What Is Ethical Hacking?

In this article, you'll learn about the concept of ethical hacking, specifically, what ethical hacking is, what are the types of hackers, what ethical hackers do, and what roles ethical hackers have in the field of cybersecurity.

What is a Hacker?
When you think about a hacker and what they do, what comes to mind?

Keep that thought as we go through the definition of a hacker. It might surprise you. According to the Internet Security Glossary, they define a hacker as "someone with a strong interest in computers, who enjoys learning about them, programming them, and experimenting and otherwise working with them." Additionally, according to the NIST definition, a hacker is an "unauthorized user who attempts to or gains access to an information system."

Many people think hackers are individuals doing mischievous things. Still, the definition mentions nothing about activities we commonly associate with hackers, such as writing malware, breaking into networks, and stealing sensitive data. While it's true that there are hackers who do all of those things, there are also hackers who do none of them. Hackers are not necessarily criminal or malicious, despite the widespread public perception of them.

What Are The Different Types of Hackers?
There are three different types of hackers, which fall on a spectrum from *unethical hackers* and *ethical hackers*. We have our **black hat hackers**, also known as *unethical hackers*, who are hackers who commit cyber crimes for personal gain. Then we have our **grey hat hackers** who are hackers who hack into systems, often without permission and often without any malicious intent. Finally, we have our **white hat hackers**, also known as *ethical hackers*, who are hackers that hack within the confines of the law.

What Does It Mean To Be An Ethical Hacker?
To be an **Ethical Hacker**, we must act ethically and within the confines of the law when hacking. That said, ethical hackers often follow three basic tenants:

1. **Act Ethically**: Defining exactly what is and isn't ethical is a subject for an ethics and philosophy course, which this course is not. Generally speaking, acting ethically means acting without malice or intent to cause harm.

2. **Follow The Law**: Computers have an element of depersonalization that can make us forget the potential consequences of our actions. People can and do go to prison for computer crimes. The laws surrounding digital activities can be complicated and vary from place to place. *In general*, unauthorized access to or use of computers or networks is illegal, but we should familiarize ourselves with the specific laws in our jurisdiction.
3. Remember that something can be legal without being ethical, and vice-versa.

What Do Ethical Hackers Do?

Broadly speaking, ethical hackers do the same things as all hackers. They learn, explore, and try new things on a system, computer, or application. The skills and knowledge gained from this can be applied for ethical or unethical purposes, but there isn't a clear divide between "ethical skills" and "unethical skills."

Take, for example, the 2022 Russian invasion of Ukraine. The invasion saw hackers from around the world taking part, ethically and unethically, on both sides. Hackers targeted government organizations and stole the personal information of soldiers. Hackers also disrupted communications during combat and used open-source intelligence and electronic warfare to locate enemy soldiers.

In the modern world, hackers can have enormous power, which comes with responsibility. That said, the skills and knowledge we will gain in this course are intended to be used ethically, but we are ultimately responsible for how we choose to use them.

The good news is there are many, many ways that ethical hackers can apply their skills. Here are three examples:

Penetration Testers

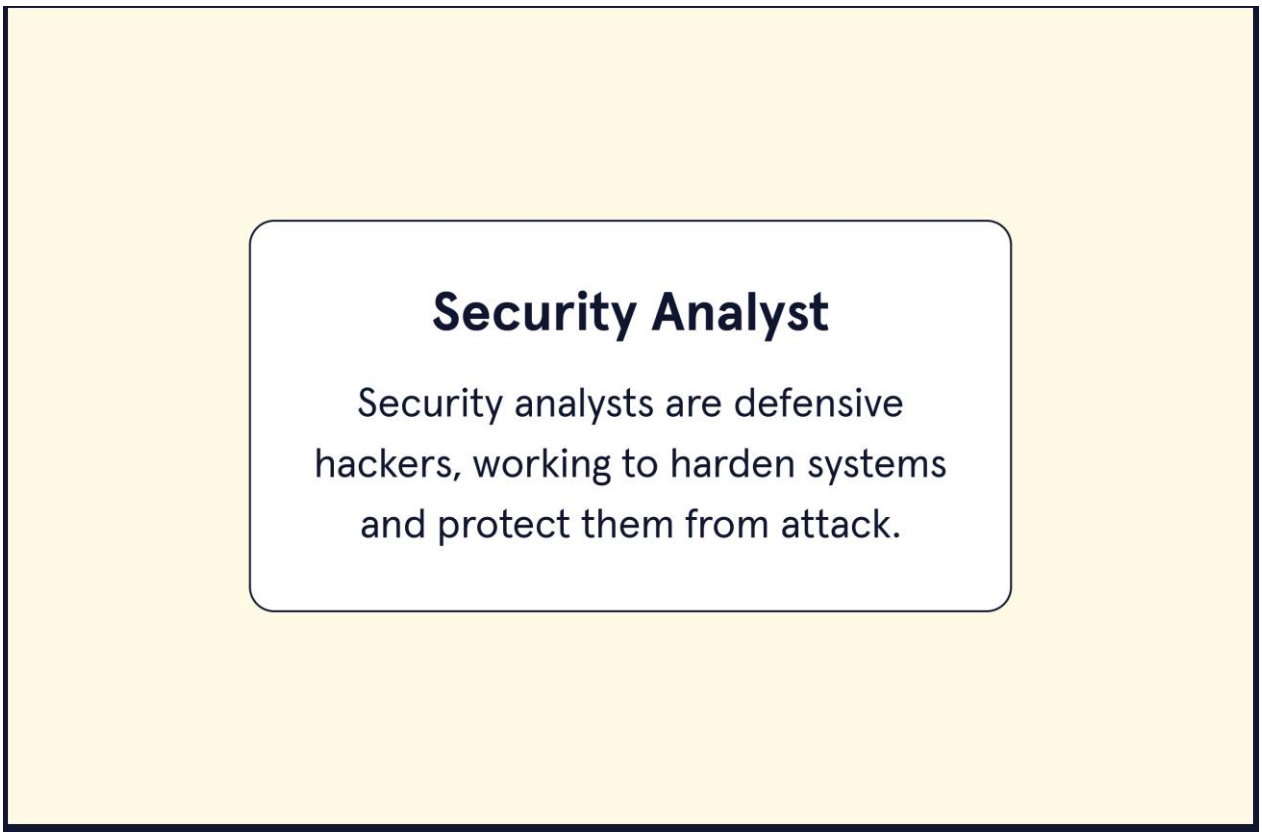
Penetration testing (pentesting for short) is when an organization hires one or more ethical hackers to try to break into their network and provide feedback on how to improve their security.

Penetration testing (pentesting for short) is when an organization hires one or more ethical hackers to try to break into their network and provide feedback on improving security. This is a simulated cyber attack conducted to identify security weaknesses. Pentesting uses the same skills and knowledge malicious hackers use when conducting real cyberattacks.

Malware Analyst

Malware analysts are hackers who examine malicious software.

When a new piece of malware comes out, it needs to be studied and analyzed so that we can defend against it. Malware analysts are hackers who, as we might infer, analyze malware. Of course, the hackers who write the malware don't want their malware to be analyzed and take steps to hamper the efforts of analysts. As such, malware analysts need to be familiar with the techniques used to create and obfuscate malware to do their job.



Security analysts are defensive hackers, working to harden systems and protect them from attack. If an attack does occur, they are usually the first to respond. Because they often work directly against other hackers, it is not unheard of (though it is rare) for Hollywood-esque "hacker duels" to take place, with two hackers attempting to lock each other out of a network or computer.

Conclusion

Hackers aren't necessarily criminal or malicious. Ethical hackers are hackers who use their skills ethically, protecting the computers we have come to rely on, often without realizing it, in our day-to-day lives. There is little difference in the skill set of an ethical and unethical hacker - what matters the most is what the skills are used for and why.