

Ethical hackers use the same methods and techniques to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security.

The purpose of ethical hacking is to evaluate the security of a network or system's infrastructure. It entails finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible. Vulnerabilities tend to be found in poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures. One of the first examples of ethical hacking occurred in the 1970s, when the United States government used groups of experts called "red teams" to hack its own computer systems. It has become a sizable sub-industry within the information security market and has expanded to also cover the physical and human elements of an organization's defenses. A successful test doesn't necessarily mean a network or system is 100% secure, but it should be able to withstand automated attacks and unskilled hackers.

Any organization that has a network connected to the Internet or provides an online service should consider subjecting it to a penetration test. Various standards such as the Payment Card Industry Data Security Standard require companies to conduct penetration testing from both an internal and external perspective on an annual basis and after any significant change in the infrastructure or applications. Many large companies, such as IBM, maintain employee teams of ethical hackers, while there are plenty of firms that offer ethical hacking as a service. Trustwave Holdings, Inc., has an Ethical Hacking Lab for attempting to exploit vulnerabilities that may be present in ATMs, point-of-sale devices and surveillance systems. There are various organizations that provide standards and certifications for consultants that conduct penetration testing including:

Ethical hacking is a proactive form of information security and is also known as penetration testing, intrusion testing and red teaming. An ethical hacker is sometimes called a legal or white hat hacker and its counterpart a black hat, a term that comes from old Western movies, where the "good guy" wore a white hat and the "bad guy" wore a black hat. The term "ethical hacker" is frowned upon by some security professionals who see it has a contradiction in terms and prefer the name "penetration tester."

Before commissioning an organization or individual, it is considered a best practice to read their service-level and code of conduct agreements covering how testing will be carried out, and how the results will be handled, as they are likely to contain sensitive information about how the system tested. There have been instances of "ethical hackers" reporting vulnerabilities they have found while testing systems without the owner's express permission. Even the LulzSec black hat hacker group has claimed its motivations include drawing attention to computer security flaws and holes. This type of hacking is a criminal offence in most countries, even if the purported intentions were to improve system security. For hacking to be deemed ethical, the hacker must have the express permission from the owner to probe their network and attempt to identify potential security risks.