Glossary

IT Support

Terms and definitions from all courses

#

404 Not Found: An error message you might see on websites that have been moved or deleted

802.1X: It is the IEEE standard for encapsulating EAP or Extensible Authentication Protocol traffic over the 802 networks

802.1X with EAP-TLS: Offers arguably the best security available, assuming proper and secure handling of the PKI aspects of it

A

AAA (authentication, authorization, accounting): The services that the directory services provide to all the computers within a company or organization

Abstraction: To take a relatively complex system and simplify it for our use

Absolute path: It is one that starts from the main directory

Access Control Entries: The individual access permissions per object that make up the ACL

Access Control List (ACL): It is a way of defining permissions or authorizations for objects

Accounting: Keeping records of what resources and services your users access or what they did when they were using your systems

ACI: Access Control Lists

ACK flag: One of the TCP control flags. ACK is short for acknowledge. A value of one in this field means that the acknowledgment number field should be examined

Acknowledgement number: The number of the next expected segment in a TCP sequence

Activation threshold: Triggers a pre-configured action when it is reached and will typically block the identified attack traffic for a specific amount of time

Active directory (AD): The Microsoft alternative to directory services that offers customization and added features for the Windows platform

Active directory users and computers (ADUC): The client tools that are used for accessing and administering a directory server

Address bus: Connects the CPU to the MCC and sends over the location of the data, but not the data itself

Address class system: A system which defines how the global IP address space is split up

Address Resolution Protocol (ARP): A protocol used to discover the hardware address of a node with a certain IP address

Ad-Hoc network: A network configuration without supporting network infrastructure. Every device involved with the ad-hoc network communicates with every other device within range, and all nodes help pass along messages

Administrator: A user that has complete control over a machine

Advanced Encryption Standard (AES): The first and only public cipher that's approved for use with top secret information by the United States National Security Agency

Advanced group policy management (AGPM): A set of add-on tools from Microsoft that gives some added provision control abilities in GPMC

Adware: Software that displays advertisements and collects data

Algorithm: A series of steps that solves specific problems

Alias: A nickname for common commands

Analyzing logs: The practice of collecting logs from different network and sometimes client devices on your network, then performing an automated analysis on them

Android: A mobile operating system based on Linux

Antivirus software: It monitors and analyze things like new files being created or being modified on the system in order to watch for any behavior that matches a known malware signature

Anycast: A technique that's used to route traffic to different destinations depending on factors like location, congestion, or link health

Appending flags: A way to add the data of the file without erasing existing data

Application: A computer program designed for a specific use

Application layer: The layer that allows network applications to communicate in a way they understand

Application layer payload: The entire contents of whatever data applications want to send to each other

Application policies: Defines boundaries of what applications are permitted or not, but they also help educate folks on how to use software more securely

Application software: Any software created to fulfill a specific need, like a text editor, web browser, or graphics editor

App store apps: A Package Manager that acts as a repository

App store repository: A app store service that also acts as a repository

App stores: A central managed marketplace for app developers to publish and sell mobile apps

APPX: An APPX is another way to package contents of a file to act like a unit of distribution

Archive: An archive is comprised of one or more files that are compressed into a single file" for verb agreement

A record: The most common resource record, used to point a certain domain name at a certain IPv4 IP address

ARPANET: The earliest version of the Internet that we see today, created by the US government project DARPA in the 1960s

ARP table: A list of IP addresses and the MAC addresses associated with them

ASCII: The oldest character encoding standard used is ASCII. It represents the English alphabet, digits, and punctuation marks

ASN: Autonomous System Number is a number assigned to an individual autonomous system

Assembly language: A language that allowed computer scientists to use human readable instructions, assembled into code that the machines could understand

Asymmetric Digital Subscriber Line (ADSL): A device that establishes data connections across phone lines and different speeds for uploading and downloading data

Asymmetric encryption: Systems where different keys are used to encrypt and decrypt

ATA: The most common interface that hard drives use to connect to our system

Attack: An actual attempt at causing harm to a system

Attack surface: It's the sum of all the different attack vectors in a given system

Attack vector: Method or mechanism by which an attacker or malware gains access to a network or system

ATX (Advanced Technology eXtended): The most common form factor for motherboards

Auditing: It involves reviewing records to ensure that nothing is out of the ordinary

Authentication: A crucial application for cryptographic hash functions

Authentication server (AS): It includes the user ID of the authenticating user

Authorization: It pertains to describing what the user account has access to or doesn't have access to

Automatic allocation: A range of IP addresses is set aside for assignment purposes

Automation: It makes processes work automatically

Autoscaling: A system that allows the service to increase or reduce capacity as needed, while the service owner only pays for the cost of the machines that are in use at any given time

Availability: Means that the information we have is readily accessible to those people that should have it

B

Backdoor: A way to get into a system if the other methods to get in a system aren't allowed, it's a secret entryway for attackers

Background processes/Daemon processes: Processes that run or take place in the background

Backup and restore: A Microsoft offer and first party solution that has modes of operation, as a file based version where files are backed up to a zip archive

Backward compatible: It means older hardware works with newer hardware

Baiting: An attack that happens through actual physical contact, enticing a victim to do something

Bash: The language used to interact with the shell

Bastion hosts or networks: A server used to provide access to a private network from an external network

Baud rate: A measurement of how many bits could be passed across a phone line in a second

Binary system: The communication that a computer uses is referred to as binary system, also known as base-2 numeral system

Binary whitelisting software: It's a list of known good and trusted software and only things that are on the list are permitted to run

Bind: It is how clients authenticate to the server

Bind operation: The operation which authenticates clients to the directory server

Biometric authentication: Authentication that uses Biometric data

Biometric data: A way of protecting your accounts and information using biometric data such as facial recognition and fingerprint

BIOS/UEFI: A low-level software that initializes our computer's hardware to make sure everything is good to go

Bios (Basic Input Output Services): The BIOS is software that helps initialize the hardware in our computer and gets our operating system up and running

Bit: The smallest representation of data that a computer can understand

Block ciphers: The cipher takes data in, places that into a bucket or block of data that's a fixed size, then encodes that entire block as one unit

Block devices: A system that acts like USB drives and hard drive by transmitting data

Block storage: It improves faster handling of data because the data isn't stored in one long piece but in blocks, so it can be accessed more quickly

Bluetooth: The most common short range wireless network

Boot: To start up a computer

Bootloader: A small program that loads the operating system

Border Gateway Protocol (BGP): A protocol by which routers share data with each other

Botnet: A collection of one or more Bots

Bots: Machines compromised by malware that are utilized to perform tasks centrally controlled by an attacker

Broadband: Any connectivity technology that isn't dial-up Internet

Broadcast: A type of Ethernet transmission, sent to every single device on a LAN

Broadcast address: A special destination used by an Ethernet broadcast composed by all Fs

Browser: A user interface for displaying and interacting with web pages

Brute force attacks: A common password attack which consists of just continuously trying different combinations of characters and letters until one gets access

BYOD (Bring Your Own Device): Refers to the practice of allowing people to use their own personal devices for work

Byte: A group of 8 bits

C

CA (Certificate authority): It's the entity that's responsible for storing, issuing, and signing certificates. It's a crucial component of the PKI system

Cable categories: Groups of cables that are made with the same material. Most network cables used today can be split into two categories, copper and fiber

Cable modem: A device that sits at the edge of a consumer's network and connects it to the cable modem termination system

Cable modem termination system: Connects lots of different cable connections to an ISP's core network

Cables: Insulated wires that connect different devices to each other allowing data to be transmitted over them

Cache: The assigned stored location for recently or frequently accessed data; on a mobile app it is where anything that was changed or created with that app is stored

Cache: The assigned stored location for recently or frequently accessed data; on a mobile app it is where anything that was changed or created with that app is stored

Caching and recursive name servers: They are generally provided by an ISP or your local network, and their purpose is to store domain name lookups for a certain amount of time

Caesar cipher: A substitution alphabet, where you replace characters in the alphabet with others usually by shifting or rotating the alphabet, a set of numbers or characters

Carrier-Sense Multiple Access with Collision Detection (CSMA/CD): CSMA/CD is used to determine when the communications channels are clear and when the device is free to transmit data

CBC-MAC (Cipher block chaining message authentication codes): A mechanism for building MACs using block ciphers

CCMP (counter mode CBC-MAC protocol): A mode of operation for block ciphers that allows for authenticated encryption

Centralized logging: Parsing logs in one central location

Central management: A central service that provides instructions to all of the different parts of my IT infrastructure

Central repository: It is needed to securely store and index keys and a certificate management system of some sort makes managing access to storage certificates and issuance of certificates easier

Certificate-based authentication: It is the most secure option, but it requires more support and management overhead since every client must have a certificate

Certificate fingerprints: These are just hash digests of the whole certificate, and aren't actually fields in the certificate itself, but are computed by clients when validating or inspecting certificates

Certificate Revocation List (CRL): A means to distribute a list of certificates that are no longer valid

Certificate Signature Algorithm: This field indicates what public key algorithm is used for the public key and what hashing algorithm is used to sign the certificate

Certificate Signature Value: The digital signature data itself

Change management process: The process to notify others in the organization about the changes that you are about to make

Channels: Individual, smaller sections of the overall frequency band used by a wireless network

Character devices: A way to transmit data character by character like a keyboard and mouse

Character encoding: Is used to assign our binary values to characters so that we as humans can read them

Charge cycle: One full charge and discharge of a battery

Child directories: It is a directory housed by a parent directory

Children's Online Privacy Protection Act (COPPA): Regulates the information we show to children under the age of 13

Chipset: It decides how components talk to each other on our machine

Chocolatey: A third party package manager for Windows

Chrome OS: A Linux-based operating system designed by Google

CIA Triad: Confidentiality, integrity, and availability. Three key principles of a guiding model for designing information security policies

CLI: Command line interpreter

Client: A device that receives data from a server

Client/Server runtime subsystem: System that handles running Windows GUI and Command line

Client certificates: They operate very similarly to server certificates but are presented by clients and allow servers to authenticate and verify clients

Clients: A device that receives data from a server

Clock cycle: When you send a voltage to the clock wire

Clock speed: The maximum number of clock cycles that it can handle in a set in a certain time period

Clock wire: When you send or receive data, it sends a voltage to that clock wire to let the CPU know it can start doing calculations

CLOSE_WAIT: A connection state that indicates that the connection has been closed at the TCP layer, but that the application that opened the socket hasn't released its hold on the socket yet

CLOSE: A connection state that indicates that the connection has been fully terminated, and that no further communication is possible

Closed source packages: A source code that does not allow public access

Cloud computing: The concept and technological approach of accessing data, using applications, storing files, etc. from anywhere in the world as long as you have an internet connection

Cloud computing: The concept and technological approach of accessing data, using applications, storing files, etc. from anywhere in the world as long as you have an internet connection

CMACs (Cipher-based Message Authentication Codes): The process is similar to HMAC, but instead of using a hashing function to produce a digest, a symmetric cipher with a shared keys used to encrypt the message and the resulting output is used as the MAC

CNAME: A resource record used to map one domain to another

Code signing certificates: It is used for signing executable programs and allows users of these signed applications to verify the signatures and ensure that the application was not tampered with

Coding: Translating one language to another

Collision domain: A network segment where only one device can communicate at a time

Command line: A text interface program for a computer that inputs text commands and translates them to the operating system

Command Line Interface (CLI): A shell that uses text commands to interact with the operating system

Command line mode: When you are able to run commands while still in your current shell

Compiled programming language: A language that uses human readable instructions, then sends them through a compiler

Computer: A device that stores and processes data by performing calculations

Computer configuration: Contained within a Group Policy Object (GPO)

Computer file: Data that we store and a file can be anything, a word document, a picture, a song, literally anything

Computer management: A tool that lets you manage a local or remote computer

Computer networking: The full scope of how computers communicate with each other

Confidentiality: Keeping things hidden

Configuration management: The creation of rules about how things should work in your organization, such as printers, configure software, or mounting network file systems

Connectionless protocol: A data-transmission protocol that allows data to be exchanged without an established connection at the transport layer. The most common of these is known as UDP, or User Datagram Protocol

Connection-oriented protocol: A data-transmission protocol that establishes a connection at the transport layer, and uses this to ensure that all data has been properly transmitted

Copper cable categories : These categories have different physical characteristics like the number of twists in the pair of copper wires. These are defined as names like category (or cat) 5, 5e, or 6, and how quickly data can be sent across them and how resistant they are to outside interference are all related to the way the twisted pairs inside are arranged

Copyright: Used when creating original work

Correlation analysis: The process of taking log data from different systems, and matching events across the systems

Counter-based tokens: They use a secret seed value along with the secret counter value that's incremented every time a one-time password is generated on the device

CPU: Central processing unit

CPU sockets: A CPU socket is a series of pins that connect a CPU’s processor to the PC’s motherboard

Cross-site scripting (XSS): A type of injection attack where the attacker can insert malicious code and target the user of the service

Crosstalk: Crosstalk is when an electrical pulse on one wire is accidentally detected on another wire

Cryptanalysis: Looking for hidden messages or trying to decipher coded message

Cryptographic hashing: It is distinctly different from encryption because cryptographic hash functions should be one directional

Cryptography: The overarching discipline that covers the practice of coding and hiding messages from third parties

Cryptography: The overarching discipline that covers the practice of coding and hiding messages from third parties

Cryptology: The study of cryptography

Cryptosystem: A collection of algorithms for key generation and encryption and decryption operations that comprise a cryptographic service

Cyclical Redundancy Check (CRC): A mathematical transformation that uses polynomial division to create a number that represents a larger set of data. It is an important concept for data integrity and is used all over computing, not just network transmissions

D

DACL: Directory Control Lists

DARPA: A US government project in the 1960s that went on to create the earliest version of the Internet that we see today

Data: Actual content of a file

Databases: Databases allow us to store query, filter, and manage large amounts of data

Data binding and sealing: It involves using the secret key to derive a unique key that's then used for encryption of data

Data blocks: Data that can be broken down into many pieces and written to different parts of the hard disk

Data buffer: A region of RAM that’s used to temporarily store data while it’s being moved around

Data center: A facility that stores hundreds, if not thousands of servers

Data exfiltration: The unauthorized transfer of data from a computer. It's also a very important concern when a security incident happens

Data handling policies: Should cover the details of how different data is classified

Data information tree: A structure where objects will have one parent and can have one or more children that belong to the parent object

Datalink layer: The layer in which the first protocols are introduced. This layer is responsible for defining a common way of interpreting signals, so network devices can communicate

Data offset field: The number of the next expected segment in a TCP packet/datagram

Data packet: An all-encompassing term that represents any single set of binary data being sent across a network link

Data payload section: Has all of the data of the protocols further up the stack of a frame

Data recovery: Is the process of trying to restore data after an unexpected event that results in data loss or corruption

Data sizes: Metrics that refer to data sizes including bit, byte, kilobyte, kibibyte, and megabyte

Data tapes: The standard medium for archival backup data storage

DDR SDRAM (Double Data Rate SDRAM): A type of RAM that is faster, takes up less power, and has a larger capacity than earlier SDRAM versions

Debian(.deb): A Debian package is packaged as a .deb file

Decimal form- base 10 system: In the decimal system, there are 10 possible numbers you can use ranging from zero to nine

Decryption: The reverse process from encryption; taking the garbled output and transforming it back into the readable plain text

Default domain control policy: One of the two GPOs that are created when a new Active Directory domain has been made

Defense in depth: The concept of having multiple overlapping systems of defense to protect IT systems

Defragmentation: A process of taking all the files stored on a given disk and reorganizing them into neighboring locations

Delegation: The administrative tasks that you need to perform a lot as a part of your day to day job but you don't need to have broad access to make changes in AD

Demarcate: To set the boundaries of something

Demarcation point: Where one network or system ends and another one begins

Demultiplexing: Taking traffic that's all aimed at the same node and delivering it to the proper receiving service

Denial-of-Service (DoS) attack: An attack that tries to prevent access to a service for legitimate users by overwhelming the network or server

Deployment: Hardware is set up so that the employee can do their job

DES (Data Encryption Standard): One of the earliest encryption standards

Desktop: The main screen where we can navigate our files, folders, and applications

Destination MAC address: The hardware address of the intended recipient that immediately follows the start frame delimiter

Destination network: The column in a routing table that contains a row for each network that the router knows about

Destination port: The port of the service the TCP packet is intended for

Detection measure: The measures to alert you and your team that a disaster has occurred that can impact operations

Deterministic: It means that the same input value should always return the same hash value

Device manager: A console management system for your device

DH (Diffie-Hellman): A popular key exchange algorithm, named for its co-inventors

DHCP: A technology that assigns an IP address automatically to a new device. It is an application layer protocol that automates the configuration process of hosts on a network

DHCP discovery: The process by which a client configured to use DHCP attempts to get network configuration information

Dial-up: Uses POTS for data transfer, and gets its name because the connection is established by actually dialing a phone number

Dictionary attack: A type of password attack that tries out words that are commonly used in passwords, like password, monkey, football

Differential backup: A backup of files that are changed, or has been created since the last full backup

Digital divide: The growing skills gap between people with and without digital literacy skills

DIMM: Dual Inline Memory Module

Directory Access Protocol (DAP): A protocol that is included in the X.500 directory standard from 1988

Directory Information Shadow Protocol (DISP): A protocol that is included in the X.500 directory standard from 1988

Directory Operational Bindings Protocol (DOBMP): A protocol that is included in the X.500 directory standard from 1988

Directory server: The server that contains a lookup service that provides mapping between network resources and their network addresses

Directory services: A lookup service contained in a network server that provides mapping between network resources and their network addresses

Directory System Protocol (DSP): A protocol that is included in the X.500 directory standard from 1988

Disaster recovery plan: A collection of documented procedures and plans on how to react and handle an emergency or disaster scenario, from the operational perspective

Disaster recovery testing: A regular exercise that happens once a year or so, that has different teams, including IT support specialists, going through simulations of disaster events

Disk Management utility: Native tool for Windows that helps with managing disk space

Disk to disk cloning: A type of cloning that happens when you connect an external hard drive to the machine you want to clone

Display port: Port which also outputs audio and video

Distinguished name (DN): A unique identifier for each entry in the directory

Distributed Denial-of-Service (DDoS) attack: A DoS attack using multiple systems

Distribution: A version of the operating system

Distribution group: A group that is only designed to group accounts and contacts for email communication

Distributions: Some common Linux distributions are Ubuntu, Debian, and Red Hat

DNS Cache Poisoning Attack: It works by tricking a DNS server into accepting a fake DNS record that will point you to a compromised DNS server

DNS records: A DNS request for the SRV records matching the domain that it's been bound to

DNS zones: A portion of space in the Domain Name System (DNS) that is controlled by an authoritative name server

Domain: Used to demarcate where control moves from a top-level domain name server to an authoritative name server

Domain admin: The administrators of the Active Directory domain

Domain computers: All the computers joined to the domain except domain controllers

Domain controllers (DC): The service that hosts copies of the Active Directory database

Domain local: The tool used used to assign permission to a resource

Domain name: A website name; the part of the URL following www.

Domain Name System (DNS): A global and highly distributed network service that resolves strings of letters, such as a website name, into an IP address

Domain users: A group that contains every user account in the domain

Dotted decimal notation: A format of using dots to separate numbers in a string, such as in an IP address

DRAM: Dynamic Random Access Memory

Driver: Used to help our hardware devices interact with our Operating System

Drivers: The drivers contain the instructions our CPU needs to understand external devices like keyboards, webcams, printers

DSA (Digital Signature Algorithm): It is another example of an asymmetric encryption system, though its used for signing and verifying data

DSL: Digital subscriber line was able to send much more data across the wire than traditional dial-up technologies by operating at a frequency range that didn't interfere with normal phone calls

DSLAM: Digital Subscriber Line Access Multiplexers are devices that connect multiple DSL connections to a high-speed digital communications channel

Duplex communication: A form of communication where information can flow in both directions across a cable

Duration field: Specifies how long the total frame is

DVI: DVI cables generally just output video

Dynamic allocation: A range of IP addresses is set aside for client devices and one of these IPs is issued to these devices when they request one

Dynamic ARP inspection (DAI): A feature on enterprise switches that prevents certain types of attacks

Dynamic IP address: An IP address assigned automatically to a new device through a technology known as Dynamic Host Configuration Protocol

Dynamic-link libraries: Programs that want to use functionality that the code provides can tap into it if they need to (shared libraries)

E

.exe: A file extension found in Windows for an executable file

EAP-TLS: One of the more common and secure EAP methods

ECDH & ECDSA: Elliptic curve variants of Diffie-Hellman and DSA, respectively

Electrostatic discharge: Electrostatic discharge is a sudden and momentary flow of electric current between two electrically charged objects caused by contact, an electrical short or dielectric breakdown

Eliptic curve cryptography (ECC): A public key encryption system that uses the algebraic structure of elliptic curves over finite fields to generate secure keys

Encapsulating security payload: It's a part of the IPsec suite of protocols, which encapsulates IP packets, providing confidentiality, integrity, and authentication of the packets

Encryption: The act of taking a message (plaintext), and applying an operation to it (cipher), so that you receive a garbled, unreadable message as the output (ciphertext)

Encryption algorithm: The underlying logic or process that's used to convert the plaintext into ciphertext

End-entity (leaf certificate): A certificate that has no authority as a CA

Enterprise admin: The administrators of the Active Directory domain that has permission to make changes to the domain that affect other domains in a multi-domain forest

Enterprise app management: A management system that allows an organization to distribute custom mobile apps

Enterprise mobility management (EMM): A system that can create and distribute policies and MDMs

Entropy pool: A source of random data to help seed random number generators

Entry point: the act to determine the entry point to figure out how the attacker got in, or what vulnerability the malware exploited

Environment: Whatever settings or variables a child process inherits from the parent’s process

Error detection: The ability for a protocol or program to determine that something went wrong

Error message: Helpful indicators that can point you in the right direction

Error recovery: The ability for a protocol or program to attempt to fix an error

Escape characters: A concept that means that the next character after the back tick should be treated literally

ESTABLISHED: Status indicating that the TCP connection is in working order, and both sides are free to send each other data

Etcher.io: A tool you can use to load an install image onto your USB device and make it bootable

Ethernet: The protocol most widely used to send data across individual links

Ethernet cable: It lets you physically connect to the network through a cable

Ethernet frame: A highly structured collection of information presented in a specific order

EtherType field: It follows the Source MAC Address in a dataframe. It's 16 bits long and used to describe the protocol of the contents of the frame

Event Viewer: A place where all events that have been logged are stored

Evil twin: The premise of an evil twin attack is for you to connect to a network that is identical to yours but that is controlled by an attacker. Once connected to it, they will be able to monitor your traffic

Executable file: A file containing instructions for a computer to execute when they're run

Expansion slots: Give us the ability to increase the functionality of our computer

Exploit: Software that is used to take advantage of a security bug or vulnerability

Extensible authentication protocol (EAP over LAN, or EAPOL): A standard authentication protocol

Exterior gateway: Protocols that are used for the exchange of information between independent autonomous systems

External Data Bus (EDB): It's a row of wires that interconnect the parts of our computer

F

Factory reset: Resetting a device to the settings it came with from the factory

Fail to ban: A common open source flood guard protection tool

Fast logon optimization: The group policy engine that applies policy settings to a local machine may sacrifice the immediate application of some types of policies in order to make logon faster

Fiber optic cable: Fiber optic cables contain individual optical fibers which are tiny tubes made of glass about the width of a human hair. Unlike copper, which uses electrical voltages, fiber cables use pulses of light to represent the ones and zeros of the underlying data

File-based encryption: Guarantees confidentiality and integrity of files protected by encryption

File compression: The files and folder structures are copied and put into an archive

File extension: The appended part of a filename that tells us what type of file it is in certain operating systems

File handling: A process of storing data using a program

File permissions: A process for setting permissions for who has access to certain files

File record number: The index of the files entry in the MFT

File storage service: Allows to centrally store files and manage access between files and groups

File system: A system used to manage files

FIN_WAIT: A TCP socket state indicating that a FIN has been sent, but the corresponding ACK from the other end hasn't been received yet

FIN: One of the TCP control flags. FIN is short for finish. When this flag is set to one, it means the transmitting computer doesn't have any more data to send and the connection can be closed

Finder: The file manager for all Macs

FIPS (Federal Information Processing Standard): The DES that was adopted as a federal standard for encrypting and securing government data

Firewall: It is a device that blocks or allows traffic based on established rules

Firmware: Software that's permanently stored on a computer component

Five layer model: A model used to explain how network devices communicate. This model has five layers that stack on top of each other: Physical, Data Link, Network, Transport, and Application

Fixed allocation: Requires a manually specified list of MAC address and the corresponding IPs

Flag field: It is used to indicate if a datagram is allowed to be fragmented, or to indicate that the datagram has already been fragmented

Flat file: A collection of records/information that follow a consistent format with rules around stored values. On a host computer, one use is to have a list of network address and host name pairs (a hosts file)

Flexible single-master operations (FSMO): The single domain controller that has been tasked with making changes to the AD database that can only be made by one DC at a time

Flood guards: Provide protection against DoS or Denial of Service Attacks

Flow label field: 20-bit field that's used in conjunction with the traffic class field for routers to make decisions about the quality of service level for a specific datagram

Folders/Directories: Used to organize files

Forest: The hierarchy above a domain that contains multiple domains, allowing accounts to share resources between domains that are in the same forest

Form factor: A mathematical way to compensate for irregularities in the shape of an object by using a ratio between its volume and height

Forward secrecy: This is a property of a cryptographic system so that even in the event that the private key is compromised, the session keys are still safe

Four-Way Handshake: It is designed to allow an AP to confirm that the client has the correct pairwise master key in a WPA-PSK setup without disclosing the PMK

Fragmentation: The process of taking a single IP datagram and splitting it up into several smaller datagrams

Fragmentation offset field: It contains values used by the receiving end to take all the parts of a fragmented packet and put them back together in the correct order

Frame check sequence: It is a 4-byte or 32-bit number that represents a checksum value for the entire frame

Frame control field: 16 bits long, it contains a number of sub-fields that are used to describe how the frame itself should be processed

Frequency analysis: The practice of studying the frequency with which letters appear in ciphertext

Frequency band: A certain section of the radio spectrum that's been agreed upon to be used for certain communications

FTP: An older method used for transferring files from one computer to another, but you still see it in use today

FTTB: Fiber to the building, fiber to the business or even fiber to the basement, since this is generally where cables to buildings physically enter. FTTB is a setup where fiber technologies are used for data delivery to an individual building

FTTH: Fiber to the home. This is used in instances where fiber is actually run to each individual residents in a neighborhood or apartment building

FTTN: Fiber to the neighborhood. This means that fiber technologies are used to deliver data to a single physical cabinet that serves a certain amount of the population

FTTP: Fiber to the premises. FTTH and FTTB may both also be referred to as FTTP

FTTX: Stands for fiber to the X, where the X can be one of many things

Full backup: The full unmodified contents of all files to be backed up ~~is~~ are included in this backup mechanism whether the data was modified or not

Full control: A user or group with full control that can do anything they want to files

Full disk encryption (FDE): It is the practice of encrypting the entire drive in the system

Full duplex: The capacity of devices on either side of a networking link to communicate with each other at the exact same time

Fully qualified domain name: When you combine all the parts of a domain together

Functional levels: The different versions of Active Directory, a functional level that describes the features that it supports

G

GIT: A version control system that helps keep track of changes made to files and directories

Global: The tool that is used to group accounts into a role

Globalization: The movement that lets governments, businesses, and organizations communicate and integrate together on an international scale

Group policy management console (GPMC): The tools used for creating and viewing a group policy object

Group policy objects (GPO): The ways to manage the configuration of Windows machines, referring to the objects that represent things in your network that you want to be able to reference or manage

Group policy settings reference: A spreadsheet that details the GPO policies and preferences that are available and where to find them

Groups: A collection of users

Group scope: The way that group definitions are replicated across domains

GTK (Groupwise Transient Key): A temporal key, which is actually used to encrypt data

GUI: A graphical user interface

GUID partition table: Only used if you are using UEFI booting

H

Hacker: Someone who attempts to break into or exploit a system

Half-duplex: It means that, while communication is possible in each direction, only one device can be communicating at a time

Half-open attacks: A way to refer to SYN floods

Handshake: A way for two devices to ensure that they're speaking the same protocol and will be able to understand each other

Hard drive: It is a long term memory component that holds all of our data, which can include music, pictures, applications

Hard link: When created in NTFS, an entry is added to the MFT that points to the linked file record number, not the name of the file. This means the file name of the target can change and the hard link will still point to it

Hardware: External or internal devices and equipment that help you perform major functions

Hardware ID: A special string of characters assigned to hardware

Hardware resource deficiency: It refers to the lack of system resources like memory, hard drive space, et cetera

Hash collisions: Two different inputs mapping to the same output

Hashing (Hash function): A type of function or operation that takes in an arbitrary data input and maps it to an output of a fixed size, called a hash or a digest

Having dependencies: A process of counting on other pieces of software to make an application work since one bit of code depends on another in order to work

HDD (Hard disk drive): Hard disk drives, or HDDs, use a spinning platter and a mechanical arm to read and write information

HDMI: A type of cable that outputs both video and audio

HDSL: High Bit-rate Digital Subscriber Lines. These are DSL technologies that provision speeds above 1.544 megabits per second

Header checksum field: A checksum of the contents of the entire IP datagram header

Header length field: A four bit field that declares how long the entire header is. It is almost always 20 bytes in length when dealing with IPv4

Heatsink: It is used to dissipate heat from our CPU

Hexadecimal: A way to represent numbers using a numerical base of 16

HFS+/APFS: HFS+ is a journaling system developed by Apple Inc. and APFS is another but more encrypted Apple journaling system

Hidden files: A set of files that are not visible either to avoid alteration or simply because you don't want someone to see them

High value data: usually includes account information, like usernames and passwords. Typically, any kind of user data is considered high value, especially if payment processing is involved

HMAC (Keyed-Hash Message Authentication Codes): It uses a cryptographic hash function along with a secret key to generate a MAC

Hop limit field: An 8-bit field that's identical in purpose to the TTL field in an IPv4 header

Host-based firewalls: Protects individual hosts from being compromised when they're used in untrusted and potentially malicious environments

Host file: It is a flat file that contains, on each line, a network address followed by the host name it can be referred to as

Hostname: Used to identify the computer when it needs to talk to other computers

Hot key: A keyboard shortcut that does a particular task

HTTPS: Hypertext Transfer Protocol Secure is a secure version of HTTP that ensures the communication your web browser has with the website is secured through encryption.

HTTPS: Hypertext Transfer Protocol Secure is a secure version of HTTP that ensures the communication your web browser has with the website is secured through encryption.

HTTP status code: The codes or numbers that indicate some sort of error or info messages that occurred when trying to access a web resource

Hub: It is a physical layer device that broadcasts data to everything computer connected to it

Hubs: Devices that serve as a central location through which data travels through

Hubs: Devices that serve as a central location through which data travels through; a quick and dirty way of getting packets mirrored to your capture interface

Hybrid cloud: Used to describe situations where companies might run things like their most sensitive proprietary technologies on a private cloud or on premise while entrusting their less sensitive servers to a public cloud

Hybrid cloud: Used to describe situations where companies might run things like their most sensitive proprietary technologies on a private cloud or on premise while entrusting their less sensitive servers to a public cloud

Hypervisor: A piece of software that runs and manages virtual machines while also offering guests a virtual operating platform that's indistinguishable from actual hardware

I

I/O management: Anything that can give us input or that we can use for output of data

I/O Streams: An input stream handles data flowing into and out of a program

IANA: The Internet Assigned Numbers Authority, is a non-profit organization that helps manage things like IP address allocation

ICMP: Internet control message protocol is used by router or remote hosts to communicate error messages when network problems prevent delivery of IP packets

ICMP payload: Piece of the packet which lets the recipient of the message knows which of their transmissions caused the error being reported

Identification: The idea of describing an entity uniquely

Identification field: It is a 16-bit number that's used to group messages together

Impact: The impact of an incident is also an important issue to consider

Implicit deny: A network security concept where anything not explicitly permitted or allowed should be denied

Import: Moving a backup of the test example policy to the production example policy

Information technology: The use of digital technology, like computers and the internet, to store and process data into useful information

Infrastructure as a Service (IaaS): A subset of cloud computing where a network and servers are provided for customers to run their services

Inherit only: A permission group that means that a DACL will be inherited, but not applied to a container

Injection attacks: A common security exploit that can occur in software development and runs rampant on the web, where an attacker injects malicious code

Inode: A file structure for metadata and files

Input/Output device: A device that performs input and output, including monitors, keyboards, mice, hard disk drives, speakers, bluetooth headsets, webcams, and network adapters

Install image: A downloadable operating system image used to install an operating system on a device

Installing from source: A process of installing from a source

Instantiation: The actual implementation of something defined elsewhere

Instruction set: A list of instructions that our CPU is able to run

Integrity: Means keeping our data accurate and untampered with

Interactive mode: When the parted tool launches you into a separate program

Interface: For a router, the port where a router connects to a network. A router gives and receives data through its interfaces. These are also used as part of the routing table

Interior gateway: Interior gateway protocols are used by routers to share information within a single autonomous system

Intermediary (subordinate) CA: It means that the entity that this certificate was issued to can now sign other certificates

Internet: A worldwide system of interconnected networks

Internet Corporation for Assigned Names and Numbers (ICANN): Where website names are registered

Internet of Things (IoT): The concept that more and more devices are connected to the internet in a smarter fashion such as smart thermostats that turn off the air conditioner when you leave and turn it on when you come back

Internet Protocol (IP): The most common protocol used in the network layer

Internet Protocol version 4 (IPv4): An address that consists of 32 bits separated into four groups

Internet Protocol version 6 (IPv6): An address that consist of a 128 bits, four times the amount that IPv4 uses

Internet service provider (ISP): A company that provides a consumer an internet connection

Internet Service Provider (ISP): A company that provides a consumer an internet connection

Internetwork: A collection of networks connected together through routers - the most famous of these being the Internet

Interpreted programming language: A language that isn't compiled ahead of time

Intranet: An internal network inside a company, accessible if you are on a company's network

Intrusion detection and intrusion protection systems (IDS/IPS): Operates by monitoring network traffic and analyzing it

iOS: A mobile operating system developed by Apple Inc.

IP address: The most common protocol used in the network layer, used to helps us route information

IP datagram: A highly structured series of fields that are strictly defined

IP masquerading: The NAT obscures the sender's IP address from the receiver

IP options field: An optional field and is used to set special characteristics for datagrams primarily used for testing purposes

IPsec (Internet Protocol security): A VPN protocol that was designed in conjunction with IPv6

IP source guard (IPSG): It can be enabled on enterprise switches along with DHCP snooping

IPv6 tunnel: IPv6 tunnel servers on either end of a connection take incoming IPv6 traffic and encapsulate it within traditional IPv4 datagrams

IPv6 tunnel brokers: Companies that provide IPv6 tunneling endpoints for you, so you don't have to introduce additional equipment to your network

Issuer Name: This field contains information about the authority that signed the certificate

IT Infrastructure: The software, the hardware, network, and services required for an organization to operate in an enterprise IT environment

ITX (Information Technology eXtended): A form factor for motherboards that is much smaller than ATX boards

K

Kerberos: A network authentication protocol that uses tickets to allow entities to prove their identity over potentially insecure channels to provide mutual authentication

Kerberos: A network authentication protocol that uses tickets to allow entities to prove their identity over potentially insecure channels to provide mutual authentication

Kerckhoff's principle: A principle that states that a cryptosystem, or a collection of algorithms for key generation and encryption and decryption operations that comprise a cryptographic service should remain secure, even if everything about the system is known except for the key

Kernel: The main core of an operating system that creates processes, efficiently schedules them, and manages how processes are terminated

Kernel module: It extends the kernel's functionality so developers don't have to actually touch the Linux kernel

Key: A crucial component of a cipher, which introduces something unique into your cipher

Key escrow: Allows encryption key to be securely stored for later retrieval by an authorized party

Key length: It defines the maximum potential strength of the system

Keylogger: A common type of spyware that's used to record every keystroke you make

Key signing parties: Organized by people who are interested in establishing a web of trust, and participants perform the same verification and signing

Key size: It is the total number of bits or data that comprises the encryption key

KVM Switch: Keyboard, video, & mouse switch that looks like a hub that you can connect multiple computers to and control using one keyboard, mouse, and monitor

L

L2TP (Layer 2 Tunneling Protocol): It is typically used to support VPNs

Land Grid Array (LGA): It is a type of CPU socket that stick out of the motherboard

LDAP data interchange format: The tool that allows you to authenticate, add, remove users, groups, computers and so on in a directory service

LDAP Entry: A collection of information that's used to describe something

LDIF files: A text file that lists attributes and values that describe something

Library: A way to package a bunch of useful code that someone else wrote

Lightning adaptor: One of the standard power, data and display connector types used in mobile devices

Lightweight Directory Access Protocol (LDAP): An open industry-standard protocol for accessing and maintaining directory services; the most popular open-source alternative to the DAP

Lightweight Directory Access Protocol (LDAP): An open industry-standard protocol for accessing and maintaining directory services; the most popular open-source alternative to the DAP

Line coding: Modulation used for computer networks

Linked: A GPO that all of the computers or users under a domain, site, or OU will have a policy applied

Link-local unicast address: Allow for local network segment communications and are configured based upon a host's MAC address

Linux OS: Linux is one of the largest an open source operating system used heavily in business infrastructure and in the consumer space

Listen: It means that a TCP socket is ready and listening for incoming connections

List folder contents: A command that will execute and list folder contents and is an alias for Read and Execute

Load balancer: Ensures that each VM receives a balanced number of queries

Local Area Network (LAN): A single network in which multiple devices are connected

Logging: The act of creating log events

Logic bomb: A type of Malware that's intentionally installed

Logic gates: Allow transistors to do more complex tasks, like decide where to send electrical signals depending on logical conditions

Log rotation: A way for the OS to clean out log files to make room for new ones

Logs: Files that record system events on our computer

Logs: Files that record system events on our computer

Logs analysis systems: They are configured using user-defined rules to match interesting or atypical log entries

Loopback address: An IP address that always points to itself. This type of address is used to test internal pathing through the TCP/IP protocols

M

MAC(Media Access Control) address: A globally unique identifier attached to an individual network interface. It's a 48-bit number normally represented by six groupings of two hexadecimal numbers

MAC address: A globally unique identifier attached to an individual network interface. It's a 48-bit number normally represented by six groupings of two hexadecimal numbers

MAC filtering: Access points are configured to only allow for connections from a specific set of MAC addresses belonging to devices you trust

Mac OS: Apple's operating system

MACs (Message Authentication Codes): A bit of information that allows authentication of a received message, ensuring that the message came from the alleged sender and not a third party masquerading as them

Maintenance: Where software is updated and hardware issues are fixed if, and when, they occur

Malware: A type of malicious software that can be used to obtain your sensitive information or delete or modify files

Manifest: A library used if an application needs to use a shared library

Master boot record (MBR): a traditional partition table within a storage disk that lets you have volume sizes of 2 terabytes or less and is mostly used in the Windows OS

Master file table (MFT): A way NTFS stores and represents the files you're working with on your operating system

Mb/s: megabit per second, which is a unit of data transfer rate

MD5: A popular and widely used hash function designed in the early 1990s as a cryptographic hashing function

MDM policy: The profiles that contains settings for the device

MDM profile: The policies that contains settings for the device

Meddler in the middle (formerly known as Man in the Middle): An attack that places the attacker in the middle of two hosts that think they're communicating directly with each other

Memory controller chip (MCC): A bridge between the CPU and the RAM

Memory management: One of the functions that a kernel performs; it optimizes memory usage and make sure our applications have enough memory to run

Memory manager: A Windows OS program that helps manage virtual memory

Memory usage: The amount of memory available in your system as well as what memory is currently being used by other applications

Mesh networks: Like ad-hoc networks, lots of devices communicate with each other device, forming a mesh if you were to draw lines for all the links between all the nodes

Metadata: Tells us everything we need to know about a file, including who created it, when it was last modified, who has access to it, and what type of file it is

Metadata: Tells us everything we need to know about a file, including who created it, when it was last modified, who has access to it, and what type of file it is.

Metered connection: An internet connection where all data transfer usage is tracked. Cell phone plans that have a limit on data usage per month or that charge based on usage are examples of metered connections

MIC (Message Integrity Check): It is essentially a hash digest of the message in question

Micro display port: One of the standard power, data and display connector types used in mobile devices

Micro HDMI: One of the standard power, data and display connector types used in mobile devices

Microsoft Install Package(.msi) and MSI files: Microsoft Install Package is a file extension used to guide a program called Windows Installer in the installation, maintenance, and removal of programs of the windows operating systems. MSI files are a combination of of databases that contain installation instructions in different tables along with all the files

Microsoft Terminal Services Client: A client program used to create RDP connections to remote computers

Micro USB: One of the standard power, data and display connector types used in mobile devices

Mini HDMI: One of the standard power, data and display connector types used in mobile devices

Mini USB: One of the standard power, data and display connector types used in mobile devices

Mobile applications: Software that is distributed on mobile OS devices

Mobile device management: A system used to apply and enforce rules about how the device has to be configured and used

Modify: An umbrella permission that includes read and execute and write

Modulation: A way of varying the voltage of a constant electrical charge moving across a standard copper network cable

Monitor mode: It allows to scan across channels to see all wireless traffic being sent by APs and clients

Motherboard: The body or circulatory system of the computer that connects all the pieces together

Mounting: Making a file or hard disk accessible to the computer

Multicast: A way of addressing groups of hosts all at once

Multicast frame: If the least significant bit in the first octet of a destination address is set to one, it means you're dealing with a multicast frame. A multicast frame is similarly set to all devices on the local network signal, and it will be accepted or discarded by each device depending on criteria aside from their own hardware MAC address

Multifactor authentication (MFA): A system where users are authenticated by presenting multiple pieces of information or objects

Multilingual user interface: Interface that offers and support different languages

Multiplexing: It means that nodes on the network have the ability to direct traffic toward many different receiving services

MX record: It stands for mail exchange and this resource record is used in order to deliver email to the correct server

N

Name resolution: This process of using DNS to turn a domain name into an IP address

NAS device: A network attached storage device that has hard drives to automatically create backups and store data

Network: The interconnection of computers

Network Address Translation (NAT): A mitigation tool that lets organizations use one public IP address and many private IP addresses within the network

Network Address Translation (NAT): A mitigation tool that lets organizations use one public IP address and many private IP addresses within the network

Network file system: A protocol that enables files to be shared over a network

Network hardening: Is the process of securing a network by reducing its potential vulnerabilities through configuration changes, and taking specific steps

Networking: Managing, building and designing networks

Networking protocols: A set of rules for how we transfer data in a network

Network layer: It's the layer that allows different networks to communicate with each other through devices known as routers. It is responsible for getting data delivered across a collection of networks

Network port: The physical connector to be able to connect a device to the network. This may be attached directly to a device on a computer network, or could also be located on a wall or on a patch panel

Network separation (network segmentation): A good security principle for an IT support specialists to implement. It permits more flexible management of the network, and provides some security benefits. This is the concept of using VLANs to create virtual networks for different device classes or types

Network software hardening: Includes things like firewalls, proxies, and VPNs

Network stack: A set of hardware or software that provides the infrastructure for a computer

Network switch: It is a level 2 or data link device that can connect to many devices so they can communicate. It can inspect the contents of the Ethernet protocol data being sent around the network, determine which system the data is intended for and then only send that data to that one system

Network time protocol (NTP): A network protocol used to synchronize the time between the authenticator token and the authentication server

Next header field: Defines what kind of header is immediately after this current one

Next hop: The IP address of the next router that should receive data intended for the destination networking question or this could just state the network is directly connected and that there aren't any additional hops needed. Defined as part of the routing table

NIST: National Institute of Standards and Technology

Node: Any device connected to a network. On most networks, each node will typically act as a server or a client

Non-metered connection: A connection where your data usage is not tracked or limited, instead you are charged a flat fee for unlimited and unrestricted usage. A Wi-Fi connection is an example of a non-metered connection

Non-routable address space: They are ranges of IPs set aside for use by anyone that cannot be routed to

Normalization: It's the process of taking log data in different formats and converting it into a standardized format that's consistent with a defined log structure

Northbridge: interconnects stuff like RAM and video cards

NS record: It indicates other name servers that may also be responsible for a particular zone

NTP: Network Time Protocol, keeping clocks synchronized on machines connected to a network

NTP servers: Used to keep all computers on a network synchronized in time

NVMe (NVM Express): interface standard which allows greater throughput of data and increased efficiency

O

OAuth: An open standard that allows users to grant third-party websites and applications access to their information without sharing account credentials

Octet: Any number that can be represented by 8 bits

One-time password (OTP): A short-lived token, typically a number that's entered along with a username and password

One-time password (OTP) tokens: Another very common method for handling multifactor

One-way cryptographic hash: The method used by AD to store passwords

OpenID: An open standard that allows participating sites known as Relying Parties to allow authentication of users utilizing a third party authentication service

OpenLDAP (lightweight directory access protocol): An open source and free directory service

Open source: This means the developers will let other developers share, modify, and distribute their software for free

Open SSH: The most popular program to use SSH within Linux

Operating system: The whole package that manages our computers resources and lets us interact with it

Optical Network Terminator: Converts data from protocols the fiber network can understand to those that are more traditional twisted pair copper networks can understand

Options field: It is sometimes used for more complicated flow control protocols

Organizationally Unique Identifier (OUI): The first three octets of a MAC address

Organizational units (OU): A hierarchical model of objects and containers that can contain objects or more organizational units

Organizational units (OUs): Folders that let us group related objects into units like people or groups to distinguish between individual user accounts and groups that accounts can belong to

OSI model: A model used to define how network devices communicate. This model has seven layers that stack on top of each other: Physical, Data Link, Network, Transport, Session, Presentation, and Application

OTA update: A type of update that is installed by the mobile device itself

Overclocking: it increases the rate of your CPU clock cycles in order to perform more tasks

P

Packaged archives: The core or source software files that are compressed into one file

Packaged managers: An application that makes package installation and removal easier

Packet sniffing (packet capture): the process of intercepting network packets in their entirety for analysis

Padding field: A series of zeros used to ensure the header is the correct total size

Pairing: When a wireless peripheral connects to a mobile device, and the two devices exchange information, sometimes including a PIN or password, so that they can remember each other

Pairwise Transient Key (PTK): It is generated using the PMK, AP nonce, Client nonce, AP MAC address, and Client MAC address

Parameter: A value that is associated with a command

Parent directory & child directories: A parent directory is a directory that houses all subsequent child directories

Parent group: Groups that are principal groups and contain other groups

Partition: A logical division of a hard disk that is treated as a separate unit by operating systems and file systems

Partition table: How the disk is partitioned on an OS

Password attacks: Utilize software like password crackers that try and guess your password

Password salt: Additional randomized data that's added into the hashing function to generate the hash that's unique to the password and salt combination

Patch panel: A device containing many physical network ports

Paths: A main directory that branches off and holds other directories and files

Payload: The actual data being transported, which is everything that isn't a header

Payload length field: 16-bit field that defines how long the data payload section of the datagram is

PBKDF2 (Password Based Key Derivation Function 2): Password Based Key Derivation Function 2

PC: Personal computer, which technically means a computer that one person uses

PCI DSS: Payment Card Industry Data Security Standard

PCI Express: Peripheral Component Interconnect Express

PDA (Personal Digital Assistant): Allows computing to go mobile

Penetration testing: The practice of attempting to break into a system or network to verify the systems in place

Peripherals: the external devices which we connect to our computer that add functionality, like: a mouse, a keyboard, and a monitor

Permission denied: An error message you might find when accessing a protected file

Personal package archives: A software repository for uploading source packages to be built and published

PGP (Pretty Good Privacy) encryption: An encryption application that allows authentication of data along with privacy from third parties relying upon asymmetric encryption to achieve this

Phishing attack: It usually occurs when a malicious email is sent to a victim disguised as something legitimate

PHPLDAPadmin: A tool to manage OpenLDAP

Physical layer: It represents the physical devices that interconnect computers

Physical tokens: They take a few different forms, such as a USB device with a secret token on it, a standalone device which generates a token, or even a simple key used with a traditional lock

PIN authentication method: It uses PINs that are eight-digits long, but the last digit is a checksum that's computed from the first seven digits

Ping flood: It sends tons of ping packets to a system. If a computer can't keep up with this, then it's prone to being overwhelmed and taken down

Pin Grid Array (PGA): CPU socket where the pins are located on the processor itself

PKI system: A system that defines the creation, storage and distribution of digital certificates

Platform as a service: A subset of cloud computing where a platform is provided for customers to run their services

Platform key: It's the public key corresponding to the private key used to sign the boot files

Platform services: A platform for developers to completely build and deploy software applications, without having to deal with OS maintenance, server hardware, networking or other services that are needed to use the platform tools

Plink (PuTTY Link): A tool built into the command line after PuTTY is installed that is used to make remote SSH connections

Pointer resource record: It resolves an IP to a name

Point-To-Point VPN: Establishes a VPN tunnel between two sites but VPN tunneling logic is handled by network devices at either side, so that users don't all have to establish their own connections

Policies: Settings that are reapplied every few minutes, and aren't meant to be changed even by the local administrators

Port: It is a 16-bit number that's used to direct traffic to specific services running on a networked computer

Portable Executable (PE) format: Windows unique version of .exe

Port forwarding: A technique where specific destination ports can be configured to always be delivered to specific nodes

Port mirroring: Allows the switch to take all packets from a specified port, port range, or the entire VLAN and mirror the packets to a specified switch port

Port preservation: A technique where the source port chosen by a client, is the same port used by the router

Ports: Connection points that we can connect devices to that extend the functionality of our computer

POST (Power On Self Test): It figures out what hardware is on the computer

Post-fail analysis: Investigating how a compromise happened after the breach is detected

Post mortem: A way for you to document any problems you discovered along the when recovering data, and the ways you fixed them so you can make sure they don't happen again

Powershell: A shell (program that interprets text commands) for Windows

Power supply: Converts electricity from our wall outlet onto a format that our computer can use

Power user: Above average computer users

Preamble: The first part of an Ethernet frame, it is 8 bytes or 64 bits long and can itself be split into two sections

Precedence: When computers are processing the Group Policy Objects that apply to them, all of these policies will be applied in a specific order based on a set of precedents rules

Presentation layer: It is responsible for making sure that the unencapsulated application layer data is actually able to be understood by the application in question

Pre-shared key: It's the Wi-Fi password you share with people when they come over and want to use your wireless network

Preventative measures: Any procedures or systems in place that will proactively minimize the impact of a disaster

Primary account: The initial account you made during setup

Principle of least privilege: Helps to ensure that sensitive data is only accessed by people who are authorized to access it

Privacy policies: Oversees the access and use of sensitive data

Private cloud: When a company owns the services and the rest of the cloud infrastructure, whether on-site or in a remote data center

Private cloud: When a company owns the services and the rest of the cloud infrastructure, whether on-site or in a remote data center

Processes: Help the computer run programs

Process Explorer: A utility Microsoft created to let IT support specialists and system administrators look at running processes

Process ID: Unique identifier for processes on your computer

Process management: The capacity to manage the many programs in a system - when to run them, the order they run in, how many resources they take up, how long they run, et cetera

Process monitoring: A way of monitoring what processes are happening during installation

Process scheduler: The part of the kernel that makes multitasking possible

Procurement: Hardware is purchased or reused for an employee

Production: The parts of the infrastructure where certain services are executed and serve to its users production

Programming: Coding in a programming language

Programming language: Special languages that software developers use to write instructions for computers to execute

Programs: Basic instructions that tell the computer what to do

Programs: The applications that we can run

Promiscuous mode: A type of computer networking operational mode in which all network data packets can be accessed and viewed by all network adapters operating in this mode

Prompt: A prompt shows you which directory you're currently in

Protocol: A defined set of standards that computers must follow in order to communicate properly is called a protocol

Protocol field: A protocol field is an 8-bit field that contains data about what transport layer protocol is being used

Proxy: Can be useful to protect client devices and their traffic. They also provide secure remote access without using a VPN

Proxy server: An intermediary between a company's network and the Internet, receiving network traffic and relaying that information to the company network

Proxy service: A server that acts on behalf of a client in order to access another service

Pseudo-random: Something that isn't truly random

PSH flag: One of the TCP control flags. PSH is short for push. This flag means that the transmitting device wants the receiving device to push currently- buffered data to the application on the receiving end as soon as possible

Public cloud: The cloud services provided by a third party

Public cloud: The cloud services provided by a third party

Public DNS servers: Name servers specifically set up so that anyone can use them for free

Public key authentication: A key pair is generated by the user who wants to authenticate

Public key signatures: Digital signature generated by composing the message and combining it with the private key

Punch cards: A sequence of cards with holes in them to automatically perform calculations instead of manually entering them by hand

Q

Quad A (AAAA) record: It is very similar to an A record except that it returns in IPv6 address instead of an IPv4 address

Qwiklabs: An online platform which provides training in cloud services

R

RA (Registration Authority): It is responsible for verifying the identities of any entities requesting certificates to be signed and stored with the CA

RAID (redundant array of independent disks): A method of taking multiple physical disks and combining them into one large virtual disk

Rainbow table attacks: To trade computational power for disk space by pre-computing the hashes and storing them in a table

Rainbow tables: A pre-computed table of all possible password values and their corresponding hashes

RAM: Random Access Memory

Random numbers: A very important concept in encryption because it avoids some kind of pattern that an adversary can discover through close observation and analysis of encrypted messages over time

Ransomware: A type of attack that holds your data or system hostage until you pay some sort of ransom

RC4 (Rivest Cipher 4): Asymmetric stream cipher that gained widespread adoption because of its simplicity and speed

Read and execute permission: Permissions that grant you access to read the file that exists and execute it if its runnable

Read permission: Permissions that grant you access to read the file that exists

Read-write replicas: Domain controllers in the Active Directory network that each have a complete copy of the AD database and are able to make changes to it

Receiving address: The MAC address of the access point that should receive the frame

Recoverability: How complicated and time-consuming the recovery effort will be

Recursive name servers: Servers that perform full DNS resolution requests

Re-flash: A way to preserve end-user data on a device that you plan on resetting

Regions: A geographical location containing a number of data centers

Registers: An accessible location for storing the data that our CPU works with

Registrar: An organization responsible for assigning individual domain names to other organizations or individuals

Regular expression: A pattern matching language that describes words, phrases, or more complicated patterns; regular expressions are used to help you do advanced pattern based selection

Reimaging: The process of reimaging involves wiping and reinstalling an operating system using a disk image which is a copy of an operating system

Relative path: It is a path from your current directory

Remote attestation: The idea of a system authenticating its software and hardware configuration to a remote system

Remote Authentication Dial-in User Service (RADIUS): A protocol that provides AAA services for users on a network

Remote connection: The ability to connect an authorized person to a computer or network remotely; allows us to manage multiple machines from anywhere in the world

Remote Desktop Protocol (RDP): A secure network communication protocol developed by Microsoft that allows a user to connect to another device remotely

Remote wipe: A factory reset that you can trigger from your central MDM rather than having to do it in person on the device

Replication: the store directory data is copied and distributed across a number of physically distributed servers but still appears as one unified data store for querying and administering

Replication failure: A reason that a GPO might fail to apply as expected

Repository: A server that acts like a central storage location for packages

Reproduction case: Recreating an error to test a solution to make sure the problem is gone after a fix has been applied

Reset: When an SysAdmin restores or resets the password of a user

Resource monitoring: The most common way to quickly take a peek at how system resources are doing

Restart: A command that will let the machine reboot to complete a domain join

Restoration procedures: A recovery process and process needs to be tested regularly that is documented and accessible so that anyone with the right access can restore operation when needed

Resultant set of policy (RSOP): The policy that forms when all of the group policies have been grouped together for a specific machine and apply precedence rules to them

Retirement: Hardware becomes unusable or no longer needed, and it needs to be properly

removed from the fleet

Return merchandise authorization (RMA): The process of receiving returned merchandise and authorizing a refund

Reverse lookup zone files: They let DNS resolvers ask for an IP, and get the FQDN associated with it returned

Reverse proxy: A service that might appear to be a single server to external clients, but actually represents many servers living behind it

Reverse proxy: A service that might appear to be a single server to external clients, but actually represents many servers living behind it

RGB model: RGB or red, green, and blue model is the basic model of representing colors

Risk: The possibility of suffering a loss in the event of an attack on the system

Risk assessment: Allows you to prioritize certain aspects of the organization that are more at risk if there's an unforeseen event

Risk mitigation: Understanding the risks your systems face, take measures to reduce those risks, and monitor them

Rogue Access Point (AP) Attack: An access point that is installed on the network without the network administrator's knowledge

Rogue DHCP server attack: An attacker can hand out DHCP leases with whatever information they want by deploying a rogue DHCP server on your network, setting a gateway address or DNS server, that's actually a machine within their control

Role-based access control (RBAC): The process of changing a persons group that they are a part of when they have changed roles within a company to limit or change their access to resources

Rollback: Reverting to the previous state before you made changes

ROM chip (Read Only Memory): A read-only memory chip where the BIOS is stored

Root cause: The main factor that's causing a range of issues

Root certificate authority: They are self signed because they are the start of the chain of trust, so there's no higher authority that can sign on their behalf

Root directory: A parent directory for all other directories in a file system

Rootkit: A collection of software or tools that an admin would use

Root user: It is the first user that gets automatically created when we install a Linux OS and has all the privileges on the OS. Also called the super user. There's technically only one superuser

or root account, but anyone that's granted access to use their powers can be called a superuser too

Round robin: It is a concept that involves iterating over a list of items one by one in an orderly fashion

Router: A device that knows how to forward data between independent networks

Router: A device that knows how to forward data between independent networks

Routing protocols: Special protocols the routers use to speak to each other in order to share what information they might have

RPM: Revolutions per minute

RSA: One of the first practical asymmetric cryptography systems to be developed, named for the initials of the three co-inventors: Ron Rivest, Adi Shamir and Leonard Adleman

RSOP report: The process of troubleshooting group policy and comparing what you expect to be applied to a computer and the resultant set of policy report

RST flag: One of the TCP control flags. RST is short for reset. This flag means that one of the sides in a TCP connection hasn't been able to properly recover from a series of missing or malformed segments

S

SACL's: System Access Control List

Safe operating temperature: The temperature range in which rechargeable batteries must be kept in order to avoid demanage

SATA: The most popular serial ATA drive, which uses one cable for data transfers

Scalability: The measure of a system's ability to increase or decrease in performance and cost in response to varying loads in system processing demands

Screen lock: A security feature that helps prevent unwanted access by creating an action you have to do to gain entry

Script: It is run by an interpreter, which interprets the code into CPU instructions just in time to run them

Scripting: Coding in a scripting language

Scripts: Mainly used to perform a single or limited range task

SD devices: Mass storage devices like hard drives

SDRAM: It stands for Synchronous DRAM, this type of RAM is synchronized to our systems' clock speed allowing quicker processing of data

Secondary or stand-by machine: A machine that is the same as a production machine, but won't receive any traffic from actual users until enabled

Secure boot protocol: It uses public key cryptography to secure the encrypted elements of the boot process

Secure channel: It is provided by IPsec, which provides confidentiality, integrity, and authentication of data being passed

Secure copy: A command you can use in Linux to copy files between computers on a network

Secure element: It's a tamper resistant chip often embedded in the microprocessor or integrated into the mainboard of a mobile device

Secure Shell (SSH): A secure network protocol that uses encryption to allow access to a network service over unsecured networks

Security: It's all about determining risks or exposure understanding the likelihood of attacks; and designing defenses around these risks to minimize the impact of an attack

Security account manager (SAM): A database in windows that stores user names and password

Security filtering: A tool to make group policies apply more selectively

Security group: One of the two categories that groups in Active Directories can be part of, they can contain user accounts, computer accounts or other security groups

Security information and event management systems (SIEMS): Form of centralized logging for security administration purposes

Security keys: Small embedded cryptoprocessors, that have secure storage of asymmetric keys and additional slots to run embedded code

Security patch: A piece of software that is meant to fix up a security hole

Security principal: Any entity that can be authenticated by the system, such as a user account, a computer account, or a thread or process that runs in the security context of a user or computer account

Security through obscurity: The principle that if no one knows what algorithm is being used or general security practices, then one is safe from attackers

Seed value: A secret value that is used to initialize a process that is generated by software using one or more values

Self-signed certificate: This certificate has been signed by the same entity that issued the certificate

Sequence control field: A field that is 16 bits long and mainly contains a sequence number used to keep track of ordering the frames

Sequence number: A 32-bit number that's used to keep track of where in a sequence of TCP segments this one is expected to be

Serial number: A unique identifier for their certificate assigned by the CA which allows the CA to manage and identify individual certificates

Server: A device that provides data to another device that is requesting that data, also known as a client

Server: Software or a machine that provides services to other software or machines

Server logs: Text files that contains recorded information about activities performed on a specific web server in a defined period of time

Server operating systems: Regularly operating systems that are optimized for server functionality

Server or Service: A program running on a computer waiting to be asked for data

Servers: Devices that provide data to other devices that request that data, also known as a client

Service discovery: One of the services that the domain controller provides to the clients

Service type field: A eight bit field that can be used to specify details about quality of service or QoS technologies

Session hijacking (cookie hijacking): A common meddler in the middle attack

Session key: The shared symmetric encryption key using TLS sessions to encrypt data being sent back and forth

Session layer: The network layer responsible for facilitating the communication between actual applications and the transport layer

Session manager subsystem: Process that is in charge of setting some stuff up to work for the OS

Severity: Includes factors like what and how many systems were compromised and how the breach affects business functions

SHA1: It is part of the secure hash algorithm suite of functions, designed by the NSA and published in 1995

Shannon's maxim: It states that the system should remain secure, even if your adversary knows exactly what kind of encryption systems you're employing, as long as your keys remain secure

Shared folders: A way to share files between computers on the same network on Windows

Shell: A program that interprets text commands and sends them to the OS to execute

Shortcut: An entry in the MFT that has a reference to some destination, so that when you open it up, you get taken to that destination

Short-range wireless network: It is what mobile devices uses to connect to their peripherals

Side-by-side assemblies: A system that manages most shared libraries and resources on Windows and supports access to multiple versions of the same shared library automatically

Side-loading: A process of installing mobile apps directly without using an app store

Signal: A way to tell a process that something has just happened

Simple authentication and security layer (SASL): The authentication method that can employ the help of security protocols like TLS, it requires the client and the directory server to authenticate using some method

Simple permissions: Special or specific permissions

Simplex communication: A form of data communication that only goes in one direction across a cable

Single point of failure: When one system in a redundant pair suffers a failure

Single sign on (SSO): An account that grants you access to multiple accounts without require constant entry of a password or username

SOC (System On a Chip): Packs the CPU, Ram, and sometimes even the storage onto a single chip

Social engineering: An attack method that relies heavily on interactions with humans instead of computers

Socket: The instantiation of an endpoint in a potential TCP connection

Softlinks: A shortcut in Linux, that allows us to link to another file using a file name

Software: The intangible instructions that tell the hardware what to do

Software as a Service (SaaS): A way of licensing the use of software to others while keeping that software centrally hosted and managed

Software bug: An error in software that causes unexpected results

Software management: A broad term used to refer to any and all kinds of software that are designed to manage or help manage some sort of project or task

Software services: The services that employees use that allow them to do their daily job functions, such as word processors, Internet browsers, email clients, chat clients, and more

Software signing certificate: Trust mechanism where a software vendor can cryptographically sign binaries they distribute using a private key

Source MAC address: The hardware address of the device that sent the ethernet frame or data packet. In the data packet it follows the destination MAC address

Source port: A high numbered port chosen from a special section of ports known as ephemeral ports

Southbridge: It maintains our IO or input/output controllers, like hard drives and USB devices that input and output data

Spear phishing: Phishing that targets individual or group - the fake emails may contain some personal information like your name, or the names of friends or family

Spoofing: When a source is masquerading around as something else

Spyware: The type of malware that's meant to spy on you

SQL Injection Attack: An attack that targets the entire website if the website is using a SQL database

SRV record: A service record used to define the location of various specific services

SSD: Solid State Drive

SSH (Secure shell): A protocol implemented by other programs to securely access one computer from another

SSH authentication key: A secure authentication method for accessing a computer from other device

SSH client: A program you must have installed on your device in order to establish an SSH connection with another device

SSH server: Software installed on a machine that allows for that device to accept an SSH connection

SSL/TLS Client Certificate: Certificates that are bound to clients and are used to authenticate the client to the server, allowing access control to a SSL/TLS service

SSL 3.0: The latest revision of SSL that was deprecated in 2015

Standard error (stderr): A data stream that redirects the output of error messages in a different output stream. It works both in Linux and Windows

Standard In (stdin): A data stream in which the input that you provide through the keyboard goes to the standard in stream of the process that you're interacting with. It works both in Linux and Windows

Standardization: A systematic way of naming hosts

Standard out (stdout): A data stream that, when a process creates output, it adds data to the standard out stream, which flows out of the process. It works both in Linux and Windows

Standard user: A user who is given access to the machine but has restricted access to do thing like install software or change certain setting

Standoffs: Used to raise and attach your motherboard to the case

Start Frame Delimiter (SFD): The last byte in the preamble, that signals to a receiving device that the preamble is over and that the actual frame contents will now follow

Start of authority: A declaration of the zone and the name of the name server that is authoritative for it

StartTLS: It permits a client to communicate using LDAP v3 over TLS

Static IP address: An IP address that must be manually configured on a node

Steganography: The practice of hiding information from observers, but not encoding it

Stream ciphers: It takes a stream of input and encrypts the stream one character or one digit at a time, outputting one encrypted character or digit at a time

Subdirectories: A directory below or at a deeper level in the directory hierarchy

Subject: This field contains identifying information about the entity the certificate was issued to

Subject Public Key Info: These two subfields define the algorithm of the public key along with the public key itself

Subnet mask: 32-bit numbers that are normally written as four octets of decimal numbers

Subnetting: The process of taking a large network and splitting it up into many individual smaller sub networks or subnets

Substitution cipher: An encryption mechanism that replaces parts of your plaintext with ciphertext

Suspended apps: A command that will tell the OS to suspend background mobile apps

Swap space: The allocated space where the virtual memory is stored on the hard drive when the amount of physical memory space is used up or full

Switches: Devices that help our data travel

Symbolic links: Work similarly to shortcuts, but at the file system level. The key difference is that the operating system treats them like substitutes for the file they're linked to in almost every meaningful way

Symmetric Digital Subscriber Line (SDSL): A device that establishes data connections across phone lines and has upload and download speeds that are the same

Symmetric key algorithm: Encryption algorithms that use the same key to encrypt and decrypt messages

SYN_RECEIVED: A TCP socket state that means that a socket previously in a listener state, has received a synchronization request and sent a SYN_ACK back

SYN_SENT: A TCP socket state that means that a synchronization request has been sent, but the connection hasn't been established yet

SYN flag: One of the TCP flags. SYN stands for synchronize. This flag is used when first establishing a TCP connection and make sure the receiving end knows to examine the sequence number field

SYN flood: The server is bombarded with SYN packets

Sysinternals package: A set of tools released by Microsoft that can help you troubleshoot

System: A group of hardware components and software components that work together to fun the programs or processes in the computer

System Administration: The field in IT that is responsible for maintaining reliable computer systems, in a Multi-user environment

System properties: A control panel applet that allows you to edit the size and number and location of paging files

Systems administrator (sysadmin): A person who works only in system administration, configuring servers, monitoring the network, provisioning, or setting up new users in computers and taking responsibility of systems

System settings: Settings like display resolution, user accounts, network, devices, etc

System software: Software used to keep our core system running, like operating system tools and utilities

T

Tab completion: A way to auto-complete a command or file names and directories

TACACS+: It is a device access AAA system that manages who has access to your network devices and what they do on them

Tailgating: Gaining access into a restricted area or building by following a real employee in

Task bar: It gives us quick options and shows us information like network connectivity, the date, system notifications, sound etc

Task Manager: A Windows utility that allows you to gain information about what tasks you have running in the background

T-Carrier technologies: Technologies Invented to transmit multiple phone calls over a single link. Eventually, they also became common transmission systems to transfer data much faster than any dial-up connection could handle

TCP checksum: A mechanism that makes sure that no data is lost or corrupted during a transfer

Tcpdump: It's a super popular, lightweight command-line based utility that you can use to capture and analyze packets

TCP segment: A payload section of an IP datagram made up of a TCP header and a data section

TCP window: The range of sequence numbers that might be sent before an acknowledgement is required

Terminal: A text based interface to the computer

Termination signal: A kill command that will stop whatever process you tell it to

Test environment: A virtual machine running the same configuration as a production environment, but isn't actually serving any users of the service

Thermal paste: A substance used to better connect our CPU and heat sink, so the heat transfers from to the other better

Threat: The possibility of danger that could exploit a vulnerability

Threats & password policies: Protects Data & IP, Data Protection, Infrastructure Defense, Identity Management, and users

Ticket granting service (TGS): It decrypts the Ticket Granting Ticket using the Ticket Granting Service secret key, which provides the Ticket Granting Service with the client Ticket Granting Service session key

Time-based token (TOTP): A One-Time-Password that's rotated periodically

Time slice: A very short interval of time that gets allocated to a process for CPU execution

Time-To-Live field (TTL): An 8-bit field that indicates how many router hops a datagram can traverse before it's thrown away

TKIP (Temporal Key Integrity Protocol): To address the shortcomings of WEP security

TLS 1.2: The current recommended revision of SSL

TLS 1.2 with AES GCM: A specific mode of operation for the AES block cipher that essentially turns it into a stream cipher

TLS Handshake: A mechanism to initially establish a channel for an application to communicate with a service

Top Level Domain (TLD): The top level of the DNS or the last part of a domain name. For example, the “com” in www.weather.com

Total hops: The total number of devices data passes through to get from its source to its destination. Routers try to choose the shortest path, so fewest hops possible. The routing table is used to keep track of this

Total length field: A 16-bit field that indicates the total length of the IP datagram it's attached to

TPM (Trusted Platform Module): This is a hardware device that's typically integrated into the hardware of a computer, that's a dedicated crypto processor

Traffic class field: An 8-bit field that defines the type of traffic contained within the IP datagram and allows for different classes of traffic to receive different priorities

Transfer Control Protocol (TCP): A protocol that handles reliable delivery of information from one network to another

Transmission Control Protocol (TCP): The data transfer protocol most commonly used in the fourth layer. This protocol requires an established connection between the client and server

Transmitter address: The MAC address of whatever has just transmitted the frame

Transport layer: The network layer that sorts out which client and server programs are supposed to get the data

Transport mode: One of the two modes of operations supported by IPsec. When used, only the payload of the IP packet is encrypted, leaving the IP headers untouched

Trim: A command to delete unused data blocks so the space can be used for the computer’s storage needs

Trojan: Malware that disguises itself as one thing but does something else

Troubleshooting: The ability to diagnose and resolve a problem

Trusted execution environment (TEE): It provides a full-blown isolated execution environment that runs alongside the main OS

TTL: The lifetime limit of data given in seconds. This number can be configured by the owner of a domain name for how long a name server is allowed to cache in entry before it should discard it and perform a full resolution again

Tunnel: It is provided by L2TP, which permits the passing of unmodified packets from one network to another

Tunnel mode: One of the two modes of operations supported by IPsec. When used, the entire IP packet, header, payload, and all, is encrypted and encapsulated inside a new IP packet with new headers

Twisted pair cable: The most common type of cabling used for connecting computing devices. It features pairs of copper wires that are twisted together

Two-factor authentication: A technique where more than just a username and password are required to authenticate. Usually, a short-lived numerical token is generated by the user through a specialized piece of hardware or software

TXT record: It stands for text and was originally intended to be used only for associating some descriptive text with a domain name for human consumption

Type-C connector: A type of USB connector meant to replace many peripheral connections

Types of DNS servers: There are five primary types of DNS servers; caching name servers, recursive name servers, root name servers, TLD name servers, and authoritative name servers

U

U2F (Universal 2nd Factor): It's a standard developed jointly by Google, Yubico and NXP Semiconductors that incorporates a challenge-response mechanism, along with public key cryptography to implement a more secure and more convenient second-factor authentication solution

Ubuntu: The most popular Linux consumer distribution

UEFI: United Extensible Firmware Interface, a new standard for BIOS

Unbind: It closes the connection to the LDAP server

Unicast transmission: A unicast transmission is always meant for just one receiving address

Uniform Resource Locator (URL): A web address similar to a home address

Universal: The tool that is used to group global roles in a forest

Unix epoch: It is the number of seconds since midnight on January first, 1970. It's a 'Zero Hour' for Unix based computers to anchor their concept of time

Urgent pointer field: A field used in conjunction with one of the TCP control flags to point out particular segments that might be more important than others

URG flag: One of the TCP control flags. URG is short for urgent. A value of one here indicates that the segment is considered urgent and that the urgent pointer field has more data about this

USB (Universal Serial Bus): A connection standard for connecting peripherals to devices such as computers

USB-C adapter: One of the standard power, data and display connector types used in mobile devices

User configuration: Contained within a Group Policy Object (GPO)

User Datagram Protocol (UDP): A transfer protocol that does not rely on connections. This protocol does not support the concept of an acknowledgement. With UDP, you just set a destination port and send the data packet

User Groups: The management of resources on a computer and on a network through organizing user accounts into various groups

User name: A unique identifier for a user account

Username and password authentication: Can be used in conjunction with certificate authentication, providing additional layers of security

User space: The aspect of an operating system that humans interact with directly like programs, such as text editors, music players, system settings, user interfaces, et cetera

UTF-8: The most prevalent encoding standard used today

UUID: Universally Unique ID

V

Validity: This field contains two subfields, Not Before and Not After, which define the dates when the certificate is valid for

Variable: Files that constantly change

Vendor risk review: Questionnaire that covers different aspects of their security policies procedures and defenses

Version: What version of the X.509 standard certificate adheres to

Version field: First field in an IP header that specifies the version of IP

Virtual Box: An application you can use to install Linux and have it completely isolated from your machine

Virtual instance: A single virtual machine

Virtualization: A single physical machine called a host runs many individual virtual instances called guests

Virtual LAN (VLAN): It is a technique that lets you have multiple logical LANs operating on the same physical equipment

Virtual machine (VM): An application that uses physical resources like memory, CPU and storage, but they offer the added benefit of running multiple operating systems at once

Virtual memory: A combination of hard drive space and RAM that acts like memory which our processes can use

Viruses: The best known type of malware

VLAN header: A piece of data that indicates what the frame itself is. In a data packet it is followed by the EtherType

Volume: A format for a filesystem on a partition

VPN (Virtual Private Network): A secure method of connecting a device to a private network over the internet

Vulnerability: A flaw in the system that could be exploited to compromise the system

Vulnerability scanner: Detect lots of things, ranging from misconfigured services that represent potential risks, to detecting the presence of back doors and systems

W

WannaCry Attack: A cyber attack that started in Europe and infected hundreds of thousands of computers across the world

Web of trust: It is where individuals instead of certificate authorities sign other individuals' public keys

Web server: A web server stores and serves content to clients through the Internet.

WEP (Wired Equivalent Privacy): First security protocol introduced for Wi-FI networks

Wide area network: Acts like a single network but spans across multiple physical locations. WAN technologies usually require that you contract a link across the Internet with your ISP

Wi-Fi Protected Access (WPA): A security program that uses a 128-bit key to protect wireless computer networks, which makes it more difficult to crack than WEP

Wildcard: A character that is used to help select files based on a certain pattern

Windows domain: A network of computers and users that are added to a central database

Windows management instrumentation (WMI): The container that is used to define powerful targeting rules for your GPO

Windows registry: A hierarchical database of settings that Windows, and Windows applications, use for storing configuration data

Windows Search service: A service that indexes files on your computer by looking through them on a schedule

Windows store: A Windows store is an application repository or warehouse where you can download and instal universal Windows platform apps

Windows update client service: System that runs in the background on your computer to download and install updates and patches for your operating system

Wired Equivalence Privacy (WEP): An encryption technology that provides a very low level of privacy. WEP should really only be seen as being as safe as sending unencrypted data over a wired connection

Wireless access point: A device that bridges the wireless and wired portions of a network

Wireless LANS (WLANS): One or more access points act as a bridge between a wireless and a wired network

Wireless networking: Networks you connect to through radios and antennas

Wireshark: It's another packet capture and analysis tool that you can use, but it's way more powerful when it comes to application and packet analysis, compared to tcpdump

WMI filter: A tool to make group policies apply more selectively on the configuration of the computer

Work group computer: A Windows computer that isn't joined to a domain

World Wide Web (WWW): The information system that enables documents and other web resources to be accessed over the Internet

Worms: They are similar to viruses except that instead of having to attach themselves onto something to spread, worms can live on their own and spread through channels like the network

WPA (Wi-fi protected access): Designed as a short-term replacement that would be compatible with older WEP-enabled hardware with a simple firmware update

WPA2 Enterprise: It's an 802.1x authentication to Wi-Fi networks

WPS (Wifi Protected Setup): It's a convenience feature designed to make it easier for clients to join a WPA-PSK protected network

Write permission: A permission that allows you to make changes to a file

X

X.500 directory: The agreed upon directory standard that wa approved in 1988 that includes, DAP, DSP, DISP, DOP, DAP, and LDAP

X.509 standard: It is what defines the format of digital certificates, as well as a certificate revocation list or CRL

XTACACS: It stands for Extended TACACS, which was a Cisco proprietary extension on top of TACACS

Z

Zone Files: Simple configuration files that declare all resource records for a particular zone

0-Day Vulnerability (Zero Day): A vulnerability that is not known to the software developer or vendor, but is known to an attacker