How about windows CVEs?

Great question. When talking specifically about **Windows CVEs**, you’re focusing on **vulnerabilities that affect Microsoft Windows operating systems**—from privilege escalation bugs to remote code execution flaws. Here’s how Windows CVEs connect through the exploitation chain using tools like Metasploit, Armitage, and Cobalt Strike:

**🪟 Windows CVEs (Examples + Links)**

Here are some **notable Windows CVEs** often used in real-world attacks or training:

| **CVE ID** | **Vulnerability Name** | **Affected OS** | **Description** | **Tool/Exploit** |
| --- | --- | --- | --- | --- |
| [CVE-2017-0143](https://nvd.nist.gov/vuln/detail/CVE-2017-0143) | EternalBlue | Windows XP to Windows 7 | SMBv1 RCE used by WannaCry | Metasploit (exploit/windows/smb/ms17\_010\_eternalblue) |
| [CVE-2020-0796](https://nvd.nist.gov/vuln/detail/CVE-2020-0796) | SMBGhost | Windows 10, Server 2019 | SMBv3 RCE | Custom exploits, some modules |
| [CVE-2021-34527](https://nvd.nist.gov/vuln/detail/CVE-2021-34527) | PrintNightmare | Win 7 to 10, Server | Print Spooler RCE/LPE | Metasploit + Manual Payloads |
| [CVE-2019-0708](https://nvd.nist.gov/vuln/detail/CVE-2019-0708) | BlueKeep | Windows 7, Server 2008 | RDP vulnerability | Metasploit (unstable) |
| [CVE-2022-30190](https://nvd.nist.gov/vuln/detail/CVE-2022-30190) | Follina | All modern Windows | MSDT remote code execution via Office | Manual/Scripted Exploit |

**🔗 Connecting Windows CVEs Through the Toolchain**

**1. Vulnerability Discovery**

* Use **Nessus**, **OpenVAS**, or **Nmap scripts** to find systems vulnerable to specific Windows CVEs.
* These tools will often map findings directly to CVE IDs.

**2. Exploitation with Metasploit**

* Use search CVE-YYYY-NNNN to find a matching module:
* msfconsole
* search CVE-2017-0143
* use exploit/windows/smb/ms17\_010\_eternalblue
* Configure payloads (e.g., windows/meterpreter/reverse\_tcp) and exploit the system.

**3. GUI Workflow with Armitage**

* Connect to Metasploit.
* Import hosts.
* Automatically find and launch matching Windows CVE exploits via right-click menu.

**4. Post-Exploitation with Cobalt Strike**

* After initial access from a CVE exploit:
  + Deploy **Beacon** (payload for persistence and stealthy communication).
  + Use **mimikatz**, lateral movement, privilege escalation (some using unpatched CVEs).
* Cobalt Strike can also run custom scripts to exploit local CVEs (e.g., token impersonation or kernel LPE).

**🔧 Related Tools for Windows CVEs**

| **Tool** | **Use** |
| --- | --- |
| **WinPEAS / SharpHound** | Post-exploitation enumeration (privilege escalation paths) |
| **PowerSploit** | PowerShell-based exploitation (some CVE scripts) |
| **Mimikatz** | Credential dumping after CVE-based access |
| **CVE-Search** | API/database for querying Windows CVEs by product/version |
| **Windows Exploit Suggester** | Match known Windows exploits (CVE-based) to system info |

Would you like a ready-to-use curated list of **Windows CVEs with available Metasploit modules**, or maybe a script to check a target system against known vulnerable CVEs?