SECURITY+ NOTES 3/1/23

Chapter 1 Mastering Security Basics

CIA security triad – Confidentiality, Integrity and availability – model used to guide an orgs security principles

Use case- a goal an org wants to achieve, clarifies requirements to reach the goal.

Elements of a use case – **actor** (person initiating a process), **precondition** (steps actor must take before), **trigger** (actor follows through), **postcondition** (actor finishes process alerting other depts), **normal flow** (shows the flow from beginning to end), **alternate flow** (actor deviates and changes course of process).

To maintain ***confidentiality***, you must ensure encryption of data by using access controls which restrict access

Access controls – **Identification** (users identity), **Authentication** (ie.. password), **Authorization** (limit access 2 user)

When data has unauthorized or unintended changes, the data has lost ***integrity*****.**

hashing techniques (a variation of SHA -Secure Hash Algorithm)- used to enforce integrity, sends a hash (fixed-length irreversible output ex.123) along with original message, if hash returns different (456) data has lost integrity, if returned the same (123), no data was changed.

MD5 – Message Digest 5 is a cryptographic algo that sends a hash fixed length and irreversible and can't re-create the original file

AES – Advanced Encryption System – is an encryption algo and can re-create original file by decrypting it

Availability – indicates both data and services are open when needed time and day, also ensure latest system updates to avoid software bugs.

Redundancy adds duplication to a critical system and provides **fault tolerance**. A goal is to remove a **SPOF** (**Single Point of Failure**) ex. If a server only have a single drive it's a SPOF, if it fails the entire system fails

Some ex. Include **disk redundancies** (all systems to operate if disk fails), **server redundancies** (failover cluster hops from one failed server to an operational server in the same cluster), **network redundancies** (use multiple servers to support a single service (NIC – network interface card teaming) provides both redundancy support and bandwidth, **power redundancies** (uninterruptible power supplies UPSs – provides power when commercial power fails such as generators).

Scalability – manually scaling a static system up or out taking 16GB RAM – Random Access Memory to 32GB for ex.

Elasticity – scaling up or out a dynamic system using elasticity, able to increase/decrease as needed when demand rises or lowers

Resiliency – regularly testing faults and redundancies (ie disk, backups, NICs, UPSs, failover servers) for failures

M.O.T. control categories – **security controls Managerial** (documented written policy), **Operational** (performed in day-to-day operations), **Technical** (implemented with tech).

IDSs – Intrusion Detection Systems – monitor a network or host for intrusions and provide protection to threats

IPSs – Intrusion Prevention Systems - monitor a network or host for intrusions and provide protection to threats. IPSs can detect DoS (denial-of-service) attacks and auto blocks the ICMP ping traffic

Least Privilege -users are only granted the privileges to perform their assigned tasks or function, but no more.

Tech controls use tech to reduce vulnerabilities. Some ex include encryption, IDSs, IDPs, least privilege, firewalls, antivirus software.

Control types – preventive, detective, physical, deterrent, compensating, response controls etc.

Change mgmt. helps prevent outages from config changes.

Ping – basic command testing connectivity for remote systems (ping -t pings a specific host until stopped on windows), (ping -c on linux same count) – used to verify name resolution is working

Pinging a host name to check name resolution shows that a hostname is up and operational.

ICMP – Internet Control Message Protocol -are echo packets that communicate to and from systems when pinging.

DDoS –Distributed Denial-of-service – attacks that attempt to disrupt services and internet-based systems. One way to block them is by configuring a firewall to block ICMP traffic or block echo requests.

Hping – another command to detect if firewalls are blocking ICMP traffic using TCP UDP and ICMP (Linux sys only)

Ipconfig – (WINDOWS) shows TCP/IP config info, such as MAC, subnet mask, default gateway, IP addy, DNS addy

Ifconfig –(Linux) shows NIC properties and allow configuring of NIC, shows more thorough TCP/IP config info

Ipconfig /all and ifconfig -a – command shows comprehensive list of TCP/IP config info for each NIC, DHCP addy 2

Many attacks establish connections from an infected PC to a remote PC.

Netstat – (network statistics) – views stats for tcp/ip protocols on a system, view active network connections

Netstat– shows a full listing of all open TCP connections | **Netstat -a** – list all TCP & UDP ports sys listening on

UDP – User Datagram Protocol

Sockets – an IP addy followed by a colon and the port #. EXAMP. **192.23.1.32:80**

Tracert (W) /traceroute (L) -command lists all the routers (aka hops) between two systems. Shows both IP and sometimes the hostname for each hop. Can be used to identify modified paths.

Pathping – command act as both tracert and ping, it first finds all hops, ping then sends pings to each hop and **computes stats based on the # of responses by 25 seconds**

arp (W -a shows cache) (L shows cache)– command used to view and manipulate the ARP (Address Resolution Protocol) cache

dig (L) - command used to query the Domain Naming Service (DNS) system

cat (concatenate) – command used to display the contents of files, also make copies, and merge multiple files

sudo (super user do) – allows you to run a command with root (elevated privileges) EX. sudo cat/var/log/auth.log

(|) pipe command – allows one command to be sent to another command (**more**) displaying pages individually

grep (globally search a regular expression and print) – used to search for a specific string or pattern within a file. EX. sudo grep "authentication failure"/var/log/auth.log – this will show only entries with the text "auth failure"

head – command allows you to only see the beginning of a file (1st 10 lines of a file) and allow you to verify that the syslog file is being rotated successfully. **One of the first log entries when ran is: logrotate.service has succeeded** EX. sudo head /var/log/syslog

tail – command allows you to only see the ending of a file (last 10 lines of a file) EX. sudo tail/var/log/messages

If you would like to look at a specific # of lines of a file, can use the switch -n xx (number you require). EX. sudo tail -n 15 /var/log/messages Same with head: sudo head -n 21 /var/log/messages

logger – command allows you to add entries in the /var/log/syslog file from the terminal Ex. logger Backup started -gives you a timestamped entry with the text of "Backup started"

journalctl – command displays log entries from several sources displaying the data in text format. To limit output term the command around your parameters. EX. journalctl -- since 30 minutes ago. Can also use to view previous boot entries Ex. journalctl -- list boots to redirect place > (file name) at the end of the command

chmod (change mode) – used to modify permissions on Linux system files and folders. EX. chmod 760 filename. Also possible to can assign permissions using the text method u-file owner g=group owner o=all others EX. chmod g=r filename to remove use (switch –) Ex chmod u-r filename

Windows logs – Security, System, & Application logs

Network logs -logs traffic on the net. Can be manipulated to log specific info like logs of all traffic that passes through/blocked or both. **Entries usually return data including the: host, user-identifier, authuser, date, request, status, & bytes.**

SIEM – **Security Information and Event Mgmt** systems – used to detect trends and raise alerts in real time, analyses past alerts from multiple sources. Centralized logging - can check logs on all devices within a network.

SIEM capabilities – **Log collectors** (collects data), **Data inputs** (logs entries from various sources), **Log aggregation** (combines dissimilar items into a single similar format), **Correlation engine** (collect/analyze event log data from various sources), **Reports** (built-in reports about devices), Packet capture (aka sniffers catch net traffic for view/analyzing individual packets), **User behavior analysis** (UBA focuses on user activity who, what, when was files accessed or apps launched**), Sentiment analysis** (analyzation of text to detect an opinion or emotion, AI analyzes UBA to observer unwanted behavior), **Security monitoring** (alerts of suspicious events and monitors), **Automated triggers** (cause an action in response to a predefined number of repeated events. 5x pw example), **Time synchronization** (data sent from servers are all synched, for investigating purposes incidents are timestamped centrally), **Event deduplication** (removes duplicate entries, 10 users receive same email, deduplication allows the saving of one copy while giving all 10 users access), **Logs/WORM** (write once read many -method preventing anyone from modifying log entries).

SIEM elements – **Sensors -**agents placed on systems throughout a net to collect logs and send to SIEM system**, Alerts -** notifications sent when the event fires**, Sensitivity –** limits false positives while avoiding false negatives one wrong pw vs 100 wrong pw in 5 minutes**, Correlation -**log data is analyzed/correlated, and displayed as needed**, Trends –** while data analyzes trends can be detected Ex. High rate of login failures can be identified and raise an alert. Some SIEM display trends in graphs allowing analysis in a single pic.

Syslog protocol only defines how to format the syslog messages and send them to a collector. But doesn't define how the syslog handles these log entries.

TLS – Transport Layer Security – provides encryption on sent syslog messages when **TCP** (Transmission Control Protocol) ensures the packets arrive

Syslog-ng (open source software utility) – extends syslogd allowing the collection of logs fromo any source and correlates and routes logs to any log analysis tool. Supports both TLS & TCP

Rsyslog – new and improved syslog-ng – can also send logs directly into database engines

NXLog – supports both W & L functions as a log collector & can be integrated w/ most SIEM systems they're 2 vzns

NXLog Community Edition & NXLog Enterprise Edition

LINUX LOGS : var/log/ : **syslog –** stores all sys activity**, messages -**variety of general system messages ie startup, mail, kernel ect.**, boot.log –** logs created when system boots**, faillog -**failed login attempts**, kern.log -**info logged by system Kernal (aka central part of linux)**, httpd/ -** view access and error logs in directory, **auth.log** -info related to successful & unsuccessful logins.

Chapter 2 Understanding Identity and Access Mgmt

W/o authentication you can't identify a user. At least 2 entities know the credentials: the user with the credentials and the authenticator that verifies the credentials.

Ex. Zoey knows her user & pw so does the authenticating server. Zoey presents her credentials to the authenticating server, and the server authenticates her.

Authentication isn't limited to users: services, processes, workstations, servers, & network devices use to identify 2

Authentication, authorization & Accounting (AAA) – work together with identification to provide a comprehensive access mgmt system

Authorization – grants access to resources based on users proven identity Ex. granting user access to read data
Access control systems -include multiple security controls to ensure that users can access resources they're authorized to use, but no more.

Accounting – methods track user activity and record the activity in logs Ex audit logs track activity & admin use to create an audit trail

Audit trail – allows security professionals to re-create the events that preceded a security incident

Authentication factors:

- Something you know – pw/pin
- Something you have – token/phone/smart card
- Something you are – fingerprint/biometric

Static codes – aka passwords (because they stay the same for a long time)

Microsoft NIST & US DHS pw recommendations:

Hash all pws	Tell users not to use the same work pw anywhere else
Don't require mandatory pw resets	All special characters not req'n them, including spaces
Require pws to be at least 8 characters	Require multifactor authentication
Check for common pws and prevent their use	

A complex password uses multiple character types, such as yT7!

The **CSF** (Common Security Framework) recommends pws to be at least 15 characters long and changed every 90 days

Longer pws using more character types are more secure than short pw of 4–5-character, longer pw isn't always stronger if not complex Ex. 1234567890 – easy to guess

Maximum pw age – when a user doesn't reset their pw before the expiration Ex. 60 day expiration

Pw history system remembers the last 24 pws and prevents users from reusing them until they've used 24 new pw

Its common to use the minimum pw age setting of 1 day, and pw history set to 24. Ex. User must wait until a day has passed and will take 24 days of new pw creation before they can reuse an old pw.

Knowledge Based Authentication (KBA) -used to prove the identity of individuals. 2 types: Static & Dynamic

Static KBA -used to verify identity when pw is forgotten Ex. Security questions: What's your fav color?

Dynamic KBA -identifies users w/o an account, use for high-risk transactions like financial institution or health care company. Queries public/private data sources such as credit reports or 3rd party to craft multiple choice questions that only user would know Ex. Which address resonates? 123 Craft Street, 2433 Cantor Ave, 224 Hog Road

Account lockout policies thwart some pw attacks, such as brute force attacks and dictionary attacks.

Smart cards – have an embedded chip and a certificate, once inserted into a card reader its info is read, including details from the certificate – they use dual factor authentication

Certificates – digital files that support cryptography for increased security.

Embedded certificate – are included in smart cards they hold a user's private key (user specific) that's matched with a private key

Public Key Infrastructure (**PKI**) - supports issuing and managing certificates

HMAC – Hash based Message Authentication Code -a # created with a hashing algorithm

HTOP (HMAC One-time password) – creates a code based on cryptography for one time use only doesn't expire until used

TOTP (Time-based One-time password) – creates a pw that expires every 30 secs – used as software tokens for auth

3rd factor of authentication (something you are) is the strongest individual auth factor, it includes: **fingerprints, palm veins, retina scans, iris scans, voice recognition, facial recognition, & gait analysis**

Iris & retina scan are the strongest biometric methods, though Iris is used instead being less intrusive and doesn't reveal private medical issues. Facial and gait analysis can bypass the enrollment process when used for identification instead of authentication Ex. entering a Casino/airport, facial recognition can scan faces and gait analysis of you and others walking around and match it to other databases.

Crossover error rate (CER) – is the point where the FAR crosses over with the FRR

CACs (Common Access Cards) PIVs (Private Identity Verification) used to enter secure places and getting in/out of buildings

Authentication Attributes – somewhere you are (location identification), something you can do (picture passwords), something you exhibit (badges, employee ID), someone you know (google add-ons to check site safety)

Privileged Access Management (PAM) – systems implement stringent security controls over accounts w elevated privileges such as admin/root-level accounts. Some capabilities include: allow authorized users access to admin account w/o knowing pw, logging/monitoring all elevated privileges usage, and auto changing the admin account pw.

Requiring an admin to have 2 accounts, one for regular use and the other with elevated privileges, prevents privilege escalation attacks. Users should not use shared accounts.

Usage auditing records user activity in logs. A usage auditing review looks at the logs to see what users are doing and it can re-create an audit trail. Permission auditing reviews help ensure users have only the access they need and no more and can detect privilege creep issues.

Single Sign-On (SSO) – refers to a user's ability to log on once and access multiple systems w/o logging on again. Kerberos includes SSO capabilities in networks.

Kerberos – is a network authentication mechanism used within a MSFT Windows Active Directory domain or a Unix realm - to help prevent on-path attacks (aka man-in-the-middle attacks) and uses tickets to help prevent replay attacks. Uses UDP port 88. Its requirements include:

- **Key Distribution Center (KDC) or (TGT Server) Ticket-Granting Ticket –** a method of issuing tickets used for authentication
- **Time synchronization** -all systems to be link within 5 mins of each other enabling tickets to expire correctly – generally have a lifetime of 10 hours
- **A database of users** – in MSFT this is the Active directory but could be any database of subjects.

Federation – uses a federated identity mgmt. system to treat two identities as one using a SSO, assuming both parties agree on a standard

SAML Security Assertion Markup Language – uses a federated identity mgmt. system when two identities trust each other and doesn't need add'l auth after the initial sign on. Is an **Extensible Markup Language XML**-based standard used to exchange auth and authorization info between different parties. It provides SSO for web-based apps. It defines 3 roles.

1. Principal – usually person loggin on to use the service/resources
2. Identity provider (IdP) – creates/maintain/manages identity info for principal – (either party or a 3rd party)
3. Service Provider – service being provide to the principals (the party who's providing the actual services)

OAuth –(open authorization) an open standard for authorization – a link between two companies Ex. Paypal being integrated with Amazon, once you shop you logon with your paypal account to make the purchase. OAuth transfer data between themselves and Amzn ie money and address details. Customer doesn't have to create a new logon acct.

OpenID Connection (OIDC) – uses JSON (JavaScript Object Notation) web token JWT an ID token – where apps grant logins based on already existing account Ex. Google accounts can be used to login to other web based apps.

Access control schemes:

Role-Based access control scheme - Example would be MSFT Project Server – can host many projects managed by diff PMs, Such as the 4 roles below:

Role-BAC -admin, exec, PMs, team member	**Mandatory Access Control (MAC) –** use labels to determine access - all permissions are granted by admins, they match subjects with objects. Ex. Lattice of Labels show levels of security: TS, S, C etc. only S can access S, and lower levels on a "Need to Know" basis. Also, other labels within the same level if Need to know.
Rule-BAC – based on approved instructions like (ACL)	
Discretionary Access Control (DAC) – every object has an owner, and owner has full explicit control of the object. Ex. MFST NFTS (New Technology File System) uses the DAC system- allow admin and users to restrict access to files/folders. File system permissions: Write, Read, Read & Execute, Modify, Full Control.	**Attribute-BAC** -evaluates attributes and grants access based on the value of them. Ex. employee, researcher, nuclear-aware. Can enforce both DAC & MAC schemes: User can create policies to grant access, and use attributes to match subject to object giving access Commonly used in **Software-Defined Networks (SDNs)**

A matrix is a planning doc that matches the roles w the req'd privileges.

Some **rule-BACs** systems use rules that trigger in response to an event, such as modifying access control lists after an attack or granting permissions to a user in certain situations. Ex. IDP system detects an attack and auto modifies rule to prevent future attacks, similarly, extending permissions to a user of database when another subject is absent.

The **MAC Mandatory Access Control scheme** uses sensitivity labels for users and data. It's commonly used when access needs to be restricted based on a need to know. Sensitivity labels often reflect classification levels of data and clearances granted to individuals.

Conditional Access – MSFT implemented within Azure directory environments – requires users to log on with MFA to access sensitive documents. Ensures MFA otherwise access is blocked. Use signals/attributes to block access, for instance:

- User or group membership – may have access if part of a group, but no one else
- IP location – only specific IP address have access, can block entire countries/regions
- Device – can allow on desktop and deny on mobile

Chapter 3 Exploring Network Technologies & Tools

Sniffing attack – attacks using a protocol analyzer to capture data sent over a network in cleartext

Denial-of-service (DoS) – a service attack from a single source attempting to disrupt the service of another system

Distributed DoS (DDoS) – multiple computers attacking a single target

Poisoning attack – attacks attempting to corrupt the cache w diff data.

Open Systems Interconnection (OSI) model – the Data link layer responsible for ensuring data is transmitted to specific devices on the net. Formats data into frames & adds a header that includes MAC address for the source & destination devices.

Layer 2 attacks attempt to exploit vulnerabilities in MAC addressing and ARP

TCP/IP is a full suite of protocols. HTTP default port is 80.

TCP – provides connection-oriented traffic (guaranteed delivery) using a 3-way handshake. Sends a **SYN** packet > server responds with a **SYN/ACK** packet > client completes 3rd part of handshake with an **ACK** packet to establish connection	**UDP** – provides a connectionless session (w/o 3-way handshake) makes best effort to deliver traffic w/o using extra traffic to ensure delivery. Many net-based DoS attacks use UDP
IP – finds hosts in a TCP/IP net and delivers traffic from one host to another using IP addresses. IPv4 uses 32 bit addresses like 192.168.1.100 IPv6 uses 128-bit addresses in 8 groups of 4 hexadecimal code separated by colons like FE80:0000:0000:0000:20D4:3FF7:003F:DE62	**ICMP** – Internet Control Message Protocol -used for testing basic connectivity. Many DoS attacks use ICMP so its common to block ICMP in firewalls disabling the ping response Blocking ICMP prevents attackers from discovering devices in a net.
ARP Address Resolution Protocol– resolves IPv4 addresses to MAC addresses. TCP/IP uses IP address to get a packet to a destination net, then the MAC to get it to the correct host. ARP is required once the packet reaches the destination subnet.	

VOICE & VIDEO USE CASE

Real-time Transport Protocol (RTP) – delivers audio/video over IP networks such as VoIP comms, streaming media/video teleconferencing

Secure Real-Time Transport Protocol (SRTP) – provides encryption, authentication and integrity for RTP, protects confidentiality of data while ensuring data transmissions' integrity.

Session Initiation Protocol (SIP) – used to initiate, maintain, and terminate voice, video/messaging sessions. Uses request/response messages when est. a session captured in text and easy to read. SIP est. connection, RTP/SRTP transports the audio/video. SIP log files show time, sender IP/recipient IP. Can be useful in an investigation when combined with VoIP log files.

FILE TRANSFER USE CASE

File Transfer Protocol (FTP) – uploads/downloads large files in cleartext to/from a FTP server. FTP active mode use TCP port 21 for control signals and TCP port 20 for data, similarly in passive mode (PASV), but FTP uses random port for data in PASV.

Trivial File Transfer Protocol (TFTP) – uses UDP port 69 used to transfer smaller amounts of data. Non-essential, commonly disabled by admin.

Secure Shell (SSH) encrypts traffic over TCP port 22 & is used to transfer encrypted files over a net. **Transport Layer Security (TLS)** is **Secure Sockets Layer (SSL)** (Deprecated/obsolete) replacement & used to encrypt many diff protocols, including browser-based connections using HTTPS. **Secure FTP (SFTP)** uses SSH & **FTP Secure (FTPS)** uses TLS to encrypt traffic.

Internet Protocol security (IPsec) – encrypts IP traffic, it encloses IP packet payloads by using Tunnel mode to protect VPN traffic. Includes 2 components: Authentication Header (AH) p-ID 51 and Encapsulation Security Payload (ESP) p-ID 50.

STARTTLS – a command used to upgrade an unencrypted connection to an encrypted connection on the same port

EMAIL & WEB USE CASES

Simple Mail Transfer Protocol (SMTP) – sends emails between clients & SMTP servers. TCP port 25 for unencrypted & port 587 for encrypted. Can also use STARTTLS for secure connection.

Post Office Protocol v3 (POP3) – sends emails from servers down to clients using port 110 for unencrypt and 995 for encrypt

Internet Message Access Protocol v4 (IMAP4) – used to store email on an email server & organize/manage such as Google mail. Port 143 for unencrypt and 993 for encrypt. **SMTP, POP3, & IMAP4 are primary email protocols.**

HTTP & HTTPS use ports 80 & 443, respectively. Most browsers now use HTTPS over HTTP

Directory services, such as Microsoft Active Directory Domain Service (AD DS), provide authentication services for a net. AD DS uses LDAP, encrypted w TLS when querying the directory.

Lightweight Directory Access Protocol (LDAP) – specifies the formats & methods used to query directories. LDAPS encrypts data w TLS using port 636. Used to communicate btwn directories

REMOTE ACCESS USE CASE

Admins connect to servers remotely using protocols such as SSH & **Remote Desktop Protocol (RDP**). Some admins use VPNs to connect to remote systems. Uses port 3389 for TCP & UDP.

OpenSSH is a suite of tools that simplify the use of SSH to connect to remote servers securely. The ssh-keygen command creates a public/private key pair, and the ssh-copy-id command copies the public key to a remote server. The private key should always stay private.

TIME SYNCHRONIZATION USE CASE

Network Time Protocol (NTP) – time synchronization - allows systems to synch their time within tens of milliseconds.

Simple Net Time Protocol (SNTP) – used for time synch but isn't as complex as NTP which uses algorithms & queries multiple time servers to identify the most accurate time.

NETWORK ADDRESS ALLOCATION USE CASE

Dynamic Host Configuration Protocol (DHCP) – dynamically assign IP addresses to hosts, also assigns other TCP/IP info such as subnet masks, default gateways, DNS server addy, etc.

3 private address ranges that should be allocated within a private network:

1. 10.x.y.z – 10.255.255.255
2. 172.16.x.y – 172.31.255.255
3. 192.168.y.z – 192.168.255.255

DHCP Snooping – preventive measure to prevent unauthorized DHCP servers from operating on a net. Enabled on Layer 2 switch ports.

DHCP clients/servers normally send **4** packets back/forth: DHCP **Discover/Offer/Request/Acknowledge DORA**

DOMAIN NAME RESOLUTION USE CASE

DNS - is for domain name resolution. Their servers host data in zones (Databases) including multiple records like:

A -host record- holds hostname & IPv4 address – commonly used	AAAA – holds hostname & IPv6 addy like A but for v6	PTR –(pointer rec'd) opposite of A rec'd – queries DNS w/ IP addy
MX – (mail exchange) identifies a mail server used for EM – when more than 1 mail server, one w/ lowest pref # is primary mail server	CNAME –(canonical name) alias – allows single sys to have mult names assoc w/single IP addy	SOA (start of Authority) –info about the DNS zone & its settings. TTL (Time To Live) tells how long to cache DNS result in secs

DNS uses TCP port 53 for zone transfers and UDP port 53 for DNS client queries.

DNS Cache Poisoning – attackers modify the DNS cache (A or AAAA rec'd) with a bogus IP addy sending users to a malicious site IP addy. **DNSSEC** adds a Resource Record Signature (RRSIG), which provides integrity & authentication & helps prevent DNS poisoning attacks.

Nslookup (name server lookup) & dig (domain info groper) – command line tools used test and to troubleshoot problems related to DNS. Usually, to find host names and domain name. MSFT includes nslookup and Linux includes dig. They can be used to query specific records like mail servers

SUBSCRIPTION SERVICES USE CASE

QoS (Quality of Service) allows admins to set the priority of any traffic.

Net devices primary methods of IPv4 when addressing TCP/IP: **Unicast** (1-to-1 traffic) & **Broadcast** (1-to-All traffic)

Switch – can learn which pcs are attached to each of its physical ports. They internally switch unicast traffic, but pass broadcast traffic to all ports. Doesn't send packets to other ports as opposed to hubs.

Port security and MAC filtering – both are security methods to prevent attackers from networking hacks by disable unused ports and only allowing pcs/server to communicate with saved MAC addresses

Spanning Tree Protocol (STP) & Rapid STP (RSTP) – provide broadcast storm prevention and loop prevention for switches. This is looping protection. Looping happens when two ports of a switch are connected.

STP sends **Bridge Protocol Data Unit (BPDU) Guard** messages to detect loops, if found STP blocks traffic from switch ports.

Edge port is a switch port connected to a device such as a PC/server/printer.

A logical port is a # embedded in a packet in a packet and identifies services and protocols.

Router & stateless firewalls (or packet-filtering firewalls) perform basic filtering with an access control list (**ACL**). ACLs identify what traffic is allowed and what traffic is blocked. ACL can control traffic based on nets, subnets, IP, ports & some protocols. **Implicit deny** blocks all access that has not been explicitly granted. Routers and **firewalls** use implicit deny as the last rule in the access control list.

Host- based firewalls provide protection for individual hosts, such as servers or workstations. A **host-based firewall** provides intrusion protection for the host. Linux sys support xtables for firewall capabilities. **Net-based firewalls** are often dedicated to servers and provide protection for the net.

Firewalls use a ***deny any any***, ***deny any***, or a ***drop all*** statement at the end of the ACL to enforce an implicit deny strategy. The statement forces the firewall to block any traffic not previously allowed by ACL. The implicit deny strategy provides a secure starting point for a firewall.

Stateless firewall – use rules in ACLs to identify allowed/blocked traffic and a **Stateful firewall** – inspects traffic and makes decisions based on the state of the session and blocks if suspicious. **Web App Firewall** (WAF) – provide strong protection for web servers, they protect against several different types of attacks, focusing on web app attacks.

Next Generation Firewall (NGFW) – build on stateless/stateful firewalls in that there are improvements with added capabilities not available in the pervious firewalls. Performs deep-packet inspections, adding app-level inspection as a core feature, can also detect malicious traffic by identifying app commands.

A **screened subnet** (aka DMZ demilitarized zone) is a buffer zone btwn the internet and the internal net. It allows access to services while segmenting access to the internal net. In other words, Internet clients can access the services hosted on servers in the screened subnet, but the screened subnet provides a layer of protection for the intranet (internal network).

Network Address Translation (NAT) – translates public IP addys to private IP addys and private IP addys back to public. A common form of NAT is Port Addy Translation (PAT). **Dynamic NAT** uses multiple public IP address, while **static NAT** uses a single public IP addy.

An **air gap** isolates one net from another by ensuring there is physical space (literally a gap of air) btwn all sys & cables

Virtual Local Area Network (VLAN) – used to separate or segment traffic on physical nets and multiple can be created on a single switch. VLAN can group several different PCs together or separate w/o regards to their physical location. Used to separate traffic types such as voice & data placing them on their own VLAN.

Proxy server – forwards requests for services from a client. It provides caching to improve performance and reduce Internet bandwidth usage. **Transparent proxy** servers accept and forward requests w/o modifying them. **Non-transparent proxy servers** are URL filters/modifies to restrict access to certain sites. Both types can log user activity.

Unified Threat Mgmt (UTM) – appliance combines multiple security controls into a single appliance. Can inspect data streams and often include URL filtering, malware inspection, & content inspection components. Many UTMs include a DDoS mitigator to block DDoS attacks.

Jump Server – server placed btwn different security zones & provide secure access from devices in one zone to devices in another zone. It can provide secure access to devices in a screened subnet from an internal network.

Secure Network Mgmt Protocol (SNMPv3) – used by admins to manage & monitor network devices & use notification messages known as traps. SNMP uses UDP 161 & 162. **SNMPV3 encrypts credentials before sending them over the network & is more secure than earlier versions**.