Learn Hacking in 1 Day

By Krishna Rungta

Table Of Content

Chapter 1: What is Hacking? Introduction & Types

1. What is Hacking?
2. Types of Hackers
3. What is Cybercrime?
4. Type of Cybercrime
5. What is Ethical Hacking?
6. Why Ethical Hacking?
7. Legality of Ethical Hacking

Chapter 2: Potential Security Threats To Your Computer Systems

1. What is a Security Threat?
2. What are Physical Threats?
3. What are Non-physical threats?

Chapter 3: Skills Required to Become a Ethical Hacker

1. What is a programming language?
2. Why should you learn how to program?
3. What languages should I learn?
4. Programming languages that are useful to hackers
5. Other skills

Chapter 4: What is Social Engineering? Attacks, Techniques & Prevention

1. What is Social Engineering?
2. How social engineering Works?
3. Common Social Engineering Techniques
4. Social Engineering Counter Measures

Chapter 5: Cryptography Tutorial: Cryptanalysis, RC4, CrypTool

1. What is Cryptography?
2. What is Cryptanalysis?
3. What is cryptology?
4. Encryption Algorithms
5. Hacking Activity: Use CrypTool
6. Creating the RC4 stream cipher
7. Attacking the stream cipher

Chapter 6: How to Crack a Password

1. What is Password Cracking?
2. What is password strength?
3. Password cracking techniques
4. Password cracking tool
5. Password Cracking Counter Measures
6. Hacking Activity: Hack Now!
7. Password cracking steps

Chapter 7: Worm, Virus & Trojan Horse: Ethical Hacking Tutorial

1. What is a Trojan horse?
2. What is a worm?

3. What is a Virus?
4. Trojans, Viruses, and Worms counter measures
5. Trojan, Virus, and Worm Differential Table

Chapter 8: Learn ARP Poisoning with Examples

1. What is IP and MAC Addresses
2. Exercise
3. What is ARP Poisoning?
4. Hacking Activity: Configure ARP entries in Windows

Chapter 9: Wireshark Tutorial: Network & Passwords Sniffer

1. What is network sniffing?
2. Passive and Active Sniffing
3. Hacking Activity: Sniff network traffic
4. Sniffing the network using Wireshark
5. What is a MAC Flooding?
6. Counter Measures against MAC flooding
7. Sniffing Counter Measures

Chapter 10: How to Hack WiFi (Wireless) Network

1. What is a wireless network?
2. How to access a wireless network?
3. Wireless Network Authentication
4. WEP
5. WPA
6. How to Crack Wireless Networks
7. WEP Cracking Tools

8. WPA Cracking
9. General Attack types
10. Cracking Wireless network WEP/WPA keys
11. How to Secure wireless networks
12. Hacking Activity: Crack Wireless Password

Chapter 11: DoS (Denial of Service) Attack Tutorial: Ping of Death, DDOS

1. What is DoS Attack?
2. Types of Dos Attacks
3. How DoS attacks work
4. DoS attack tools
5. DoS Protection: Prevent an attack
6. Hacking Activity: Ping of Death
7. Hacking Activity: Launch a DOS attack

Chapter 12: How to Hack a Web Server

1. Web server vulnerabilities
2. Types of Web Servers
3. Types of Attacks against Web Servers
4. Effects of successful attacks
5. Web server attack tools
6. How to avoid attacks on Web server
7. Hacking Activity: Hack a WebServer

Chapter 13: How to Hack a Website: Online Example

1. What is a web application? What are Web Threats?
2. How to protect your Website against hacks?

3. Hacking Activity: Hack a Website
4. Session Impersonation using Firefox and Tamper Data add-on

Chapter 14: SQL Injection Tutorial: Learn with Example

1. What is a SQL Injection?
2. How SQL Injection Works
3. Hacking Activity: SQL Inject a Web Application
4. Other SQL Injection attack types
5. Automation Tools for SQL Injection
6. How to Prevent against SQL Injection Attacks
7. Hacking Activity: Use Havij for SQL Injection

Chapter 15: Hacking Linux OS: Complete Tutorial with Ubuntu Example

1. Quick Note on Linux
2. Linux Hacking Tools
3. How to prevent Linux hacks
4. Hacking Activity: Hack a Ubuntu Linux System using PHP

Chapter 16: CISSP Certification Guide: What is, Prerequisites, Cost, CISSP Salary

1. What is CISSP?
2. Important Domain of CISSP Certificate
3. Skills developed after CISSP certification
4. Who should do a CISSP certification?
5. How to become CISSP certified?
6. Why become CISSP Certified?
7. Course Objectives of CISSP Certification

8. Guide to ace CISSP certification
9. Salary of CISSP certified professional.

Chapter 17: 10 Most Common Web Security Vulnerabilities

1. SQL Injection
2. Cross Site Scripting
3. Broken Authentication and Session Management
4. Insecure Direct Object References
5. Cross Site Request Forgery
6. Security Misconfiguration
7. Insecure Cryptographic Storage
8. Failure to restrict URL Access
9. Insufficient Transport Layer Protection
10. Unvalidated Redirects and Forwards

Chapter 18: Kali Linux Tutorial: What is, Install, Utilize Metasploit and Nmap

1. What is Kali Linux?
2. Who uses Kali Linux and Why?
3. Kali Linux Installation Methods
4. Install Kali Linux using Virtual Box
5. Getting Started with Kali Linux GUI
6. What is Nmap?
7. How to Perform a Basic Nmap Scan on Kali Linux
8. What is Metasploit?

Chapter 1: What is Hacking? Introduction & Types

What is Hacking?

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a 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. 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.

Before we go any further, let's look at some of the most commonly used terminologies in the world of hacking.

Who is a Hacker? Types of Hackers

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.

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

Symbol	Description
	**Ethical Hacker (White hat):** A 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.

What is Cybercrime?

Cyber crime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out 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, 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.
- 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.

Summary

- Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks.
- Cybercrime is committing a crime with the aid of computers and information technology infrastructure.
- Ethical Hacking is about improving the security of computer systems and/or computer networks.
- Ethical Hacking is legal.

Chapter 2: Potential Security Threats To Your Computer Systems

A computer system threat is anything that leads to loss or corruption of data or physical damage to the hardware and/or infrastructure. Knowing how to identify computer security threats is the first step in protecting computer systems. The threats could be intentional, accidental or caused by natural disasters.

In this article, we will introduce you to the common computer system threats and how you can protect systems against them.

What is a Security Threat?

Security Threat is defined as a risk that which can potentially harm computer systems and organization. The cause could be physical such as someone stealing a computer that contains vital data. The cause could also be non-physical such as a virus attack. In these tutorial series, we will define a threat as a potential attack from a hacker that can allow them to gain unauthorized access to a computer system.

What are Physical Threats?

A physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.

The following list classifies the physical threats into three (3) main categories;

- **Internal**: The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.
- **External**: These threats include Lightning, floods, earthquakes, etc.
- **Human**: These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.

To protect computer systems from the above mentioned physical threats, an organization must have physical security control measures.

The following list shows some of the possible measures that can be taken:

- **Internal**: Fire threats could be prevented by the use of automatic fire detectors and extinguishers that do not use water to put out a fire. The unstable power supply can be prevented by the use of voltage controllers. An air conditioner can be used to control the humidity in the computer room.
- **External**: Lightning protection systems can be used to protect computer systems against such attacks. Lightning protection systems are not 100% perfect, but to a certain extent, they reduce the chances of Lightning causing damage. Housing computer systems in high lands are one of the possible ways of protecting systems against floods.
- **Humans**: Threats such as theft can be prevented by use of locked doors and restricted access to computer rooms.

What are Non-physical threats?

A non-physical threat is a potential cause of an incident that may result in;

- Loss or corruption of system data
- Disrupt business operations that rely on computer systems Loss of
- sensitive information
- Illegal monitoring of activities on computer systems Cyber
- Security Breaches
- Others

The non-physical threats are also known as **logical threats**. The following list is the common types of non-physical threats;

- Virus
- Trojans
- Worms
- Spyware
- Key loggers
- Adware
- Denial of Service Attacks Distributed
- Denial of Service Attacks
- Unauthorized access to computer systems resources such as data
- Phishing
- Other Computer Security Risks

To protect computer systems from the above-mentioned threats, an organization must have **logical security measures** in place. The following list shows some of the possible measures that can be taken to protect cyber security threats

To protect against viruses, Trojans, worms, etc. an organization can use anti-virus software. In additional to the anti-virus software, an organization can also have control measures on the usage of external storage devices and visiting the website that is most likely to download unauthorized programs onto the user's computer.

Unauthorized access to computer system resources can be prevented by the use of authentication methods. The authentication methods can be, in the form of user ids and strong passwords, smart cards or biometric, etc.

Intrusion-detection/prevention systems can be used to protect against denial of service attacks. There are other measures too that can be put in place to avoid denial of service attacks.

Summary

- A threat is any activity that can lead to data loss/corruption through to disruption of normal business operations.
- There are physical and non-physical threats
- Physical threats cause damage to computer systems hardware and infrastructure. Examples include theft, vandalism through to natural disasters.
- Non-physical threats target the software and data on the computer systems.