ETHICAL HACKING

SEMINAR REPORT

PRESENTED BY: SHYAM S.V.
S7-CS
6249

SEMINAR GUIDE: Mrs. SHIJI

ABSTRACT

Today more and more softwares are developing and people are getting more and more options in their present softwares. 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. It's 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.

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

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

Types of Hackers:

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

- Black-Hat Hacker

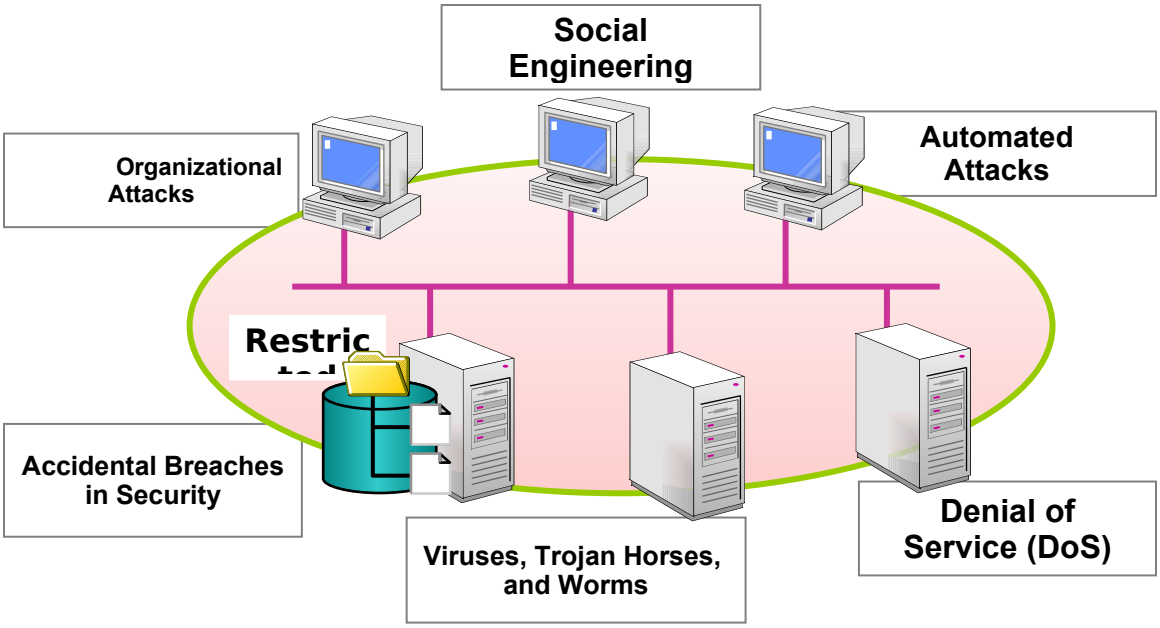
A black hat hackers or crackers are individuals with extraordinary computing skills, resorting to malicious or destructive activities. That is black hat hackers use their knowledge and skill for their own personal gains probably by hurting others.

- White-Hat Hacker

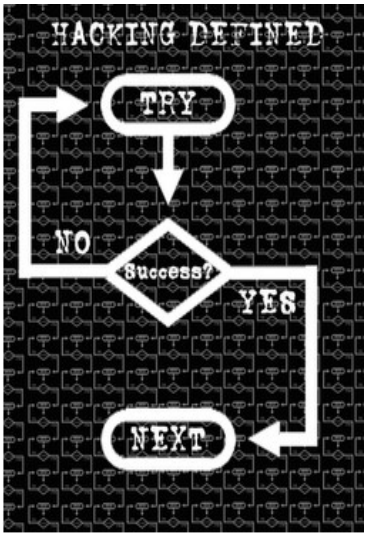
White hat hackers are those individuals professing hacker skills and using them for defensive purposes. This means that the white hat hackers use their knowledge and skill for the good of others and for the common good.

● Grey-Hat Hackers

These are individuals who work both offensively and defensively at various times. We cannot predict their behaviour. 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



General hacking

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.

What do 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.

Required Skills of 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.

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.

ETHICAL HACKING COMMANDMENTS:

Every ethical hacker must abide by a few basic commandments. If not, bad things can happen. The commandments are as follows:

- Working ethically:

  The word ethical in this context can be defined as working with high profes-sional morals and principles. Everything you do as an ethical hacker must be aboveboard and must support the company's goals. No hidden agendas are allowed! Trustworthiness is the ultimate tenet. The misuse of information is absolutely forbidden.

- Respecting privacy:

  Treat the information gathered with the utmost respect. All information you obtain during your testing — from Web-application log files to clear-text passwords — must be kept private. If you sense that someone should know there's a problem, consider sharing that information with the appropriate manager.

- Not crashing your systems:

  One of the biggest mistakes hackers try to hack their own systems is inadvertently crashing their systems. The main reason for this is poor planning. These testers have not read the documentation or misunderstand the usage and power of the security tools and techniques.

Methodology of Hacking:

As described above there are mainly five steps in hacking like reconnaissance, scanning, 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

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.

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 system 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 now a days 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.

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.

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 get in to the system the next thing he want 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. Another way to crack in to a system is by the attacks like man in the middle attack.

- Password Cracking:

There are many methods for cracking the password and then get in to the system. The simplest method is to guess the password. But this is a tedious work. But in order to make this work easier there are many automated tools for password guessing like legion. Legion actually has an inbuilt dictionary in it and the software will automatically. That is the software it self generates the password using the dictionary and will check the responses.

Techniques used in password cracking are:

- Dictionary cracking
- Brute force cracking
- Hybrid cracking
- Social engineering

- Privilege escalation:

Privilege escalation is the process of raising the privileges once the hacker gets in to the system. That is the hacker may get in as an ordinary user. And now he tries to increase his privileges to that of an administrator who can do many things. There are many types of tools available for this. There are some tools like getadmin attaches the user to some kernel routine so that the services run by the user look like a system routine rather than user initiated program. The privilege escalation process usually uses the vulnerabilities present in the host operating system or the software. There are many tools like hk.exe, metasploit etc. One such community of hackers is the metasploit.

Maintaining Access:

Now the hacker is inside the system by some means by password guessing or exploiting some of it's 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 softwares like Trojan horses, sniffers , key stroke loggers etc.

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 those the 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.

Ethical hacking tools:

Ethical hackers utilize and have developed variety of tools to intrude into different kinds of systems and to evaluate the security levels. The nature of these tools differ widely. Here we describe some of the widely used tools in ethical hacking.

- Samspade:

Samspade is a simple tool which provides us information about a particular host. This tool is very much helpful in finding the addresses, phone numbers etc

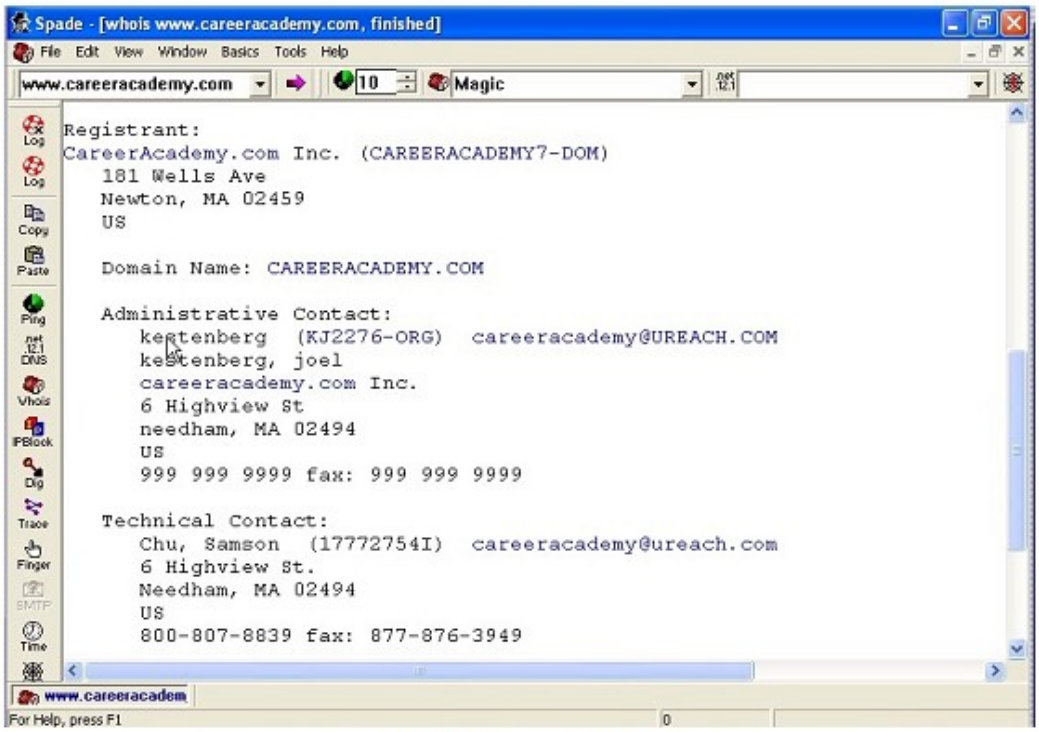


Fig 2.1 Samspade GUI

The above fig 2.1 represents the GUI of the samspade tool. In the text field in the top left corner of the window we just need to put the address of the particular host. Then we can find out various information available. The information given may be phone numbers, contact names, IP addresses, email ids, address range etc. We may think that what is the benefit of getting the phone numbers, email ids, addresses etc.

But one of the best ways to get information about a company is to just pick up the phone and ask the details. Thus we can get much information in just one click.

- Email Tracker and Visual Route:

We often used to receive many spam messages in our mail box. We don't know where it comes from. Email tracker is a software which helps us to find from which server does the mail actually came from. Every message we receive will have a header associated with it. The email tracker uses this header information for find the location.

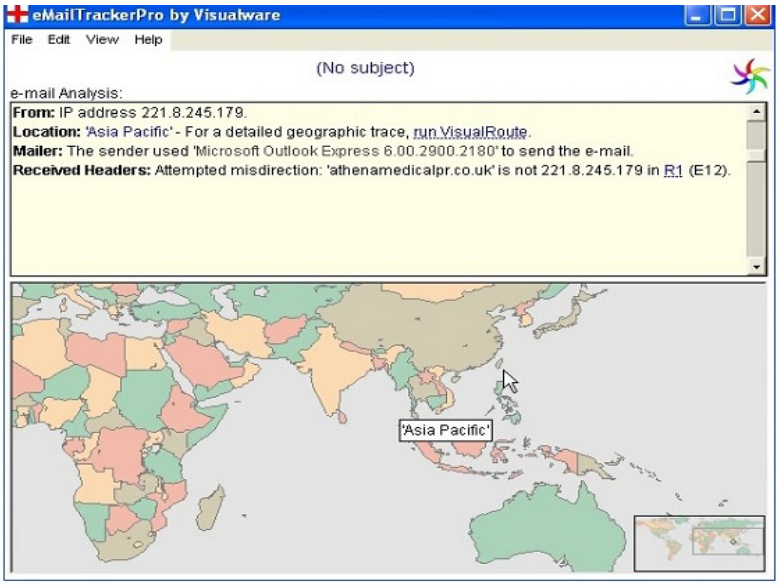


Fig 2.2 Email tracker GUI

The above fig 2.2 shows the GUI of the email tracker software. One of the options in the email tracker is to import the mail header. In this software we just need to import the mails header to it. Then the software finds from which area that mail comes from. That is we will get information like from which region does the message come from like Asia pacific, Europe etc. To be more specific we can use another tool visual route to pinpoint the actual location of the server. The option of connecting to visual route is available in the email tracker.

Visual route is a tool which displays the location a particular server with the help of IP addresses. When we connect this with the email tracker we can find the server which actually sends the mail. We can use this for finding the location of servers of targets also visually in a map

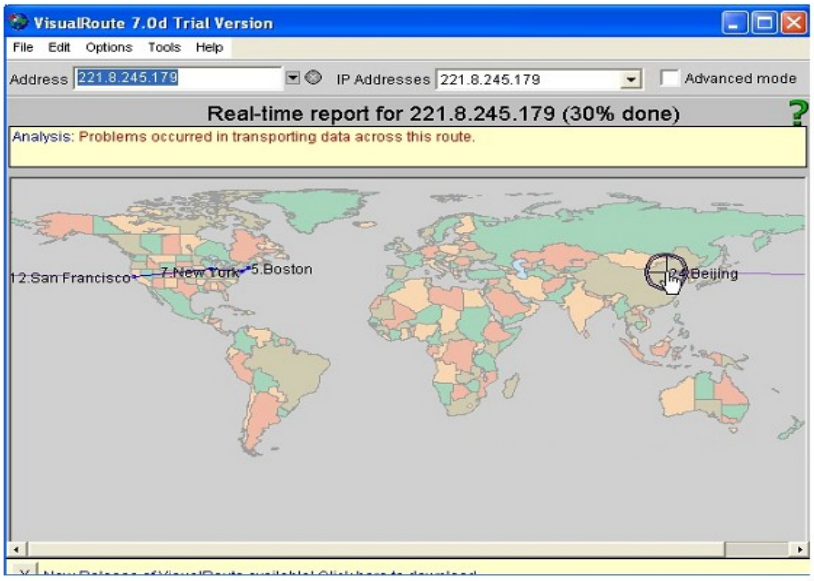


Fig 2.3 Visual route GUI

The above fig 2.3 depicts the GUI of the visual route tool. The visual route GUI have a world map drawn to it. The software will locate the position of the server in that world map. It will also depict the path though which the message came to our system. This software will actually provide us with information about the routers through which the message or the path traced by the mail from the source to the Destination.

Some other important tools used are:

- War Dialing
- Pingers
- Super Scan

- Nmap etc…

Reporting:

Assess your results to see what you uncovered, assuming that the vulnerabilities haven't been made obvious before now. This is where knowledge counts. Evaluating the results and correlating the specific vulnerabilities discovered is a skill that gets better with experience. You'll end up knowing your systems as well as anyone else. This makes the evaluation process much simpler moving forward. Submit a formal report to upper management or to your customer, outlining your results

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

- "To catch a thief you have to think like a thief"
- Helps in closing the open holes in the system network
- Provides security to banking and financial establishments
- Prevents website defacements
- An evolving technique

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 softwares 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.

In the preceding sections we saw the methodology of hacking, why should we aware of hacking and some tools which a hacker may use. Now we can see what we can do against hacking or to protect ourselves from hacking.

● The first thing we should do is to keep ourselves updated about those softwares we and using for official and reliable sources.

● Educate the employees and the users against black hat hacking.

● Use every possible security measures like Honey pots, Intrusion Detection Systems, Firewalls etc.

● every time make our password strong by making it harder and longer to be cracked.