Hacking

Mohammad Homayoon Fayez, Associate professor, Zealand Akademy of techologies and business

21.04.2020

Hacking

- Hacking is a broad area, which covers a wide range of topics.
- The term hacking is originated at MIT in 1960
- Hacking is the act of finding vulnerabelities in a computer system or network (software and communication protocols)
- Hacking could be used to gain unautherized access to a computer or network
  - Harm the system
  - Steal information
- Hacking could be used ligally – Ethical hacking
  - Find weaknesses in a computer system or network
  - Testing computer system or network

Types of Hacking

- **Website Hacking** − unauthorized access and control of a web server and its associated software such as databases.
- **Network Hacking** − gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
- **Computer Hacking** − The process getting unauthorized access to a computer system.
- **Email Hacking** − getting unauthorized access on an Email account
- **Ethical Hacking** −Finding weaknesses in a computer or network system for getting them fixed.
- **Password Hacking** − The process of recovering passwords from hashed data that has been stored in a database or transmitted by a computer system.

Hacker

- A person who does the act of hacking
- Seek knowledge
- Understand how the computer system works
- Harms the system
- Steals sensitive information

Types of Hackers

- **White Hat Hackers** – aka Ethical hackers
  - Do penetration testing
  - Do not harm the system.
  - Try to find out about weaknesses
- Black Hat Hackers – aka Crackers
  - Hack to gain unauthorized access
  - Harms a systems operation
  - Steal sensitive information
  - Violate privacy
  - Block network communication
- Gray Hat Hackers
  - A blend of white and Black Hat Hackers
  - Have no malicious intent
  - Exploit security weakness without permission or owners knowledge
  - The intent is to get appreciation or a little bounty by informing the owner about the weakness

Types of Hackers

- Red Hat Hackers
  - Like grey hat hackers but target the goverment agencies, sencitive information hubs
- Blue Hat Hackers
  - Bug tests the system before its launch
- Elite Hackers
  - Most skilled hackers
  - Newly discovered exploit circulate amoung these hackers
- Script kedies
  - Non-expert
  - Uses tools made by others
  - With little understanding of underlying concepts
- Neophyte – n00b, newbie, Green Hat Hacker
  - New to hacking, has almost no knowledge of underlying concepts and technologies
- Hacktivist
  - A hacker who uses technology to announce a social, religious, ideological or political message
  - Most of them involved in Denial Of Service and defame of websites

Ethical Hacking - Terminologies

- **Adware Attack**
- **Back door**
- **Bot Botnet**
- **Brute force attack**
- **Buffer Overflow**
- **Clone phishing**
- **Cracker**
- **Cross-site Scripting**
- **Denial of service attack (DoS)**
- **DDoS**
- **Exploit Kit**
- **Exploit**
- **Firewall**
- **Key**
- **Logic bomb**
- **Malware**
- **Master Program**
- **Phishing**
- **Phreaker**
- **Rootkit**
- **stroke logging**
- **Shrink Wrap code**
- **Social engineering**
- **Spam**
- **Spoofing**
- **Spyware**
- **SQL Injection**
- **Threat**
- **Trojan**
- **Virus**
- **Vulnerability**
- **Worms**
- **Zombie Drone**

Ethical Hacking - Tools

- NMAP
- Metasploit
- Burp Suit
- Angry IP Scanner
- Cain & Abel
- Ettercap
- EtherPeek
- SuperScan
- QualysGuard
- WebInspect
- LC4
- LANguard Network Security Scanner
- Network Stumbler
- ToneLoc

Ethical Hacking - Skills

As an ethical hacker, you will need to understand various hacking techniques such as −

- Password guessing and cracking
- Session hijacking
- Session spoofing
- Network traffic sniffing
- Denial of Service attacks
- Exploiting buffer overflow vulnerabilities
- SQL injection

Ethical Hacking - Process

The following Ethical hacking processes are not a standard. You may use a very different process as long as you are able to get the desired results.

- **Reconnaissance**
  - Reconnaissance is the phase where the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks.
- **Scanning**
  - In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.
- **Gaining Access**
  - In this process, the vulnerability is located and you attempt to exploit it in order to enter into the system. The primary tool that is used in this process is Metasploit.

Ethical Hacking - Process

- **Maintaining Access**
  - It is the process where the hacker has already gained access into a system. After gaining access, the hacker installs some backdoors in order to enter into the system when he needs access in this owned system in future. Metasploit is the preferred tool in this process.
- **Clearing Tracks**
  - This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process.
- **Reporting**
  - Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.