

To: Ma'am Aminah

Presented By;
M_63 - Muhammad Ammar
M_65 - Shaban Zaman
M_84 - Harris Bin Abid
M_87 - Noman Shoib

June 22nd, 2021

The Hacking

As a field

Overview

Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply saying, it is the unauthorised access to or control over computer network security systems for any illicit purpose.

Explanation

For a better understanding of hackers, we should first understand the term hacker. We can easily assume the hackers to be intelligent and highly skilled in computers. In fact,

"Breaking a security system requires more intelligence and expertise than actually creating one"

In general, we divide the hackers in white hats, black hats and grey hats according to their intent. White hat professionals hack to check their own security systems, or work for any organization to make their systems more secure. In most cases, they are part of the same organisation. Black hat hackers hack to take control over the system for personal gains. They can modify, destroy, steal or even prevent authorized users from accessing the system. They do this by finding loopholes and weaknesses in the system. They are also called crackers instead of hackers. Grey hat hackers comprise curious people who have just about enough computer language skills to enable them to hack a system to locate potential loopholes in the network security system. Grey hats differ from black hats in the sense that the former notify the admin of the network system

about the weaknesses discovered in the system, whereas the latter is only looking for personal gains. All kinds of hacking are considered illegal barring the work done by white hat hackers.

After having a general overview of what the hackers actually are, let's jump into the Origin of the 1st Hackers in History.

Origin

- ❖ **It all began in the 1960s at MIT**, origin of the term “hacker”, where extremely skilled individuals practiced hardcore programming in FORTRAN and other older languages. Some may ignorantly dub them “nerds” or “geeks” but these individuals were, by far, the most intelligent, individual, and intellectually advanced people who happen to be the pioneers and forefathers of the talented individuals that are today the true hackers. The true hackers amongst our societies have an unquenchable thirst for knowledge. Boredom is never an object of challenge for hackers. They have an almost anomalous ability to absorb, retain, and exert vast amounts of knowledge with regard to intricate details
- ❖ **In the 1970s**, “Captain Crunch” devised a way to make free long distance calls and groups of phone hackers, later dubbed “phreakers” emerged. Throughout the 1970s and halfway into the 1980s, XEROX’s Palo Alto Research Center (PARC) spit out fresh new innovations such as the laser printer and LANs.
- ❖ **During the 1990s**, Kevin Mitnick was arrested after being tracked down by Tsutomu Shimomura. The trials of Kevin Mitnick were some of the most publicized hacker trials in hacker history.

Well-Known Hackers

- ❖ **H4ck3R_777**: The Ethical hacker and enthusiast, having multiple hacking communities around the globe, having voluntary Hackers and Specialists who collaborate and guide the people in the communities.

- ❖ **Captain Zap:** Ian Murphy, known to his friends as Captain Zap, was the first cracker to be tried and convicted as a felon. Murphy broke into AT&T's computers in 1981 and changed the internal clocks that measured billing rates. People were getting late-night discount rates when they called at midday.
- ❖ **Linus Torwards:** and thousands of disparate **hackers** created **Linux**, perhaps the only alternative to Windows NT

"Every knowledge has a purpose behind it".

The purposes of hacking can be Ethical and Unethical, depending on the mindset of the Programmer or Developer. Let us discuss them, one by one.

Ethical Purposes

1. Problem Solving

Having expertise in problem solving is one of the main purposes of being a hacker. A hacker can solve complex puzzles, and crack challenging encryptions to achieve perfection in their professional jobs and to secure the organizational systems

2. Mental Exercise

Hacking is an absolute source of mental exercise. Hackers spend most of the time in Cracking, Problem Solving and figuring out new ways and techniques to solve the problem. Hackers are always expert programmers and developers as well

3. Information Harvesting

For a person, having the Hacking techniques, may know that, the information gathering phase in the hacking jobs is crucial. The first phase to hack any information, is harvesting the information from the web. This skill comes in handy if Google is unable to help us find the particular data on the internet.

4. Patching Softwares

Most of the Softwares are always Shareware or having the Paid Licences. Ethical hackers and crackers use their skills to crack the encryption methods of those protected softwares to make that available to general public

5. Personal Security

For a person, knowing the methods and ways about how the Hackers invade and how they use the techniques of social engineering to manipulate people to do what they want, and eventually steal the credentials of the user, always has an upper hand in self-defence against the Bad-Hackers (Black Hats)

6. Vulnerability Finding

Hackers use their knowledge of problem solving and bug hunting to hunt down serious vulnerability issues in websites and databases of organizations and report their findings to their respective owners. This leads to more secure Networks, and hackers are highly paid for vulnerability testing and bug hunting.

Unethical Purposes

1. Invading Databases of Organizations

Black-Hat hackers invade the websites of the organizations and then gain unauthorized access to their databases which leads to data compromise and data leaks. The intent of this activity is to black-mail the organization for a handsome amount of ransom. If not paid, they usually leak the data, or most probably sell the data at auctions. Which may eventually lead to expose millions of credentials of the users as well

2. Stealing the information

The intent of Hacking a Database of organization might be to Get, or Delete particular data, which may otherwise be legally impossible. In most of the cases, Hackers gain access to their profiles in Police Databases and delete their profiles and criminal

records. In some cases, some hackers have also upgraded their GPAs at Universities' databases.

3. Installation of Backdoors

After a successful attempt of unauthorized access to a particular organization's Database, hackers always want to access that database in the future for further hacks. For that purpose, they will never like to repeat the same process all again to achieve what they achieved before. Hackers always have smart minds, and they leave Backdoors in the System, once hacked. A Backdoor lets them access the database again without repeating the process all over again.

4. Installing Botnets

The intent of DDOS Attackers is to hack any System and make it a Botnet. A Botnet serves as a Zombie System which helps the hacker to evade the particular system, by providing the computational power of that Botnet System. This leads to more Massive DDOS Attacks.

5. Cyber Wars

Cyber wars are the wars between hackers of different countries or states, for their Religion, or Political affairs. In these wars, Hackers may target the Databases of Governments and other Sites and Databases of the Organizations and may publicize their secrets.