**HACKERS AND HACKING**

**A SEMINAR REPORT**

***Submitted by***

**PENDYALA CHINMAYEE(17B91A12C7)**

***In partial fulfilment for the award of the degree***

***Of***

**BACHELOR OF TECHNOLOGY**

***in***

**INFORMATION TECHNOLOGY**

**SAGI RAMAKRISHNAM RAJU ENGINEERING COLLEGE**

**(AUTONOMOUS)**

**BHIMAVARAM,534 204. ANDHRA PRADESH**

**2017-2021**

**SAGI RAMAKRISHNAM RAJU ENGINEERING COLLEGE(A)**

**CHINAMIRAM, BHIMAVARAM-534 204.**

**BONAFIDE CERTIFICATE**

Certified that this project report “**HACKERS AND HACKING**” is the bonafide work of “**PENDYALA CHINMAYEE(17B91A12C7**)” who carried out the seminar work under my supervision.

**SIGNATURE**

**Dr. Bh. Rama Krsihnam Raju V S**

**Professor**

Dept. of Information Technology, Dept. of Information Technology,

Sagi Rama krishnam Raju Engineering College (A),

Chinamiram, Bhimavaram-534 202

**SIGNATURE**

**P.D.S.S. Lakshmi Kumari**

**Assistant Professor**

Dept. of Information Technology, Dept. of Information Technology,

Sagi Rama krishnam Raju Engineering College (A),

Chinamiram, Bhimavaram-534 202 Chinamiram, Bhimavaram-534 202

|  |  |
| --- | --- |
| **CONTENTS** | |
| List of Figures | *iv* |
| 1. Introduction   1.1 Security  1.2 Need for Security | 1-2  1  2 |
| 1. Types of Hackers | 3 |
| 1. Hacking Methodology   3.1 Reconnaissance  3.2 Scanning Network  3.3 Gaining Access  3.4 Maintaining Access  3.5 Clearing Logs and Traces | 4-7  4  5  5-6  7  7 |
| 1. Hacking Tools   4.1 VPN and TMAC  4.2 Key Loggers  4.3 Anti Key Loggers | 8-13  8-9  10  11-13 |
| 1. Conclusion | 14 |
| 1. References | 15 |

|  |  |  |
| --- | --- | --- |
| **LIST OF FIGURES** | | |
| **Figure No.** | **Titles** | **Page No.** |
| 4.1 | VPN | 9 |
| 4.2 | MAC address | 9 |
| 4.3.1 | Zemana Anti Key Logger | 13 |

**CHAPTER 1**

## INTRODUCTION

Hacking is the process of gaining access or control over computer network security systems. Hacking done under the supervision of owner of the system or organization is known as Ethical Hacking and the hacking done without any supervision and with no permission of user is known as Unethical Hacking.

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.

Unethical Hacking is the process of intruding into a network or a system without the permission of system’s owner. This type of hacking is unprofessional and is not certified by the government. This type of hacking practice is unethical and is considered as a criminal offense and is punishable under law. Such attacks can cause massive loss to the organizations in terms of finances as well as other resources.

**1.1 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.

Security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. The field is becoming increasingly significant due to the increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of “smart devices”, including smart phones, televisions and the various devices that constitute the “Internet of Things”.

**1.2 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

**CHAPTER 2**

**TYPES OF HACKERS**

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

Hackers can be broadly classified on the basis of why they are hacking system or why the are indulging hacking. They are of different types like:

* **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.
* **Suicide Hackers** : Individuals with extraordinary skills but mostly are of sensitivity. If they get caught, they are ready to suicide or facing years in jail. Suicide Hackers are same as Suicide Bombers. In most cases they hack a particular organization for revenge or for money etc.
* **Script Kiddies**: Individuals with no technical knowledge , they tend to watch YouTube videos, learn by themselves and showcase themselves to their friends and relatives or to neighbor's stating that they are hackers.
* **Cyber Terrorists**: Individuals with rationalistic behavior on to the internet media are known as Cyber Terrorists.

**CHAPTER 3**

**HACKING METHODOLOGY**

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

**3.1 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.

**3.2 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.

**3.3 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.

**3.4 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.

**3.5 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 software’s like Trojan horses, sniffers , key stroke loggers etc.

**3.6 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.

**CHAPTER 4**

**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.

**4.1 VPN and TMAC**

A person or a system is identified with its IP address in a particular network. This IP address is of two versions:

* IPv4: It is older version of IP address. IPv4 has 32-bit address length. IPv4 has header of 20-60 bytes. Address representation of IPv4 in decimal.
* IPv6: It is newer version of IP address. IPv6 has 128-bit address length. IPv6 has header of 40 bytes fixed. Address Representation of IPv6 is in hexadecimal.

There will be two IP addresses for a system in network. The one that is open and viewed to everybody in the network which is known as public IP and the other which is private IP.

In order to protect the system from being hacked one has to change these IP addresses while browsing or sending sensitive information like an organization details etc. These IP addresses can be changed using VPN ( Virtual Private Network). VPN's are used in order to hide identity of a particular system. There are anonymous browsers to hide our IP but VPN changes IP to a precise location. We can change our IP to a particular location's IP address using VPN. There are many paid VPN tools like "Hide My Ass", "ProtonVPN", "Nord VPN", "Cyber ghost" etc. Script Kiddies mostly use a tool called "BetterNet" to hide their IP. "Windscribe" is a VPN tool and also free which hides our IP address. The below given fig 4.1.1 shows the change of public IP address using Windscribe VPN.

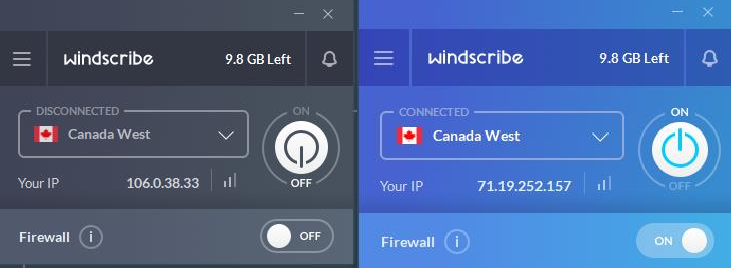


Fig 4.1.1

There is also a private MAC address used to recognize a particular system in deeper layers. Even this can be changed using some tools like Tmac ( Technitium MAC address Changer). This selected tool changes the MAC address of a particular system on request. The below given fig 4.1.2 show the change in the MAC address in a particular system.

Graphical user interface, text, application

Description automatically generated

Fig 4.1.2

**4.2 Key Loggers**

**Keyloggers** or keystroke loggers are software programs or hardware devices that track the activities (keys pressed) of a keyboard. Keyloggers are a form of spyware where users are unaware their actions are being tracked. Keyloggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities. Some keyloggers can also capture your screen at random intervals; these are known as screen recorders. Keylogger software typically stores your keystrokes in a small file, which is either accessed later or automatically emailed to the person monitoring your actions.

**Key Logger Software :**Remote- access software keyloggers can allow access to locally recorded data from a remote location. This communication can happen by using one of the following methods:

* Uploading the data to a website, database or FTP server.
* Periodically emailing data to a predefined email address.
* Wirelessly transmitting data through an attached hardware system.
* Software enabling remote login to your local machine.

Additional features that some software keyloggers come with can capture additional information without requiring any keyboard key presses as input. They include:

* Clipboard logging – Anything that can be copied to the clipboard is captured.
* Screen logging – Randomly timed screenshots of your computer screen are logged.
* Control text capture – The Windows API allows for programs to request the text value of some controls, meaning that your password may be captured even if behind a password mask (the asterisks you see when you type your password into a form).
* Activity tracking – Recording of which folders, programs and windows are opened and also possibly screenshots of each.
* Recording of search engine queries, instant message conversations, FTP downloads along with any other internet activities.

**Key Logger Hardware:**

Hardware-based keyloggers can monitor your activities without any software being installed at all. Examples of these include:

* Keyboard hardware - These loggers take the form of a piece of hardware inserted somewhere between the computer keyboard and the computer, typically along the keyboard's cable connection. There are of course more advanced implementation methods that would prevent any device from being visible externally. This type of hardware keylogger is advantageous because it is not dependent on any software nor can it be detected by any software.
* Wireless keyboard sniffers - It is possible for the signals sent from a wireless keyboard to its receiver to be intercepted by a wireless sniffer.
* Keyboard overlays - Overlays are popular in ATM theft cases where thieves capture a user's PIN number. This device is designed to blend in with the machine so that people are unaware of its presence.

**4.3 Detecting Key Loggers**

There are a variety of ways to detect a keylogger, though none are a catchall, so if you have reason to suspect your computer has a keylogger, we recommend trying a variety of these tactics:

* Begin by running your antivirus, which can often detect a keylogger on your system.
* Run a program like Spybot Search and Destroy or MalwareBytes to check for certain types.
* Check your task list by pressing ctrl+alt+del in Windows. Examine the tasks running, and if you are unfamiliar with any of them, look them up on a search engine.
* Scan your hard disk for the most recent files stored. Look at the contents of any files that update often, as they might be logs.
* Use your system configuration utility to view which programs are loaded at computer start-up. You can access this list by typing “msconfig” into the run box.

One of the tool to detect hidden keyloggers is Zemana Anti KeyLogger. The below fig 4.3.1 shows the detected keyloggers in a particular system.

Graphical user interface, website

Description automatically generated

Fig 4.3.1

**CHAPTER 5**

**CONCLUSION**

One of the main aim of the seminars is to make others understand that there are so many tools through which a hacker can get in to a system. There are many reasons for everybody should understand about these basics. Let’s check its various needs from various perspectives. A student should understand that no software is made with zero vulnerability. 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 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. Users The software is meant for the use of its users. Even if the software menders make the software with high security options without the help of users it can never be successful.

It’s like a highly secured building with all doors open carelessly by the insiders. So users must also be aware of such possibilities of hacking so that they could be more cautious in their activities. 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 can we do against hacking or to protect ourselves from hacking. The first thing we should do is to keep ourselves updated about those software’s 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. The final and foremost thing should be to try ETHICAL HACKING at regular intervals.

**REFERENCES**

* S. Patil, A. Jangra, M. Bhale, A. Raina and P. Kulkarni, "Ethical hacking: The need for cyber security," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), 2017, pp. 1602-1606, doi: 10.1109/ICPCSI.2017.8391982.
* C. C. Palmer, "Ethical hacking," in IBM Systems Journal, vol. 40, no. 3, pp. 769-780, 2001, doi: 10.1147/sj.403.0769.
* M. Wazid et al., "A framework for detection and prevention of novel keylogger spyware attacks," 2013 7th International Conference on Intelligent Systems and Control (ISCO), 2013, pp. 433-438, doi: 10.1109/ISCO.2013.6481194.
* D. Sukhram and T. Hayajneh, "KeyStroke logs: Are strong passwords enough?," 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017, pp. 619-625, doi: 10.1109/UEMCON.2017.8249051.
* <https://en.wikipedia.org/wiki/White_hat_(computer_security)>
* <https://en.wikipedia.org/wiki/Hacker>
* <https://home.sophos.com/en-us/security-news/2019/what-is-a-keylogger.aspx>
* <https://en.wikipedia.org/wiki/Black_hat_(computer_security)>
* <https://en.wikipedia.org/wiki/Anti-keylogger>
* <https://www.geeksforgeeks.org/anti-keylogger/>