CYBER SECURITY

1) A security administrator wants to deploy security controls to mitigate the threat of company employees' personal information being captured online. Which of the following would best serve this purpose?
   A) antivirus
   B) host-based firewall
   C) anti-spyware
   D) web content filter

2) The below report indicates that the system is most likely infected by which of the following? Protocol LOCAL IP FOREIGN IP STATE, TCP 0.0.0:445 0.0.0.0:0 Listening, TCP 0.0.0.0:3390 0.0.0.0:0
   A) worm
   B) trojan
   C) listening
   D) logic bomb

3) The network manager has obtained a public IP address for use with a new system to be available via the internet. This system will be placed in the DMZ and will communicate with a database server on the LAN. Which of the following should be used to allow for secure communication between internet users and the internal systems?
   A) NAT
   B) SSL
   C) DNS
   D) VLAN

4) The SS ID broadcast for wireless router has been stopped, but a LAN administrator has noticed that authorized users are still accessing the wireless LAN. The administrator has determined that the attackers are still able to detect the presence of the wireless LAN even though the SS ID has been stopped. What would further obscure the presence of the wireless LAN?
   A) reroute wireless users to honeypot
   B) disable responses to a broadcast probe request
   C) create a non-zero length SS ID for the wireless router
   D) upgrade the encryption to WPA or WPA2

5) Which of the following is a Data Loss Prevention (DLP) strategy that addresses data in transit issues?
A) scanning of outbound IM
B) scanning copying of documents to USB
C) scanning of SharePoint document library
D) scanning printing of documents

6) An employee in the accounting department recently received a phishing email that instructed them to click a link in the email to view an important message from the IRS which threatened penalties if a response was **not** received by the end of the business day. The employee clicked on the link and the machine was infected with malware. Which of the following principles best describes why this social engineering ploy was successful?
A) scarcity
B) urgency
C) social proof
D) familiarity

7) A system administrator would like to safeguard the integrity of data while in transit over the local LAN. What should be implemented to fulfill this requirement?
A) encryption
B) data loss prevention
C) access control lists
D) HIPS

8) An attacker wants to get confidential data from an organization. The attacker decides to implement stenography as the method of hacking. Which of the following techniques should the attacker use?
A) use a substitution cipher
B) add information to a sound file
C) encrypt an existing image file
D) hash an existing document

9) What is a protocol that could be used to support authentication services for several local devices from a central location without the use of tokens or tickets?
A) biometrics
B) TACACS+
C) PKI
D) smartcards

10) Which of the following offerings typically allows the customer to apply operating system patches?
A) cloud-based storage
B) software as a service
C) public clouds
D) infrastructure as a service

11) A security analyst is investigating a potential breach. Upon gathering, documenting, and securing the evidence, which of the following actions is the next step to minimize the business impact?
A) launch an investigation to identify the attacking host
B) review lessons learned in the process
C) remove malware and restore the system to normal operation
D) initiate the incident response plan

12) An external auditor visits the human resource department and performs a physical security assessment. The auditor observes documents on printers that are unclaimed. A closer look at these documents reveals employees' names, addresses, ages, and type of medical and dental coverage options each employee has selected. Which of the following is the most appropriate action to take?
A) flip the documents face down so no one knows these documents are PII sensitive
B) retrieve the documents, label them with PII cover sheets, and return them to the printer
C) shred the documents and let the owner of the printer discover the missing documents on their own
D) report to the human resources manager that their personnel are violating a privacy policy

13) Following a system review, one corporate workstation was found to be storing passwords in plain text. Which of the following is the correct method for storing passwords?
A) hashing the password prior to storing
B) creating a digital certificate of the password prior to storing
C) using cryptography to conceal the password prior to storing
D) run the passwords through a quaternion system of equations

14) Which of the following best describes the initial processing phase used in mobile device forensics?

A) the phone and storage cards should be examined as a complete unit after examining the removable storage cards separately

B) the phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device

C) the mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again

D) the removable data storage cards should be processed first to prevent data alteration when examining the mobile device

15) The Chief Information Officer (CIO) is concerned with moving an application to a SaaS cloud provider. Which of the following can be implemented to provide for data confidentiality assurance during and after the migration to the cloud?

A) HPM technology

B) DLP policy

C) TPM technology

D) Full-disk encryption

1) C
2) C
3) B
4) D
5) A
6) B
7) A
8) B
9) B
10) D
11) C
12) D
13) A
14) B
15) B