Steps Used in Typical Digital Attacks

1. Reconnaissance

In this initial phase, attackers gather information about the target. This can include researching employees, finding out which software and systems are in use, and identifying potential entry points. Information can be collected through public sources, social engineering, or more technical methods.

2. Weaponization

With the information gathered, attackers create a weapon tailored to their target. This often involves packaging a payload, such as malware, with an exploit into a deliverable format that can trigger the vulnerability. The aim is to create a tool that can be used to gain entry or control over a system or network.

3. Delivery

The weaponized payload is delivered to the target. This could be through email attachments, websites, USB drives, or other methods. The goal is to get the target to trigger the exploit, thereby executing the payload.

4. Exploitation

Upon delivery, the exploitation phase begins when the payload is activated, exploiting a vulnerability within the target?s system or network. This allows the attacker to gain initial access.

5. Installation

After exploiting a system, the attacker installs a backdoor or other malicious software to secure a foothold within the target?s environment. This software can allow the attacker to maintain access to the network and potentially avoid detection.

Steps Used in Typical Digital Attacks

6. Command and Control (C2)

The installed malware establishes a command and control channel back to the attacker. This enables the attacker to remotely manipulate the compromised system, issue commands, exfiltrate data, or spread to other systems within the network.

7. Actions on Objectives

Finally, the attacker takes actions to achieve their goals, whether that?s data theft, destruction of data, encrypting files for ransom, espionage, or otherwise disrupting the target?s operations.