Ethics in IT

Class 8

Lab 3

UNITED TRUST

bdeducation
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা

Lab Objectives:

- Ethical Hacking

As you need to apply ethics in all sectors of your daily life you need to learn ethics also for the IT sector. As an ethical hacker plays an important role to the IT industry so you need to learn ethical hacking for the sake of IT.

Ethical hacker

An ethical hacker, also referred to as a white hat hacker, is an information security expert who systematically attempts to penetrate a computer system, network, application or other computing resource on behalf of its owners -- and with their permission -- to find security vulnerabilities that a malicious hacker could potentially exploit.

Purpose of Ethical Hacking

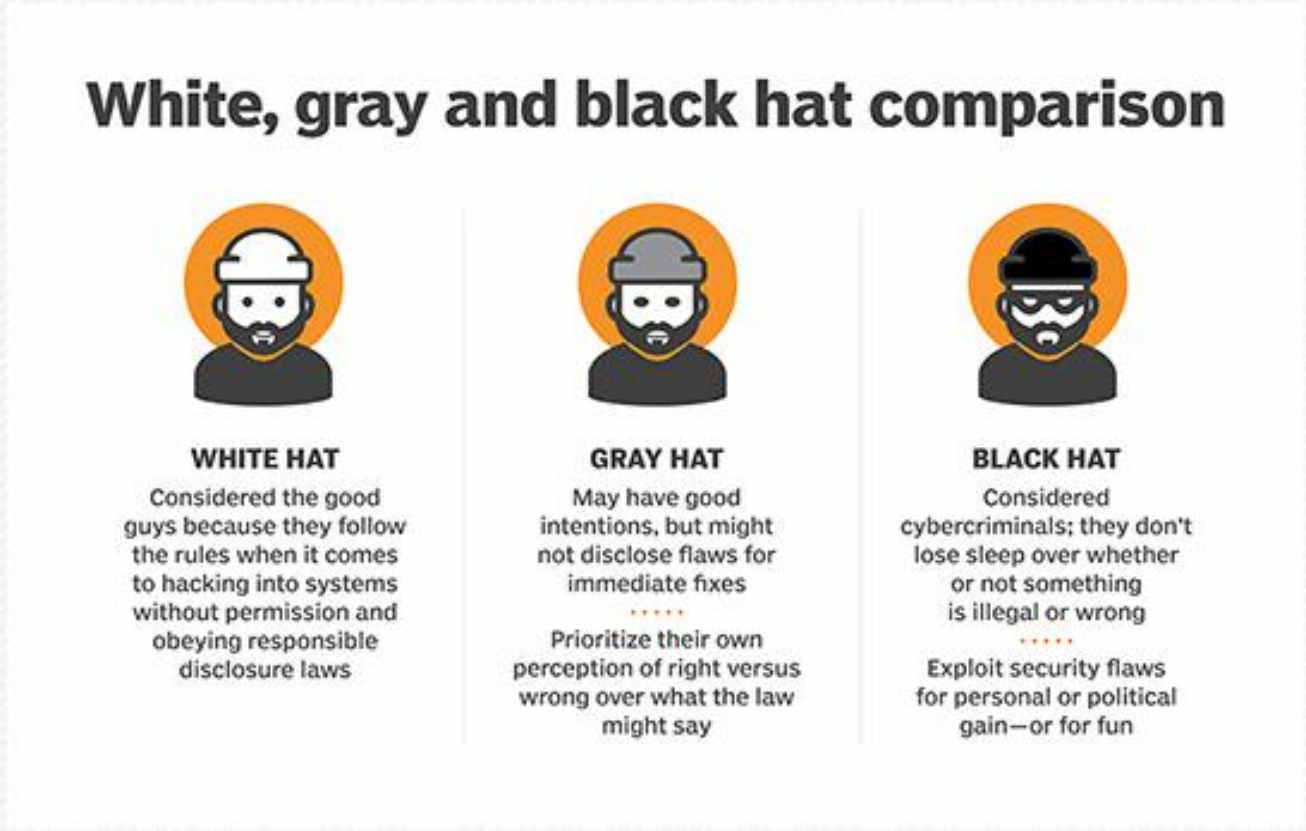
The purpose of ethical hacking is to evaluate the security of and identify vulnerabilities in systems, networks or system infrastructure. It includes finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible.

Ethical hackers use their skills and many of the same methods and techniques to test and bypass organizations' IT security as their unethical counterparts, who are referred to as black hat hackers.

However, rather than taking advantage of any vulnerabilities they find for personal gain, ethical hackers document them and provide advice about how to re mediate them so organizations can strengthen their overall security.

Ethical hackers generally find security exposures in insecure system configurations, known and unknown hardware or software vulnerabilities as well as operational weaknesses in process or technical countermeasures.

Any organization that has a network connected to the Internet or provides an online service should consider subjecting it to penetration testing conducted by ethical hackers.



Uses of ethical hacking

There are a number of ways ethical hackers can help organizations, including:

- ***Finding vulnerabilities***

Ethical hackers help companies determine which of their IT security measures are effective, which need to be updated and which contain vulnerabilities that can be exploited.

When ethical hackers finish evaluating organizations' systems, they report back to company leaders about those vulnerable areas, for instance, a lack of sufficient password encryption, insecure applications or exposed systems running unpatched software. Organizations can use the data from these tests to make informed decisions about where and how to improve their security posture to prevent cyberattacks.

- ***Demonstrating methods used by cybercriminals***

These demonstrations show executives the hacking techniques that malicious actors use to attack their systems and wreak havoc with their businesses. Companies that have in-depth knowledge of the methods the attackers use to break into their systems are better able to prevent them from doing so.

- ***Helping prepare for a cyber attack***

Cyberattacks can cripple or destroy a business, especially a small business. However, most companies are completely unprepared for cyberattacks.

Ethical hackers understand how threat actors operate and they know how these bad actors will use new information and techniques to attack systems. Security professionals who work with ethical hackers are better able to prepare for future attacks because they can better react to the constantly changing nature of online threats.

Ethical hacking techniques

Ethical hackers generally use the same hacking skills that malicious actors use to attack enterprises. Some of these hacking techniques include:

√ Scanning ports to find vulnerabilities. Ethical hackers use port scanning tools, such as Nmap, Nessus or Wireshark, to scan a company's systems, identify open ports, study the vulnerabilities of each port and take remedial action.

√ Performing network traffic analysis and sniffing by using appropriate tools.

How to become an ethical hacker

There are no standard education criteria for an ethical hacker, so an organization can set its own requirements for that position. Those interested in pursuing a career as an ethical hacker should consider a bachelor's or master's degree in information security, computer science or even mathematics as a strong foundation.

Other technical subjects including programming, scripting, networking and hardware engineering, can help those pursuing a career as ethical hackers by offering a fundamental understanding of the underlying technologies that form the systems that they will be working on. Other pertinent technical skills include system administration and software development.

Certified Ethical Hacker (CEH)

This is a vendor-neutral certification from the EC-Council, one of the leading certification bodies. This security certification, which validates how much an individual knows about network security, is best suited for a penetration tester role.

This certification covers more than 270 attacks technologies. Prerequisites for this certification include attending official training offered by the EC-Council or its affiliates and having at least two years of information security-related experience.

According to the www.payscale.com an Ethical Hacker earns average $89k USD per year.

So who wants to become an Ethical Hacker?