EXECUTIVE SUMMARY OF UGC MINOR RESEARCH PROJECT TITLED
'CYBER SECURITY: THE PREREQUISITE OF TODAY'

SANCTINED WITH REF. NO MRP(S)-0816/13-14/ KLMG032/UGC- SWRO

1. INTRODUCTION

The astonishing advance of Internet usage has instigated many advantages like electronic commerce, trouble-free access to huge stores for online purchase, shared computing, e-mail, new possibility for advertising and information distribution etc. The dealers have observed this and they started contributing their entire services online. So the clients are enforced to depend on internet for their routine activities. The increasing dependence on networks and information technology has created opportunity for both job seekers and hackers. So enhancing the security of a networked computer is very important and certainly an area that generates much discussion is that of ethical hacking to lock the way for intruders thereby making the computer more secure and reliable. In today‘s context where the communication techniques have brought the world together; have also brought into being anxiety for the system owners all over the globe. The main reason behind this insecurity is Hacking- more specifically cracking the computer systems.

Hence the necessity of protecting the systems from the danger of hacking caused by the hackers increased and so the need for Ethical Hackers- the persons who will punch back the illegal attacks on our computer systems increased. This study discloses the concise suggestion of the ethical hacking and its relationships with the corporate security, ethical hacking as the counter measure to cracking in harmony with the corporate security as well as the individual protection. This project attempts to build up a centralized plan of the ethical hacking and its feature all together.

The motive of this project is to protect the centralized networking systems from vulnerabilities through the method of ethical hacking which opens up the loop holes for the hackers. Network Security can be achieved only if all vulnerabilities in both hardware and software elements of the networked system are identified and treated.

Here many types of attacks, attack models, IDSs (Intrusion Detection Systems) and IPSs (Intrusion Prevention Systems) are analyzed and the solution is reached.

2. COMPUTER SECURITY AND INTRUSION DETECTION

2.1. Introduction

As time passed by, the intruders or the so called hackers became more refined and classy in the line of attack that they use to encroach an into corporate networks and systems. They pay out the largest part of their time and effort in discovering latest ways to utilize the flaws and faults in the data communication mechanisms and systems used by frequent services like websites, E – Mails etc. In such a situation the traditional firewalls and anti – virus software were not able to assess the validity of many communications because the intrusion methods were too novel. In such a situation a study on computer security and intrusion detection has great significance.

2.2 Security Policy

Every organization must have a security policy which can be described as the skeleton within which the organization institutes the required stages of information security to accomplish the preferred confidentiality aspirations. A policy is a testimonial of information values, protection responsibilities and organization obligation for a system. Before one can appraise attacks against a system and settle on the right method to resist these threats, it is indispensable to stipulate a security policy. A security policy that is adequate for the data of one organization may not be enough for another organization.

2.3 Security Attack Types

The Data/Information communication can be graphically represented as follows:

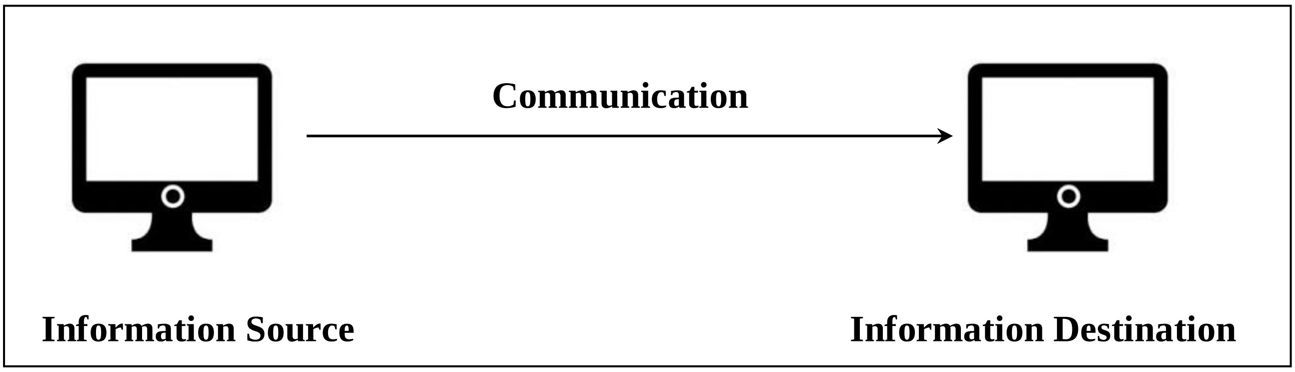
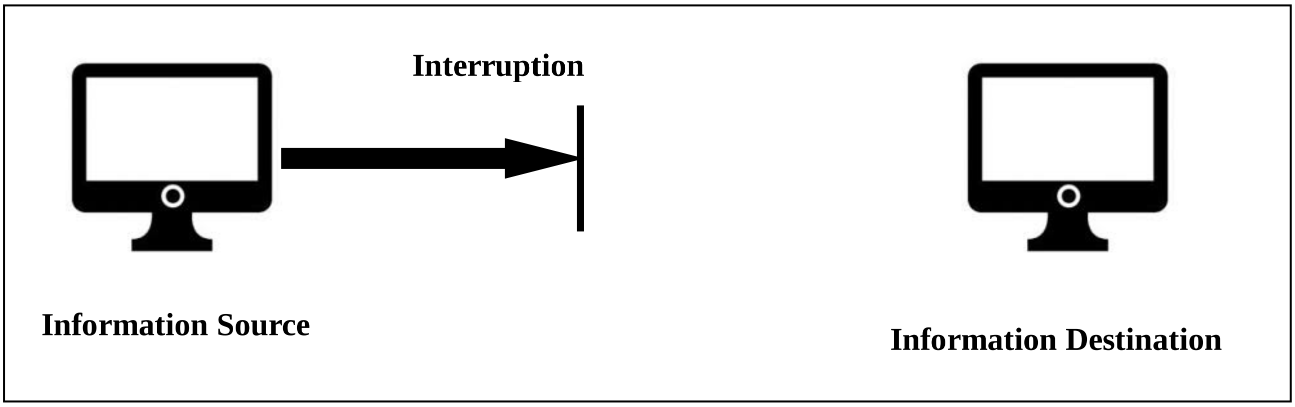


Fig2.1 Information Flow

2.3.1 Interruption

Interruption is the condition where the asset of a system gets damaged or turned out to be busy. This category of attack aims the source or the communication channel and stops the information from getting at the anticipated target. For example, the hacker could cut the physical cable, averting the information from reaching the desired destination or by performing DOS (Denial of Service) Attack. That is denying the requested services by overloading the communication channel unnecessarily.



The chemicals used for the ire listed below in table 2.1.

Fig: 2.2 Interruption

2.3.2 Interception

A process by which an unauthorized third party intruder accesses the information by intruding into the information channel is termed as Interception.

E.g. Intruding into the telephone line for gaining unauthorized access.

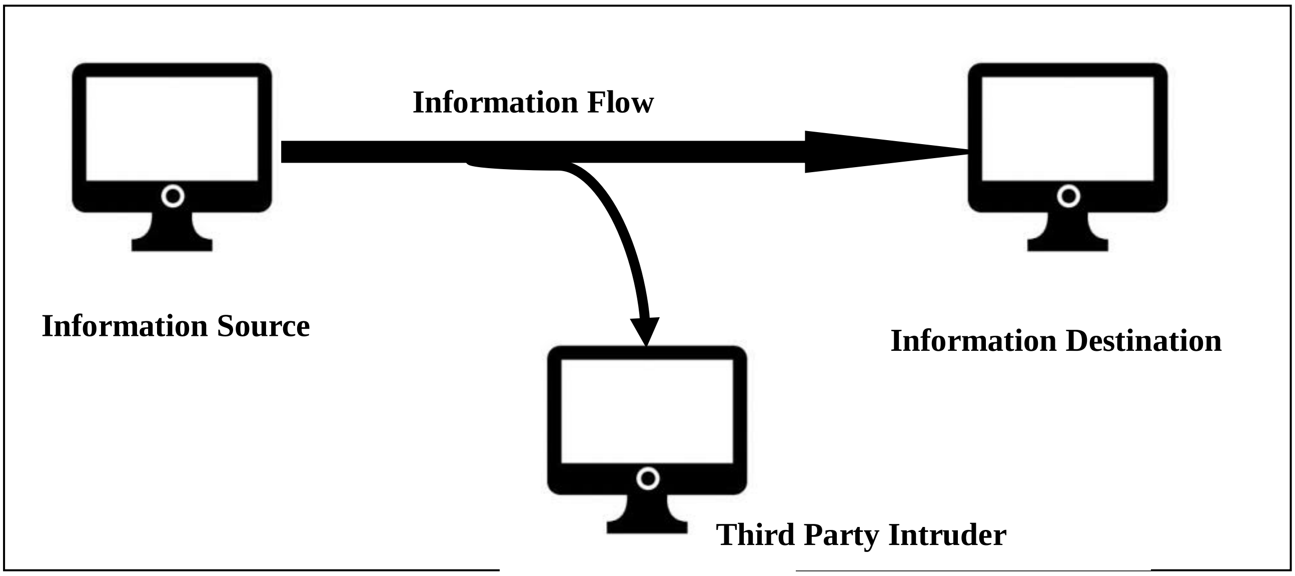


Fig: 2.3 Interceptions

2.3.3 Modification

Here the unauthorized third party intruder intrudes into the communication channel and accesses the information and modifies it. So the required/actual information may not reach the destination.

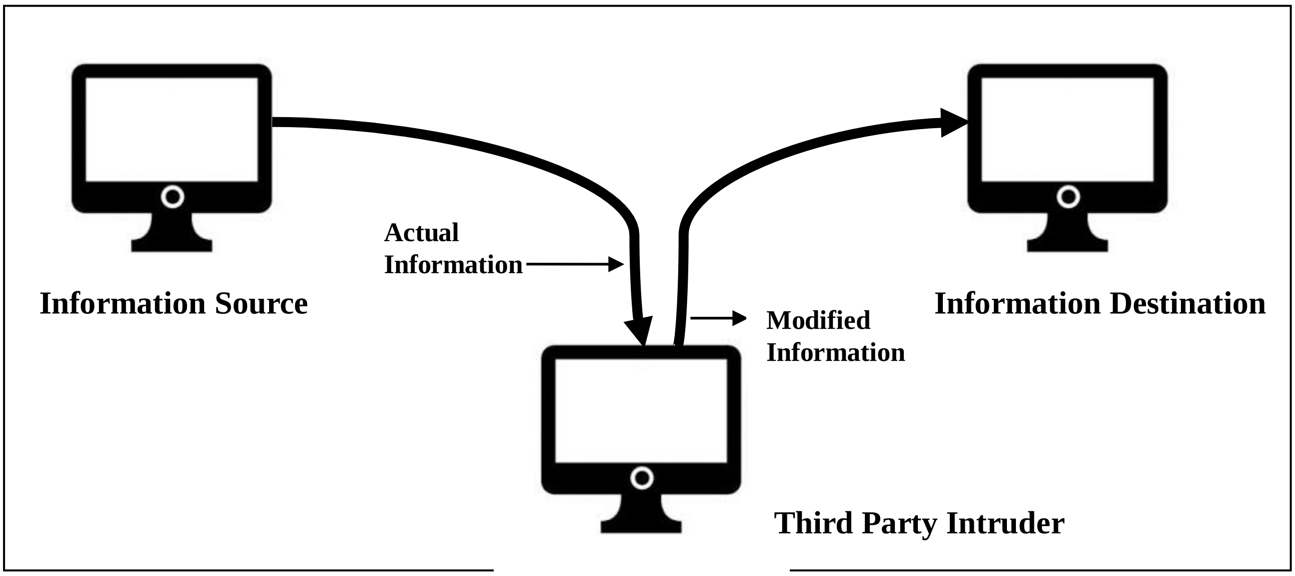


Fig: 2.4 Modifications

2.3.4 Fabrication

The unauthorized third party intruder fabricates the information that has been transmitted from information source to destination. This is done either by:

a. **Replaying** – By inserting previously intercepted entity.

b. **Masquerading** – Attacker pretends to be a genuine source and fabricates the information as they intend.

3. Security property

Every information system must require some security properties, which describes the desired feature of a system with regard to certain type of attacks. The above said classes of attacks violate most of the security properties of the target information system while they gain unauthorized access. The main security properties include:-

- Confidentiality
- Integrity
- Availability
- Authentication
- Non – Repudiation

3.1 Security Mechanisms

Security properties are the core qualities of an information system. These properties can be enforced using various security mechanisms. The various security mechanisms that can be used to restrict the attacks on security properties are:

1. Attack Prevention
2. Attack Avoidance
3. Attack Detection

3.2 Minutiae on Attack

A clever action that is consciously attempted to crack the security services and breach the security policy of a system effects in an assault on system security that has been derived from an intelligent threat. The following are the components of attack:

1. Attack Realization Tool – This is a kind of tool used by the attacker to perform an attack. The tool may vary depending on the type of attack. For example ‘nmap’ tool is usually used for performing port scanning attacks.
2. Vulnerability – Every information system will have any one of the following vulnerabilities:
    a. Design Vulnerability: The vulnerability that is inbuilt in the project or design of the information system. As this kind of vulnerability is inherent in the product, it is complicated to identify and abolish it.
    b. Implementation Vulnerability: The hardware/software faults that are commenced into the mechanism of the information system during its implementation stage.
    c. Operational/Configuration Vulnerability: These type of vulnerabilities are introduced into the system when the responsible system administrator doesn’t perform proper configuration.

3. Security Event.
4. Result of Attack.

3.3 Intruders

Intruders are of many types based on the kid of intrusion they perform on the information/communication channel. They include:

3.3.1 Script Kiddies: A script kiddie (also known as a skid or skiddie) is an unskilled hacker who breaks into computer systems by using automated tools written by others (usually by other black hat hackers), hence the term script (i.e. a prearranged plan or set of activities) kiddie (i.e. kid, child—an individual lacking knowledge and experience, immature),[23] usually with little understanding of the underlying concept.

3.3.2 White Hat Hackers: A white hat hacker breaks security for non-malicious reasons, either to test their own security system, perform penetration tests or vulnerability assessments for a client - or while working for a security company which makes security software. The term is generally synonymous with ethical hacker

3.3.3 Grey Hat Hackers: A grey hat hacker lies between a black hat and a white hat hacker. A grey hat hacker may surf the Internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect, for example. They may then offer to correct the defect for a fee.

3.3.4 Black Hat Hackers: A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2005).[19] The term was coined, to contrast the maliciousness of a criminal hacker versus the spirit of playfulness and exploration in hacker culture, or the ethos of the white hat hacker who performs hacking duties to identify places to repair or as a means of legitimate employment.[20] Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal".[21]

3.3.5 Red Hat Hackers: These are the vigilantes of the hacker world. They're like White Hats in that they halt Black Hats, but these folks are downright SCARY to those who have ever tried so much as PenTest. Instead of reporting the malicious hacker, they shut him/her down by uploading viruses, DoSing and accessing his/her computer to destroy it from the inside out. They leverage multiple aggressive methods that might force a cracker to need a new computer.

3.3.6 Blue Hat Hackers: A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term BlueHat to represent a series of security briefing events.

3.3.7 Hacktivist/ Cyber Terrorists: A hacktivist/ Cyber Terrorists is a hacker who utilizes technology to publicize a social, ideological, religious or political message.

3.3.7. a Hacktivism can be divided into two main groups:

3.3.7. b. Cyberterrorism — Activities involving website defacement or denial-of-service attacks; and,Freedom of information — Making information that is not public, or is public in non-machine-readable formats, accessible to the public.

3.3.8 Nation State/ Hacker Spies Supported by Government: Intelligence agencies and cyberwarfare operatives of nation states.

3.3.9 Elite Hackers: A social status among hackers, elite is used to describe the most skilled. Newly discovered exploits circulate among these hackers. Elite groups such as Masters of Deception conferred a kind of credibility on their members.

3.3.10 Neophyte: A neophyte ("newbie", or "noob") is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.

3.3.11 Corporate Spies: People trying to illegally obtain information about companies or government organisations are known as **corporate spies**. Typically when the attack is against a business it is profit-driven, while when it’s against government organisations it is espionage.

3.3.12 Professional Criminals:

3.3.13 Vandals: Cyber vandals are individuals who damage information infrastructures purely for their own enjoyment and pleasure. Their primary motivation is not financial; it is the desire to prove that the feat could be accomplished. Once inside they leave their mark so there is no denying their presence. At first brush this may seem more of a prank than an attack aimed at destruction. The effect on business, however, is undeniable. These types of attacks fall into the category of DOS or Denial of Service attack. The affected site must be shut down and repaired before it can be returned to normal operation. The massages left behind vary in tone: sometimes racial, sometimes profane, and sometimes political. Whatever the message, the effect is always disruptive.

4. **Intrusion Detection & Prevention System**

As far as an educational institution is concerned, a lot of intrusion attempts can be detected. Most of these attacks aim at logging into blocked social networking sites, movie downloading pages, on-line game zones etc. They commonly use proxy servers for this purpose. Antivirus software and firewalls cannot do much here. So there has to be some concrete intrusion detection and prevention systems to play against these intruders.

ETHICAL HACKING

4.1 INTRODUCTION

The Internet contains lot of vulnerabilities. The attackers or the hackers exploit these vulnerabilities and generates the route map for the attacks. There exist many bugs and faults with the networks, especially with the internet. So the hackers drafts newer and more sophisticated attacks using sophisticated Hacker Tools.

Attack scripts and Penetration Tools are freely available to anyone on the Internet. In this situation, concept of Ethical hacking, otherwise known as Penetration testing emerged as a solution. This can be considered as a technique that breaking into your own system to see yourselves how an unethical hacker or a cyber criminal do the same. Contrary to this simplistic view, a penetration test requires a detailed analysis of the threats and potential attackers in order to be most valuable [3]. Alternatively, Ethical Hacking can be considered as the process of thinking and acting as if we are hackers.

4.2 ADVANTAGES OF ETHICAL HACKING

The main advantage of Ethical Hacking or the so called Penetration Tests is to recognize the vulnerabilities sooner than they are exploited. A firm understanding of what is visible and possibly vulnerable in the computers or the network is offered by the process of Ethical Hacking.

This is a dominant defensive measure against hacking. The mechanism is very effective in finding the path of malicious intruders. The Ethical hacking technique includes a remediation phase through which some remedy or resolution can be designed for the appropriately identified vulnerabilities and Exposures.

4. 3 HOW IT IS DONE

The vulnerabilities and misuse opportunities in computers and network are always changing. So the remedial mechanisms are to be performed frequently. There exist many hacking tools and methods.

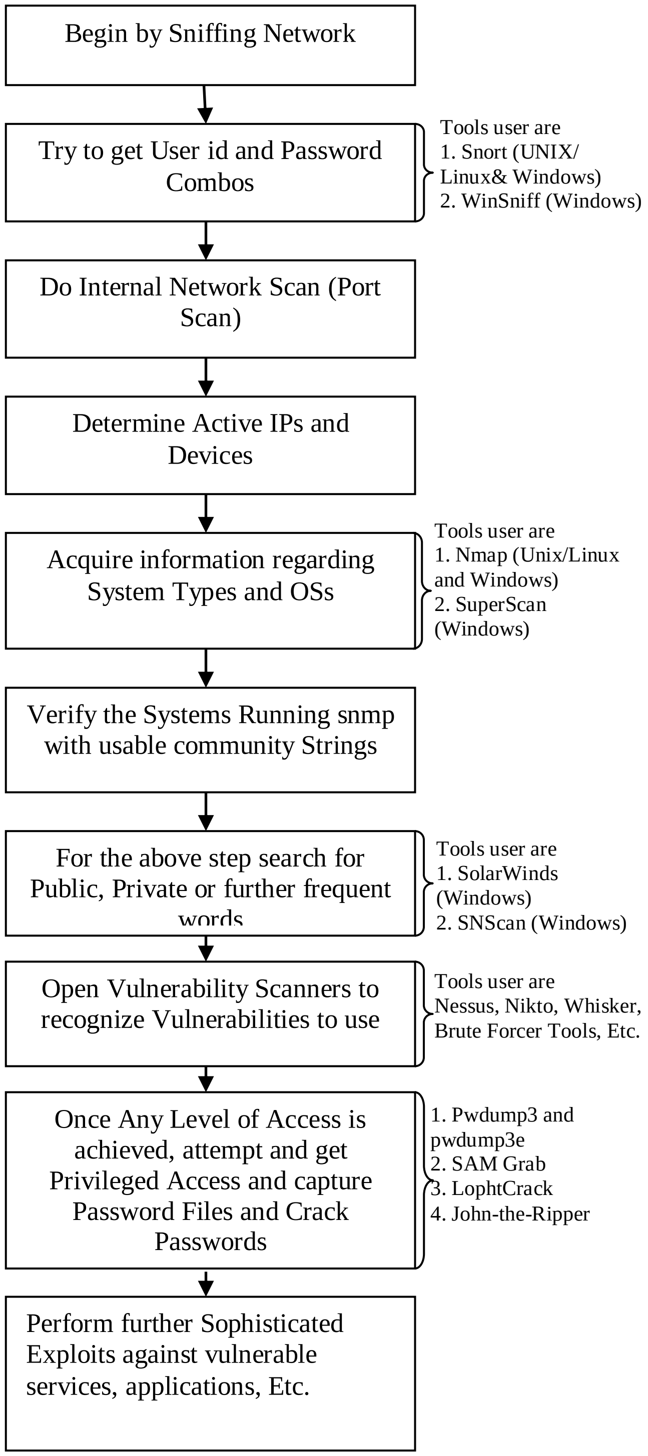
These tools and methods have to be used with utmost care, or else it can cause harm the system and the network. There exist different types of attacks on the computers and network. Some attacks are passive, some are not. Some attacks are e destructive, some are not. The process of Ethical Hacking requires and includes a definite process and attack methodology, and a set of tools for its fruitful execution.

4.3.1 Three Basic Attack Models:

Ethical Hackers make use of three basic models sequentially to attack the network. These models are the Black Box Model, the White Box Model and the Gray Box Model. Regarding the Black Box model, Ron Gula states that, in order to establish the response to the attack, the penetration test is only exposed to a handful of members of the network security team. [5] Nevertheless, it must also be mentioned that the Black Box model also assumes that the Ethical Hacker has limited knowledge of the network. This forces the ethical hacking team to gather a lot of information about the company from various sources prior to launching the penetration attack. With respect to the White Box approach, Gula points out that this model presupposes an expansive amount of knowledge about the company and its network.

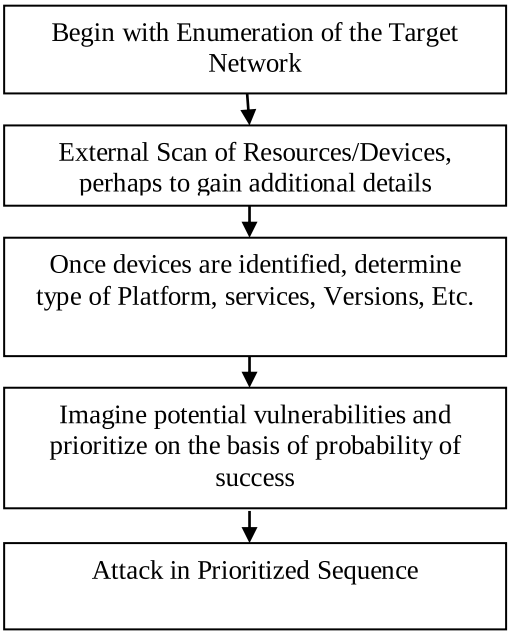
Furthermore, he indicates that the scope of the pre-attack information gathering might include interviews, access to internal network assets, physical security inspections and security policy evaluations. [5] The last category of attack models is the Gray Box model. This model combines elements of both the Black Box model and the White Box model providing a hybrid method of attack. [5] In other words, knowledge concerning some areas will be clearly defined. In the routine practice, Ethical hacking can also be either internal or external. In internal scheme its goal is to gain unauthorized access to the data/information. Its final objective is to get administrator, system, or root access from the indoors, depending on platform. This generally commence with just a network connection. It may possibly need a standard, non-privileged account.

The steps involved in Internal Scheme of Ethical Hacking are as follows:


Begin by Sniffing Network
Try to get User id and Password Combos
Tools user are
1. Snort (UNIX/ Linux& Windows)
2. WinSniff (Windows)
Do Internal Network Scan (Port Scan)
Determine Active IPs and Devices
Acquire information regarding System Types and OSs
Tools user are
1. Nmap (Unix/Linux and Windows)
2. SuperScan (Windows)
Verify the Systems Running snmp with usable community Strings
For the above step search for Public, Private or further frequent words
Tools user are
1. SolarWinds (Windows)
2. SNScan (Windows)
Open Vulnerability Scanners to recognize Vulnerabilities to use
Tools user are
Nessus, Nikto, Whisker, Brute Forcer Tools, Etc.
Once Any Level of Access is achieved, attempt and get Privileged Access and capture Password Files and Crack Passwords
1. Pwdump3 and pwdump3e
2. SAM Grab
3. LophtCrack
4. John-the-Ripper
Perform further Sophisticated Exploits against vulnerable services, applications, Etc.

The tools specified along with each steps assists to execute the actions described in the corresponding step. And these tools may show a discrepancy according to the Operating System used by the hacker and the supposed to be target. In internal scheme of Ethical Hacking, the goal is to get privileged access.

The steps involved in External Scheme of Ethical Hacking are as follows:


Begin with Enumeration of the Target Network
External Scan of Resources/Devices, perhaps to gain additional details
Once devices are identified, determine type of Platform, services, Versions, Etc.
Imagine potential vulnerabilities and prioritize on the basis of probability of success
Attack in Prioritized Sequence

Ethical Hacking or the Penetration Testing depends on a variety of tools to perform the intended task. These tools include Port Scanners, Demon Dialers, Vulnerability Scanners, Password Grabbers and Crackers, Vulnerability and Exploit Databases, Default Password Databases, above all Experience and the Good Old Internet.

The Process of Ethical Hacking can be subdivided into many other processes. All these processes altogether accomplish the task of Ethical Hacking. The sub processes in Ethical Hacking or the Penetration Testing are:

The Vulnerability Assessment Process: The vulnerability assessment process is the prime process in ethical hacking. This step is intended for analyzing the vulnerabilities of the target machine or the network that can be exploited by the hacker. The steps involved in analyzing the vulnerabilities include

- Collect Information regarding the target

- Scan IP Addresses
- Find out Service Versions
- Gather Target List
- Test and Assemble Exploits
- Execute exploits against live targets
- Evaluate Results
- Interactive Access on Host(s)
- Root/Admin Access on Host(s)
- Go over until no more targets existing or the preferred results are attained.

The Preliminary Work: The most important stuffs you require prior to starting the test are:

- Authority to Perform Test and this must be in writing.
- A detailed set of ground rules that should answer at least the following questions
- Is this test secret or evident?
- Are there any inaccessible systems or networks?
- Is there a specific target (system, type of information, etc) of this test?

Gathering Information: The First thing to be known is the IP address range(s) of the target computer, network or the organization. This can be made possible with the help of whois Lookup- a tool that helps to get details regarding the domain ownership. Other Sources of Information include IP address of Webserver(s), Mail Server(s), DNS Server(s), using whois lookup and verify who owns those IP addresses and the network space that contains those IP Addresses, IP Addresses of other organizations that may have been purchased by the primary organization, SamSpade.org. Also verify that all IP addresses and ranges with trusted POC prior to proceeding.

Scanning IP Addresses: The main purpose of this step is to discover what network ports /services are open. The tools like nmap can be used for this purpose. This tool is written for Unix/Linux Systems, and is freely available in the internet. The tool is ported to Windows NT/2000 by eEye Digital Security. This tool provides many features like multiple different scanning methods, Operating System detection, Ping sweeps, Changeable scan speed and multiple logging formats.

Determining Service Versions: A network service is expected to be provided by every open TCP Port. Well-Known services are usually provided by well-known port numbers. E.g.

TCP port 23 is probably be a telnet daemon. Version Numbers with very little urging are provided by well-known services.

Assembling the Target List: Assemble a comprehensive list of open ports and known service versions. Examine list for likely vulnerable versions of software, e.g. For Web Servers, examine the results of Whisker or Nikto scans for potentially vulnerable Scripts or Programs. Pick the top five most likely exploitable Hosts/Services.

Gathering and Testing Exploits: In no way execute or test the exploit code against a live target. It should be done only with prior testing against a test system. These exploits can be very dangerous. Only run it after a test. Its performance may not be as anticipated or desired. The nominal condition for exploit to be worth testing is that, it should match both target operating system and target service version number. The exploits have many prospective outcomes similar to reading and modifying any file on the target system, tolerating non-interactive implementation of Commands, allowing interactive access to remote system as an unprivileged user, as a Root, as an admin, or as other privileged user. When a candidate exploit is located, compile the code on a suitable platform and test it against test system and then review the results. If the exploit is unsuccessful, then move on to the next candidate. If the exploit is successful, then it can be tested against live targets.

Interactive Access on Host(s): Even as an interactive access is gained, the local exploits can be run. These are more common than remote exploits. It is easier to acquire root or admin-level rights. Subsequent to determining the available network interfaces and settings, check whether the system is behind a network address translator. Also check whether this system is on a DMZ or an internal network. Carry out port scans from this system against others on its local network. The privileged command access directs to a lot of additional alternatives. Start a network sniffer on every interface to obtain access to a host. Observe for trust relationships among this host and others. Acquire encrypted passwords or password hashes and begin cracking passwords. If the purpose is an explicit piece or kind of information, make sure that the system for that information. As each new piece of information is obtained, re-prioritize the target list and take action appropriately continue until all objectives are accomplished, or no further access can be obtained

IDENTIFYING THE NEED TO HACK SYSTEMS

The main aim behind ethical hacking is to act, think and work like a hacker. This may help in finding out all loop holes through which an intruder can enter into and hack the computer. A moment will arrive when all computer systems are hacked or negotiated in some way due to the enlarged numbers and escalating knowledge of hackers combined with the increasing number of system vulnerabilities and other unknowns. It is extremely serious to guard the systems from the hackers and not just the basic vulnerabilities that everybody knows about. When we know hacker tricks, we can see the intensity of vulnerabilities with our systems.

Hacking aims at weak security practices and secret vulnerabilities. A fake sense of security can be created through Firewalls, virtual private networks (VPN s), and encryption. These security systems frequently scan for sophisticated vulnerabilities, for example viruses and traffic through a firewall etc. Attacking the personal systems to determine vulnerabilities is a method through which the systems can be made more protected. This is the only established technique of significantly solidifying our systems from attack. If the weaknesses are not recognized, the vulnerabilities of the system will be effortlessly exploited.

CONCLUSION

Seeing that hackers amplify their knowledge, so should we. We have to think like them to guard our systems from the hackers. All activities of hackers must be identified along with methods to stop them. We should know the possible attacks from the hackers and how to get protected from hackers' efforts. We cannot get protected from the entire attacks by the hackers. The only way to get protected from each and every attack is to unplug our computer systems and lock it in order that no one including the owner touches them. That‘s not the best approach to information security. The significant aim is to protect our systems from identified vulnerabilities and common hacker attacks. It‘s impossible to support all possible vulnerabilities on all our systems. It's not probable to prepare for all likely attacks particularly the ones that are presently unidentified. Though, the more combinations we try, the more we test entire systems instead of individual units, the better our probability of identifying the vulnerabilities that influence the whole things. Ethical Hacking generates slight sense to solidify our systems from doubtful attacks. Nevertheless, don‘t fail to keep in mind regarding insider threats from malicious employees who may the most harmful hackers.