# Computer Hacking

By

Dr.Vinod Kumar Singh

Associate Professor Physics K .S. Saket P G College Ayodhya

Email: vks423272@gmail.com

**Hacking** is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data. An example of computer hacking can be: using a password cracking algorithm to gain access to a computer system.

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. System hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

**Who is a Hacker?**

A **Hacker** is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

**Types of Hackers**

Hackers are classified according to the intent of their actions. The following list classifies types of hackers according to their intent:

| Symbol | Description |
|---|---|
| | **Ethical Hacker (White hat):** A security hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments. |
| | **Cracker (Black hat):** A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc. |
| | **Grey hat:** A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner. |
| | **Script kiddies:** A non-skilled person who gains access to computer systems using already made tools. |
| | **Hacktivist:** A hacker who use hacking to send social, |

| | |
|---|---|
| | religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website. |
| | **Phreaker:** A hacker who identifies and exploits weaknesses in telephones instead of computers. |

**Introduction of Cybercrime**

**Cybercrime** is the activity of using computers and networks to perform illegal activities like spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrime hacks are committed through the internet, and some cybercrimes are performed using Mobile phones via SMS and online chatting applications.

**Type of Cybercrime**

- The following list presents the common types of cybercrimes:
- **Computer Fraud:** Intentional deception for personal gain via the use of computer systems.
- **Privacy violation:** Exposing personal information such as email addresses, phone number, account details, etc. on social media, hacking a websites, etc.
- **Identity Theft:** Stealing personal information from somebody and impersonating that person.
- **Sharing copyrighted files/information:** This involves distributing copyright protected files such as eBooks and computer programs etc.

- **Electronic funds transfer:** This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.

- **Electronic money laundering:** This involves the use of the computer to launder money.

- **ATM Fraud:** This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.

- **Denial of Service Attacks:** This involves the use of computers in multiple locations to attack servers with a view of shutting them down.

- **Spam:** Sending unauthorized emails. These emails usually contain advertisements.

**What is Ethical Hacking?**

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get **written permission** from the owner of the computer system and/or computer network before hacking.

- **Protect the privacy of the organization** been hacked.

- **Transparently report** all the identified weaknesses in the computer system to the organization.

- **Inform** hardware and software vendors of the **identified weaknesses**.

**Why Ethical Hacking?**

- Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's image and save an organization a lot of money.

- Fake hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

**Legality of Ethical Hacking**

**Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking**. The International Council of E-Commerce Consultants (EC-Council) provides a certification program that tests individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.

**Exploitation: Break into the target asset**

This is what the ethical hacker is being paid for – the "break-in." Using the information learned in the discovery phase, the pen tester needs to exploit a vulnerability to gain unauthorized access (or denial of service, if that is the goal). If the hacker can't break-in to a particular asset, then they must try other in-scope assets. Personally,

if I've done a thorough discovery job, then I've always found an exploit. I don't even know of a professional penetration tester that has not broken into an asset they were hired to break into, at least initially, before their delivered report allowed the defender to close all the found holes. I'm sure there are penetration testers that don't always find exploits and accomplish their hacking goals, but if you do the discovery process thoroughly enough, the exploitation part isn't as difficult as many people

believe. Being a good penetration tester or hacker is less about being a genius and more about patience and thoroughness.

Depending on the vulnerability and exploit, the now gained access may require "privilege escalation" to turn a normal user's access into higher administrative access. This can require a second exploit to be used, but only if the initial exploit didn't already give the attacker privileged access.

Depending on what is in scope, the vulnerability discovery can be automated using exploitation or vulnerability scanning software. The latter software type usually finds vulnerabilities,but does not exploit them to gain unauthorized access.

Next, the pen tester either performs the agreed upon goal action if they are in their ultimate destination, or they use the currently exploited computer to gain access closer to their eventual destination. Pen testers and defenders call this "horizontal" or "vertical" movement, depending on whether the attacker moves within the same class of system or outward to non-related systems. Sometimes the goal of the ethical hacker must be proven as attained (such as revealing system secrets or confidential data) or the mere documentation of how it could have been successfully accomplished is enough.

**Document the pen-test effort**

Lastly, the professional penetration tester must write up and present the agreed upon report, including findings and conclusions.

**How to become an ethical hacker**

Any hacker must take some common steps to become an ethical hacker, the bare minimum of which is to make sure you have documented permission from the right people before breaking into something. Not breaking the law is paramount to being an ethical hacker. All professional penetration testers should follow a code of ethics

to guide everything they do. The EC-Council, creators of the Certificated Ethical Hacker (CEH) exam, have one of the best public code of ethics available.

Most ethical hackers become professional penetration testers one of two ways. Either they learn hacking skills on their own or they take formal education classes. Many, like me, did both. Although sometimes mocked by self-learners, ethical hacking courses and certifications are often the gateway to a good paying job as a full-time penetration tester.

Today's IT security education curriculum is full of courses and certifications that teach someone how to be an ethical hacker. For most of the certification exams you can self-study and bring your own experience to the testing center or take an approved education course. While you don't need an ethical hacking certification to get employed as professional penetration tester, it can't hurt.

As CBT Nuggets trainer, Keith Barker said, "I think the opportunity to have 'certified ethical anything' on your resume can only be a good thing, but it's more of an entry way into more study. Plus, if companies see that you are certified in ethical hacking, they know you have seen and agreed to a particular code of ethics. If an employer is looking at resumes and they see someone who has an ethical hacking certification and someone that didn't, it's got to help."