Started on	Friday, 31 May 2024, 2:57 PM
State	Finished
Completed on	Friday, 31 May 2024, 3:17 PM
Time taken	20 mins 48 secs
Marks	19.08/25.00
Grade	**7.63** out of 10.00 (**76.33**%)

Question 1

Partially correct

Mark 0.50 out of 1.00

Potriviți următoarele vulnerabilități cu măsurile de mitigare peste care pot trece cu ușurință?

Return Oriented Programming	Write ⊕ Execute	✔
Just in Time spraying	ASLR (Address-Space Layout Randomization)	✖
Stack-based memory leakage	Stack Canaries	✔
NOP sleding	Stack Canaries	✖

The correct answer is: Return Oriented Programming → Write ⊕ Execute, Just in Time spraying → Write ⊕ Execute, Stack-based memory leakage → Stack Canaries, NOP sleding → ASLR (Address-Space Layout Randomization)

Question 2

Correct

Mark 1.00 out of 1.00

Ce proprietate de securitate este încălcată atunci când un furnizor mare de cloud (G.) șterge, din greșeală, datele unei companii stocate pe serverele acestuia?

a. Integritatea
b. Licența
c. Disponibilitatea ✔
d. Confidențialitatea

The correct answer is: Disponibilitatea

Question 3

Incorrect

Mark 0.00 out of 1.00

Care dintre următoarele tipuri de malware NU SE POT propaga automat (fără intervenție umană)?

- a. Worm
- b. Backdoor
- c. Trojan Horse ✔
- d. Ransomware ✖

The correct answers are: Trojan Horse, Backdoor

Question 4

Correct

Mark 1.00 out of 1.00

Ce este un Zero Day?

- a. O vulnerabilitate populară, puternic mediatizată în momentul descoperirii
- b. Un bug nou apărut într-un issue tracker / CVE database în ziua respectivă
- c. O vulnerabilitate necunoscută până în momentul descoperirii unui exploit ce o folosește ✔
- d. O vulnerabilitate nouă, apărută în ziua descoperirii

The correct answer is: O vulnerabilitate necunoscută până în momentul descoperirii unui exploit ce o folosește

Question 5

Correct

Mark 1.00 out of 1.00

Ce proprietăți are cifrul AES (Advanced Encryption Standard)?

- a. Folosește substituție + transpoziție pe runde, lucru pe blocuri de bytes, algoritm liber; ✔
- b. Folosește substituție, lucru pe blocuri de bytes, algoritm liber;
- c. Folosește S-P tip Feistel pe runde, lucru pe flux de bytes (stream), algoritm proprietate U.S.;
- d. Folosește transpoziție, lucru pe blocuri de bytes, algoritm proprietar;

The correct answer is: Folosește substituție + transpoziție pe runde, lucru pe blocuri de bytes, algoritm liber;

Question 6

Correct

Mark 1.00 out of 1.00

Care dintre următorii algoritmi de integritate folosește o funcție de hash și cheie simetrică?

a. RSA
b. HMAC ✔
c. SHA-256
d. ECDSA (Elliptic Curve Digital Signature Algorithm)

The correct answer is: HMAC

Question 7

Correct

Mark 1.00 out of 1.00

Care dintre algoritmii de mai jos pot fi folosiți atât pentru criptare, cât și pentru semnături digitale?

a. RSA ✔
b. Diffie-Hellman (DH / ECDH)
c. Elliptic Curve Digital Signature Standard (ECDSA)
d. Elliptic Curve Integrated Encryption Scheme (ECDIE)

The correct answer is: RSA

Question 8

Correct

Mark 1.00 out of 1.00

Care dintre urmatoarele mecanisme hardware sunt folosite pentru a oferi pornirea securizata a unui sistem de operare nativ (secure boot sau echivalent)?

a. Intel Software Guard Extensions (SGX)
b. Trusted Platform Module (TPM) ✔
c. Hipervizor SeL4
d. AMD SEV

The correct answer is: Trusted Platform Module (TPM)

Question 9

Incorrect

Mark 0.00 out of 1.00

Se poate extrage cheia rădăcină (Storage Root Key) de pe un chip Trusted Platform Module (TPM) sau Hardware Token?

a. Da, folosind timing side-channel attack ✖
b. Da, folosind un aparat cu raze X
c. Nu
d. Da, folosind azot lichid în timp ce funcționează și citirea offline

The correct answer is: Nu

Question 10

Partially correct

Mark 0.25 out of 1.00

Ce protocoale de autentificare se pot folosi de către două entități care nu se cunosc în prealabil, dar au încredere într-o entitate terță?

a. OAuth
b. SSL/TLS
c. Kerberos ✔
d. Needham-Schroeder

The correct answers are: Needham-Schroeder, Kerberos, SSL/TLS, OAuth

Question 11

Correct

Mark 1.00 out of 1.00

Ce tip + factori are, de regulă, un proces de autentificare format din username, parolă plus primirea unui SMS?

a. N-factori (n-step): ceea ce știi + inerent (ceea ce ai cumpărat);
b. N-factori (n-factor): ceea ce știi + ceea ce deții; ✔
c. N-pași (n-step): ceea ce știi + ceea ce deții;
d. N-pași (n-step): ceea ce știi;

The correct answer is: N-factori (n-factor): ceea ce știi + ceea ce deții;

Question 12

Correct

Mark 1.00 out of 1.00

Care din următoarele modele de implementare a autorizării reține perechi acțiune + obiect pentru fiecare subiect (utilizator)

a. Discretionary Access Control
b. Access Control Lists
c. Capabilities ✔
d. Mandatory Access Control

The correct answer is: Capabilities

Question 13

Incorrect

Mark 0.00 out of 1.00

Se dă următoarea secvență:

```
florin@local:~$ ls -ld
dr-xr-xr-- 2 mihai teachers   37 May 28 22:58 .
florin@local:~$ ls -l
----r-x--- 1 razvan admins    37 May 28 22:58 secret.txt
```

Ce utilizator (aveți grupurile în paranteză) va putea citi fișierul secret.txt?

a. nici unul ☹
b. doar mihai (grup: `teachers`);
c. doar razvan (grup: `admins`); ✖
d. ambii utilizatori;

The correct answer is: nici unul ☹

Question 14

Partially correct

Mark 0.33 out of 1.00

Care din următoarele modele de autorizare sunt susceptibile accesului neautorizat cu ajutorul unui cal troian -- presupunând o configurare fără alte vulnerabilități?

a. Role-Based Access Control
b. Mandatory Access Control
c. Bell La-Padula
d. Discretionary Access Control ✔

The correct answers are: Discretionary Access Control, Bell La-Padula, Role-Based Access Control

Question 15

Correct

Mark 1.00 out of 1.00

Care dintre următoarele tipuri de vulnerabilități pot apărea DOAR în programe care folosesc HEAP-ul?

a. Stack overflow
b. Type confusion
c. Use after free ✔
d. Dangling Pointer

The correct answer is: Use after free

Question 16

Correct

Mark 1.00 out of 1.00

Ce metoda se poate folosi pentru a proteja aplicatiile împotriva atacurilor de tip buffer overflow pe stiva?

a. ASLR
b. Data Execution Prevention
c. Canary ✔
d. ValGrind

The correct answer is: Canary

Question 17

Correct

Mark 1.00 out of 1.00

Pe ce sistem de operare este verificată automat integritatea kernelului folosind tehnologii de hipervizor?

a. iOS
b. Windows ✔
c. Android
d. GNU/Linux

The correct answer is: Windows

Question 18

Correct

Mark 1.00 out of 1.00

Care dintre următoarele sisteme de operare rulează fiecare aplicație cu conturi Unix separate pentru izolare a drepturilor de acces?

a. iOS
b. GNU/Linux
c. Android ✔
d. Windows

The correct answer is: Android

Question 19

Correct

Mark 1.00 out of 1.00

Care dintre atacurile de mai jos sunt ACTIVE?

a. Port Scanning ✔
b. Sniffing
c. Man in the Middle ✔
d. Reflection ✔

The correct answers are: Man in the Middle, Port Scanning, Reflection

Question 20

Correct

Mark 1.00 out of 1.00

Care dintre următoarele măsuri de protecție sunt specifice / acționează strict asupra nivelului 3 (Network) al stivei OSI?

a. Deep Packet Filtering
b. IP Blacklisting ✔
c. BPDU Guard
d. 802.1x

The correct answer is: IP Blacklisting

Question 21

Incorrect

Mark 0.00 out of 1.00

Care din următoarele atacuri NU poate fi aplicat asupra protocolului TLS?

a. SSL Stripping ✖
b. Padding Oracle Attack
c. Brute Force
d. Man in the Middle

The correct answer is: Brute Force

Question 22

Correct

Mark 1.00 out of 1.00

Ce măsuri poate lua dezvoltatorul unei aplicații web pentru a bloca atacurile de tip Cross Site Scripting?

a. CSRF Tokens
b. HTML Tag Stripping ✔
c. CAPTCHA forms
d. JavaScript blocking

The correct answer is: HTML Tag Stripping

Question 23

Correct

Mark 1.00 out of 1.00

Care dintre următoarele afirmații despre TOR NU este adevărată?

a. Tor folosește MixNet pentru a anonimiza relația dintre sursă și destinație; ✔
b. Tor NU criptează datele până la destinație (end to end encryption)
c. Sistemul destinație va primi în clar adresa IP sursă
d. Tor este susceptibil atacurilor de tip side channel

The correct answer is: Tor folosește MixNet pentru a anonimiza relația dintre sursă și destinație;

Question 24

Correct

Mark 1.00 out of 1.00

Care este cea mai importanta componenta pentru un CEO dintr-un raport de forensics?

a. sumarul ✔
b. numele investigatorului
c. detalierea informațiilor identificate
d. procedura folosită

The correct answer is: sumarul

Question 25

Correct

Mark 1.00 out of 1.00

Care din următoarele surse este cea mai volatilă și ar trebui salvată prioritar?

a. Lista de procese
b. Backup-urile în cloud
c. Tabela ARP ✔
d. Fișiere scrise pe un SSD

The correct answer is: Tabela ARP