Department of Artificial Intelligence and Data Science

TE-AI&DS- CYBER SECURITY

Unit-5

[MAY-2024]

Q**1) Differentiate packet filtering router and stateful Inspection firewall. [6]**

[MAY-2024]

Ans –

	Stateless Packet Filtering Firewalls	**Stateful Packet Filtering Firewalls**
1.	The stateless firewalls are designed to protect networks based on static information such as source and destination.	Stateful firewalls filter packets based on the full context of the connection.
2.	It uses some predefined packet filtering rules, the packets are judged based on that, if it conforms to the predefined rules then it is considered to be "safe" and allowed to pass through. If the conditions are not met, the packet is considered to be "unidentified" or "malicious" and it will be blocked.	It uses the concept of a state table where it stores the state of legitimate connections. Stateless firewall filters are only based on header information in a packet but stateful firewall filter inspects everything inside data packets, the characteristics of the data, and its channels of communication.
3.	Less secure than stateless firewalls.	Stateful firewalls are more secure.
4.	Cheaper or cost-efficient.	Expensive as compared to stateless firewall
5.	Faster than Stateful packet filtering firewall.	Slower in speed when compared to Stateless firewall.
6.	For small businesses, a stateless firewall could be a better option, as they face fewer threats and also have a limited budget in hand.	For larger enterprises, a stateful firewall would be a smarter option, as they have larger outgoing traffic that needs monitoring and enough money to afford it. Stateful firewalls offer dynamic packet filtering, so they can provide a thick security layer to mitigate attacks.

Q.2) What is trusted system? Explain in brief. [6]

[MAY-2024]

Ans- A trusted system is a computer system or network that has been designed, implemented, and tested to meet specific security requirements. Trusted systems are used to protect sensitive information, prevent unauthorized access, and ensure the integrity and availability of data and systems.

A trusted system is typically designed with a set of security features, such as access controls, authentication mechanisms, and encryption algorithms, that are carefully integrated to provide a comprehensive security solution. These security features are often implemented using hardware, software, or a combination of both, and are rigorously tested to ensure they meet the security requirements of the system.

Trusted systems are often used in government, military, financial, and other high-security environments where the protection of sensitive information is critical. They are also used in commercial settings where the protection of intellectual property, trade secrets, and other confidential information is important.

Overall, a trusted system is one that can be relied upon to provide a high level of security and protection against various types of cyber threats, including malware, hacking, and other forms of cyber attacks.

Trusted systems are designed with a set of security principles and practices that are used to build a system that can be trusted to operate securely. These principles include the following:

1. **Least Privilege:** Trusted systems are designed to provide users with the minimum level of access necessary to perform their tasks. This principle ensures that users cannot accidentally or intentionally access information or resources they are not authorized to use.
2. **Defense in Depth:** Trusted systems implement multiple layers of security controls to protect against threats. This principle involves using a combination of physical, technical, and administrative controls to create a comprehensive security solution.
3. **Integrity:** Trusted systems ensure that data and systems are not modified or altered in an unauthorized manner. This principle ensures that data remains accurate and trustworthy over time.
4. **Confidentiality:** Trusted systems protect sensitive information from unauthorized access. This principle ensures that sensitive data remains private and confidential.
5. **Availability:** Trusted systems ensure that systems and data are available to authorized users when needed. This principle ensures that critical information and systems are accessible and operational at all times.

Q.3) List limitations of Firewall. [5] [MAY-2024]

Ans –

1. User Restriction

It is an undisputed fact that a firewall secures the system from unauthorized access, but the firewall is more advantageous to the single user but ineffective for the organization. It damages the organization's productivity and forces the employees to undertake shortcuts, which can lead to serious compromises with security. Employees are not permitted to perform a certain function that is not part of the policies used by the firewall.

2. Cost

Firewall cost depends upon the type of installation. Hardware Firewall is more expensive than software firewalls because for the installation, hardware firewall requires an expert IT professional, and its maintenance is also costly. On another side, an average user can install software firewalls easily.

3. Complex Operations

It becomes very difficult for a large organization to bear the huge maintenance cost of the firewall. A firewall is very efficient in individual cases. A separate team has to be constituted for the firewall's operation and to ensure the other networks remain secure from intrusion. It gives rise to an additional financial burden on the organization.

4. Malware Attack

A firewall secures the system from the simple type of trojans. It cannot secure the system from sophisticated malware that can enter the system in the form of trusted data. This requires installing powerful, sophisticated, and effective anti-malware for quick action.

5. Effect on the Performance

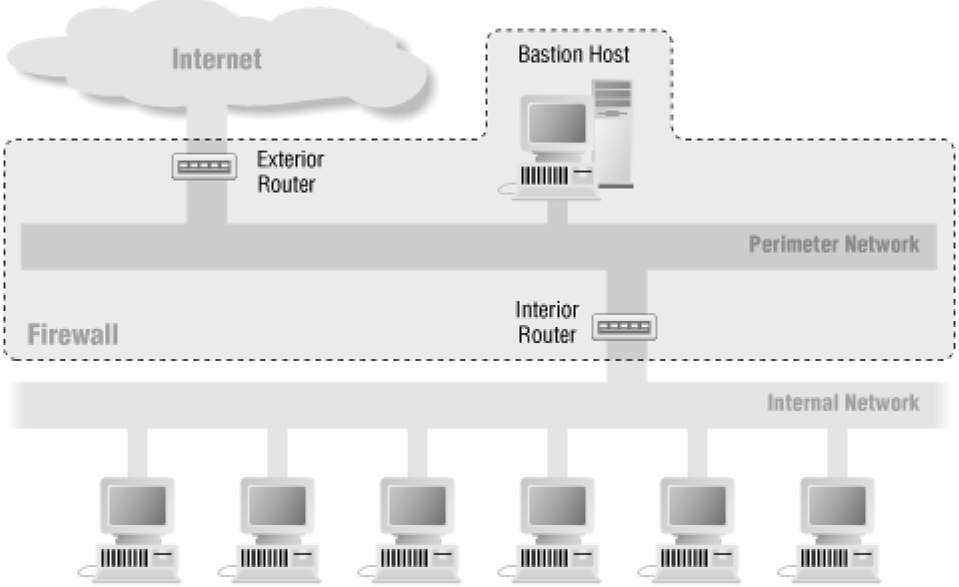
The computer system's performance is affected by the usage of software firewalls. It is a known fact that the RAM (Random Access Memory) and processing power have a vital and important role in giving a good performance, but when a firewall runs in the background, it draws more power from the RAM and processing power. This has an overall impact on the performance of the system. Hardware firewalls are independent of the computer system, and therefore, they do not utilize the computer devices; hence the performance of the system remains unaffected.

OR

Q 4) What is Digital Signature Standard? Explain the DSS approach. [6] [MAY-2024]

Ans-

The screened subnet architecture adds an extra layer of security to the screened host architecture by adding a perimeter network that further isolates the internal network from the Internet. Why do this? By their nature, bastion hosts are the most vulnerable machines on your network. Despite your best efforts to protect them, they are the machines most likely to be attacked because they're the machines that can be attacked. If, as in a screened host architecture, your internal network is wide open to attack from your bastion host, then your bastion host is a very tempting target. No other defenses are between it and your other internal machines (besides whatever host security they may have, which is usually very little). If someone successfully breaks into the bastion host in a screened host architecture, that intruder has hit the jackpot. By isolating the bastion host on a perimeter network, you can reduce the impact of a break-in on the bastion host. It is no longer an instantaneous jackpot; it gives an intruder some access but not all. With the simplest type of screened subnet architecture, there are two screening routers, each connected to the perimeter net. One sits between the perimeter net and the internal network, and the other sits between the perimeter net and the external network (usually the Internet). To break into the internal network with this type of architecture, an attacker would have to get past both routers. Even if the attacker somehow broke in to the bastion host, he'd still have to get past the interior router. There is no single vulnerable point that will compromise the internal network. Figure 6-4 shows a possible firewall configuration that uses the screened subnet architecture. The next few sections describe the components in this type of architecture.



Q. 5) List and Explain types of intrusion detection system (IDS). [6] [MAY-2024]

Ans-

Classification of Intrusion Detection System(IDS)

Intrusion Detection System are classified into 5 types:

- **Network Intrusion Detection System (NIDS):** Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

- **Host Intrusion Detection System (HIDS):** Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.

- **Protocol-based Intrusion Detection System (PIDS):** Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol. As HTTPS is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

- **Application Protocol-based Intrusion Detection System (APIDS):** An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.

- **Hybrid Intrusion Detection System:** Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system. The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Q. 6) Identify and explore any two-password management practice. [5] [MAY-2024]

Ans-

A password is a secret word or phrase or code that you need to know in order to have access to a place or system. In technical terms, it is a series of letters or numbers that you must type into a computer or computer system in order to be able to use it. A password is a real-life implementation of challenge-response authentication (a set of protocols to protect digital assets and data).

Methods to Manage Password:

There are a lot of good practices that we can follow to generate a strong password and also the ways to manage them.

- **Strong and long passwords:** A minimum length of 8 to 12 characters long, also it should contain at least three different character sets (e.g., uppercase characters, lowercase characters, numbers, or symbols)
- **Password Encryption:** Using irreversible end-to-end encryption is recommended. In this way, the password remains safe even if it ends up in the hands of cybercriminals.
- **Multi-factor Authentication (MFA):** Adding some security questions and a phone number that would be used to confirm that it is indeed you who is trying to log in will enhance the security of your password.
- **Make the password pass the test:** Yes, put your password through some testing tools that you might find online in order to ensure that it falls under the strong and safe password category.
- **Avoid updating passwords frequently:** Though it is advised or even made mandatory to update or change your password as frequently as in 60 or 90 days.