**WHITE HAT HACKING**

* A white hat (or a white hat hacker) is an ethical computer hacker, or a computer security expert, who specializes in penetration testing and other testing methodologies that ensure the security of an organization's information systems
* White hat hackers use their skills to help protect against attacks. White hat hackers work to proactively find security weaknesses in order to fix them before they can be exploited by attacks.

**BLACK HAT HACKING**

* A black hat hacker (or black-hat hacker) is a [hacke](https://en.wikipedia.org/wiki/Hacker_(term))r who violates computer security for their own personal profit.
* They may also release malware that destroys files, holds computers hostage, or steals passwords, credit card numbers, and other personal information.

**GREY HAT HACKING**

* A grey hat(grey hat or gray hat) is a computer hacker expert who may sometimes violate laws or typical [ethical standards](https://en.wikipedia.org/wiki/Hacker_ethic), but does not have the malicious intent typical of a black hat hacker.
* The grey hat generally has the skills and intent of the white hat but will break into any system or network without permission. One of the most common examples given of a gray hat hacker is someone who exploits a security vulnerability in order to spread public awareness that the vulnerability exists

**RED HAT HACKING**

* A red hat hacker could refer to someone who targets Linux systems. However, red hats have been characterized as vigilantes. Like white hats, red hats seek to disarm black hats, but the two groups' methodologies are significantly different.
* Rather than hand a black hat over to the authorities, red hats will launch aggressive attacks against them to bring them down, often destroying the black hat's computer and resources.