Technical Ethical Hacking

A hacker/hackers is an individual/group who uses computer, networking or other skills to overcome a technical problem. The term hacker may refer to anyone with technical skills, but it often refers to a person who uses his or her abilities to gain unauthorized access to systems. While "hacker" can refer to any computer [programmer](https://en.wikipedia.org/wiki/Programmer), the term has become associated in [popular culture](https://en.wikipedia.org/wiki/Popular_culture) with a "[security hacker](https://en.wikipedia.org/wiki/Security_hacker)", someone who, with their technical knowledge, uses [bugs](https://en.wikipedia.org/wiki/Bug_(computing)) or [exploits](https://en.wikipedia.org/wiki/Exploit_(computer_security)) to break into computer systems.

Ethical Hacking is hacking a computer network or any other device in order to test or evaluate its security, rather than with malicious or criminal intent.

Types of Hackers: There are 7 types of ethical hackers

1. **White Hat –** They are also known as ethical hackers. They are the good guys of the hacker world. They’ll help you remove a virus or PenTest a company. Most of them hold a degree in IT security or computer science and must be certified to pursue a career in hacking. The most popular certifications are GIAC (Global Information Assistance Certification) by SANS, CEH (Certified Ethical Hacker) by Ec-Council, OSCP (Offensive Security Certified Professional) by Offensive Security.
2. **Red Hat –**These are the vigilantes of the hacker world. They are stronger than White hat hackers. They’re like White Hats who halt Black Hats, but these guys are so scary to those who have ever tried so much as Pen Test. Instead of reporting the malicious attack, they shut him/her (attacker) down by uploading viruses, DoSing and accessing his/her computer to destroy it. They deploy multiple aggressive methods that might force an attacker move to a new computer.
3. **Gray Hat –** Gray Hat hackers don’t steal money or information (although, they perform an attack or two), yet they don’t help people for good (but, they could if they wanted to). These hackers comprise most of the hacking world, even though Black Hat hackers attract most of the media’s attention.
4. **Black Hat –** Also known as crackers (‘cause they crack encryption), these are the folks you hear about in the news. They find banks or other companies with vulnerable security and steal money or any valuable information. The surprising truth about their methods of attack is that they often use common hacking practices they learned early on.
5. **Green Hat –** These are the hacker noob, but unlike Script Kiddies, they care about hacking and strive to become great hackers. The hacker community for asking many basic questions often blames them. When their questions are answered, they’ll listen with the intent and very much curiosity.
6. **Script Kiddie –** Script Kiddies normally don’t care about hacking (if they did, they’d be Green Hats. See Above). They copy code and use it for a virus or any code and perform attacks. Script Kiddies will never hack for themselves; they’ll just download third party software (LOIC or Metasploit, for example) and watch tutorials on how to use it. A common Script Kiddie attack is DoSing or DDoSing (Denial of Service and Distributed Denial of Service), in which they flood an IP with so much information it collapses under the strain. This attack is frequently used by the “hacker” group anonymous, which doesn’t help anyone’s reputation.
7. **Blue Hat –** If a Script Kiddie took revenge, he/she might become a Blue Hat. Blue Hat hackers will seek vengeance on those who’ve them angry. Most Blue Hats are n00bz, but like the Script Kiddies, they have no desire to learn.

Types of Hacking:

1. **Bait and Wait:**

Using bait and switch hacking technique, the hacker runs a malicious program, which the user believes to be authentic. This way, after installing the malicious program on your computer, the hacker gets unprivileged access to your computer.

1. **Cookie Theft:**  
   The cookies of a browser keep our personal data such as browsing history, username, and passwords for different sites that we access. Once the hacker gets the access to your cookie, he can even authenticate himself as you on a browser.
2. **Click Jacking Attacks:**

Click Jacking is also known by a different name, UI Redress. In this attack, the hacker hides the actual UI where the victim is supposed to click.In another word, the attacker hijacks the clicks of the victim that aren’t meant for the exact page, but for a page where the hacker wants you to be.

1. **Virus, Trojan etc.:**

Virus or Trojans are a malicious software program, which get installed into the victim’s system and keeps sending the victims data to the hacker.

1. **Phishing:**

Phishing is a hacking technique using which a hacker replicates the most-accessed sites and traps the victim by sending that spoofed link.

Once the victim tries to login or enter some data, the hacker gets that private information of the target victim using the Trojan running on the fake site.

1. **Eavesdropping:**

Unlike other attacks, which are active in nature, using a passive attack, a hacker just monitors the computer systems and networks to gain some unwanted information. The motive behind eavesdropping is not to harm the system but to get some information without being identified.

1. **Fake WAP:**

Even just for fun, a hacker can use software to fake a wireless access point. This WAP connects to the official public place WAP. Once you get connected the fake WAP, a hacker can access your data, just like in the above case.

1. **Waterhole attacks:**

If you are a big fan of Discovery or National Geographic channels, you could relate easily with the waterhole attacks. To poison a place, in this case, the hacker hits the most accessible physical point of the victim.

For example, if the source of a river is poisoned, it will hit the entire stretch of animals during summer. In the same way, hackers target the most accessed physical location to attack the victim. That point could be a coffee shop, a cafeteria etc.Once hackers are aware of your timings, they might create a fake Wi-Fi access point and modify your most visited website to redirect them to you to get your personal information.

1. **Denial of Service (DoS\DDoS):**

A Denial of Service attack is a hacking technique to take down a site or server by flooding that site or server with a lot of traffic that the server is unable to process all the requests in the real time and finally crashes down.For DDoS attacks, hackers often deploy botnets or zombie computers, which have got the only work to flood your system with request packets.

1. **Keylogger :**

A Denial of Service attack is a hacking technique to take down a site or server by flooding that site or server with a lot of traffic that the server is unable to process all the requests in the real time and finally crashes down. For DDoS attacks, hackers often deploy botnets or zombie computers, which have got the only work to flood your system with request packets.