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

Assignment-2

1) **Explain Firewall and how it defences our system.**

Ans :

A firewall is hardware or software (or both) security system that acts as your computer's or your application's first line of defense by screening out hackers, viruses, worms, and malware that try to reach your computer through network traffic — or over the Internet.

Quite simply put, a firewall protects your computer from intrusion (scanning or attack) by hackers while it is connected to the Internet. A firewall examines electronic data coming in or out of a computer (or network) and compares it to the rules it has been given. If the data matches the rules, it's allowed to pass.

You can think of a firewall as a piece of software that keeps the bad guys out and lets the good ones in.

Research shows that an unprotected computer system will come under attack within the first 15 minutes of Internet use. This is why it's so important that you have security software installed on your PC before you connect to the Internet.

If your computer is new and has no internet security software installed, we recommend you download and install such software along with all necessary Windows updates and patches needed to make it secure before starting to browse the Internet.

2) **Explain different types of firewall – stateful and stateless.**

Ans:

Stateless firewalls are designed to protect networks based on static information such as source and destination. Whereas stateful firewalls filter packets based on the full context of a given network connection, stateless firewalls filter packets based on the individual packets themselves.

To do so, stateless firewalls use packet filtering rules that specify certain match conditions. If match conditions are met, stateless firewall filters will then use a set of preapproved actions to guide packets into the network. If match conditions are not met, unidentified or malicious packets will be blocked.

Because stateless firewalls do not take as much into account as stateful firewalls, they're generally considered to be less rigorous. For example, stateless firewalls can't consider the overall pattern of incoming packets, which could be useful when it comes to blocking larger attacks happening beyond the individual packet level.

3) **Describe the working of Network Address Translation (NAT).**

Ans:

It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

As part of this capability, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address. NAT offers the dual functions of security and address conservation and is typically implemented in remote-access environments.

Basically, NAT allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network.

In order to configure traditional NAT, you need to make at least one interface on a router (NAT outside) and another interface on the router (NAT inside) and a set of rules for translating the IP addresses in the packet headers (and payloads if desired) need to be configured. In order to configure Nat Virtual Interface (NVI), you need at least one interface configured with NAT enable along with the same set of rules as mentioned above.

4) **Explain Intrusion Detection System (IDS).**

Ans:

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notifications.

5) **Describe Web Vulnerability in your own Words.**

Ans: In cyber security, a vulnerability is a weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries (i.e. perform unauthorized actions) within a computer system. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerabilities are also known as the attack surface.

Vulnerability management is the cyclical practice that varies in theory but contains common processes which include: discover all assets, prioritize assets, assess or perform a complete vulnerability scan, report on results, remediate vulnerabilities, verify remediation - repeat. This practice generally refers to software vulnerabilities in computing systems.

A security risk is often incorrectly classified as a vulnerability. The use of vulnerability with the same meaning of risk can lead to confusion. The risk is the potential of a significant impact resulting from the exploit of a vulnerability. Then there are vulnerabilities without risk: for example, when the affected asset has no value. A vulnerability with one or more known instances of working and fully implemented attacks is classified as an exploitable vulnerability—a vulnerability for which an exploit exists. The window of vulnerability is the time from when the security hole was introduced or manifested in deployed software, to when access was removed, a security fix was available/deployed, or the attacker was disabled—see zero-day attack.

Security bug (security defect) is a narrower concept. There are vulnerabilities that are not related to software: hardware, site, personnel vulnerabilities are examples of vulnerabilities that are not software security bugs.

6) Explain the use of Curl and OpenSSL Command.

Ans:

Curl:

- Curl is a command line tool to transfer data to or from a server, using any of the supported protocols (HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP or FILE). curl is powered by Libcurl. This tool is preferred for automation, since it is designed to work without user interaction. curl can transfer multiple file at once.
- **Syntax:** curl [options] [URL...]

OpenSSL:

- OpenSSL is an open-source command line tool that is commonly used to generate private keys, create CSRs, install your SSL/TLS certificate, and identify certificate information.
- **Syntax:** openssl version -a

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

Ans:

John the Ripper works by using the dictionary method favored by attackers as the easiest way to guess a password. It takes text string samples from a word list using common dictionary words. It can also deal with encrypted passwords, and address online and offline attacks.

Password crackers and cryptanalysis tools typically work in three different ways. The common objective in all these is ultimately to correctly guess ("crack") a password:

- **Dictionary attack:** In this type of attack the tool tries passwords provided in a pre-fed list of large number of words, phrases and possible passwords derived from previously leaked data dumps or breaches. The tool enters every single password in the application from the list, in an attempt to find the correct one.

- **Brute-force attack:** In this type of attack, the tool asks the user to configure a few settings, for example, the minimum and maximum lengths the correct password may fall into and what types of characters it could possibly consist of (e.g., letters only, letters and numbers, or special characters) and at what positions (say, for every password it generates, first four would be alphabets followed by two digits and two special characters). It takes a bit of guesswork and expertise to find the ideal brute-forcing configuration. The tool then guesses every combination of password possible within this range and specified by the criteria.

- On a successful match, user is notified of the correct password. The process can be effective but excruciatingly slow. For example, a nine-character password comprising a mix of upper- and lowercase letters along with digits and special characters will take over nine years to be guessed by a computer, making it virtually uncrackable. This is why you hear security professionals suggest all the time to choose a long and complex password that consists of a combination of different character types.

- **Rainbow tables:** Because mission-critical and security-oriented applications seldom store passwords in plaintext and instead store their fixed-length hashes, rainbow tables can be efficient especially if a large list of hashed passwords is available (for example, from a leaked data dump). In this case,

a pre-computed list of password hashes (derived from commonly set passwords) is compared against an existing data dump to find the correct password in its plaintext form. Using rainbow tables is faster than brute-forcing as the hashed data is precalculated.

A rainbow table will be ineffective when password hashes are salted and salt values are too large, all of which increases the overall complexity. That is also why salting is used a security defense in addition to storing hashed user passwords in databases. Salting when done correctly ensures even if a password database is leaked, it would be virtually impossible for a hacker to reverse user passwords to their original plaintext form.

8) What is SAM (security account manager) file, how it is important to the system.

Ans:

The Security Accounts Manager (SAM) is a database in the Windows operating system (OS) that contains user names and passwords. SAM is part of the registry and can be found on the hard disk.

In the SAM, each user account can be assigned a local area network (LAN) password and a Windows password. Both are encrypted. If someone attempts to log on to the system and the user name and associated passwords match an entry in the SAM, a sequence of events takes place ultimately allowing that person access to the system. If the user name or passwords do not properly match any entry in the SAM, an error message is returned requesting that the information be entered again.

In personal computers (PCs) not connected into a LAN and for which there is only one user, Windows asks for only one password when the system is booted up. This function can be disabled if the user does not want to enter authentication data every time the computer is switched on or restarted. The main purpose of the SAM in a PC environment is to make it difficult for a thief to access the data on a stolen machine. It can also provide some measure of security against online hackers.

In a domain-joined computer, there can be two types of logons: a local logon (that is handled by the SAM as described above) and a domain user logon using the Active Directory (AD) database with the WinLogon service. However, when a user logs on to a computer as a local user, the user will not be able to access the network resources. A Windows server that has been promoted to a DC will use the AD database instead of the SAM to store data. The only instance it will use the SAM would be to boot into DSRM for performing maintenance operations. This is because the DSRM administrator password is stored locally in the SAM and not in AD.

To put it simply, be it a domain-joined computer or a standalone computer, local logon can occur only through the SAM.