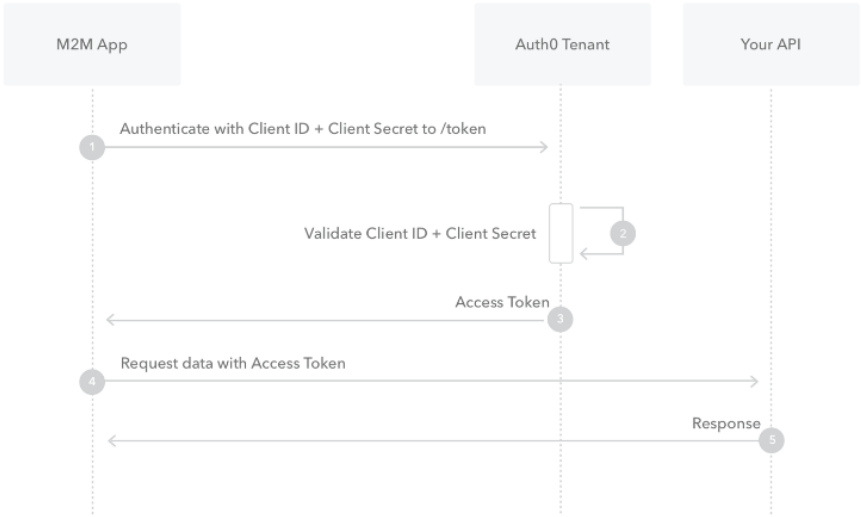
Vraag 1: Onderstaande figuur geeft de OAuth Client Credentials flow weer. Zet de juiste nummers/letters bij de juister termen.



ANTW:

C: Access Token
A: STS
H: API

Vraag 2: Wat is een attack vector?

ANTW: Een methode of pad waar een onbevoegde gebruiker kan proberen gegevens in te voeren in of gegevens uit een omgeving te halen.

Vraag 3: Wat bedoelen we met “The principle of least privilege?”?

ANTW: We geven enkel toegang tot de resources die strikt noodzakelijk zijn voor de rol in kwestie.

Vraag 4: Duid bij elke statement aan of dit een eigenschap is van een Executive Summary of een Technical Report (A = Technical Report / B = Executive Summary)

ANTW:

- **B:** De doelen van de test worden duidelijk gespecificeerd en toegelicht ?
- **B:** High level bevindingen worden gedeeld in niet-technische termen duidelijk voor alle stakeholders
- **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
- **A:** Duidelijke stappen om het probleem te reproduceren worden toegevoegd

Vraag 5: Welke van de volgende uitspraken is GEEN OWASP best practice bij het gebruiken van databases:

ANTW: Gebruik indien mogelijk de default configuration van de database

Vraag 6: Welke van de volgende uitspraken is GEEN OWASP best practice bij het gebruik van een externe library wat betreft security:

ANTW: Vertrouwn een libraries die al 6 maanden niet meer geüpdatet zijn

Vraag 7: Welke van volgende stappen is GEEN onderdeel van het Root Cause Analyse Process?

ANTW: Elimineer bijzaken van hoofdzaken door het systeem vanaf de grond opnieuw te installeren/configureren tot het programma zich terug voordoet

Vraag 8: Wat zijn GEEN kenmerken van Thrust Boundaries in Threat Modeling?

ANTW:

- Security-through-obscurity helpt Trust boundaries beveiligen
- De idempotentie van gegevens moet gegarandeerd blijven

Vraag 9: Wat is het belang van persistence bij het exploiten van systemen?

ANTW: Makkelijk toegang tot de systemen over een lange tijd zonder dat dit opgemerkt wordt

Vraag 10: Waarvoor kan Shodan gebruikt worden binnen Red Teaming?

ANTW: Het scannen en inventariseren van open poorten en services die publiek te vinden zijn op het internet

Vraag 11: Catalogeer volgende eigenschappen onder hun meest typische soort assigment. (A = Red Teaming, B = Vulnerability Assertment, C = Pen Test)

ANTW:

- **A**: Scope gedefnieerd door het team zelf
- **C**: Gedeeltelijke, manuele Threat Emulation
- **B**: Brede, voor gedefineerde scope, automatisch getest en eventueel manueel geverifieerd
- **A:** Simulutane systeem- en fysieke testen
- **C:** Gebruikers, developers en project team zijn op voorhand duidelijk op de hoogte van de test

Vraag 12: Welke zijn de voordelen van Threat modeling van een product VOOR het gebouwd wordt?

ANTW:

- Door je requirements onder de loop 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
- Helpt om designproblemen te detecteren voor er nog maar één lijn code is geschreven

Vraag 13: Welk van de volgende detectie methodes past bij een NIDS?

ANTW:

- Signature-based detection
- Stateful protocol analysis detection

Vraag 15: Wat betekend single Sign On?

ANTW: Dat je maar eenmaal moet aanmelden op een website en dat je de volgende keer automatisch aangemeld bent.

Vraag 16: Zet de volgende termen in de juiste volgorde naarmate het maturity model beter wordt:

ANTW:

1. Nietbestaand
2. Compliance focused
3. Awareness & gedragsverandering promotend
4. Langetermijnvisie en cultuur vverandering
5. Robuust meet framework

Vraag 17: Een van de belangrijkste punten bij Incident Response is “Protect the present”, welk zijn concrete punten hierbij?

ANTW:

- Test de systemen voor ze opnieuw in gebruik te nemen
- Herstel de systemen (indien mogelijk)
- Zet de systemen zo snel mogelijk uit om verdere schade te voorkomen

Vraag 18: Welk van onderstaande techniekne kunnen gebruikt worden bij het actie footprinten van servers?

ANTW:

- Virtual Host Detection & Enumeration
- Forward/Reverse DNS
- Web Application Discovery

Vraag 19: Duidt aan tussen welke kanalen OAuth https nodig heeft om veilig te functioneren: (A = HTTPS noodzakelijk, B = HTTPS gewenst, C = GEEN HTTPS nodig)

ANTW:

- **A**: Tussen Client en STS
- **A:** Tussen Client en API
- **A:** Tussen API en STS

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?

ANTW:

- Mitigate
- Eliminate

Vraag 21: Welk van de volgende zaken zit NIET in een OAUTH Access Token?

ANTW:

- Client Secret
- Redirect URI

Vraag 22: Welke van volgende statements i.v.m. File Systems Forensics is waar?

ANTW:

- File Carving gebruikt de magic byte om het begin en einde van een file te vinden

Vraag 23: Waarom zijn soft-skills een belangrijk onderdeel van DFIR skills?

ANTW:

- Communicatie is de key om met slachtoffers, management, klanten en exteren te praten

Vraag 24: Link de volgende cases aan de correcte ISO27001 Controls:

- De procedure die zegt dat we doorzichtige vuilniszakken moeten gebruiken -> Pyshical and Environmental security
- De procedure die het responsible disclosure programma van het bedrijf beschrijft -> Information Security Incident Management
- De procedure die de werknemers vertelt welke chat platformen ze mogen gebruiken binnen het bedrijf -> Communications security
- De procedure die de maandelijkse patch strategie van de servers omschrijft -> Operational security

- De procedure om ervoor te zorgen dat alle gebruikersaccounts (zowel intern als extern) worden afgesloten van werknemers die het bedrijf verlaten -> Human resources security
- De procedure die de backup policies van de productieomgeving van een webshop omschrijft -> Operational Security

Vraag 25: Zet de juiste term bij het juiste nummer:

- A: 6
- C: 5
- D: 4
- B: 3
- H: 2
- I: 1

Red team: Recon -> Delivery -> Exploit -> C2 -> Priv esc -> Lateral Movement -> Objective

Blue team: Gather -> Aggregate -> Analyse -> Identity -> Triage -> Investigate -> Contain