**Hacking stages**

**1. Reconnaissance**

* Also known as **footprinting**, **fingerprinting** or **information gathering**
* 📝 Reconnaissance, *noun*, preliminary surveying or research about the target.
* 📝 Necessary first step as an attack would not be successful without it.

**2. Scanning**

* Hacker utilizes information from previous stage to conduct more technical scan.
* Often maps the routers and firewalls
* Use tools such as port scanners, network mappers, vulnerability scanners, etc.

**Reconnaissance vs Scanning**

* In scanning you're acting on gathered information to gather information
* Examples

| [**Reconnaissance**](https://github.com/undergroundwires/CEH-in-bullet-points/blob/master/chapters/01-introduction/hacking-stages.md#1-reconnaissance) | [**Scanning**](https://github.com/undergroundwires/CEH-in-bullet-points/blob/master/chapters/01-introduction/hacking-stages.md#2-scanning) |
| --- | --- |
| Scan the perimeter network you need the IP addresses | Use e.g. nmap to figure out what the configuration is. |
| Get e-mails. | Use phishing to gather personal data |
| Learn where service physically are | Do dumpster diving |

**3. Gaining Access**

* Attack stage
* Steps:
  1. Find an entry point to the target OS or application on the system
  2. Use it to perform the attack
     + Hackers may escalate privileges to gain complete control over the system/network.
* Examples:
  1. Password crack with brute-force or dictionary attack
  2. Exploit buffer overflow
  3. Session hijack
  4. DoS attacks

**4. Maintaining Access**

* Keeping admin/root privileges so hacker can continue using the system.
  + After breaking into a system, you attempt to elevate privileges to do more.
* Maintain persistent access, because your connection might break, then you start again
* Can prevent other hackers from accessing the system by installing backdoors, rootkits, or trojans.
* 💡 You can install tools to give you persistance access and gathers data to use compromise more such as keylogger.
* 💡 You can use the machine as proxy so all traces are lead back to the proxy.
  + You can minimize the risks being discovered this way.
  + ❗ As pen-tester document those as you'll get other people in trouble

**5. Clearing tracks**

* Hackers do everything they can do to hide their activities
* Goal is to maintain the access to the system but remain unnoticed in the process.
  + If you're detected: the vulnerability will be patched and you'll lose access.
* Vital to clear all tracks as fast as possible, or if it's possible generate none.
* Activities:
  + Clear certain entries in log files: Not all, or it'll be suspicious
  + Masquerade your activities: Make them as similar as possible as legitimate activities
    - E.g. a good keylogger masquerade itself behind legitimate activities
      * Mimics other programs behavior by adding more behavior.