Attack Structure

Practice describing security concepts in the context of an attack. These categories are a rough guide on attack structure for a targeted attack. Non-targeted attacks tend to be a bit more "all-in-one".

- Reconnaissance
    - OSINT, Google dorking, Shodan.
- Resource Development
    - Get infrastructure (via compromise or otherwise).
    - Build malware.
    - Compromise accounts.
- Initial Access
    - Phishing.
    - Hardware placements.
    - Supply chain compromise.
    - Exploit public-facing apps.
- Execution
    - Shells & interpreters (powershell, python, javascript, etc.).
    - Scheduled tasks, Windows Management Instrumentation (WMI).
- Persistence
    - Additional accounts/creds.
    - Start-up/log-on/boot scripts, modify launch agents, DLL side-loading, Webshells.
    - Scheduled tasks.
- Privilege Escalation
    - Sudo, token/key theft, IAM/group policy modification.
    - Many persistence exploits are PrivEsc methods too.
- Defense Evasion
    - Disable detection software & logging.
    - Revert VM/Cloud instances.
    - Process hollowing/injection, bootkits.
- Credential Access
    - Brute force, access password managers, keylogging.
    - etc/passwd & etc/shadow.
    - Windows DCSync, Kerberos Gold & Silver tickets.
    - Clear-text creds in files/pastebin, etc.
- Discovery
    - Network scanning.
    - Find accounts by listing policies.
    - Find remote systems, software and system info, VM/sandbox.
- Lateral Movement
    - SSH/RDP/SMB.
    - Compromise shared content, internal spear phishing.
    - Pass the hash/ticket, tokens, cookies.
- Collection
    - Database dumps.
    - Audio/video/screen capture, keylogging.

    - Internal documentation, network shared drives, internal traffic interception.
- Exfiltration
    - Removable media/USB, Bluetooth exfil.
    - C2 channels, DNS exfil, web services like code repos & Cloud backup storage.
    - Scheduled transfers.
- Command and Control (C2)
    - Web service (dead drop resolvers, one-way/bi-directional traffic), encrypted channels.
    - Removable media.
    - Steganography, encoded commands.
- Impact
    - Deleted accounts or data, encrypt data (like ransomware).
    - Defacement.
    - Denial of service, shutdown/reboot systems.