Seminar Report

Topic:

Paper Code : CS 782

Presented By:

Kunal Nandy (11101031007)
Amit Bhusan Srivastava (11101031002)
Deba Prasad Hazra (11101031005)
Kunal Das (11101031016)

4th Year, C.S.E. Dept.
Govt. College of Engg. & Textile Technology
Berhampore, West Bengal

What is Windows Hacking?

What is Windows?

- **Windows** is a family of Microsoft operating systems.
- **Microsoft Windows** is the name of several families of operating systems by Microsoft. They can run on several types of platforms such as servers, embedded devices and, most typically, on personal computers.

What is Hacking?

- Hacking is an act of penetrating computer systems to gain knowledge about the system and how it works.
- Hacking means illegally accessing other people's computer systems for destroying, disrupting or carrying out illegal activities on the network or computer systems.
- Unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network.

History of Hacking

Hacking has been around for more than a century. In the 1870s, several teenagers were flung off the country's brand new phone system by enraged authorities. Here's a peek at how busy hackers have been in the past 35 years.

- Early 1960s

University facilities with huge mainframe computers, like **MIT's artificial intelligence lab,** become staging grounds for hackers. At first, "hacker" was a positive term for a person with a mastery of computers who could push programs beyond what they were designed to do.

- Early 1970s

John Draper makes a long-distance call for free by blowing a precise tone into a telephone that tells the phone system to open a line. Draper discovered the whistle as a give-away in a box of children's cereal. Draper, who later earns the handle "Captain Crunch," is arrested repeatedly for phone tampering throughout the 1970s.

John Draper

- Early 1980s

In one of the first arrests of hackers, the FBI busts the Milwaukee-based 414s (named after the local area code) after members are accused of **60 computer break-ins** ranging from Memorial Sloan-Kettering Cancer Center to Los Alamos National Laboratory.

Two hacker groups form, the **Legion of Doom** in the United States and the **Chaos Computer Club** in Germany.

- Late 1980s

At 25, veteran hacker **Kevin Mitnick** secretly monitors the e-mail of MCI and Digital Equipment security officials. He is convicted of damaging computers and stealing software and is sentenced to one year in prison.

An Indiana hacker known as **"Fry Guy"** — so named for hacking McDonald's — is raided by law enforcement. A similar sweep occurs in Atlanta for **Legion of Doom** hackers known by the handles "Prophet," "Leftist" and "Urvile."

- Early 1990s

Hackers break into **Griffith Air Force Base,** then pewwwte computers at **NASA** and the **Korean Atomic Research Institute.** Scotland Yard nabs "Data Stream," a 16-year-old British teenager who curls up in the fetal position when seized.

Kevin Mitnick is arrested (again), this time in Raleigh, N.C., after he is tracked down via computer by **Tsutomu Shimomura** at the San Diego Supercomputer Center.

- Late 1990s

A Canadian hacker group called the Brotherhood, angry at hackers being falsely accused of electronically stalking a Canadian family, break into the Canadian Broadcasting Corp. Web site and leave message: **"The media are liars."** Family's own 15-year-old son eventually is identified as stalking culprit.

Hackers pierce security in **Microsoft's NT operating system** to illustrate its weaknesses.

- 1997

Popular Internet search engine Yahoo! is hit by hackers claiming a **"logic bomb"** will go off in the PCs of Yahoo!'s users on Christmas Day 1997 unless Kevin Mitnick is released from prison. "There is no virus," Yahoo! spokeswoman Diane Hunt said.

- 1998

Hackers claim to have broken into a Pentagon network and stolen software for a **military satellite system.** They threaten to sell the software to terrorists.

Hacker group L0pht, in testimony before Congress, warns it could **shut down nationwide access to the Internet** in less than 30 minutes. The group urges stronger security measures.

- 2000

Hackers break into Microsoft's corporate network and access source code for the latest versions of Windows and Office.

- 2001

Microsoft becomes the prominent victim of a new type of hack that attacks the domain name server. In these denial-of-service attacks, the DNS paths that take users to Microsoft's Web sites are corrupted. The hack is detected within a few hours, but prevents millions of users from reaching Microsoft Web pages for two days.

Types of Hacking

- Password Hacking

This is a simple hacking process coming from the invention of network. We generally copy our password, that can be hacked by using simple ASP or JavaScript program.

```
<Script Language="JavaScript">
var content = clipboardData.getData("Text");
alert(content);
</Script>
```

- Customization of Windows System

The Windows' many non-changable area can be changed by hacking Windows. The word "Start" or the right-clicked pop-up menu or the logo or the Strart up screen, everything can be hacked by simply editing the registry.

- Change in Server Database

Hacking in the server may change the server database. Hacking is as if the person gets a right to access the machine without any interruption.

- Data Thefting

Accessing the remote machine may cause the thieving of data from that machine.

- Unauthorized Access

As hacking is a process to access the remote machine, it is fully unauthorized and the hacker may keep the remote machine into his catch.

Types of Hackers

- Black Hat Hacker

Those hackers make any kind of loss of hacked machine and a problem for general people, are called as black hat hackers.

- White Hacker

Those hackers are registered and help the persons only by searching the weakness of a system, are called white hackers.

Disadvantages of Hacking

- Publishing of secret data
- Unauthorized access of mailbox, server etc.
- Error in online banking
- Losing of data

Advantages of Hacking

- Finding the weakness part of the system
- Prevent of hacking
- To isolate hacker

Differences with Hacking

- Patching

Patch is a fix for a software program where the actual binary executable and related files are modified. Often this is used to repair a software bug.

- Cracking

Password cracking is the process of discovering the plaintext of an encrypted computer password.

System cracking or security cracking is the defeating of security devices in computer networks.

Software cracking is the defeating of software copy protection

- Thefting

Thefting is generally the stealing of password.

Updration of Hacking

- Fishing

The name fishing has come to know as if the hackers catches the fish from the network stream. Generally secret data are stolen from the network data stream.

Tools of Hacking

- Spyware

Spyware is computer software that collects personal information about users without their informed consent. The term, coined in 1995 but not widely used for another five years, is often used interchangeably with adware and malware (software designed to infiltrate and damage a computer).

- Adware

Adware or **advertising-supported software** is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.

- Malware

Malware or **malicious software** is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a portmanteau of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

- Trojan-horse

a **Trojan horse** is a malicious program that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed.

There are two common types of Trojan horses. One, is otherwise useful software that has been corrupted by a cracker inserting malicious code that executes while the program is used. Examples include various implementations of weather alerting programs, computer clock setting software, and peer to peer file sharing utilities.

The other type is a standalone program that masquerades as something else, like a game or image file, in order to trick the user into some misdirected complicity that is needed to carry out the program's objectives.

Prevention of Hacking

To prevent hacking, we have to be concious about the usage and every step we do. A wrong step may hack the system and when it will be done, we will be full hopeless. There nothing be left.

Conclusion

We cannot take a end in the conclusion, because the hacking is still going on. It was running from the past and will run for hundreds of years. As everything have a negative side, the computing system has also a negative side and through it some black hat hackers trespass. So the main thing is to detect the way and seal these way. This may draw a conclusion in hacking history,