PENETRATIETEST VERSLAG

Windows Privilege Escalation - Insider Threat Scenario

Klant	Vanguard Logistics / Red Mango Transport
Testomgeving	VULN01 - Windows AD Lab (LAB-AD Domain)
Classificatie	Vertrouwelijk
Testtype	Grey Box - Insider Threat
Startdatum	15/05/2026
Einddatum	01/06/2026
Versie	1.0
Auteur	Lenny Bos

Dit document bevat vertrouwelijke informatie over de uitgevoerde security assessment. Verspreiding is alleen toegestaan aan de direct betrokken partijen binnen de afgesproken scope.

Versiebeheer

Versie	Datum	Auteur	Omschrijving
0.1	15/05/2026	Lenny Bos	Eerste concept
0.2	16/05/2026	Lenny Bos	Gevonden kwetsbaarheden toevoegen

Managementsamenvatting

Inleiding

Vanguard Logistics heeft een security assessment en penetratietest laten uitvoeren op de Windows werkomgeving van Red Mango Transport (RMT). Het doel van deze pentest was om te ontdekken en beoordelen in tot hoeverre een interne gebruiker zoals een ex-medewerker met beperkte rechten bepaalde misconfiguraties kan misbruiken om toegang te krijgen tot hogere rechten of toegang tot gevoelige onderdelen van het system.

Belangrijkste bevindingen

Ernst	Aantal gevonden	Aantal opgelost	Voorbeeld
Kritiek	1	0	AlwaysInstallElevated misconfiguratie
Hoog	4	0	Unquoted Service Path, insecure file permissions, zwakke service permissies en schrijfbare systeem-PATH map
Gemiddeld	0	0	-
Laag	0	0	-
Informatief	0	0	-

Risico-heatmap voor en na mitigatie

Onderstaande heatmaps tonen de risicopositie van de bevindingen vóór het toepassen van maatregelen en het verwachte restrisico na mitigatie. De inschatting is gebaseerd op de kans en impact uit de bevindingenlijst.

Heatmap vóór mitigatie

Impact \ Kans	Laag	Gemiddeld	Hoog
Kritiek		**B-02**	
Hoog		**B-05**	**B-01** **B-03** **B-04**
Gemiddeld			
Laag			

De heatmap vóór mitigatie laat zien dat de meeste bevindingen een hoog tot kritiek risicoprofiel hebben. Vooral B-02 zou een kritisch risico kunnen vormen, omdat een standaardgebruiker hiermee code met SYSTEM-rechten kan uitvoeren. De service-gerelateerde bevindingen blijven hoog risico door de kans op lokale privilege escalation.

Als toepassing van de aanbevolen maatregelen is genomen daalt het verwachte risico aanzienlijk. Door AlwaysInstallElevated uit te schakelen, servicepaden te quoten, schrijfrechten te beperken en serviceconfiguraties periodiek te controleren wordt misbruik door standaardgebruikers sterk beperkt.

rood = kritisch/hoog risico, oranje/geel = gemiddeld risico, groen = laag restrisico.

Conclusie

De geteste omgeving bleek meerdere configuratiefouten te hebben die een standaardgebruiker kan misbruiken om lokale beheersrechten / SYSTEEM-rechten te krijgen. Vooral configuratiefouten zoals zwakke serviceconfiguraties en onveilige installer-instellingen zijn getroffen in de omgeving, deze kwetsbaarheden konden allemaal leiden tot privilege escalation van een standaardgebruiker tot administrator.

De aanbevelingen zijn vooral gericht op het verwijderen van de configuratie fouten en het beperken van schrijfrechten op systeemlocaites, ook implementatie van structurele monitoring van privilege-escalation indicatoren.

Aanvullende validatie

Naast de bevestigde kwetsbaarheden zijn twee medium PrivescCheck kwetsbaarheden extra onderzocht. De finding Configuration - COM Image File Permissions is getest door een DLL te plaatsen en het COM-object te triggeren. De DLL werd uitgevoerd, maar het bewijsbestand toonde aan dat de code draaide als HELAB\lowpriv en niet als SYSTEM of Administrator. Hierdoor kon geen COMAdmin-gebruiker worden aangemaakt en is privilege escalation niet aangetoond. De LAPS hardening finding is ook gecontroleerd, hieruit bleek dat de host is lid van HELAB.LOCAL, maar er werden geen LAPS policy keys gevonden. Dit is daarom opgenomen als aandachtspunt en niet als succesvolle privilege-escalation kwetsbaarheid.

Aanbevelingen met prioriteit

1. Schakel AlwaysInstallElevated uit op machine- en gebruikersniveau.
2. Quote servicepaden en beperk schrijfrechten op mappen in servicepaden.
3. Voer periodieke hardeningcontroles uit op Windows-clients en domeinbeleid.

Inhoud

1. Inleiding

Deze penetratietest is in opdracht van Vanguard Logistics / Red Mango Transport uitgevoerd. Het onderzoek richtte zich op een Windows Active Directory omgeving waar een scenario afspeelft omtreffend een insider threat, hierbij is getest hoe ver een gebruiker met beperkte rechten misconfiguraties en kwetsbaarheden kan misbruiken om toegang te krijgen tot hogere privileges te krijgen.

Het doel van dit rapport is om de gevonden kwetsbaarheden, risico's en aanbevolen mitigerende maatregelen duidelijk en overzichtelijk vast te leggen. De manier waarop de test is uitgevoerd word ook zorgvuldig gerapporteerd, de nadruk van het rapport ligt op privilege escalation binnen de windows omgeving waar de impact op vertrouwelijkheid, integriteit en beschikbaarheid ook wordt beoordeeld.

De resultaten in het rapport zijn bedoeld om een beeld te creeeren in de beveiligingstatus van de omgeving en duidelijke mogelijke punten aan te wijzen die verbeterd kunnen worden en hoe dit kan, om een duidelijke visie te creeeren zodat de risico's worden verlaagd.

1.1 Achtergrond

Vanguard Logistics is een transport en logistiekbedrijf wat internationaal opereert, Vanguard Logistics heft recentelijk Red Mango Transport overgenomen, bij het assessment is uitgegaan van een insider scenario waarbij er een interne gebruiker beschikt over standaard rechten en account dus geen beheersrechten.

1.2 Doel

Het doel van de penetratietest is om vast te kunnen stellen of een gebruiker met beperkte toegang en rechten tot staat is om zijn privileges te escaleren, beveiligingsmaatregelen kan omzeilen of eventueel toegang zou kunnen krijgen tot gevoelige informatie.

1.3 Scope

In scope	VULN01 - Windows 11 client
In scope	ADMINPC - beheerwerkplek
Uit scope	Externe netwerken en productiesystemen
Testaccount	lowpriv - standaard domeingebruiker
Testtype	Grey Box - beperkte voorkennis

1.4 Labomgeving

Systeem	Rol
ADMINPC	Beheerwerkplek
VULN01	Kwetsbare Windows 11 host
Aanvaller	Interne gebruiker met domeinaccount

2. Methodiek

2.1 Gebruikte frameworks

- **MITRE ATT&CK for Enterprise** – MITRE ATT&CK is een groot framework met enorm veel bekende aanvalstechnieken die door aanvallers worden gebruikt. In dit rapport is MITRE gebruikt om gevonden bevindingen te koppelen aan herkenbare technieken, zodat het duidelijk is welk aanvalsgedrag bij de kwetsbaarheid hoort.
- **Unified Kill Chain** – De Unified Kill Chain beschrijft verschillende fases binnen een aanval, van de verkenning tot uitvoering en mogelijke acties die daarna volgen. Dit framework wordt gebruikt om de test stappen op een logische wijze te laten zien en in welke fases van een aanval de uitgevoerd acties gebeuren.
- **ISO/IEC 27005** – ISO/IEC 27005 is een standaard voor informatie, beveiliging en risicobeheer. Binnen dit rapport wordt deze methode gebruikt op de risico's te beoordelen op basis van de kans en impact, waarbij ook wordt gekeken naar de BIV (beschikbaarheid, integriteit, vertrouwelijkheid).
- **PTES** – PTES oftewel Penetration Testing Execution Standard geeft een structuur an de pentest waardoor de voorbereiding, verkenning, exploitative, validatie gestructureerd uitgevoerd kan worden binnen de scope. In dit rapport wordt de PTES gebruikt om de test op een herhaalbare en gestructureerde wijze uit te voeren.

2.2 Testfasen

Fase	Beschrijving
IN	Initiële toegang en verkenning van de omgeving
THROUGH	Privilege escalation, discovery, lateral movement
OUT	Niets uitgevoerd, er is geen data geëxfiltreerd. De tests waren gestopt na het kunnen aantonen van de kwetsbaarheden.

2.3 Gebruikte tools

Tool	Doel
PrivescCheck	Scannen op privilege-escalation paden
Sysinternals Suite	Analyse van processen, services en ACLs
WiX Toolset	Maken van MSI-installatiebestanden voor het testen van AlwaysInstallElevated
Local Users and Group Management	Controleren van aangemaakte gebruikers en lokale administratorrechten
VirtualBox	Draaien van de virtuele test machine binnen de labomgeving.
Windows Event Viewer	Controleren van system logs tijden validaite.
winPEAS	Windows privilege-escalation checks
cmd.exe / PowerShell	Handmatige validatie en bewijsvoering

2.4 Risicomethodiek

Risico wordt bepaald op basis van kans en impact. De impact wordt gekoppeld aan de BIV-factoren: Beschikbaarheid, Integriteit en Vertrouwelijkheid. Bevindingen worden geclassificeerd als Kritiek, Hoog, Gemiddeld, Laag of Informatief.

3. Risicoanalyse

3.1 Assetinventarisatie

Laag	Asset	Type	Locatie	Belang
Infrastructuur	VULN01	Windows 11-client	LAB-AD / lokaal netwerk	Hoog
Infrastructuur	ADMINPC	Beheerwerkplek	LAB-AD / lokaal netwerk	Hoog
Identiteit	Lowpriv testaccount	Standaard domeingebruiker	VULN01	Hoog
Identiteit	Lokale gebruikers en groepen	Accounts en groepen	VULN01	Hoog
Identiteit	Lokale administratorgroep	Lokale beheerdersgroep	VULN01	Kritiek
Configuratie	Windows Installer Policy	MSI-installatiebeleid	Windows Register / GPO	Kritiek
Configuratie	Windows Services	Serviceconfiguratie	VULN01	Hoog
Configuratie	Service binaries en servicepaden	Uitvoerbare servicebestanden	Servicepaden op VULN01	Hoog
Configuratie	Bestands- en maprechten	NTFS-permissies	Service- en systeemmappen	Hoog
Configuratie	Windows Register	Systeeminstellingen	HKLM / HKCU	Hoog
Configuratie	Systeem-PATH variabele	Omgevingsvariabele	Windows systeemconfiguratie	Hoog
Informatie	Credential Store	Opgeslagen credentials	Lokale Windows-host	Kritiek
Logging	Windows Event Logs	Beveiligings- en systeemlogs	Event Viewer / VULN01	Gemiddeld

De assetinventarisatie is uitgebreid met de systemen, accounts, configuraties, permissies en logbronnen die relevant zijn voor privilege escalation binnen de Windows-labomgeving. Hierdoor wordt duidelijk welke onderdelen invloed hebben op het aanvalspad en waar mitigerende maatregelen toegepast moeten worden.

3.2 Dreigingen en kwetsbaarheden

Asset	Bedreiging	Kwetsbaarheid	BIV	Impact	Maatregel
Windows Services	Service manipulatie	Unquoted service paths / zwakke maprechten	I, A	Codeuitvoering als SYSTEM	Servicepaden quoten en ACLs hardenen
Windows Register	Misbruik van installatiebeleid	AlwaysInstallElevated staat aan	C, I, A	MSI uitvoerbaar als SYSTEM	Beleid uitschakelen via GPO
Windows Installer Policy	Privilege Escalation	Standaardgebruikers kunnen met MSI installaties verhoogde rechten uitvoeren	C,I,A	Lokale admin rechten verkrijgen	AlwayInstallElevated uitschakelen en applocker toepassen
Lokale gebruikers en groepen	Ongeautoriseerde rechten	Nieuw account toegevoegd aan lokale administratorgroep	C,I,A	Volledige controle over VULN01	Lokale adminleden beperken + monitoren

4. Bevindingen

4.1 Overzicht

ID	Bevinding	Ernst	Kans	Impact	Status
B-01	Unquoted Service Path	Hoog	Hoog	Hoog	Open
B-02	AlwaysInstallElevated	Kritiek	Gemiddeld	Kritiek	Open
B-03	Insecure File Permissions op servicebestand	Hoog	Hoog	Hoog	Open
B-04	Zwakke service permissies	Hoog	Hoog	Hoog	Open
B-05	Schrijfbare systeem-PATH map	Hoog	Gemiddeld	Hoog	Open

4.2 Bevinding B-01 - Unquoted Service Path

Ernst	Hoog
MITRE ATT&CK	T1574.009 - Hijack Execution Flow: Path Interception by Unquoted Path
CVSS	7.8 - CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Beschrijving

De service bevat een uitvoerpad zonder aanhalingstekens terwijl het pad spaties bevat. Hierdoor kan Windows bij een servicestart zoeken naar uitvoerbare bestanden op tussenliggende padniveaus. Wanneer een gebruiker daar schrijfrechten heeft, kan dit worden misbruikt voor privilege escalation.

Bewijs

1. PrivescCheck uitgevoerd en kwetsbaar servicepad vastgesteld.
2. Schrijfrechten op de relevante map gecontroleerd en payload uitgevoerd.
3. Aangemaakte gebruiker met admin rechten gecontroleerd.
4. Bewijs vastgelegd in screenshot.

Impact

Een aanvaller met schrijfrechten op de betreffende map kan code laten uitvoeren met verhoogde rechten. Dit kan er tot leiden dat een aanvaller alles kan uitvoeren naar wens met administrator rechten.

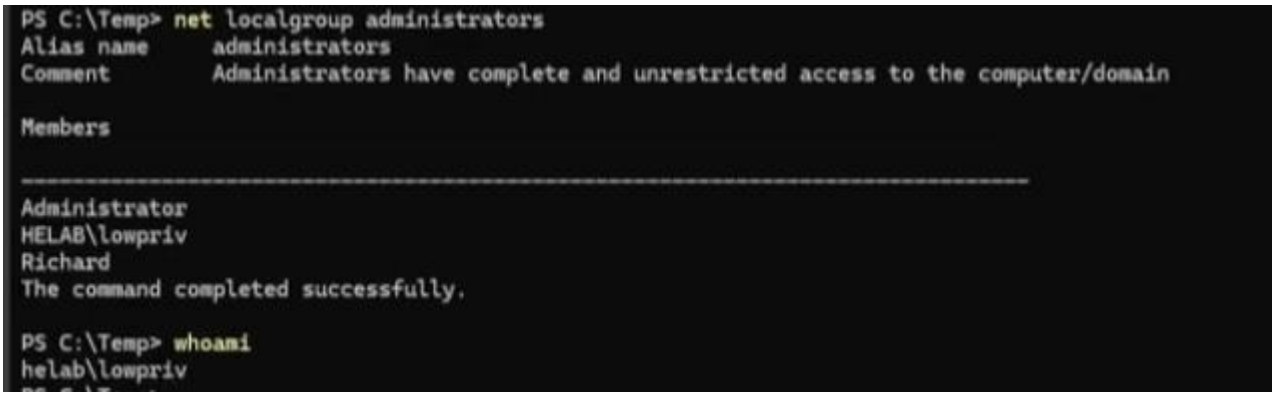
Aanbeveling

Zet servicepaden tussen aanhalingstekens, beperk schrijfrechten op alle mappen in het servicepad en controleer serviceconfiguraties periodiek.

MITRE ATT&CK maatregel

Maatregel beperkt T1574.009 door de servicepaden te quoten en schrijfrechten op de tussenliggende mappen te verwijderen.

Bewijs



4.3 Bevinding B-02 - AlwaysInstallElevated

Ernst	Kritiek
MITRE ATT&CK	T1548.002 - Abuse Elevation Control Mechanism: Bypass User Account Control
CVSS	7.8 - CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Beschrijving

De registersleutels voor AlwaysInstallElevated staan aan op zowel machine- als gebruikersniveau. Hierdoor kunnen MSI-installatiebestanden met verhoogde rechten worden uitgevoerd, ook wanneer de gebruiker zelf beperkte rechten heeft.

Bewijs

1. PrivescCheck toont dat AlwaysInstallElevated kwetsbaar is.
2. Registersleutels gecontroleerd in HKLM en HKCU.
3. Bewijs vastgelegd in screenshot.

Impact

Een standaardgebruiker kan willekeurige code uitvoeren met SYSTEM-privileges via een MSI-bestand. Dit raakt vertrouwelijkheid, integriteit en beschikbaarheid. En kan ervoor zorgen dat code van een hacker wordt uitgevoerd op de machine met verhoogde gebruikers rechten, waardoor er bijvoorbeeld een administrator account aangemaakt zou kunnen worden.

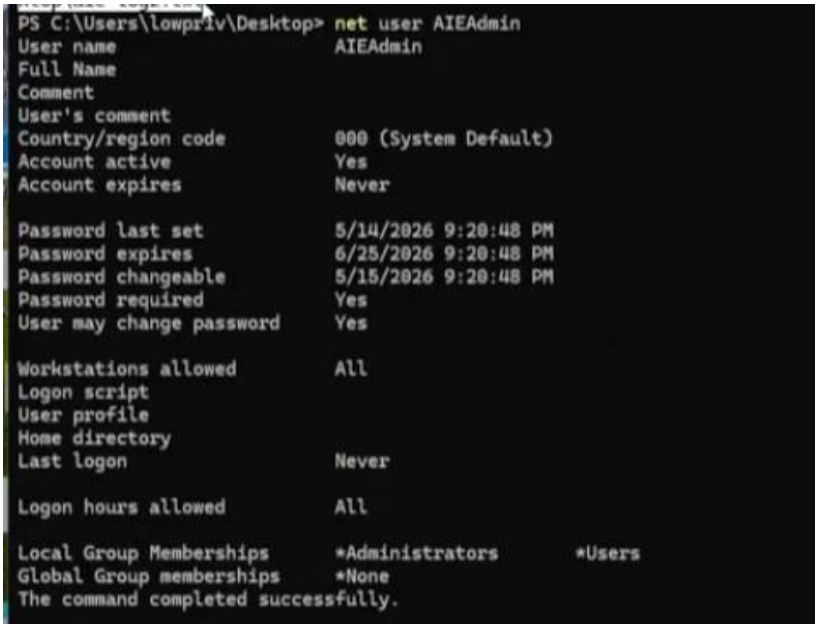
Aanbeveling

Schakel AlwaysInstallElevated uit via Groepsbeleid op zowel Computer Configuration als User Configuration. Gebruik aanvullend AppLocker of WDAC om ongewenste installatiebestanden te blokkeren.

MITRE ATT&CK maatregel

Maatregel beperkt T1548.002 door AlwaysInstallElevated uit te schakelen en de MSI uitvoering door standaardgebruikers te blokkeren.

Bewijs



4.4 Bevinding B-03 - Insecure File Permissions op servicebestand

Ernst	Hoog
MITRE ATT&CK	T1574.010 - Hijack Execution Flow: Services File Permissions Weakness
CVSS	7.8 - CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Beschrijving

De PrivescCheck-scan toont dat de huidige gebruiker schrijfrechten heeft op een servicebestand. Bij de WsFp Service verwijst het servicepad naar C:\Program Files\Svc WsFp\wsfpsvc.exe. De service draait onder LocalSystem, terwijl BUILTIN\Users volledige rechten heeft op het servicebestand. Hierdoor kan een standaardgebruiker het uitvoerbare bestand vervangen en bij het starten van de service code laten uitvoeren met verhoogde rechten.

Bewijs

1. PrivescCheck uitgevoerd en de finding Services - Image File Permissions vastgesteld voor de WsFp Service.
2. De serviceconfiguratie is gecontroleerd met sc.exe qc "WsFp Service". Hierbij werd vastgesteld dat de service draait als LocalSystem en dat het binary path verwijst naar C:\Program Files\Svc WsFp\wsfpsvc.exe. De ACL is gecontroleerd met icacls, waaruit bleek dat BUILTIN\Users volledige rechten had op het servicebestand.
3. Het servicebestand is vervangen door een testpayload die de lokale gebruiker FilePermAdmin aanmaakt en toevoegt aan de lokale administratorsgroep. Na het starten van de service is gecontroleerd dat FilePermAdmin lokale administratorrechten had. De exploitatie en validatie zijn vastgelegd in de screenshot en video FilePermAdmin.

Impact

Een aanvaller kan via een kwetsbaar servicebestand code uitvoeren met verhoogde rechten. Dit kan leiden tot volledige controle over het apparaat en raakt vertrouwelijkheid, integriteit en beschikbaarheid.

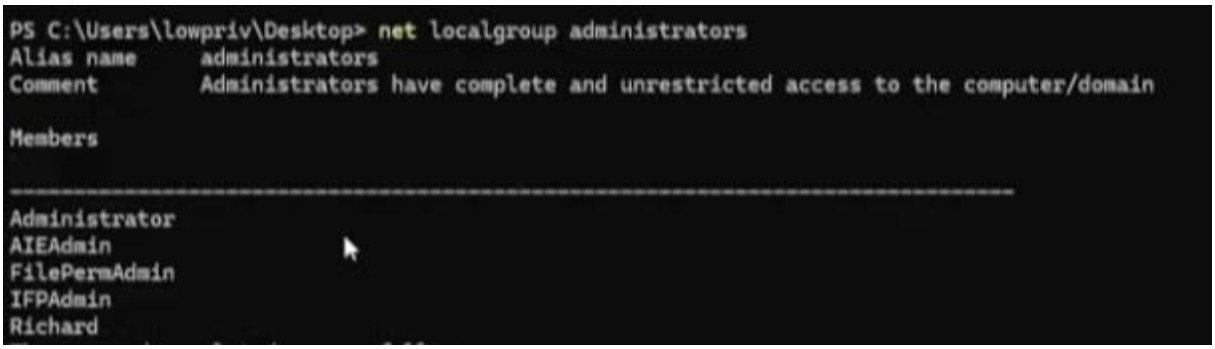
Aanbeveling

Beperk schrijfrechten op servicebestanden en servicemappen tot Administrators en SYSTEM. Controleer periodiek ACLs op servicepaden en voorkom dat standaardgebruikers bestanden in systeem- of servicelocaties kunnen aanpassen.

MITRE ATT&CK maatregel

Deze maatregel beperkt T1574.010 door schrijfrechten op servicebestanden alleen toe te staan aan Administrators en SYSTEM.

Bewijs



4.5 Bevinding B-04 - Zwakke service permissies

Ernst	Hoog
MITRE ATT&CK	T1543.003 - Create or Modify System Process: Windows Service
CVSS	7.8 - CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Beschrijving

De PrivescCheck-scan toont dat de huidige gebruiker permissies heeft op een Windows-service die niet passend zijn voor een standaardgebruiker. Wanneer een gebruiker een service kan wijzigen, starten of stoppen, kan dit worden misbruikt om code met verhoogde rechten uit te voeren.

Bewijs

1. PrivescCheck uitgevoerd en de finding Services - Permissions vastgesteld.
2. Service permissies zijn gecontroleerd en als kwetsbaar beoordeeld.
3. Bewijs is vastgelegd in screenshot B-04, waarin de validatie van de service-misconfiguratie wordt getoond.

Impact

Onveilige service permissies kunnen leiden tot privilege escalation naar lokale administrator of systeem rechten. Een aanvaller kan hierdoor bijvoorbeeld software aanpassen, beveiligingsinstellingen wijzigen of persistente toegang behouden.

Aanbeveling

Beperk servicebeheerrechten tot beheerdersaccounts. Controleer service ACLs met tools zoals PowerShell, Sysinternals en PrivescCheck en monitor wijzigingen in serviceconfiguraties.

MITRE ATT&CK maatregel

Deze maatregel beperkt T1543.003 door servicebeheerrechten alleen toe te staan aan beheerdersaccounts.

Bewijs

4.6 Bevinding B-05 - Schrijfbare systeem-PATH map

Ernst	Hoog
MITRE ATT&CK	T1574.007 - Hijack Execution Flow: Path Interception by PATH Environment Variable
CVSS	7.1 - CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Beschrijving

De PrivescCheck-scan toont dat de huidige gebruiker schrijfrechten heeft op een map die in de systeem-PATH voorkomt. Wanneer een proces of service een bestand zonder volledig pad aanroept, kan een aanvaller een eigen uitvoerbaar bestand plaatsen dat door Windows wordt geladen.

Bewijs

1. PrivescCheck uitgevoerd en de finding Configuration - PATH Folder Permissions vastgesteld.
2. De schrijfbare PATH-locatie is gecontroleerd.
3. Bewijs is vastgelegd in screenshot B-05.

Impact

Een schrijfbare systeem-PATH map kan worden misbruikt voor DLL of executable hijacking. Dit kan leiden tot uitvoering van ongeautoriseerde code met verhoogde rechten wanneer een kwetsbaar proces de map gebruikt. Dus kan een gebruiker met normale rechten code uitvoeren als een administrator.

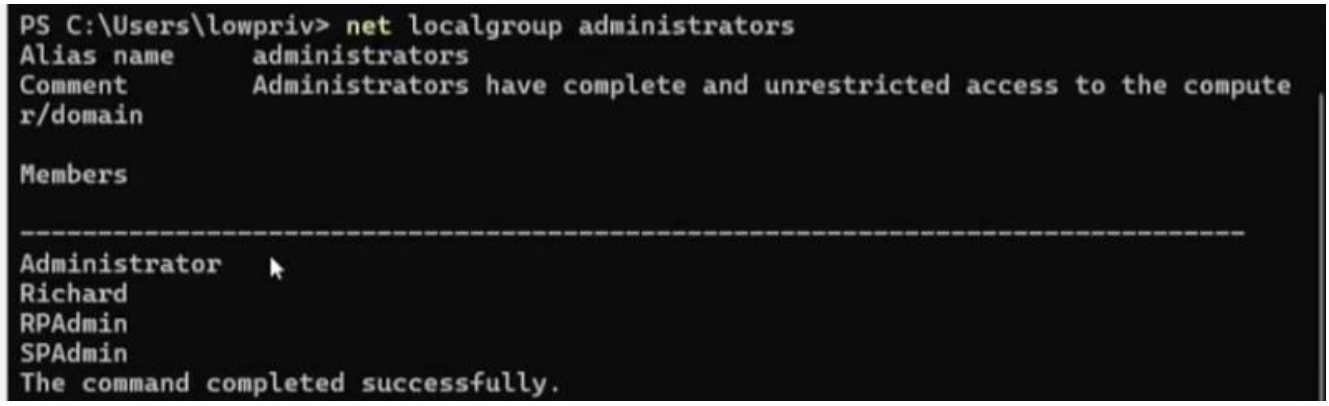
Aanbeveling

Verwijder schrijfbare mappen uit de systeem-PATH of beperk de schrijfrechten tot beheerders en SYSTEM. Controleer de PATH-variabelen periodiek en voorkom dat standaardgebruikers systeemlocaties kunnen wijzigen.

MITRE ATT&CK maatregel

Deze maatregel beperkt T1574.007 door schrijfbare mappen uit de systeem-PATH te verwijderen en de rechten te beperken.

Bewijs



5. Bronvermelding

- MITRE ATT&CK. (z.d.). Enterprise tactics and techniques. https://attack.mitre.org/
- Lockheed Martin. (z.d.). Cyber Kill Chain. https://www.lockheedmartin.com/
- Pols, P. (2021). The Unified Kill Chain.
- ISO/IEC 27005. Information security risk management.
- itm4n. (z.d.). PrivescCheck. https://github.com/itm4n/PrivescCheck
- Microsoft. (z.d.). Sysinternals Suite. https://learn.microsoft.com/sysinternals/
- PEASS-ng. (z.d.). winPEAS. https://github.com/peass-ng/PEASS-ng
- WiX Toolset. (z.d.). WiX Toolset. https://wixtoolset.org/
- Oracle. (z.d.). Oracle VM VirtualBox. https://www.virtualbox.org/
- Microsoft. (z.d.). Windows Installer. https://learn.microsoft.com/windows/win32/msi/windows-installer-portal
- Microsoft. (z.d.). Service Control Manager. https://learn.microsoft.com/windows/win32/services/service-control-manager

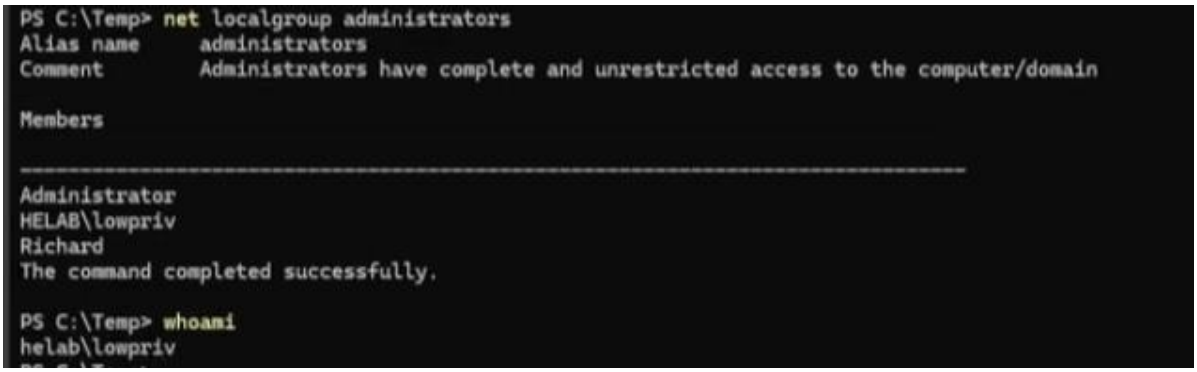
Bijlage A - Verklarende woordenlijst

Term	Uitleg
Privilege Escalation	Het verhogen van rechten op een systeem, bijvoorbeeld van standaardgebruiker naar Administrator of SYSTEM.
MITRE ATT&CK	Framework met tactieken en technieken die aanvallers gebruiken.
Unquoted Service Path	Servicepad zonder aanhalingstekens, waardoor Windows mogelijk een ander uitvoerbaar bestand start.
AlwaysInstallElevated	Windows Installer-instelling waardoor MSI-bestanden met verhoogde rechten kunnen draaien.
ACL	Access Control List: rechtenstructuur die bepaalt wie wat mag doen met bestanden, mappen of services.
SYSTEM-account	Het meest bevoorrechte lokale account in Windows.
BIV	Beschikbaarheid, Integriteit en Vertrouwelijkheid.
Grey Box	Testvorm met beperkte voorkennis, zoals een regulier gebruikersaccount.

Bijlage B - Schermafbeeldingen en bewijs

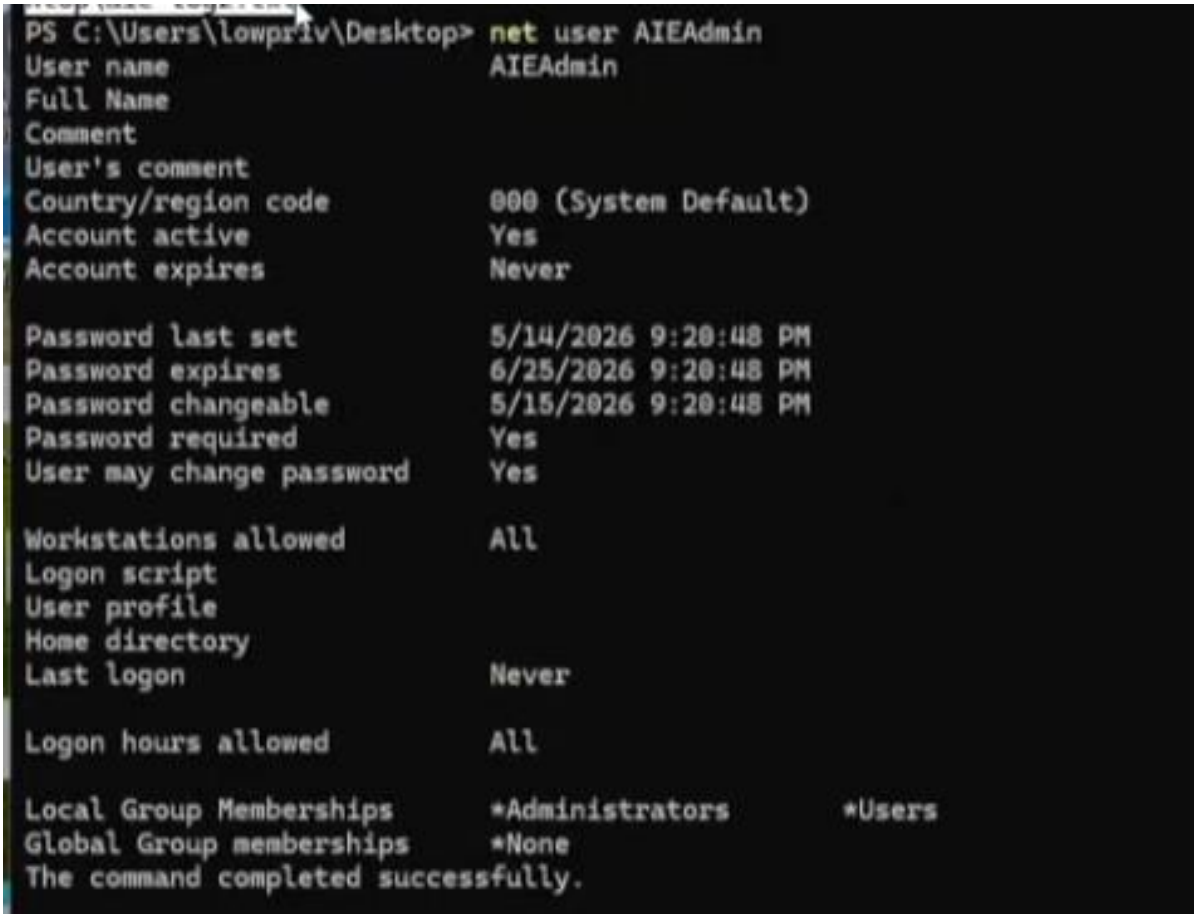
Onderstaande screenshots zijn als bewijsstukken opgenomen per bevinding. Per screenshot staat aangegeven bij welke bevinding het bewijs hoort en wat ermee wordt aangetoond. Aan het einde van deze bijlage zijn optionele videolinks opgenomen als aanvullend naslagbewijs.

Screenshot B-01 - Unquoted Service Path



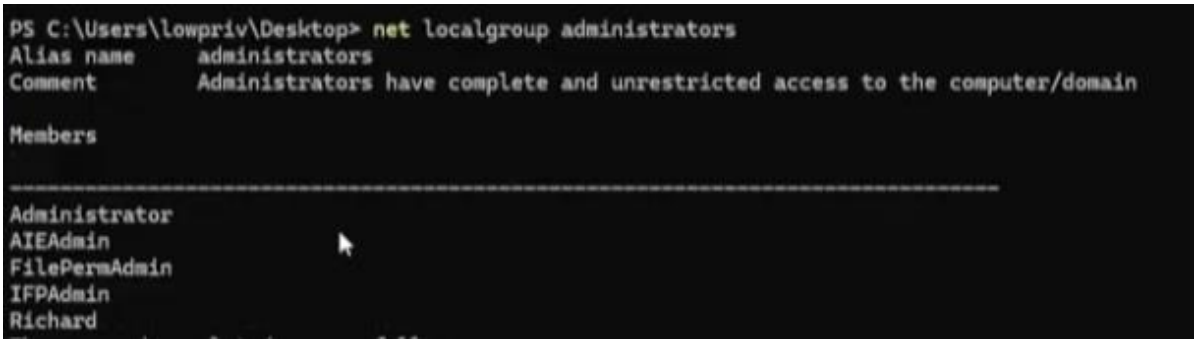
Screenshot B-01 toont de controle van de lokale administratorsgroep en de gebruikerscontext tijdens de validatie. Dit bewijs hoort bij de bevinding waarbij een onveilig servicepad misbruikt kan worden voor privilege escalation.

Screenshot B-02 - AlwaysInstallElevated



Screenshot B-02 toont de validatie van het aangemaakte account AIEAdmin en de bijbehorende lokale groepslidmaatschappen. Dit ondersteunt de bevinding dat MSI-uitvoering met verhoogde rechten kan leiden tot lokale administratorrechten.

Screenshot B-03 - Insecure File Permissions op servicebestand

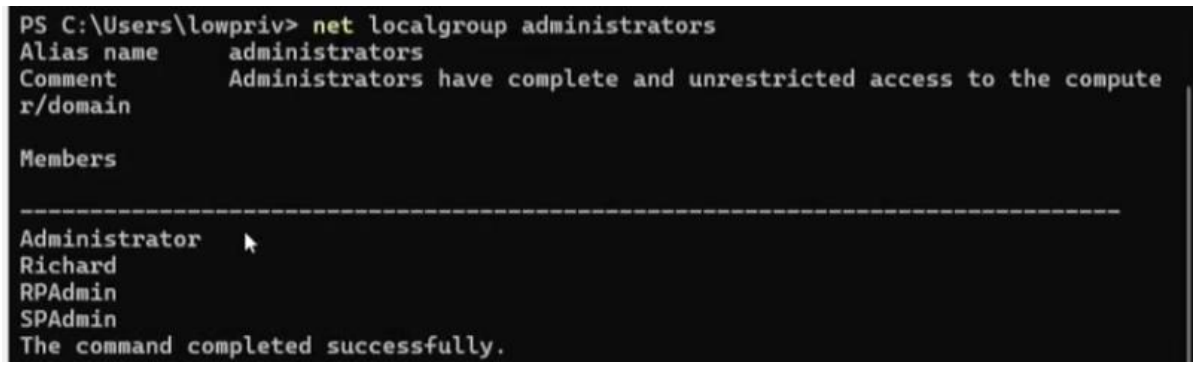


Screenshot B-03 toont dat het testaccount FilePermAdmin is toegevoegd aan de lokale administratorsgroep. Dit ondersteunt de bevinding dat onveilige schrijfrechten op een servicebestand kunnen leiden tot privilege escalation.

Screenshot B-04 - Zwakke service permissies

Screenshot B-04 toont de validatie van het aangemaakte account RPAdmin en de controle van de lokale administratorsgroep. Dit bewijs hoort bij de bevinding waarbij zwakke servicepermissies misbruikt kunnen worden om verhoogde rechten te verkrijgen.

Screenshot B-05 - Schrijfbare systeem-PATH map

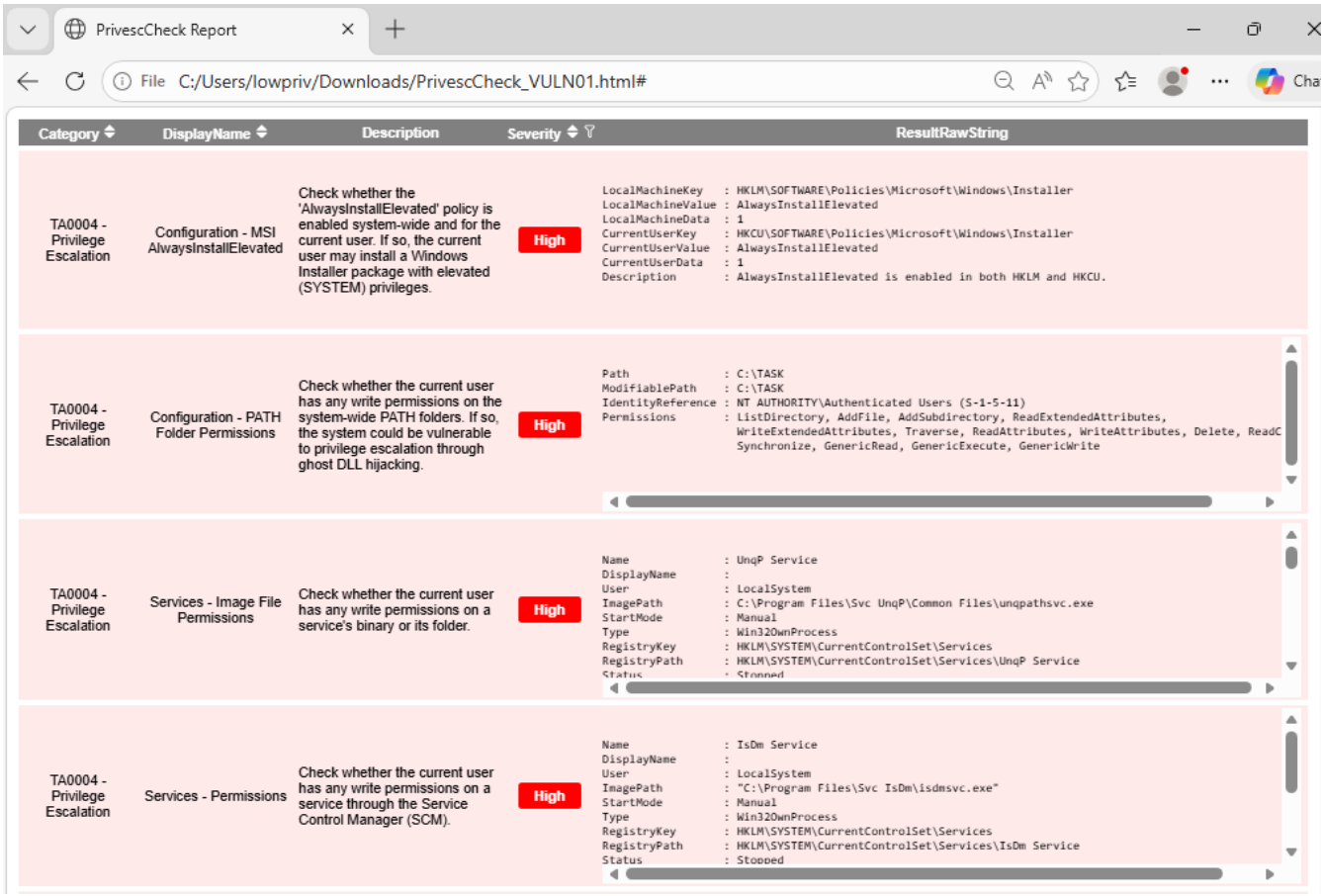


Screenshot B-05 toont de controle van de lokale administratorsgroep waarin onder andere SPAdmin zichtbaar is. Dit ondersteunt de bevinding dat een schrijfbare systeem-PATH map kan bijdragen aan privilege escalation via path hijacking.

PrivescCheck scanoverzicht

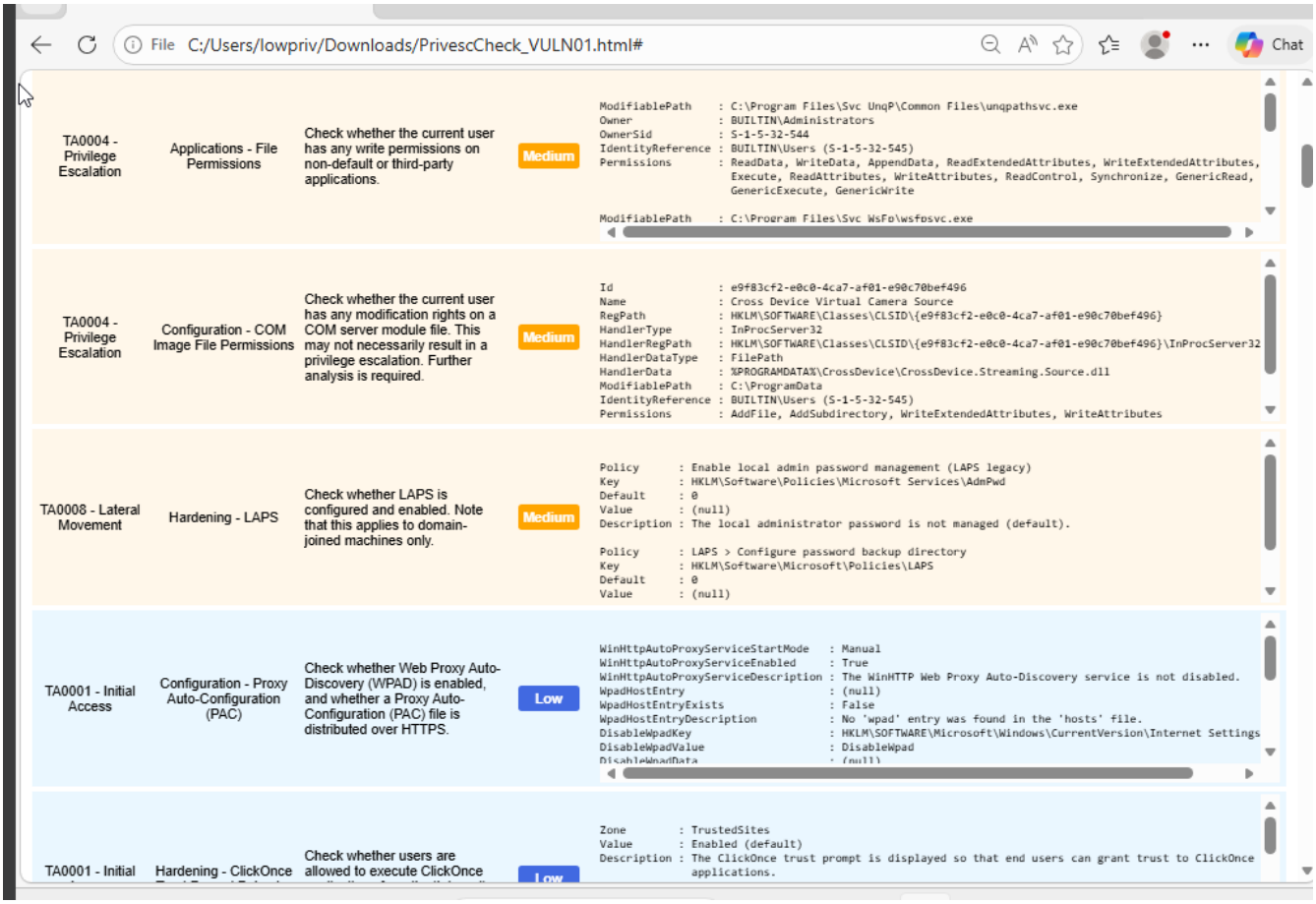
Onderstaande screenshots tonen de samenvatting van de PrivescCheck-scan. Deze bewijsstukken ondersteunen de algemene recon en laten zien welke privilege-escalation bevindingen door de tool zijn aangemerkt als hoog, gemiddeld of laag risico.

Screenshot B-00a - PrivescCheck high findings



Screenshot B-00a toont de belangrijkste high-risk PrivescCheck-resultaten, waaronder AlwaysInstallElevated, PATH Folder Permissions, Services - Image File Permissions en Services - Permissions. Deze resultaten vormen de basis voor de bevindingen B-01 t/m B-05.

Screenshot B-00b - PrivescCheck aanvullende findings



Screenshot B-00b toont aanvullende PrivescCheck-resultaten, waaronder Applications - File Permissions, Configuration - COM Image File Permissions, Hardening - LAPS en enkele low-risk hardeningobservaties. De COM- en LAPS-finding zijn aanvullend onderzocht en daarom in de managementsamenvatting als aandachtspunt opgenomen.

Bijlage C - Commando-overzicht

Doel	Commando	Bevinding
PrivescCheck uitvoeren	PS> . .\PrivescCheck.ps1; Invoke-PrivescCheck -Extended -Report PrivescReport -Format HTML,CSV	Algemeen
Huidige gebruiker controleren	cmd> whoami	Algemeen
Lokale administratorgroep controleren	cmd> net localgroup administrators	Algemeen
Gebruiker controleren	cmd> net user AIEAdmin	B-02
Gebruiker controleren	cmd> net user UnQPAdmin	B-01
Gebruiker controleren	cmd> net user FilePermAdmin	B-03
Gebruiker controleren	cmd> net user RPAdmin	B-04
Gebruiker controleren	cmd> net user SPAdmin	B-05
AlwaysInstallElevated controleren (machine)	cmd> reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated	B-02
AlwaysInstallElevated controleren (gebruiker)	cmd> reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated	B-02
MSI uitvoeren met logging	cmd> msiexec /i "C:\Users\lowpriv\Desktop\aie-test.msi" /qn /L*v "C:\Users\lowpriv\Desktop\aie-log2.txt"	B-02
MSI-log controleren	PS> Select-String -Path "C:\Users\lowpriv\Desktop\aie-log.txt" -Pattern "AddAdminUser","net user","cmd.exe","Return value 3","error"	B-02
Naar tijdelijke werkmap gaan	PS> cd C:\Temp	B-01
Bestanden in werkmap tonen	PS> ls	Algemeen
PowerShell execution policy tijdelijk aanpassen	PS> Set-ExecutionPolicy Bypass -Scope Process -Force	B-01
Payload-script uitvoeren	PS> . C:\Temp\payload.ps1	B-01
Kwetsbare service starten	cmd> net start "UnqP Service"	B-01
Serviceconfiguratie opvragen	cmd> sc.exe qc "WsFp Service"	B-03
Servicestatus controleren	cmd> sc.exe query "WsFp Service"	B-03
Rechten op servicebestand controleren	cmd> icacls "C:\Program Files\Svc WsFp\wsfpsvc.exe"	B-03
Servicebestand vervangen	PS> Copy-Item -Path "C:\Users\lowpriv\Desktop\wsfpsvc.exe" -Destination "C:\Program Files\Svc WsFp\wsfpsvc.exe" -Force	B-03
Service starten	cmd> net start "WsFp Service"	B-03
Serviceconfiguratie opvragen	cmd> sc.exe qc "WsRegP Service"	B-04
Service ImagePath aanpassen via register	cmd> reg add "HKLM\SYSTEM\CurrentControlSet\Services\WsRegP Service" /v ImagePath /t REG_EXPAND_SZ /d "C:\Windows\System32\cmd.exe /c net user RPAdmin RPAdmin /add && net localgroup administrators RPAdmin /add" /f	B-04
Service starten	cmd> net start "WsRegP Service"	B-04
Serviceconfiguratie opvragen	cmd> sc.exe qc "IsDm Service"	B-05
Service binary path aanpassen	cmd> sc.exe config "IsDm Service" binPath= "C:\Windows\System32\cmd.exe /c C:\TASK\LabTool.exe"	B-05
Gewijzigde serviceconfiguratie controleren	cmd> sc.exe qc "IsDm Service"	B-05
Service starten	cmd> net start "IsDm Service"	B-05
Gebruiker SPAdmin controleren	cmd> net user SPAdmin	B-05

Alleen de relevante en succesvolle commando's zijn opgenomen. Typfouten, mislukte pogingen en herhaalde controles zijn weggelaten om het overzicht leesbaar te houden.