Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2019/2020

COURSE NAME	:	WEB SECURITY
COURSE CODE	:	BIS 20303
PROGRAMME CODE	:	BIS / BIW
EXAMINATION DATE	:	DECEMBER 2019 / JANUARY 2020
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **NINE (9)** PAGES

SECTION A

Instruction: Choose the BEST answer for each of the following questions

Q1 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. Virtual Private Network (VPN) service.

Q2 Which stage of the kill chain used by attackers focuses on the identification and selection of targets?

A. Weaponization.
B. Reconnaissance.
C. Exploitation.
D. Delivery.

Q3 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. Social engineering.
B. Adware.
C. Phishing.
D. Distributed Denial of Service (DDos).

Q4 What is the main purpose of cyberwarfare?

A. To develop advanced network devices.
B. To gain advantages over adversaries.
C. To simulate possible war scenarios over nations.
D. To protect cloud-base data centers.

Q5 What is the best approach to prevent a compromised Internet of Things (IoT) device from maliciously accessing data and devices on a local network?

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

Q6 What is the best method to avoid getting spyware on a machine?

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

Q7 Which statement describes cybersecurity?

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

Q8 What type of attack uses zombies?

A. Trojan horse.
B. DDoS.
C. Spear phishing.
D. Search Engine Optimization (SEO) poisoning.

Q9 What tool or technique is used to lure an attacker so that an administrator can capture, log and analyze the behavior of a web attack?

A. Netflow.
B. Nmap.
C. Intrusion Detection System (IDS).
D. Honeypot.

Q10 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.

Q11 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 launch a Distributed Denial of Service (DoS) attack (but not a DDoS), but a worm can be used to launch both DoS and DDoS attacks.
C. A virus replicates itself by attaching to another file, whereas a worm can replicate itself independently.
D. A virus can be used to deliver advertisements without user consent, whereas a worm cannot.

Q12 Choose **TWO (2)** tools or techniques that can be used to detect anomalous behavior, command and control (C&C) traffic and infected hosts.

A. Nmap.
B. A reverse proxy server.
C. NetFlow.
D. IDS.
E. Honeypot.

Q13 What action will an IDS take upon detection of malicious traffic?

A. Drop only packets identified as malicious.
B. Reroute malicious traffic to a honeypot.
C. Block or deny all traffic.
D. Create a network alert and log the detection.

Q14 What is the main function of the Security Incident Response Team?

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

Q15 Choose **TWO (2)** objectives of ensuring data integrity.

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

Q16 What is a purpose of the Nmap tool used by network administrator?

A. Identification of specific network anomalies.
B. Protection of the private Internet Protocol (IP) addresses of internal hosts.
C. Detection and identification of open ports.
D. Collection and analysis of security alerts and logs.

Q17 A medical office employee sends emails to patients about recent patients' visits to the facility. What information would put the privacy of the patients at risk if it was included in the email?

A. First and last name.
B. Patient records.
C. Contact information.
D. Next appointment.

Q18 What is an example of the Cyber Kill Chain?

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

Q19 Choose **TWO (2)** security implementations that use biometrics.

A. Smartwatch.
B. Voice recognition.
C. Credit card.
D. Fingerprint.
E. Phone.

Q20 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. Availability.
B. Confidentiality.
C. Integrity.
D. Scalability.

(40 marks)

SECTION B

Instruction: Determine whether these statements are TRUE or FALSE

Q21 Like Java applets, ActiveX controls also run in a sandbox.

Q22 In an active man-in-the-middle attack, the contents are intercepted and altered before they are sent on to the recipient.

Q23 The term "exploit" means to take advantage of a vulnerability.

Q24 JavaScript resides inside Hypertext Markup Language (HTML) documents.

Q25 The syntax of SQL is considered to be very much like the English language.

(10 marks)

SECTION C

Q26 Questions **Q26(a) – Q26(d)** are based on Figure **Q26**.

One morning in 2019, Ahmad turned on his computer. He found that all of the software and files in his computer are inaccessible. A message on the screen said he had 14 days to pay a ransom in Bitcoin to a given Bitcoin's e-wallet address, else all of his files would be deleted.

FIGURE Q26

(a) Name an attack faced by Ahmad.

(2 marks)

(b) Explain how the attack in **Q26(a)** work.

(4 marks)

(c) Propose **TWO (2)** countermeasures for the attack in **Q26(a)**.

(8 marks)

(d) Should Ahmad pay the ransom? Justify your answer.

(6 marks)

Q27 (a) Define Open Web Application Security Project (OWASP)

(2 marks)

(b) Explain the following web security risk based on OWASP definition.

(i) Injection
(ii) Broken Authentication
(iii) Sensitive Data Exposure
(iv) Cross-Site Scripting
(v) Extensible Markup Language Entities (XEE)

(10 marks)

(c) Describe **FOUR (4)** characteristics of fraud's email.

(8 marks)

Q28 Common web security concept are:

"Confidentiality, Integrity, Availability, Non-repudiation, Privacy, Authentication, Authorization"

Map only **ONE (1)** web security concept for each of following:

(i) Ali hacked the salary system and changed his salary from RM2500 to RM5500.

(ii) Ahmad received One Time Password message in his phone when purchasing book via online shopping cart.

(iii) Health care providers are required to keep a patient's personal health information private unless consent to release the information is provided by the patient.

(iv) The ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

(v) The ability of the users to access and use a website or web service.

(10 marks)

- END OF QUESTIONS -