Report

on

ETHICAL HACKING

Prepared by:-

BHARGAV DABHI

(090010107040)

A.D.PATEL INSTITUTE OF TECHNOLOGY

CERTIFICATE

This is to certify that Mr. / Ms. _____

Mr. / Ms._____ Is studying in

Sem – VI of B.E. Computer Engineering having Roll No. _____

has / have completed his / her / their seminar on the following topic

Successfully.

Topic Name: ETHICAL HACKING

Date : _____

INDEX

ABSTRACT

- Today more and more software are being developed and people are getting more and more options in their present software‘s. But many are not aware that they are being hacked without their knowledge. One reaction to this state of affairs is a behavior termed —Ethical Hacking" which attempts to pro-actively increase security protection by identifying and patching known security vulnerabilities on systems owned by other parties.
- A good ethical hacker should know the methodology chosen by the hacker like reconnaissance, host or target scanning, gaining access, maintaining access and clearing tracks. For ethical hacking we should know about the various tools and methods that can be used by a black hat hacker apart from the methodology used by him.
- From the point of view of the user one should know at least some of these because some hackers make use of those who are not aware of the various hacking methods to hack into a system. Also when thinking from the point of view of the developer, he also should be aware of these since he should be able to close holes in his software even with the usage of the various tools. With the advent of new tools the hackers may make new tactics. But at least the software will be resistant to some of the tools.

INTRODUCTION

Ethical hacking also known as penetration testing or white-hat hacking, involves the same tools, tricks, and techniques that hackers use, but with one major difference that Ethical hacking is legal. Ethical hacking is performed with the target‘s permission. The intent of ethical hacking is to discover vulnerabilities from a hacker‘s viewpoint so systems can be better secured. Its part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors‘ claims about the security of their products are legitimate.

A) Security:

Security is the condition of being protected against danger or loss. In the general sense, security is a concept similar to safety. In the case of networks the security is also called the information security. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

B) Need for Security:

Computer security is required because most organizations can be damaged by hostile software or intruders. There may be several forms of damage which are obviously interrelated which are produced by the intruders. These include:

- Lose of confidential data
- Damage or destruction of data
- Damage or destruction of computer system
- Loss of reputation of a company

Hacking

Eric Raymond, compiler of —The New Hacker's Dictionary, defines a hacker as a clever programmer. A "good hack is a clever solution to a programming problem and "hacking is the act of doing it. Raymond lists five possible characteristics that qualify one as a hacker, which we paraphrase here:

- A person who enjoys learning details of a programming language or system
- A person who enjoys actually doing the programming rather than just theorizing about it
- A person capable of appreciating someone else's hacking
- A person who picks up programming quickly
- A person who is an expert at a particular programming language or system.

A) Types of Hackers:

Hackers can be broadly classified on the basis of why they are hacking system or why they are indulging hacking. There are mainly three types of hacker on this basis

- Black-Hat Hacker

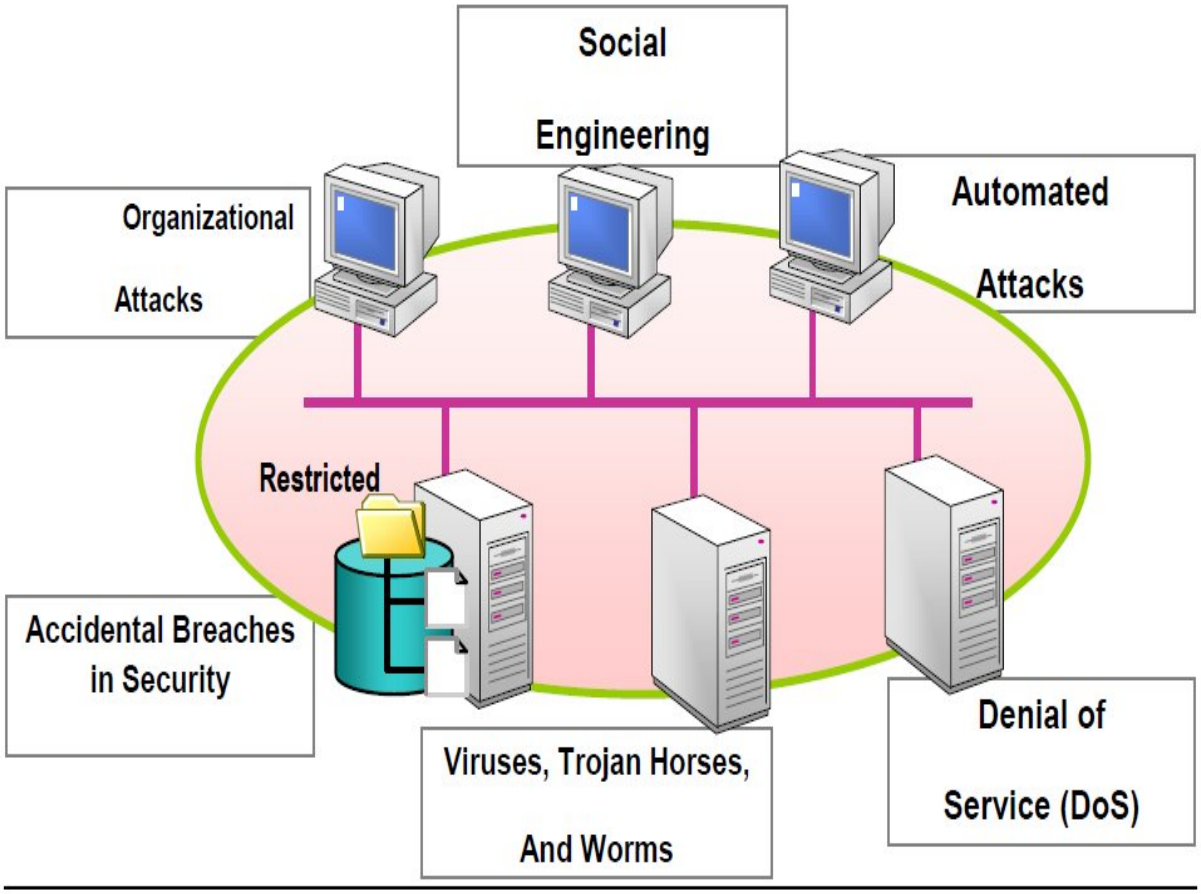
A black hat hackers or crackers are individuals with extraordinary computing skills, resorting to malicious or destructive activities. That is black hat hackers use their knowledge and skill for their own personal gains probably by hurting others.

- White-Hat Hacker

White hat hackers are those individuals professing hacker skills and using them for defensive purposes. This means that the white hat hackers use their knowledge and skill for the good of others and for the common good.

 Grey-Hat Hackers

These are individuals who work both offensively and defensively at various times. We cannot predict their behavior. Sometimes they use their skills for the common good while in some other times he uses them for their personal gains.



Different kinds of system attacks

ETHICAL HACKING

Ethical hacking – defined as —a methodology adopted by ethical hackers to discover the vulnerabilities existing in information systems operating environments.

With the growth of the Internet, computer security has become a major concern for businesses and governments.

In their search for a way to approach the problem, organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to break into their computer systems.

A) What does an Ethical Hacker do?

An ethical hacker is a person doing ethical hacking that is he is a security personal who tries to penetrate in to a network to find if there is some vulnerability in the system. An ethical hacker will always have the permission to enter into the target network. An ethical hacker will first think with a mindset of a hacker who tries to get in to the system.

He will first find out what an intruder can see or what others can see. Finding these an ethical hacker will try to get into the system with that information in whatever method he can. If he succeeds in penetrating into the system then he will report to the company with a detailed report about the particular vulnerability exploiting which he got in to the system. He may also sometimes make patches for that particular vulnerability or he may suggest some methods to prevent the vulnerability.

B) Required Skills of an Ethical Hacker:

Following are the skills at mostly required by an Ethical Hacker:

- Microsoft: skills in operation, configuration and management.
- Linux: knowledge of Linux/Unix; security setting, configuration, and services.
- Firewalls: configurations, and operation of intrusion detection systems.
- Routers: knowledge of routers, routing protocols, and access control lists Mainframes
- Network Protocols: TCP/IP; how they function and can be manipulated.
- Project Management: leading, planning, organizing, and controlling a penetration testing team.

C) HISTORY HIGHLIGHTS:

In one early ethical hack, the United States Air Force conducted a security evaluation of the Multics operating systems for potential use as a two-level (secret/top secret) system. With the growth of computer networking, and of the Internet in particular, computer and network vulnerability studies began to appear outside of the military establishment. Most notable of these was the work by Farmer and Venema, which was originally posted to Usenet in December of 1993.

Methodology of Hacking:

As described above there are mainly five steps in hacking like reconnaissance, scanning, and gaining access, maintaining access and clearing tracks. But it is not the end of the process. The actual hacking will be a circular one. Once the hacker completed the five steps then the hacker will start reconnaissance in that stage and the preceding stages to get in to the next level. The various stages in the hacking methodology are

- Reconnaissance
- Scanning & Enumeration
- Gaining access
- Maintaining access
- clearing tracks

A) Reconnaissance:

The literal meaning of the word reconnaissance means a preliminary survey to gain information. This is also known as foot-printing. This is the first stage in the methodology of hacking. As given in the analogy, this is the stage in which the hacker collects information about the company which the personal is going to hack. This is one of the pre-attacking phases. Reconnaissance refers to the preparatory phase where an attacker learns about all of the possible attack vectors that can be used in their plan

B) Scanning & Enumeration:

Scanning is the second phase in the hacking methodology in which the hacker tries to make a blue print of the target network. It is similar to a thief going through your neighborhood and checking every door and window on each house to see which ones are open and which ones are locked. The blue print includes the ip addresses of the target network which are live, the services which are running on those systems and so on. Usually the services run on predetermined ports. There are different tools used for scanning war dialing and pingers were used earlier but nowadays both could be detected easily and hence are not in much use. Modern port scanning uses TCP protocol to do scanning and they could even detect the operating systems running on the particular hosts.

C) Enumeration:

Enumeration is the ability of a hacker to convince some servers to give them information that is vital to them to make an attack. By doing this the hacker aims to find what resources and shares can be found in the system, what valid user account and user groups are there in the network, what applications will be there etc. Hackers may use this also to find other hosts in the entire network.

D) Gaining access:

This is the actual hacking phase in which the hacker gains access to the system. The hacker will make use of all the information he collected in the pre-attacking phases. Usually the main hindrance to gaining access to a system is the passwords. System hacking can be considered as many steps. First the hacker will try to get in to the system. Once he gets in to the system the next thing he wants will be to increase his privileges so that he can have more control over the system. As a normal user the hacker may not be able to see the

confidential details or cannot upload or run the different hack tools for his own personal interest.

E) Maintaining Access:

Now the hacker is inside the system by some means by password guessing or exploiting some of its vulnerabilities. This means that he is now in a position to upload some files and download some of them. The next aim will be to make an easier path to get in when he comes the next time. This is analogous to making a small hidden door in the building so that he can directly enter in to the building through the door easily. In the network scenario the hacker will do it by uploading some software like Trojan horses, sniffers, key stroke loggers etc.

F) Clearing Tracks:

Now we come to the final step in the hacking. There is a saying that —everybody knows a good hacker but nobody knows a great hacker. This means that a good hacker can always clear tracks or any record that they may be present in the network to prove that he was here. Whenever a hacker downloads some file or installs some software, its log will be stored in the server logs. So in order to erase that hacker uses man tools. One such tool is windows resource kit's auditpol.exe. This is a command line tool with which the intruder can easily disable auditing. Another tool which eliminates any physical evidence is the evidence eliminator. Sometimes apart from the server logs some other in formations may be stored temporarily. The Evidence Eliminator deletes all such evidences.

Advantages and Disadvantages:

Ethical hacking nowadays is the backbone of network security. Each day its relevance is increasing, the major pros & cons of ethical hacking are given below:

Advantages

- Provides security to banking and financial establishments
- Prevents website defacements
- An evolving technique
- To catch a thief you have to think like a thief

Disadvantages

- All depends upon the trustworthiness of the ethical hacker
- Hiring professionals is expensive.

Future enhancements:

- As it an evolving branch the scope of enhancement in technology is immense. No ethical hacker can ensure the system security by using the same technique repeatedly. He would have to improve, develop and explore new avenues repeatedly.
- More enhanced software should be used for optimum protection. Tools used, need to be updated regularly and more efficient ones need to be developed

Conclusion:

One of the main aims of the seminar is to make others understand that there are so many tools through which a hacker can get in to a system. Let‘s check its various needs from various perspectives.

 Student

A student should understand that no software is made with zero Vulnerabilities. So while they are studying they should study the various possibilities and should study how to prevent that because they are the professionals of tomorrow.

 Professionals

Professionals should understand that business is directly related to Security. So they should make new software with vulnerabilities as less as possible. If they are not aware of these then they won‘t be cautious enough in security matters.

References:

- www.mycollegebook.net
- www.wikipedia.org
- www.pdfcloud.net