International Journal of Students Research in Technology & Management
Vol 1(2), April 2013, pg 89-93

CYBER SECURITY

Mandar Tawde, Pooja Singh, Maithili Sawant, Girish Nair

Information Technology, Government Polytechnic Mumbai
49, Kherwadi Ali Yawar Jung Marg, Bandra (E), Mumbai-400051, India
mandar258@gmail.com, maithilisawant229@gmail.com

Abstract

This document gives information about Hacking. Some Types of hacking, some tools of hacking and some preventive measures in order to stop hacking. It will help every computer user for the security of his system. As hacking is very upcoming and serious problem for many fields, the study of cyber security is important.

Keywords - The best way of offending is defending

I. WHY HAVE WE OPT CYBER SECURITY ?

Hacking is hot and rapid growing national problem for which the market may fail to make a solution because individuals often select less than optimal security levels in a world of positive transaction cost.

II. SCANDALOUS HACKINGS

To show the seriousness of hacking we have included some very scandalous hacking incidences.

A. 1960s

The Dawn of Hacking

The advent of 1st computer hacking emerged at MIT. They were the group of people, who forcefully entered into model train group and began to hack the electrical trains, tracks and switches to make them perform faster and differently. But few due to their curiosity became typical hacker.

B. 1995

The Mitnick Takedown

Serial cyber trespasser Kevin Mitnick is captured by federal agents and charged with stealing 20,000 credit card numbers.

C. 1998

The Cult of Hacking and the Israeli Connection

The hacking group Cult of the Dead Cow releases its Trojan horse program, Back Orifice—a powerful hacking tool--at Def. Con. Once a hacker installs the Trojan horse on a machine running Windows 95 or Windows 98, the program allows unauthorized remote access of the machine.

D. 1999

E. Havoc of Mellisa virus

Mellisa virus hit Microsoft and other big company which lead them to temporarily terminate their e-mail systems.

III. WHAT IS CYBER SECURITY?

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

IV. HACKING

- Hacking is a process to bypass the security mechanisms of an information system or network.
- In common usage, hacker is a generic term for a computer criminal, often with a specific specialty in computer intrusion. While other definitions peculiar to the computer enthusiast community exist, they are rarely used in mainstream context.
- Hacking is an unauthorized use of computer and network resources. (The term "hacker" originally meant a very gifted programmer. In recent years though, with easier access to multiple systems, it now has negative implications.)

V. TYPES OF HACKING

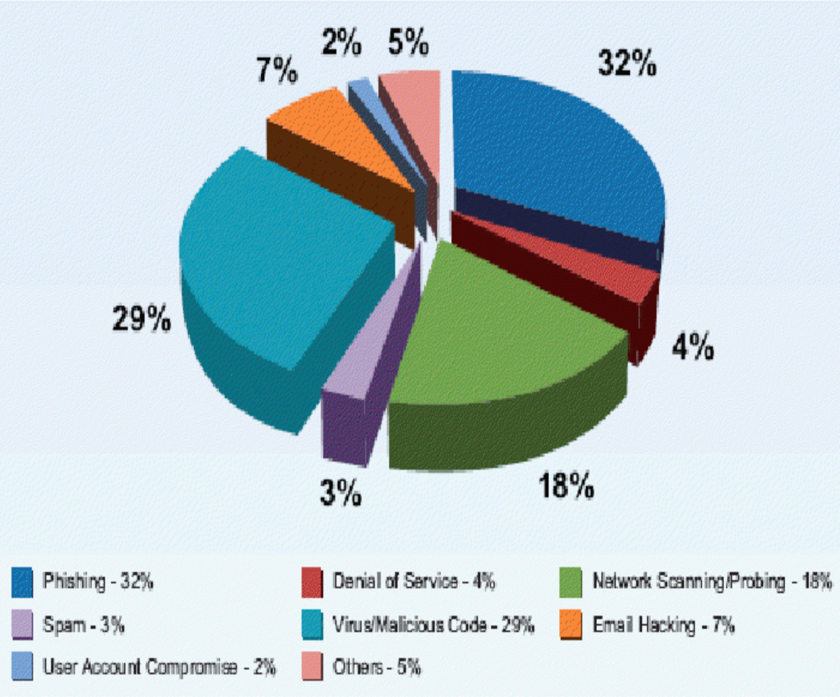


Fig 1 Security Incidents reported during 2009

A. Computer Hacking

Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose.

Types of Computer Hackers-There are two types of computer hackers.

- Attitude
- Purpose

B. *Password Hacking*

- Password hacking is the process of recovering secret password from data that has been stored in or transmitted by a computer system.
- Password hacking can help a legitimate user retrieve a forgotten password.
- System administrators may use password hacking as a preventive tactic, to check for easily hacked passwords in order to modify them for increased security.
- Unauthorized users hack passwords to gain access to a secure system.

C. *Phishing*

- Its art of managing the victim to access a duplicate web pages
- Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
- Case study: eBay, yahoo.

D. *Virus 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 attempt to shut down networks by flooding them with massive amounts of bogus traffic, usually through e-mail.

VI. TOOLS OF HACKING

A. *RAT*

- RAT is a remote administration tool or Remote Access Trojan
- It gives the admin privileges to the attacker

B. *NetCat*

- Netcat has been dubbed the network Swiss army knife.
- It is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol

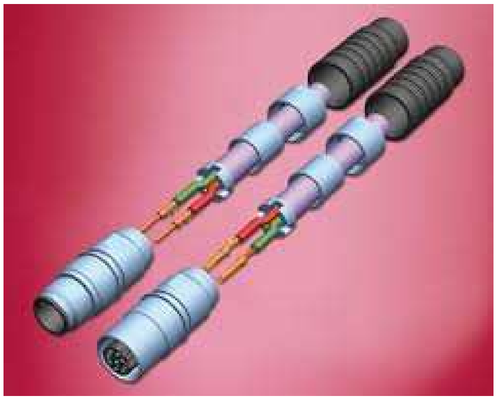
- Netcat is designed to be a dependable "back-end" device that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and investigation tool; since it can produce almost any kind of correlation you would need and has a number of built-in capabilities.
- Its list of features includes port scanning, transferring files, and port listening, and it can be used as a backdoor.

C. *Ethereal*

- Ethereal is a free network protocol analyzer for UNIX and Windows.
- Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session.

D. *NetBus*

Netbus is programmed software which requires, a device which looks like this.



This devise is attached at the ports. This method is used for getting passwords, banking details, etc.

- In 1999, Net Bus was used to plant child pornography on the work computer of a law scholar at Lund University. The 3,500 images were discovered by system administrators, and the law scholar was assumed to have downloaded them knowingly. He lost his research position at the faculty, and following the publication of his name fled the country and had to seek professional medical care to cope with the stress. He was acquitted from criminal charges in late 2004, as a court found that Net Bus had been used to control his computer.

VII. PREVENTIVE MEASURES.

To Prevent Hacking we should use:-

A. *Anti-viruses*

In order to damage our security system hackers generally try to send malwares, spam wares, etc. Antivirus is best tool to defend their access in our system.

B. *Eraser*

Eraser is an advanced security tool (for Windows), which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns. Works with Windows 95, 98, ME, NT, 2000, XP and DOS. Eraser is free software and its source code is released under GNU General Public License.

C. *Firewall*

One way of being warned that malware has infected your machine is by using a software firewall (this also works well for viruses too). When a software firewall catches a program trying to make a connection, it will alert you, give you the name of the program, and ask if you want to block it from the Internet.

VIII. INFERENCE

If with a few advancements in the way we are using the internet we can avoid a big threat and make web a safer place. Some of them would be

- Using a good proxy server
- Using vulnerability testers like nmap
- Limiting the number of open ports

IX. ACKNOWLEDGMENT

Cyber security has become an important part of our life. We have nurtured it from last days and while doing so we received in addition the compliments a lot of suggesting from publisher, authors, and professors.

REFERENCES

[1] Vaidihi and Gaurav “Hacker5”ed.2nd.

[2] Ankit Fadiya-“Ethical hacking” ed.2d.

[3] The google website. www.google.org

[4] *The Wikipedia website. www.wikipedia.org*