Final Exam

1. Which statement describes cybersecurity?

- It is a framework for security policy development.
- It is a standard-based model for developing firewall technologies to fight against cybercriminals.
- It is a standard-based model for developing firewall technologies to fight against cybercriminals.
- It is an ongoing effort to protect Internet-connected systems and the data associated with those systems from unauthorized use or harm.

Explanation:
Cybersecurity is the ongoing effort to protect Internet-connected network systems and all of the data associated with the systems from unauthorized use or harm.

2. What are two objectives of ensuring data integrity? (Choose two.)

- Data is available all the time.
- Data is unaltered during transit.
- Access to the data is authenticated.
- Data is not changed by unauthorized entities.
- Data is encrypted while in transit and when stored on disks.

Explanation:

The objectives for data integrity include data not being altered during transit and not being changed by unauthorized entities. Authentication and encryption are methods to ensure confidentiality. Data being available all the time is the goal of availability.

3. A web server administrator is configuring access settings to require users to authenticate first before accessing certain web pages. Which requirement of information security is addressed through the configuration?

- integrity
- scalability
- availability
- confidentiality

Explanation:
Confidentiality ensures that data is accessed only by authorized individuals. Authentication will help verify the identity of the individuals.

4. A company is experiencing overwhelming visits to a main web server. The IT department is developing a plan to add a couple more web servers for load balancing and redundancy. Which requirement of information security is addressed by implementing the plan?

- integrity
- scalability
- availability
- confidentiality

Explanation:
Availability ensures that network services are accessible and performing well under all conditions. By load balancing the traffic destined to the main web servers, in times of a huge volume of visits the systems will be well managed and serviced.

5. True or False?

An employee does something as a company representative with the knowledge of that company and this action is deemed illegal. The company would be legally responsible for this action.

- true
- false

Explanation:
This is a bit of a grey area and would also depend on local laws. In many cases, if the employee did something with the knowledge or approval of the company, then the legal responsibility would probably be with the company not the employee. In some areas or situations, both the company and employee could be held legally responsible.

6. What is the main purpose of cyberwarfare?

- to protect cloud-based data centers
- to gain advantage over adversaries
- to develop advanced network devices
- to simulate possible war scenarios among nations

Explanation:
Cyberwarfare is Internet-based conflict that involves the penetration of the networks and computer systems of other nations. The main purpose of cyberwarfare is to gain advantage over adversaries, whether they are nations or competitors.

7. When describing malware, what is a difference between a virus and a worm?

- A virus focuses on gaining privileged access to a device, whereas a worm does not.
- A virus can be used to deliver advertisements without user consent, whereas a worm cannot.
- A virus replicates itself by attaching to another file, whereas a worm can replicate itself independently.
- A virus can be used to launch a DoS attack (but not a DDoS), but a worm can be used to launch both DoS and DDoS attacks.

Explanation:
Malware can be classified as follows:

– Virus (self replicates by attaching to another program or file)
– Worm (replicates independently of another program)
– Trojan Horse (masquerades as a legitimate file or program)
– Rootkit (gains privileged access to a machine while concealing itself)
– Spyware (collects information from a target system)
– Adware (delivers advertisements with or without consent)
– Bot (waits for commands from the hacker)
– Ransomware (holds a computer system or data captive until payment is received)

8. What type of attack uses zombies?

- Trojan horse
- DDoS
- SEO poisoning
- spear phishing

Explanation:
The hacker infects multiple machines (zombies), creating a botnet. Zombies launch the distributed denial of service (DDoS) attack.

9. The IT department is reporting that a company web server is receiving an abnormally high number of web page requests from different locations simultaneously. Which type of security attack is occurring?

- adware
- DDoS
- phishing
- social engineering
- spyware

Explanation:
Phishing, spyware, and social engineering are security attacks that collect network and user information. Adware consists, typically, of annoying popup windows. Unlike a DDoS attack, none of these attacks generate large amounts of data traffic that can restrict access to network services.

10. What is the best approach to prevent a compromised IoT device from maliciously accessing data and devices on a local network?

- Install a software firewall on every network device.
- Place all IoT devices that have access to the Internet on an isolated network.
- Disconnect all IoT devices from the Internet.
- Set the security settings of workstation web browsers to a higher level.

Explanation:
The best approach to protect a data network from a possibly compromised IoT device is to place all IoT devices on an isolated network that only has access to the Internet.

11. What is the best method to avoid getting spyware on a machine?

- Install the latest operating system updates.
- Install the latest web browser updates.
- Install the latest antivirus updates.
- Install software only from trusted websites.

Explanation:
The best method to avoid getting spyware on a user machine is to download software only from trusted websites.

12. What are two security implementations that use biometrics? (Choose two.)

- voice recognition
- fob
- phone
- fingerprint
- credit card

Explanation:
Biometric authentication can be used through the use of a fingerprint, palm print, and facial or voice recognition.

13. Which technology creates a security token that allows a user to log in to a desired web application using credentials from a social media website?

- password manager
- Open Authorization
- in-private browsing mode
- VPN service

Explanation:
Open Authorization is an open standard protocol that allows end users to access third party applications without exposing their user passwords.

14. A medical office employee sends emails to patients about recent patient visits to the facility. What information would put the privacy of the patients at risk if it was included in the email?

- patient records
- first and last name
- contact information
- next appointment

Explanation:
An email message is transmitted in plain text and can be read by anyone who has access to the data while it is en route to a destination. Patient records include confidential or sensitive information that should be transmitted in a secure manner.

15. Which two tools used for incident detection can be used to detect anomalous behavior, to detect command and control traffic, and to detect infected hosts? (Choose two.)

- intrusion detection system
- Honeypot
- NetFlow
- Nmap
- a reverse proxy server

Explanation:
Although each of these tools is useful for securing networks and detecting vulnerabilities, only an IDS and NetFlow logging can be used to detect anomalous behavior, command and control traffic, and infected hosts.

16. For what purpose would a network administrator use the Nmap tool?

- detection and identification of open ports
- protection of the private IP addresses of internal hosts
- identification of specific network anomalies
- collection and analysis of security alerts and logs

Explanation:
Nmap allows an administrator to perform port scanning to probe computers and the network for open ports. This helps the administrator verify that network security policies are in place.

17. Which stage of the kill chain used by attackers focuses on the identification and selection of targets?

- delivery
- exploitation
- weaponization
- reconnaissance

Explanation:
It is the first stage, reconnaissance, of the the kill chain that focuses on the identification and selection of targets.

18. What is an example of the a Cyber Kill Chain?

- a group of botnets
- a planned process of cyberattack
- a series of worms based on the same core code
- a combination of virus, worm, and Trojan Horse

Explanation:
The Cyber Kill Chain describes the phases of a progressive cyberattack operation. The phases include the following:
Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command and control
Actions on objectives
In general, these phases are carried out in sequence. However, during an attack, several phases can be carried out simultaneously, especially if multiple attackers or groups are involved.

19. What tool is used to lure an attacker so that an administrator can capture, log, and analyze the behavior of the attack?

- Netflow
- IDS
- Nmap
- honeypot

Explanation:
A honeypot is a tool set up by an administrator to lure an attacker so that the behavior of the attacker can be analyzed. This information can help the administrator identify weaknesses and build a stronger defense.

20. What is one main function of the Cisco Security Incident Response Team?

- to design polymorphic malware
- to design next generation routers and switches that are less prone to cyberattacks
- to provide standards for new encryption techniques
- to ensure company, system, and data preservation

Explanation:
The time between a cyberattack and the time it takes to discover the attack is the time when hackers can get into a network and steal data. An important goal of the CSIRT is to ensure company, system, and data preservation through timely investigations into security incidents.

21. What action will an IDS take upon detection of malicious traffic?

- block or deny all traffic
- drop only packets identified as malicious
- create a network alert and log the detection
- reroute malicious traffic to a honeypot

Explanation:
An IDS, or intrusion detection system, is a device that can scan packets and compare them to a set of rules or attack signatures. If the packets match attack signatures, then the IDS can create an alert and log the detection.