Unit 9 Quiz

**Question 1 (1 point)**

In the past 24 hours, several employees have called the help desk to question the validity of e-mails from the organization's official credit card provider. The e-mails cite a possible security breach in the financial institution's records and ask recipients to follow a link to the institution's Web site and create a new password, after identifying themselves by providing their existing passwords and account information.

What attack does this scenario describe?

|  |  |
| --- | --- |
|  | Phishing |
|  | Ransomware |
|  | SCADA attack |
|  | DDoS |

**Question 2 (1 point)**

The digital forensics process consists of four phases. Which of the following denotes the correct sequence of these four phases?

|  |  |
| --- | --- |
|  | Collection, analysis, examination, reporting |
|  | Examination, analysis, collection, reporting |
|  | Examination, collection, analysis, reporting |
|  | Collection, examination, analysis, reporting |

**Question 3 (1 point)**

Which of the following denotes the correct sequence of layers in the TCP/IP model of networking, from top to bottom?

|  |  |
| --- | --- |
|  | Application, Network, Data, Transport |
|  | Data, Network, Transport, Application |
|  | Application, Transport, Network, Data |
|  | Application, Data, Transport, Network |

**Question 4 (1 point)**

Which of the following refers to software that monitors network traffic on wired or wireless networks and captures packets?

|  |  |
| --- | --- |
|  | NIDS |
|  | Protocol Analyzer |
|  | Steganography |
|  | Packet sniffer |

**Question 5 (1 point)**

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ perform packet sniffing and analyze network traffic to identify suspicious activity and record relevant information, while \_\_\_\_\_\_\_\_\_\_ monitor characteristics of a particular system and events occurring within the system, which can include network traffic

|  |  |
| --- | --- |
|  | Network IDSs, Host IDSs |
|  | Host IDSs, Network IDSs |

**Question 6 (1 point)**

 Over the course of a week, the number of phone calls coming into the organization's help line for online bill  payment increases by 400 percent. Most callers complain of having to resubmit payment information multiple times, and many cannot complete their payment.

As a forensic analyst, what is your first step? Answer in 1-2 sentences.

As a forensic analyst, my first step towards this scenario is to identify potential sources of data including transaction information and acquire data from them. This step includes identifying payment processing servers, network storage devices, network logs, and so on, followed by acquiring the data from these sources using set of procedures to maintain the integrity of the data.



**Question 7 (1 point)**

Antiforensics refers to techniques for concealing or destroying data so that others cannot access it.

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 8 (1 point)**

On a Saturday afternoon, external users start having problems accessing the organization's public Web sites. Over the next hour, the problem worsens to the point where nearly every attempt to access any of the organization's public Web sites fails. Meanwhile, a member of the organization's networking staff responds to automatically generated alerts from an Internet border router and determines that much of the organization's Internet bandwidth is being consumed by an unusually large volume of User Datagram Protocol (UDP) packets to and from both of the organization's public Domain Name System (DNS) servers.

What kind of attack does this describe?

|  |  |
| --- | --- |
|  | DDoS |
|  | Social Engineering |
|  | POODLE |
|  | Spoofing |

**Question 9 (1 point)**

A firewall that receives a request from a client, and then sends a request on the client's behalf to the desired destination is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |
| --- | --- |
|  | Network-based firewall |
|  | Routing firewall |
|  | Proxy firewall |
|  | Sniffing firewall |

**Question 10 (1 point)**

During which phase of the forensics process does the following happen?

Using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

|  |  |
| --- | --- |
|  | Analysis |
|  | Examination |
|  | Collection |
|  | Reporting |