**Cyber-attack Query Development: Lateral Movement**

1) **Kerberos – Pass the Ticket**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Malware | Vulnerability | O/S | Windows Event Id | Windows Port | Process/  Executables | DLL/  SharedLibrary | Other Parameters | Present in LANL Dataset (Y/N) |
| Empire |  | Windows | 4768 |  | lsass.exe |  | Authentication Package = ‘Kerberos’ | Y |
|  |  |  | 4769 |  |  |  |  |  |

**Kerberos PTT Attack Flow**

Step1: Forge 4768(TGT REQUEST) using tools like mimikatz. This prevents generation of 4768 for TGT REQUEST.

Step2: Make a legitimate Service ticket request. This generates 4769.

Step3: Look for 4769 logged for which 4768 has not been logged for a given time duration.

Step4: Check for LM in shortlisted Devices in Step 3

2) **Windows Remote Management**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Malware | Vulnerability | O/S | Windows Event Id | Windows Port | Process/  Executables | DLL/  SharedLibrary | Other Parameters | Present in LANL Dataset (Y/N) |
| Bronze union | [CVE-2014-6324](https://nvd.nist.gov/vuln/detail/CVE-2014-6324), vulnerability in Microsoft's implementation of the Kerberos network authentication protocol. | Windows | **4768/4769** | **5985/5986** | lsass.exe w.exe/ms.exe  Quser.exe Javaws.exe |  | Authentication Package = ‘Kerberos’ | Y |

**Windows Remote Management Flow**

Step1: Forge 4768(TGT REQUEST) using tools like mimikatz. This prevents generation of 4768 for TGT REQUEST.

Step2: Make a legitimate Service ticket request. This generates 4769.

Step3: Look for 4769 logged for which 4768 has not been logged for a given time duration.

Step4: Check for LM in shortlisted Devices in Step 3

Step5: Further, Check for Exfiltration. \*\*(Still being worked upon)