نموذج فاينل 471 مقرر IT 221 د.أسماء و د.مراد

الصح و الخطأ و الاختياري عليهم نص

Q1) Technical Access Control uses hardware doors to limit contact.
❌ False

Q2) Hacktivists are individual attackers with limited knowledge.
❌ False

Q3) Script kiddies are highly skilled attackers with a strong position and advanced technical abilities.
❌ False

Q4) Single Sign-On (SSO) increases security by reducing password fatigue and centralizing authentication.
✅ True

Q5) Redundancy is used to achieve high availability in systems.
✅ True

Q6) A weakness of symmetric key cryptography is that it uses a single shared key, which creates a key distribution risk.
✅ True

Q7) Smishing is a type of attack carried out via email.
❌ False

Q8) Zero-day vulnerabilities are already known to the software .
❌ False

Q9) Containment is a response to an incident that aims to identify the root cause of the problem.
❌ False

Q10) Role-Based Access Control Access permissions are based on the user's job function
✅ True

Q: Which of the following describes an Incremental Backup?
A) Backs up all data every time a backup is performed
B) Backs up any data that has changed since the last full backup or last incremental backup ✅
C) Backs up data that has changed since the last full backup only
D) Only backs up system files

Q2: What is Static Code Analysis?
A) Tests run on the program only after deployment
B) Tests run on compiled code at runtime
C) Tests run before the source code is even compiled and may be accompanied by manual peer reviews ✅
D) Tests that only check network traffic

Q3: What is the difference between a RAT and a Trojan?
A) RAT is harmless, while a Trojan is malicious
B) Trojan only targets servers
C) RAT allows remote access and control, while a Trojan disguises itself as legitimate software ✅
D) There is no difference between them

Q4: Which of the following is NOT a source of threat intelligence?
A) Twitter ✅
B) Vendor Website
C) Industry Group
D) Scientific Conferences

Q5: Which of the following is NOT correct about Penetration Testing?
A) It is fully automated ✅
B) It is performed periodically
C) It simulates real-world attacks
D) It helps identify security vulnerabilities

Q6: Which of the following is NOT typically a feature of a SIEM?
A) Aggregation
B) Remediation ✅
C) Correlation
D) Automated alerts and triggers

Q7: Which type of attack is NOT a form of social engineering attack?
A) Watering hole
B) Hoax
C) Zero-day ✅
D) Tailgating

Q8: Which of the following is an example of adversarial artificial intelligence in cybersecurity?
A) Buffer overflows
B) Improper input handling
C) Device driver manipulation
D) Tainted training data ✅

Q9: Which enterprise deployment model of mobile devices stores sensitive applications and data on a remote server that you can access through a smartphone?
A) VDI ✅
B) CYOD
C) BYOD
D) COPE

Q10 : Which type of password is affected by events in authentication?
A) TOTP (Time-based One-Time Password)
B) HOTP (HMAC-based One-Time Password) ✅
C) Static password
D) Biometric password

[5 marks]
-Define penetration test and its benefits. And who performs it?

[5 marks]
-define Business continuity plan (BCP) and List three goals of it

[6 marks]
-List the incident response six steps

[3 marks]
What are the confinement tools - several tools can be used to restrict malware ?
• Application whitelisting/blacklisting
• Sandbox
• Quarantine

[6 marks]
-List THREE sources of threat intelligence and Explain each on

Q) Give the right access control for each describe

Access Control Model	Simplified Definition
Discretionary (DAC)	Least restrictive; permissions are managed entirely by the object's owner.
Mandatory (MAC)	Most restrictive; access is strictly enforced by the system based on labels.
Role-Based (RBAC)	Job function; access is tied to defined organizational roles, not individuals.
Attribute-Based (ABAC)	Most flexible; uses complex policies based on user, resource, and environmental data.
Rule-Based	Dynamic roles; permissions change automatically based on specific global conditions.

Q) عطانا سيناريو يقول حطي كل وحدة من CIA في مكانها الصحيح حسب السيناريو و بري

Justification	Affected CIA	Case
		Hospital attacked by ransomware and went **offline**, preventing doctors from accessing patient records
		Person modified payroll data
		Company encrypted user information

✅ الحل تقريبًا

تمام 👍 هذا الحل كامل ومعبّي الجدول:

Justification	Affected CIA	Case
The system was offline, so doctors could not access patient records when needed.	**Availability**	Hospital attacked by ransomware and went **offline**, preventing doctors from accessing patient records
The payroll data was altered without authorization, making it inaccurate.	**Integrity**	Person modified payroll data
Encryption protects user information	**Confidentiality**	Company encrypted user information

Q) For each of the following scenarios, identify the associated Risk and suggest a Recommended Control to mitigate it

Scenario	Risk	Recommended Control
Downloading apps from an untrusted app store		
Information leakage from a stolen phone		
Bypassing manufacturer restrictions during installation		
Not updating the system for months		