ETHICAL HACKING

(USCS607)

Smitha Renny

UNIT - II

- **Ethical Hacking – I (Introduction and pre-attack)**
- **Introduction**: Black Hat vs. Gray Hat vs. White Hat (Ethical) hacking, Why is Ethical hacking needed?, How is Ethical hacking different from security auditing and digital forensics?, Signing NDA, Compliance and Regulatory concerns, Black box vs. White box vs. Black box, Vulnerability assessment and Penetration Testing.
- **Approach : Planning** - Threat Modeling, set up security verification standards, Set up security testing plan – When, which systems/apps, understanding functionality, black/gray/white, authenticated vs. unauthenticated, internal vs. external PT, Information gathering, Perform Manual and automated (Tools: WebInspect/Qualys, Nessus, Proxies, Metasploit) VA and PT, How WebInspect/Qualys tools work: Crawling/Spidering, requests forging, pattern matching to known vulnerability database and Analyzing results, Preparing report, Fixing security gaps following the report
- **Enterprise strategy** : Repeated PT, approval by security testing team, Continuous Application Security Testing,
- **Phases:** Reconnaissance/foot-printing/Enumeration, **Phases**: Scanning, Sniffing

ETHICAL HACKING – I
(INTRODUCTION AND PRE-ATTACK)

INTRODUCTION :

Black Hat vs. Gray Hat vs. White Hat (Ethical) hacking

Hackers can be divided into three groups: white hats, black hats, and grey hats. Ethical hackers usually fall into the white-hat category, but sometimes they're former grey hats who have become security professionals and who use their skills in an ethical manner.

➢ **White hats**

- White Hats are the good guys, the ethical hackers who use their hacking skills for defensive purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement countermeasures.

➢ Black hats

- Black hats are the bad guys: the malicious hackers or *crackers* who use their skills for illegal or malicious purposes.
- They break into the system integrity of remote machines, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and basically cause problems for their targets.
- Black-hat hackers and crackers can easily be differentiated from white-hat hackers because their actions are malicious.

➢ Grey hats

- Grey hats are hackers who may work offensively or defensively, depending on the situation.
- This is the dividing line between hacker and cracker. Both are powerful forces on the Internet, and both will remain permanently.
- Some individuals qualify for both categories. The existence of such individuals further clouds the division between these two groups of people.

TESTING TYPES

- When performing a security test or penetration test, an ethical hacker utilizes one or more types of testing on the system.
- Each type simulates an attacker with different levels of knowledge about the target organization. These types are as follows:
- **Black box:** Black-box testing involves performing a security evaluation and testing with no prior knowledge of the network infrastructure or system to be tested. Testing simulates an attack by a malicious hacker outside the organization's security perimeter.

- **White box:** White-box testing involves performing a security evaluation and testing with complete knowledge of the network infrastructure such as a network administrator would have.

- **Grey box:** Grey-box testing involves performing a security evaluation and testing internally.
- Testing examines the extent of access by insiders within the network.

WHY IS ETHICAL HACKING NEEDED?

- Cyber crimes are becoming more common and attackers more sophisticated with terrorist organizations funding criminals to breech security networks either to extort hefty ransoms or compromise national security features.

- Businesses are faced with the challenge of dealing with complex security requirements that need to be updated as per changing hacking tactics, handling hidden vulnerabilities and evolving technologies.

- Ethical hacking firms with specially trained professionals come to the rescue of businesses while ensuring effectiveness of service and confidentiality.

- Although, many new businesses are better prepared in case of cyber attacks, traditional businesses still lack the proactive understanding of the need for ethical hacking.

- For example, in India, banks having faced the brunt many-a-times, are hiring professional help to secure their networks. Still the investment infrastructure for banks against cybercrime is quite minute compared to that of banks in the US.

HOW IS ETHICAL HACKING DIFFERENT FROM SECURITY AUDITING?

- **Security auditing** – involves comparing a company's security policies to what's actually taking place. The intent of security auditing is to validate that security controls exist.
  - Auditing often involves reviewing business processes and might not be technical. Not all audits are high-level, but the majority are quite simplistic.
- **Ethical hacking** – focuses on vulnerabilities that can be exploited. It validates that security controls *do not* exist or are ineffectual.
  - Ethical hacking can be both highly technical and non-technical. Even if formal methodology is used, it still is less structured than formal auditing.

HOW IS ETHICAL HACKING DIFFERENT FROM DIGITAL FORENSICS?

- **Computer forensics/Digital Forensics** is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.
- The goal of computer forensics is to **perform a structured investigation** while **maintaining a documented chain of evidence** to find out exactly what happened on a computing device and who was responsible for it.
- Forensic investigators typically follow a standard set of procedures. After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media.

- Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy.

- Investigators use a variety of techniques and software forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files.

- Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation.

SIGNING NDA (NON-DISCLOSURE AGREEMENT)

- In general, an ethical hacker will first meet with the client and sign a contract.
- The contract defines not only the permission and authorization given to the security professional, but also confidentiality and scope.
- No client would ever agree to having an ethical hacker attempt to breach security without first ensuring the hacker will not disclose any information found during the test.
- Usually, this concern results in the creation of a Non-Disclosure Agreement (NDA).
- A contract and non-disclosure agreement (NDA) is usually signed between the ethical hacker and the organization. This ensures that what they are doing is legal and that both parties are protected.

TYPES OF NON-DISCLOSURE AGREEMENTS

- NDA are of three types:-
- **Unilateral NDA**: It involves two parties, out of which only one party discloses certain information to the other and expects that the information is prevented from any further disclosure.
- **Bilateral NDA**: It involves two parties; both the parties disclose information to each other, and both of them intend to protect the information from disclosing to another. E.g.- Joint Venture.
- **Multilateral NDA:** It involves three or more parties to the agreement, out of which one of the parties discloses the information to other parties and wishes to have that information protected from any further disclosures. These types of NDAs also eliminate the need for distinct unilateral or bilateral NDA.

IMPORTANT CLAUSES OF NDA

- Timeframe of the NDA
- What is the Confidential Information ought to be protected under the NDA?
- Duties and obligation of the parties to NDA
- Consequences of breach of an NDA
- Right to seek an injunction in an NDA
- Dispute Resolution clause in an NDA

PENETRATION TESTING (PEN TEST)

- Penetration Testing is used to find flaws in the system in order to take appropriate security measures to protect the data and maintain functionality.
- Penetration testing replicates the actions of an external or/and internal cyber attacker/s that is intended to break the information security and hack the valuable data or disrupt the normal functioning of the organization.
- So, with the help of advanced tools and techniques, a penetration tester makes an effort to control critical systems and acquire access to sensitive data.

VULNERABILITY ASSESSMENT

- A vulnerability assessment is the technique of identifying and measuring security vulnerabilities in a given environment.
- It is a comprehensive assessment of the information security position (result analysis).
- It identifies the potential weaknesses and provides the proper mitigation measures (remediation) to either remove those weaknesses or reduce below the risk level.

PENETRATION TESTING VS. VULNERABILITY ASSESSMENTS

Penetration Testing	Vulnerability Assessments
Determines the scope of an attack.	Makes a directory of assets and resources in a given system.
Tests sensitive data collection	Discovers the potential threats to each resource.
Gathers targeted information and/or inspect the system.	Allocates quantifiable value and significance to the available resources
Cleans up the system and gives final report.	Attempts to mitigate or eliminate the potential vulnerabilities of valuable resources
It is non-intrusive, documentation and environmental review and analysis.	Comprehensive analysis and through review of the target system and its environment.
It is ideal for physical environments and network architecture.	It is ideal for lab environments.
It is meant for critical real-time systems.	It is meant for non-critical systems.

THREAT MODELING

- Threat modeling is the process of defining assets and the possible attacks that they may face.
- The threat model tries to break down assets or individual components of an application to better quantify what is being threatened.
- Once things are diagrammed and defined, you have a clearer picture of what needs to be assessed and have more guidance as to how to proceed.
- The threat-modeling process concentrates on gaining information in four key ways:
  - Gather relevant documentation.
  - Identify and categorize primary and secondary assets.
  - Identify and categorize threats and threat communities.
  - Map threat communities against primary and secondary assets.

SECURITY VERIFICATION STANDARD

- The Application Security Verification Standard is a list of application security requirements or tests that can be used by architects, developers, testers, security professionals, and even consumers to define what a secure application is.

- **Application Security Verification Levels**
  - The Application Security Verification Standard defines three security verification levels, with each level increasing in depth.
  - ASVS Level 1 is meant for all software. (Opportunistic)
  - ASVS Level 2 is for applications that contain sensitive data, which requires protection. (Standard)
  - ASVS Level 3 is for the most critical applications - applications that perform high value transactions, contain sensitive medical data, or any application that requires the highest level of trust. (Advanced)

TESTING APPROACHES

- **Black Box Penetration Testing**: In this approach, the tester assesses the target system, network or process without the knowledge of its details. They just have very high level of inputs like URL or company name using which they penetrate into the target environment. No code is being examined in this method.
- **White Box Penetration Testing**: In this approach, the tester is equipped with complete details about the target environment – Systems, network, OS, IP address, source code, schema, etc. It examines the code and finds out design & development errors. It is a simulation of internal security attack.
- **Grey Box Penetration Testing**: In this approach, the tester has limited details about the target environment. It is a simulation of external security attack.

AUTHENTICATED SCAN

- An authenticated security scan is vulnerability testing performed as a logged-in (authenticated) user. The method is also known as logged-in scanning.
- Authenticated scans determine how secure a network is from inside. The method finds many vulnerabilities that cannot be detected through an unauthenticated scan.
- Visibility into those security holes helps administrators identify what needs to be done to ensure that should an attacker gain access to the network or a user account, important accounts and data will be protected. The information yielded by authenticated scans also helps ensure that insider threats do only limited in the damage.

UNAUTHENTICATED SCANS

- Thousands of IT organizations across the world use vulnerability scanners to perform unauthenticated scans and find threats within their network.
- These scans find basic weaknesses and detect issues within operating systems, open network ports, services listening on open ports, and data leaked by services.
- This gives companies the ability to see their network from the eyes of an attacker.

EXTERNAL PENETRATION TEST

- An External Penetration Test exploits the vulnerabilities to determine what information is actually exposed to the outside world.
- An External Penetration Test mimics the actions of an actual attacker exploiting weaknesses in the network security without the usual dangers.
- This test examines external IT systems for any weakness that could be used by an external attacker to disrupt the confidentiality, availability or integrity of the network, thereby allowing the organization to address each weakness.

INTERNAL PENETRATION TEST

- An Internal Penetration Test differs from a vulnerability assessment in that it actually exploits the vulnerabilities to determine what information is actually exposed.
- An Internal Penetration Test mimics the actions of an actual attacker exploiting weaknesses in network security without the usual dangers.
- This test examines internal IT systems for any weakness that could be used to disrupt the confidentiality, availability or integrity of the network, thereby allowing the organization to address each weakness.

INTERNAL VS. EXTERNAL PENETRATION TEST

- External pen-testing is the traditional, more common approach to pen-testing. It addresses the ability of a remote attacker to get to the internal network. The goal of the pen-test is to access specific servers within the internal network by exploiting externally exposed servers, clients, and people.
- Whether it's an exploit against a vulnerable Web application or tricking a user into giving you his password over the phone, allowing access to the VPN, the end game is getting from the outside to the inside.

- Internal pen-testing takes a different approach -- one that simulates what an insider attack could accomplish. The target is typically the same as external pen-testing, but the major differentiator is the "attacker" either has some sort of authorized access or is starting from a point within the internal network.

- Insider attacks have the potential of being much more devastating than an external attack because insiders already have the knowledge of what's important within a network and where it's located, something that external attackers don't usually know from the start.

AUTOMATED PENETRATION TESTING TOOLS

- Automated penetration testing tools have robust, high-quality exploits that are tested and proven; the tools are also frequently augmented with additional exploits.
- They provide replicable processes that ensure consistent results.
- One can focus on the process rather than having to experiment with exploits, thus saving time. Further, the professional framework reduces the chances of testing false exploits over a particular application.
- Reports are automatically produced and are customizable.

MANUAL PENETRATION TEST

- It is difficult to find all vulnerabilities using automated tools. There are some vulnerabilities which can be identified by manual scan only.
- Penetration testers can perform better attacks on application based on their skills and knowledge of the system being penetrated. The methods like social engineering can be done by humans only.
- Manual checking includes design, business logic as well as code verification.

WebInspect

- WebInspect is a web application security scanning tool offered by HP. It helps the security professionals to assess the potential security flaws in the web application.
- WebInspect is a dynamic black box testing tool which detects the vulnerabilities by actually performing the attack.
- After initiating the scan on a web application, there are ‘assessment agents’ that work on different areas of the application. They report their results to ‘security engine’ which evaluates the results.

- It uses ‘Audit engines’ to attack the application and determine the vulnerabilities. At the end of the scan a report called ‘Vulnerability Assessment Report’ is generated which would list the security issues in desired format. Using this report client can fix the issues and then go for validation scanning to confirm the same. As with every other tool there are both advantages and disadvantages associated with using WebInspect.

Share WebInspect.pdf

VULNERABILITY ASSESSMENT

- A vulnerability assessment is the technique of identifying (discovery) and measuring security vulnerabilities (scanning) in a given environment. It is a comprehensive assessment of the information security position (result analysis).
- Further, it identifies the potential weaknesses and provides the proper mitigation measures (remediation) to either remove those weaknesses or reduce below the risk level.

PENETRATION TESTING

- Penetration testing replicates the actions of an external and/or internal cyber attacker/s that is intended to break the information security and hack the valuable data or disrupt the normal functioning of the organization.
- So, with the help of advanced tools and techniques, a penetration tester (also known as **ethical hacker**) makes an effort to control critical systems and acquire access to sensitive data.

PENETRATION TESTING VS. VULNERABILITY ASSESSMENT

Penetration Testing	Vulnerability Assessments
Determines the scope of an attack.	Makes a directory of assets and resources in a given system.
Tests sensitive data collection.	Discovers the potential threats to each resource.
Gathers targeted information and/or inspect the system.	Allocates quantifiable value and significance to the available resources.
Cleans up the system and gives final report.	Attempts to mitigate or eliminate the potential vulnerabilities of valuable resources.
It is non-intrusive, documentation and environmental review and analysis.	Comprehensive analysis and through review of the target system and its environment.
It is ideal for physical environments and network architecture.	It is ideal for lab environments.
It is meant for critical real-time systems.	It is meant for non-critical systems.

TYPES OF PEN TESTING

The type of penetration testing normally depends on the scope and the organizational wants and requirements..

Types of Pen Testing

- Black Box Penetration Testing
- White Box Penetration Testing
- Grey Box Penetration Testing
-

BLACK BOX PENETRATION TESTING

In black box penetration testing, tester has no idea about the systems that he is going to test.

He is interested to gather information about the target network or system. For example, in this testing, a tester only knows what should be the expected outcome and he does not know how the outcomes arrives.

He does not examine any programming codes.

- Advantages –
  - Tester need not necessarily be an expert, as it does not demand specific language knowledge
  - Tester verifies contradictions in the actual system and the specifications
  - Test is generally conducted with the perspective of a user, not the designer
- Disadvantages –
  - These kinds of test cases are difficult to design.
  - It does not conduct everything.

WHITE BOX PENETRATION TESTING

This is a comprehensive testing, as tester has been provided with whole range of information about the systems and/or network such as Schema, Source code, OS details, IP address, etc.

It is normally considered as a simulation of an attack by an internal source. It is also known as structural, glass box, clear box, and open box testing.

- White box penetration testing examines the code coverage and does data flow testing, path testing, loop testing, etc.

Advantages –

- It ensures that all independent paths of a module have been exercised.
- It ensures that all logical decisions have been verified along with their true and false value.
- It finds the design errors that may have occurred because of the difference between logical flow of the program and the actual execution.

GREY BOX PENETRATION TESTING

- In this type of testing, a tester usually provides partial or limited information about the internal details of the program of a system.
- It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents.

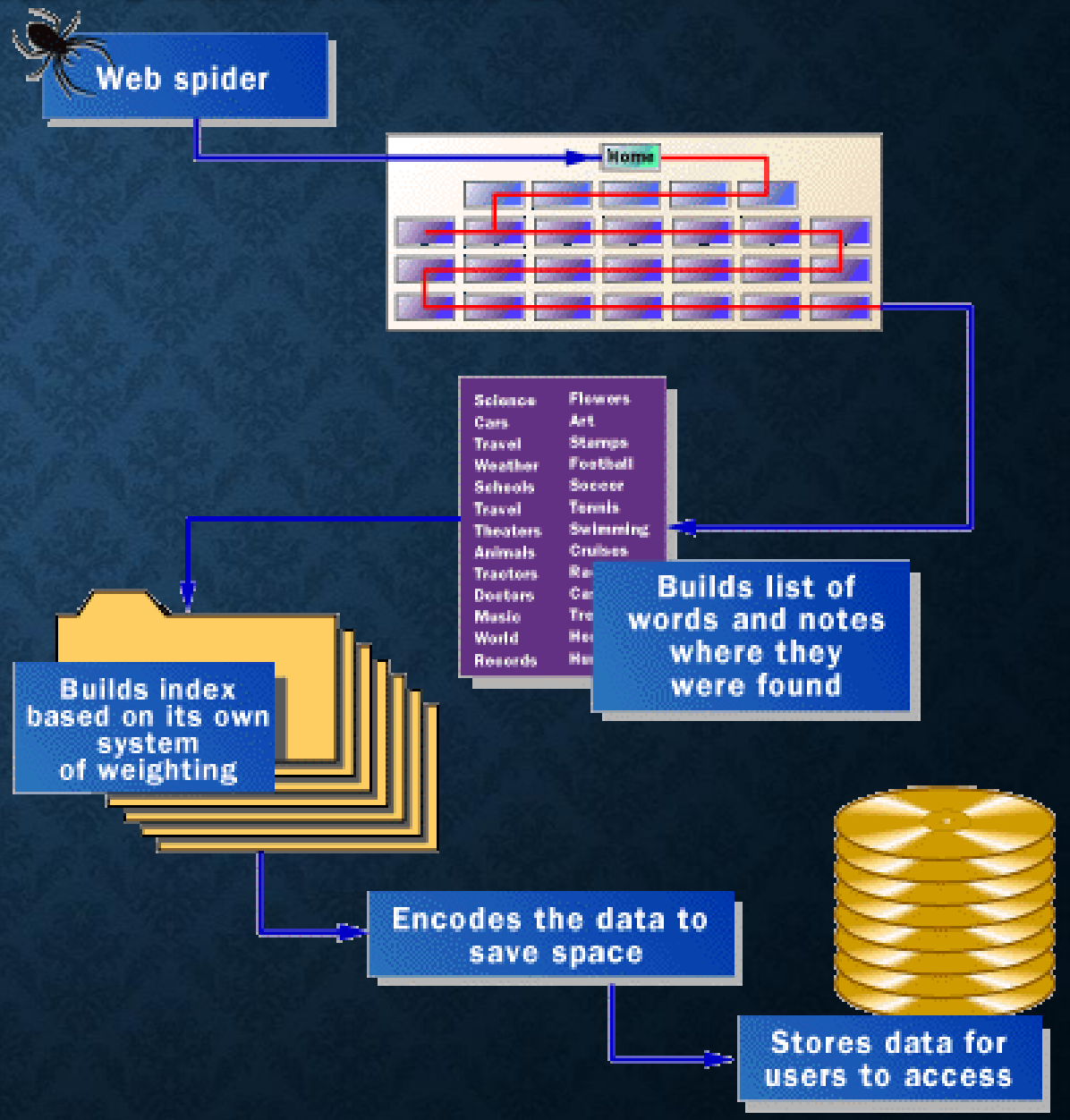
- **Advantages** –
  - As the tester does not require the access of source code, it is non-intrusive and unbiased
  - As there is clear difference between a developer and a tester, so there is least risk of personal conflict
  - You don’t need to provide the internal information about the program functions and other operations

AREAS OF PENETRATION TESTING

- Penetration testing is normally done in the following three areas –
- **Network Penetration Testing** – In this testing, the physical structure of a system needs to be tested to identify the vulnerability and risk which ensures the security in a network. The devices, which are tested by a tester can be computers, modems, or even remote access devices, etc
- **Application Penetration Testing** – In this testing, the logical structure of the system needs to be tested. It is an attack simulation designed to expose the efficiency of an application's security controls by identifying vulnerability and risk.
- **The response or workflow of the system** – This is the third area that needs to be tested. Social engineering gathers information on human interaction to obtain information about an organization and its computers. It is beneficial to test the ability of the respective organization to prevent unauthorized access to its information systems. This test is exclusively designed for the workflow of the organization/company.

SPIDERS & WEB CRAWLING

- To find information on the hundreds of millions of Web pages that exist, a search engine employs special software robots, called **spiders**, to build lists of the words found on Web sites.
- When a spider is building its lists, the process is called **Web crawling**.



SEARCH ENGINE COMPONENTS

Generally there are three basic components of a search engine as listed below:

- Web Crawler
- Database
- Search Interfaces

Web crawler

- It is also known as **spider** or **bots.** It is a software component that traverses the web to gather information.

Database

- All the information on the web is stored in database. It consists of huge web resources.

Search Interfaces

- This component is an interface between user and the database. It helps the user to search through the database.

SEARCH ENGINE WORKING

- Web crawler, database and the search interface are the major component of a search engine that actually makes search engine to work. Search engines make use of Boolean expression AND, OR, NOT to restrict and widen the results of a search. Following are the steps that are performed by the search engine:

1. The search engine looks for the keyword in the index for predefined database instead of going directly to the web to search for the keyword.
2. It then uses software to search for the information in the database. This software component is known as **web crawler**.
3. Once web crawler finds the pages, the search engine then shows the relevant web pages as a result. These retrieved web pages generally include title of page, size of text portion, first several sentences etc.

SEARCH ENGINE COMPONENTS

I. Indexing Process

Indexing process comprises of the following three tasks:

1. Text acquisition
2. Text transformation
3. Index creation

Text acquisition

- It identifies and stores documents for indexing.

Text Transformation

- It transforms document into index terms or features.

Index Creation

- It takes index terms created by text transformations and create data structures to support fast searching.

II. Query Process

Query process comprises of the following three tasks:

1. User interaction
2. Ranking
3. Evaluation

User interaction

- It supports creation and refinement of user query and displays the results.

Ranking

- It uses query and indexes to create ranked list of documents.

Evaluation

- It monitors and measures the effectiveness and efficiency. It is done offline.

WHAT ARE THE HACKING STAGES?

- Hacking, or targeting on a machine, should have the following 5 phases :
- **Surveillance/Reconnaissance :** This is the principal stage where the hacker endeavours to gather as much data as possible about the target
- **Scanning :** This stage includes exploiting the data accumulated amid Surveillance stage and utilizing it to inspect the casualty. The hacker can utilize computerized devices amid the scanning stage which can incorporate port scanners, mappers and vulnerability scanners.
- **Getting/Gaining access :** This is where the real hacking happens. The hacker attempts to exploit data found amid the surveillance and Scanning stage to get access.
- **Maintaining Access/Access Maintenance :** Once access is gained, hackers need to keep that access for future exploitation and assaults by securing their exclusive access with backdoors, rootkits and Trojans.
- **Covering/Clearing tracks :** Once hackers have possessed the capacity to pick up and maintain access, they cover their tracks and to keep away from getting detected. This likewise enables them to proceed with the utilization of the hacked framework and keep themselves away from legitimate activities.

WHAT ARE THE TOOLS USED FOR ETHICAL HACKING?

There are several moral hacking tools for different purposes, they are:

- **NMAP** – NMAP stands for Network plotter. It's associate degree open source tool that's used wide for network discovery and security auditing.
- **Metasploit** – Metasploit is one amongst the most powerful exploit tool to conduct basic penetration tests.
- **Burp Suit** – Burp Suite could be a widespread platform that's widely used for playing security testing of internet applications.
- **Angry IP Scanner** – Angry information processing scanner could be a light-weight, cross-platform information processing address and port scanner.
- **Cain & Abel** – Cain & Abel is a password recovery tool for Microsoft operational Systems.
- **Ettercap** – Ettercap stands for local area network Capture. It is used for Man-in-the-Middle attack using a network security tool.

PHASES: RECONNAISSANCE/FOOT-PRINTING/ENUMERATION

- Information Gathering and getting to know the target systems is the first process in ethical hacking.
- Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system.
- During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible.

Following are the seven steps of reconnaissance listed below –

- Gather initial information
- Determine the network range
- Identify active machines
- Discover open ports and access points
- Fingerprint the operating system
- Uncover services on ports
- Map the network

Reconnaissance takes place in two parts –

- **Active Reconnaissance**
- In this process, the hacker directly interacts with the computer system to gain information. This information can be relevant and accurate. But there is a risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then system admin can take severe action against you and trail your subsequent activities.

- **Passive Reconnaissance**
- In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

FOOTPRINTING

- Footprinting(also called fingerprinting) is a part of reconnaissance process which is used for gathering possible information about a target computer system or network.
- Footprinting could be both **passive** and **active**.
- Reviewing a company's website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.
- Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

During this phase, a hacker can collect the following information −

- Domain name
- IP Addresses
- Namespaces
- Employee information
- Phone numbers
- E-mails
- Job Information

- **Domain Name Information**
- You can use http://www.whois.com/whois website to get detailed information about a domain name information
- **Finding IP Address**
- You can use **ping** command at your prompt.
- This command is available on Windows as well as on Linux OS.
- **Finding Hosting Company**
- Once you have the website address, you can get further detail by using **ip2location.com** website.

OS FINGERPRINTING

- Before attacking a system, it is required that we know what operating system is hosting a website. Once a target OS is known, then it becomes easy to determine which vulnerabilities might be present to exploit the target system.
- **nmap** command is used to identify the operating system serving a website and all the opened ports associated with the domain name, i.e., the IP address.
- OS fingerprinting could be –
- **Active Fingerprinting** – Active fingerprinting is accomplished by sending specially crafted packets to a target machine and then noting down its response and analyzing the gathered information to determine the target OS.
- **Passive Fingerprinting** – Passive fingerprinting is based on sniffer traces from the remote system. Based on the sniffer traces (such as Wireshark) of the packets, you can determine the operating system of the remote host.

- There are four important elements to determine the operating system –.

- **TTL** – What the operating system sets the **Time-To-Live** on the outbound packet.
- **Window Size** – What the operating system sets the Window Size at.
- **DF** – Does the operating system set the **Don't Fragment** bit.
- **TOS** – Does the operating system set the **Type of Service**, and if so, at what.

By analyzing these factors of a packet, you may be able to determine the remote operating system. This system is not 100% accurate, and works better for some operating systems than others.

ENUMERATION

- Enumeration belongs to the first phase of Ethical Hacking, i.e., "Information Gathering".
- This is a process where the attacker establishes an active connection with the victim and try to discover as much attack vectors as possible, which can be used to exploit the systems further.
- Enumeration can be used to gain information on –
    - Network shares
    - SNMP data, if they are not secured properly
    - IP tables
    - Usernames of different systems
    - Passwords policies lists

Enumerations depend on the services that the systems offer. They can be −

- DNS enumeration
- NTP enumeration
- SNMP enumeration
- Linux/Windows enumeration
- SMB enumeration

SCANNING

- In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.

SNIFFING

- Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools.
- It is a form of "tapping phone wires" and get to know about the conversation. It is also called wiretapping applied to the computer networks.
- There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.
- In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

The following sensitive information can be sniffed from a network −

- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

HOW THE SNIFFER WORKS

- A sniffer normally turns the NIC of the system to the promiscuous mode so that it listens to all the data transmitted on its segment.
- Promiscuous mode is a unique way of Ethernet hardware (network interface cards - NICs) that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC.
- By default, a NIC ignores all traffic that is not addressed to it. Non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.

SNIFFING NETWORKS

- A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

- Types of Sniffing
- Sniffing can be either Active or Passive in nature.

PASSIVE SNIFFING

- In passive sniffing, the traffic is locked but it is not altered in any way.
- Passive sniffing allows listening only. It works with Hub devices.
- On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic.
- Therefore, an attacker can easily capture traffic going through.
- The good news is that hubs are almost obsolete nowadays. Most modern networks use switches.
- Hence, passive sniffing is no more effective.

ACTIVE SNIFFING

- In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack.
- Active sniffing is used to sniff a switch-based network.
- It involves injecting address resolution packets (ARP) into a target network to flood on the switch content addressable memory (CAM) table. CAM keeps track of which host is connected to which port.

Following are the Active Sniffing Techniques –

- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Spoofing Attacks
- ARP Poisoning

END OF UNIT II