**First Question:** Do we have permission to attack this target? All networks or only one? All devices or only one?

**Step 1: Information Gathering/Reconnaissance**

* Gathering information about your target to better plan out your attack
* Can perform on any website/target
* **Active:** Interacting with target (target website, network, systems in company)  
  - Directly exchanging packets with target or using social engineering to obtain information
* **Passive:** Not interacting with target   
  - Have a middle source (person, website, etc) and get information about the target from that third party source

**Step 2: Scanning**

* A more advanced form of reconnaissance where you use technical tools to find openings in the target (open gateways, open ports, operating systems)
* Also perform vulnerability scanning where we search for vulnerable software in target system or network

**Step 3: Gaining Access/Exploitation**

* Actually gain access into network through previously identified methods
* Can steal data from target or utilize target to attack other devices on the same network
* Can consider a Penetration Test successful after this step with no need to continue further

**Step 4: Maintaining Access**

* Commonly done by installing backdoors and rootkits that allow us to gain access to target whenever we want after initial penetration

**Step 5: Covering Tracks**

* Removing all evidence that an attack ever took place
* Deleting or hiding files, editing logs, and reverting all changes made