Here's a high-level overview showing the typical relationship and workflow between **CVE**, **Metasploit**, **Armitage**, and **Cobalt Strike**, along with brief descriptions. I’ll also mention a few related tools that can be part of a broader exploitation workflow.

**🛠️ 1. CVE (Common Vulnerabilities and Exposures)**

* **Description**: A publicly disclosed list of security flaws. Each CVE entry identifies a known vulnerability (e.g., CVE-2021-44228 - Log4Shell).
* **Use**: Researchers and attackers use CVEs to identify targets with known weaknesses.

**🔗 → Metasploit Framework**

* **Description**: An open-source penetration testing tool with a large collection of exploits, payloads, and post-exploitation modules.
* **Link to CVE**: Many Metasploit modules are tied directly to CVEs (e.g., an exploit module for CVE-2017-0143 - EternalBlue).
* **Workflow**:
  + Search for a CVE.
  + Look for an exploit module in Metasploit using search CVE-XXXX-XXXX.
  + Launch the exploit and manage the payload (e.g., meterpreter shell).
* **Tool type**: Exploitation framework.

**🔗 → Armitage**

* **Description**: A GUI frontend for Metasploit designed to assist with team-based penetration testing.
* **Link to Metasploit**: Directly interfaces with the Metasploit Framework.
* **Features**:
  + Graphical view of targets and sessions.
  + Drag-and-drop exploit and post-exploit tools.
  + Good for training and red-team collaboration.
* **Workflow**:
  + Discover hosts and services.
  + Launch exploits visually.
  + Manage sessions and post-exploitation via UI.

**🔗 → Cobalt Strike**

* **Description**: A commercial red team tool focused on advanced post-exploitation, persistence, lateral movement, and threat emulation.
* **Link to Metasploit**: Inspired by Metasploit but functions independently; originally integrated with Metasploit but now uses its own framework (Beacon payload).
* **Key Features**:
  + Stealthy command-and-control (C2) via HTTP/HTTPS/DNS.
  + In-memory execution.
  + Malleable C2 profiles to mimic APT behavior.
  + Collaboration for red teams.
* **Workflow**:
  + Use CVEs/Metasploit/Armitage to gain initial access.
  + Deploy **Cobalt Strike Beacon** for long-term access and movement.

**🔗 Additional Tools in the Exploitation Chain:**

**🧪 Nmap**

* **Use**: Port scanning, service detection, and OS fingerprinting.
* **Position**: Pre-exploitation phase to identify targets.

**🔍 Nessus/OpenVAS**

* **Use**: Vulnerability scanners that map findings to CVEs.
* **Position**: Vulnerability discovery and validation.

**💣 Exploit-DB**

* **Use**: Repository of proof-of-concept exploits.
* **Position**: Manual exploitation when Metasploit modules don’t exist.

**👣 BloodHound**

* **Use**: Post-exploitation tool to map Active Directory relationships.
* **Position**: Useful after gaining a foothold.

**🐚 Empire / PoshC2 / Sliver**

* **Use**: Post-exploitation C2 frameworks (alternatives or complements to Cobalt Strike).
* **Position**: For stealthy command-and-control and persistence.

**Summary Diagram (Workflow)**

[CVE Database]

↓

[Nmap/Nessus/Exploit-DB]

↓

[Metasploit] ←→ [Armitage]

↓

[Initial Shell/Access]

↓

[Cobalt Strike / Empire / Sliver]

↓

[Post-exploitation & Persistence]

Let me know if you want a visual diagram or a markdown/HTML table of tools with links.