

Ethical Hacking

Susidharthaka Satapathy , Dr.Rasmi Ranjan Patra

CSA, CPGS, OUAT, Bhubaneswar, Odisha, India

Abstract- In today's world where the information communication technique has brought the world together there is one of the increase growing areas is security of network ,which certainly generate discussion of ETHICAL HACKING . The main reason behind the discussion of ethical hacking is insecurity of the network i.e. hacking. The need of ethical hacking is to protect the system from the damage caused by the hackers. The main reason behind the study of ethical hacking is to evaluate target system security & report back to owner. This paper helps to generate a brief idea of ethical hacking & all its aspects.

Index Terms- Hacker, security, firewall, automated, hacked, crackers

I. INTRODUCTION

The increasingly growth of internet has given an entrance passage to many things : e-commerce , email , social networking , online shopping & information distribution. As the technology advances it has its dark side; hackers. Govt. organization , private citizen & many companies of the world wants to be the part of this revolution. Being afraid of hackers as they could break into the web-server & create nuisance. To counter attack them ethical hacker's are used in the Govt. organization, companies etc. This paper describes the skills, attitude & how they helps the customer with the increasingly growth rate of internet network security has been a measure concern of Govt.& private organization. As different organization wants to take advantage of the internet but fail to do so, because of the possibility of being hacked. To minimize the risk of being hacked by the hackers the organizations realized the best possible ways to introduced the independent computer security professionals to make their way out. In computer security the ethical hackers employ's some tools & techniques that would neither damaged the system nor still information from it. Instead they would evaluate ways to secure then system & report back the owner with the threat they had found & how to cure them.

II. HACKING

It is a technique of modifying the features of system . The person who is continuously engaged in hacking activities and has accepted hacking as their choice are called hackers.

III. ETHICAL HACKING

Ethical hacking is the process which is focuses on securing & protecting computer system . Independent computer security professional breaks into the computer system and neither

damaged the target system nor steal the information, they evaluate target system security and report back to the owner about the threats found.

IV. FATHER OF HACKING

In 1971, John Draper , aka captain crunch, was one of the best known early phone hacker & one of the few who can be called one of the father's of hacking.

V. IS HACKING NECESSARY

Hacking is not what we think , It is an art of exploring the threats in a system . Today it sounds something with negative shade , but it is not exactly that many professionals hack system so as to learn the deficiencies in them and to overcome from it and try to improve the system security. Hacking is not about breaking security of computer and network. Programmers, who know different computer languages very well, they themselves define as hackers, who are good at programming. Hacking in simple words: breaking into private party in silence and enjoy it. Which logically means trying to get into some ones private account or to steal the sensitive data and do things that are illegal? Ethical hackers are the people who can create a firewall according to your knowledge and needs and protect all weak spots to protect private data from being hacked. The word hacking is not illegal, computer programmers called themselves hackers because they can break into the system and solves the problem.

VI. ROLE OF HACKERS

Historically hackers plays a number of roles some of them are good and some of them are bad. On the one hand hackers are the programmer's to break into the system and find the problem causing the system and solve them which result in improved security. On the other hand hackers are the programmer's who break into the system and cause in security. Hacking is very important practice in the modern day society because hacker's are the experts in how the system functions and how the system can fail.

VII. FEATURES OF ETHICAL HACKING

----- E.H. has some distinct features which when compared to security and problem scanning.

-----It is highly or completely automated.

----- E.H. typically exploits the security in order to access the data or access another system.

- It provides security to the system and network.
- It helps to exposes the true risk causing to the system or network.

VIII. ETHICAL HACKING PROCESS

Ethical hacking needs advance planning strategic and tactical issues in the ethical hacking process should be determined , planning is important for testing.

For example: - from a simple password cracking to all out penetration test on a web application. Approval of plan for ethical hacking is essential for the process of hacking.

Sponsorship of the project is the most important step for ethical hacking process because one needs someone to protect the plan , otherwise testing can be unexpectedly called off.

A well define plan includes the following information:-

- System to be tested
- Risks that are involved
- When the tests are performed and your overall timeline
- how the tests are performed
- how much knowledge of the systems you have before you start testing
- what is done when a major threat is discovered.

IX. EVENT&TIMELINE

1878 Teenage boys mischievously misdirect and disconnect telephone calls at Bell Telephone Company

1960 The term "hacker" is used by MIT train enthusiasts who hacked their train sets to change how they work. Later, these same enthusiasts emerge as the first computer hackers

1968 Dennis Ritchie and Keith Thompson develop the UNIX operating system, possibly the most elegant hack of all time 1969 The Advanced Research Projects Agency (ARPA) launches the first four nodes of ARPANET (the system that eventually morphs into the Internet) at UCLA, Santa Barbara, University of Utah, and Stanford

1970 Phreakers, another type of hacker, exploits the newly all-electronic telephone network to make free long distance calls 1971 Ray Tomlinson writes the first email program and uses it on ARPANET (now at 64 nodes)

1975 Bill Gates and Paul Allen form Microsoft

1976 Stephen Wozniak, Steve Jobs, and Ron Wayne form Apple Computer

1978 Randy Seuss and Ward Christiansen create first personal computer bulletin board system, still in operation today

1980 Usenet is created by networking UNIX machines via telephone

1981 Ian Murphy is the first hacker tried and convicted as a felon

1983 ARPANET splits into military and civilian sectors; the civilian sector later evolves into the present-day Internet The film *War Games* popularizes hacking Richard Stallman makes the first GNU announcement via Usenet

1984 William Gibson coins the term "cyberspace" in his novel *Necromancer*, the first hacking-related novel The most famous hacker group, Legion of Doom, is formed Steven Levy

publishes *Hackers: Heroes of the Computer Revolution*, which summarizes the hacker credo of "freedom of technology"

ARPANET 1969 Phreaker John Draper in 1970s The film *War Games* released in 1983 Gibson's *Necromancer* published 1984 .

1986 The US Congress passes the Computer Fraud and Abuse Act, the

first hacking-related legislation A small accounting error alerts astronomer and computer manager Cliff Stoll to the presence of hackers using his computer system; a year-long investigation results in the arrests of five German hackers, and Stoll later recounts the events in his book, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*

1988 Robert T. Morris, Jr. launches the first self-replicating worm on the government's ARPANET to test its effect on UNIX systems; he is the first person to be convicted under the Computer Fraud Act of 1986 Stoll publishes his account of tracking a hacker across multiple computer systems and countries 1989 Herbert Zinn is the first juvenile convicted under the Computer Fraud Act 1990 The Electronic Frontier Foundation is formed, in part to defend the rights of those investigated for hacking The United States Secret Service and the Arizona Organized Crime and Racketeering Bureau implement Operation Sun Devil, a twelve city multi-state crackdown and the largest hacker raid to date Electronic Frontier Foundation founded 1990 1991 The federal ban barring business from the Internet is lifted Justin Petersen, arrested three months earlier for hacking, is released from prison to help the FBI track hacker Kevin Mitnick Linus Torvalds publicly releases Linux version 0.01

1992 Mark Abene (aka "Phiber Optik") and other members of the Masters of Deception, a gang of phreakers, are arrested from evidence obtained from wiretaps. Mark Abene of Masters of Deception arrested 1992

1995 Kevin Mitnick, probably the world's most prolific and best known hacker, is arrested and charged with obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers, and educational institutions; and stealing, copying, and misappropriating proprietary computer software from Motorola, Fujitsu, Nokia, Sun, Novell, and NEC. Mitnick was also in possession of 20,000 credit card numbers. Christopher Pile is the first person jailed for writing and distributing a computer virus. Mitnick's Wanted Poster

1997 AOHell, a freeware application that allows script kiddies to wreak havoc on AOL, is released 1998 Two hackers, Hao Jinglong and Hao Jingwen (twin brothers) are sentenced to death by a court in China for stealing ~\$87,000 from a bank in China; Hau Jingwen's sentence was upheld, while Hao Jinglong was acquitted in return for further testimony 1999 Napster begins to gain popularity; created by Shawn Fanning and Sean Parker (ages 19 and 20 at the time), Napster attracts 65 million registered users before being shut down in July of 2001.

[How To Completely Clean Your Hacked Word Press Installation](#)

Getting hacked sucks, plain and simple. It can affect your rankings, cause your readership to be exposed to virus and Trojan attacks, make you an unwilling promoter to subject material you may not actually endorse, and in many cases cause

the loss of valuable content. However, once it happens it is usually best to not procrastinate on the cleanup process, since a speedy restore will most times minimize the damage that was caused.

While almost all sources will recommend that you upgrade your Word Press to the latest version, what the majority neglect to tell you is that in most cases simply doing so will *not* prevent the attackers from getting back in, even if there are no known exploits with the latest version. The hackers may have left a back door file hidden in a directory where it wouldn't get overwritten with an upgrade, or inserted code into your theme, or simply created an account that they then granted admin privileges to. Any one of those would allow them back in, even after you patched what was wrong the first time. Therefore I am providing this step by step process on how to completely clean out and restore a Word Press installation that has been hacked.

a. Backup the site and the database.

Even a hacked copy of your blog still probably contains valuable information and files. You don't want to lose this data if something goes wrong with the cleanup process. Worst case scenario you can just restore things back to their hacked state and start over.

b. Make a copy of any uploaded files, such as images, that are referenced.

Images are generally exempt from posing a security risk, and ones that you uploaded yourself (as opposed to ones included with a theme, for instance) will be harder to track down and replace after things are fixed again. Therefore it is usually a good idea to grab a copy of all the images in your upload folder so as to avoid broken images in posts later. If you have any non-image files that could potentially have been compromised, such as zip files, plug-in, or php scripts that you were offering people, then it is a good idea to grab fresh copies of those from the original source.

c. Download a fresh version of WP, all of the plug-in you need, and a clean template.

Using the Word Press automatic upgrade plug-in does make it easier to upgrade every time a new version comes out. However, it only replaces Word Press specific files, and does not delete obsolete ones. It also leaves your current themes and plug-in in place, as is. This means that if used to upgrade a blog that has already been compromised, it can very well leave the attackers a way back in. It is best to start over from scratch as far as the files portion of your installation goes. Note that if you use the [Easy WP Word Press Installer](#) script that I wrote it saves you from having to download, unzip, and then upload all of the core Word Press files, although you will still need to grab fresh copies of the themes and plug-in that you want to use.

d. Delete all of the files and folders in the WP directory, either through FTP (slower) or through panel's File Manager (faster).

Now that you have fresh copies of all the files you need, and copied all of your uploaded images, completely delete the entire directory structure your blog is in. This is the only sure-fire way to completely remove all possibly infected files. You can do this through FTP, but due to the way that FTP handles folder deletion (ie. it walks the directory structure, stores each and every file name that needs to be deleted, and then sends a delete command for each one), this can be slow and in some instances cause you

to get disconnected due to flooding the server with FTP commands. If available it is much faster to do this through either panel's File Manager or via command line if you happen to have shell access.

e. Re-upload the new fresh copies you just grabbed.

This step should be self explanatory, but I would like to mention that if your FTP client supports it (I use [FileZilla](#), which does) and your host allows it, then increasing the number of simultaneous connections you use to upload can greatly reduce your overall transfer time, especially on servers or ISP's where latency is more of an issue than bandwidth.

f. Run the database upgrade (point your browser at /wp-admin/upgrade.php).

This will make any necessary changes to your database structure to support the newest version of Word Press.

g. Immediately change your admin password.

If you have more than one admin (meaning any user with editing capabilities), and cannot get the others to change their passwords right then, I would change their user levels until they can change their passwords as well. If there is anyone in your user list that has editing capabilities, and you do not recognize them, it's probably best to just delete them altogether. If changing passwords is something you hate doing, then maybe my new [memorable password generator](#) can make that a little less stressful for you.

h. Go through the posts and repair any damage in the posts themselves.

Delete any links or frames that were inserted, and restore any lost content. Google and Yahoo's caches are often a good source of what used to be there if anything got overwritten. The following query run against the database can help you isolate which posts you want to look at:

```
SELECT * FROM wp_posts WHERE post content LIKE '%<iframe%'
UNION
SELECT * FROM wp_posts WHERE post content LIKE '%<no
script%'
UNION
SELECT * FROM wp_posts WHERE post content LIKE '%display:%'
```

If you did not change the default prefix for Word Press tables, then you can copy and paste that directly into a query window and run it, and it should pull up any posts that have been modified to hide content using any of the methods I have come across so far (iframes, no script tags, and display: none style attributes). To get to a query window in cPanel, you would click on the MySQL® Databases icon, scroll to the bottom of the page, and then click on php MyAdmin. Once the new window or tab opens, you would click on the database in the left hand side that your blog was in, and then in the right side at the top click on the SQL tab. Then just paste the query into the large text area and hit the Go button.

Note, however, that there may be other types of injected content that I haven't seen yet, and that a manual inspection looking for the types of patterns that first alerted you to the fact that your blog was hacked is always a good idea.

X. CRIMINALIZATION

Legislators and law enforcement began to get serious about criminalizing and prosecuting these activities in the mid-1980s. Congress passed its first hacking-related legislation, the Federal Computer Fraud and Abuse Act, in 1986. The act made computer tampering a felony crime punishable by significant jail time and monetary fines. By the mid-1990s several high-profile arrests had taken place and signalled the seriousness with which government and businesses were dealing with these activities. Kevin Mitnick, perhaps the best known hacker of this era, was arrested twice, served significant jail time, and was barred from touching a computer for several years after completing his sentence.

XI. HACKER GOOD, CRACKER BAD

Although the term “hacker” is in widespread use, the sense in which it is employed is generally incorrect. Popular media and entertainment providers have long used it to describe anyone who tampers with a system, particularly in connection to criminal activity. 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: “crackers.” Crackers are vandals and thieves whose sole purpose is unauthorized “cracking” into secure systems for personal gain.⁵ This darker side of hacking has three main motivations with varying degrees of harm. The most benign cracks are attempts to gain unauthorized access in order to satisfy a personal motive such as curiosity or pride. More malicious cracking seeks to gain unauthorized access in order to tamper with or destroy information. The goal of the most serious and professional crackers is unauthorized access to systems or computer services in order to steal data for criminal purposes. Systems commonly under attack are universities, government agencies, such as the Department of Defence and NASA, and large corporations such as electric utilities and airlines. Many crackers are professional criminals involved in corporate or government espionage and have links to organized crime. A relative newcomer to the “hacker” field, script kiddies are another break-off group mistakenly called hackers by the media. A lower form of crackers, script kiddies are not particularly knowledgeable about computer and networking details. Instead, they download ready-made tools to seek out weaknesses on systems accessible via the Internet. They do not target specific information or a specific

company but rather scan for opportunities to disrupt and vandalize systems. Most “hackers” and “hacking” events reported on by the popular press are actually of this type.

REFERENCES

- [1] <<http://tlc.discovery.com/convergence/hackers/articles/history.html>>. Stallman, Richard.
- [2] “The GNU Manifesto.” The New Media Reader. Eds. Noah Wardrip-Fruin and Nick Mön fort. Cambridge: MIT Press, 2003. Sterling, Bruce.
- [3] Encyclopaedia Britannica. 2003. Encyclopaedia Britannica Premium Service. 28 Oct, 2003 <<http://www.britannica.com/eb/article?eu=102011>>.
- [4] Cyber Terrorism. Online. Discovery Communications. 28Oct.2003.<<http://tlc.discovery.com/convergence/hackers/articles/cyberterror.html>> Quittner, Jeremy.
- [5] Hacker Psych 101. Online. Discovery Communications. 28Oct.2003.<<http://tlc.discovery.com/convergence/hackers/articles/psych.html>>.
- [6] Hackers: Methods of Attack and Defense. Online. Discovery Communications.28Oct.2003 <<http://tlc.discovery.com/convergence/hackers/articles/method.html>>.

AUTHORS

First Author – Susidharthaka Satapathy persuing Master in Computer Application from O.U.A.T, Odisha, India in 2012-2015.He is working in the area of Ethical Hacking for last 6 months., Email: satathysusidharthaka@gmail.com



Second Author – Dr.Rasmi Ranjan Patra received Master In Computer Application With 1st Class With distinction from O.U.A.T, Odisha, India in 2001, M.Tech in Computer Science and Technology from C.E.T Bhubaneswar ,India in 2010 and PhD Degree in 2013 from Utkal University, India .He is working as Assistant professor in Department of Computer Science and Application under Orissa University of Agriculture and Technology(O.U.A.T).He has Published many papers at national /international Journals and Conferences in the areas of Sensor Network, Soft Computing, Cloud computing and Big data. Mr. Patra has authorized one book in Computer Science area., Email: hellorasmi@gmail.com

