International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

Ethical Hacking Tools: A Situational Awareness

M.Rajendra Prasad[#1], Dr.B.Manjula[*2]
[#1]*Department of Computer Science, Alluri Institute of Management Sciences, Warangal, Telangana State.*
[#1]mrpaims@yahoo.com
[*2]*Department of Computer Science, Kakatiya University, Warangal, Telangana State.*
[*2]manjulabairam@gmail.com

***Abstract*— Today World Wide Web (WWW) is a promising reusable resource of web data for all kinds of domain. The web users, academicians, researchers, and developers are searching, gathering, and executing millions of web queries retrieving (downloading) and fetching (uploading) from the web. This is the universal leading information hub and it has excellent progress since its beginning. With the growth of Internet, computer's web security has become a major concern for public (governments) and private (businesses) sectors. Victims of hacking are increasing at fast rate due to quick identity and accessibility of unsecured systems by hackers. Hacking becomes a critical and sensitive issue for both enterprises. Ethical Hacking may become a challenge, pragmatically ethical as a self-conscious, code of conduct and acceptable tool for security concern. In the usage and supervision of web, if ethics are bypassed the control system goes into wrong hands of criminal hackers, straight away they will execute vulnerable operations it will cause massive logical and physical damage. This paper will explore the various aspects of hacking, definition, what ethical hackers can perform and ethical hacking methodology, terminology as well as identifying types of ethical hacking tools.**

Keywords-Internet, Hacking, Vulnerabilities, Security, Tools.

I. INTRODUCTION

The explosive growth and evolution of the Internet has brought many innovative utilities and programs such as electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and further new avenues for advertising and information distribution etc., are a few of them. There is also a dark side of web and web technological advancements in form of "Criminal Hackers" that are posing a threat to websites and web related services as well as corporate activities. The number of these hackers are increasing while the resources available to law-enforcement agencies are also increasing, but at a much slower rate. So, the hackers are clearly winning the battle with law-enforcement agencies, which are must content themselves with investigating and prosecuting the most spectacular cases.

There are various loopholes in legal system against the cyber crime. Due to which, the private firms have begun to take matters into their own hands, responding to hacker attacks with a variety of some active defense measures that are aggressive in the sense that they are intended to inflict the same kind of harm on the attacker's machine or network as the attack is intended to have on the victim's machine or network but sometimes they may cause harm to innocent people having lack of knowledge about their act or behavior. Now, it is generally accepted that it is the duty of state not the aggrieved individual, to respond an offender for the purposes of punishing for their wrong doing things and the aggressive active defense is characterized as wrongful event. Also the corporate as well as government enterprises are hiring hackers of their own for the purpose of identifying the loopholes within their network and these hackers are termed as "Ethical Hackers".

Darlington believes hacking is not limited to accessing data or information but also includes an attack on the privacy of all people. Almost all different opinions agree on the illegality of hacking. On the other hand the term hacker is the agent of hack or hacking and it was defined as a person who enjoys accessing files whether for fun, imposing power or the interest related to the accessed files or data according to Taylor. While Marotta has a negative view of the hacker as a data lord, a barbarian who takes what he wants. Himanen defines hacker as any person who performs illegal actions whether they were related to computer or not which means the usage of a device apart from its functionality.

Hacking

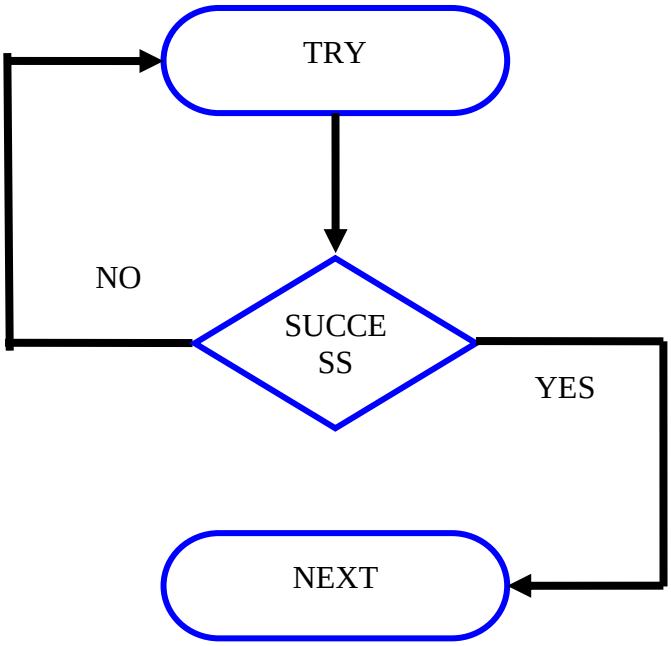

Figure.1 Flowchart of Hacking

"Hacking" is a buzzword that suspect and think every professional whenever it is pronounced or heard by someone. Everyone born in this professional world with attitude wants to be a Hacker. A hacker needs a brilliant mind to hack anything. His or her skill set should be so powerful that no other hacker can hack himself or herself.

Types of Hacking

White Hat Hacker- Also referred as Ethical Hacker and mainly focuses on securing corporate network from outsider threats. They are with good intention that fights against Black Hat Hacker. Sometimes called as Sneakers.

Grey Hat Hacker- These people are skilled professionals who sometimes act as legally and sometime not. In simple word we may call a Grey Hat hacker as Hybrid between White Hat and Black Hat Hacker.

Black Hat Hacker- Also referred as Cracker and intention is to break into others Network, and wish to secure his own machine. They often use different techniques for breaking into systems which can involve advanced programming skills and social engineering.

Hacking Methods

Phising Method- Phising is the method that you are familiar with. You can create a fake account and e-mail ID in any mailing service account and fool your friends by telling them to send the victim's ID, their own ID and their own password in your fake that particular account.

Brute Force Hack- This kind of hacking which takes much time to get password of the victims and target users.

Fake Login Hack- Hacking used by most of attacker for their goal by creating a fake login page and sharing the information to target users and login there the password would come to attacker.

Cookie Steal Hack- This is somewhat similar to fake login hacking as attacker intention to prepare a cookie stealer and pass to target victims to open attacker cookie so that the login credentials would come to attacker.

Web Mail Hack- This is the toughest method to learn for hacking as it also needs a hacker to learn about scripting skills, systems tricks and much more and there is also a software for this type of hacking.

II. HACKING TECHNOLOGIES

In the world wide web particularly middleware, web and open source technologies many methods and tools exist for locating vulnerabilities, running exploits, and compromising systems. Once vulnerabilities are found in a system, a hacker can exploit that particular vulnerability and install malicious software. Trojans, backdoors, and root kits are all forms of malicious software, or malware. When a malware is installed on a hacked system after vulnerability has been exploited accordingly. Most hacking tools exploit weaknesses in one of the following four major areas:

Operating Systems- Different platforms many system administrators install operating systems with the default settings only, it will cause the potential vulnerabilities that remain unpatched.

Applications- When designing and developing applications usually not thoroughly tested for vulnerabilities when developers are writing the source code or snippets, which can leave many bugs and flaws that a hacker can exploit. Most application development is “feature-driven” and under a deadline to turn out the most robust application in the shortest amount of time.

Shrink-Wrap Code-These kinds of programs are extra features and a common user is not aware of these functionalities can be used to exploit the system. For example, macros in Microsoft Office Word, can allow a hacker to execute programs from within the application.

Misconfigurations-The target System or network can also be misconfigured or left at the lowest or poor security settings to increase ease of use for the user; this may cause in vulnerability and an attack.

Ehical Hacking

Ethical hackers always acting as a professional to differentiate themselves from malicious hackers. Gaining the trust of clients or stakeholders, taking all precautions to do no harm to their systems and critical to being a professional. Another key step of ethical hacking is to always gain permission from the data owner prior to accessing the target system. This is one of the ways ethical hackers can overcome stereotype of hackers and gain trust of clients or stakeholders.

III. TYPES OF ETHICAL HACKING

Ethical hackers are usually security professionals or network penetration testers who use their strong hacking skill sets and tools for defensive and protective purpose. The term cracker describes a hacker who uses their hacking skill sets and tools for destructive or offensive purposes such as disseminating viruses or performing denial-of service (DoS) attacks to compromise or bring down systems and networks. No longer just looking for fun and enjoy, these hackers are sometimes paid to damage corporate reputations or steal or reveal credit card sensitive information, while slowing business processes and compromising the integrity of the stakeholders and organization. Here are the most common entry points for attackers:

Remote Network: Hacking attempts to simulate an intruder launching an attack over the Internet. The ethical hacker tries to break or find vulnerability in the outside defenses of the network, such as firewall, proxy, or router vulnerabilities. The Internet is thought to be the most common hacking medium of vehicle, while in reality most organizations have strengthened their security defenses sufficient to prevent hacking from the public network.

Remote Dial-Up Network: This kind of hack tries to simulate an intruder launching an attack against the client's modem pools. War dialing is the process of repetitive dialing to find an open system.

Local Area Network: It hacks and simulates someone with physical access gaining additional unauthorized access using the local network. The ethical hacker must gain direct access to the local network in order to launch this type of attack. Wireless LANs (WLANs) fall in this category and have added an entirely new avenue of attack. Because the WLAN signals or Wi-Fi signals can be identified and captured outside attackers, hackers no longer have to gain physical access to the building and network to perform an attack on the LAN. The huge growth of WLANs has made this an increasing source of attack and potential risk to many organizations.

Stolen Equipment or Device: A stolen-equipment hack simulates theft of a critical information resource such as a laptop owned by an employee.Information such as usernames, passwords, security settings, and encryption types can be gained by stealing a laptop. This is usually a commonly overlooked area by many organizations. Once a hacker has access to a laptop authorized in the security domain, a lot of information, such as security configuration, can be gathered. Many times laptops disappear and are not reported quickly enough to allow the security administrator to lock that device out of the network.

Social Engineering: In this attack checks the security and integrity of the organization's employees by using the mobile or face-to-face communication to gather information for use in an attack. Social-engineering attacks can be used to acquire usernames, passwords, or other organizational security measures. Social-engineering scenarios usually consist of a hacker calling the help desk and talking the help desk employee into giving out confidential security information.

Physical Entry: A physical-entry attack attempts to compromise the organization's physical premises. An ethical hacker who gains physical access can fix viruses, Trojans, rootkits, or hardware or software key loggers directly on systems in the target network. Additionally, confidential documents that are not stored in a secure location can be gathered by the hacker.

IV. PROCESS OF ETHICAL HACKING

The Ethical hacking process needs to be planned in advance. All technical, management and strategical issues must be considered. Planning is most important for any amount of testing – from a simple password test to all out penetration test on a web application. Backup off data must be ensured, otherwise the testing may be called off unexpectedly if someone claims they never approve for the tests. So, a well defined scope involves the following significant information:

1. Specific system to be identified and tested.
2. What risks identified and involved.
3. Preparing the schedule to carry test and on timeline.
4. Get and explore knowledge of system before testing.
5. What happened vulnerability is discovered?

6.Specifying the deliverables - It includes security assessment reports and a higher level report outlining the general and identified vulnerabilities to be addressed, along with counter measures and comments that should be implemented when selecting systems to test, start with the most critical or vulnerable system. The overall hacking methodology consists of certain phases which are as fallows:

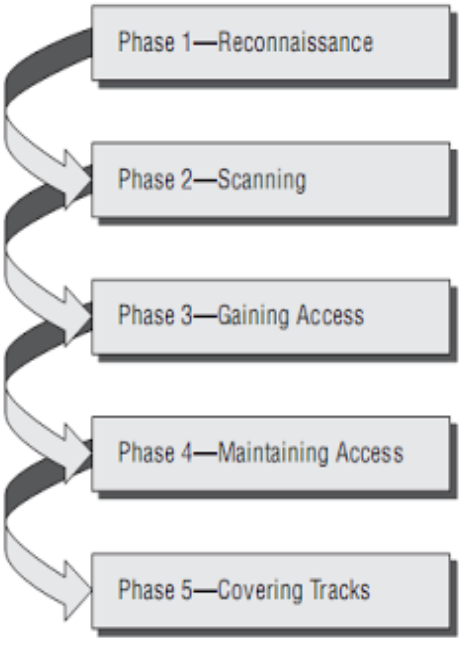

Figure.2 Phases of Hacking

Phase 1- Reconnaissance

To be able to attack a system systematically, a hacker has to know as much as possible about the target. It is important to get an overview of the network and the used systems. Information as DNS servers, administrator contacts and IP ranges can be collected. During the reconnaissance phase different kind of tools can be used – network mapping, network and vulnerability scanning tools are the commonly used. Cheops-ng for example is a very good network mapping tool which is able to generate networking graphs. They can be of huge help later on during the attack phase or to get an overview about the network. A network mapping tool is very helpful when doing an internal ethical hack. At the end of the reconnaissance phase, an attacker should have a bunch of information about the target. With all these pieces of information, a promising attack path can be constructed.

Phase 2- Scanning

In this phase the scanning involves taking information discovered during reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase it include:

Dialers
Port scanners
ICMP scanners
Ping sweeps
Network mappers
SNMP sweepers
Vulnerability scanners

Hackers are seeking any information that can help them commit an attack on a target system or network, such as the following:

Computer names
Operating system (OS)
Installed software
IP addresses
User accounts

Phase 3- Gaining Access

Practically hacking take place vulnerabilities exposed during the reconnaissance and scanning phase are now exploited to gain access to target system or network. The hacking attack can be delivered to the target system via a local area network (LAN), either wired or wireless; local access to a PC; the Internet; or off-line. Examples include stack based buffer overflows, denial of service (DoS), and session hijacking. Gaining access is known in the hacker world as owning the system because once a system has been hacked, the hacker has control and can use that system or network as they wish.

Phase 4- Maintaining Access

Once a hacker has gained access to a target system, they want to keep that access for future exploitation and attacks. Sometimes, hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, root kits, and trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system.

Phase 5- Covering Tracks

Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal actions. Hackers try to remove all traces of the attacks, such as log files or intrusion detection system (IDS) alarms. Examples of activities during this phase of the attacks include:

Steganography
Using a tunneling protocol
Altering log files

V. ETHICAL HACKING TERMINOLOGY

To understand ethical hacking terminology is an important part of CEH (Certified Ethical Hacker) responsibility. This terminology is how security professionals acting as ethical hackers and communicated as a code of conduct. Some of the significant terms as follows:

Threat: An environment or situation that could lead to a potential violation of security. Ethical hackers look for and prioritize threats when performing a security analysis. Malicious hackers and their use of software and hacking techniques are themselves threats to an organization's information security.

Exploit: A piece of software or technology that take advantage of a bug, fault, or vulnerability, leading to unauthorized access, privilege escalation, or denial of service (DoS) on a computer system. Malicious hackers are looking for exploits in computer systems to open the door to an initial attack. Most exploits are small strings of sample code or snippets that, when executed on a system, expose vulnerability.

Vulnerability: The existence of a software flaw, logic design, or implementation error that can lead to an unexpected and undesirable event executing bad or damaging instructions to the system. Exploit code is written to target vulnerability and cause a fault in the system in order to retrieve valuable data.

Target of Evaluation (ToE): A system, program, or network that is the subject of a security analysis or attack. Ethical hackers are usually concerned with high-value ToEs, systems that contain sensitive information such as account numbers, e-mail credentials, social security numbers, or other sensitive data.

Attack: An attack occurs when a system is compromised based on vulnerability. Many attacks are perpetuated via an exploit. Ethical hackers use tools to find systems that may be vulnerable to an exploit because of the operating system, network configuration, or applications installed on the systems, and to prevent an attack.

Remote Exploit: The exploit is sent over a network and exploits security vulnerabilities without any prior access to the vulnerable system. Hacking attacks against corporate or

academic systems or networks initiated from the outside world are considered remote.

Local Exploit: The exploit is delivered directly to the target system or network, which requires prior access to the vulnerable system to increase privileges. Information security policies should be created in such a way that only those who need access to information should be allowed to access and they should have the lowest level of access. These concepts are commonly referred as "need to know" and "least privilege". Most hacking attempts occur from within an organization and are perpetuated by employees, academicians, or others in a trusted position.

VI. ETHICAL HACKING TOOLS

It is very much essential to make sure right and strong tool for ethical hacking process. It is important to know the professional or personal as well as technical limitations. Many tools focus on specific tests, but no one tool can test for everything. The more tools are avilable in web, the easier to do ethical hacking successfully. Make sure that choose the right tool for right task.There are various characteristics and functionalities for the use of tools for ethical hacking which are as follows:

1. Adequate documentation or help.
2. Reports on vulnerabilities, how it can be fixed.
3. Updates and technical support is neccesary.
4. Reports that can be presented to authorities.

These features can save the time and effort when composing or writing the report. Time and patience are important factors in ethical hacking process. The team or individual should be careful when performing ethical hacking tests. It is not practical to make sure that no hackers are on our own system or network. Just make sure to keep everything private and independent.The list and description of various tools used in ethical hacking process are as follows:

Scanning Tools

The Scanning tools are more helpful in ethical hacking process. In technical defination, a scanner sends a message requesting to open a connection with a system on a particular port.It has an option of ignoring the message,responding negatively to the message, or opening a session. Ignoring the message is the safest since if there are no open services it may be hard for a cracker to determine if a system exists. Once a port scan reveals the existence of an open service, a cracker can attack known vulnerabilities. Once a cracker scans all systems on a network and creates a network map showing what systems are active or alive, what operating systems and what are the services are available, almost any kind of attacks are possible including automated scripting program attacks and social engineered attacks.Crackers look for unauthorized services such as someone running a server with known problems, an unauthorized server on a high port. Port scanning can be done manually from a single computer to learn about target systems or it can be done automatically by program originating from multiple computers on different networks to a single target system over a long period of time. Port scanners like other tools, have both offensive and defensive applications what makes a port scanner good or evil is how it is used. Actually, a port scanner is simultaneously both the most powerful tool an ethical hacker can use in protecting the network of computers and the most powerful tool a cracker can use to generate attacks. The below table shows some of scanning tools that help in ethical hacking process:

Purpose	Tool
Network scanners	SATAN, strobe, rprobe
Firewall scanners	Firewalk
Password crackers	John Ripper, L0pth crack
Sniffers	Ethercap, tcpdump
War- dialing	TheScan, LoginH
Security and vulnerability	Nessus, ISS, Cyber cop

Table.1 Scanning Tools of Ethical Hacking

Password Cracking Tools

Password cracking does not have to involve fancy tools, but it is a tedious process from the begining. If the target doesn't lockout and identify after a specific number of tries, attacker can spend an infinite amount of time trying every combination of alphanumeric characters. It is just a question of time and bandwidth before attacker break into a system or network. There are three basic types of password cracking tests that can be automated with the following:

Dictionary: A file of words is run against user accounts, and if the password is a simple word, it can be found quickly.

Hybrid: A common method utilized by users to change passwords is to add a number or symbol to end.A hybrid attack works like a dictionary attack, but adds simple numbers or symbols to the password attempts.

Brute Force: The most time consuming, but comprehensive way to crack a password. Every combination of characters are tried until the password is broken.

Port Scanning Tools

Port scanning is one of the most common reconnaissance techniques used by testers to discover vulnerabilities in services listening at well-known ports. Once attacker identified the IP address of a target system through foot printing, process begin the port scanning and looking for holes in system through which attacker or a malicious intruder can gain control and access. A typical system has 2^16 -1 port numbers, each with its own TCP and UDP ports that can be used to gain access if un-protected. The most popular port scanner for Nmap is also available for Windows. Nmap can scan a system in variety of stealth modes, depending upon how un-detectable. Nmap can determine a lot of information about a target system, like what hosts are available, what services are offered and what operating system is running.

Vulnerability Scanning Tools

A Vulnerability scanner allows attacker to connect to a target system and check for such vulnerabilities as configuration errors. A popular vulnerability scanner is freely available open source tool called Nessus. Nessus is an extremely powerful scanner that can be configured to run a variety of scans. While a windows graphical front-end is available, the core Nessus product requires Linux to run. Microsoft's Baseline Security Analyser is a free Windows vulnerability scanner. MBSA can be used to detect security configuration errors on local systems or remotely across a network. Popular commercial vulnerability scanners include Retina Network Security Scanner, which runs on Windows, and SAINT, which runs on various UNIX or Linux flavors and versions.

VII. CONCLUSION

This paper explores and addressed the hacking, ethical hacking and tools from several perspectives. The present poor security on the Internet, ethical hacking may be most effective way to plug security holes and prevent intrusions. On the other hand ethical hacking tools have also notorious tools for crackers. The main tactical objective is to stay one step ahead of the crackers. Ethical hacking is a tool, which is properly utilized, can prove useful for understanding the weaknesses of a network and how they might be exploited. After all, ethical hacking will play a certain role in the security assessment offering and certainly earned its place among other security assessments. In this conclusion section, Ethical hacker is an educator and having strong skill sets who seeks to enlighten not only the stakeholders, but also the Information Technology security industry. This paper is educational purpose only and security concern try to secure your personal computer or laptop when you are in the on-line from attackers and hackers. Ethical hacking is not a crime depends upon users thinking view and users mind set will be change. In current 3G, 4G generations every process along with systems we need to know whether sensitive and critical data is secure or not this is purely self-conscious and a situational awareness.

VIII. REFERENCES

[1] B. Kevin, “Hacking for Dummies”, 2nd edition, 408 pages, Oct 2006

[2] D. Manthan “Hacking for Beginners”, 254 pages, 2010.

[3] M.Rajendra Prasad, B.Manjula, V.Bapuji,“A Novel Overview and Evolution of World Wide Web: Comparison from Web 1.0 to Web 3.0”, International Journal of Computer Science and Technology (IJCST) Vol.4,Issue 1, Jan-Mar 2013, pp. 349~354, ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print); http://ijcst.com

[4] H.M David, “Three Different Shades of Ethical Hacking: Black, White and Gray,” in GSEC Practical Assignment, Version 1.4b, Feb,2004.

[5] my.safaribooksonline.com/.../introduction-to-ethical-hacking-ethics-legality.

[6] Smith B., Yurcik W., Doss D., “Ethical Hacking: The Security Justification Redux”, IEEE Transactions, pp. 375-379, 2002.

[7] Sanctum Inc, “Ethical Hacking Techniques to Audit and Secure Web Enabled Applications”, 2002.

[8] media.techtarget.com/searchNetworking- Introduction to ethical hacking-Tech Target.

[9] Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala, “Ethical Hacking”, International journal of Computer Applications (0975-8887), Vol. 1 No. 10, pp. 14-20, 2010.

[10] http://bedaone.blogspot.in/p/chapter-1-introduction-to-ethical.html

[11] B. Reto, “Ethical Hacking”, in GSEC Practical Assignment, Version 1.4b, Option 1, Nov 24, 2002

[12] J.Danish and A.N.Muhammad, "Is Ethical Hacking Ethical?", International Journal of Engineering Science&Technology,Vol.3 No. 5, pp. 3758-3763, May 2011.

[13] The Secret of Hacking by Manish Kumar, Leo Impact Security

[14] cheops-ng.sourceforge.net

[15] Certified Ethical Hacking(CEH): www.eccouncil.org