Ik heb deze praktijkexamen gemaakt op mijn eigen laptop zodat er gezien kan worden dat dit mijn eigen laptop is en ik niet screenshots gefraudeerd heb. Ook deed mijn laptop soms een beetje traag/hangend voor geen verklaarbare/aanzienlijke redenen. Vandaar dat ik het op deze manier doe.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

**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

Afbeelding met tafel

Automatisch gegenereerde beschrijving

Hier is mijn naam te zien als bewijs:

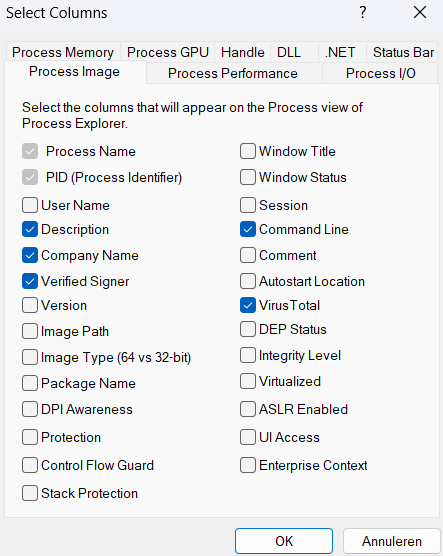
Afbeelding met tekst, computer, computer, zwart

Automatisch gegenereerde beschrijving

F**eedback sysinternals**

**Vermeld niet alleen een screenshot maar ook teksten als:**

**'na gebruik van Sysinternal zijnv lees hieronder de processen die niet gekoppeld konden worden aan een filter"**



**2. MBSA-tool.**  
Beschrijf na de scan met MBSA wat de aandachtspunten zijn.

Mijn laptop voert automatisch geen updates uit, dus als ik het zelf niet doe voor een bepaalde tijd dan kan dat gevolgen hebben aangezien het systeem van mijn device dan verouderd is en het dan makkelijker te kraken heeft. Ook verloopt mijn wachtwoord nooit, of eigenlijk alle wachtwoorden en dat kan ook een risico zijn als ik het nooit om de zoveel tijd een update geef.

**Feedback je kon dit ook doen op een VM die als het goed is hebt geisntaleerd.**

**In ieder geval ook dat had je als volgt moeten melden:**

**'Afwijkingen na gebruik tool MBSA:**

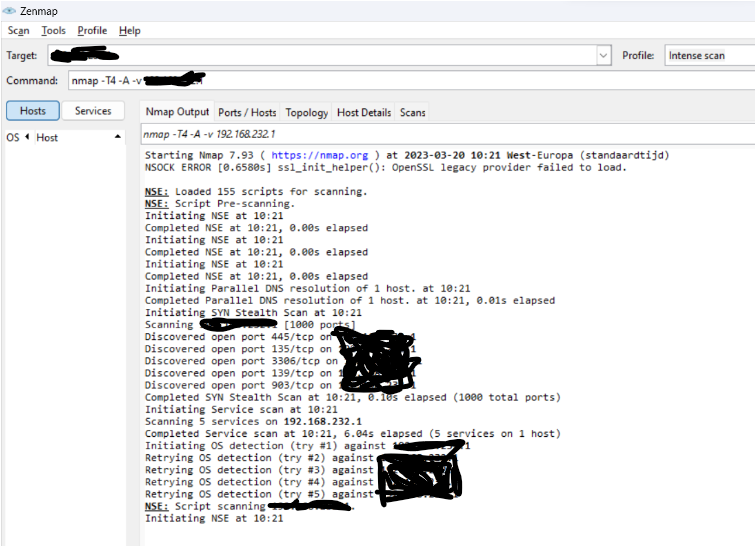
**afwijking 1**

**afwijking 2**

**etc'**

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.



Afbeelding met tekst

Automatisch gegenereerde beschrijving

Poort 135, 139, 445, 903, 3305/TCP staan allemaal op Open. Ik zie dat 903 de port van de VMware is die op mijn laptop draait in de background. Uit mijn kennis weet ik dat port 445 normaal is als het open staat en dat port 135 potentieel een risico kan zijn en dat er een externe partij is die remote spionage uitvoert en op mijn device kan meekijken. Dat is omdat port 135 op Open staat. Poort 139 representeert de communicatie van Endpoints. Het wordt gebruikt voor file sharing etc. Dit kan ook gevaarlijk zijn omdat dit de risico geeft dat de hard disk van mijn device exposed wordt aan hackers. Dit kan een serieus probleem zijn als ik bijvoorbeeld administratierechten heb met gevoelige documenten en informatie of erger: Als ik deze laptop gebruik voor een organisatie en er dus veel op deze laptop staat.

**Feedback nmap:**

**Heel veel tekst, inhoudelijk wel prima, maar ook dit vermeld als als volgt:**

**Na gebruik van NMAP zijn dit de poorten die open staan en de poorten die direct gesloten moeten worden**

**Poortnummer**

**Poortnummer**

DEZE OPDRACHT DOE JE THUIS

**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.

Ik zie bijvoorbeeld al dat er bytes zijn verzonden aan of ontvangen zijn van meerdere verschillende netwerken. Een aantal voorbeelden zijn 202.12.27.33192.203.230.10192.228.79.201192.36.148.17.

Zelf vind ik dit ook een beetje raar:

Afbeelding met tekst, brief

Automatisch gegenereerde beschrijving

Het Internet Control Message Protocol is een onderdeel van het Internetprotocol wat wordt gebruikt door besturingssystemen voor het sturen van foutmeldingen, bijvoorbeeld om te melden dat een bepaalde netwerkvoorziening niet beschikbaar is, of dat een bepaalde host of router niet bereikbaar is. Dit staat er een paar keer in. Het kan zijn dat het normaal is, maar het lijkt me vreemd dat het naar die unreachable IP-adressen worden gestuurd dat buiten het reachable netwerk is.

**Feedback:**

**Wat is je analyse nou precies na doorlopen van de log? Er is niets verzonden dat heb ik bewust gedaan. Ook hier vermeld je het als volgt:**

**Mijn conclusie na het analyseren van de firewall log:**

**(wel/niet te zien dat er sprake is van een datalek)**

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.

**2. Interview Mr. Ouwaardgee**  
Vraag 1: Hoe lang werkt u voor KAS?  
Antwoord: Bijna 4 maanden, ik ben begonnen als stage, student van het ROCvA en mocht na mijn afstuderen hier blijven.  
Vraag 2: Bent u de enige Databasebeheerder?  
Antwoord: Ja  
Vraag 3: Vind u het ook belangrijk dat een security Audit uitgevoerd door ons zal worden?  
Antwoord: Ja, ik heb zelf niet heel veel kennis van Database security, want vaak denk ik dat er iets aan de hand is met de Database Server.  
Vraag 4: Ohw, hoe vaak en waarom denkt u dat?  
Antwoord: Ik ben de enige die in de database kan, maar ik heb al 2 keer gezien dat er toch query’s zijn uitgedraaid terwijl ik dat niet heb gedaan.  
Vraag 5: Weet u zeker dat u de enige bent die in de database kan inloggen?  
Antwoord: Ja, ik ben wel de enige, echter vanwege personeelstekort heb ik het wachtwoord niet aangepast, mocht ik een keer ziek raken dan kan als nog mijn college de database in.  
Vraag 6: Misschien heeft je collega wel die query’s uitgedraaid?  
Antwoord: Nee, wij hebben afgesproken als hij in de database moet inloggen dat het altijd gemeld moet worden. En dat is de afgelopen 3 maanden niet het geval geweest.  
Vraag 7: Wat voor gegevens zijn te vinden in jullie database?  
Antwoord: NAW Klantgegevens, welke product zij bij ons hebben ingekocht, welke diensten afgenomen zijn, etc.  
Vraag 8: Die Query’s die jij niet kan plaatsen, maar jij toch wel terug kan zien in de database log. Wat bevatten die Query’s aan informatie?  
Antwoord: Het lijkt wel een dump van de database met gegevens van onze klanten.  
Vraag 9: Weet je ook hoeveel records er dan opgevraagd zijn uit de database?  
Antwoord: Ja, in de log is dat terug te zien.  
Vraag 10: Heb je dit wel vermeld aan je leidinggevende.  
Antwoord: Nee, ik heb die uitdraai niet gemaakt dus niet mijn fout.  
Vraag 11: Wat nou als het hier gaat om hack en bedrijfsdata dat weggelekt is naar externe partijen?  
Antwoord: Ja lastig..

Bij de antwoord van vraag 3, het zou wel zo handig zijn als meneer Ouwaardgee meer kennis had over Database security

Bij de antwoord van vraag 4 zou het alsnog wel slim zijn om de standaard wachtwoord aan te passen, stel nou dat het nog ergens te vinden is. Gewoon voor de zekerheid zou het aangepast kunnen worden.

Bij vraag 5-6 kan het zijn dat de collega alsnog zonder te melden in SQL is gekomen en misschien wel queries heeft aangepast. Een oplossing zou kunnen zijn om altijd de wachtwoord te veranderen, zodat de collega zeker wel contact op moet nemen om in te loggen. Dan heeft hij namelijk geen keus en kan er heel goed teruggedacht worden hoe die queries zijn aangepast.

Bij vraag 8-11, altijd moet er goed gecommuniceerd worden en vooral binnen de ICT. Ook zal er feller moeten worden gedenkt worden.

**FeedbACK:**

**Je bevindingen zijn ook maar ook hier graag iets netter vermelden:**

**'Na interview zijn dit mijn bevindigen:**

**1:**

**2:**

**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

Afbeelding met tekst

Automatisch gegenereerde beschrijving

1. Alle processen in het groen en paars zijn normale processen, niks aan de hand.
2. Medewerkers die spamberichten krijgen moeten les krijgen over malware en de risico’s. Het zou basiskennis moeten zijn dat je niet op linkjes in spamberichten klikt want dit kan best wel een impact hebben.
3. Mijn laptop voert automatisch geen updates uit, dus als ik het zelf niet doe voor een bepaalde tijd dan kan dat gevolgen hebben aangezien het systeem van mijn device dan verouderd is en het dan makkelijker te kraken heeft. De risico is er altijd en de schade zal niet aangenaam zijn!
4. Ook verloopt mijn wachtwoord nooit, of eigenlijk alle wachtwoorden en dat kan ook een risico zijn als ik het nooit om de zoveel tijd een update geef. De risico is er altijd en de schade zal niet aangenaam zijn!
5. Uit mijn kennis weet ik dat port 135 potentieel een risico kan zijn en dat er een externe partij is die remote spionage uitvoert en op mijn device kan meekijken. Dat is omdat port 135 op Open staat. De kans is mogelijk, maar de schade kan groot zijn!
6. Poort 139 representeert de communicatie van Endpoints. Het wordt gebruikt voor file sharing etc. Dit kan ook gevaarlijk zijn omdat dit de risico geeft dat de hard disk van mijn device exposed wordt aan hackers. Dit kan een serieus probleem zijn als ik bijvoorbeeld administratierechten heb met gevoelige documenten en informatie of erger: Als ik deze laptop gebruik voor een organisatie en er dus veel op deze laptop staat. De risico is mogelijk, maar de schade kan enorm zijn!
7. Van de eerste scan, zelfde als antwoord 1 & 2, als er iets in het rood staat hoeft er niet per se iets ergs aan de hand te zijn. Als er 0/73 bijvoorbeeld staat dan is het prima, wel is er iets aan de hand als er dan meer dan 0 staat zoals 1/73. Het kan pas zijn dat de malware ofzo pas geactiveerd wordt als je er op klikt of het probeert te openen. Je kunt het ook weghalen met de tool zelf, VirusTotal.
8. Ik zie bijvoorbeeld al dat er bytes zijn verzonden aan of ontvangen zijn van meerdere verschillende netwerken. Een aantal voorbeelden zijn 202.12.27.33192.203.230.10192.228.79.201192.36.148.17. Dit kan een probleem zijn. Stel nou dat er iemand voor gezorgd heeft de bytes expres naar die adressen zijn gestuurd. Dit runt ook op background, niet veel mensen snappen wat er gebeurd maar echte ICT-experts zouden het zo kunnen manipuleren en hun kennis gebruiken op het slechte pad. Het kan zijn dat er gevoelige informatie naar die IP-adressen gestuurd worden. Ook als het door security kan worden gevonden, hoeft de locatie van de IP-adressen niet bijvoorbeeld het schuilplaats van de manipulator te zijn, maar kan het ook zijn dat hij/zij het gewoon ergens in een ander gebouw heeft gebruikt als tussenstop om de informatie op te halen en dan om sporen uit te wissen.
9. Het Internet Control Message Protocol is een onderdeel van het Internetprotocol wat wordt gebruikt door besturingssystemen voor het sturen van foutmeldingen, bijvoorbeeld om te melden dat een bepaalde netwerkvoorziening niet beschikbaar is, of dat een bepaalde host of router niet bereikbaar is. Dit staat er een paar keer in. Het kan zijn dat het normaal is, maar het lijkt me vreemd dat het naar die unreachable IP-adressen worden gestuurd dat buiten het reachable netwerk is.

Afbeelding met diagram

Automatisch gegenereerde beschrijving

Feedback:

Je geeft een prima optellingen van de zaken die jehebt gevonden.

Alleen onderbouw je niet echt je keuze in de matrix:

Doe het als volgt:

Onderbouwing afwijking 1 KANS: (hier je text)

Onderbouwing afwijking 1 IMPACT: (hier je text)