Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
(ONLINE)
SEMESTER II
SESSION 2020/2021

COURSE NAME	:	COMPUTER SECURITY
COURSE CODE	:	BEC 41903
PROGRAMME CODE	:	BEJ
EXAMINATION DATE	:	JULY 2021
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER ALL QUESTIONS. **OPEN BOOK EXAMINATION**

THIS ANSWER SCHEME PAPER CONSISTS OF **NINE (9)** PAGES

PART A: Objective Questions

Q1 A SYN flood is an example of what type of attack?

(A) Malicious code
(B) Denial-of-services
(C) Man-in-the-middle
(D) Spoofing

(1 mark)

Q2 An attack in which the attacker simply listens for all traffic being transmitted across a network, in the hope of viewing something such as user ID and password combination, is known as _____ .

(A) a man-in-the-middle attack
(B) a denial-of-service attack
(C) a sniffing attack
(D) a backdoor attack

(1 mark)

Q3 An attack in which an attacker attempts to lie and misrepresent himself in order to gain access to information that can be useful in an attack is known as

(A) Social science
(B) White-hat hacking
(C) Social engineering
(D) Social manipulation

(1 mark)

Q4 Your manager has ensured that a policy is implemented that requires all employees to shred sensitive documents. What type of attack is your manager hoping to prevent?

(A) Tailgating
(B) Denial-of-service
(C) Social engineering
(D) Dumpster diving

(1 mark)

Q5 What type of attack involves the hackers sending too much data to a service or application that typically results in the hacker gaining administrative access to the system?

(A) SQL Injection
(B) Brute force
(C) Eavesdrop
(D) Buffer overflow

(1 mark)

Q6 What can be done to secure a wireless network?

(A) Decrease power transmission level to cover only intended area.
(B) Use a wireless encryption standard such as 802.3
(C) Change the DHCP supplied default gateway address.
(D) Configure wireless router admin access to use HTTP.

(1 mark)

Q7 Which standard requires stations to authenticate prior to gaining network access?

(A) 802.11a
(B) 802.11b
(C) 802.1x
(D) 802.3

(1 mark)

Q8 SNMP is a protocol used for _____.

(A) secure e-mail
(B) secure encryption of network packets
(C) remote access to user workstations
(D) remote access to network infrastructure

(1 mark)

Q9 A university student has a wired network connection to a restrictive university network. At the same time, the student connected to a Wi-Fi hotspot for a nearby coffee shop that allows unrestricted Internet access. What potential problem exists in this case?

(A) The student computer could link coffee shop patrons to the university network.
(B) The student computer could override the university default gateway setting.
(C) Encrypted university transmissions could find their way onto the Wi-Fi network.
(D) Encrypted coffee shop transmissions could find their way onto the university network.

(1 mark)

Q10 Users store company files on USB flash drives so that they can work from various computers outside of the corporate network. What should you do to secure this data?

(A) Generate file hashes for USB flash drive content.
(B) Scan USB flash drives for viruses.
(C) Encrypt USB flash drives.
(D) Digitally sign files on USB flash drives.

(1 mark)

Q11 Bob is a lawyer in Kuala Lumpur. He requires secure, high-quality voice communication with Indonesian clients. What can he do?

(A) Use VOIP with packet encryption over the Internet.
(B) Use cell phone voice encryption.
(C) Use only landline telephones.
(D) Use his cell phone on a special voice network for legal professional.

(1 mark)

Q12 Your IT manager asks you to ensure e-mail messages and attachments do not contain sensitive data that could be leaked to competitors. What type of solution should you propose?

(A) Antivirus software
(B) NIDS
(C) DLP
(D) HIDS

(1 mark)

Q13 Discovered in 1991, the Michelangelo malware was said to be triggered to overwrite the first 100 hard disk sectors with null data each year on March 6, the date of the Italian artist's birthday. What type of malware is Michelangelo?

(A) Zero day
(B) Worm
(C) Trojan
(D) Logic bomb

(1 mark)

Q14 A piece of malicious code uses dictionary attacks against computers to gain access to administrative accounts. The code can links compromised computers together for the purpose of receiving remote commands. What term best applies to this malicious code?

(A) Exploit
(B) Botnet
(C) Logic Bomb
(D) Backdoor

(1 mark)

Q15 What will prevent frequent repeated malicious attacks against user account passwords?

(A) Minimum password age
(B) Password hints
(C) Password history
(D) Account lockout

(1 mark)

Q16 Your organization hosts a web site with a back-end database. The database stores customer data, including credit card numbers. Which of the following is the BEST way to protect the credit card data?

(A) Full database encryption
(B) Whole disk encryption
(C) Database column encryption
(D) File-level encryption

(1 mark)

Q17 The Nuclear Power Plant has created an online application teaching nuclear physics. Only students and teachers in the Batu Pahat secondary School can access this application via the cloud. What type of cloud service model is this?

(A) IaaS
(B) PaaS
(C) SaaS
(D) Public

(1 mark)

Q18 Which security role is responsible for establishing access to data and enforcing related policies, laws and regulations?

(A) Custodian
(B) Data Owner
(C) Data User
(D) Database administrator

(1 mark)

Q19 Database administrators have created a database used by a web application. However, testing shows that the application is taking a significant amount of time accessing data within the database. Which of the following actions is MOST likely to improve the overall performance of a database?

(A) Normalization
(B) Client-side input validation
(C) Server-side input validation
(D) Obfuscation

(1 mark)

Q20 Your organization is preparing to deploy a web-based application, which will accept user input. Which of the following will BEST test the reliability of this application to maintain availability and data integrity?

(A) Model verification
(B) Input validation
(C) Error handling
(D) Dynamic analysis

(1 mark)

Q21 Which concepts exposes employees to varying job roles to increase their overall knowledge of business?

(A) Mandatory vacations
(B) Least privilege
(C) Separation of duties
(D) Job rotation

(1 mark)

Q22 Which of the following best describes security fuzzing?

(A) Providing random data to test application security.
(B) Conducting a quick overview security audit.
(C) Jamming Wi-Fi radio frequencies to prevent rogue access points.
(D) Injecting spoofed packets on a network.

(1 mark)

Q23 A military division uses a portable computing units to aid in flight take-off and landings at ad hoc landing strips. How can the military track the position of these portable units?

(A) SSL
(B) GPS
(C) TPM
(D) Bluetooth

(1 mark)

Q24 Tour disaster recovery plan requires the quickest possible data restoration from backup tape. Which strategy should you employ?

(A) Weekly full backup, daily incremental backup
(B) Daily full backup, weekly incremental backup
(C) Daily full backup
(D) Daily differential backup

(1 mark)

Q25 Users store company files on USB flash drives so that they can work from various computers outside of the corporate network. What should you do to secure this data?

(A) Generate file hashes for USB flash drive content.
(B) Scan USB flash drives for viruses.
(C) Encrypt USB flash drives.
(D) Digitally sign files on USB flash drives.

(1 mark)

PART B: True/False Questions

Q26 Privilege escalation occurs when a user or process accesses elevated rights and permissions.

Q27 Trojan horse trigger malicious code when specific conditions are satisfied, sush as a date.

Q28 Botnets are collections of computers under the sole control of the attacker.

Q29 Rotation of duties allows employees to learn more about the business as a whole while enhancing their skills.

Q30 A network-based intrusion detection system (NIDS) is not able to detect anomalies on individual systems or workstations.

Q31 S/MIME can be used with three different symmetric encryption algorithms: DES, 4DES, and RC2.

Q32 Renoissance is the information gathering phase in ethical hacking from the target user.

Q33 Data integrity means ensuring correctness and consistency of data.

Q34 Security associations defined by 3 parameters e.g. Security Parameters Index (SPI), IP Destination Address and Security Protocol Identifier.

Q35 The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network.

PART C: Subjective Questions

Q36 (a) Analyze the following source code whether they cause buffer overflow or not. Show your answer using memory allocation diagram.

(i)
```
char A[5];
A[5]='a';
```

(ii)
```
int A[5];
for (int i=0; i<5; i++)
    A[i]=100;
```

(iii)
```
int A[5];
for (int i=4; i>0; i--)
    A[i]=100;
```

(iv)
```
int A[2][3];
for (int i=0; i<2; i++)
  for (int j=0; j<3; j++)
    A[j][i]=100;
```

(v)
```
char A[8];
strcpy(A, "pass word");
```

(10 marks)

(b) Describe two (2) steps to secure operating systems.

(4 marks)

Q37 (a) Discuss three differences between EMI and EMP.

(6 marks)

(b) Besides using password as human authentication, explain another human authentication based on these following categories.

(i) Something you have
(ii) Something you are
(iii) Somewhere you are
(iv) Something you do

(8 marks)

Q38 (a) Illustrates a diagram to show the protection of Statistical Database from inference attacks.

(4 marks)

(b) As a computer security expert, suggest three (3) solutions to protect database from any security threats.

(9 marks)

Q39 (a) In the form of figure, investigate how El Gamal, SHA dan 3DES are used in secure e-mail delivery process.

(5 marks)

(b) Differentiate the following malicious code:

(i) Virus vs Worm
(ii) Spyware vs Trojan Horses

(8 marks)

Q40 (a) During Covid19 Pandemic, many education institutions implement online teaching and learning. As an IT security officer, discuss a policy guidelines for lecturer works outside the office.

(5 marks)

(b) Adam and Brian are having several debates about computer and network security. Adam says that it is the job of security professionals to find all vulnerabilities and every threat and make sure the system is always 100% secure. Do you agree with Adam? You should explain your answer with FIVE (5) reasons.

(6 marks)

-END OF QUESTION-