Chapter 2: Reconnaissance Techniques

* What is an attack? Attempting to destroy, alter, steal data, or break into a system.
* Penetration testing? An authorized audit
* What are the types of hackers?

|  |  |
| --- | --- |
| White Hat🡪good | Penetration tester performing an authorized engagement on a company |
| Grey Hat🡪 does not exactly follow the rules | Someone taking down a scamming site |
| Black Hat🡪criminals | Ransomware authors infect people’s devices to get money from them, holding data for ransom |

* What are the three things that the Rules of Engagement have? Permission, Test Scope, and Rules
* What are the 5 phases of hacking?

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Covering Tracks

* Reconnaissance: gathering information about internal structure of the organization

|  |  |
| --- | --- |
| Active Recon | Passive Recon |
| Acquiring info with directly interacting with the target | Acquiring info without directly interacting with the target |
|  |  |

* Resources of Renaissance:

1. Search engines🡪google
2. Social media🡪Instagram, Twitter
3. Forum🡪 Microsoft
4. History🡪 archive.com
5. Domain names, mail messages, 🡪Nslookup command

* Google tips and tricks:

1. Quotes🡪 “Smart Homes”🡪 exact search
2. Colons and website🡪Smart Homes site: Wikipedia.com🡪only search Wikipedia.
3. Excluding words🡪 Smart Homes -phones🡪 excludes phones from the result.
4. If you don’t know the words🡪 “Smart \*sth\* homes”
5. If you want to look for multiple phrases🡪 “Best ways to prepare for a job interview” OR “How to prepare for a job interview”

* *Google hacking database:* <https://www.exploit-db.com/google-hacking-database/>-->The GHDB is **an index of search queries (we call them dorks) used to find publicly available information**, intended for pentesters and security researchers.
* Hacked Emails🡪pwned.com
* Port Scanning🡪nmap tool
* Shodan.io-🡪 collect valuable information🡪 Shodan (Sentient Hyper-Optimised Data Access Network) is a [search engine](https://www.techtarget.com/whatis/definition/search-engine) designed to map and gather information about internet-connected devices and systems. Shodan is sometimes referred to as a search engine for the internet of things ([IoT](https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT)).  Applications of the software include market research, [vulnerability analysis](https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis) and [penetration testing](https://www.techtarget.com/searchsecurity/definition/penetration-testing), as well as hacking. Shodan scans the whole internet and indexes the services run on each IP address.
* Recon-ng: gathering information and assessing the vulnerability of web applications. Target a domain and find its subdomains.

1. marketplace install all
2. modules load recon/domains-hosts/bing\_domain\_web
3. modules load recon/domains-hosts/google\_site\_web
4. modules load recon/domains-hosts/brute\_hosts
5. modules load recon/hosts-hosts/resolve

* netcraft: (<https://sitereport.netcraft.com/)-->> information related to web server, network, SSL/TLS, hosting history,sender policy framework
* WAY BACK MACHINE
* Social Media