**P2-K2 Examenvoorbereiding/samenvatting**

**Naam: Ervin Klas: OITITO0E**

**Uitleg over het examen W1 en W2**

**W1: Geeft securityadvies en verbetert**

**Op het examen ga je een Security Audit/Jaarlijks check up uitvoeren. Jij moet na het houden van interviews met medewerkers, het scannen van de systemen met de juiste tools een auditrapport opleveren.**

**W2: Reageert op securityincidenten**

**Na een Security incident, de situatie analyseren, hoe heeft dit kunnen gebeuren, hoe beperkt je de schade, etc.**

**Omgeving waarin je werkt tijdens het examen**

**Je gaat met deze omgevingen werken tijdens het examen:**

* **Windows Server 2016 met de volgende rollen:**

**ADDS, DNS, File&storage**

* **Windows Server 2016 met SQL Server MYSQL geïnstalleerd**
* **En 3x client pc’s geïnstalleerd met Windows 10.**

**Onder heb ik een screenshot gezet over de omgeving waarin we gaan werken.**

**Afbeelding met schermopname, lijn, diagram, ontwerp

Automatisch gegenereerde beschrijving**

**W1: Geeft securityadvies en verbetert**

**Een security audit is een uitgebreid overzicht van de IT-infrastructuur van een bedrijf. Het geeft een overzicht of alle verplichte regels en regelgevingen zijn doorgevoerd en worden gehanteerd.**

**Opdracht 1**

**Wat moet een bank aan voldoen?**

**Noem er 3 op:**

**Security, Privacy wet en Verzekering**

**Opdracht 2**

**Zoek op het internet en vind minimaal 3 regels waaraan het MBO moet voldoen. Vermeld ook wie (bedrijf/organisatie) is die regels het MBO heeft opgelegd.**

**Antwoord:**

**Gegevens van studenten en docenten moeten beveiligd zijn in de database.**

**Lespannen moeten goed zijn en school contract.**

**Opdracht 3**

**Stel minimaal 10 vragen aan mensen die ergens werkzaam zijn zoals op school, bank, etc.**

**De vragen die jij moet bedenken moeten jou een beeld geven over regels die zijn moeten hanteren, Hierdoor krijg je een betere beeld dat bijna alle organisaties wel regels van buitenaf als zowel interne regels moeten naleven.**

**Hieronder ga ik de vragen zetten wat ik had gemaakt voor deze opdracht.**

**Rood is het antwoord!**

1. **Hoe zij omgaan met data van studenten/klanten**

**Geen privacywetgeving gehanteerd**

1. **Is er een 4 ogen beleid, aangezien medewerkers diverse zaken kunnen aanpassen in het leerlingvolgsysteem/banksysteem?**

**Nee**

1. **Bezoeken zij ook sites die niets te maken heeft met de dagelijkse werkzaamheden?**

**Jazeker**

1. **Achterhaal of er dan niet veilige sites bezocht worden, (stel de juiste vraag) http doen wij**
2. **Hoe laten zij hun werkplek achter, als zij iets moeten doen buiten de vaste werkplek. Etc.?**

**Niet geen clean desk policy. W+L doen om de laptop op lock te zetten.**

1. **Krijgen de studenten de juiste stof/leermiddelen voor hun opleiding**

**Ja, de studenten hebben recht daarop en staat ook in hun school contract**

1. **Is er binnen een mbo school een goeie beveiliging aan security?**

**Ja, er is een team die ervoor zorgt dat alles beveiligd is en in orde is.**

1. **Zijn er bedrijven in Nederland die ook gewoon kwetsbaar kunnen zijn?**

**Ja, dat zijn met een paar applicaties zoals Adobe en magento want hun bieden bedrijven aan webshops en dat kan gevaar opbrengen voor de mensen die adobe en magento gebruiken. Gevoelige informatie zoals wachtwoorden etc.**

1. **Is het software van bedrijven in Nederland in orde?**

**Ja en nee, goed dat ze een bijv. de nieuwste software hebben maar het kan leiden naar gaten in hun software omdat er nieuwe mogelijkheden komen voor hackers zoals jouw gegevens etc.**

1. **Zijn de cookies die je meestal ziet bij websites wel betrouwbaar?**

**Nee niet altijd de cookies tracken je eigenlijk wel voor persoonsgegevens maar ook als je naar websites of naar YouTube kijkt. Blijven dezelfde cookies jouw tracken met dezelfde reclames/advertenties.**

**Opdracht 4**

**Observeer de Administrator**

Lees de informatie in document Examenvoorbereiding en vermeld in het kort maar duidelijk wat de gevaren zijn (je rapporteert aan de directeur)

Beste bestuurder,

Hierbij wil ik u meegeven wat de consequenties zijn van u devices.

**Consequentie 1:** De noodzakelijk is dat ze data kunnen erachter halen bij e devices en dan ook uit de mail. Want de toegang is niet beveiligd.

**Consequentie 2:** de toegang is niet beveiligd van de servers, andere mensen ook wel hackers etc. kunnen makkelijk een virus opzetten etc. wat de servers en devices het niet meer goed.

Met deze consequenties wil ik u adviseren om beter op te letten met uw servers en devices. En ook dat het nu duidelijk is wat het gevaar is.

Met vriendelijke groet,

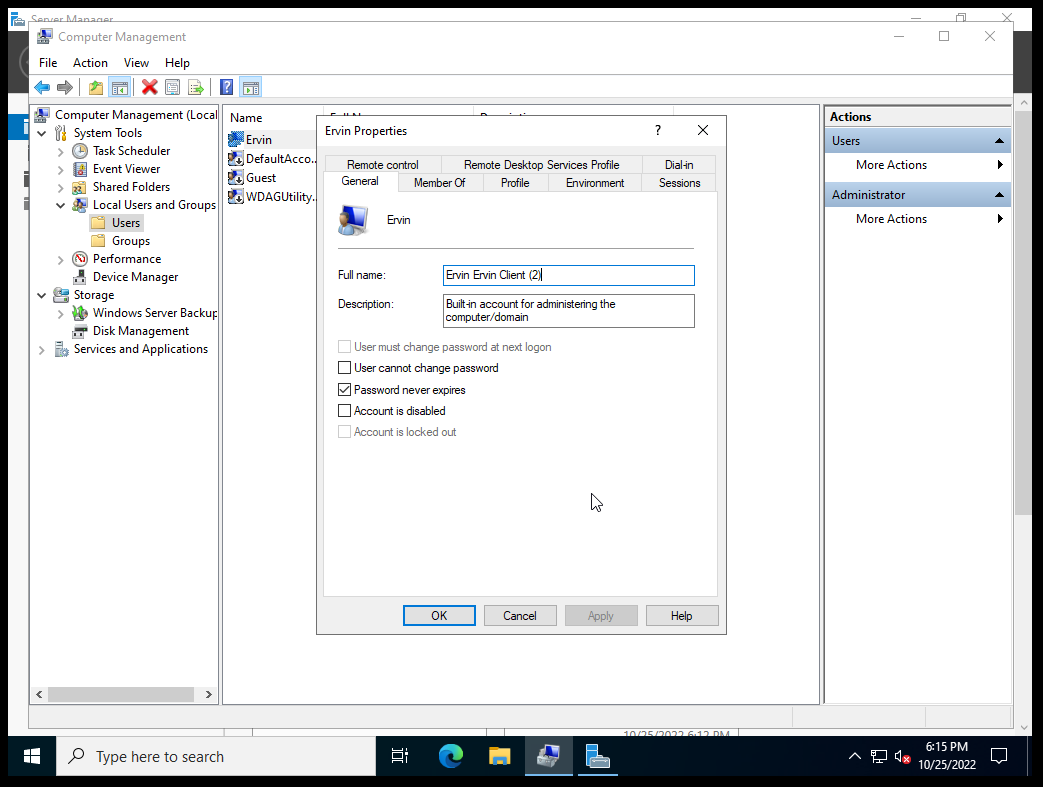
ICT team Amsterdam

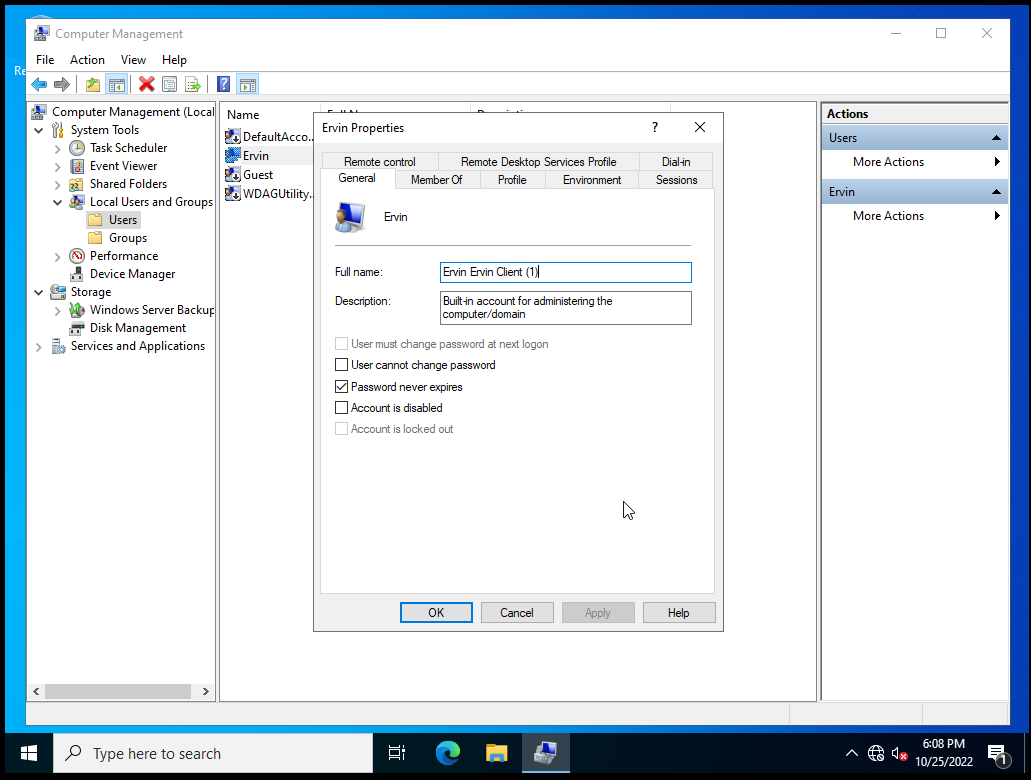
**Opdracht 5**

**Installeer 2 servers en 3 clients en router. Lever screendumps. Deze moeten minimaal bevatten, bij elke screendump dat het bewijs uit jouw pc is!**

**Client 1 t/m 3**

**Het kan zijn dat we dit niet hoeven te doen tijdens het examen vanwege dat we de VMS al hebben. Maar als dat niet het geval is komt dit goed van pas.**

****

****

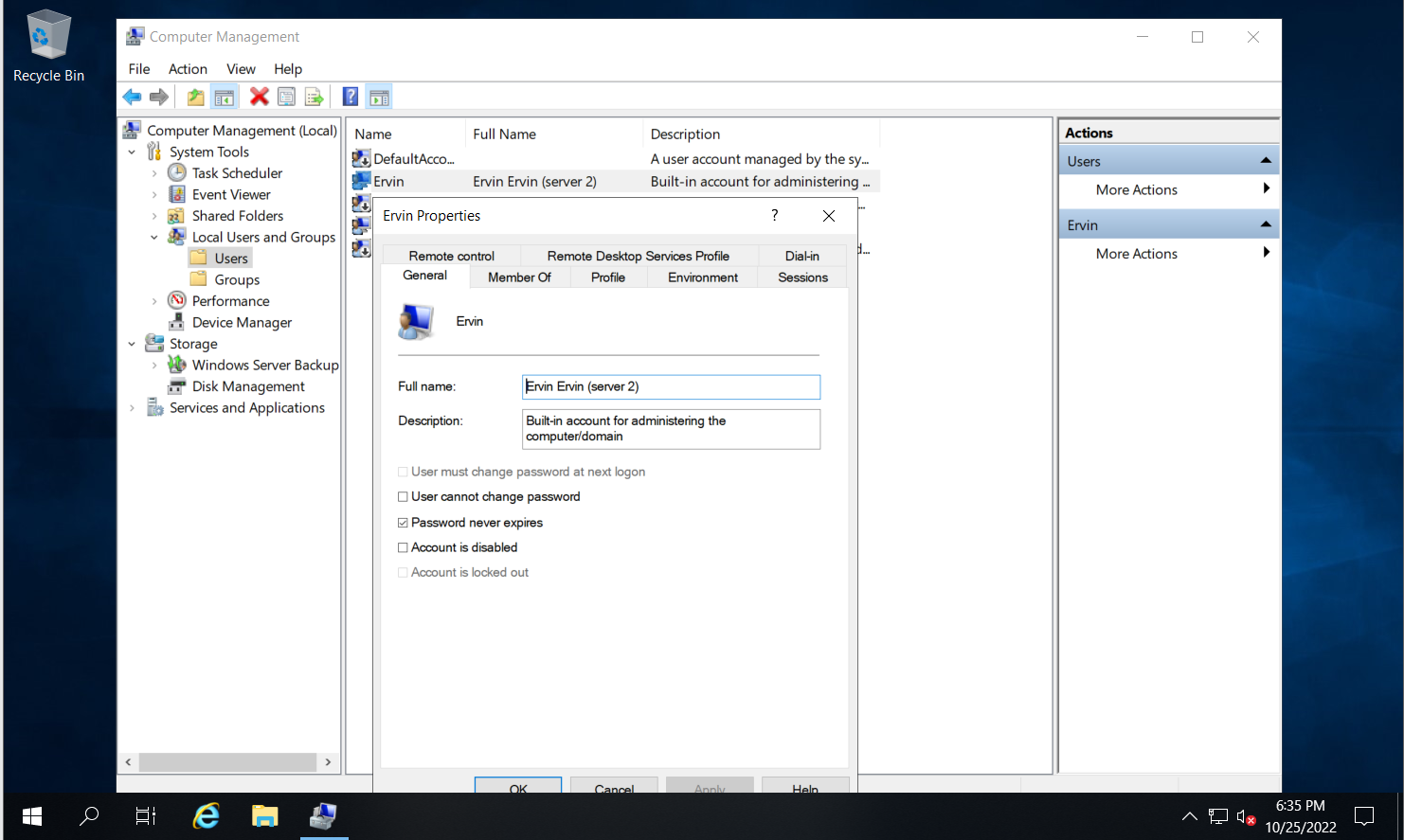
Afbeelding met tekst

Automatisch gegenereerde beschrijving

**Server 1 en 2**

Afbeelding met tekst

Automatisch gegenereerde beschrijving



**Router**

Afbeelding met tekst

Automatisch gegenereerde beschrijving

**W2: Reageert op securityincidenten**

**Opdracht 6:**

**Tools voor scannen network**

**Sysinternal Tools Suite**

**Onderdeel: proceexp**

**Process Explorer gebruik om Malware te ontdekken**

**Herkenbare zaken m.b.t (met betrekking tot) Malware**

**Geen (meestal) geen Discription en Company name**

**Voorbeeld:**

**2 processen van Google, bij Chrome en Drive zie je een Discription staan een Company nam.**

**Als je de kolommen aanpast (rechtermuis op een kolom> kies voor Select Colomms > kies voor Verify Image Signatures. Of ga naar Options en kies voor Verify Image Signatures. Dit laat zien welke applicaties/processen van bedrijven een certificaat hebben. Deze certificaat is meestal uitgegeven door een derde partij. Of door bijvoorbeeld Microsoft die goedkeuring (certificaat) heeft gegeven aan een partij waarvan de software geïnstalleerd mag worden op een Microsoft OS/platform. VirusTotal voor het checken van de Hashwaarde van een proces. Met VirusTotal kan je ook checken of een proces of bestand de juiste hash waarde bevat. VirusTotal check of je een hashwaarde niet ergens is geflaged als suspicious /verdacht. Om VirusTotal te activeren in Proces Explorer, ga op een proces staan met een Discription en Company name > rechtermuis > kies Check VirusTotal**

**Vinden, waarvandaan een proces is opgestart Om erachter te komen waarvandaan een proces is opgestart. Kies Select Columms > Selecteer Command Line Je ziet nu waar een proces is opgestart**

**Checken of een file verbinding maakt naar buiten Om erachter te komen of een file verbinding maakt naar buiten. Ga naar de verdachte proces > rechtermuis > kies voor Properties > kies voor Tabblad TCP/IP In dit overzicht zie naar welke IP adress je applicatie verbinding heeft gemaakt. Voer deze stap ook uit met een Webbrowser om het verschil te zien.**

**Welke bestanden (DLL) zijn geassocieerd met een proces.1/2 Kies een bestand > druk de Control key en de letter H. Je ziet alle bestanden die verbonden zijn met je proces. DLL = Dynamic-link library DLL zijn codes uit diverse applicaties, die gebruikt kunnen worden voor meerdere programma’s. Deze codes staan in een Libary en kunnen bijvoorbeeld gebruikt worden voor MS Words, en tegelijk voor Excel. Deze codes worden dan in het geheugen geplaatst. Een applicatie kan dus bij het opstarten en gebruik van de applicatie een verzoek doen voor DLL (codes) uit de Libary. Bijvoorbeeld deze DLL-file comdllg32.dll zorgt ervoor dat een applicatie een venster kan openen met daarin een bericht. Diezelfde dll bestand kan ook een andere applicatie gebruiken voor bijvoorbeeld het weergeven van foutmelding.**

**Welke bestanden (DLL) zijn geassocieerd met een proces.2/2 Selecteer een proces > Kies Properties > Ga naar tabblad Image. In dit overzicht kan je o.a. het pad zien.**

**Opdracht 7: Nmap**

**Scannen van website + Toploly + aantal poorten gescand en hoeveel open/Closed**

**Target ip adres, vul in Target het IP-adres**

**Nmap -T4 – A v 192.168.2. \***

**nmap – F (snelle scan op top 100 poorten) -Pn (niet alle ip adressen pingen alleen de online) – n (geen reverse lookup)**

**Eigen scan maken en opslaan met ip scan in target : 192.168.2.0./24**

**Rapporten opslaan en vergelijk**

**Gebruik deze instructies op het examens!**

**Opdracht 8: Risicomatrix**

**Gebruik de risicomatrix om de risico’s aan te geven. Gebruik 3 problemen die je hebt genoteerd. En verwerk deze in de risicomatrix.**

**Hieronder de risicomatrix.**

**Afbeelding met Rechthoek

Automatisch gegenereerde beschrijving**

**Op het examen moet je de risicomatrix invullen:**

**Onderbouwing afwijking 1 KANS: (vul hier je tekst in)**

**Onderbouwing afwijking 1 Impact: (vul hier je tekst in)**

**Voorbeeld hoe ik het had gedaan op mijn proefexamen**

**1 Afwijking: een beschrijving van het gevonden issue**

**MBSA Tool: Computer name, security update, Incomplete updates, Password expiration.**

**a Details van het Issue:  Naam van de computer staat niet goed of te wel geen naam, Updates van security en andere updates is nog niet up-to-date en nog niet beveiligd, Password is al over datum**

**b Conclusie met impact: Deze dingen kunnen gevaar brengen. Want als deze dingen niet goed staan in het systeem kan een hacker/crimineel makkelijk in het computer/pc komen.**

**Probeer dit te doen maar op de manier hoe ik het boven hebt uitgelegd. Als we het anders doen tijdens het examen wordt dit misschien niet goed gekeurd!**

Tools

Een aantal standaard tools voor het scannen van systemen:

* Antivirus (MS Defender)
* Performance Monitor (cmd: permon/report)

Tools die je tijdens het examen moet beheren:

* Nmap/Zenmap
* MBSA
* SystinternalSuite

Deze tools gebruiken tijdens het examens!