|  |  |  |
| --- | --- | --- |
| Role | Machine | Tool Used |
| Attacker | Kali Linux VM | Netcat |
| Victim | Windows 10 VM | PowerShell |
|  |  |  |

**10. Command and Control (C2) Traffic Detection**

## Step-by-Step: Mock C2 Attack Using Netcat

**Step 1: Get Kali IP Address**

In Kali terminal:

ip a

Look for your IP, something like: 192.168.1.131

### **Step 2: Start Netcat Listener on Kali (Attacker)**

In Kali terminal:

nc -lvnp 4444

* -l = Listen mode
* -v = Verbose output
* -n = Don’t resolve DNS
* -p = Port number (4444 in this case)

**Kali is now waiting for connections from the victim.**

### **Step 3: Simulate Beacon on Windows (Victim)**

On your **Windows VM**, open PowerShell as Administrator, then paste this:

while ($true) {

Invoke-WebRequest http://192.168.1.131:4444

Start-Sleep -Seconds 30

}

This tells the victim to:

* Send a **web request to the attacker's Netcat listener every 30 seconds** (like a beacon).

### **Step 4: Watch Kali for Connections**

Back on Kali (in the Netcat window), you should see:

listening on [any] 4444 ...

Each time the victim checks in, you'll see a connection.

### **Step 5: Analyze with Wireshark or tcpdump (Optional)**

To inspect beacon traffic patterns:

#### On Kali:

sudo wireshark

Filter:

ip.addr == 192.168.157.140 && tcp.port == 4444

You’ll see **regular traffic every 30 seconds** — that’s the beaconing pattern.