not hold archived copies.

- ☒ **B** is incorrect because Google cache holds a copy of the site only from the latest “crawl”—usually nothing older than a couple to a few days.

- ☒ **C** is incorrect because, as far as I know, Pasthash.com doesn’t even exist.

25. Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?

A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.

B. CSIRT provides a computer security surveillance service to supply the government with important intelligence information on individuals traveling abroad.

C. CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multinational corporations.

D. CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.

☑ **A.** EC-Council *loves* CSIRT, and I promise you'll see it mentioned somewhere on the exam. Per its website (www.csirt.org/), the Computer Security Incident Response Team (CSIRT) "provides 24x7 Computer Security Incident Response Services to any user, company, government agency or organization. CSIRT provides a reliable and trusted single point of contact for reporting computer security incidents worldwide. CSIRT provides the means for reporting incidents and for disseminating important incident-related information." A privately held company that started in 2001, CSIRT seeks "to raise awareness among its customers of computer security issues, and provides information for secure protection of critical computing infrastructure and equipment against potential organized computer attacks."

☒ **B, C,** and **D** are incorrect because these statements do not match CSIRT's purpose or actions.

26. Your client's business is headquartered in Japan.

Which regional registry would be the best place to look for footprinting information?

A. APNIC

B. RIPE

C. ASIANIC

D. ARIN

E. LACNIC

☑ **A.** This one is easy as pie and should be a freebie if you see it on the test. There are five regional Internet registries that provide overall management of the public IP address space within a given geographic region. APNIC handles the Asia and Pacific realms.

☒ **B** is incorrect because RIPE handles Europe, Middle East, and parts of Central Asia/Northern Africa. If you're wondering, the name is French and stands for Réseaux IP Européens.

☒ **C** is incorrect because ASIANIC is not a regional registry. It's purely a distractor here.

☒ **D** is incorrect because the ARIN service region includes Canada, many Caribbean and North Atlantic islands, and the United States. Caribbean islands falling under ARIN include Puerto Rico, the Bahamas, Antigua, American and British Virgin Islands, Turks and Caicos Islands, and the Cayman Islands (among others).

☒ **E** is incorrect because LACNIC handles Latin America and parts of the Caribbean. It stands for Latin America and Caribbean Network Information Center. LACNIC coverage includes most of South America, Guatemala, French Guiana, Dominican Republic, and Cuba (among others). Exam takers most often get this one and ARIN confused.