Hacking: intimidation and Defenses

Jagjit Bhatia, Asst prof,
Department of Computer Science, Hans Raj Mahila Maha Vidyalaya, Jalandhar

Abstract

This era is digital era, everywhere and everything is now converting into its digital contour like money, business etc. There are serious problems arising about the security of digital objects and worst part is that our digital society is least concerned about this problem. Simple tricks and techniques are there to damage a lot. With this consideration my paper is about the various common attacks and remedies. In introduction part my aim is to sensitize the seriousness of hacking by quoting some incident and the losses that has to bear the society. Next my aim is to explain the various generations of hackers from their emergence to their existing maturity level. Next I have explained some very simple and serious attack which can be performed by the intermediate user of computer and also suggest the remedies to secure our system.

Keywords: SMTP (Simple mail transfer protocol), TCP, BIOS, LM/NTLM, SAM

Introduction

In this digital era every thing is organized as electronic data. Banks, Government offices, School, hospitals and even money in your wallet in the form of credit or debit card. This means all the sensitive information is organizes in the form of electronic data. Even your money is travelling in air in the form of electronic data. Whenever we make monetary transaction through net banking, from credit card or debit card. Do we ever think about the security of this electronic data or money? The ever-increasing computer world is also increasing the exposure to malignant computer hacker. We know about these mysterious hackers but we are unaware about the damage they can do. In 2003 a computer viruses damage the business cost $55 billion which was created by the hacker [1]. In 2004 Computer security Institute conducted a survey and reported that during 12 months 100 percent respondent indicated a web related attack [2] . According to joint survey conducted by CSI and FBI in American businesses, more than 50% firms are affected by system intrusion over last year but no one report this intrusion to anyone [3].

1. History of Hacking

The culture of hacking begins during 1960s. In this year there was an intellectual movement. There was a bustling of exploring the unknown, unconstitutionally knowing the secret. The implementation ARPANET during 1967 the computers of four universities interlinked [4]. With the completion of ARPANET many other universities had become the part of network. So these campuses were able to share their experiences and knowledge. In this way they formed the first hacker culture [5].Computing think tank AT&T Bell Lab was one of the locus of hacking. With the open source UNIX operating system had prominent the first stage of hacking. This distribution the knowhow of expertise to society freely which was further used for activities like breach in security. At that time the word ‘hack’ actually considered as programming shortcuts to complete task faster. These hackers were not interested in hacking for any malicious reasons [6]. The second generation of hacker emerges during the early days in 1970s. The main target of these generation hackers was telephone system. A phone phreaks Jhon Drapers emerged as a hacker during this generation. Jhon invented a toy known as blue box to access AT&T's long-distance switching system to allow making free long distance call. Steve Wozniak and Steve Jobs, the founders of Apple Computer, had started manufacturing and by selling of these blue boxes [7]. The third generation of hacking is considered as “Golden age” during the period 1980 through 1991. During this period various hacking groups emerged like Legion Doom and the Chaos Computer Club. During this time a popular movie “War Games” introduces a term hacking [7] . During this time hackers also started his publication called “Zines” in which they had published 2600 papers and articles. During 1994 US government passes legislation i.e. to break into computer system is a crime and considered as computer fraud and abuse. Two year later, by Robert T. Morris a Cornell university graduate student a self replicated worm was invented and released and as first convicted under new law [8]. During 1994 to 1998 the internet was becoming more commercialized and era of ecommerce has started. A gang of Russian hackers is charged with breaking into Citibank’s computers and draw off $ 10 million. After year 2000 internet had become more prominent toy as well as playground for the hackers and crackers. They are classified and known for destructive acts via internet.

1.1 Classification of Hackers

1.1.1 Coders

Coders are the programmers who have the ability to find the unique vulnerability in existing software and to create working exploit codes. These are the individuals with a deep understanding of the OSI Layer Model and TCP/IP Stacks.

1.1.2 Admin

Admin the computer guys who have experience with several operating systems, and know how to exploit several existing vulnerabilities. A majority of Security Consultants fall in this group and work as a part of Security

1.1.3 Script Kiddies

Script Kiddies are the bunnies who use script and programs developed by others to attack computer systems and Networks. They get the least respect but are most annoying and dangerous and can cause big problems without actually know are doing.

2. <u>Simple hacking techniques used by hackers and how to flee</u>

2.1 Email Hacking : Electronic mail often abbreviated as e-mail or email is any method of creating, transmitting, or storing primarily text-based human communications with digital communications systems.

Fake Email: Fake Email means an Email which has come from an Email ID which was not sent by the Original Email ID Owner. There are so many ways to send the Fake Emails even without knowing the password of the Email ID. The Internet is so vulnerable that you can use anybody's Email ID to send a threatening Email to any official personnel.

Methodology

An **open mail relay** is an SMTP server configured in such a way that it allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users. An attacker can connect the Open Relay Server via Telnet and instruct the server to send the Email [9]. It requires no password to send the Email. Hackers normally search for open relay SMTP server on the web and use that SMTP server to generate spam on the net by simple Telnet commands. If your SMTP server accepts incoming TCP connections from the Internet, your server can be used by spammers/hackers as a mail relay engine. Mail relays can distribute their messages (SPAM) all over using your server as an open relay.

To test for open relay telnet into your mail server as follows [10]:

```
C:\>telnet mailserver.domainname.com 25
220 mailserver.domainname.com ESMTP server (InterMail vK.4.04.00.00) ready Mon, 13 April 2015 13:56:00 -0500
helo
250 mailserver.domainname.com
mail from:<sender@xyz.com>
250 Sender <sender@xyz.com> Ok
rcpt to:<receiver@abc.com>
250 Recipient <receiver@abc.com> Ok
data
354 Ok Send data ending with <CRLF>.<CRLF>
hello this is a test .
250 Message received: 20020311193728.DLVD25322.mailserver@[123.45.98.765]
quit
221 mailserver.domainname.com ESMTP server closing connection
```

Instead of that many websites are freely available on the internet which provides the services to check out open relay. I did try to find out the open relay with the help of such website and I find the dangerous result about the site of a reputed university.

One of the website used by hackers to find open relay server on the web

http://www.mydnstools.info/smtprelay/

Result shows most dangerous part [11].

<< 220 mail.lathawinserver.com ESMTP MailEnable Service, Version: 6.0-- ready at 04/12/15 12:50:48

Test 1 from	**Test 2 from**

<relaytest@mydnstools.info> to <returntest%mydnstools.info@www.gndu.ac.in>... ok
>>> RSET
<<< 250 Requested mail action okay, completed
>>> MAIL FROM:<relaytest@mydnstools.info>
<<< 250 Requested mail action okay, completed
>>> RCPT TO:<returntest%mydnstools.info@www.gndu.ac.in>
<<< 503 Requested mail action okay, completed
	<relaytest@www.gndu.ac.in> to <returntest@mydnstools.info>... ok
	>>> RSET
	<<< 250 Requested mail action okay, completed
	>>> MAIL FROM:<relaytest@www.gndu.ac.in>
	<<< 250 Requested mail action okay, completed
	>>> RCPT TO:<returntest@mydnstools.info>
	<<< 503 Requested mail action okay, completed

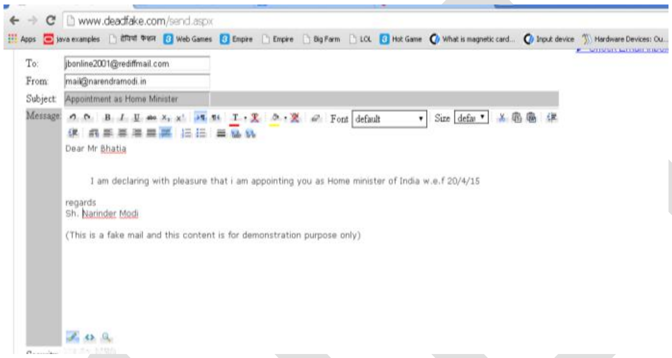
Remedies: Stopping the relay

If you discover that your organization has an open relay, you need to stop it. To stop open relaying on the Default SMTP Virtual Server, follow these steps:

1. Go to Start | All Programs | Microsoft Exchange | Exchange System Manager.
2. Expand Servers, expand <Servername> (the name of your Exchange server), expand Protocols, and expand SMTP.
3. Right-click Default SMTP Virtual Server, and select Properties.
4. On the Access tab, click the Relay button at the bottom.
5. Select the Only The List Below check box, and remove any entries in the list that aren't a part of your business network.
6. Select the Allow All Computers Which Successfully Authenticate To Relay, Regardless Of The List Above check box.
7. Close all dialog boxes.

Your Exchange server will now only relay mail for authenticated computers and computers that you have specifically allowed.

2.2 Sending Fake Email via Web Scripts



To: jbonline2001@rediffmail.com
From: mail@narendramodi.in
Subject: Appointment as Home Minister
Message:
Dear Mr Bhatia

I am declaring with pleasure that i am appointing you as Home minister of India w.e.f 20/4/15

regards
Sh. Narinder Modi

(This is a fake mail and this content is for demonstration purpose only)

Figure – 1.

Methodology : Web languages such as PHP and ASP contain the mail sending functions which can be used to send Emails by programming Fake headers i.e. From: To: Subject: .There are so many websites available on the Internet which already contains these mail sending scripts. Most of them provide the free services as shown in figure-1 [11].

Remedies : Email Tracing

Tracing an Email means locating the Original Sender and getting to know the IP address of the network from which the Email was actually generated. Locating Original Sender in not always possible but we have tried our best to get it. To get the information about the sender of the Email we first must know the structure of the Email. As we all know the traveling of the Email. Each message has exactly one header, which is structured into fields. Each field has a name and a value. Header of the Email contains all the valuable information about the path and the original sender of the Email.

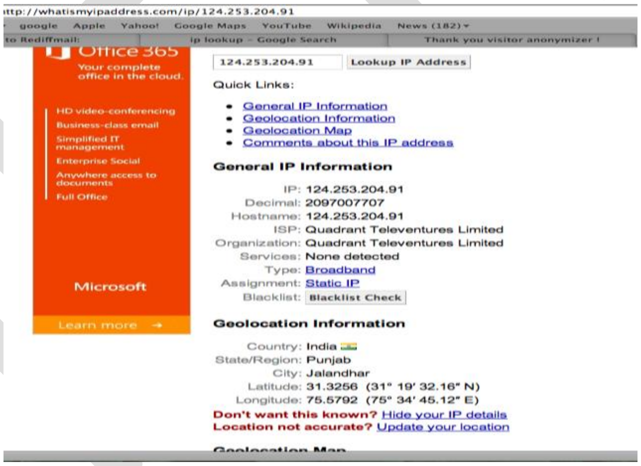
Header Fields

From: Email Address where the Email has come from.
To: Email Address of the destination.
Subject: Subject of the Email
Date: The Local Time of the server when the message was sent.
Bcc: Blind Carbon Copy
Cc: Carbon copy
Content-Type: Information about how the message has to be displayed, usually a MIME type
In-Reply-To: Message-ID of the message that this is a reply to.
Received: Tracking information generated by mail servers that have previously handled

a message **References:** Message-ID of the message that this is a reply to, and the message-id of this message, etc.

Email Headers
Return-Path: < mail@narendramodi.in >
Delivered-To: jbonline2001@f5.p22.mail.in.rediffmail.com
Received: (qmail 8193 invoked from network); 20 April 2015 08:11:36 -0000
X-IN-CTCH-RefID: str=0001.0A150202.518F4EB8.0115,ss=1,re=0.000,fgs=0
X-REDIFF-SENDER-VERIFY: D=-2, P=D
Received: from zebra732.startdedicated.com (188.138.112.172)
by 0 with SMTP; 20 April 2015 08:11:36 -0000
Received: from zebra732 ([127.0.0.1]) by zebra732.startdedicated.com with Microsoft SMTPSVC(7.5.7601.17514);
Mon, 20 April 2015 09:11:34 +0100
X-Mailer: DeadFake Mailer (http://deadfake.com)
X-Originating-Ip: 124.253.204.91
MIME-Version: 1.0
From: mail@narendramodi.in
To: jbonline2001@rediffmail.com
Date: 20 April 2015 09:11:34 +0100
Subject: About Refresher Professional Studies
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: base64
Return-Path: mail@narendramodi.in

You can easily get the IP Address of the sender from the header and then can locate the sender. Check the email header, from there you will find the IP address of mail sender and you can get the location of that IP i.e. This IP belongs to which city. When you will open the mail there will be a hyperlink on the upper side of the mail like **show full header when you click on that header you will find like** Here You can find the IP address in shaded red that means you have received this mail from this particular IP address. Now we have to find out the location of this particular IP by any ip lookup site[13]. Here we can find out that mail is sent from anywhere in Jalandhar not from Prime minister office New Delhi as shown in Figure-2.



Quick Links:

- General IP Information
- Geolocation Information
- Geolocation Map
- Comments about this IP address

General IP Information

IP: 124.253.204.91
Decimal: 2097007707
Hostname: 124.253.204.91
ISP: Quadrant Televentures Limited
Organization: Quadrant Televentures Limited
Services: None detected
Type: Broadband
Assignment: Static IP
Blacklist: Blacklist Check

Geolocation Information

Country: India
State/Region: Punjab
City: Jalandhar
Latitude: 31.3256 (31° 19' 32.16" N)
Longitude: 75.5792 (75° 34' 45.12" E)
Don't want this known? Hide your IP details
Location not accurate? Update your location

Geolocation Map

Figure-2

2.3 System Hacking : Windows User account Password Security Architecture. Windows User Login Passwords are stored and transmitted in an Encrypted form called a Hash[14]. These Hashes are saved in the SAM File. SAM stands for Security Account Manager. SAM File can be found at **C:\Windows\System32\Config\SAM**

When a User is created, the Username and Password are stored in the SAM file in the form of Hash. When a user logs on to the System and Enters the password, a Hash is generated and compared to the stored Hash. If the entered and the stored hashes match, the user is authenticated. This is called the LM/NTLM Challenge/Response. Passwords may be cracked manually or with automated tools such as a Brute-force method or the Rainbow table attack. Once the Windows start it start using the information in the SAM file, so the SAM file becomes Inaccessible. It cannot be Opened, Copied, Moved, Renamed or Deleted

Methdology: How Windows User Login Password can be attacked

Live Boot Disk Attack Software: Active Password Recovery can be used to create Live Boot Disks for Windows Operating System Live Boot Disk can be used to start the Windows and access the SAM File [15]. Attacker can Remove the Passwords from the User Accounts or can set new Passwords on the Accounts.

Brute Force Attack: Brute force Password Guessing is just what it sounds like: Trying a Random approach by Attempting Different Passwords and hoping that One works. Some logic can be applied by hacker by trying passwords related to the person’s name, job title, hobbies, or other similar items[16]. Brute force randomly generates passwords and their associated hashes. Various tools are used by hackers to perform the Brute force attack on the Windows SAM File. One of the most famous of them is Cain and Able[17].

Net User: Command Prompt : Windows Command Prompt Utility, Net User, can be also be used to manipulate the User accounts in Windows. The Commands are as follows:

- To check the User Accounts: **Net User**
- To Add a New User Account**: Net User Username Password /add**
- To Delete a User Account: **Net User Username /delete**
- To Change the Password of User Account: Net **User Username ***

Sticky Keys Backdoor : Sticky Keys application can be used by hacker as the Backdoor in Windows Operating System. Command Prompt file ‘CMD.EXE’ can be renamed to SETHC.EXE’ in **C:\Windows\System32** Folder. After this one can hit the Shift Key 5 times on the User Login Screen and will get the Command Prompt right there. Net User can be used to modify User Accounts thereafter [18].

Privilege Escalation: Once the Administrator account is hacked, one can easily Login with the Administrator User Account and promote any User Account to give him the Administrator privileges. One more thing which an attacker can do is to boot the computer from the Live CD and change the SAM file to promote any Limited User account to Administrator [19].

Remedies : Counter Measures for the Windows User Login Password Attack

Configuring a Strong Login Password : A strong password is less susceptible to attack by a hacker. The following rules should be applied when you’re creating a password, to protect it against attacks:

- Must not contain any part of the user’s account name
- Must have a minimum of eight characters

Change the Boot Sequence: You should change the boot sequence in the BIOS so that your computer is not configured to boot from the CD first. It should be configured as Hard Disk as the First Boot Device. This will protect your computer from the Live Boot Disks Attack

Conclusion

Digital era is changing the lifestyle and shaping the life of human being but the bad or even worst part if digital world is security threats. The dangerous issue is our ignorance about this security threats. I feel bad while quoting this even some technological institutions important data is on web without any security. Now this is time to realize the need of security to our digital objects. Now these days computer has become the toy of kids. They are getting technological knowhow by self learning process. With their growth they are getting more expertise and this expertise can used as other end of mirror. Awareness and protection is must to protect ourselves and to our techo-savy generation.

.

References

[1] Blake, Roger (1994). Hackers in the Mist. Chicago, IL: Northwestern University. *Computer Economics Institute (2002)*.

[2] SecurityStats.com (2004). Virus Statistics, January 16, 2004. Available at: http://www.securitystats.com.

[3] Computer Security Institute (2002). CSI/FBI Computer Crime and Security Survey. Available at: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

[4] History of ARPANET Behind the Net - The untold history of the ARPANET Or - The "Open" History of the ARPANET/Internet By Michael Hauben march 2009

[5] http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_Symantec Internet Security Threat Report, Trends for January 06–June 06, Volume X. Sep. 2006.

[6] Frontline: Cyber war: Interviews: Hacker. Retrieved September 25, 2005 from http://www.pbs.org.

[7] Slatalla, M. A brief history of hacking. Retrieved November 5, 2005 from http://tlc.discovery.com.

[8] Leung, L. (2005, June 20). Hackers for hire: Bringing in ethical hacker consultants is the latest in security defense. Retrieved November 5, 2005 from http://www.networkworld.com.

[9] http://www.mydnstools.info/smtprelay/www.yahoomail.com

[10] http://mxtoolbox.com/diagnostic.aspx

[11] http://www.mydnstools.info/smtprelay/

[12] http://deadfake.com/Send.aspx

[13] http://whatismyipaddress.com/ip

[14] D. Srinivasan, "*SYSTEM SECURITY AND ETHICAL HACKING" IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013, ISSN: 2320 – 8791*

[15] Kriyon Digital Securities "ethical hacking & information security" course material

[16] http://www.microsoft.com/security.

[17] Check out Hacking Exposed Windows, Third Edition, McGraw-Hill Professional, 2007

[18] http://www.cracked.com/article_19412_8-things-you-wont-believe-can-be-hacked.html

[19] Federal Computer Week, Cyber Storm II Stirring; Feb. 29, 2008;