Ethical hacking

- An information security enhancement technique

Shri.V.Balasubramaniam, Instructor Telecom/IRISET

Abstract

As public and private organizations migrate more of their critical functions to the Internet, criminals have more opportunity and incentive to gain access to sensitive information through the Web application. The state of security on the internet is bad and getting worse. One reaction to this state of affairs is termed as Ethical Hacking which attempts to increase security protection by identifying and patching known security vulnerabilities on systems owned by other parties. Thus the need of protecting the systems from the nuisance of hacking generated by the hackers is to promote the persons who will punch back the illegal attacks on our computer systems. So, Ethical hacking is an assessment to test and check an information technology environment for possible weak links and vulnerabilities. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions. So, to overcome from these major issues, ethical hackers or white hat hackers came into existence. One of the fastest growing areas in network security, and certainly an area that generates much discussion. The main purpose of this study is to reveal the brief idea of the ethical hacking and its affairs with the corporate security. This paper describes what ethical hacking is, what it can do, an ethical hacking methodology as well as some tools which can be used for an ethical hack.

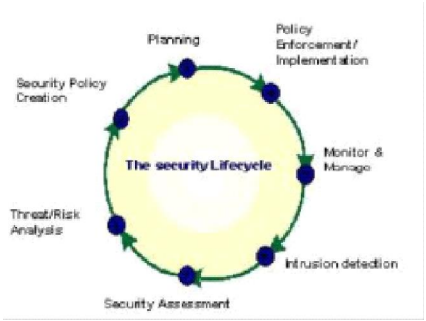
1. INTRODUCTION

The Internet is enormously growing and e-commerce is on it's own advance. The vast growth of Internet has brought many good things like electronic commerce, email, easy access to vast stores of reference material etc. More and more computers get connected to the Internet, wireless & mobile devices and networks are booming. Due to the vast usage of the Internet technology, the government, private industry and the every computer user have fears of their data or private information being comprised by a cyber criminal called hackers. There are different types of hackers like black hat hacker, white hat hackers or the ethical hackers etc. Those types of hackers are called black hat hackers who will secretly steal the organization's information and transmit it to the open internet .

So, to overcome from these major issues caused by black hat hackers, another category of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers. So, this paper describes ethical hackers, their skills and how they go about helping their customers and plug up security holes. Ethical hackers perform the hacks as security tests for their systems. This type of hacking is always legal and trustworthy. In other terms ethical hacking is the testing of resources for the betterment of technology and is focussed on securing and protecting IP systems. So, in case of computer security, the teams or ethical hackers would employ the same tricks and techniques that hacker use but in a legal manner and they would neither damage the target systems nor steal information. Instead, they would evaluate the target system's security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them.

Ethical hacking is a way of doing a security assessment. Like all other assessments an ethical hack is a random sample and passing an ethical hack doesn't mean there are no security issues. An ethical hack's results is a detailed report of the findings as well as a testimony that a hacker with a certain amount of time and skills is or isn't able to successfully attack a system or get access to certain information. Ethical hacking can be categorized as a security assessment, a kind of training, a test for the security of an information technology environment.

An ethical hack shows the risks an information technology environment is facing and actions can be taken to reduce certain risks or to accept them. We can easily say that Ethical hacking does perfectly fit into the security life cycle shown in the figure.



2. TYPES OF ATTACKS

Nontechnical attacks

Exploits that involve manipulating people ,end users and even yourself, are the greatest vulnerability within any computer or network infrastructure. Humans are trusting by nature, which can lead to social-engineering exploits. Social engineering is defined as the exploitation of the trusting nature of human beings to gain information for malicious purpose. Other common and effective attacks against information systems are physical. Hackers break into buildings, computer rooms, or other areas containing critical information or property. Physical attacks can include dumpster diving (rummaging through trash cans and dumpsters for intellectual property, passwords, network diagrams, and other information).

Network-infrastructure attacks

Hacker attacks against network infrastructures can be easy, because many networks can be reached from anywhere in the world via the Internet. Here are some examples of network-infrastructure attacks:

- Connecting into a network through a rogue modem attached to a computer behind a firewall.
- Exploiting weaknesses in network transport mechanisms, such as TCP/IP and NetBIOS.
- Flooding a network with too many requests, creating a denial of service (DoS) for legitimate requests.
- Installing a network analyzer on a network and capturing every packet that travels across it, revealing confidential information in clear text, Piggybacking onto a network through an insecure 802.11b wireless configuration.

Operating-system attacks

Hacking operating systems (OSs) is a preferred method of the bad guys. OSs comprise a large portion of hacker attacks simply because every computer has one and so many well-known exploits can be used against them. Occasionally, some operating systems• that are more secure out of the box, such as Novell NetWare and the flavors of BSD UNIX, are attacked, and vulnerabilities turn up. But hackers prefer attacking operating systems like Windows and Linux because they are widely used and better known for their vulnerabilities. Here are some examples of attacks on operating systems:

- Exploiting specific protocol implementations
- Attacking built-in authentication systems.
- Breaking file-system security.
- Cracking passwords and encryption mechanisms.

Application and other specialized attacks

Applications take a lot of hits by hackers. Programs such as e-mail server software and Web applications often are beaten down:

- **Hypertext Transfer Protocol (HTTP**) and Simple Mail Transfer Protocol (SMTP) applications are frequently attacked because most firewalls and other security mechanisms are configured to allow full access to these programs from the Internet.
- **Malicious software (malware)** includes viruses, worms, Trojan horses, and spyware. Malware clogs networks and takes down systems.
- **Spam (junk e-mail)** is wreaking havoc on system availability and storage space. And it can carry malware. Ethical hacking helps reveal such attacks against your computer systems.

3. THE INTRUDER'S MAIN MOTIVES ARE

- To perform network scanning to find out vulnerable hosts in the network.
- To install an FTP server for distributing illegal content on network (ex. pirated software or movies)
- To use the host as a spam relay to continuous flood in the network.
- To establish a web server (non-privileged port) to be used for some phishing scam.

4. TOOLS USED BY HACKERS

There are several common tools used by computer criminals to penetrate network as:

- Trojan horse- These are malicious programs or legitimate software is to be used set up a back door in a computer system so that the criminal can gain access.
- Virus- A virus is a self-replicating program that

spreads by inserting copies of itself into other executable code or documents.

- Worm - The worm is a like virus and also a self replicating program. The difference between a virus and a worm is that a worm does not attach itself to other code.
- Vulnerability scanner – This tool is used by hackers & intruders for quickly check computers on a network for known weaknesses. Hackers also use port scanners. This check to see which ports on a specified computer are "open" or available to access the computer.
- Sniffer – This is an application that captures password and other data in transit either within the computer or over the network.
- Exploit – This is an application to takes advantage of a known weakness.
- Social engineering – Through this to obtain some form of information.
- Root kit - This tool is for hiding the fact that a computer's security has been compromised.

5. TYPES OF HACKING

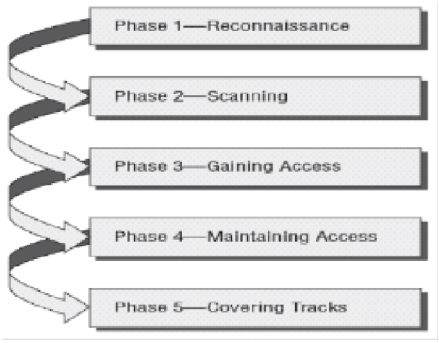
- **Inside Jobs** : Most security breaches originate inside the network that is under attack. Inside jobs include stealing passwords (which hackers then use or sell), performing industrial espionage, causing harm (as disgruntled employees), or committing simple misuse. Sound policy enforcement and observant employees who guard their passwords and PCs can thwart many of these security breaches.
- **Rogue Access Points :** Rogue access points (APs) are unsecured wireless access points that outsiders can easily breech. Rogue APs are most often connected by well-meaning but ignorant employees.
- **Back Doors Hackers** can gain access to a network by exploiting back doors administrative shortcuts, configuration errors, easily deciphered passwords, and unsecured dial-ups.
- **Denial of Service** : DOS attacks give hackers a way to bring down a network without gaining internal access. DOS attacks work by flooding the access routers with bogus traffic (which can be e-mail or Transmission Control Protocol, TCP, packets).
- **Distributed Doss :** (DDOSS) are coordinated DOS attacks from multiple sources. A DDOSS more difficult to block because it uses multiple, changing, source IP addresses.
- **Anarchists, Crackers, and Kiddies Anarchists** are people who just like to break stuff. They usually exploit any target of opportunity. Crackers are hobbyists or professionals who break passwords and develop Trojan horses or other SW (called wares). They either use the SW themselves (for bragging rights) or sell it for profit. Script kiddies are hacker wannabes. They have no real hacker skills, so they buy or download wares, which they launch.
- **Sniffing and Spoofing** Sniffing refers to the act of intercepting TCP packets. This interception can happen through simple eavesdropping or something more sinister. Spoofing is the act of sending an illegitimate packet with an expected acknowledgment (ACK), which a hacker can guess, predict, or obtain by snooping.

6. ETHICAL HACKING PROCESS

The Ethical hacking process needs to be planned in advance. All technical, management and strategical issues must be considered. Planning is 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 authorises for the tests. So, a well defined scope involves the following information:

1. Specific systems to be tested.
2. Risks that are involved.
3. Preparing schedule to carry test and overall timeline.
4. Gather and explore knowledge of the systems we have before testing.
5. What is done when a major vulnerability is discovered?
6. The specific deliverables- this includes security assessment reports and a higher level report outlining the general vulnerabilities to be addressed, along with counter measures that should be implemented when selecting systems to test, start with the most critical or vulnerable systems.

The overall hacking methodology consists of certain steps which are as follows:



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.
2. **Probe and Attack:** This is a phase 2 process as shown in the above fig. The probe and attack phase is about digging in, going closer and getting a feeling for the target. It's time to try the collected, possible vulnerabilities from the reconnaissance phase.
3. **Listening:** This is again a phase 2 process i.e. scanning which is a combination of Probe and attack and listening. Listening to network traffic or to application data can sometimes help to attack a system or to advance deeper into a corporate network. Listening is especially powerful as soon as one has control of an important communication bottleneck. Sniffers are heavily used during the listening phase.
4. **First Access:** This is a phase 3 process which is not about getting root access, it's about getting any access to a system be it a user or root account. Once this option is available it's time to go for higher access levels or new systems which are now reachable through the acquired system.
5. **Advancement:** Phase 4 i.e. Maintaining access is a combination of Advancement and Stealth process. The advancement phase is probably the most creative demanding stage, as unlimited possibilities are open. Sniffing network traffic may unveil certain passwords, needed usernames or e-mail traffic with usable information. Sending mails to administrators faking some known users may help in getting desired information or even access to a new system.
6. **Stealth:** Some systems may be of high value – systems which act as routers or firewalls, systems where a root account could be acquired. To have access to such systems at a later time it is important clean relevant log files.
7. **Takeover:** Takeover is a phase 5 process. Once root access could be attained, the system can be considered won. From there on it's possible to install any tools, do every action and start every services on that particular machine.
8. **Cleanup:** This could be instructions in the final report on how to remove certain trojans but most of the time this will be done by the hacker itself. Removing all traces as far as possible is kind of a duty for the hacking craft.

CONCLUSION

This paper addressed ethical hacking from several perspectives. Ethical hacking seems to be a new buzz word although the techniques and ideas of testing security by attacking an installation aren't new at all. But, with the present poor security on the internet, ethical hacking may be the most effective way to plug security holes and prevent intrusions. So, at present the tactical objective is to stay one step ahead of the hackers. Ethical Hacking is a tool, which if 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 offerings and certainly has earned its place among other security assessments.