Cyber Security

Assignment - 2

Vishwas Acharya
18124011600

Q. 1) What is firewall ? explain its types in detail?

Ans A firewall is a type of cyber security tool that is used to filter traffic on a network.

- Firewalls can be used to separate network from external traffic sources, internal traffic sources, or even specific applications.
- Firewalls can be software, hardware, or cloud-based, with each type of firwall having its own unique pros & cons.
- The primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through.

- These are eight-types of firewalls:

- Packet-filtering firewalls:
- It basically create a checkpoint at a traffic router or switch.
- The firewall performs a simple check of the data packets coming through th

routers - inspecting information such as the destination and origination IP address, packet type, port number, and other surface-level information without opening up the packet to inspect its contents.

- Circuit-level Gateways:
- This firewall type is meant to quickly and easily approve or deny traffic without consuming significant computing resources, circuit-level gateways work by verifying the transmission control protocol TCP handshake.
- This TCP handshake check is designed to make sure that the session the packet is from is legitimate

- Stateful Inspection Firewalls:
- These firewalls combine both packet inspection technology and TCP handshake verification to create a level of protection greater than either of the previous two architectures could provide alone.

IANT
Date
Page

- Proxy Firewalls (Application-Level Gateways/ cloud Firewalls)
- This firewalls operate at the application layers to filter incoming traffic b/w your network and the traffic source - hence, the name "application-level gateway".
- These firewalls are delivered via a cloud-based solution or another proxy device.
- The proxy firewall first establishes a connection to the source of the traffic and inspects the incoming data packet.

- Next-Generation Firewalls
- The common features of next-generation firewalls architectures include deep-packet inspection, TCP handshake checks, and surface-level packet inspection.
- Next-generation firewalls may include othe technologies as well, such as intrusion prevention system (IPSs) that work to automatically stop attacks against your network.

- Software Firewalls
- It includes any type of firewall that

is installed on a local device rather than a separate piece of hardware.
- The big benefit of a software firewall is that it's highly useful for creating defense in depth by isolating individual network endpoints from one another.

- Hardware Firewalls
- It uses a physical appliance that acts in a manner similar to a traffic router to intercept data packets and traffic requests before they're connected to the network's servers.
- Physical appliance-based firewalls from outside the network is intercepted before the company's network endpoints are exposed to risk.

- Cloud Firewalls
- It is considered as synonyms with proxy firewalls by many, since a cloud server is often used in a proxy firewall setup.

Q.26 Discuss network address Translation (NAT) in detail?

Ans - An Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and second set of address for external traffic.

- A NAT box located where the LAN meets the Internet makes all necessary IP address translations.

- NAT serves three main purposes:
  - Provides a type of firewall by hiding internal IP address
  - Enables a company to use more internal IP addresses. Since they're used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations.
  - Allows a company to combine multiple ISDN connections into a single Internet connection.

- There are two types of NAT which are explained further.

IANT
Date
Page:

- **Dynamic NAT** : It is defined as mapping of private IP address to a public IP address from a group of public IP addresses called as NAT pool.

- **Static NAT** : It is a one-to-one mapping of a private IP address to a public IP address, and is useful when a network device inside a private network needs to be accessible from internet.

- **Advantages**

- It hides the internal network's IP address
- The universal connection can flow through NAT
- NAT is transparent to the client so it allows you to support a wides range of clients.

- **Disadvantages**

- It provides minimum logging services.
- It can break certain applications, or make these applications more difficult to run.
- You must enable IP forwarding before you can use NAT to make an Internet connection.

IANT
Date
Page:

Q.3) What is port forwarding explain in detail.

Ans Port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as routes or firewall.

- Types

1) Local port forwarding:
- It is the most common type of port forwarding.
- It is used to let a user connect from the local computer to another server, i.e. forward data securely from another client application running on the same computer as a secure shell (SSH) client.
- By using local port forwarding, firewalls that block certain web pages are able to by bypassed.

IANT
Date
Page:

2) Remote port forwarding:
- This form of port forwarding enables applications on the server side of secure shell (SSH) connection to access services residing on the SSH's client side.
- To used remote port forwarding, the address of the destination server and two port numbers must be known.
- The port numbers chosen depend on which application is to be used.

3) Dynamic port forwarding:
- DPF is an on-demand method of traversing a firewall or NAT through the use of firewall pinholes.
- The goal is to enable clients to connect securely to a trusted server that acts as a intermediary for the purpose of DPF can be implemented by setting up a local application, such as SSH, as a socks proxy server, which can be used to process data transmissions through the network or over the Internet, Programs, such as web browsers.

Q.4) Discuss Intrusion Detection System in detail?

Ans An Intrusion Detection system (IDS) is a device or software application that monitors network or system activities for malicious activites or policy violations & produces reports to a management station.

- IDS Detection Types

- There is a wide array of IDS, ranging from antivirus software to tiered monitoring systems that follow the traffic of an entire network.
- The most common classifications are:

1. Network intrusion detection system (NIDS)
   - A system that analyzes incoming network traffic.

2. Host-based intrusion detection system (HIDS)
   - A system that monitors important operating system files.

IANT
Date
Page:

3. Wireless intrusion ~~de~~ prevention system (WIPS).
- Analyzes network protocol activity across the entire wireless network, looking for any untrustworthy traffic.

- These is also subset of IDS types. The most common variants are based on signature detection and anomaly detection.

- Signature-based: Signature-based IDS detects possible threats by looking for specific patterns, such a byte sequences in network traffic, or known malicious intrusion sequences used by malware.

- Anomaly-based: a newer technology designed to detect and adapt to unknown attacks, primarily due to the explosion malware.
- This detection method uses machine learning to create a defined model of trustworthy activity, and then compose new behaviour against this trust model.

Q.5] Explain packet characteristic to filter.

Ans - A packet-filtering firewall examines each packet that crosses the firewall and tests the packet according to a set of rules that you set up.
- If the packet passes the tests, it is allowed to pass.
- If it doesn't pass then it's rejected.
- Packet filtering are the least expensive type of firewall.
- As a result, it is very common firewall.
- However, it has many flaws in it ~~which~~ which a knowledgable hackers can exploit.
- So on that result, it does not make for a fully effective firewall.

- Packet filtering are very efficient :
- They hold up each inbound and outbound packet for only a few milliseconds while they look inside the to determine the destination and source ports and address.

- After these addresses and ports are determined, the packet filter quickly applies its rule & either sends the packet along or rejects it.
- In contrast, other firewall techniques have or more noticable performance overhead.

- Packet filters are almost completely transparent to users:
- The only time a user will be aware that a packet filter firewall is being used is when the firewall rejects packet
- Other firewall techniques require that clients &/or servers be specially configured to work with the firewall.

- Packet filter are inexpensive:
- Most routers include built-in packet filtering.

Q.6] Difference between firewall and packet filter?

Ans The difference between firewall & packet filters is given further.

IANT
Date
Page

- **Firewalls:**

- It is a computer connected to both public and private network, which receives and resubmits specific kinds of network requests on behalf of network clients on either the private or public network.
- It involves proxies. A proxy acts a middle-man in a network transaction. Rather that allowing a client to speak directly to a server, the proxy server receives the requests from the client, & then resubmits the requests, on behalf of the client, to the target server.
- They are not routers or address translators.
- Never does a firewall copy or forward a packet from the internal network to the external ~~no~~ network, or vice versa.
- The internal network uses private address space.

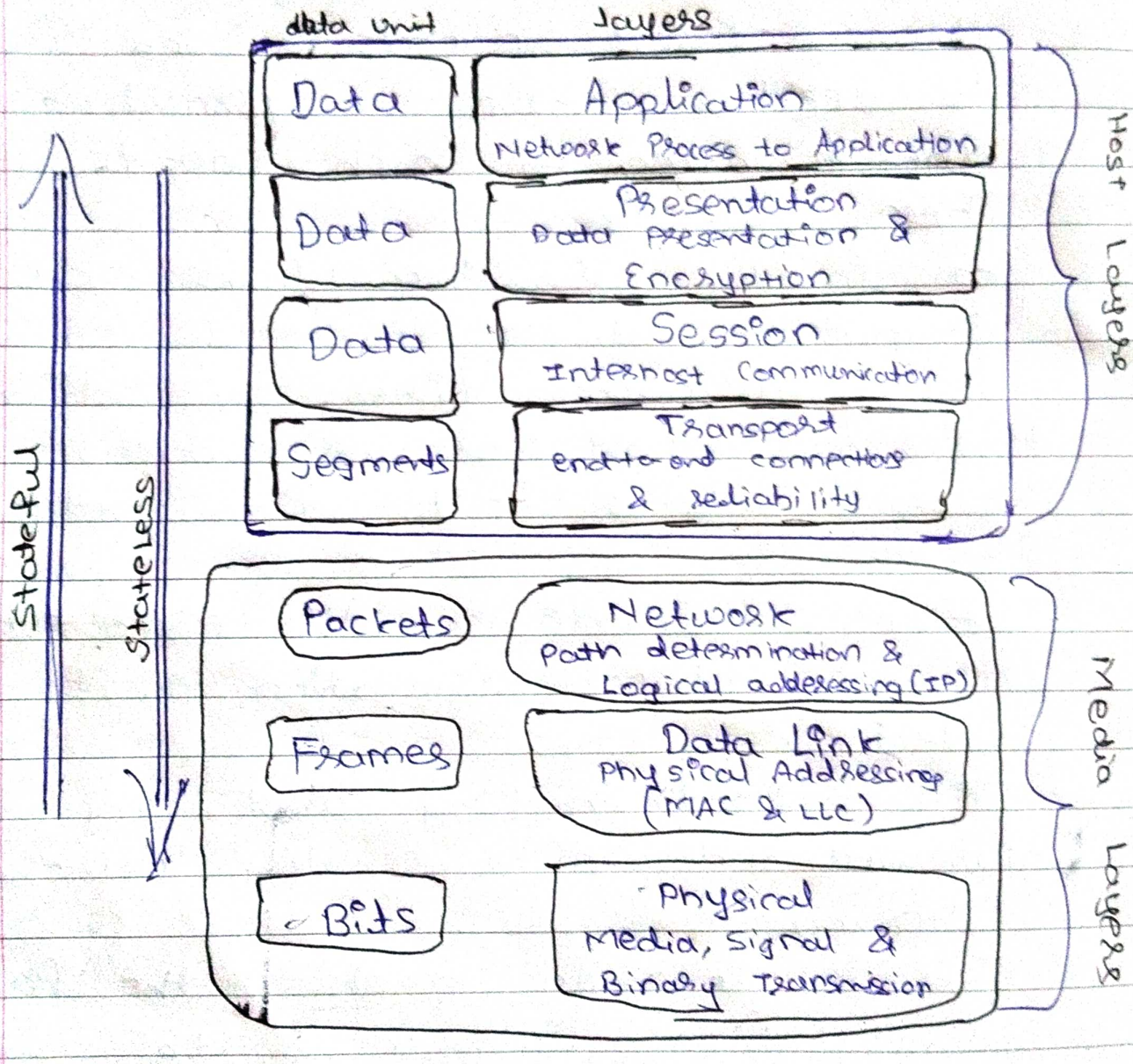
IANT
Date
Page:

- **Packet Filters:**

- It is a set of rules, applied to a stream of data packets, which is used to decide whether to permit or deny the forwarding of each packet.
- These rules are usually on a routers or in the routing layer of a computer's network protocol stack.
- Using a packet filter, an admin can dictate what types of packets are allowed into or out of a network or computer.
- Some devices, such as the Cisco PIX, combine address translation with packet filtering.
- It is worth nothing that any good firewall will also employ packet filtering.
- This is done to protect the firewall itself from intrusion & to isolate intruders from the internal work should an attacker gain control of the firewall.

Q.7] Explain stateless vs stateful firewall in detail?

Ans



- Stateless & Stateful Firewalls may sound pretty similar with being denoted with a single distinction, but they are in fact two very different approaches with diverging functions & capabilities.

IANT
Date
Page

-:- STATELESS

- These firewalls uses clues from the destination address, source and other key values to assess whether threats are present, then block or restrict those deemed untrusted.

- The purpose of stateless firewalls is to protect computer & network - specifically: routing, engine processes & resources.

- **Pros →**

- It delivers fast performance
- Heavy traffic is no match for stateless firewall.
- It has historically been cheaper to purchase although these days stateful firewall have significantly come down in price.

- **Cons →**

- It do not inspect traffic and does not examine an entire packets.
- It require some config. to arrive at a suitable level of protection.

IANT
Date
Page:

STATEFUL

- These firewall monitors all aspects of the traffic streams, their characteristics & communication channels.
- These firewalls can integrate encryption of tunnels, identity TCP connection stages, packet state & other key status updates

- **Pros →**

- These are highly skilled at detecting unauthorized attempts and forged messages
- It does not need many port to open for proper connection
- It offers extensive logging capabilities & robust attack prevention

- **Cons →**

- Man-in-the-middle attacks may pose greater vulnerabilities
- Some can be tricked to allow outside connection with an action as simple as viewing a web pages