**Network hardening**

Et bilde som inneholder tekst, skjermbilde, Font, nummer

KI-generert innhold kan være feil.

Regularly performed

* Firewall rules maintenance
* Network log analysis

The process of examining network logs to identify events of interest (could use SIEM tool)

* Patch updates
* Server backups

Irregularly performed

* Port filtering on firewalls

A firewall function that blocks or allows certain port numbers to limit unwanted communication

Any unused ports should be disallowed this protects against port vulnerabilities

Networks should be set up with the most up to date wireless protocols and older wireless protocols should be disabled

* Network access privilege

Network segmentation to create isolated subnets for different groups of for example an organization for easier isolation of possible infected systems

Security zones with perimeters in between:

Internet Zone — No Trust

-------------------------------------------------

External DMZ — Low Trust

-------------------------------------------------

Enterprise Zone — Medium Trust

-------------------------------------------------

Extranet Zone — Medium Trust

-------------------------------------------------

Internal DMZ — High Trust

-------------------------------------------------

Management Zone — Highest Trust

-------------------------------------------------

Restricted Zone — Highest Trust

* Encryption for communication

All network communication should be encrypted using the latest encryption standards which are rules and methods used to conceal outgoing data and uncover/decrypt incoming data.

Data in restricted zones that might include, for example, sensitive information should have much higher encryption standards which obviously makes it a lot more difficult to access.

**Full packet capture devices** can be incredibly useful for network administrators and security professionals. These devices allow you to record and analyze all the data that is transmitted over your network. They also help by investigating alerts created by an IDS.

Security Information and Event Management is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools work in real time to report suspicious activity in a centralized dashboard. SIEM tools additionally analyze network log data sourced from IDSs, IPSs, firewalls, VPNs, proxies, and DNS logs. SIEM tools are a way to aggregate security event data so that it all appears in one place for security analysts to analyze…..

* **Intrusion Detection System** is an application that monitors system activity and alerts possible intrusions. An IDS alerts based on the signature of malicious traffic

The IDS is configured to detect known attacks.

Often, they sniff data packets as they move across the network and analyze them for the characteristics of known attacks.

Some also look for anomalies that could be the sign of malicious activity

Really good tool for network administrators for getting alerted so anomalies and signatures can be investigated further

Some new and sophisticated attacks might not get caught

NOTE:

IDS don’t stop the incoming traffic if it detects something awry. It is up to the network administrator to catch the malicious activity before it does anything damaging to the network. Combining the IDS with a firewall adds another layer of defense. The IDS is placed behind the firewall and before entering the LAN, which allows the IDS to analyze data streams after network traffic that is disallowed by the firewall has been filtered out. This is being done to reduce noise in IDS alerts, also referred to as false positives.

Et bilde som inneholder skjermbilde, tekst, diagram, Font

KI-generert innhold kan være feil.

**Intrusion Prevention System**

IPS is an application that monitors system activity for intrusive activity and takes action to stop the activity. It offers even more protection than an IDS because it actively stops anomalies when they are detected, unlike the IDS that simply reports the anomaly to a network administrator. An IPS searches for signatures of known attacks and data anomalies. An IPS reports the anomaly to security analysts and blocks a specific sender or drops network packets that seem suspicious.

Et bilde som inneholder tekst, diagram, Font, design

KI-generert innhold kan være feil.

Et bilde som inneholder tekst, skjermbilde, Font, meny

KI-generert innhold kan være feil.