MARWADI EDUCATION FOUNDATION'S GROUP OF INSTITUTIONS
FACULTY OF ENGINEERING
DEPARTMENT OF INFORMATION TECHNOLOGY

Assignment-1

1) Explain the meaning of System Vulnerability in brief.

Ans:

A computer vulnerability is a cybersecurity term that refers to a defect in a system that can leave it open to attack. This vulnerability could also refer to any type of weakness present in a computer itself, in a set of procedures, or in anything that allows information security to be exposed to a threat.

It is possible for network personnel and computer users to protect computers from vulnerabilities by regularly updating software security patches. These patches are capable of solving flaws or security holes found in the initial release. Network personnel and computer users should also stay informed about current vulnerabilities in the software they use and look out for ways to protect against them.

Common Computer Security Vulnerabilities

The most common computer vulnerabilities include:

- Bugs
- Weak passwords
- Software that is already infected with virus
- Missing data encryption
- OS command injection
- SQL injection
- Buffer overflow
- Missing authorization
- Use of broken algorithms
- URL redirection to untrusted sites
- Path traversal
- Missing authentication for critical function
- Unrestricted upload of dangerous file types
- Dependence on untrusted inputs in a security decision
- Cross-site scripting and forgery
- Download of codes without integrity

2) Define the term Probe, show different ways to acquire traffic probe.

Ans:

Probe: a probe is an attempt to gain access to a computer and its files through a known or probable weak point in the computer system.

Port Scanning: is the name for the technique used to identify open ports and services available on a network host. It is sometimes utilized by security technicians to audit computers for vulnerabilities; however, it is also used by hackers to target victims.

Enumeration: is defined as the process of extracting user names, machine names, network resources, shares and services from a system. In this phase, the attacker creates an active connection to the system and performs directed queries to gain more information about the target. The gathered information is used to identify the vulnerabilities or weak points in system security and tries to exploit in the System gaining phase.

Vulnerability: assessment is the testing process used to identify and assign severity levels to as many security defects as possible in a given timeframe. This process may involve automated and manual techniques with varying degrees of rigor and an emphasis on comprehensive coverage. Using a risk-based approach, vulnerability assessments may target different layers of technology, the most common being host-, network-, and application-layer assessments.

3) Explain Netcat tools and its function.

Ans:

Netcat is a tool capable of writing data across a network using TCP or UDP protocol but this simple capability allows it to perform many functionalities. Its capability to create almost any kind of connection makes it a simple and efficient network debugging and exploration tool. It has been built in such a manner that it can act as a client as well as a server, which elevates its utility to a higher level.

Netcat provides the following functionalities that can be useful for a hacker/pentester or a network admin:

- Chatting
- Port Scanning
- Banner Grabbing
- Port Redirection/Proxying

- File Transfer
- Honeypot
- RAT/Backdoor

Before describing Netcat functionalities in detail, some terms need to be explained briefly:

Port Scanning: The act of systematically scanning a host for open ports. Once determined, these open ports can be utilized to gain access to the host or to launch an attack.

Banner Grabbing: A fingerprinting technique aimed at extract information about a host such as operating system, web server, applications etc. A simple form of banner grabbing is to send a request and analyze the response received.

Port Redirection: A simple technique used to transfer traffic from one port to another. It is utilized to access services which are restricted in any specific environment.

Honeypot: A Honeypot is a monitored decoy used to attract attackers away from critical resources and also a tool to analyze an attacker's methods and characteristics. It can emulate various services provided by an OS and also generate responses for those services. It provides an environment which is capable of interacting with an attacker and monitors his/her activities without any real resources at risk.

First of all let's see all the options provided by Netcat:

root@bt:~# nc -h

[v1.10-38]

connect to somewhere: nc [-options] hostname port[s] [ports] …

listen for inbound: nc -l -p port [-options] [hostname] [port]

options:

-c shell commands	as `-e'; use /bin/sh to exec [dangerous!!]
-e filename	program to exec after connect [dangerous!!]
-b	allow broadcasts
-g gateway	source-routing hop point[s], up to 8
-G num	source-routing pointer: 4, 8, 12, …
-h	this cruft
-i secs	delay interval for lines sent, ports scanned
-k	set keepalive option on socket

-l	listen mode, for inbound connects
-n	numeric-only IP addresses, no DNS
-o file	hex dump of traffic
-p port	local port number
-r	randomize local and remote ports
-q secs	quit after EOF on stdin and delay of secs
-s addr	local source address
-T tos	set Type Of Service
-t	-t answer TELNET negotiation
-u	UDP mode
-v	-v verbose [use twice to be more verbose]
-w secs	timeout for connects and final net reads
-z	zero-I/O mode [used for scanning]

port numbers can be individual or ranges: lo-hi [inclusive]; hyphens in port names must be backslash escaped (e.g. 'ftp-data').

Let's now dive into the details of Netcat as a tool.

Chatting: Netcat can be used for the purpose of chatting from one system to another.

4) List down some Linux Command and explain each command in detail.

Ans :

Here is a list of basic Linux commands:

1. pwd command
Use the pwd command to find out the path of the current working directory (folder) you're in. The command will return an absolute (full) path, which is basically a path of all the directories that starts with a forward slash (/). An example of an absolute path is /home/username.

2. cd command
To navigate through the Linux files and directories, use the cd command. It requires either the full path or the name of the directory, depending on the current working directory that you're in.

Let's say you're in /home/username/Documents and you want to go to Photos, a subdirectory of Documents. To do so, simply type the following command: cd Photos.

Another scenario is if you want to switch to a completely new directory, for example,/home/username/Movies. In this case, you have to type cd followed by the directory's absolute path: cd /home/username/Movies.

There are some shortcuts to help you navigate quickly:

- cd .. (with two dots) to move one directory up
- cd to go straight to the home folder
- cd- (with a hyphen) to move to your previous directory

On a side note, Linux's shell is case sensitive. So, you have to type the name's directory exactly as it is.

3. ls command
The ls command is used to view the contents of a directory. By default, this command will display the contents of your current working directory.

If you want to see the content of other directories, type ls and then the directory's path. For example, enter ls /home/username/Documents to view the content of Documents.

There are variations you can use with the ls command:

- ls -R will list all the files in the sub-directories as well
- ls -a will show the hidden files
- ls -al will list the files and directories with detailed information like the permissions, size, owner, etc.

4. cat command
cat (short for concatenate) is one of the most frequently used commands in Linux. It is used to list the contents of a file on the standard output (sdout). To run this command, type cat followed by the file's name and its extension. For instance: cat file.txt.

Here are other ways to use the cat command:

- cat > filename creates a new file
- cat filename1 filename2>filename3 joins two files (1 and 2) and stores the output of them in a new file (3)
- to convert a file to upper or lower case use, cat filename | tr a-z A-Z >output.txt

5. cp command
Use the cp command to copy files from the current directory to a different directory. For instance, the command cp scenery.jpg /home/username/Pictures would create a copy of scenery.jpg (from your current directory) into the Pictures directory.

6. mv command
The primary use of the mv command is to move files, although it can also be used to rename files.

The arguments in mv are similar to the cp command. You need to type mv, the file's name, and the destination's directory. For example: mv file.txt /home/username/Documents.

To rename files, the Linux command is mv oldname.ext newname.ext

7. mkdir command
Use mkdir command to make a new directory — if you type mkdir Music it will create a directory called Music.

There are extra mkdir commands as well:

- To generate a new directory inside another directory, use this Linux basic command mkdir Music/Newfile
- use the p (parents) option to create a directory in between two existing directories. For example, mkdir -p Music/2020/Newfile will create the new "2020" file.

8. rmdir command
If you need to delete a directory, use the rmdir command. However, rmdir only allows you to delete empty directories.

9. rm command
The rm command is used to delete directories and the contents within them. If you only want to delete the directory — as an alternative to rmdir — use rm -r.

Note: Be very careful with this command and double-check which directory you are in. This will delete everything and there is no undo.

5) Define the term ports and its importance in Cybersecurity.

Ans When referring to a physical device, a hardware port or peripheral port is a hole or connection found on the front or back of a computer. Ports allow computers to access external devices such as printers. Below is a short listing of the different computer ports you may find on a computer. The picture shows an example of a type of port on the back of a computer.

2. In addition to the hardware port mentioned above, a hardware port or port may also refer to a computer memory I/O port. See our I/O port definition for further information on this term.

3. A port is a term used to describe the process of taking a program that has been written for specific operating systems and moving it to another operating system. For example, taking a program written for Microsoft Windows and moving it to Linux.

4. When referring to a network or the Internet, a software or network port is a location where information is sent. For example, port 80 is the http network port. A listing of commonly known and used ports can also be found on the below listing. Users running Microsoft Windows can utilize the netstat command to view currently active connections that include ports currently being used.

   Users who want to block ports on their computer or network can use a software or hardware firewall. If you cannot get access to a particular port it's likely that a firewall is already present on the Network or other network settings set by the administrators have been set up.

6) Explain OSI Layer with function of each layer.

Ans :

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:

- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The

physical layer is mainly responsible for placing the information on the physical medium.

Functions of the OSI Layers

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Physical layer

- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- **Topology:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.

Data-Link Layer

- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.

- It contains two sub-layers:
  - **Logical Link Control Layer**
    - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
    - It identifies the address of the network layer protocol from the header.
    - It also provides flow control.
  - **Media Access Control Layer**
    - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
    - It is used for transferring the packets over the network.

Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

Network Layer

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.

- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Transport Layer

- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.
  - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer:

- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation Layer

- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

Application Layer

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Functions of Application layer:

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

7) Explain the difference between vulnerability scanning and penetration testing.

Ans:

When people misunderstand the differences between penetration testing and vulnerability scans, they are often missing a vital component in their overall network security profile and both are crucial for cybercrime prevention.

Vulnerability scans and vulnerability assessments search systems for known vulnerabilities. A penetration test attempts to actively exploit weaknesses in an environment. While a vulnerability scan can be automated, a penetration test requires various levels of expertise.

Regular vulnerability scanning is necessary for maintaining information security. Secureworks incident response (IR) analysts have observed some clients performing vulnerability scans weekly and others not performing these vital scans at all. Secureworks analysts recommend scanning every new piece of equipment before it is deployed and at least quarterly afterwards. Any changes to the equipment should immediately be followed by another vulnerability scan. The scan will detect issues such as missing patches and outdated protocols, certificates, and services.

Organizations should maintain baseline reports on key equipment and should investigate changes in open ports or added services. A vulnerability scanner (e.g., Nessus, GFI LANGuard, Rapid7, Retina, Qualys) can alert network defenders when unauthorized changes are made to the environment. Reconciling detected changes against change-control records can help determine if the change was authorized or if there is a problem such as a malware infection or a staff member violating change-control policies.

Penetration testing is quite different, as it attempts to identify insecure business processes, lax security settings, or other weaknesses that a threat actor could exploit. Transmission of unencrypted passwords, password reuse, and forgotten databases storing valid user credentials are examples of issues that can be discovered by a penetration test. Penetration tests do not need to be conducted as often as vulnerability scans but should be repeated on a regular basis.

Penetration tests are best conducted by a third-party vendor rather than internal staff to provide an objective view of the network environment and avoid conflicts of interest. Various tools are used in a penetration test, but the effectiveness of this type of test relies on the tester. The tester should have a breadth and depth of experience in information technology, preferably in the organization's area of business; an ability to think abstractly and attempt to anticipate threat actor behaviors; the focus to be thorough and comprehensive; and a willingness to show how and why an organization's environment could be compromised.

A penetration test report should be short and to the point. It can have appendices listing specific details, but the main body of the report should focus on what data was compromised and how. To be useful for the customer, the report should describe the actual method of attack and exploit, the value of the exploited data, and recommendations for improving the organization's security posture.

Table 1 lists the differences between vulnerability scans and penetration tests.

	Vulnerability scan	Penetration test
Frequency	At least quarterly, especially after new equipment is loaded or the network undergoes significant changes	Once or twice a year, as well as anytime the Internet-facing equipment undergoes significant changes
Reports	Provide a comprehensive baseline of what vulnerabilities exist and what changed since the last report	Concisely identify what data was compromised
Focus	Lists known software vulnerabilities that could be exploited	Discovers unknown and exploitable weaknesses in normal business processes
Performed by	Typically conducted by in-house staff using authenticated credentials; does not require a high skill level	Best to use an independent outside service and alternate between two or three; requires a great deal of skill
Value	Detects when equipment could be compromised	Identifies and reduces weaknesses

Table 1. Comparison of vulnerability scans versus penetration tests.

Vulnerability scanning and penetration testing are both critical to a comprehensive security strategy. They are powerful tools to monitor and improve an organization's network environment.

8) Explain different types of Hackers available in cyber domain.

Ans:

1. White Hat Hackers

White hat hackers or ethical hackers are known to many of us for their ethical behavior. They are the cybersecurity experts who are hired by government and private organizations to hack their systems and surface the vulnerabilities most ethically. Ethical hackers penetrate and identify loopholes to protect the IT infrastructure from other malicious cyber attackers.

In short, these are the right people who hack your system intending to find vulnerabilities and help you in protecting it from malware or other types of attacks.

2. Black Hat Hacker

Black hat hackers are the real culprits that we should be worried about. Whenever you hear about an incident, remember that a black hat hacker is behind it.

These attackers are inspired mostly by monetary benefit or other criminal intention. They usually target financial institutions, healthcare, or businesses where they can reach the crucial personal information. These hackers also intrude the personal computers of individuals to access personal business and financial information.

3. Gray Hat Hackers

Gray hat hackers stand in the mid of white hat and black hat hackers. Though they may not use the hacked information for personal gains, however, their act is backed by both good as well as bad intentions.

For example, a gray hat hacker intrudes an organization's infrastructure and leaks the vulnerability over the internet or informs this to the management, to prove his hacking skills or to ruin the brand image.

A gray hat hacker does not take any information from the victim organization while intruding their network. That means he is not a white hat hacker. Neither he holds any legal authorization to hack the organization's infrastructure to consider him like a black hat hacker either.

In brief, a gray hat hacker is someone who hacks without ethical permissions but does not use the compromised data for any benefit.

4. Script Kiddies

An amateur hacker who has no good coding skills usually download ready tools or uses available hacking codes from other developers and hackers to impress their friends or gain attention.

Script Kiddies don't care about learning the hacking script seriously. They launch an attack without bothering about its quality by using off-the-shelf codes and tools. The most common cyberattacks by script kiddies would include DoS and DDoS attacks.

5. Green Hat Hackers

Green hat hackers are similar to Script Kiddies, but they have the curiosity to learn to code to hack. They often join and follow online hacking communities and gets into a potential discussion with fellow hackers. They are amateurs with a passion for learning more about the hacking trade. They will always be loaded with a lot of curious questions and will seek replies like a pro.

6. Blue Hat Hackers

Blue Hat Hackers are also similar to Script Kiddies who are a novice with an agenda to take revenge on personal reasons. They don't have any willingness to grow as a hacker and learn to script. Their attacks can be as simple as flooding IP by sending an overloaded packet, which will result in DoS attacks.

Any script kiddie with a revengeful motive can be considered as a blue hat hacker.

7. Red Hat Hackers

Red hat hackers are similar to white hat hackers in a way that their acts are meant to restrict the actions of black hat hackers. However, they are ruthless, and that is what makes them different from other hackers.

They are aggressive by nature and thus launches a series of attacks on the hacker that may force the hacker to replace the entire system. Red hat hackers believe in taking down the black hat hacker instead of reporting a malicious attack.

8. State/ Nation Sponsored Hackers

These hackers are hired by the state or national government to snoop in and penetrate other country's IT infrastructure. A respective government executes hacking with complete security to gain confidential information related to targeted government.

This is done either to retrieve sensitive information or to demonstrate the vulnerabilities of the victim nation. The hacking government allocates an unlimited budget and applies extremely advanced tools while targeting companies, individuals, or agencies of rival countries.

9. Hacktivist

Hacktivist is an online version of an activist. Like a social activist propagandized a social, political, or religious agenda, hacktivist does the same online. Hacktivists believe that they can bring social changes by opposing the acts of government. They hack government and organizations information to express their disapproval against any movement.

10. Malicious Insider or Whistleblower

A whistleblower or a malicious hacker is a strategic employee who either operates individually or has been compromised by rivals to garner trade secrets. This is often done by competitor agencies to retrieve trade information and stay ahead in the competition. These hackers can benefit rivals as they are aware of the entire system.