Experiment No. :..... Date :.....

UNIT-5

Q. Types of Spread Spectrum Technology

(i) Direct Sequence Spread Spectrum [DSSS] -
This method divides the stream of info to be transmitted into small bits. These bits of data are mapped to a pattern of ratios called spreading code. The transmitter and the receiver must be synchronized to the same spreading code / ratio.

(ii) Frequency Hopping Spread Spectrum [FHSS] -
This method operates by taking a broad slice of bandwidth spectrum & dividing it into smaller subchannels of 1MHz. The transmitter then hops between subchannels, sending out ~~four~~ short bursts of data on each subchannel for a short period of time (called dwell time)
→ FHSS supports more wireless devices, uses less power and is cheaper than DSSS.

(iii) Orthogonal Division Multiplexing [ODM] -
This method uses frequency division multiplexing and distributes data over carriers that are spaced apart at precise frequencies. Spacing provides "orthogonality" & prevent demodulators from seeing frequencies other than their own.
→ Used for digital TV in Europe, Japan & Australia

Q. Wi-Fi Security = [WEP + WPA + 802.1X].

i) Wired Equivalent Privacy [WEP] -

→ security protocol for wireless networks to provide data confidentiality comparable to traditional wired network
→ It uses a security algorithm for 802.11 wireless network that is as secured a wired network.
→ It ensures wireless security through the use of an encryption key called initialization vector (IV). The IV is added to a preshared key to encrypt each packet with a different key.
Result = IV + PSK.
→ It can be an open system authentication or closed system authentication.
→ WEP doesnot ensure the authenticity of the data packets.

ii) Wi-Fi Protected Access [WPA] -

→ security protocol developed for the Wi-Fi alliance to secure wireless network replacing WEP.
→ It is a temporary solution to WEP's problems. WPA still uses WEP's insecure RC4 stream cipher but provides extra security using TKIP (Temporal key Integrity Protocol), which scrambles the keys using a hashing algorithm.
→ Wireless security is ensured through the use of password, that is, IV + TKIP.
→ Authentication is ensured through the use of a 64 digit hexadecimal key or 8-63 character passcode

Q. Steps in WEP Encryption:

There are 7 steps in encrypting a message -

(1) the transmitting and receiving stations are initialized with the secret key. This key must be distributed by using an out-of-band mechanism such as email, posting it on website, or giving it on a piece of paper.

(2) The transmitting station produces a seed, which is obtained by appending the 40 bit secret key to the 24 bit IV key, for input as pseudo-random number generator (PRNG)

(3) The transmitting station inputs the seed of the WEP PRNG to generate a key stream of random bytes.

(4) The key stream is XOR'd with plaintext to obtain the cipher text.

(5) The transmiting station appends the cipher text to the IV and sets a bit that indicates that it is a WEP-encrypted packet. This completes WEP encapsulation. WEP encrypts only data. Header & trailer are sent as a frame of data.

(6) The receiving station checks to see whether the encrypted bit of the frame is set. If so, the receiving station extracts the IV from the frame & appends the IV to secret key

(7) The receiver generates a key stream that must match the transmitting station's key. This key stream is XOR'd with ciphertext to obtain the sent plaintext.

Q. Components of IDS:

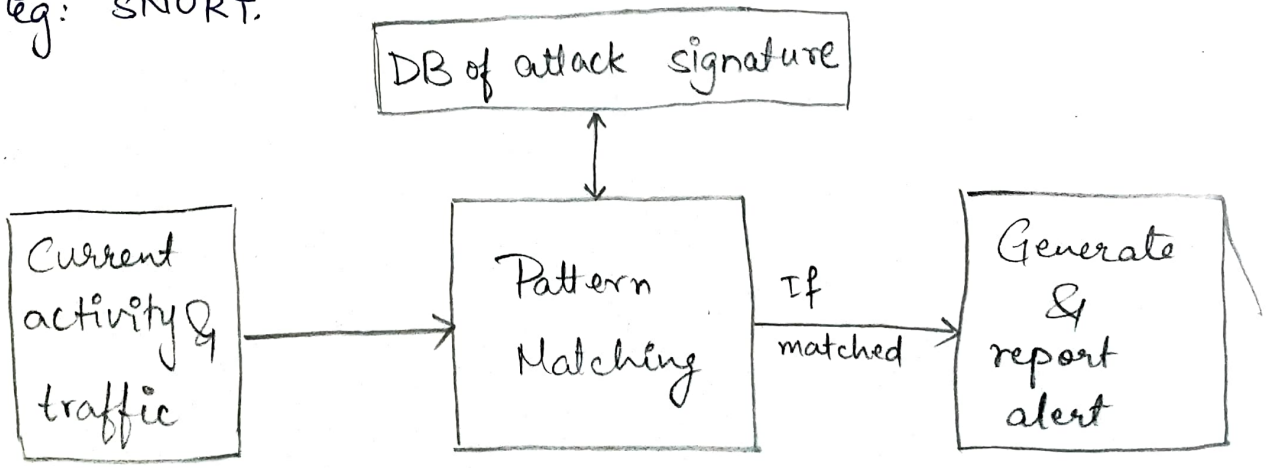
Intrusion Detection System components:

(1) Network Sensors – these sensors detect and send data to the system
(2) Central Monitoring System – processes and analyzes the data sent from sensors.
(3) Report Analysis – offers information about how to counteract a specific event.
(4) Database & Storage components – perform trend analysis and store the IP address and information about the attacker.
(5) Response Box – Inputs information from the previously listed components and forms an appropriate response

Q. Types of IDS Engines –

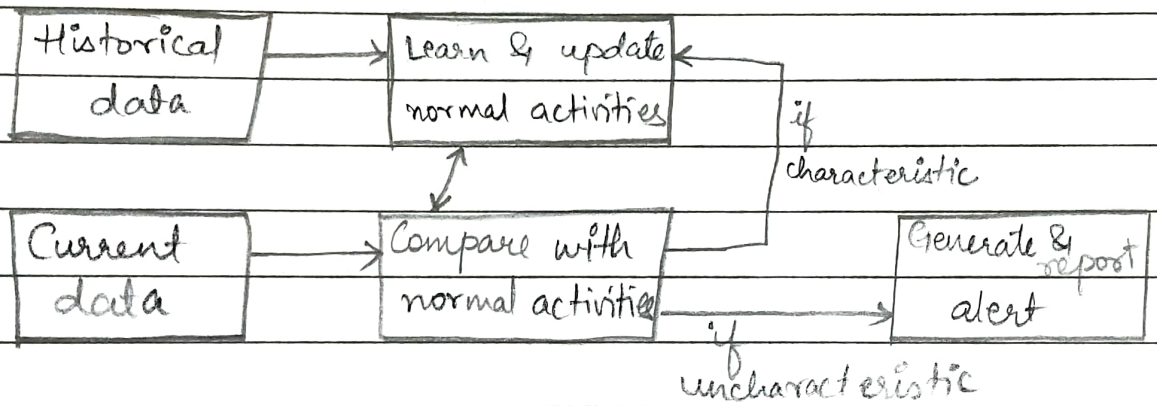
(1) Signature Based IDS Engines

* signature based (pattern matching) IDS engine works on identifying an attack based on signature loaded into database previously
* alerts are triggered based on IP packets, SYN packets and malformed ICMP packets.
* Eg: SNORT.



(2) Anomaly based IDS Engine –

* Anomaly based IDS engines places IDS in learning mode so that it can learn what constitutes normal activity
* It performs deep packet inspection (decoding of pkts).
* Eg: If DNS responses are detected without DNS request, the activity is termed cache poisoning.



Q. Need for IDS or Importance of IDS.

* Modern business (networked) environments require high level of security to ensure safe and trusted comm^{n} of information between various organizations.
* IDS acts as an adaptable safeguard technology for system security after traditional technologies like firewall and spyware fail.
* IDS enables to detect and respond to malicious traffic.
* IDS ensures IT personnel is notified when an attack or network intrusion might be taking place.

Q. 2 Types of IDS.

(1) Network Intrusions Detection System [NIDS] –

* examines the packet on network & look at data in an attempt to recognize an attack.
* NIC is placed in pcosmiscuous mode to identify all packets & not just ones addressed to it.
* NIDS can be plugged into hub if system is operating on it.
* If switch is used, port must be spanned/mirrored.
* Advantage →
  Can support many sensors to monitor DMZ, internal network or specific nodes on network.
* Disadvantage →
  event if it can see certain types of traffic, it doesn't mean that it knows what the traffic is actually doing.
* Eg: SNORT, Cisco Intrusion Detection System.

(2) Host Intrusion Detection System [HIDS] –

* monitors traffic on one specific system.
* doesnot place NIC in promiscuous mode
* looks for unreal events / patterns that may indicate problems.
* efficiently detects unauthorized access & activity
* Eg: Swatch, RealSecure

Q. Securing Wireless Network.

Securing wireless networks can be a challenge but can be accomplished by -
(i) Defense in Depth (ii) Misuse Detection

(1) Defense in Depth -

* Builds many layers of protection
  → encryption to hide data from unauthorized individuals.
  → providing physical protection to hardware
  → using authentication to verify network users identity
  → limiting access based on least privilege.
* one can change the defaut value of SSID.
* MAC filtering uses a MAC address assigned to each network adapter to enable block access to the network.
* Limit access to wireless network to specific network adapters.
* Site-survey - i.e., gathers information to check if client has the right number and placement of APs to provide enough coverage throughout the facility.
* Deploying many layers of security makes it harder for attacker to overcome the combined security mechanism.

(2) Misuse Detection -

* Wireless IDS work like wired IDS as it can monitor traffic and alert admin of unusual traffic patterns.
* It can be centralized/decentralized and should have a combination of sensors that collect and forward data from 802.11.
* Some wireless IDS can provide general estimate of the hacker.

* Commercial IDS products → IBM RealSecure Server Sensor, AirDefense, Rogue Watch.
* Open Source solutions →
(1) AirSnare – alerts to unfriendly MAC addresses on the network as well as DHCP requests taking place
(2) WIDZ Intrusion Detection – can be integrated with snort or RealSecure; It is used to guard WAPs.
(3) Snort-Wireless – can be integrated with SNORT. It is used to detect Rogue APs, ad hoc devices.

Q. Wireless LAN Threats.

(1) Wardriving –

(i) Wardriving – the act of finding & marking the location and status of wireless networks. It uses GPS device to ~~locate~~ record location & a discovery tool (NetStumbler).
(ii) Warchalking – the act of marking buildings / sidewalks with chalks to show others where its possible to access an exposed company wireless network.
(iii) Warflying – similar to wardriving except the fact that a plane is used instead of a car. One of the first publicized acts occured in San Francisco Area.

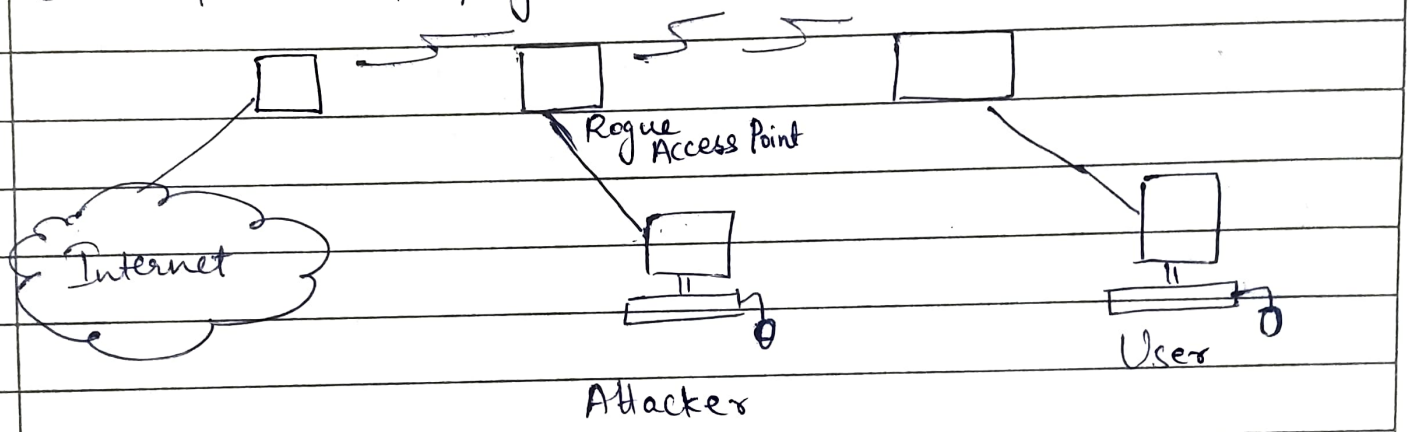
* Tools to detect : NetStumbler and Kismet.

(2) Eavesdropping –

* Eavesdropping also known as sniffing / snooping is theft of information as it is transmitted over a wireless network.
* It takes advantage of unsecured network communication to access data as it is being sent or received by its user.
* Tools : Dsniff, Win Sniffer.

(3) Rogue & Unauthorized Access Points :-

* A rogue A.P is an unauthorized connection to the corporate network.
* 2 primary threats -
(i) the employees ability to install unmanaged APs. The ease of use of wireless equipment & the lure of freedom is just too much for some employees to resist.
(ii) The ability to perform WAP spoofing.
* Access point Spoofing -



* → access point spoofing occurs when the hacker sets up their own rogue WAP near the victim's network or in a public place where victim might try & connect.
→ If the spoofed WAP has strong signal, the victim's computer will choose the spoofed WAP. The attacker can then attempt to steal usernames & passwords or simply monitor traffic.
* → This attack is called as "evil twin attack".

(4) Denial of Service [DoS] -

* DoS attack doesnot get the attacker access, but it renders the network unusable/degrade services for the real users.
* Common types of DoS attacks:
(i) Authentication flood attack - generates flood of EAPOL messages requesting 802.1x authentication
(ii) Deauthentication flood attack - targets an individual client and works by spoofing a deauthentication frame from WAP.
(iii) Network Jamming attack - attacks the entire wireless network by building a transmitter to flood the airwaves in the vicity of the wireless network.
(iv) Equipment Destruction attack - targets the AP. Attackes uses high-output transmitter with directional high-gain atenna to pulse the AP.

Q. 802.1x AUTHENTICATION

* provides port-based access control
* used in conjuction with EAP to authenticate devices that attempt to connect to a specific LAN port.
* EAP bundled with WAP is used for communication authentication information and encrypt keys b/w clients & an access control server like RADIUS.
* Ways to implement EAP - password, digital certificates, & token cards
* EAP can be deployed as - EAP-MD5, EAP-TLS, EAP with Tunneled TLS (EAP-TTLS), Cisco Lightweight EAP (LEAP).