CIS

Assignment - 2

Name: KHAGENDRA

Sec: D

Reg.No.: 219302355

Ans1) A firewall is a network security device that monitors incoming & outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

i) Packet-filtering firewall - It's one of the most basic firewall. It's used to protect internal users from the external network threats. Most routers have it built-in..

ii) Stateful inspection - It keeps track of the state of network connections and is able to hold significant attribute of each connection in memory. Those attributes collectively called the state of the connections and may include details like IP address.

iii) Application-level gateway - A WAF is to be implemented to a web server running which is hosting any type of website. It's an appliance, server plugin that applies a set of rules to HTTP connection. By customizing the rules to your application many attacks can be identified / blocked.

Ans 2) Advantages:-

- Network security: Firewalls act as barrier btw internal network and internet, preventing unauthorized access and against cyber threats.
- Access control: Firewalls allows to control which traffic is allowed in & out of network, which prevents unauthorized access to data.
- Monitoring and Logging: Firewalls provide valuable info. about network traffic, helping to identify and respond to security threats.

CIS

Assignment -2

Name: KHAGENDRA

Sec: D

Reg.No.: 219302355

Ans1) A firewall is a network security device that monitors incoming & outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

i) Packet-filtering firewall – It's one of the most basic firewall. It's used to protect internal users from the external network threats. most routers have it built-in..

ii) State-full inspection – It keeps track of the state of network connections and is able to hold significant attribute of each connection in memory. Those attributes collectively called the state of the connections and may include details like IP address.

iii) Application-level gateway – A WAF is to be implemented to a web server running which is hosting any type of website. It's an appliance, server plugin that applies a set of rules to HTTP connection. By customizing the rules to your application many attacks can be identified / blocked.

Ans 2) Advantages:–

- Network security: Firewalls act as barrier btw internal network and internet, preventing unauthorized access and against cyber thr
- Access control: Firewalls allows to control which traffic is allowed in & out of network, which prevents unauthorized access to data.
- monitoring and Logging: Firewalls provide valuable info. about network traffic, helping to identify and respond to security threats.

Disadvantages:-

- Complexity: Configuring and maintaining a firewall can be complex and require specialized knowledge.
- Single point failure: If a ~~failure~~ firewall malfunctions it can leave network vulnerable to attacks.

Ans 3) An Intrusion Detection System tracks any suspicious behaviour that might compromise network security. IDS notifies the admin of the issue, but it may not take further actions.

IDS	IPS
- Intrusion Detection System	Intrusion Prevention System
- Only alerts the network admin when it detects an intrusion	Actively blocks and drops the malicious packets before they reach the target
- Passive as it only monitors and then notify the admin	Active as it monitors as well as defend the network.
- Sends notification to user	Drops / modify malicious packet
- Low impact on network speed	High impact on network speed

Ans 4) Passwords are critical line of defence protecting our digital lives. They act as gatekeepers, controlling access to our personal information, data, financial accounts, etc common methods to breach password protections:-

- Brute-Force attack: Attackers use automated tools to systematically try every possible combination until they guess the correct one.

- Dictionary Attack: These attacks leverage lists of commonly used words, names & combinations to guess passwords.
- Social engineering: It involves tricking users into revealing their passwords. Attackers use fake website, phishing emails, etc.
- Keyloggers: These are malicious programs that record every keystroke typed on an user's device

Ans 5) Password Policies:-

- Min password length: 12 characters is effective in preventing simple brute force.
- Complexity: combination of upercase and lowercase letters, numbers and symbols.
- Expiration: Regularly changing passwords

Authentication methods:-

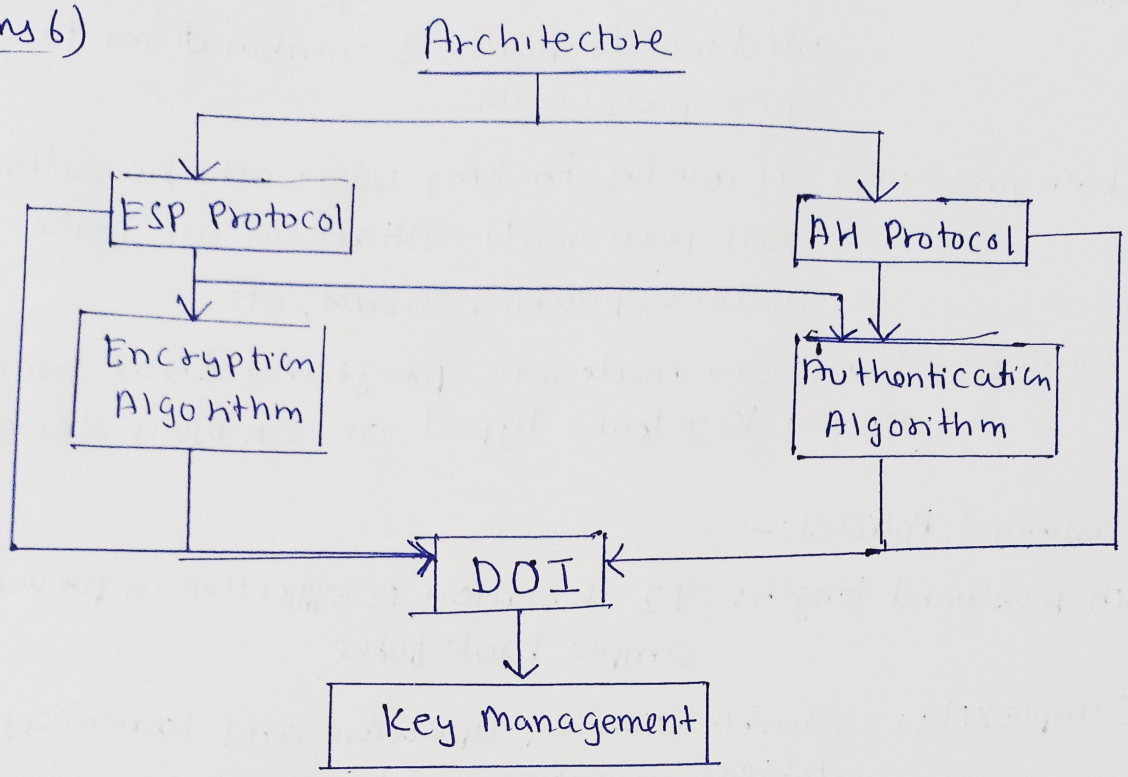
- 2FA: This adds a significant layer of security by adding a second verification factor beyond the password such as OTP sent to phone.
- Biometric Authentication: Fingerprint scanners, facial recognition offer a convenient and more secure way to authent

Effectiveness -

Password policies can improve security to an extent but they can be bypassed / cracked by complex attacks.

2FA significantly improve security compared to passwords Biometric auth. offers convenience but with trade-offs.

Ans 6)



(IP Security Architecture)

IPSec architecture uses two protocols to secure traffic or dataflow. These are i) ESP (Encapsulation Sec. Payload) and
ii) AH (Authentication Header)

It includes protocols, algo, DOI & key management which are very imp in providing a CIA.

Ans 7) IPSec relies on 2 main protocols :-

i) Authentication Header (AH) a

Function - Provides data integrity and origin authentica
for the packet header.
= Ensures data hasn't been tampered within transit and verify senders identity.

ii) Encapsulating Security Payload (ESP) :-

Function - provides data confidentiality, integrity and origin authentication for entire payload

- Encrypts the entire data portion of the packet to ensure confidentiality while also offering data integrity & sender verification.