Network: 2 or more computers linked together to share data, information, or resources. 2 basic types of networks:

1. Local area network (LAN): within a single floor/building
2. Wide Area network (WAN): wide distance between geographical remote areas

Network devices:

1. Hub: connect divices. Not as smark as switches/routers. More common in homes than business setting
2. Switch: aka intelligent hub. Knows the address of devices connected to it and routes data directly to the devices rather than broadcasting. Not as smark at routers though.
3. Router: connects devices and they can be either wired/wireless. Determines most efficient route to flow across the network
4. Firewall: lets things get in or out
5. Server: provides information for client systems
6. Endpoint: beginning or end of a network (can be a server or a client)

Terms:

1. VLAN: groups of devices that appear to be in the same geographical area but they are not
2. Ethernet: standard that specify how data transmitted across cables are formatted
3. Device address:
   1. MAC (Media Access Control): unique to every device. First 3 bytes indicates vendor.
   2. Internet Protocol (IP): the address of the network

Network layers (sample segregation):

1. Upper layer (application/host): made up of application, presesentaion and session layers. Controls the integrity of a connection and establish and maintains a session.
2. Lower layer (media/transport): made up transport, network, data link and physical layer. Gets data from other physical connection, converts the data into frames. Frames are converted into packets by adding route data

OSI (Open System interconnection):

1. is an abstract model that specifies an ideal connection on an ideal computer.
2. Made of up 7 layers. The layers are referenced by either name or layer number. Layers are Application <- Presentation <- Session (Logical ports eg. NetBIOS will reside here)<- Transport (TCP/UDP will reside here) <- Network (routers sending packets will reside here) <- Data Link (switches, bridges, or WAPs sending frames will reside here)<- Physical
3. Layers 5-7 are called data.
4. Encapsulation (adding a header and footer to the data) happens at each level. What data is moving out, encapsulation starts at the upper level and more items are added as it moves to the lower levels. The inverse happens as data moves to higher level. This process is called de-encapsulation or decapsulation

TCP/IP:

1. Most commonly used protocol. Developed in the late 1970s
2. Made up of different protocols and is platform dependent
3. Made up of 4 layers:
   1. Application: defines protocol for the transport layer. Includes Telnet, File Transfer Protocol (FTP), Simple Mail Transport Protocol (SMTP), Doman Name Service (DNS). Corresponds to the application, presentation, and session layer of of the OSI model
   2. Transport: permit data to move among devices. Includes TCP(a full-duplex connection-oriented protol) and UDP (a simplex connectionless protocol).
   3. Internet: creates/inserts packages. Includes Internet Control Message Protocol (ICMP, used to determine the health of a network or specific link. Utilized by ping, traceroute etc. ping uses ICMP echo packets and bounce then off remote systems. Thus you can use ping to determine if the remote system is online)
   4. Network interface: how data moves across networks
4. Consumes a lot of resources and easy to hack because it was designed for ease of use rather than security

Internet Protocol (IPv4 and IPv6):

1. IP current exists in 2 version, IPv4, IPv6
2. IPv4:
   1. is a 32-bit address spaces which was projected to tbe exhausted by the late 1980s
   2. divided into 4 octets divided by a dot.
   3. Each octet has values ranging from 0 to 255 (0 is the network itself, not for any devices. 255 is reserved for broadcasting)
   4. The address is divided into 2 (network number and host)
   5. The network number is assigned by external organization eg. ICANN (Internet Corporation for Assigned Names and Numbers) and represents the organization’s network. It typically divided into subnets. A subnet maks is used to define the part of the addresss used for the subnet
   6. The host represents the network interface within the network
   7. It was later divided into public and private ranges. Private address can be shared by people living in a street for example.
   8. Private addresss groups are also established. For example every SOHO (Small Office, Home Office) uses 192.168.2.xxxx in its interal network without fear that some other system can intercept traffic on their LAN
   9. IPs available for everyone; 10.0.0.0 to 10.255.255.254,  172.16.0.0 to 172.31.255.254, and  192.168.0.0 to 192.168.255.254
   10. The first octed of 127b is reserved ofr a computers loopback (used for self-diagnosis and troubleshooting at the machine level) address (127.0.0.1 is commonly used). This helps a network administrator to treat a local machine as it it were a remote machine and ping the network interface to establish whether it is operational.
3. IPv6:
   1. was introducted in 1995 and provides a 128-bit address pace along with several other important features (so more space than IPv4)
   2. Improved security: IPsec was optional in IPv4 but mandatory in IPv6. This ensures confidentiality and integrity and help systems authenticate each other.
   3. Improved Quality of Service (QoS): helps services get an appropriate share fo a network’s bandwidth
   4. Displayed as 8 groups of 4 digits and it is represented in hex. Every group ranges from 0000-ffff and are separated by columns.
   5. Example : 2001:0db8:0000:0000:0000:ffff:0000:0001. Groups beginign with zeros can have the zeros removed to shorten it. Therefore, above can be represented as 2001:db8::ffff:0:1
   6. Reserved ranges: :1 (is the local loopback address, used the same as 127.0.0.1 in IPv4), 2001:db8:: to 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff (is reserved for documentation use), fc00:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff (are addresses reserved for internal network use and are not routable on the internet)

In a home setting, the router, firewall and network switch are all bundled into 1 device. In an org however, they are separated

Firewall can be a hardware or software

Wifi:

1. Provice connection without wires. They have ranges. But can be extended using wifi ranges.
2. It is less safe than LAN cables because attack can be done from a distance

Example of attacks:

1. DoS/DDoS ((Distributed)-Denial-of-service): consumption attack that has the primary goal of preventing legitimate activity on victimized system. DDoS (multiple systems (botnets) will be conducting the attacks)
2. Fragment attack: traffic is fragmented in such a way that the system wll not be able to put everything together back again
3. Oversized packet attack: make systems to fail by sending oversized packages
4. Spoofing attack: Faking the sending of address of a transmission to gain illegal entry to a secure system
5. Man-in-the-middle attack: attack is found between server and client and can intercept and alter traveling data. Also known as On-path attack
6. Network monitoring and sniffing: monitoring network system to determine traffic patterns to obtain information about a network
7. Virus: bad code that has the ability to replicate. They might need humn intervention eg. Clicking by user
8. Worm: bad code that can replicate and doesn’t need intervention by user
9. Trojan: named after the Trojan Horse. It might appear harmless but has malicious code that can cuase damage. Eg. Randsomeware sometimes use Trojan Horse to infect target machines, use encryption to encrypt data and the key is only known by the malware
10. Side-channel: non-invasive attack to observe the operation of a device. Methods include power monitoring, timing and fault analysis attacks
11. Advanced Persistent Threat (APT): sophisticated attacks for an extended period of time
12. Insider threat: done by insiders willingly or not
13. Malware: bad code inserted into a system for ill intents
14. Randsomware: malware used in randsonware

Port types:

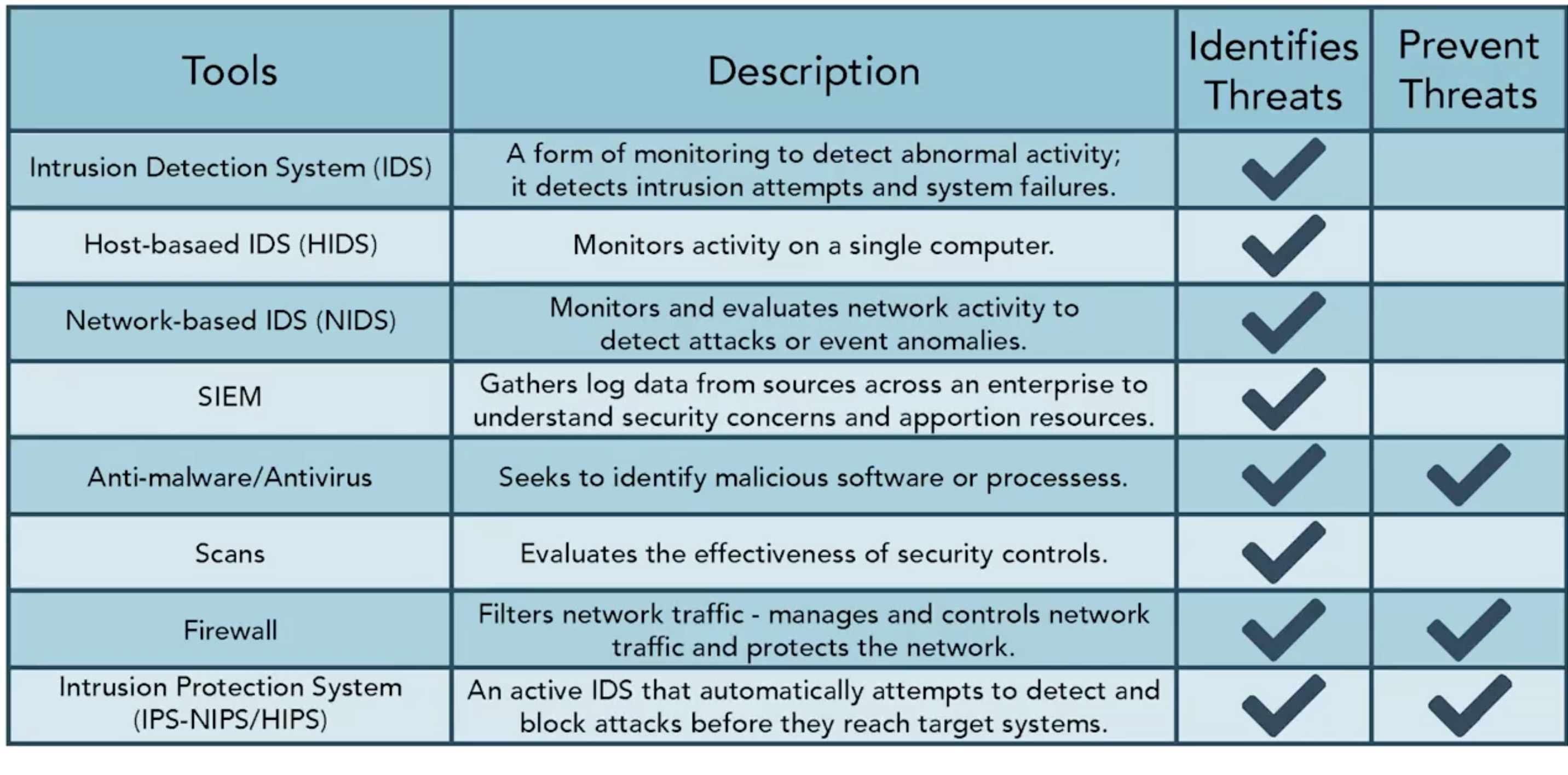
1. Physical: ports on routers, switches, server, computers, etc.
2. Logical (sockets):
   1. Allows one IP address to respond to different requests coming from the same port
   2. Dedicated ports: web traffic (http, 80), secure web traffic (Https, 443), FTP (21, sends username and password for authentication, SFTP should be used instead as it is encrypted), SFTP (Secure File Transfer Protocol, 22), Telnet (text-based terminal used by Linux systems, 23), SSH (The encrypted version of Telnet, 22), SMTP (defult port for mai, l25), SMTP with TLC layer (more secure than just SMTP, 587), Time (might be used by legacy systmes and has mostly been replaced by NTP, 37), NTP (Netowrk Time Protocol, 123), DNS (better version is DoT, 53), DoT (DNS over TLS, 853), IMAP(Used to retrieve emails. It is suscpetible to network sniffing. Altenative is to use Image with SSL/TLS (port 993), 143), SNMP (Simple Netork Management Protocol sends and recieves data used for managing infrastructure devices, might contain sensitive data, 161/162), SMB (Server Message Block is used by Windows to access files over the network. A more secure version is NFS (Network File System, 2049), 445), LDAP (389). LDAPS (adds SSL/TLS security for more protection, 636(
   3. Types of ports:
      1. Well-know ports (0-1023): commonly used by establised protocols
      2. Register ports (1024-49151): associated with 3rd party applications. Some are approved by the Internet Assigned Numebrs Authority (IANA) but vendors can choose whatever they like. Eg. Docker uses 2375/2376 and Microsoft SQL Server uses 1433/1434
   4. Dynamic/private ports: used to respond to requests made using well-known and dynamic ports
3. SSL (Secure Socker Layer) is no more secure

3-way handshake:

1. Used by server and client to communicate
2. Client sends SYN package to server (request to establish connection)
3. SYN/ACK (sent by server to client for acknowledgment)
4. ACK: sent by client to server acknowledgement

Security tools or operations:

1. If a system is not needed, it should not be running
2. Systems should be up to date
3. If a protocol is not absolutely needed, don’t use it. It is another point of attack
4. Firewall are great. Both network and host firewal exist
5. Use anti-malware software and intrution detection and prevention systems
6. Tools:



1. More on tools:
   1. SIEM (Security Information Management, pronounced as SIM): gather log data from various sources
   2. In intrution detection: a lower pid of a process might show that the attack happened closer to the boot time
2. Allowed or denied at firewall:
   1. Denied: ICMP, inbound traffic with IP or email address inside network (not normally routed through firewall)
   2. Allowed: Email with no attachment (not very harmful and if all are restricted, no email will be recived by the business

Data centers:

1. can be hosted by org or outsourced
2. Optimized temperatures are 64-81F (18-27C). And 3 temperatures should be kepet (top rack, middle rack and bottom rack)
3. Fluctuations in power can affect the lifespan of machines

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

Proper loging system design and log reviews are best no matter the computer system used

Ingress monitoring: surveillance and assessment of all inbound communication traffic and access attempts. Tools include: firewalls, gateway remote authentication servers, IDS/IPS tools, SIEM solutions, Anti-malware solutions

Egress monitoring: regulate data leaving the system. A philosophy used to conduct this type of monitoring is called Data Loss Prevention/ Data Leak Protection. Data egress can occur through email, copy of portable media, File Transfer Protocol (FTP), posting to web pages/websites, Application, APIs

Plaintext is anything that can be stored, processed or transferred in a computer system. It includes files, database, audio, videos etc.

Man-In-The-Middle: a spy in a communication link

Out-of-band-key distribution: encryption and key are sent using different channels (bands)

Other names for symmetric keys: same key, single key, shared key, secret key, session key

In a company, public keys might be stored in a corperate website or key server

Assymertric encryption is slower than symmetric but less key might be needed and might be more scalable, for example a 1K-employeed company might 2K using assymetric encryption but 499,500 keys with symmetric.

Message digest: encrypts data in a way that if even a single bit is changed, a different output will be obtained.

Checksum: sum of digits in a file which can be compared to later versions to determine if data changed. Some parts of the data is not added to the sum and also after adding, some parts of the sum might be dropped. Not only for security. If is used to determine whether packets have been lost or data have been altered by noise

Checksums in software downloads to used to determine integrity

Configuration management: System changes will be happening everytime, therefore, they should be catered for. For configurations, factors that matter incldues:

1. Idenfication: identify all components involved
2. Baseline: changes should be compared to reference point
3. Change control: includes changeds and patches and the processes involved in the change
4. Verification and audit; testing to ensure that the change is the right

Regression testing: used to ensure that nothing else break when changes were made

Security governance: security policies, rules, and regulations or an organization. This includes password usages, limits of the use of personal devices, data handling policy, change management policy, RBAc, security testing, Acceptable Use Policy (AUP) (defines acceptable use of the orgs network and computer systems. It can legally protect the org.), Bring Your Own Device (BYOD) policy, etc.

Although policies are org, department dependent, there should be consequence for noncompliance.

Everyone is undergo security training.

SMS phising aka smishign, vishing = making fraudulent phone calls, whaling attacks: attacks of senior employees

Good point: a lot of times the big point is expressed rather than the details. For example a 10-character password might take 50 years to break with brute force. Well, this is only considering the worst case scenario. Best case scenario is the password is right in the first time. So yeah, something glossing over the fine-details might make information more consumable, but it can also cause lack of awareness.