Chapter 4

Securing your network

horizontal line

# IDSs and IPSs

IDSs monitor and send alerts when they detect suspicious activity.

## HIDS

Host-based intrusion detection system protects host, can detect potential attacks and protect critical files installed on individual systems, and Monitors traffic passing through NIC. It can detect malware that antivirus software can miss.

## NIDS

Network-based intrusion detection system. Installed on sensors or collectors on network devices such as routers/firewalls, and monitors activity on a network.

Cannot detect anomalies on individual systems or workstations, and cannot monitor encrypted traffic

Tap/port mirror: Admins can configure a switch to send all traffic received to a single port, which can then be used as a tap to send all switch data to a sensor/collector, and forward it to NIDS

Taps can also be configured on routers to send data to IDS

## Sensor and collector placement

Sensors can be placed anywhere on a network to monitor traffic,e.g. Outside firewall to see all traffic, or before to see traffic that has been allowed through

## Detection methods

IPSs prevent attacks by detecting them and stopping them before they reach the target. There are 2 types of detection, signature-based and behaviour-based, which can be detected by any type of IDS.

**Signature-based detection**: Uses a database of known vulnerabilities/known attack patterns, e.g. SYN attacks are known and have a specific pattern of SYN packets being sent. An IDS can detect these patterns, in a process similar to antivirus software used to detect malware.

IDS signatures and detections need to be updated regularly to protect against current threats

**Heuristic/Behavioural detection:** Identifies a normal behaviour of a network by creating a performance baseline under normal operating conditions.

IDS constantly compares current network performance with the baseline, and gives an alert when it detects behaviour outside normal boundaries identified in baseline.

Data sources and trends: IDSs can record logs, such as firewall logs, system logs, etc. These can be analysed and used to predict patterns, and flag up items of interest

Reporting based on rules: IDSs report based on rules defined in the IDS, and admins investigate whether reports are valid

False positives vs false negatives: IDSs are susceptible to both, but the threshold/sensitivity needs to be adjusted depending on purpose. A high incidence of false positives increases workload on admins.

**IPS vs IDS**

IPSs are an extension of IDSs. They both have protocol analyser capabilities

* IPS can detect, react and prevent attacks
* IDS monitors and responds only after detecting an attack
* IPS is inline with traffic; all traffic passes through it, which it can block
* IDS is out-of-band; it monitors network traffic, but traffic does not go through IDS. It can also modify ACLs to block offending traffic

## NIPS

Network intrusion prevention system. Many APTs (Advanced persistent threats) have installed RATs (remote access trojans) through phishing/malware. If an attack takes place, it will be seen as coming from an internal system, so won’t be blocked by the firewall, but NIPs will prevent it from reaching the private network.

## SSL/TLS accelerators

Hardware handling TLS traffic. By offloading this to another device, it frees up CPU power and RAM. It is best to place it close to the device that is using it.

## SSL decryptors

Can decrypt encrypted malware, e.g. one that is transferred through a HTTPS session. Unencrypted traffic passes normally, but a separate TLS session is created for encrypted traffic, where it is decrypted and inspected. They are often used with NIPS, allowing it to inspect unencrypted traffic and prevent attacks.

## SDN

Software defined network. Uses virtualisation techniques instead of routers and switches to redirect traffic.

It can use protocols such as OSPF (Open shortest path first) and BGP (Border gateway protocol) without the hardware routers

## Honeypots

A server that is left unsecure, and with fake data; used as bait for an attacker, diverting it from a live network. They are used to gather intelligence on an attacker, and can also help admins learn about zero-day exploits.

## Honeynets

Group of honeypots within a separate network, created using multiple VMs contained within a single server; an attacker can’t tell whether the servers are virtual or physical

## IEEE 802.1x security

Requires users to authenticate when they connect to a specific WAP or port, preventing rogue devices from connecting.

This can be implemented as a Remote Authentication Dial in user Service (RADIUS) or Diameter server

## Wireless basics

WAP: wireless access point, connects wireless clients to wired network.

All wireless routers are APs, with additional capability of routing. However, not all APs are wireless routers, as not all have routing capabilities.

**Fat vs Thin APs**

**Fat AP:** Contains everything you need to connect wireless clients to wireless network, e.g. NAT, DHCP, ACLs, etc. however, they must be configured separately from each other, which is inefficient

**Thin APs:** Controller based, managed by a wireless controller, making administration easier.

**Band selection and Channel widths**

Wireless networks use either 2.4GHz or 5GHz. Wider channels allow you to transfer more data. However, this decreases radio transmission distance, and increases chance of interference and overlap

**AP SSID:** Service set identifier, which is the name of the wireless network.

**SSID broadcasting**: if SSID broadcasting is disabled, then the SSID entry on other devices searching is blank. However, the AP includes the SSID in probe responses sent to probe requests, so it is easy to install a wireless protocol analyser and detect the SSID

**MAC filtering:** Can be used to restrict access to wireless networks. However, an attacker can use a sniffer to discover allowed MAC addresses, and spoof the MAC address to gain access to the network.

Antenna types and placement:

* Omnidirectional antenna: transmit and receive signals at the same time, allowing devices to connect from any direction
* Directional antenna: Can only receive signals in one direction, but because of this it is more powerful.

It is recommended to place antenna both horizontally and vertically.

Antenna power and signal strength: Power level can be increased or decreased to change the access range of the AP. this is useful if you want to limit the range to a single room or building to prevent other people from connecting.

## Wireless cryptographic protocols

* WPA: WIFI protected access, a replacement for WEP. However it is prone to password attacks, where an attacker uses a wireless protocol analyser to gain the authentication traffic, then an offline brute force attack to get the password. They can also use a dissociation attack to force the user to reauthenticate.
* WPA2: Permanent replacement for wpa, using a stronger cryptography.
* TKIP vs CCMP: TKIP is Temporal Key Integrity Protocol, and CCMP is a newer protocol used by WPA2, which is more secure.
  + TKIP does not require new hardware
  + WPA2, with AES (based on CCMP) is a better algorithm for encryption

WPA and WPA2 operate in PSK (pre shared key) mode or Enterprise modes. PSK allows users access anonymously with a PSK or password (this does not provide authentication)

Enterprise forces users to authenticate with credentials. It is often implemented as a 802.1 server implemented as RADIUS server.

RADIUS port is 1812, but can also use 1645. The port and the server must use the same port

## Authentication protocols

* EAP: Extensible authentication protocol. Provides method for 2 systems to create secure authentication key, Pairwise Master Key (PMK)
* EAP-flexible authentication via secure tunneling: EAP-FAST. Replacement for LEAP (lightweight EAP). supports certificates.
* PEAP: Protected EAP. Encapsulates EAP traffic with TLS. Requires certificate on 802.1x server but not on the client.
* EAP-Tunneled TLS: EAP-TTLS. Extension of PEAP, allowing users to use older protocols such as PAP (password authentication protocol). Requires cert on servers but not on clients.
* EAP TLS: One of the most secure EAP standards. Requires certificates on both server and all clients.
* RADIUS federation: Can create a federation using 802.1 and RADIUS servers.

## Captive portals

Forces clients to complete a specific process before they are allowed access to the network, e.g. free wifi points all have one, where they make you sign up first.

* Free internet access: Requires users to acknowledge and agree to a set of rules (Acceptable Use Policy AUP)
* Paid internet access: Sell access to users, PAYG
* Alternative to IEEE 802.1x: Can use captive portals instead of 802.1x

**Wireless attacks**

**Dissociation attacks**

Removes a client from a wireless network. A wireless device can send a dissociation frame with the client’s MAC (spoofed), causing the AP to terminate the connection and deallocate the memory it was using for the connection.

Client must go through authentication process to reconnect, and a WPS attack allows the attacker to get the password.

## WPS and WPS attacks

WIFI protected setup (WPS) allows users to configure wireless devices without typing a passphrase, so they can configure using short PIN or pressing physical buttons.

It is susceptible to brute force attacks, such as WPS attacks. It is recommended to turn WPS off.

## Rogue AP

It is an AP placed in a network without official authorisation, allowing attackers to connect to network devices in wireless closets. It acts as a sniffer to capture traffic passing through the wired network device, allowing data exfiltration.

It can be prevented by unplugging ethernet to stop access to network traffic.

## Evil twin

Rogue AP with same SSID as legitimate AP. Can be used to make other users unknowingly connect to it, and then capture their data, by configuring a wireless access card as an AP.

A site survey can help an admin find an evil twin, as the signal will get stronger as the admin gets closer.

## Jamming attacks

Attacker can broadcast noise/radio signal over a network, disrupting performance. It is a type of DoS attack.

Users can have intermittent connectivity, as the interference causes them to lose connection and forces them to reconnect.

You can increase the power level of an AP to overcome an attack, or use different wireless channels, and change channels when one gets too noisy. However, an attacker can also change channels.

## IV attacks

Wireless Initiation Vector attack attempts to discover the Preshared Key from the IV, which is a number.

Some wireless protocols use IV by combining it with the PSK to encrypt data-in-transit.

An IV attack is successful when an encryption system reuses the same IV.

The attacker uses packet injection attacks to add additional packets into the data stream, causing the AP to respond with more packets. This increases the chance that it will reuse a key, causing the attacker to crack the WEP key. WEP is a deprecated protocol.

## NFC attacks

Near field communication allows mobiles to communicate with each other. An attacker can use an NFC reader to capture data from another NFC device, through an eavesdropping attack, where the reader intercepts data transfer between 2 devices.

## Bluetooth attacks

Used in personal area networks (PANs).

* Bluejacking: Sending unsolicited messages/media via bluetooth
* Bluesnarfing: theft of info from bluetooth device.
* Bluebugging: Similar to bluesnarfing, but allows the attacker to gain full access by installing a backdoor.

When bluetooth devices are configured, they are in discovery mode, so they broadcast their MAC addresses. Ensuring users cannot connect without manual user intervention prevents these attacks.

## Wireless replay attacks

Attacker captures data sent between 2 entities, modifies it, and then impersonates one of the parties by replaying the data. WPA with TKIP is vulnerable to these attacks, but WPA2 with CCMP is secure.

WPA uses a sequence counter to number packets, and an AP will reject packets out of order. TKIP uses Message Integrity Check to verify integrity of packets, but attackers can discover this key. They can then transmit and decrypt packets

## RFID attacks

Radio Frequency Identification systems (RFID) are used to track objects, they have no signal but can transmit data between each other. Some RFID attacks are:

* **Sniffing/eavesdropping:** If an attacker knows the frequency used by a chip, it can have a receiver tuned to that frequency.
* **Replay**: An attacker can configure a fake tag to mimic the tag on a valuable object, then steal it without it being detectable.
* **DoS**: if an attacker knows the frequency of a chip, it can launch a jamming/interference attack.

## Misconfigured Access Points cause all these attacks!

## 

## VPNs and VPN connectors

You can create a VPN by enabling services on a server, such as Direct Access VPN role.

A VPN concentrator includes all the services needed to create a VPN, and is placed in the DMZ. The firewall between the internet and DMZ would forward VPN traffic to the VPN concentrator, which would then route private VPN traffic to the firewall between DMZ and intranet.

## Remote access VPNs

VPN server is in a DMZ, and when a user logs on, it sends the credentials to a RADIUS server. This server can either authenticate, or pass onto another authenticating server such as LDAP

## IPSec

It is a way of encrypting data-in-transit.

* Tunnel mode: Encrypts the IP packet, so IP addressing of internal network is not visible to anyone on the internet.
* Transport mode: Used in private networks, so isn't any need to encrypt IP addresses

It provides security with:

* Authentication: Includes an AH to allow hosts to authenticate each other before exchange. Uses protocol number 51
* Encryption: Includes Encapsulating Security Payload (ESP) to encrypt and provide confidentiality, authentication and integrity. Uses protocol number 50

Packet filters use protocol numbers to identify AH and ESP.

IPSec uses IKE over port 500 to authenticate clients in an IPSec conversation. It creates Security associations (SAs) for VPNs.

## TLS for tunneling

TLS is sometimes used to secure a VPN channel. SSTP (Secure socket Tunneling Protocol) encrypts VPN traffic using TLS port 443. This port is a useful alternative when a tunneling device must go through NAT, and IPSec is not feasible. OpenVPN and OpenConnect use TLS to create a secure channel

## Split tunnel vs Full tunnel

Split tunnel: VPN administrator determines which traffic should use the encrypted tunnel

Full tunnel: All traffic connected to VPN goes through encrypted tunnel. However, it can be slow.

## Site to site VPNs

2 VPNs that act as gateways for 2 systems, so they can connect remotely. However it is slower than connecting to a local server.

## Always-on VPNs

They can be used with site-to-site VPNs and remote access VPNs, and attempt to create a connection as soon as a device is turned on.

## Network access control

NAC methods provide monitoring by inspecting computers and preventing them from accessing the network if they don’t meet certain standards.

## Host health checks

Health conditions checked:

* Up-to-date antivirus
* Up-to-date OS
* Firewall enabled on client.

NAC systems use authentication agents to inspect NAC clients.

If it doesn’t meet health condition standards, the client is redirected to a remediation network by the VPN, where the client can use the resources to pass the health conditions, such as antivirus etc.

## Permanent vs Dissolvable

Permanent agent: Installed on client and stays on client

Dissolvable agent: Downloaded and run when client connects remotely. Sends report back to NAC client and then removes itself

## Identity and access services

These are the authentication methods used by VPNs:

* PAP: Password authentication protocol, used with PPP (point to point protocol) to authenticate clients. However, it sends passwords over a network in cleartext
* CHAP: Challenge handshake authentication protocol, uses PPP but more secure than PAP. Handshake process is used when client tries to connect to server, and then authentication details are encrypted and sent.
* MS-CHAP and MS-CHAPv2: Microsoft CHAP. improved version of chap, with mutual authentication.
* RADIUS: Can be used with 802.1x and WPA2 Enterprise, to act as a central authentication service, with a centralised database. It usually accesses LDAP with the user details, and uses UDP. Centralised authentication.
* TACACS+: Terminal access controller access control system plus. Cisco alternative to RADIUS, and encrypts entire authentication process, whereas RADIUS only encrypts password. It also uses multiple challenges between server and client. Centralised authentication.
* Diameter: Extension of RADIUS, which has new commands, and uses TCP instead of UDP. Centralised authentication.
* AAA protocols: Provides authentication, authentication, authorisation, accounting.

**ACRONYMS**

**IDS and IPS**

HIDS: Host-based intrusion detection system

NIDS: Network-based intrusion detection system

NIPS: Network intrusion prevention system

SDN: Software defined network

**Wireless cryptography protocols**

TKIP: Temporal key integrity protocol, cryptography protocol. CCMP is better

PSK: Pre-shared key, used with WPA2 to authenticate users.

EAP: Extensible authentication protocol. Provides a secure authentication key

EAP-FAST: EAP flexible authentication via secure tunneling, supports certificates

EAP-TTLS: eap tunneled TLS, cert on servers not clients

PEAP: Protected EAP. Cert on 802.1X server

EAP-TLS: cert on server and client

**Wireless attacks**

IV attack: Initiation vector attack, which attempts to discover preshared key from IV

RFID: Radio frequency ID systems, Used to track objects. Attacker can tune into fequency and steal data.

**VPNs and VPN connectors**

ESP: Encapsulating security payload, used by IPSec to encrypt data in transit

SSTP: Secure socket tunneling protocol, used with TLS to encrypt VPN traffic.

**Identity and access protocols**

PAP: Password authentication protocol

CHAP: Challenge handshake protocol, uses handshake process to connect and authenticate

MS-CHAP: Microsoft CHAP, improved version of CHAP

TACACS+:Terminal access controller access control system plus, cisco alternative to RADIUS