How to Collect Cybersecurity Risk Parameters on Windows

1. Number of Vulnerabilities

Definition: Known flaws or bugs in your system/software that attackers can exploit.

Tools/Methods:

- Use Nessus (Tenable) to scan and report system vulnerabilities.

  -> Download: https://www.tenable.com/products/nessus

- Microsoft Defender (for malware-related vulnerabilities)

  -> Go to Windows Security -> Virus & threat protection -> Protection history

2. System Uptime (in days)

Definition: The number of days your system has been running continuously.

Command Prompt:

```
systeminfo | find "System Boot Time"
```

PowerShell:

```
(get-date) - (gcim Win32_OperatingSystem).LastBootUpTime
```

Calculate the difference between current time and boot time.

3. Number of Security Incidents

Definition: Events like failed logins, malware detection, unauthorized access.

Steps:

- Open Event Viewer: Press Win + R -> type: eventvwr.msc
- Navigate: Windows Logs -> Security
- Count specific Event IDs:
  * 4625: Failed login attempts
  * 4688: Process creation (monitor suspicious processes)
  * 4720: New user account created

Windows Defender Logs:

-> Windows Security -> Virus & Threat Protection -> Protection history

4. Patch Update Frequency

Definition: How frequently system updates are applied (Daily/Weekly/Monthly).

Steps:

- Go to Settings -> Update & Security -> View update history
- Based on update pattern, assign frequency:
  * Daily: Every 1-2 days
  * Weekly: Once a week
  * Monthly: Once or twice a month

5. Number of Open Ports

Definition: Network ports that are open and accepting connections (can be exploited).

Command Prompt:

```
netstat -an | find "LISTEN"
```

PowerShell:

```
Get-NetTCPConnection | Where-Object {$_.State -eq "Listen"} | Measure-Object
```

Each "LISTENING" line indicates one open port.