UNIVERSITY OF ESWATINI

Faculty of Science and Engineering

Department of Computer Science

MAIN EXAMINATION - OCTOBER 2021

Title of Paper: COMPUTER SECURITY II

Course Number: CSC462

Time Allowed: 3 hours

Instructions to candidates:

This question paper consists of ***Four*** **(4)** *questions. Answer Question 1 & Choose 3 questions from the others.*
Marks for each individual question are indicated in square brackets.
All questions carry equal marks (25 Marks Each).

DO NOT OPEN THE PAPER UNTIL PERMISSION HAS BEEN GIVEN BY THE INVIGILATOR.

QUESTION 1 (Compulsory: Multiple choice)

1. **Which statement describes cybersecurity?**

   A. It is a framework for security policy development.
   B. It is a standard-based model for developing firewall technologies to fight against cybercriminals.
   C. It is the name of a comprehensive security application for end users to protect workstations from being attacked.
   D. It is an ongoing effort to protect Internet-connected systems and the data associated with those systems from unauthorized use or harm.

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

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

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?**

   A. integrity
   B. scalability
   C. availability
   D. confidentiality

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?**

   A. integrity
   B. scalability
   C. availability
   D. confidentiality

5. **True or False?**

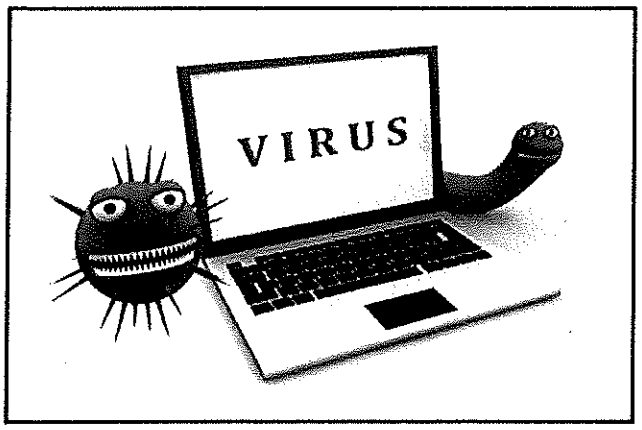
An employee does something as a company representative with the knowledge of that company and this action is deemed illegal. The company would be legally responsible for this action.

A. true
B. false

6. **What is the main purpose of cyberwarfare?**

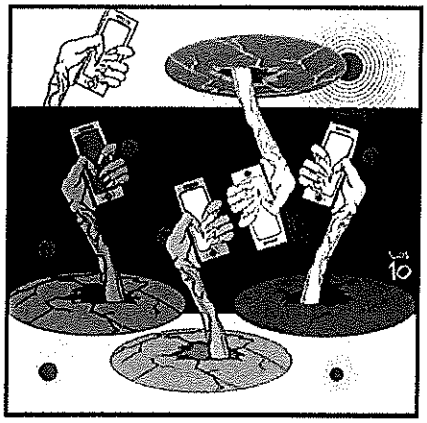
A. to protect cloud-based data centers
B. to gain advantage over adversaries
C. to develop advanced network devices
D. to simulate possible war scenarios among nations

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



A. A virus focuses on gaining privileged access to a device, whereas a worm does not.
B. A virus can be used to deliver advertisements without user consent, whereas a worm cannot.
C. A virus replicates itself by attaching to another file, whereas a worm can replicate itself independently.
D. 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.

8. **What type of attack uses zombies?**

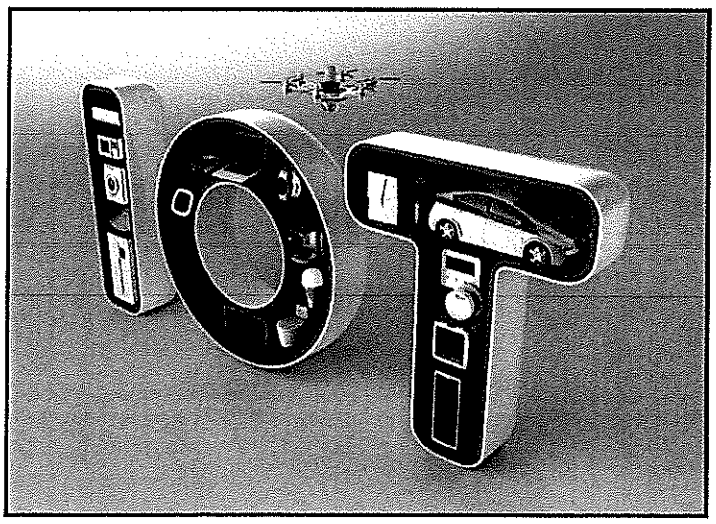


A. Trojan horse
B. DDoS
C. SEO poisoning
D. spear phishing

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?

A. adware
B. DDoS
C. phishing
D. social engineering
E. spyware

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

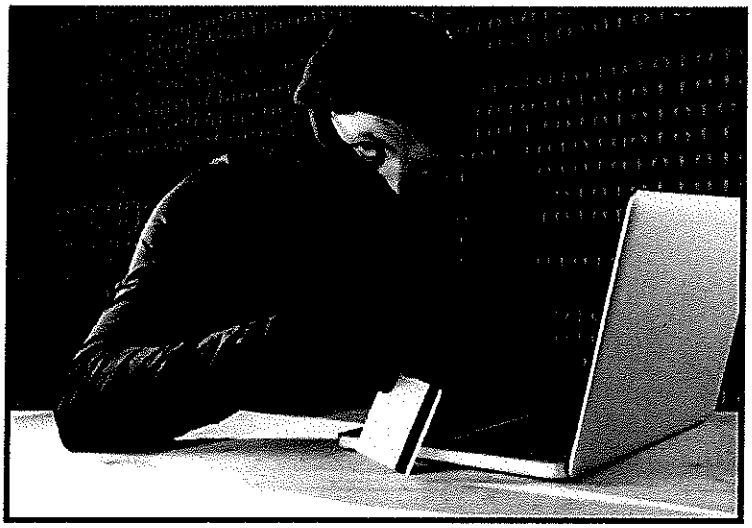


A. Install a software firewall on every network device.
B. Place all IoT devices that have access to the Internet on an isolated network.
C. Disconnect all IoT devices from the Internet.
D. Set the security settings of workstation web browsers to a higher level.

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

A. Install the latest operating system updates.
B. Install the latest web browser updates.
C. Install the latest antivirus updates.
D. Install software only from trusted websites.

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



A. voice recognition
B. fob
C. phone
D. fingerprint
E. credit card

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?

A. password manager
B. Open Authorization
C. in-private browsing mode
D. VPN service

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?

A. patient records
B. first and last name
C. contact information
D. next appointment

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.)

A. intrusion detection system
B. Honeypot
C. NetFlow
D. Nmap
E. a reverse proxy server

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

A. detection and identification of open ports
B. protection of the private IP addresses of internal hosts
C. identification of specific network anomalies
D. collection and analysis of security alerts and logs

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

A. delivery
B. exploitation
C. weaponization
D. reconnaissance

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

A. a group of botnets
B. a planned process of cyberattack
C. a series of worms based on the same core code
D. a combination of virus, worm, and Trojan Horse

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

A. NetFlow

B. IDS
C. Nmap
D. Honeypot

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

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

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

A. block or deny all traffic
B. drop only packets identified as malicious
C. create a network alert and log the detection
D. reroute malicious traffic to a honeypot

QUESTION 2

A. What is Cybersecurity and why is it needed at a personal and organizational level? [4]

B. What is a security breach and what is its impact? [2]

C. Briefly describe the different types of Cyber attackers available out there. [10]

D. Usually, internal security threats can cause greater damage than external threats. Why is that so? [1]

E. What is Cyberwarfare? What are the purposes of a Cyberwarfare? [8]

QUESTION 3

A. Distinguish between a vulnerability, an exploit and an attack. [3]

B. What is a Malware? Discuss the different types of Malwares. [12]

C. What are some of the symptoms of a Malware? [10]

QUESTION 4

A. With an aid of diagrams, distinguish between DoS and DDoS. [12]

B. What is a blended attack? [3]

C. Describe the different ways on how you can protect your data. [10]

QUESTION 5

A. What is a firewall? Discuss the different types of firewalls. [12]

B. Discuss some of the security best practices that organizations can use in order to ensure that they are well secure. [13]

*****End of Question Paper*****