9. Lateral Movement Detection

**Purpose:**  
To **simulate lateral movement** inside a network (how attackers move from one compromised system to others) and monitor/detect that activity using event logs and network traffic.

|  |  |
| --- | --- |
| **SMB (Server Message Block)** | A protocol used for file and printer sharing between Windows computers. Attackers use it to execute remote commands or transfer files. |
| **WMI (Windows Management Instrumentation)** | Used to manage Windows systems, and can also be used by attackers to execute commands remotely. |
| **RDP (Remote Desktop Protocol)** | Allows remote graphical access to a Windows system. |

## Step-by-Step Guide to Perform and Monitor Lateral Movement

* At least **two Windows systems** (VMs or real), one acting as attacker, one as target.
* Admin credentials or a way to authenticate.

## 🛠️ Step 1: Simulate Lateral Movement

Let’s simulate lateral movement using **CrackMapExec** and **wmiexec**.

### 🔧 Option 1: CrackMapExec (using SMB)

1. Install CME:
2. pip install crackmapexec
3. Check connectivity to a target:
4. crackmapexec smb 192.168.1.100 -u Administrator -p 'Password123'
5. Execute a command remotely:
6. crackmapexec smb 192.168.1.100 -u Administrator -p 'Password123' -x "whoami"

### 🔧 Option 2: wmiexec.py (from Impacket)

1. Install Impacket:
2. pip install impacket
3. Execute command on target using WMI:
4. python3 wmiexec.py Administrator:Password123@192.168.1.100
5. This opens a semi-interactive shell. You can run commands like whoami, ipconfig, etc.

## 🕵️ Step 2: Detect and Monitor Activity

### 🔍 Monitor Sysmon and Event Logs

#### Sysmon Setup

1. Install Sysmon:  
   Download Sysinternals Sysmon: <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>
2. Install with a good config:
3. sysmon -accepteula -i sysmonconfig.xml

(Use a config like [SwiftOnSecurity’s Sysmon config](https://github.com/SwiftOnSecurity/sysmon-config))

* **Sysmon Event ID 3**: Logs network connections (e.g., remote SMB or WMI usage).
* **Windows Security Event ID 4624**: Successful logins. Helps detect which user logged in and from where.

#### Review:

* Open Event Viewer (eventvwr.msc)
* Navigate to:
  + Applications and Services Logs > Microsoft > Windows > Sysmon > Operational
  + Windows Logs > Security

Use filters to find:

* Event ID **3** (Sysmon): Source IP and Destination Port (e.g., 445 for SMB)
* Event ID **4624** (Security): Type 3 = network logon

## 📊 Step 3: Correlate Logs with Activity

Match timestamps from:

* The time you ran wmiexec or CME
* To the entries in Sysmon and Security logs