Page No.
Date

INS Module 5.

* Network Reconnaissance

→ Testing for potential vulnerabilities in a computer network by acquiring information through information gathering.

→ Network owner/operator engaging in reconnaissance to protect the network, enforce acceptable use policies, and understand potential attack vectors.

→ Attackers using reconnaissance as a pre-cursor to external attacks, discovering and analyzing targets.

Eg. Port scanning : Using tools like Nessus and NMAP to identify open ports.

Ping sweeps: Identifying active hosts on the network.

Sniffing : Monitoring and capturing network traffic.

x x

Page No.
Date

* Motives of Reconnaissance.

① Discover IP address of hosts: Identify devices connected to the network.

② Identify accessible UDP and TCP port: Understand potential entry points.

③ Identify OS Types: Knowing the OS types helps to tailor attacks

④ Discover Active Hosts: Identify currently operational devices.

⑤ Identify Network structure: Understand how devices are interconnected.

⑥ Identify Applications and Services: Recognise running software on devices.

⑦ Discover Vulnerabilities: Uncover weaknesses that might be exploited.

* Types of Reconnaissance Attacks.

① Social Engineering: Manipulating individuals to disclose sensitive information.

Page No.
Date

* Motives of Reconnaissance.

① Discover IP address of hosts: Identify devices connected to the network.

② Identify accessible UDP and TCP port: Understand potential entry points.

③ Identify OS Types: Knowing the OS types helps to tailor attacks

④ Discover Active Hosts: Identify currently operational devices.

⑤ Identify Network structure: Understand how devices are interconnected.

⑥ Identify Applications and services: Recognise running software on devices.

⑦ Discover Vulnerabilities: Uncover weaknesses that might be exploited.

* Types of Reconnaissance Attacks.

① Social Engineering: Manipulating individuals to disclose sensitive information.

Date

② Site Reconnaissance: Gathering information by physically visiting locations.

③ Internet Reconnaissance: Collecting data from publicly available online sources.

④ Network Reconnaissance: Probing and scanning network addresses.

⑤ DNS Reconnaissance: Gathering information from the Domain Name System. (DNS):

---

* Reconnaissance Procedure.

① Information Gathering: Obtaining details about the network environment, such as website organisation, owner, location, contact person, and ~~person~~ phone number.

Tools: WHOIS lookup, DNSstuff.

② Network Mapping: Creating a blueprint of the organisation's network.

Tools: Wireshark, cheops.

③ Port Scanning: Identifying open ports that are accessible and the underlying applications

Tools: NMap, Nessus.

④ OS Detection / TCP Stack Fingerprinting: Identifying the target OS and system responses by exploiting the ambiguity in handling illegal combinations of TCP code bits.

Tools: Nmap, POF

⑤ Identifying Active Elements.: Utilizing tools such as ping, traceroutes and latency calculation to identify active elements in the network.

* Packet Sniffing.

→ Involves capturing IP data packets flowing across a computer network. It is a passive attack on ongoing conversations.

Tools: Wireshark, ngrep.

— X — X —

Date

* Types of Sniffing.

① Active Sniffing

→ Conducted on a switch.

→ The attacker floods the switch with bogus ARP requests to fill the CAM tables, forcing the switching to send network traffic to all ports.

→ This allows attacker to sniff the traffic.

→ Takes advantage of the switch's MAC address-based forwarding.

② Passive Sniffing

→ Uses hubs instead of switches.

→ Hubs operate at the physical layer, receiving network traffic on one port and retransmitting it on all other ports without knowledge of source and destination.

→ Attackers connect to the LAN, place a sniffer at the hub, and passively sniff data traffic in the network.

Page No.
Date

* Packet Snitting Techniques

* Session Hijacking

→ HTTP uses multiple TCP connections and the web server needs a method to recognize each user's connections.

→ After a successful client authentication, the web server sends a session token to the client browser.

→ The session token is composed of a string of variable width.

→ Session ID is typically stored within a cookie or URL.

→ Cookies allow the web server to identify the user and provide content accordingly

→ The cookie contains a random, non-guessable ID; no sensitive information is stored.

→ Compromising the session token to gain unauthorized access to the web server.

→ Also known as cookie stealing, hijacking, or man-in-the-middle attacki.

Date

* Procedure for Session Hijacking

① Session Sniffing: Attacker captures a valid session token using a sniffer.

→ The captured token is used for unauthorised access to the web server.

② Cross-site Script Attack: Attacker compromise the session token using malicious code or programs at the client side.

→ <SCRIPT> alert(document.cookie) </SCRIPT>

③ Session Fixation: Attacker sets a user's session ID to a known value, typically by sending a manipulated link.

→ The attacker waits for the user to log in with the fixed session ID.

④ IP Spoofing: Attacker gains unauthorised access by spoofing the IP address of a trusted host.

→ Requires obtaining the client's IP addres and injecting spoofed packets into the TCP session

Page No.
Date

⑤ Blind Attack: If unable to sniff packets, the attacker attempts to guess the correct sequence number through brute force.

→ SessionID : Name of the session.

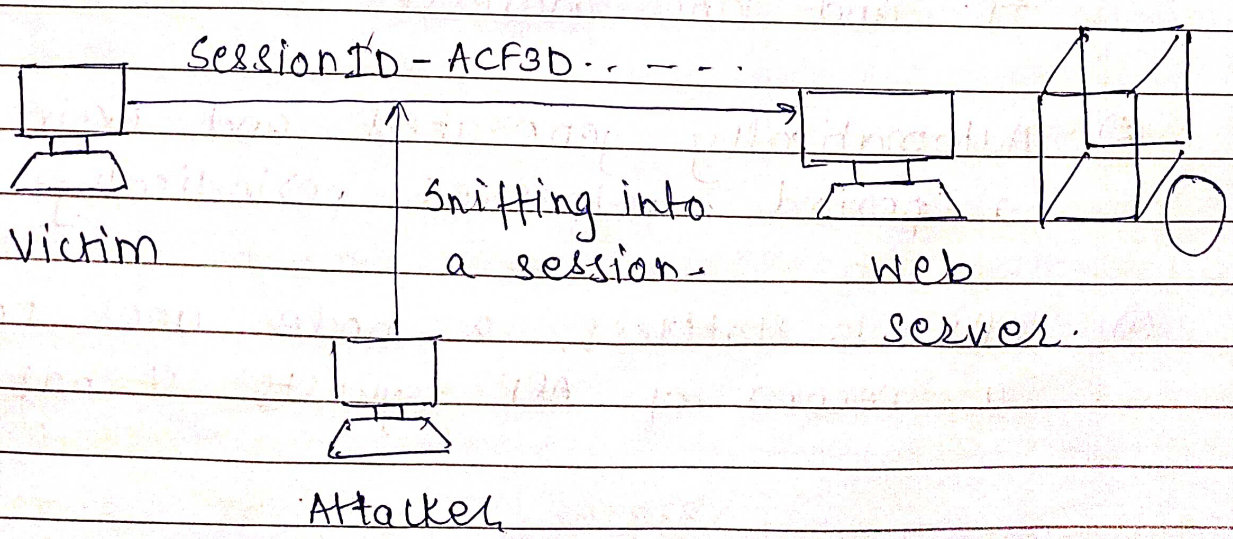
→ Sequence Number: It's a number assigned to each data packet so the receiving device knows the order used to reassemble the data.

* Mitigation.

→ Encryption of packets to prevent deciphering packet headers.

→ Encryption protocols: IPSEC, SSL, SSH etc.

→ Eg - Internet Security Protocol (IPSEC).



Page No.
Date

* ARP (Address Resolution Protocol.)

→ Stateless protocol used to find MAC address corresponding to given IP addresses in a LAN.

→ IPv4 or IPv6 is used to uniquely identify a computer or device on a network.

→ MAC addresses uniquely identify network interfaces for communication at the physical layer.

• ARP operation.

① All network devices broadcast ARP queries to find other machines MAC addresses.

② ARP table / ARP cache :- contains mappings b/w IP and MAC addresses.

③ Automatically generated and expires after a period, refreshed periodically.

④ ARP is stateless, a node does not have a record of ARP requests it has sent.

Page No.
Date

* How ARP works.

① Machine looks up its ARP table when needing to communicate with another.

② If MAC address is not found, ARP request is broadcasted on the network.

③ All machines compare IP address to MAC address.

④ Machine identifying the address responds with its IP and MAC.

⑤ Requesting computer stores the pair in its ARP table, and communication takes place

* ARP Spoofing

→ ARP Spoofing is an attack where an attacker sends forged ARP messages to clients within a LAN.

→ Process: The attacker responds to ARP requests, claiming to have the requested IPv4 addresses

→ Once the attacker's MAC is mapped to a legitimate IPv4 address, it receives data intended for that address.

Date

Objective: overload the switch with forged ARP packets.

- Consequences of ARP spoofing

① Denial of service (DoS) attacks

② Session Hijacking

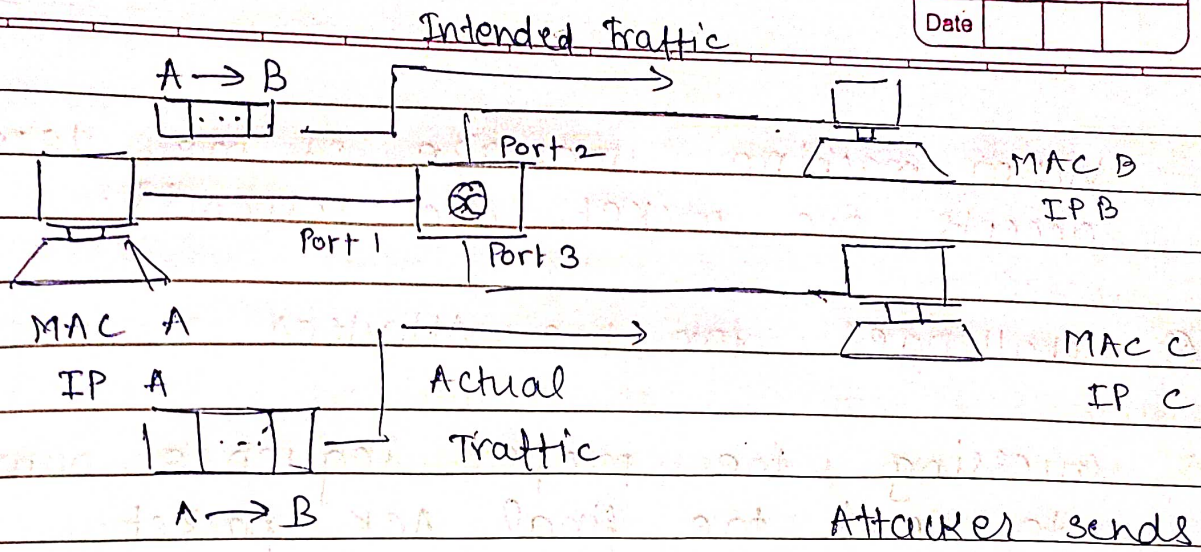
③ Man-in-the-Middle Attacks.

- Counter Measures.

① Detection Tool: Implement a dedicated tool to detect and alert on ARP spoofing attempts.

② Packet Filtering: Set up packet filtering to identify and block ARP packets that deviate from expected patterns.

③ Static ARP entries: Define static ARP entries in the local ARP cache.



Attacker sends ARP to say 'IP B' is at MAC C.

* IP Spoofing

→ IP Spoofing is a technique used by attacker to send packets with malicious content to a target machine while disguising their true identity.

→ objective: Gain unauthorised access to machine by sending messages that appear to be from a trusted source.

• Attack Process.

① Masquerading as a Trusted source:

→ Attackers send messages that appear to be from a trusted source.

→ Victim machine, unaware of the deception, accepts the packet and responds.

② challenges for the Attacker

→ Guessing the proper sequence number to send the final ACK packet.

→ Using various techniques to find the address of a trusted source.

→ Modifying packet headers to make it appear as if the packets are coming from a trusted source.

③ Connection duration.

→ If successful, the attacker may establish a connection to the victim's machine as long as it remains active.

• Countermeasures.

① Network Ingress Filtering

→ Packet filtering technique designed to prevent source address spoofing in internet traffic.

→ Aims to help prevent IP spoofing by verifying source address of incoming packets.

Page No.
Date

* DoS and DDoS

→ DoS Attack: Denial of service (DoS) Attack attempts to make a machine or network resource unavailable to its intended users by disrupting services temporarily or indefinitely.

→ DDoS Attack: Distributed DoS is a type of DoS Attack that involves multiple compromised computers attacking a targe, often coordinated by a central controller

· Attack Mechanism (DoS)

① The attacker send excessive messages requesting network or server authentication

② These messages contain invalid return addresses, making it difficult for the server to locate the attacker when sending authentication approvals.

③ The server, unable to find the return address waits before closing the connection.

Attak Process (DOS)

The attacker sends more authentication messages with invalid return addresses which keeps the server and network busy.

Effects.

Resource Exhaustion: The targetted server's resources (CPU, memory, bandwidth) are all exhausted, thus not available for legitimate users.

Altering and Destruction of configuration Information: In some cases, the attacker may attempt to alter or destroy configuration information, leading to long-term service disruption.

× ×

Page No.
Date

* Firewall:

→ A firewall is a network security device that monitors incoming and outgoing network traffic, deciding whether to allow or block specific traffic based on a defined set of security rules.

• Key characteristics:

① Protection layer:

→ Installed to protect information system, providing additional layer of security with dedicated rules.

② Vendor Diversity

→ It's recommended to use two different hardware vendors for added security against vulnerabilities in firewall code.

③ Rule-Based Traffic Matching

→ Firewalls match network traffic against defined security rules.

→ Accept, reject or drop actions are applied based on matched rule.

④ Rule components

a) Traffic source
b) Traffic Destination.
c) Service (Port, Protocol)
d) Action (Allow, Reject, Drop)

→ Firewall acts as an access control mechan b/w internal and external networks, regulati traffic in both directions.

* Types of Firewalls.

① Packet filtering

→ Layer of operation: Network Layer

→ Filtering Criteria: Source and destination IP addresses, source and destination ports, TCP flag bits.

→ Advantages: Inexpensive and efficient; process only header information.

→ Disadvantages: No state maintenance; vulnerable to IP spoofing.

Page No.
Date

② Stateful Packet filter.

→ Layer of Operation : Transport Layer.

→ Additional Capability : validates attributes of multi-packet flows (state).

→ Advantages : Maintains connection state, prevents attacks like TCP ACK SCAN.

→ Disadvantages : Cannot examine application data. Slower than packet filtering.

③ Application Proxy.

→ Layer of Operation : Application Layer.

→ Functionality : Acts as a proxy and allows data in/out of a process based on process type.

→ Advantages : Complete view of connections and application data, filters at application and transport layers.

→ Disadvantages : slower filtering speed.

* Proxy server

→ An intermediate connection b/w server on the internet and internal servers.

→ Acts as a server for incoming data to internal network clients and as a client sending data to the internet.

* Demilitarized zone (DMZ)

→ A DMZ describes a network configuration in which host servers are located. Limited connections from the internet are allowed into a DMZ.

→ Connections from the DMZ to the internal network are not usually allowed by default, protecting internal computer from compromised hosts in the DMZ.

. Key characteristics.

① Purpose

→ Provides a secure buffer zone between an external network (eg. the Internet) and the internal network.

→ Hosts in DM2 are exposed to the outside world but have limited connectivity to the internal network.

→ Hosts in the DM2 are often protected using NAT or PAT (Network Address Translation) and (Port Address Translation) to obscure the network config.

→ Implemented using a third ~~party~~ physical interface on the firewall or two firewalls in series for added protection.

· Ideal configuration

① Internal hosts can access DM2 and the Internet
② External hosts can access DM2 only.
③ DM2 hosts can access the Internet only.

* Firewall Defenses

① Systems in DM2.

→ Systems exposed to the outside world, requiring careful maintainance by administrators.

Date

② Traffic Management-

→ Amount of traffic into the internal network is relatively small.

→ Application proxy firewall is employed to manage traffic.

③ Layered security

→ Three different layers of security added with different firewalls.

* Firewall Rules in DM2.

→ DM2 is an independant network which acts as a buffer zone b/w internal and external networks.

→ Buffer networks contains servers (web, mail) monitored by firewall.

→ Users from the internet can access servers in the DM2 but not internal network resources directly.

→ Internal users typically access external resources via a proxy server.

→ Firewalls reject packets from DMZ without corresponding input packets towards the internet.

* Implementation of DMZ.

① Two Firewall.

→ one b/w the DMZ and the internal network (inner firewall).

→ Another b/w the DMZ and the external network (outer firewall)

→ Prevents security gaps by having firewalls from different manufacturers.

② Single Firewall.

→ More cost effective

→ Still provides effective DMZ but with less redundancy.

* Intrusion Detection System (IDS)

→ An IDS is a device or software applicatio that monitors networks or systems for malicious activity or policy violations.

→ Identifies unusual or suspicious behaviour on a network, protecting against known software exploits.

• Key components:

→ Uses intrusion signatures, patterns of behaviour (eg. ping sweeps) to detect potential threats.

→ Contigency plans are crucial for effective IDS utilization.

* Methods of Intrusion Detection.

① Signature - Based (Misuse Detection)

→ Monitors all network packets, comparing them against a signature database

→ Advantages: Widely available, easy to implement

→ Disadvantages

① Cannot detect attacks without signature

② Static signature mechanism can be adjusted by dedicated attackers.

③ Volume of signatures may result in false positives.

② Anomaly - Based (Statistical Detection)

→ Monitors network traffic against an established baseline, identifying deviations.

→ Uses statistics, neural networks, and data mining for adaptability.

→ Advantages

a) Detects new vulnerabilities and recognises authorized usage outside normal pattern.

→ Disadvantages

a) Slower, resource intensive

b) More complex.

Page No.
Date

* Architecture of IDS.

① Network - Based IDS

→ Monitors inbound/outbound traffic at strategic network points.

→ Advantages

a) Easy deployment, unobtrusive, difficult to evade at a low level of network operation.

→ Disadvantages

a) Fail-open scenario : different hosts process packets differently, requires completely network topology.

② Host - Based IDS.

→ Runs on all devices with direct access to the Internet and internal network.

→ More accurate than NIDS, less overhead due to lower traffic volume.

→ Expensive deployment, challenges when hosts get compromised.

Page No.
Date

* Honey pots

→ A honeypot is a cybersecurity tool, designed as a trap to attract potential attackers, filled with fabricated information.

→ Any access triggers monitors and sensors, helping understand threats and detect new ones

· Aims

① Detection and Diversion: Detect attacks or or divert potential attackers away from the system.

② Information Gamering: Gain insights into cybercriminal operations and intruder's action.

③ Observation and Swift Action: Encourage intruders to stay for observation, allowing admins to work swiftly.

* Working of Honey pots.

① Appearance of Legitimacy.

→ Honeypots resemble real computer systems with applications and data, fooling cybercriminals into targeting them.

→ Deliberate security vulnerabilities are built in. such as open ports or weak password

② Placements :

Honeypots can be strategically placed.

① In front of a firewall (Internet)

② In the DMZ.

③ Behind the firewall.

* Types of Honeypots.

① Based on Deployment

a) Production Honeypots : Low interaction, easy to use, capture limited information, primarily used by corporation.

b) Research Honeypots : Complex, used to gather information about motives and tactics of the black hat community.

(2) Based on Level of Involvement

a) Decoy Database Honeypot : Monitors software vulnerabilities, detects attacks exploiting insecure system architecture or using SQL injection.

b) Malware Honeypot: Mimics software apps and APIs, invites malware attacks for analysis to develop anti-malware software.

c) Spider Honeypot: Traps web crawlers by creating webpages and links only accessible to web crawlers.

d) Email Traps / Spam Traps: Places fake email addresses to trap automated address harvestors.

X X

Date

* Web Security Basics

- Web Security Vulnerability

→ Weakness in custom web application servic architecture, design, configuration, languages, servers, interpreters, or code can be exploited by hackers

→ Regularly update and patch your web server software to address known web vulnerabilities!

* Secure Web Programming

① Maintain security

→ Incorporate security throughout the entire web application development lifecycle.

② Input Validation

→ Implement data type, format and value validation to ensure the correctness and integrity of input.

Page No.
Date

③ Data Encryption.

→ Encrypt sensitive data to protect it from unauthorized access.

④ Exception Management

→ Use proper exception handling to gracefully handle errors and prevent information disclosure

⑤ Authentication, Role Management, Access control.

→ Implement robust authentication mechanisms

→ Enforce role-based access control to limit user priviledges

⑥ Security configurations

→ Avoid security misconfigurations, which can lead to vulnerabilities.

* SQL Injection

→ Attacker submits HTTP requests with a malicious parameter value that modifies an existing SQL query, or adds new queries.

→ Error messages and special queries are also added.

Examples

$username = $_POST['username']; $query = "SELECT * FROM users WHERE username = $username

* SSL / TLS

→ SSL (Secure Socket Layer) was created by Netscape in 1994 to encrypt application layer data.

→ SSL operates in the transport layer and enables secure communication b/w a client and a server, commonly used for web browsing (HTTPS)

→ SSL has evolved into TLS (Transport Layer Security).

① Encryption / Decryption

→ Public / private are used for encryption/decryption during the handshake

→ A session key is generated and used for the actual encrypted data exchange.

② Handshake Steps

→ Browser initiates the handshake by sending a hello message with details like protocol version, cipher suite, and random nonces

→ Server responds with its chosen cipher suite, certificate, and its own random nonce.

→ Server authenticates the client, decrypts the pre-master secret, creates a master secret, and informs the client about using the master key for the session.

→ Both client and server acknowledge and use master key for encrypted communication.

* Socket Layer

→ SSL/TLS operate as a 'socket layer' b/w the application and transport layers in the IP stack.

→ It is used for securing transactions over the Internet, ensuring authentication and confidentiality.

* Secure SSL Protocols

① SSL Handshake Protocol.

a) Purpose

→ Negotiation of security algorithms and parameters.

→ Key exchange

→ Server authentication and optionally client authentication.

b) Key Elements.

→ Security algorithm negotiation.

② SSL Record protocol.

→ Fragmentation: Breaking large messages int smaller fragments.

→ compression: Reducing the size of data for efficient transmission.

→ Message authentication and integrity protection.

→ Encryption of data.

(3) SSL Alert Protocol.

→ Handling error messages, including fatal alerts and warnings.

(4) Supported Algorithms

a) Public Key Algorithms: RSA, DH (Diffie-Hellman) DSA (Digital signature Algorithm)

b) Symmetric Key Algorithms: RC2, RC4, IDEA, DES, 3DES, AES.

c) Hashing Algorithms: MD5, SHA

* SSL Session.

→ An SSL session is an association b/w client and a server.

→ Sessions are stateful, including security algorithms and parameters.

→ Session establishment is resource intensive due to public key operations.

→ A session may encompass multiple secure connections b/w same client and server

• Components of a session.

① Session Identifier : A byte sequence chosen by the server to identify the session

② Certificate : X.509 certificate of the peer (may be null)

③ Compression method.

④ Cipher spec : Details of bulk DES, MAC algorithm and cryptographic attributes.

⑤ Master secret : A 48-byte secret shared b/w client and server.

Date

* IPSec Protocol.

→ IPSec (Internet Protocol Security) is a suite of protocols designed to provide secure private communications across IP networks.

→ It operates at the network layer (Layer 3) and ensures security for all traffic passing through the IP layer.

. Key Goals

① Authentication: Verifying the identity of communicating parties.

② Confidentiality: Encrypt data to ensure its confidentiality.

③ Integrity: Ensure the integrity of transmitted data.

④ Key management: Establish and manage cryptographic keys.

. Components of IPSec.

① IKE (Internet Key Exchange)

Page No.
Date

Purpose: Sets up Keys and algorithms for AH (Authentication Header) and ESP (Encapsulating Security Payload)

Functions:

① Provides mutual authentication and establishes a shared symmetric key.

② Initiates the establishment of security associations for AH and ESP.

② AH and ESP

a) AH (Authentication Header)

→ Provides integrity and authentication for IP packets

→ Uses cryptographic hash-based message authentication code. (HMAC)

→ Operates on port 51.

b) Encapsulating Security Payload. (ESP)

→ Provides confidentiality or integrity of IP packets.

→ offers encryption

→ operates on IP port 50.

* IPsec sessions

① Security Associations (SA)

→ An IPSec protected connection is called a security association, which can be either end-to-end or link-to-link.

→ IPSec sessions are stateful and include security algorithms and parameters

② Session State.

→ Components include

a) Session Identifier
b) Certificate
c) Compression method.
d) Cipher spec
e) Master secret.

* IKE Phases

① IKE Phase 1 (Authentication Keying)

→ Establishes a secure, authenticated channel b/w two computer.

→ Authenticates and protects the identities of the peers.

→ Negotiates SA policy, performs a shared secret key exchange, and sets up a secure tunnel for Phase 2.

→ Utilizes ephemal Diffie-Hellman for perfect forward secrecy. (PFS).

It has 4 options and two modes.

Options	Modes
1) Public Key (OG)	1) Main Mode
2) Public Key (new)	2) Aggressive Mo
3) Public Key signature	
4) Symmetric Key.	

Page No.
Date

① Main Mode IKE

→ Negotiates algorithms and hashes.

→ Hides user identity

→ Generates shared secret using Diffie-Hellman

→ Verifies Identities.

② Aggressive Mode IKE

→ Condenses negotiation, key exchange, etc into fewer packets.

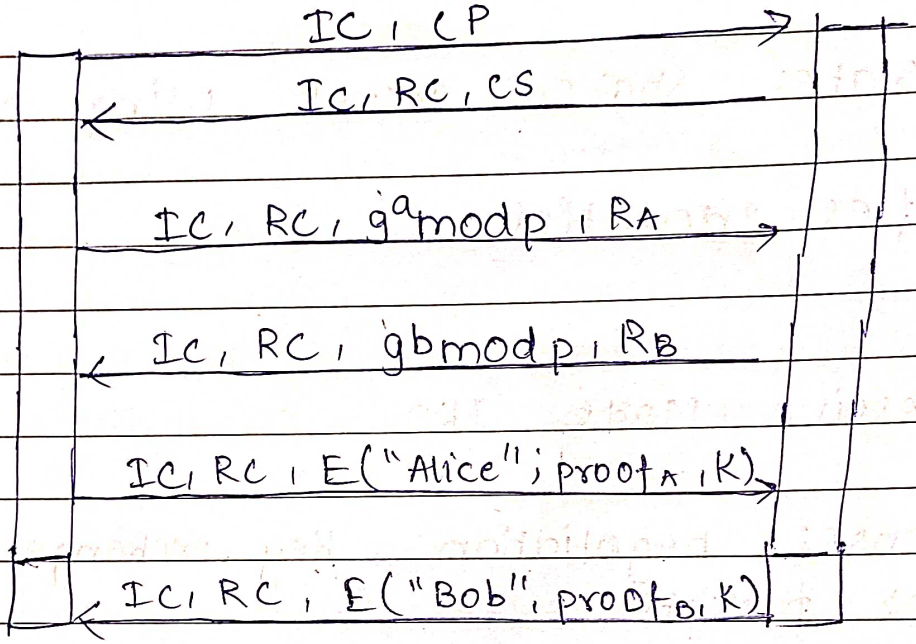
→ Reveals user identity.

→ Provides mutual authentication and a shared secret for deriving keys.

Date

6 versions of IKE Phase 1.

① IKE Phase 1 (Main Mode) Digital Signature



Here CP = crypto proposed
CS = crypto selected
IC = initiator cookie
RC = responder cookie

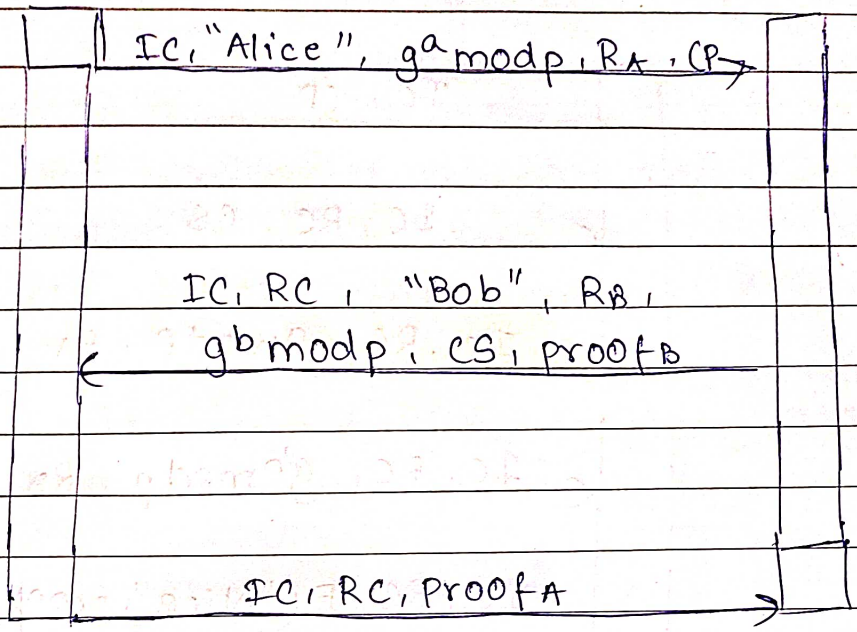
$$K = h(IC, RC, g^{ab} \bmod p, R_A, R_B)$$

$$proof = [h(SKEYID, g^a \bmod p, g^b \bmod p, IC, RC, CP, \text{"ALICE"})]_{Alice}$$

$$SKEYID = h(R_A, R_B, g^{ab} \bmod p)$$

Page No.
Date

(2) IKE Phase 1 (Aggressive Mode) Public key Signature.

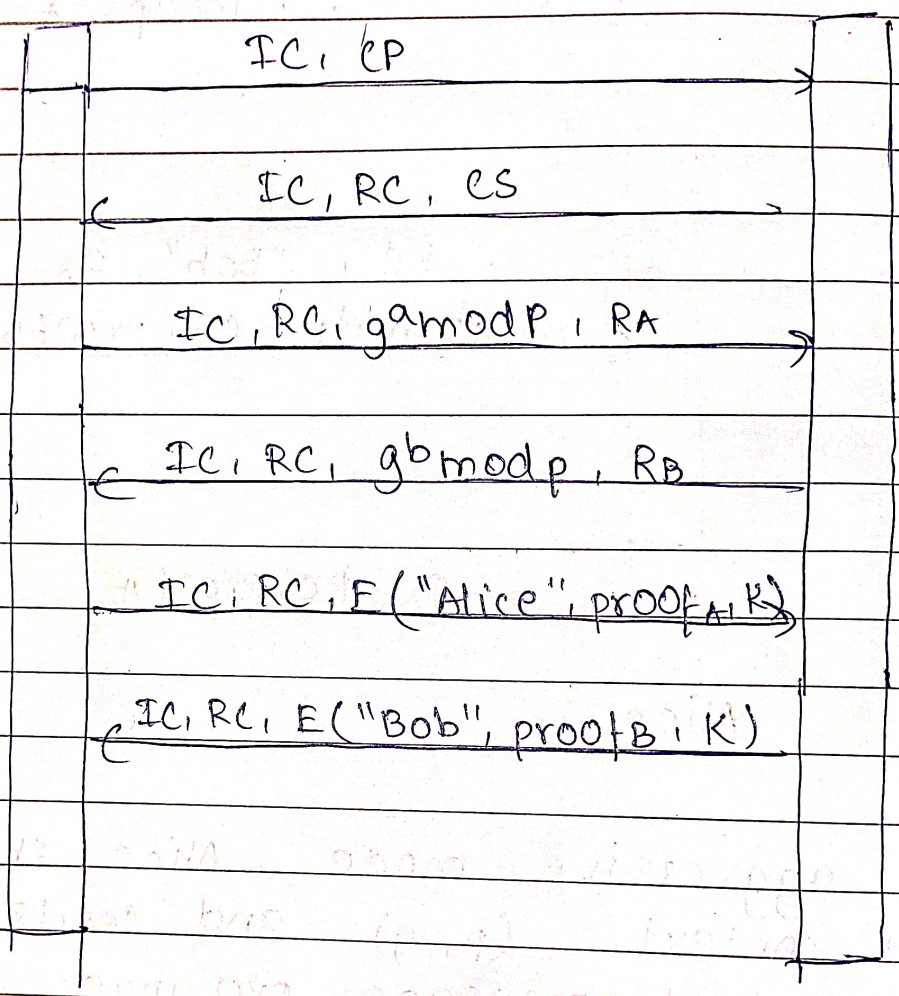


$

→ In aggressive mode, Alice chooses some DH context (p, g) and sends that in the first message exchange.

→ Bob may not support it, ~~but~~ and may reject the connection. If that happens, Alice should try to connect using main mode.

③ IKE Phase 1 (Main Mode) Symmetric Key Encryption:



K_{AB} = Shared symmetric Key.

$K = h(IC, RC, g^{ab} \bmod p, R_A, R_B, K_{AB})$

$SKEYID = h(R, g^{ab} \bmod p)$

Page No.
Date

* Problem with Symmetric Mode:

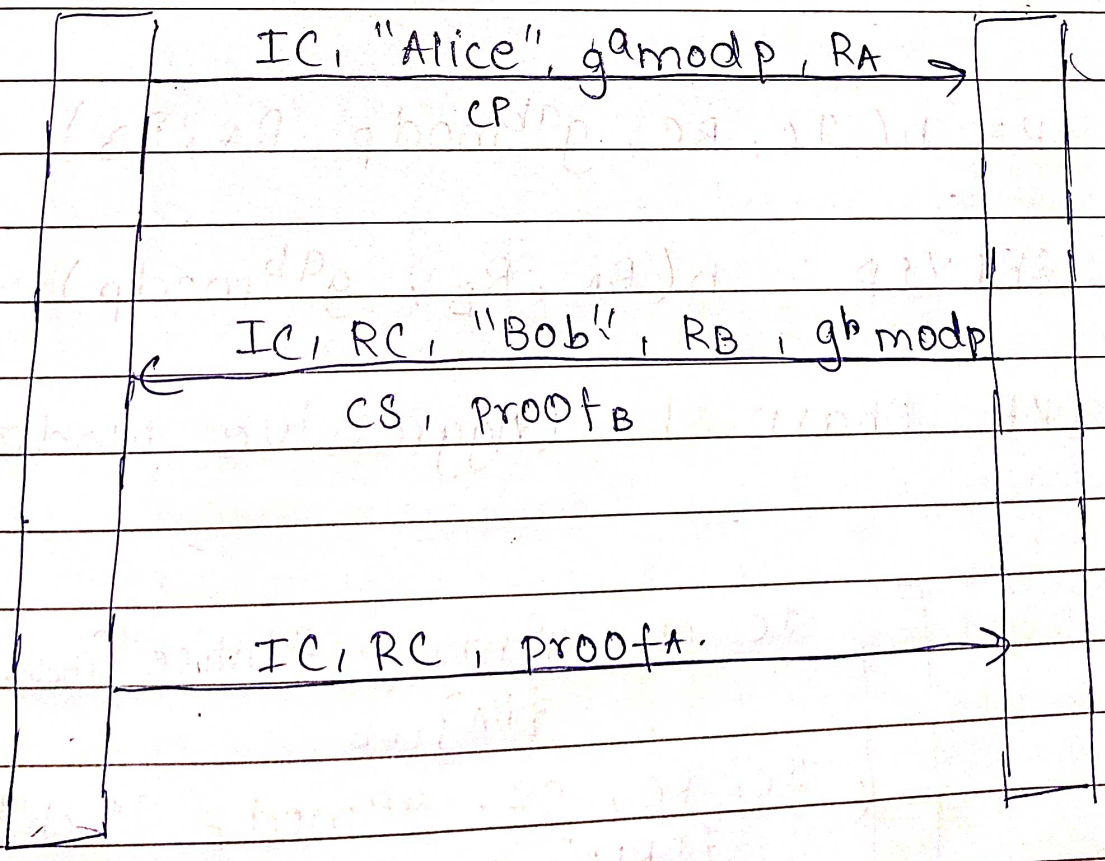
→ Alice sends her identity encrypted with K in message 5

→ To find K Bob must know K_{AB}.

→ To get K_{AB}, Bob must verify Alice.

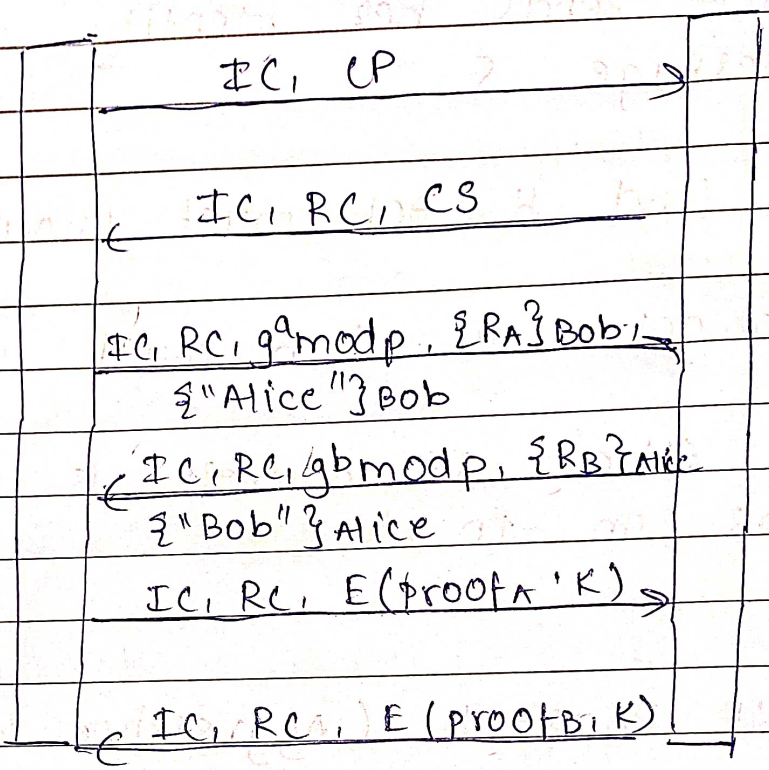
So Alice's IP Address is shared and used as an ID.

① IKE Phase 1 (Aggressive Mode) Symmetric Key.



Date

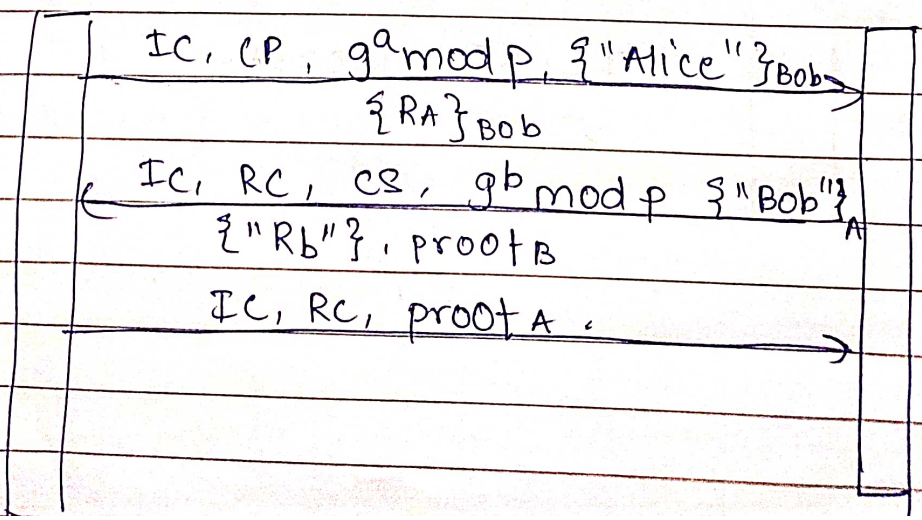
⑤ IKE Phase 1 (Main Mode) Public Key.



$K = h(IC, RC, g^{ab} \bmod p, R_A, R_B)$

$SKEYID = h(R_A, R_B, g^{ab} \bmod p)$

⑥ IKE Phase 1 (Aggressive Mode)



* IKE Phase 2

→ Establishes IPSec SA (Security Association)

→ Comparable to SSL connections

→ Negotiates IPSec SA parameters, establishes IPSec security associations for specific connections and periodically re-negotiates IPSec SAs

→ Optionally performs and additional DH exchange

→ All traffic on a connection established in Phase 2 is communicated through SAs.

* IPSec Modes

① Transport Mode:

→ IPSec header (ESP/AH) is inserted into the IP packet b/w IP header and data.

→ Efficient, as it adds minimal additional header data.

→ Only IP payload is encrypted and authenticated. IP headers may or may not be authenticated.

→ Passive attackers can see communicating parti

• Use cases.

→ Used for end-to-end association.

→ Efficient for host-to-host or host-to-gatew communication within the same network.

② Tunnel Mode:

→ Entire IP packet, including IP header and payload, is encapsulated into a new packet.

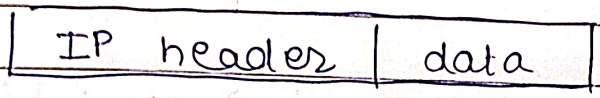
→ New IP headers are generated for the encapsulated packet, making the orignal IP header invisible to attackers.

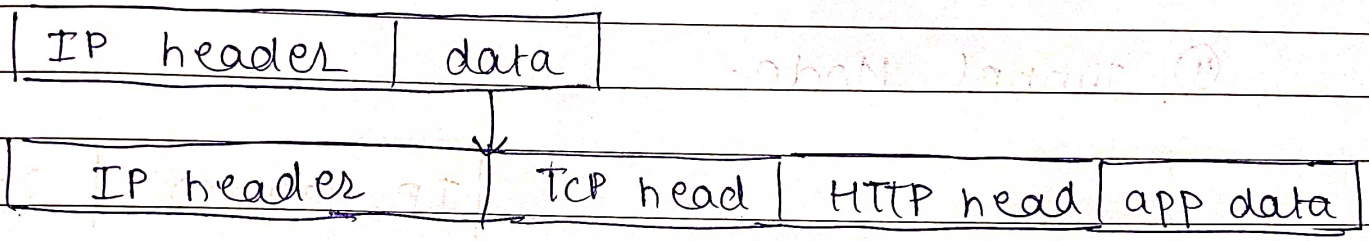
→ Used for firewall-firewall traffic, host-to-network or network-to-network communicati

→ Overhead of an additional IP header.

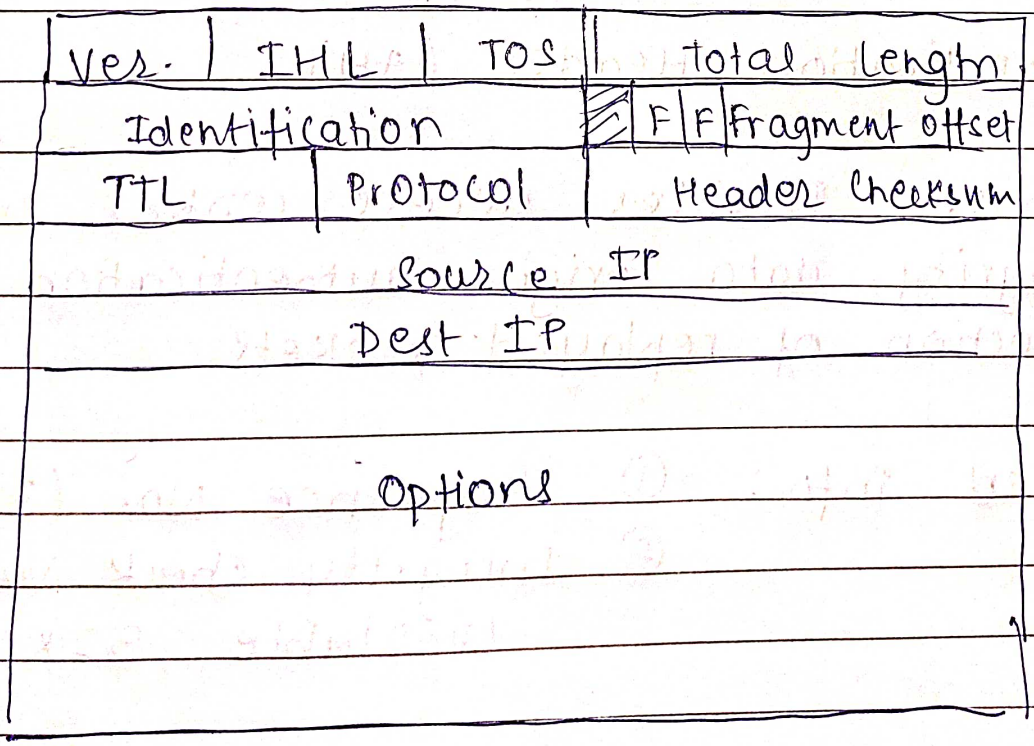
* IP header and datagram.

① IP datagram

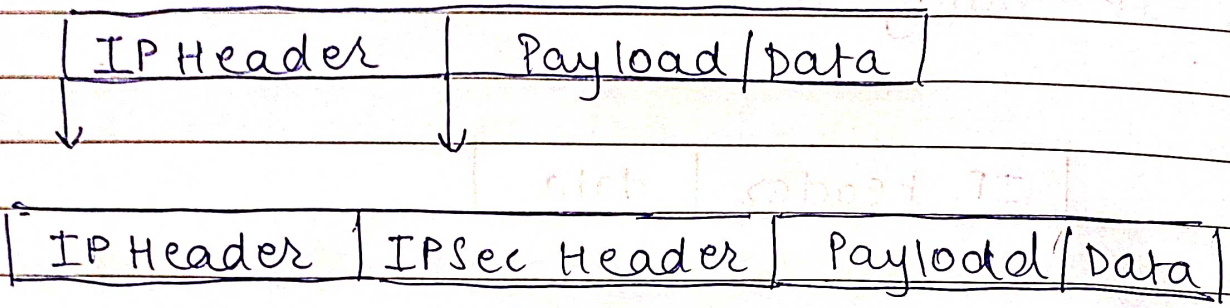




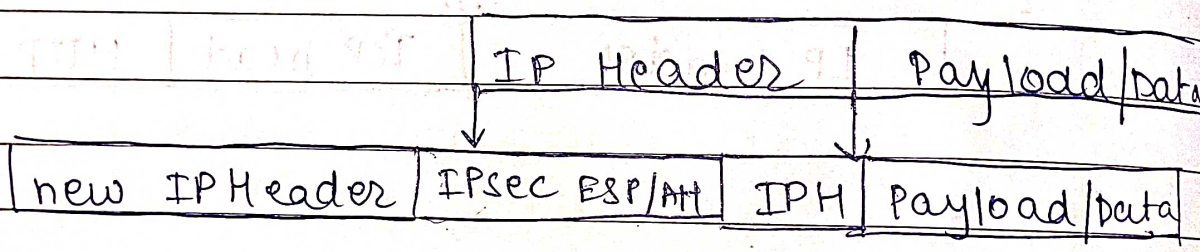
② IP Header.



③ Transport Mode



④ Tunnel Mode.



---

* Authentication Header (AH)

→ Purpose: Provides access control, connectionless integrity, data origin authentication, and rejection of replayed packets

→ Added Info: ① Sequence No. (32-bit)
② Integrity check value (variable, 32 x n bits)

→ Sequence No. prevent reuse of numbers within a session.

→ Range of sequence no. lies from 0 to $2^{32}-1$.

→ ICV (Integrity check value) is keyed using MAC algos like SHA, MD5 etc.

* ESP (Encapsulating security Payload)

→ Purpose: Protects data from tampering, provides authentication, replay-prooting and integrity checking.

→ Components: ① ESP Header
② ESP Trailer.
③ ESP Auth Block

* SSL vs IPSec.

IPSec	SSL
① Lives in network layer.	① Lives in socket layer
② & complex	② Simple.
③ Secure VPN also for IPV6	③ Secure web transactions