ANALYSIS OF INCREASING HACKING AND CRACKING TECHNIQUES

1Ms. Mayuri S. Bawane and 2Mr. Chetan J. Shelke

1M.E. First Year CSE, P.R.Pote COET, Amravati, Maharashtra, India.
2Prof. IT Department, P.R.Patil COET, Amravati, Maharashtra, India.

Abstract

In this work, the explanation is about how the computer’s containing valuable information is being unsecured and the techniques to make it secure. This technique contains information on the tools and skills a hacker uses to infiltrate computer systems and networks. This work proposes the study of hacking; as the cost of hacking attacks continues to rise, many of the businesses have been forced to increase spending on network security. However, hackers have also developed new skills and techniques that allow them to break more complex systems. Hacking involves compromising the security of networks, breaking the security of application software’s or creating malicious program such as viruses, threats, logic bombs, worms, etc[1]. This work describes the various techniques of hacking and cracking, also how they work. I proposed that the term ”hacking and cracking” historically referred to constructive, clever technical work that was not necessarily related to computer systems. Today, however, hacking and hackers are most commonly associated with malicious programming attacks on the Internet and other networks.

Keywords— Hacking, Cracking, Malicious.

1. INTRODUCTION

An intrusion can be defined as an attempt to break into or to misuse a computer system for personal use. The word misuse; is a broad, and that can mean to something as severe as stealing confidential data to something as minor such as misusing your email system for spam, using your personal profiles, etc [1]. Today, both the Internet and corporate intranets are simply crawling with people from all walks of life that are continuously trying to test the security of various systems and networks for securing their data. Although the term “hacker” is in widespread use, the sense in which it is employed is generally incorrect. Popular media and entertainment providers have used it to describe anyone who tampers with a system, particularly involved in criminal activity. The hacker penetrates a system remotely across the network. This journalistic misuse of the name upset many “traditional” hackers, who responded to the vilification of their good name by offering a new term for these individuals i.e. “crackers.” Crackers are vandals and thieves whose sole purpose is unauthorized “cracking” into secure systems for personal gain[2].

2. HACKING

In computer networking, hacking is any technical effort to manipulate the normal behavior of network connections and connected systems. Hacking is an attitude and practice surrounding the use, consumption, and production of computer-related work. Hacking uses Authorized or Unauthorized attempts to bypass the security mechanisms of an information system or network. In simple words, Hacking means finding out weaknesses in a computer or computer networks.

The term “hacker” can mean two different things:

1. Someone who is very good at computer programming, networking, or other related computer functions and loves to share his knowledge with other people.
2. Someone who uses their expert computer skills and knowledge to gain unauthorized access to systems, corporations, governments, or networks for his personal use.

Hacker seeks to understand computer, phone or other systems strictly for the satisfaction of having that knowledge. Hackers wonder how things work and have an incredible curiosity[3]. Hackers will sometimes do questionable legal things, such as breaking into systems, but they generally will not cause harm once they break in. Contrast a hacker there is a term called cracker. Hacking is the practice of modifying the features of a computer system, in order to accomplish a goal outside of the creator's original purpose. The main goal of hacker is to steal the important or the secrete information or to destroy the enemies computer network[3],[4]. Computer hacking is the most popular form of hacking nowadays, especially in the field of computer security, but hacking exists in many other forms, such as phone hacking, brain hacking, server hacking, email hacking, etc. and it's not limited to either of them.
Hackers can be of three types i.e.
1. **White hat hackers**
   
   White hat hackers are the good guys who identify the security weakness of the system or network and inform the owner about them.

2. **Gray hat hackers**
   
   A grey hat, in the hacking community, refers to a skilled hacker who is somewhere in between white and black hat hackers.

3. **Black hat hackers**
   
   A black hat hacker is the villain or bad guy, who crash into victim’s security to steal information and destroy the victims security network.

### 3. **TECHNIQUES OF HACKING**

These techniques comprises of either taking control over terminal or server to make it useless or to crash it. Following are the techniques used for hacking purpose explained as,

#### 3.1 **Denial of Service**

DoS attacks give hackers a way to bring down a network without gaining internal access. DoS attacks work by flooding the access routers with bogus traffic which can affect e-mail, TCP, packets.

#### 3.2 **Sniffing**

Sniffing refers to the act of intercepting TCP packets. This interception can happen through simple eavesdropping or something more sinister which modifies the packets.

#### 3.3 **Spoofing**

Spoofing means pretending to be something you are not. In Internet terms it means pretending to be a different Internet address from the one you really have in order to gain something.

#### 3.4 **Viruses and Worms**

Viruses and worms are self-replicating programs or code fragments that attach themselves to other programs (viruses) or machines (worms). Both viruses and worms affect the networks by flooding them with huge amounts of bogus traffic, usually through e-mail.

#### 3.5 **Keyloggers**

Suppose, everything you type in the system is mailed to the hacker...!! It would be easy to track your password from that. Key loggers perform similar functionalities. So next time you type anything. Beware...!!

#### 3.6 **Social Engineering**

This was one of the oldest tricks for hacking. If the hacker try to convince user that you are a legitimate person from the system and needs your password for the continuation of the service or some maintenance. But it won’t work because it is an old technique.

#### 3.7 **Fake Messengers**

In this hacking technique, attacker send the fake messages so that the user can fill his own information like login id, password, etc[4],[5].

### 4. **CRACKING**

Cracker is the common term used to describe a malicious hacker. Crackers get into all kinds of mischief, including breaking or "cracking" copy protection on software programs, breaking into systems and causing harm, changing data, or stealing. Hackers regard crackers as a less educated group of individuals that cannot truly create their own work, and simply steal other people's work to cause mischief, or for personal gain. Crackers break into or crack systems with
malicious intent. They are out for personal gain: fame, profit, and even revenge. They modify, delete, and steal secret information, often making other people miserable[6].

Figure 2 Cracking

5. TECHNIQUES OF CRACKING
There are three basic types of password cracking techniques that can be explained below,

1. Dictionary
Cracker can run a file of words against user accounts, and if the password is found to be a simple word, it can be found pretty quickly.

2. Hybrid
We know that the user utilize common method to change passwords is to add a number or symbol to the end. A hybrid attack works like a dictionary attack, but adds simple numbers or symbols to the password attempt.

3. Brute force
This technique of hacking is complex one and time-consuming, but comprehensive way to crack a password. Every combination of character is tried until the password is broke[6],[7].

6. PROPOSED IDEA
There are a few variations on the types of attacks that successfully employ hacking. Although some are relatively dated, others are very pertinent to current security concerns. Hacking consists of several steps, which I will briefly outline here, then explain in detail[8]. First, the target host is chosen. Next, a pattern of trust is discovered, along with a trusted host. The trusted host is then disabled, and the target’s TCP sequence numbers are sampled. The trusted host is impersonated, the sequence numbers guessed, and a connection attempt is made to a service that only requires address-based authentication. If successful, the attacker executes a simple command to leave a backdoor.

Details of an Attack
Hacking in brief consists of several steps:
1. Selecting a target host (or victim).
2. The trust relationships are reviewed to identify a host that has a “trust” relationship with the target host.
3. The trusted host is then disabled and the target’s TCP sequence number are sampled.
4. The trusted host is then impersonated, the sequence number forged (after being calculated).
5. A connection attempt is made to a service that only requires address-based Authentication (no user id or password).
6. IF a successful connection is made, the attacker executes a simple command to leave a backdoor.

7. DIFFERENCE BETWEEN HACKING AND CRACKING
The main difference between these two techniques is “Hacking builds things” and “Cracking breaks them”. Hacking and cracking are the two different forms of Internet and computer related privacy, usually hazardous. In this article, I’ll be discussing the differences between hacking, and cracking[8]. They are two completely different things, but people usually get confused between the two, they both end with a similar sound ‘acking’ and they’re both malicious forms of cyber activity. In this article, I’ll be talking about the difference between hacking, and cracking.
A hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multiple of reasons, such as profit, protest, or challenge. Malicious attacks on computer networks are officially known as cracking, while hacking truly applies only to activities having good intentions. Most non-technical people fail to make this distinction. Besides all these, it’s extremely common to see the term “hack” misused and be applied to cracks as well[9],[10].
8. CONCLUSION
In this work, at last I want to conclude that, how the attacker affect the security which tremendously affect our growing environment. Many security experts are predicting a shift for hacking in which hackers can exploit a weakness in a particular service to send and receive information under false identities. As Security professionals, we must remain current with the Operating Systems that we use in our day to day activities. A steady stream of changes and new challenges is assured as the hacker community continues to seek out vulnerabilities and weaknesses in our systems and our networks. Understanding how and why attacks are used, combined with a few simple prevention techniques, can help protect your network from hacking[7],[11]. Our main goal in this paper is to show how these two techniques i.e. hacking and cracking are performed in various ways and how the attacker can easily attack the users system using these two techniques.

REFERENCES
[9] Practical Hacking Techniques and Countermeasures by Mark D. Spivey, CISSP
[10] Is Ethical Hacking Ethical?, Danish Jamil et al. / International Journal of Engineering Science and Technology (IJEST)

AUTHOR
Miss. Mayuri S. Bawane is a student of M.E in Computer Science & Engineering from P.R. Pote COET, Amravati under SGBAU, India.

Prof. Chetan J. Shelke is a Professor in P.R. Patil College of Engg. He did his M.E from MIRPM, India.