

Forum:[Hack Forums](#)

Thread: [The Beginner's Guide to the Basics of Hacking \[CHEAT SHEET\]](#)

Popular - January 22, 2024, 7:20 pm

Introduction:

Hacking, a term often misunderstood, simply refers to the act of gaining unauthorized access to computer systems or networks. It is crucial to understand that hacking can be both legal and illegal, depending on the intent and permission obtained. This beginner's guide aims to provide an overview of the basics of hacking to those interested in ethical hacking or cybersecurity.

1. Terminology:

- a. **Hacker:** An individual who explores and exploits vulnerabilities in computer systems for various purposes. They can be divided into ethical hackers (white-hat hackers) and malicious hackers (black-hat hackers).
- b. **Exploit:** A flaw or vulnerability in a system, software, or network that can be used to gain unauthorized access or perform malicious activities.
- c. **Vulnerability:** A weakness or gap in a system's security that exposes it to potential attacks or unauthorized access.

2. Ethical Hacking:

Ethical hacking involves legitimate, authorized efforts to identify and fix security vulnerabilities in computer systems, networks, or software. It is crucial for protecting valuable information and upholding cybersecurity.

3. Key Concepts:

- a. **Reconnaissance:** Gathering information about the target system, such as network topology, IP addresses, open ports, or software versions. This helps assess potential vulnerabilities.
- b. **Scanning:** Using network scanning tools like Nmap or Nessus to identify active hosts, open ports, and services running.
- c. **Exploitation:** Identifying and exploiting vulnerabilities to gain unauthorized access to systems. It is essential to obtain permission before undertaking any hacking activities.
- d. **Post-Exploitation:** Maintaining unauthorized access and extracting sensitive information for analysis or further exploitation.
- e. **Social Engineering:** Manipulating individuals to obtain sensitive information like passwords or access credentials through human interaction.

4. Legal Considerations:

- a. It is crucial to understand the legal implications of hacking. Unauthorized access to systems or networks without explicit permission is illegal and can lead to severe consequences.
- b. Ethical hacking should begin with obtaining permission and ensuring adherence to relevant laws and regulations.
- c. Various certifications such as Certified Ethical Hacker (CEH) or Offensive Security Certified Professional (OSCP) can help demonstrate skills and knowledge required for ethical hacking.

5. Learning Resources:

There are several resources available to learn about ethical hacking and cybersecurity, such as online courses, books, and workshops. Some popular websites and platforms include:

- Cybrary
- Udemy (warez disallowed)

- Coursera
- Offensive Security (OffSec)
- Hack The Box (HTB)

Conclusion:

Hacking, when performed ethically and legally, is a valuable skill for ensuring robust cybersecurity. It requires a deep understanding of computer systems, networks, and software, as well as the ability to identify and fix vulnerabilities. Remember, always obtain explicit permission before engaging in any hacking activities, and prioritize ethical hacking to contribute positively to the realm of cybersecurity.