## QUESTIONS

1. The result of a whois search on a target is listed here:

```
Registrant:
      AnyBusiness Inc.
      1377 somewhere street
New York, NY 10013
      US
Phone: +13219667786
      Email: noemailhere@anybus.com

   Domain Name: anybusiness.com
      Created on..............: Mon, Jul 07, 1997
      Expires on..............: Sat, Jul 06, 2013
      Record last updated on..: Mon, Jul 02, 2012

    Administrative Contact:
      anybusiness.com
      P. O. Box 8799 615 N. Riverside Dr
      Somewhere, FL 32903
      US
      Phone: +1.3215550587
      Email: admin@anybus.com

   Technical  Contact:
      Mark Sensei
      187 Someplace drive
      Indialantic, FL 32903
      US
      Phone: +1.3215550879
      Email: M.sensei@gmail.com

DNS Servers:
      ns2.anybus.com
      ns1.anybus.com
```

   Which of the following is a true statement regarding this output?

   **A.** Anybusiness.com was registered using GoDaddy.com.

   **B.** The technical contact for this website may have entered personal information at registration.

   **C.** There is no information within this output useful for a zone transfer.

   **D.** The administrative and technical contacts are the same.

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 invalid 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: Wed, 13 Apr 2011 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; Wed, 13 Apr 2011 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; Wed, 13 Apr 2011 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; Tue, 12 Apr 2011 20:36:08 -0100
Message-ID: <xxxxxxxx.xxxxxxxx@anybiz.com>
Date: Tue, 12 Apr 2011 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 files with the terms *CEH* and *V8* in their titles. Which Google hack is the appropriate one?

A. inurl:CEHinurl:V7

B. allintitle:CEH V7

C. intitle:CEHinurl:V7

D. allinurl:CEH V7

5. You've just kicked off a penetration test against a target organization and have decided to perform a little passive footprinting. One of the first sites you visit is a job board, where the company has listed various openings. What is the primary useful footprinting information to be gained through this particular search?
   - **A.** Insight into the HR processes of the company
   - **B.** Insight into the operating systems, hardware, and applications in use
   - **C.** Insight into corporate security policy
   - **D.** None of the above
6. Which of the following activities is not considered passive footprinting?
   - **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
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 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. You are footprinting information for a pen test. Social engineering is part of your reconnaissance efforts, and some of it will be active in nature. You take steps to ensure that if the social engineering efforts are discovered at this early stage, any trace efforts point to another organization. Which of the following terms best describes what you are participating in?
   - **A.** Anonymous footprinting
   - **B.** Pseudonymous footprinting
   - **C.** Passive footprinting
   - **D.** Redirective footprinting

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 publicly 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. Within the DNS system a primary server (SOA) holds and maintains all records for the zone. Secondary servers will periodically ask the primary if there have been any updates, and if updates have occurred, they will ask for a zone transfer to update their own copies. Under what conditions will the secondary name server request a zone transfer from a primary?

   **A.** When the primary SOA record serial number is higher than the secondary's

   **B.** When the secondary SOA record serial number is higher than the primary's

   **C.** Only when the secondary reboots or restarts services

   **D.** Only when manually prompted to do so

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 two 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 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. 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]
```

How long will the secondary server wait before asking for an update to the zone file?

**A.** 1 hour

**B.** 2 hours

**C.** 10 minutes

**D.** 1 day

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

```
intitle:intranetinurl:intranet+intext:"human resources"
```

Which of the following 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 *human resources* 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 *human resources* 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 a 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