Proefexamen Security Profieldeel 2 (P2-K2)

In dit document het scenario voor het proefexamen.
Het proefexamen zal binnen 60 minuten (1 lesuur) uitgevoerd/ingeleverd moeten worden.
Dit is uiteraard heel kort in vergelijking met het examen P2-K2, deze duurt in totaal 6 uur.
Je begint echter al thuis met het maken van een deel van het proefexamen.

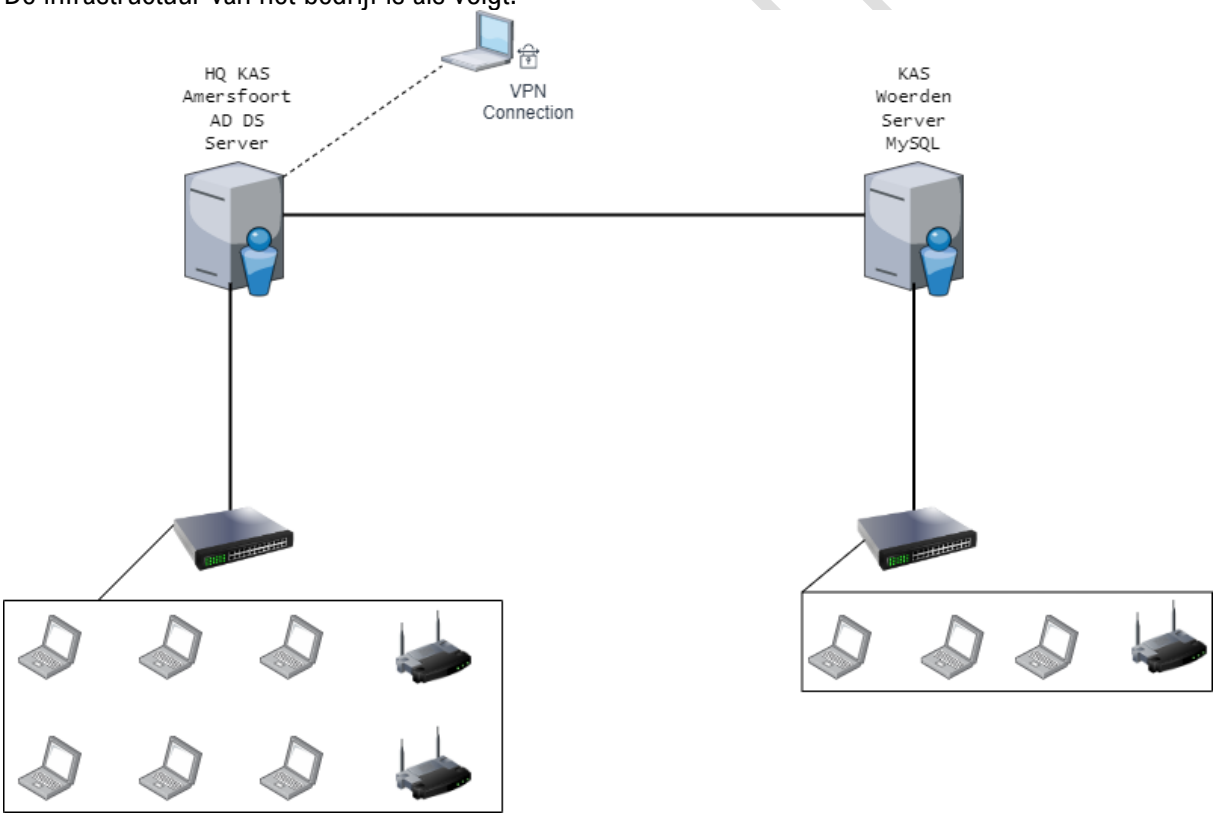
Tijdens deze proefexamen zal je per werkproces 2 essentiële onderdelen moeten uitvoeren.

Het document bevat 3 onderdelen:

1. **SCENARIO PROEFEXAMEN**
2. **OPDRACHT 1 SECURITY AUDIT**
3. **OPDRACHT 2 HERSTELLEN VAN INCIDENTEN**

1. SCENARIO PROEFEXAMEN

Bedrijf KAS (Kassa Afreken Systemen) handelt in kassa afrekensysteem en verkoopt deze aan Mkb'ers.
KAS heeft een hoofdkantoor in Amersfoort en een kantoor in Woerden.
De infrastructuur van het bedrijf is als volgt:



Op beide locaties een Server en switch.
Amersfoort: Server ADDS Domain Server.
1 Switch + 2 Wireless routers + 6 laptops
Woerden: Server gekoppeld aan Domain Server + MySQL Database
1 Switch + 1 Wireless routers + 1 laptops
De Administrator mevr. Van der Min, heeft ook een optie om via VPN in te bellen op de Server van Amersfoort

De Administrator merkt dat diverse medewerkers steeds vaker klagen over spamberichten. Er zijn medewerkers geweest die onbewust toch spambericht hebben geopend en een website bezocht hebben waardoor de device bevuilt is geraakt met een virus. Enkele medewerkers worden gewaarschuwd door de browser instellingen en andere medewerkers niet. Er zijn ook medewerkers die de waarschuwingen negeren en toch doorklikken naar de aangeven site.
De Administrator werkt 2 keer per week vanuit huis. Zij heeft aan een directe collega mr. Wengel van de afdeling Sales de rechten gegeven van Administrator mocht er het nodig zijn dat de Administrator niet beschikbaar is. Dit is overigens een besluit van de directeur.
In Woerden draait de database, de database wordt beheerd door mr. Ouwaardgee. Mr. Ouwaardgee is geen ervaren Database beheerder.

2. OPDRACHT 1 SECURITY AUDIT

De firma KAS heeft aan jou gevraagd om een security audit uit te voeren. Er zijn diverse reden voor verzoek, onder andere de groei van het bedrijf.
Voorafgaande aan de fysieke audit heb je een aantal medewerkers geïnterviewd. Lees onderaan de opdracht de vragen en antwoorden.

2.1 Tools gebruiken

Je dient de volgende tools te gebruiken (op je eigen VM Windows 10):

1. Sysinternals > tool Proces checker
   Je scant je eigen pc met deze tool en je gebruik de minimale filters om diverse processen bloot te leggen.
   Je levert een printscreen waarin duidelijk te zien:
   a. Welke filters je gebruikt hebt
   b. De processen die niet gefilterd konden worden door de tool
   DEZE OPDRACHT DOE JE THUIS
2. MBSA-tool.
   Beschrijf na de scan met MBSA wat de aandachtspunten zijn.
   DEZE OPDRACHT DOE JE THUIS
3. NMAP.
   Scan voor alle openstaande poorten in je VM. Benoem minimaal 2 willekeurige poortnummer die Open staan, voor welke protocol/programma deze 2 poorten worden gebruikt. Je mag poort 443, 80, 465, 587, 25 en poort 53 niet benoemen.
   DEZE OPDRACHT DOE JE THUIS
4. Gebruik ook de ingebouwde tools binnen Microsoft. Zoals de virusscanner en Firewall

2.2 Firewall log analyseren

Zie in bijlage 1, op bladzijde 1 en 2 een uitsnede van een Firewall-log. Bekijk of er vreemde zaken te zien zijn in de log. Denk hierbij aan aantal bytes Send/verzonden naar een niet IP-adres binnen het netwerk. Het bedrijfsnetwerk is 172.16.x.
DEZE OPDRACHT DOE JE THUIS

2.3 Analyseer de interviews en geef advies

Zie bijlage 1, Interview. De database beheerder mr. Ouwaardgee is geïnterviewd door een collega van jou. Deze collega helpt jou bij de security audit. Lees de antwoorden van mr. Ouwaardgee.
Maak een overzicht van de niet gewenste handelingen beschrijf hierbij wat de gevolgen zijn als zij er geen verandering zal plaats vinden.
Maak ook een adviesrapport om de niet gewenste handelingen te stoppen. Je beschrijft duidelijk wat er aangepast dient te worden. Als er technische handelingen aangebracht moeten worden dan vermeld je stap voor stap hoe dit doorgevoerd moet worden.
DEZE OPDRACHT DOE JE THUIS

2.4 Risicomatrix

Je neemt 3 afwijkingen die je gevonden hebt tijdens opdracht 2.1 t/m 2.3 en vermeld deze in een risicomatrix. Onderbouw je keuze in de risicomatrix.

Zie bijlage 1 om de risico matrix in te vullen

3. OPDRACHT 2 HERSTELLEN VAN INCIDENTEN

Er is sprake van een datalek! Je hebt bij opdracht 2 een aantal externe tools gebruikt en de ingebouwde tools binnen Microsoft.
Na een full scan met de virusscanner van MS Defender is er gebleken dat de server is besmet met een RAT tool (Remote Acces Tool). Hiermee kan een Hacker op afstand in de server inloggen.
Tijdens de scan met een van de tools, is het ook gebleken dat er sprake is van de standaard inlog op de server.
Blijkbaar heeft de Hacker ingelogd op de database en data gestolen uit de database.
Je gaat een aantal zwakheden die jij hopelijk hebt gevonden bij opdracht 2 oplossen.

3.1. Hoe kon het gebeuren dat er nu sprake is van een data(base)lek?
In bijlage 1 heb je een uitsnede van een database log. Vind in de log de database lek.
   a. Maak een printscreen van de databaselek (zie bijlage 1).
   b. Welke zwakheden hebben geleid dat dit kon gebeuren?
   c. Benoem het risiconiveau elk van de zwakheden.
      (Geen risicomatrix, slechts een goede onderbouwing)
   d. Om welke informatie zou het concreet gaan en hoe groot is de datalek?
   e. Vind op je eigen database de logfile, map: C:\ProgramData\MySQL\MySQL Server 8.0\Data.
      Maak een printscreen van deze map.

3.2. Communiceren van de datalek.
Je bent gevraagd om de datalek te onderzoeken. Na het afronden van je onderzoek heb je informatie die je dient te delen met de opdrachtgever, de firma KAS. Hoe communiceer je en aan wie? Communiceer conform AVG-wetgeving.
In bijlage 1 vind je een communicatiematrix, vul deze in. Aan wie communiceer je wel/niet over de datalek?

3.3. Oplossen van zwakheden.
Je hebt tijdens opdracht 2, diverse scans uitgevoerd met diverse tools en dit zijn de zwakheden die je o.a. hebt gevonden. Zie hieronder een lijst met afwijkingen/zwakheden.
Geef in tekst en printsceens aan hoe je de gevonden zwakheden zou oplossen/verwijderen.
Ook al zijn de 6 zwakheden die hieronder kunt lezen niet gevonden tijdens opdracht 2.
a. Een Remote Access tool is geïnstalleerd en actief waardoor toegang tot de Database server.
b. Het Root Password van MySQL is root, hierdoor kan iedereen in de server.
c. De Firewall is uit.
d. Er is geen sterk wachtwoord afgedwongen in de database.
e. Anti-Virus is uit.
f. Er is een virus gevonden

Vermeld duidelijk wat de stappen zijn die je gaat uitvoeren. (tijdens het echte examen zal je de zwakheden eerst moeten lokaliseren, dat hoeft bij deze opdracht niet)