18) Network Operations

Tuesday, November 26, 2024 2:16 PM

Risk Management:

Hardening and Security Policies:
A Security Policy is going to define how an organization will protect its infrastructure. There are several different kinds of policies

Acceptable Use Policies(AUP):
This defines what and what shouldn't be done on company devices.

Ownership
Network Access
Privacy/Consent to monitoring
Illegal Use

Network Access Policies:
It defines who can access the network, what they can access and how they access. Here, the principle of least privilege works where defining the permission based on role works

Password Policy
Data loss prevention Policy
Remote Access Policy

Mobile Deployment Models:

BYOD(Bring Your Own Device):

COBO(Corporate-Owned Business Only):
Owned by the corporate and issued to employees

COPE(Corporate-Owned Personally Enabled):
Similar to COBO but employees can install some whitelisted applications

CYOD(Choose Your Own Device):
Similar to COPE, but we can choose

Onboarding and Offboarding Policies:
There is a system in an organization which handles mobile devices called **Mobile Device Management(MDM)**. When any onboarding/offboarding happens, some of the devices might have to be registered and some have to be de-registered. This happens both manually and automatically depending upon MDM system

Enternally Imposed Policies:
These policies cover as to what kind of data is allowed to be carried onto a device. Several export control officers also do watch this thing

Adherence to Policies:
It is also important for an organization to adhere to its policies strictly

Change Management:
There is a dedicated team for change management, Change Management Team. There are two kinds of changes, one which is made by the organization and one which is understood by the people working and done upon their request. We are focusing on the latter

Initiating the Change:
A good change request will include the following

Type of Change:
Configuration Procedures:
What is it going to take, who will help and how long is it going to take

Rollback Process:
What is it going to take to roll-back to previous configuration

Potential Impact:
Impact, time, money, efficiency, perception, how will they be affected

Dealing with the Change Management Team:

Making the Change Happen:

Documenting the Change:
All the changes must be clearly documented

Updating SOP:
Standard Operating Procedures must be updated

Patching and Updates:

What Do We Update:
OS updates are the most common types of update. Since October of 2003, Microsoft has sent out patches that have been in development and are ready for deployment on the second Tuesday of the month. This has become known as **Patch Tuesday**. There are both scheduled patches and update-based patches

How to Patch:

Research:
Before patching, it is critical to search what is happening with the patch which has already been released.

Test:
Test, if possible on another system

Configuration Backups:
Backup is important

Tracking the updates is also good because sometimes we need to roll-back to the previous Patch.

Training:
Employees need to be trained on the IT resources

Security Policies:
Users need to read, understand and sign

Passwords:
Maintain complexity

Physical workplace and system security:
Not leaving written passwords, shredding off documents, reporting suspicious behaviors

Social engineering:
Recognize typical social-engineering and how to counter them

Malware:
Teach users to recognize malware attacks

Common Agreements:
When dealing with third-party vendors, there are basically five types of agreements

Service-Level Agreement(SLA):
It is a common agreement where services, equipment, tech support etc. are defined. For ex: an ISP might be providing services and defining their bandwidth, downtime, equipment they are providing, type of connection, troubleshooting support etc.

Memorandum of Understanding(MOU):
It is an agreement between two parties where the individual parties need to perform their duties mentioned in the MOU. For ex, suppose there is a fire in a hospital so if this generates an MOU, it would request for hospital in its surroundings to accept their patients for the time frame of their MOU

Multi-Source Agreement(MSA):
Companies agreeing on the fact that their hardware will be working with different components. For ex, an NIC manufacturer might claim that their NIC would be supportable with both Cisco and Juniper

Statement of Work(SOW):

It defines the services and products which vendor agrees to provide and the time frame for which they are going to provide

Nondisclosure Agreement(NDA):

Security Preparedness:

Security Risk Assessments:
To protect a company's asset, they have categorized aspects of risk assessments

Threat Assessment:
This is analyzing what's out there that could be a threat actor to an asset. It could be an employee, organization or even a nation state

Vulnerability Assessment:
Looking for vulnerabilities in the network. This could be done by running a vulnerability scanner. Popular vulnerability scanner tool is **NMAP(Network Mapper)**, can run on **Zenmap** GUI. More advanced ones are **Nessus, OpenVAS**

Note that vulnerability scanning is a part of vulnerability management

Penetration Testing:
Assigning a White-Hat to check for the exploits and vulnerabilities. Tools can be **Aircrack-ng** and **Metasploit**(Massive library of attacks)

Posture Assessment:
It covers the overall aspects to which the company is vulnerable including negative events like disasters and death of a personnel

Business Risk Assessments:
This is more focused on operations in the organization. This looks for overall risks faced by an organization

Process Assessment:
This involves assessing all the process in the company from manufacturing to sales. For ex: Looking for a new hire if he/she is vulnerable to the company in any way

Vendor Assessment:
Looking for potential risks from a vendor

Contingency Planning:
Contingency plans cover documentation about limiting the damage and recovering quickly afterwards. There are basically three different categories of these: **Incident Response(Damage), Disaster Recovery(Recoverable Damage) and Business Continuity(Recovering Damage Outside Organization)**

Incident Response:
Incident Response Team looks after it. Organizations have detailed incident response policies and plans

Disaster Recovery:
There is a disaster recovery team which looks after things like what kind of data can be backed up, how often backups should be made, making sure backups are available in case of emergencies

Network Device Backup/Restore:
A network devices have two things to be backed up, **Configuration Data and State Data**. Configuration looks after the settings like Router, Switch, Load Balancer, IDS/IPS etc. State Data includes things like Active Directory

Backup Plan Assessments:
A proper assessment of a backup plan records how much data might be lost and how long would it take to restore it. A **Recovery Point Objective(RPO)** defines how much lost data the organization can tolerate if it must restore from a backup point and this also decides how often the backups should be performed. Real-time backup is also a thing in servers. **Recovery Time Objective(RTO)** defines how long the organization can tolerate without system being restored. There are some of the terms

MTBF	**Mean time between failures:** how long it is going to take for a part to fail after one is failed

MTFF	**Mean time to failure:** how long the device is going to last in case of a failure
MTTR	**Mean time to repair:** The amount of time it takes to fix a system after it fails

Business Continuity:
This is dealt with Business Continuity Plan. There is a concept of backup sites, continuing the business at different sites. There are four different kind of sites

Cold Site:
It has all the infrastructure necessary to run a faulted site

Warm Site:
Similar to the Cold one but it make sure that the systems are functioning with loaded software and servers

Hot Site:
Similar to the Warm one but it also has a backup ready already which could be made ready pretty soon

Cloud Site:
A site available on the cloud with everything into place to run remotely as a backup

Forensics:
At the very basic, if we are the first responder, we can do the following

Secure the Area:
Document the Scene:
Collect Evidence:

Three top certifications are:

Certified Forensic Computer Examiner(CFCE)
Certified Computer Examiner(CCE)
GIAC Certified Forensic Analyst(GCFA)

19) Protecting Your Network

Saturday, November 30, 2024 7:23 PM

Security Concepts:

CIA(Confidentiality, Integrity and Availability):
Every security technique, practice and mechanism that is implemented to protect systems and data ensures at least one goat of the CIA

Confidentiality:
Integrity:
There shouldn't be any unauthorized modification, alteration, creation or deletion of data

Availability:
Ensuring systems and data are available for authorized users whenever needed. An extremely secure system that's not functional is not available in practice

Zero Trust:
Meaning that every resource should be treated as if it's hostile and proper authentication/authorization should be performed

Defense in Depth:
It says that the security posture should be designed with the assumption that every single defense can be beaten and also that every specific thing like physical security, network segmentation, separation of duties, strong passwords, patch management etc. should be considered very important

Separation of Duties:
It is about trying to identify what are the potential corners needed altogether to misuse and system and then separating those areas so that people alone cannot do anything

Network Threats:
It is the action of using vulnerabilities to harm a system. **CVE(Common Vulnerabilities and Exposures)** database holds a list of known vulnerabilities. **Exploit** is an actual procedure for taking advantage of a vulnerability whereas, **Attack** simply means trying to compromise CIA for an organization or its systems

Spoofing:
The process of pretending to be someone or something you are not. Not basically a threat but tool to make threats

MAC Spoofing
IP Spoofing: To make you think a packet come from somewhere
ARP Spoofing: To make you think a message is from a trusted source
E-mail Spoofing
Web Address Spoofing
Username Spoofing

DNS Poisoning: Poisoning a DNS cache to point clients to an evil web server. To prevent this, **DNSSEC(DNS Security Extension)** can be used

Packet/Protocol Abuse:
Using protocols in an improper way

NTP(Network Time Protocol)	This protocol is designed for each NTP server to correct its time by querying its peer servers. If a user puts the **ntpdc** command, it puts him in the interactive mode and later further queries can be made into that mode. One of the queries is **monlist**. This will list all the traffic which is going on between the queried NTP and its peers with a lot of other information A hacker can hit multiple NTP servers with the same command with a spoofed source IP. This will put the source IP into target with tons of requests and there would be a **DOS Attack**

	Further, this system can be compromised by hacker by putting **malformed packets** using **Scapy** tool

Zero-Day Attacks:
There are still a lot of vulnerabilities which are unknown in the market and get traded off in black-market

When a new vulnerability is discovered as an attack and given a very short amount of time to fix, this is termed as Zero-Day attack

Rogue Devices:
Tricking the clients in believing that the devices they are using are legitimate

DHCP Snooping:
It is a way of keeping the DHCP Servers safe from attack. This is usually enabled by Network Admins in a protected environment

DHCP Snooping	This creates a **DHCP Snooping Binding Database** of all the trusted ports and monitors the traffic on all untrusted ports. If someone tries to send untrusted DHCP Messages, the snooper identifies it and informs the client

RA-Guard:
It is similar to DHCP Snooping but well suited for **IPv6** networks. What it does is that it looks after the false **Router Advertisements** from untrusted ports

ARP Cache Poisoning:
This is the act of poisoning either the host's ARP cache or MAC Tables on Switches

ARP Cache Poisoning	In general, ARP enables any device any time to announce their MAC without first creating a request. Since ARP has no security, it enables anybody to create ARP Requests and Responses unstoppably. This way, an hacker can create a rogue ARP Broadcast claiming itself to be the router. Any software which isn't patched well and hears the ARP Request might try to respond to it. Once the system has been poisoned, it could be treated as a **Man-In-The-Middle** attack

Dynamic ARP Inspection(DAI):
This is a technology which makes the use of DHCP Snooping to protect a switch port. The DAI technology would look for the good-known IP and MAC Addresses in the **DHCP Snooping Binding Database**. If the ARP Information is untrusted it would be blocked right away and this is a good practice of **Switch Port Protection**. Another tool used for switch protection is **Flood Guards**

Denial of Service(DOS):
It is a targeted attack on a server with the goal of making that service unable to process anything. This is usually done when a particular service/weakness is unable to exploit. **Physical DOS** is attacking the server in-person

The main way to make a DOS work is by getting help from other users to make more requests. This is called a **DDOS(Distributed Denial Of Service)**. A single computer performing the attack is called **Zombie or Bot** and a group of these is called **Botnet**

Reflection is the method of spoofing target's IP Address as Source IP address and use it to aim at the target

Amplification is the process that comes under reflection and it focuses on sending very small requests to trigger a very big response

RUDY	**R U Dead Yet** attack is where the hacker tries to keep the target engaged for as long as possible until he is not done with his work
Deauth Attack	It is a form of DOS attack where wi-fi networks are targeted by creating a rogue access point. This connects the client to it and data is collected

DHCP Starvation Attack	When a DHCP client runs out of DHCP addresses after distributing all its leases, it is termed as **DHCP Scope Exhaustion**. An hacker intentionally does this to encourage clients to switch to a rogue DHCP server and this is called **DHCP Starvation Attack**
Unintentional Dos	When a DOS attack is unintentional, say the site literally gets super busy this is termed as **Slashdotting** or **Hug of Death**

On-Path Attack:
Also man-in-the-middle attack. This is usually done by ARP Poisoning or **SSID Spoofing**

Session Hijacking:
This is similar to man-in-the-middle attack but instead of listening to the ongoing traffic, the hacker tries to get the authentication information

Password Attacks:
The ways of discovering password

Brute Force:
Trying out password permutations and combinations

Dictionary:
Advanced form of Brute-Forcing

Physical/Local Access:

Insider Threats:
Malicious Employees

Trusted and Untrusted Users:
Sometimes an untrusted user is given some trusted permission which are intended to finish some work and it later becomes a threat to the organization

Malicious Users:
Sometimes users try to gain further access to the data by using packet sniffing

Packet Sniffing	Hackers try to gain access to the system by probing a user's ports as to which one is open which one is closed. The tool used can be **Nmap or Netcat**. Once an open port if found, the user might try to learn details about running services. This is called **Banner Grabbing**. For ex: A user might found an exposed SSH port, he can then connect to this port using SSH. Now, user can learn more about the product using SSH and take advantage of the vulnerabilities
Zombified IOT	In NIC devices, the first 24-bits of a MAC are vendor specific called **Organizationally Unique Identifier(OUI)**. A user in the organization might try to grab all these OUIs using common lookup tools and can perform several DDOS. For IOT devices, these attack can be termed as **Zombified IOT**

VLAN Hopping:
In this type of attack, the user in the VLAN tries to convince the switch by sending command in such a way that it wants itself to be treated as another switch and create a **Trunk Link**(connection between switches)

Administrative Access Control:
The admin accounts in Windows is **Administrator**, **Linux** and **MacOS** is **Root**

Unused Components and Devices:
Organizations make sure the proper use/destroy of unused items and resources

Malware:
It is a program designed to do something that is not good for the system

Crypto-malware/Ransomware:
Locking a user out of a system using cryptographic code and in-return asking for the cryptocurrency

Any form of malware which makes a user pay some amount is called **Ransomware**. The above can be termed as **Crypto-Ransomware**

Virus:
It is a type of malware which can do two things, **Replication and Activation**. Replication is when some executable file runs and the virus is attached to its end. Activation is like wiping out a drive or boot sector etc.

Worm:
A virus which actions in networks. Unlike virus, it doesn't need to get activated by anybody but gets to work as soon as the computer is connected to the network

Macro:
It is type of virus which works inside applications which run some kind of **macro programs**. For ex: A macro could be attached to an excel file and later, running that file can cause a big problem

Logic Bomb:
It is a form of code which is written to execute when certain conditions are met. For ex: A company has planted a logic bomb which would delete all the user files as soon as the user leaves the company

Trojan Horse:
It is a form of malware that pretends to do something else but deep inside it is doing something evil. It could be game or anything

Rootkit:
A rootkit is a type of malware which would make itself hide in the system in such a way that it is undetectable even to the best of anti-malware programs

Adware/Spyware:
Adware are the fake-looking ads on a website that would track websites we use often and based on them, prompt us to use deceptive-looking software/services/website in order to gain access

Spyware is a program installed in the system that would send the user's information over to the person controlling it. It could be keystrokes, contacts, list of software/services we are using etc.

Social Engineering:
Manipulating people to gain information like network login, credit card, company customer data etc. The most classic example if telephone scam

Phishing:

Shoulder Surfing:
Monitoring people while they are using passwords

Physical Intrusion:
Breaking into the server room etc.

Common Vulnerabilities:

Unnecessary Running Services:
Some of the services inside a system are not of any use so they should be disabled. Sometimes, the TCP/UDP ports are left open to listen but they are potentially the way for hackers to attack

Make sure that the ports are **not excessively blocked/filtered** because that would cause several network service issues inside the network

Unpatched/Legacy Systems:
Patching and Firmware Management should be done in order to make systems more secure. For the older systems inside the network, we can either isolate them with heavy firewalls or just completely remove if not used

Unencrypted Channels:
Using proper protocols for protection and not just getting insecure at several areas

Cleartext Credentials:
Make sure everything is well encrypted

RF Emanation:
TEMPSET are a set of technologies which allows to protect walls from **RF Emanation**

Hardening Your Network:
There are three aspects of hardening network security, Physical Security, Network Security and Host Security

Physical Security:

Prevention and Control:
Only giving the access to trusted personnel. **Tailgating** is coming through an open door without letting anybody know. **Piggybacking** is the same but the difference is that some authorized personnel help him in doing this intentionally

Smart Lockers:
Company assigning lockers via networking

Monitoring:
CCTV cameras can be used to watch for the people coming in and out of the building

Network Security:

Controlling User Accounts:
Controlling what users can and cannot do. **Improper Access** means though the user is authorized but he is accessing things in a different way

Edge:
These are the devices which are installed on like security doors, cameras etc. For security purpose and they are centrally managed

Posture Assessment:
Network Access Control(NAC) is a way of verifying that a node meets certain criteria before connecting to the network. However, Cisco also implements **Posture Assessment** as a part of NAC. Using this, it wants to check certain things for the connecting host like type and version of anti-malware, level of QoS, and type/version of operating system etc.

Persistent and Non-Persistent Agents:
Whenever a user is requested to respond to a posture assessment, the user answers this using an **Agent**. It is basically a program or piece of software in a computer which gathers all the information in a computer like configuration, assets, resources and then responds to the assessment accordingly. Now there are two different kind of Agents in a computer

Persistent Agent:
It is a basically an agent which is made when the computer **boots up**. It captures all the information as soon as booting up is finished. Though answers to posture assessment queries are made by Non-Persistent Agents but, when it is not available, node is permitted to respond with Persistent Agent

Non-Persistent Agents:
These types of agents are created for a temporary period of time and are made destroyed as soon as the work is done. **For ex:** a user might be connecting to the secure VPN. In this case, the user will try to search for queries at the other end. The endpoint device will then create an agent and made it available on the user computer. This will only create the answer to queries which are requested and as soon as the connection ends, the agents are made disappear

Network Segmentation:
This could be termed as creating separate parts in a network such that even when someone is trying to fiddle with the network, it could be separated or say make other systems safer. For ex: For a coffeeshop, the private wi-fi is separated from the public wi-fi

When someone in Guest Network is denied to get into the Private Network, he is kind of considered suspicious and got put into a **Quarantine Network**

Device Hardening:
Change default passwords, keep update, disabling unnecessary services, using secure network protocols, using QOS filter, **Control Plane Policy** helps in securing the control plane of the network devices

Host Security:
It is preventing dangerous things that users do like propagating to the rest of the network

Malware Prevention and Recovery:

Malware Prevention:
The symptoms of a malware can be seen early like some kind of wonkiness in the system. If our system doesn't let us Patch new updated, there could be a problem. It can also be seen if some configuration tool is showing Access Denied error

Symptoms of a Compromised System:
The most common is general sluggishness and random crash. Website might be redirecting and outgoing traffic would be spiking.

Top Talkers are systems with very high network output

Dealing with Malware:
Anti-malware programs, user awareness, patch management and remediation

Anti-Malware Programs:
A **Signature** is basically a coding pattern in which a Malware is written. Anti-Malware programs have a lot of existing signatures and they compare the executable files with these signatures and if they match, virus is detected

Also, these programs scan the **boot sector** of a system and compare it with a standard boot sector. If there's a change, it would reflect the viruses

Firewalls:
The most basic job of a firewall is to decide packets based on the rules of firewall whether to block or allow the inbound/outbound traffic

Types of Firewalls:

Software vs. Hardware Firewalls:
A **Hardware** firewall can be treated as the one which is installed in the networking device, it could be either Switch, Router anything. It is sometimes also referred as **SOHO Firewall**

A **Software** firewall is the one which is installed on the host computer. Ex is **Windows Defender Firewall**

Advanced Firewall Techniques and Features:
Stateful Inspection is a feature in firewall which would tell if the packet flowing is part of the current connection or no. Before we had **Stateless Inspection** but now it is upgraded

There is a kind of Firewall called **Application/Context Aware Firewall**. This works at OSI Layer 7 and filters according to the use of application/context. This is sometimes invaluable because services like BitTorrent run on **port-hopping**(changing ports dynamically) and hence the firewalls wouldn't be able to stop them.

There comes a **Next-Generation Firewall(NGFW)** which would work at multiple layers of the OSI Model and filters at individual layers. For ex: It would be filtering packets based on IP on layer 3, port numbers on layer 5 and protocols on layer 7

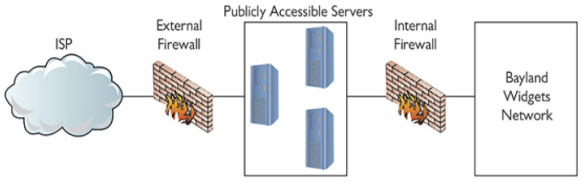
Web Filtering is filtering based on websites. **Content Filtering** is filtering based on signatures and keywords. **IP Filtering** is IP Add filtering. **Port Filtering** is blocking on specific ports

Implementing and Configuring Firewalls:

To protect the internal network from the external, **Cisco's Adaptive Security Appliance(ASA)** device can be used which comes with a hardware-based firewall. Some of the Routers and Switches comes with built-in ports for firewalls, it is similar to connecting other physical devices in the network

Restricting Access via ACLs:
Once we have configured our firewall physically, we need to defined what rules as to what kind of traffic is allowed and what kind of traffic is not allowed. For doing so, we define rules in the **Access Control List**. Certain rules need to be defined like whether it is for the outbound traffic or for the inbound traffic etc.

DMZ and Firewall Placement:
A Demilitarized Zone(DMZ) is basically a zone of network devices which are arranged in a special way for enhancing the security. Suppose our network has a web server which is accessible by the public. Since it is accessible by a lot of people, there could be chances of people getting into our network. In such cases we want to secure the network in a manner that though both the networks will have their individual firewalls but we want our systems to be completely secure or say some kind of enhanced firewall. Here, the picture of DMZ comes into play. It is also known as **Screened Subnet** or **Perimeter Network**. It would look something like this:



Honeypots and Honeynets:
To kill hackers time into accessing a system is what some of the network admins want. They want to increase the roadblocks and make it hard for them to enter into the system or network. Infact, sometimes admins want hackers to check their potential and intentionally challenge them to get into the system in order to check vulnerabilities and get reward

For the roadblock reasons, admins implement some kind of fake systems or say traps to get those hackers waste their time in those systems. These systems too fake, with fake data and everything. Such systems are called **Honeypots** and a collection of these systems or say a network is called a **Honeynet**. This is usually done either with network segmentation or running in virtual machines

Firewall Troubleshooting:
There could be incorrect ACL settings, misconfigured applications etc. We need to make sure if the rules assigned in ACL are working in order, especially for a newly installed Firewall.

Also, when we are talking about **network-based firewall**, we need to make sure that we are also checking is applications are being filtered well from the firewalls because sometimes these applications are treated as Protocols by these firewalls.

In case of an **host-based firewall**, though it is well aware of the applications and filters the inbound/outbound traffic. In some cases, the applications are accidentally listed in the ACL as Deny which we need to check

Sometimes when it is encountered that a certain Service/Port or Address is blocked, Firewalls could be checked

20) Network Monitoring

Sunday, December 01, 2024 5:51 PM

SNMP(Simple Network Management Protocol):
It is a network management protocol for **TCP/IP**

Components of SNMP:
It is basically made up of three main components **Managed Devices, SNMP Manager** and **SNMP Agent**

Managed Devices:
Printers, Workstations, etc

SNMP Agent:
Software which runs on managed devices

SNMP Manager:
Request and processes information from the agent software. Also known as **Network Management System(NMS)**

SNMP uses mainly 8 different kind of PDUs(Protocol Data Units) for querying and responding to the managed devices. Four of them are:

Get:
Sending **GetRequest** or **GetNextRequest** for the query

Response:
Agent responds to the query

Set:
If there needs a change in the query response, NMS sends **SetRequest**

Trap:
A trap is basically a notification/alert sent by the managed device irrespective of any query made

Net-SNMP package in Linux contains a command called **snmpwalk** which is for troubleshooting SNMP related issues. SNMP has three versions, SNMPv1, SNMPv2c and SNMPv3

NOTE that SNMP categorizes data using **MIB(Management Information Base)**, depending upon the type/format of data being queried

SNMP protocol is **UDP** on port **161 and 162**. With TLS, ports are **10162 and 10161**

Monitoring Tools:

Packet Sniffer:
A program that queries a NIC and stores all the captured packets in a file called **Capture File**. These programs can run on computers, dedicated hardware or routers etc. A packet sniffer is usually connected to a **mirrored port**

Protocol Analyzers:
It is a program for reading the **Capture File**. It performs **packet/traffic** analysis like IP and MAC of a packet etc.

NOTE: Filtering in Wireshark is a very good paying skill

NetFlow:
It is basically a tool for monitoring, developed by Cisco. It is based on the idea of the type of flow we want to track

- A **flow** is a sequence of packets from one specific place to another. These flow are stored in a **Flow Cache**

Top Talkers are the devices sending the most data and **Top Listeners** are the opposite

Sensors:
For controlling things like temperature, device/chassis etc.

Interface Monitors:
Tracks the bandwidth and utilization of ports in a network. Some of the terms that can be seen in a interface monitor are: Link State, Speed/Duplex, Send/Receive Traffic, CRC Errors, Protocol Packet and Byte Counts, Giants, Runts, Encapsulation Errors, Uptime/Downtime etc.

Performance Monitors:
It basically tracks the performance for some part of the OS like how much the web server is putting, etc. **Syslog** is a tool in Linux and **perfmon** is a tool in Windows

Logs:
These are basically the system log file to track performance

Baselines:
It is basically a baseline for as to how the optimal network should perform so that if networks breaks down or boosts up, the baseline could be compared

Log Management:
The log files should be secured and managed well. The protection and management of it is called **Log Management**

Log files are **cyclical**, means that if they grow to a certain size, the older ones are deleted. **Also, there are many laws according to which the log files should be kept for a certain period of time**

Putting It All Together:

Monitoring and Managing:
A centralized location for tech and admins to manage the network in an environment is called **NOC(Network Operations Center)**. Some of the tools used are **Cacti, Grafana, Zabbix, SolarWinds, etc.**

SIEM(Security Information and Event Managment):
It is basically a term used for calling out monitoring and management of network. It is made-up of two different processes, **SEM(Security Event Managment) and SIM(Security Information Management)**.

SEM:
It is the real-time monitoring of security events and saving them in a single viewing point say, a log file. What is also does is that it centralizes the other security monitors and event logs

SIM:
It reviews and analyzes log file things like file size, configuration values, content, credentials, hash values etc. Are seen as to what changes have been made and usually compared to the baseline. This is also known as **File Integrity Monitoring(FIM)**. These are either self-implemented or managed by an admin under contract by **Managed Security Service Provider(MSSP)**