Vraag 1

Bovenstaande figuur geeft de OAuth Client credentials flow weer. Zet de juiste nummers/letters bij de juiste termen:

E. Access Token	A. 1
H. STS	B. 2
G. API	C. 3
	D. 4
	E. 5
	F. A
	G. B
	H. C

Vraag 2

Wat is een attack vector?

- ○ De aanvalsmethode die direct tot rootrechten leidt.
- ○ De mogelijkheid om toegang te kopen tot een systeem door de system administrator geld te geven.
- ◉ Een kwetsbaarheid in de software die nog onbekend is door de maker van de software en dus nog niet gepatched is.
- ○ Een methode of pad waar een onbevoegde gebruiker kan proberen gegevens in te voeren in of gegevens uit een omgeving te halen.

⚠ Als u naar de volgende vraag gaat, kunt u geen wijzigingen meer aanbrengen in dit antwoord.

Vraag 3

Wat bedoelen we met “The principle of least privilege?”

- ◉ We geven enkel toegang tot de resources die strikt noodzakelijk zijn voor de rol in kwestie
- ○ Een nieuwe account heeft ‘by default’ geen toegang en toegang tot nieuwe resources moet steeds verleend worden door een administrator
- ○ De autorisatie in ons systeem gebeurt op basis van privileges of rollen. Het is de rol die je toegang bepaalt, niet je individuele user account.

⚠ Als u naar de volgende vraag gaat, kunt u geen wijzigingen meer aanbrengen in dit antwoord.

Vraag 4

Duid bij elke statement aan of dit een eigenschap is van een Executive Summary of een Technical Report.

B. De doelen van de test worden duidelijk gespecificeerd en toegelicht	A. Technical Report
B. High level bevindingen worden gedeeld in niet-technische termen duidelijk voor alle stakeholders.	B. Executive Summary
A. Technische inzichten en bevindingen worden gedeeld om het team beter te maken	
A. Praktische suggesties worden gedaan om het specifieke issue op te lossen.	
B. Duidelijke stappen om het probleem te reproduceren worden toegevoegd.	

⚠ Als u naar de volgende vraag gaat, kunt u geen wijzigingen meer aanbrengen in dit antwoord.

Vraag 5

Welke van de volgende uitspraken is **geen** OWASP best practice bij het gebruik van databases:

- [x] Gebruik indien mogelijk de default configuratie van de database
- [ ] Beveilig je queries indien mogelijk met parametrisatie
- [ ] Authenticeer en autoriseer elke toegang tot de database via een veilig kanaal

⚠ Als u naar de volgende vraag gaat, kunt u geen wijzigingen meer aanbrengen in dit antwoord.

Vraag 6

Welke van de volgende uitspraken is **geen** OWASP best practice bij het gebruik van een externe library wat betreft security:

- [ ] Vertrouw geen libraries die al 6 maanden niet meer geupdate zijn
- [ ] Hou de library up-to-date
- [x] Encapsuleer de library en gebruik enkel de minimal functionaliteit die je nodig hebt

⚠ Als u naar de volgende vraag gaat, kunt u geen wijzigingen meer aanbrengen in dit antwoord.

Vraag 7

Welk van volgende stappen is **geen** onderdeel van het Root Cause Analyse process?

- [ ] Identificeer en beschrijf duidelijk het probleem
- [ ] Creëer een tijdslijn vanaf het punt van normale operatie tot het probleem zich voordoet
- [x] Maak een onderscheid tussen oorzaak en gevolg (causaliteit) om zo tot de echte oorzaak te komen.
- [ ] Elimineer bijzaken van hoofdzaken door het systeem vanaf de grond opnieuw te installeren/configureren tot het probleem zich terug voordoet.

⚠ Als u naar de volgende vraag gaat, kunt u geen wijzigingen meer aanbrengen in dit antwoord.

Vraag 8

Wat zijn **GEEN** kenmerken van thrust boundaries in Threat Modeling? [2 antwoorden, -1 per fout antwoord]

- [ ] Grenzen om te laten zien wie wat controleert
- [x] Security-through-obscurity helpt thrust boundaries beveiligen
- [ ] Bedreigingen die die grenzen overschrijden, zijn waarschijnlijk belangrijke bedreigingen
- [ ] Verschillende mensen beheersen verschillende dingen
- [x] De idempotentie van gegevens moet gegarandeerd blijven

⚠ Als u naar de volgende vraag gaat, kunt u geen wijzigingen meer aanbrengen in dit antwoord.

Vraag 9

Wat is het belang van persistence bij het exploiten van systemen?

- ○ Direct administrator rechten hebben bij het activeren van een exploit zonder hiervoor iets extra te moeten doen.
- ○ Snelle, makkelijke toegang over een korte tijd.
- ○ Een reverse shell kunnen opzetten om zo de connectie stabieler te maken.
- ◉ Makkelijke toegang tot de systemen over een lange tijd zonder dat dit opgemerkt wordt

⚠ Als u naar de volgende vraag gaat, kunt u geen wijzigingen meer aanbrengen in dit antwoord.

Vraag 10

Waarvoor kan Shodan gebruikt worden binnen Red Teaming?

- ○ Het scannen en inventariseren van open poorten en services die publiek te vinden zijn op het internet
- ◉ Hiermee kan men surfen op het internet zonder dat ze je IP adres kunnen achterhalen
- ○ Het opzoeken van bekende kwetsbaarheden in software versies zodat we deze kunnen misbruiken.

⚠ Als u naar de volgende vraag gaat, kunt u geen wijzigingen meer aanbrengen in dit antwoord.

Vraag 11

Catalogeer volgende eigenschappen onder hun meest typische soort assignment: Red Teaming, Pen Test of Vulnerability Assessment.

A. Scope gedefinieerd door het team zelf	A. Red Team
C. Gedeeltelijke, manuele Threat Emulation	B. Vulnerability Assessement
A. Brede, voor gedefinieerde scope, automatisch getest en eventueel manueel geverifieerd	C. Pen Test
A. Simultane systeem- en fysieke testen	
B. Gebruikers, developers en project team zijn op voorhand duidelijk op de hoogte van de test	

⚠ Als u naar de volgende vraag gaat, kunt u geen wijzigingen meer aanbrengen in dit antwoord.

Vraag 12

Welk zijn de voordelen van Threat modeling van een product VOOR het gebouwd wordt? [3 antwoorden, -1 per fout antwoord]

- [x] Door je requirements on de loep te nemen kan je gaten in je requirements vroeg ontdekken.
- [ ] Het helpt om business requirements af te stemmen op security requirements, business requirements < security requirements.
- [x] Engineer en lever betere producten af op een regelmatiger en strakker schema.
- [x] Helpt om design problemen te detecteren voor er nog maar een lijn code geschreven is.
- [ ] Threat modeling focust op dezelfde issues als je andere veiligheids- en security engineering, maar gaat deze dubbelchecken. Het is dus vooral redundancy en niet een nieuw perspectief.

⚠ Als u naar de volgende vraag gaat, kunt u geen wijzigingen meer aanbrengen in dit antwoord.

Vraag 13

Welk van de volgende detectie methodes past bij een NIDS? [2 antwoorden, -1 per fout antwoord]

- [x] Signature-based detection
- [ ] Stateful protocol analysis detection
- [x] Statistical Blockchain-based detection

⚠ Als u naar de volgende vraag gaat, kunt u geen wijzigingen meer aanbrengen in dit antwoord.

Vraag 15

Wat betekent single sign on?

- ○ Dat je eenmaal toestemming geeft aan een systeem om in jouw naam te data op te halen van een ander systeem
- ○ Dat je maar eenmaal moet aanmelden op een website en dat je de volgende keer automatisch aangemeld ben
- ◉ Het gebruik van dezelfde credentials voor meerdere websites

⚠ Als u naar de volgende vraag gaat, kunt u geen wijzigingen meer aanbrengen in dit antwoord.

Vraag 16

Zet de volgende termen in de juiste volgorde naarmate het maturity model beter wordt:

(minst (1) naar meest matuur (5))

4. Robuust meet framework

3. Compliance focused

5. Langetermijnsvisie en cultuur verandering

1. Nietbestaand

2. Awareness & gedragsverandering promotend

Vraag 17

Een van de belangrijke punten bij Incident Response is “protect the present”, welk zijn concrete punten hierbij? [3 antwoorden, -1 per fout antwoord]

- [x] Test de systemen voor ze opnieuw in gebruik te nemen
- [x] Herstel de systemen (indien mogelijk)
- [ ] Verwijder de systemen uit het productie netwerk
- [ ] Beperk down-time, bescherm de business door zo snel mogelijk een backup terug te zetten op de systemen
- [x] Zet de systemen zo snel mogelijk uit om verdere schade te voorkomen

Vraag 18

Welk van onderstaande technieken kunnen gebruikt worden bij het actief footprinten van servers?

[3 antwoorden, -1 per fout antwoord]

- [x] Virtual Host Detection & Enumeration
- [ ] Wifi scanning
- [ ] Whois lookups
- [x] Forward/Reverse DNS
- [x] Web Application Discovery

Vraag 19

Duidt aan tussen welke kanalen OAuth https nodig heeft om veilig te functioneren:

A. Tussen Client en STS — A. HTTPS noodzakelijk

B. Tussen Client en API — B. HTTPS gewenst

B. Tussen API en STS — C. Geen HTTPS nodig

Vraag 20

Welk van onderstaande zijn acties die we kunnen ondernemen in het S.T.R.I.D.E. model als we een threat hebben vastgesteld? [2 antwoorden, -1 per fout antwoord]

- [x] Mitigate
- [ ] Fix
- [ ] Dance
- [x] Eliminate
- [ ] Abolish

Vraag 21

Welk van de volgende zaken zit **niet** in een OAuth access token? [2 Antwoorden, -1 per fout antwoord]

- [ ] Client Secret
- [x] Redirect Uri
- [ ] Scope
- [x] Signature

Vraag 22

Welk van volgende statements ivm File system Forensics is waar?

- (●) File Carving gebruikt de magic byte om het begin en einde van een file te vinden.
- ( ) Disk-to-image imaging wordt enkel gebruikt als disk-to-disk niet mogelijk is.
- ( ) Logical acquisition gaat enkel de Logical Volumes (LVM) van een HDD capteren.
- ( ) Alle gecapteerde disks/files/images worden door het forensisch team van een watermerk voorzien om te voorkomen dat ze aangepast worden

Vraag 23

Waarom zijn soft-skills een belangrijk onderdeel van DFIR skills?

- ( ) Communicatie is de key om met slachtoffers, management, klanten en externen te praten
- ( ) Omdat goede en duidelijke rapporten schrijven zeer belangrijk is
- (●) Social engineering skils zijn goed om hogerop te geraken

Vraag 24

Link de volgende cases aan de correcte ISO27001 Controls:

A. De procedure die zegt dat we doorzichtige vuilniszakken moeten gebruiken

C. De Procedure die het responsible disclosure programma van het bedrijf beschrijft

D. De procedure die de werknemers vertelt welke chat platformen ze mogen gebruiken binnen het bedrijf

A. De procedure die de maandelijkse patch strategie van de servers omschrijft

D. De procedure om ervoor te zorgen dat alle gebruikersaccounts (zowel intern als extern) worden afgesloten van werknemers die het bedrijf verlaten.

E. De procedure die de backup policies van de productieomgeving van een webshop omschrijft

A. A.11 Physical and environmental security

B. A.13 Communications security

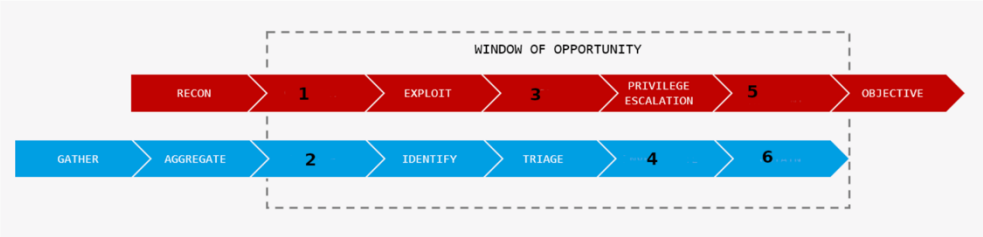
C. A.16 Information security incident management

D. A.7 Human resources security

E. A.12 Operational security

Vraag 25

Zet de juiste term bij het juiste nummer:



A. 6

C. 5

D. 4

B. 3

H. 2

I. 1

A. Contain

B. C2

C. Lateral movement

D. Investigate

E. Compliance

F. Dominate

G. Incident response

H. Analyse

I. Delivery