

POP Project

Academic year 2021-2022

Technology  
Elektronics-ICT / Applied informatics

CAMPUS

Geel

Tiziano Van der Waals 1ITF-3

r0889630

Thomas More Kempen

Voorwoord

Recent is een hacker groep bezig geweest met data van grote bedrijven te stelen. Een van de bedrijven die ze hebben gehackt is Nvidia. Nvidia is een van de grootste verkopers van grafische kaarten en produceert hiervoor ook drivers. In de hack zijn veel dingen gestolen, zoals de plannen voor de opkomende 40-series kaarten, maar ook driver signatures. Kwaadaardige mensen kunnen deze signatures gebruiken om hun RAT’s, ransomware of andere virussen te laten lijken op een legitiem programma. Hier is waar mijn project over gaat. De bedoeling is dat elke keer als er iets wordt gedownload op een computer, er een Windows Defender scan wordt gerund. Als er dan iets mis blijkt te zijn moet er een message worden gestuurd naar een andere pc via remote PowerShell.

Inhoud

[Voorwoord 3](#_Toc104146859)

[1 Drivers 5](#_Toc104146860)

[1.1 Wat zijn drivers? 5](#_Toc104146861)

[1.2 Driver signatures 5](#_Toc104146862)

[1.3 Vervallen signatures 5](#_Toc104146863)

[2 Windows Defender 6](#_Toc104146864)

# Drivers

## Wat zijn drivers?

Drivers zijn programma’s op je computer die ervoor kunnen zorgen dat bepaalde hardware, denk aan je toetsenbord of muis, kunnen communiceren met je besturingssysteem. Als je een nieuw apparaat aansluit op je computer, zal je besturingssysteem automatisch zoeken naar gepaste drivers om te downloaden en gebruiken. (Device driver, 2022) Windows doet dit via Windows Update en gebruikt hiervoor hun eigen database met signed drivers. (Mutahar, 2022)

## Driver signatures

Elke driver die wordt gemaakt, moet een driver signature hebben. Deze signature is een soort identifier voor die driver, wie de maker is van de driver, wanneer de driver vervalt, etc. (Cymoki & tedhudek, 2021) In de Nvidia hack zijn ook oude driver signatures gestolen (Constantin, 2022), mensen die kwade plannen hebben kunnen deze signatures gebruiken om hun programma’s echt te laten lijken.

## Vervallen signatures

Omdat Microsoft altijd heel er veel belang zette op backwards compatibility van devices, laat Windows het toe om vervallen signatures te blijven gebruiken, en ziet deze dus ook als legitiem. (Mutahar, 2022) De gestolen Nvidia signatures zijn verlopen, maar omdat Windows deze dus nog toelaat, kunnen kwadaardige mensen nog steeds gebruik maken van deze signatures om hun programma echt te laten lijken. (Constantin, 2022) Dit is waarom het zo’n gevaar is om die oude signatures kwijt te zijn.

# Windows Defender

## Wat is Defender?

Windows Defender is de standaard antivirus oplossing van Microsoft. Defender staat na automatisch op je systeem nadat je Windows hebt geïnstalleerd. (Defender, n.d.) Veel mensen denken dat Defender een slechte antivirus scanner is, maar eigenlijk is deze heel goed. Dit is omdat Microsoft alle data van Defender krijgt. Als Defender een virus vindt dat nog niet eerder is gezien, weet Microsoft dit meteen, wordt hun database van gekende virussen geupdate, en elk ander systeem met Windows weet dan ook meteen dat het een virus is.

# PowerShell

## Remoting

PowerShell is de shell omgeving van Windows en kan worden gebruikt om verschillende commando’s uit te voeren. Er zijn veel verschillende dingen die je ermee kan doen, en een van die dingen is remoting. Remoting kan worden gebruikt om vanaf een bepaalde pc, commando’s uit te kunnen voeren op een andere pc (sdwheeler, chasewilson, & nschonni, 2021).

## Defender met PowerShell

We hebben net al gesproken over Defender. In PowerShell zijn er verschillende commands die je kan uitvoeren die bepaalde functies van Defender kunnen oproepen, een zo’n voorbeeld is Start-MpScan cmdlet. Deze cmdlet zorgt ervoor dat Defender een scan uitvoert op je systeem, standaard is dit een quick scan, maar je kan met de flag -ScanType specifieren of je een quick, full of zelfs custom scan op een bepaald pad wilt uitvoeren. (Defender, n.d.)

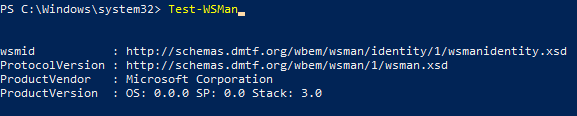
# Uitvoering van het project

## Virtuele machine’s

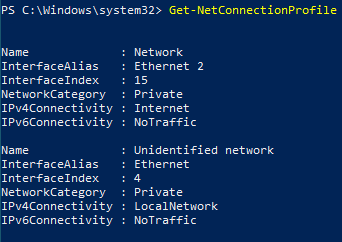
Als eerste stap om mijn project uit te voeren heb ik twee virtuele machine’s aangemaakt die beide deel uitmaken van een intern netwerk, ik heb de machines ook nog een tweede netwerkkaart gegeven om verbinding te kunnen maken met internet. Ik heb beide pc’s een static IP gegeven.

### Remote PowerShell

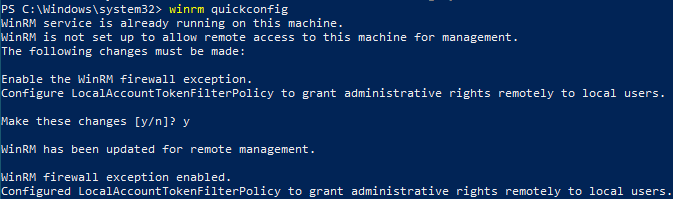
Om Remote PowerShell te gebruiken, is het nodig om te kijken of de service voor Remoting op het systeem staat, hiervoor heb ik de Test-WSMan cmdlet gebruikt.



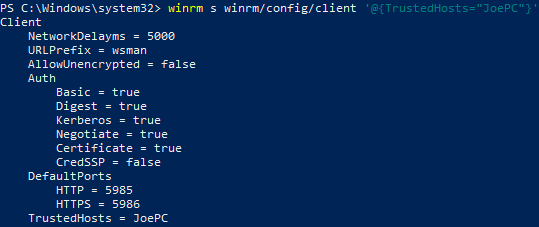
Voor veiligheidsredenen, is het niet mogelijk te remoten op een publiek netwerk, het is daarom van belang dat we kijken of onze netwerken prive zijn. Om te kijken of dit is ingesteld in Windows gebruiken we de Get‑NetConnectionProfile cmdlet. Als ze niet al op Private stonden, hadden we de Set-NetConnectionProfile cmdlet kunnen gebruiken om deze te veranderen.



De volgende stap is om winrm te configureren, dit is de Windows Remoting command. Voor een simpele configuratie runnen we winrm quickconfig



Om nu een computer toe te voegen als vertrouwde pc, moeten we deze toevoegen aan de lijst van TrustedHosts dit doen we met winrm s winrm/config/client ‘@{TrustedHosts=”[pc-naam]”}’. Aangezien mijn tweede pc ‘JoePC’ heet, heb ik [pc-naam] vervangen met JoePC.

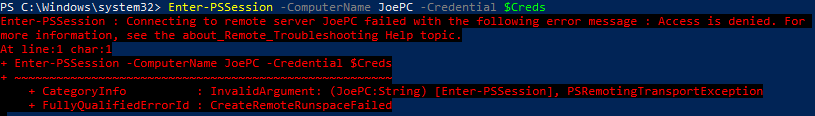


Om nu te kunnen verbinden, moet ik de credentials van een account op de remote pc hebben. Om de credentials op te slaan in een variable, gebruik ik de Get-Credential cmdlet.

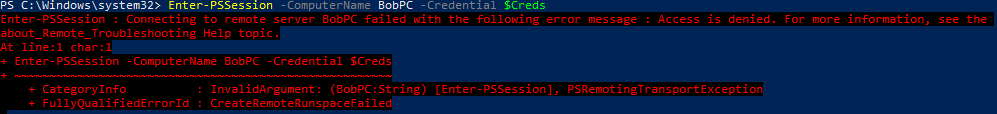
Afbeelding met tekst

Automatisch gegenereerde beschrijving

Nu dat we alle setup hebben gedaan, kunnen we eindelijk verbinding maken met de andere pc.



En we krijgen een error. Ik heb eerlijk gezegd geen idee waarom ik deze error krijg. Ook als ik probeer van PC2 naar PC1 te remoten krijg ik dezelfde error.



Ik heb meerdere uren mijn hoofd over dit probleem zitten draaien, maar ik heb niks gevonden om het op te lossen. Helaas is mijn project dus gefaald.

# Conclusie

Na alle research die ik heb gedaan is het project uiteindelijk toch gefaald, wat jammer is. Hier is daarentegen niks aan te doen, gewoon accepteren dus. Ik vond het wel leuk om alle research te doen naar het onderwerp omdat het me toch wel interesseerd. Later in het security-veld werken is waar ik nu al een tijd van droom en ik denk dat dit project me toch wel wat heeft geleerd over beheer en het veilig houden van netwerken.

# Bibliografie

Constantin, L. (2022, Maart 4). *Nvidia hackers release code-signing certificates that malware can abuse*. Opgehaald van CSOOnline: https://www.csoonline.com/article/3652694/nvidia-hackers-release-code-signing-certificates-that-malware-can-abuse.html

Cymoki, & tedhudek. (2021, December 15). *Driver Signing*. Opgehaald van Microsoft: https://docs.microsoft.com/en-us/windows-hardware/drivers/install/driver-signing

*Defender*. (sd). Opgehaald van Microsoft: https://docs.microsoft.com/en-us/powershell/module/defender/?view=windowsserver2022-ps

*Device driver*. (2022, Maart 20). Opgehaald van Wikipedia: https://en.wikipedia.org/wiki/Device\_driver

Huculak, M. (2019, Januari 4). *How to check device driver versions on Windows 10*. Opgehaald van Windows Central: https://www.windowscentral.com/how-check-device-driver-version-windows-10

Mutahar, S. (2022, Maart 9). *Hackers Are Trying To Hack Your Graphic Card...* Opgehaald van YouTube: https://www.youtube.com/watch?v=uO6vOnv7f1k

Robins, S. (2022, Maart 7). *Beware fake Nvidia drivers, leaked certificate code from hack may now have malware*. Opgehaald van PCInvasion: https://www.pcinvasion.com/nvidia-data-breach-malware-gpu-drivers/

sdwheeler, chasewilson, & nschonni. (2021, Augustus 10). *Security Considerations for PowerShell Remoting using WinRM*. Opgehaald van Microsoft Docs: https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/winrmsecurity?view=powershell-7.2

Wickens, K. (2022, Maart 7). *Nvidia's stolen data is being used to disguise malware as GPU drivers*. Opgehaald van PCGamer: https://www.pcgamer.com/nvidias-stolen-data-is-being-used-to-disguise-malware-as-gpu-drivers/