# The CIA Triad

**Confidentiality**

* Prevent unauthorized disclosure of information from prying eyes.

**Integrity**

* Used to prevent unauthorized modification, tampering or corrupting of data.

**Availability**

* Ensure information is available when needed.

# AAA Concept

**Authentication**

* Verifies a user’s identification via the process of logging into a system.

**Authorization (Access Control)**

* Determines what a user has the authority to do and have access to.

**Accounting**

* Tracks and records user access and actions with system logs.

# Least Privilege Concept

A user, system, process, or application is only given the permissions necessary to compete its assigned tasks or functions and nothing more.

# Risk Management

**Risk Management** is the process of identifying, assessing, monitoring, and limiting risk to an acceptable level.

# Risk Assessment Process

A **risk assessment**, where risks are identified and assessed, is the first step in the risk management process.

Example Risk Assessment Process:

1. Identify and categorize your risks
2. Assess each risk’s probability and impact
3. Assign each risk a risk score and prioritize accordingly
4. Respond Accordingly

# Risk Response Categories

**Avoidance**: The process of eliminating a risk by not engaging in an activity. We avoid a risk by eliminating its source altogether.

**Acceptance**: Accepting an identified risk, meaning no action will be taken when a risk assessment score is low.

**Mitigation**: The process of taking steps to minimize the impact of a risk.

**Transference**: Transferring the responsibility of a risk to a third party, such insurance.

# Attack Surface

An **attack surface** is a vulnerability. It’s any way an attacker can gain access to pose a security risk.

There are three common attack surfaces:

* Application
* Network
* User

# Social Engineering

Social engineering bypasses technology protections by using a variety of different tactics and methods to **encourage another person** to **perform a specific action** or **give up a piece of crucial information**.

# Social Engineering Attacks

**Conning and flattery:** Social engineering attacks often start as simple con jobs.

**Phishing:** Phishing is the practice of sending unwanted email to users with the purpose of tricking them into revealing personal information (such as bank account information) or clicking on a link.

# Social Engineering Attacks

**Dumpster diving:** Dumpster diving is the practice of searching through trash to gain information from discarded documents.

Social Engineering Attacks

**Piggybacking or tailgating:** Piggybacking or tailgating occurs when one user follows closely behind another use without using valid credentials. It can often be prevented with a mantrap.

# Social Engineering Attacks

**Impersonation:** Impersonation is a specific social engineering tactic where an attacker masquerades as someone else, such as a repair technician.

**Physical & Logical Access Control**

**Physical** security includes implementing different access control methods with technology you can touch. Physically locking down the equipment and securing the building.

**Logical** security methods include those elements that are implemented through technological means. Password policies, logical access control lists, etc.

# Common Physical Access Control Measures

* Employee ID Badges
* Physical Access Logs
* Door Access Systems
* Proximity Cards
* Mantraps
* Hardware Locks
* Video Surveillance
* Security Guards
* Building Alarms
* Fences

# Common Logical Access Control Measures

* Access Control Lists
* NTSF Permissions
* Windows Group Policies
* Password Policies
* Account Policies
* Device Policies

# Methods to Keep Devices Secure

* Computer Security Cable Locks
* Server Security Racks
* Secure Server Rooms
* Locked Offices
* In-Room Safes

# Removable & Mobile Device Security

* Education, Training, Policies, and Procedures
* Device Encryption: BitLocker to Go
* Remote Data Wiping Software
* Disabling USB and SD Ports
* Physically Blocking Ports

# Keyloggers

* A keylogger is a device that captures keyboard input.
* Can be:
  + Physical (USB)
  + Logical (Software)
  + Wireless (Transmission & Wireless Keyboards)

**Prevention**:

* Physical inspection, Anti-malware Software, and Encrypted Wireless Keyboards

# Wireless Encryption Standards

* Wireless Equivalent Privacy (**WEP**) - Compromised
* Wi-Fi Protected Access (**WPA**) - Compromised
* Wi-Fi Protected Access 2 (**WPA2**) – Current Standard

# WPA Personal Mode

* Uses “Pre-Shared Keys” for authentication.
* Pre-Shared Key = Password
* Common for small wireless networks without an authentication serve:
  + home, small office, coffee shop, airport, etc.

# WPA Enterprise Mode

* WPA-802.1x Standard
* Used with a central authentication server, such as Windows Active Directory
* Requires the use of a **RADIUS** authentication server
* Uses **EAP** (extensible authentication protocol) for authentication

# Authentication Basics

* Authentication is the process of determining if someone or something is, in fact, who it declares itself to be through the use of authentication technology.
* Can be used to prove the identity of:
  + A User
  + A Service or Process Running on a Computer or Server
  + A Workstation or Server Itself
  + A Network Device

# Three Factors of Authentication

**Something You Know**

* + Password
  + PIN

**Something You Have**

* + Smart Card
  + RSA Token

**Something You Are**

* + Biometrics

# Multi-Factor Authentication

* **Multi-Factor Authentication is a Common Practice to Increase Security**
  + Uses a combination of two of the three factors of authentication (something you have, something you know, something you are)
  + **Examples**:
    - **Banks**: ATM Card & PIN
    - **Gym Access**: Biometrics Palm Scan & ID Card
    - **Work ID Badges:** SmartID Card & PIN Number

# Remote Access Authentication via RADIUS

Remote Access:

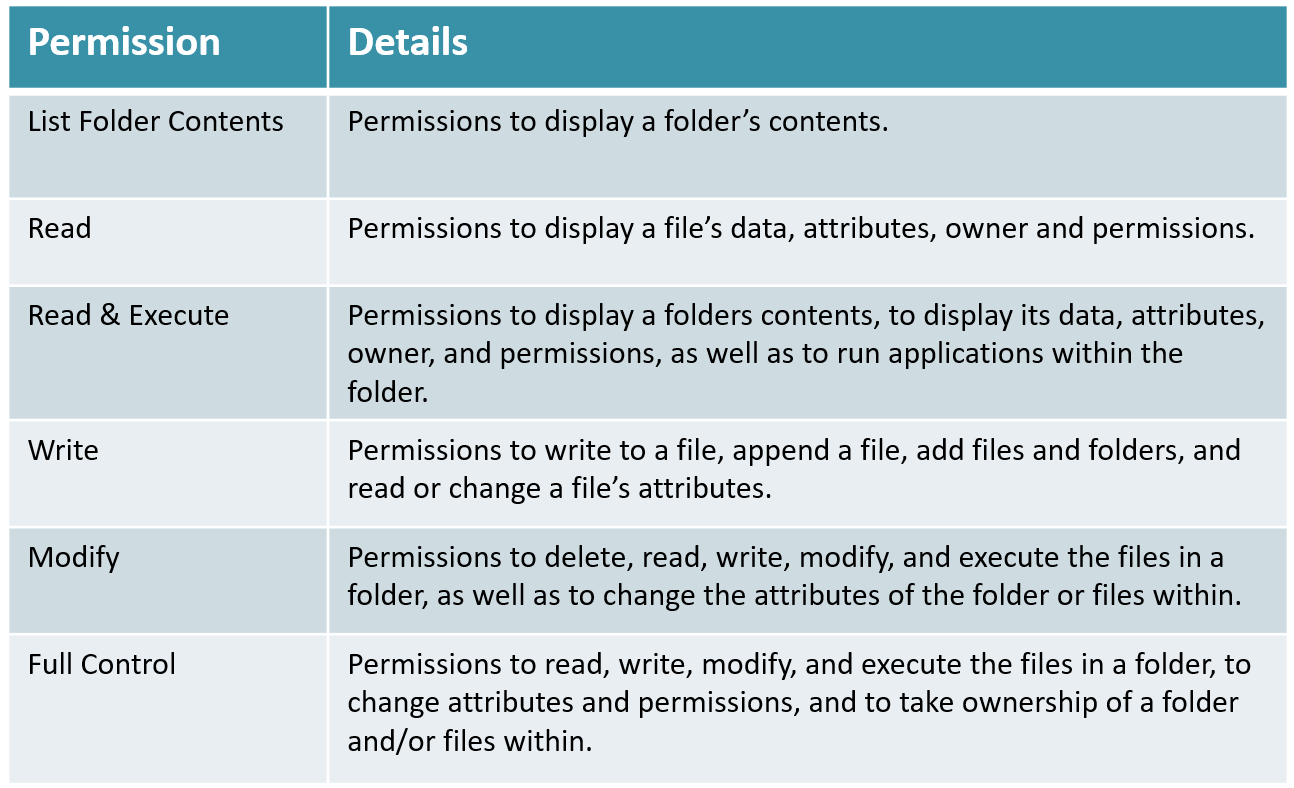
Ability to login to a network remotely from geographically distant locations

VPN Access

Remote network administration

Wireless Access with 802.1x

# Basic NTFS Permissions



# NTFS Inheritance

* In NTFS, permissions applied to a parent folder are automatically inherited by subfolder and files (child objects).
* This is called **inherited permissions**. We can break inheritance by telling Windows
* **Explicit permissions** are those that are set by default on parent objects when it’s created, or by user action on parent or child objects.

# Moving & Copying Files/Folders in Same Partition

**Copying Files and Folders**

* Inherits the destination folder permissions.

**Moving Files and Folders**

* Will retain its original permissions.

# Moving & Copying Files/Folders to Different Partition

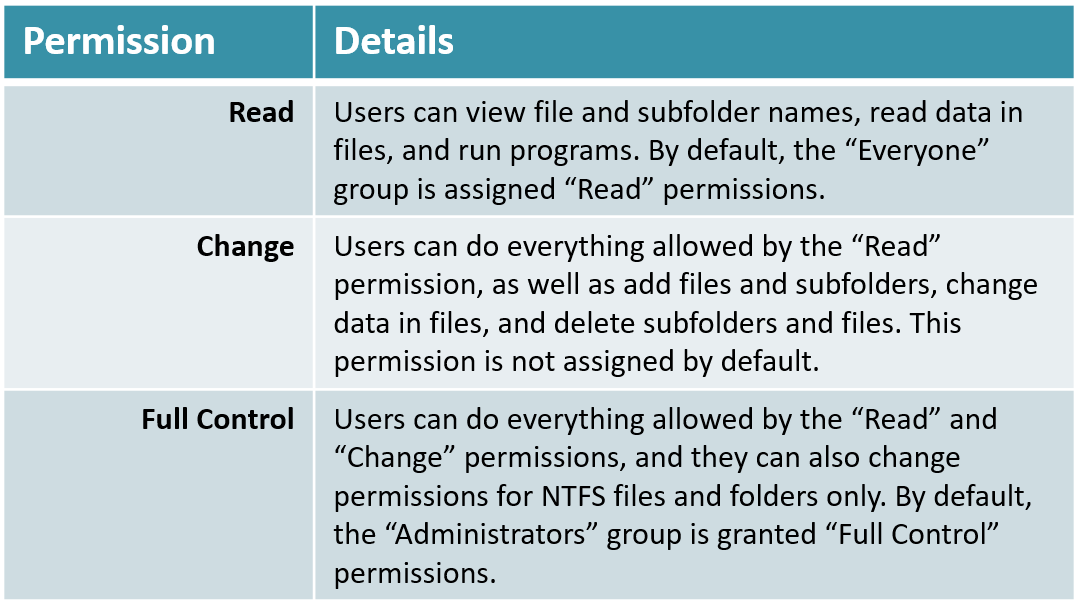
**Copying Files and Folders**

* Inherits the destination folder permissions.

**Moving Files and Folders**

* Inherits the destination folder permissions.

# Network Share Permissions



# Network Share vs. NTFS Permission

When share and NTFS permissions are used simultaneously, the most restrictive permission always wins.

# Active Directory (AD) Groups

* Groups are used to collect user accounts, computer accounts, and other groups into manageable units. Working with groups instead of with individual users helps simplify network maintenance and administration.
* There are two types of groups in Active Directory:
  + **Distribution groups:** Used to create email distribution lists (Microsoft Exchange Server).
  + **Security groups:** Used to assign permissions to shared resources.

# AD Security Groups

* Security groups provide an efficient way to assign access to resources on your network.
* By using security groups, you can:
  + Assign user rights to security groups in Active Directory.
  + Assign permissions to security groups for resources.

# AD Group Scope

* Groups are characterized by a scope that identifies the extent to which the group is applied in an Active Directory domain.
* The scope defines where the group can be granted permissions.
* There are three scopes of groups in AD:
  + Universal
  + Global
  + Domain Local

# Domain Local Groups

Used to manage access permissions to resources (files, folders and other types of resources) only in the domain where it was created.

# Global & Universal Groups

**Global Groups**

* Used to provide access to resources in the another domain.

**Universal Groups**

* Recommended for use in large Active Directory forests.
* Using this group scope, you can define roles and manage resources that are distributed across multiple domains.

# AD Organizational Units

* An organizational unit (OU) is a container in AD, where you can place users, groups, computers, and other OUs.
* Typically OUs mirror an organization’s business structure.
* OUs are used to assign group policy settings and account permissions.
* With OUs, you can also delegate administrator tasks to specific user(s) and/or group(s) within making them Domain Administrators.

# Windows Registry

* Windows Registry is a database that stores Operating System, hardware, software, and user configuration as well as security policy settings.
* It’s configured in a hierarchical system composed of hives, keys, and values.
* It can be modified via the Registry Editor, but modifying it and not knowing what you’re doing can significantly or permanently damage your operating system.

# Registry Hives, Keys, and Values

* The primary folders are called **hives**. There are five main **hives**:
  + HKEY\_CLASSES\_ROOT
  + HKEY\_CURRENT\_USER
  + HKEY\_LOCAL\_MACHINE
  + HKEY\_USERS
  + HKEY\_CURRENT\_CONFIG
* Each **hive** contains sub-folders called **keys**. **Keys** can contain **sub-keys** and **values**.
* **Values** contain the actual information stored in the Registry.

# Registry Permissions

* Registry permissions are configured at the top level and inherited by child objects.
* Permissions can be viewed and modified by right-clicking a registry object.
* The registry uses two NTFS permissions:
  + **Read**: Permission to read key contents, but not save any registry changes.
  + **Full Control**: Permission to open, edit, and take ownership of a registry key.

# Microsoft Password Complexity Requirements

Not contain the user's account name or parts of the user's full name that exceed two consecutive characters

Be at least six characters in length

Contain characters from three of the following four categories:

* English uppercase characters (A through Z)
* English lowercase characters (a through z)
* Base 10 digits (0 through 9)
* Non-alphabetic characters (for example, !, $, #, %)
* Complexity requirements are enforced when passwords are changed or created.

# Microsoft Minimum Password Length

We can also enable Microsoft’s **Minimum password length** policy to further make a password more secure, which ensures user passwords are complex. This value is set to 7 by default for the Default Domain Policy in AD.

# Microsoft Enforce Password History

We can also enable Microsoft’s **Enforce Password History** policy to further make a password more secure, which ensures user’s don’t reset their password to previously used passwords. This value is set to 24 by default for the Default Domain Policy in AD.

# Microsoft Maximum Password Age

We can also enable Microsoft’s **Maximum Password Age** policy to further make a password more secure, which ensures are changed after a certain amount of time. This value is set to 42 by default for the Default Domain Policy in AD.

# Microsoft Minimum Password Age

We can also enable Microsoft’s **Minimum Password Age** policy to further make a password more secure, which ensures users must wait a certain amount of time before they can change a password. This value is set to 2 by default for the Default Domain Policy in AD.

# Microsoft Reversible Encryption

We can also enable Microsoft’s **Store Passwords using Reversible Encryption** policy if we want to be able to decrypt passwords and view them in plain text. This is not recommended and is disabled in the Default Domain Policy in AD. When disabled, passwords are stored as a hash that cannot be decrypted.

# Microsoft Account Lockout Threshold

In Windows 10 and Active Directory, we can enable Microsoft’s **Account Lockout Threshold** policy, which determines the number of failed logon attempts that causes a user account to be locked out. This is set to 0 by default in the Default Domain Policy in AD.

# Microsoft Account Lockout Duration

We can also enable Microsoft’s **Account Lockout Duration** policy, which determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. This is not defined by default in the Default Domain Policy in AD.

# Microsoft Reset Account Lockout Counter

We can also enable Microsoft’s **Reset Account Lockout Counter After** policy, which determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts. This is not defined by default in the Default Domain Policy in AD.

# Common Password Attack Methods

**Social Engineering**

* Phishing, conning, and deception.

**Key Loggers**

* Key logging passwords.

**Network Sniffing**

* Sniffing for plain text unencrypted network traffic.

# Common Password Attack Methods

**Dictionary Attacks**

* Tries every word in a dictionary.

**Brute Force Attacks**

* Tries all possible password combinations.

**Rainbow Tables**

* A large table with pre-calculated hashes and their associated password.

# Computer Audit Trails

An *audit trail* is a series of records of computer events, about an operating system, an application, or user activities.

A computer system may have several audit trails, each devoted to a particular type of activity.

# Audits Logs Provide Nonrepudiation

* **Nonrepudiation** is the assurance that someone cannot deny something.
* Logging events into audit logs provides nonrepudiation.

# Types of Audits

* We can audit the “success” or “failure” of an event.
* For example:
  + User Login Success
  + File Access Failure

# What Can Be Audited?

* Account Logon Events
* Account Management
* Directory Service Access
* Logon Events
* Object Access
* Policy Change
* Privilege Use
* Process Tracking
* Audit System Events

# Saving Audit Information

Audit logs should be saved regularly:

* Archiving audit logs on a regular basis.
* Windows Event Collector and Event Subscriptions allow you to get events from remote computers and store them in a local event log on a event collector computer.

# Securing Audit Information

Audit logs should be stored in a secure manner.

* Store backups in an offsite location.
* Store logs on another server.
* Store logs on write-once media (DVDs).
* Protect your logs via NTFS permissions and personnel policies.

# Auditing Best Practices

Critical applications, processes handling valuable or sensitive information, previously compromised or abused systems, and systems connected to third parties or the Internet all require active monitoring.

Any seriously suspicious behavior or critical events must generate an alert that is assessed and acted on.

# Encrypting a Message

# Decrypting a Message

# Symmetric (Private Key) Encryption

* Symmetric encryption uses a **single key** for **encryption** and **decryption**.
* Both the **sende**r and **receiver** have the **same key** and use it to encrypt and decrypt all messages.
* It’s also known as **secret-key encryption** or **private-key** encryption.

# Asymmetric (Public Key) Encryption

* Asymmetric encryption uses **two keys**, a **public key** and a **private key** created as a matched pair.
  + **Private Key**: Kept secret and never shared.
  + **Public Key**: Shared with others.
* Commonly referred to as:
  + Public Key Encryption
  + Public Key Infrastructure (PKI) Encryption

# Hashing

* Hashing is the process of converting an input (data) into a fixed size string of text.
* It’s a one-way function, meaning you can’t use a hash value to determine its input data.
* Hashing is used to provide data integrity because each unique input will have a unique output.
* We use hashing to verify that something has not been tampered with.
* MD5 and SHA are common hash algorithms.

# What Is a Digital Certificate?

* A **digital certificate** is an electronic document used to identify an individual, a server, an organization, or some other entity, as well as to associate that entity with a **public key**.
* Digital certificates are used in **public key infrastructure** (**PKI**) encryption.
* We can think of a digital certificate as our “online” **digital credential** that verifies our identity.

# The Role of Certificate Authorities

* Digital certificates are issued by a **Certificate Authority** (**CA**).
* **Certificate Authorities** are a trusted entity, typically an organization such as VeriSign, that verify an entity’s identity, then issues, manages, and signs that entity’s digital certificate.
* Just like we trusted the DMV to issues drivers licenses, we trust CAs to issue digital certificates.

# What's Included in a Digital Certificate?

* **Serial Number**: Used to uniquely identify the certificate.
* **Signature Algorithm**: The algorithm used to create the signature.
* **Issuer**: The entity that verified the information and issued the certificate.
* **Valid-From**: The date the certificate is first valid from.
* **Valid-To**: The expiration date.
* **Public Key**: The public key.
* Plus Additional Information…

# Windows Encrypted File System

* Windows Encrypted File System (EFS) allows us to encrypt individual files and folders.
* Uses a combination of symmetric and asymmetric encryption.

# Introduction to BitLocker

* **BitLocker** is Microsoft’s **full disk** encryption, where it encrypts the entire hard drive.
* It protects your hard drive and data from offline attacks.
* **BitLocker To Go** allows you to encrypt external drives (USB flash drives, hard drives, SD cards, etc.
* Runs on Windows 10 Professional & Enterprise, not Home Edition.

# Software-Based Encryption

* Uses software tools to encrypt your data:
  + BitLocker, Windows EFS, VeraCrypt, 7zip
* Typically as secure as the Operating System.
* A vulnerability in the Operating System can compromise the encryption software.

# Hardware-Based Encryption

* Uses hardware to perform encryption:
  + TPM (Crypto Processor)
  + Processors with x86 Instruction Set (AES Encryption)
* Many times, stand alone USB hard drives.

# Security Token Devices

* Can be hardware or software based.
* Increasingly popular in two-factor authentication for online services (banking, investing, etc.).
* Produces a temporary numeric one-time passcode (token), usually in 30-60 second intervals.
* Synced with authentication server that knows the token.

# Malware

Malicious software (malware) is a wide range of different software that has malicious intent. It includes many types of malicious software, including:

* Buffer Overflow, Viruses & Polymorphic Viruses, Worms, Trojan Horses, Logic bombs, Spyware, Ransomware, Adware, Rootkits, Backdoors, and Zero day Attacks

# Buffer Overflows

* A **buffer overflow** is a programming error that occurs when a program (or system process) attempts to write more data to a fixed length block of memory (buffer) than the buffer is allocated to store.
* The overflow is then written to adjacent memory locations, which can be exploited with malicious code with the intent to cause an application or system crash or to introduce malware to the system.

# Viruses

* A virus is a set of malicious code that infects a host.
* It’s executed when typically when an application is executed.
* **It will replicate, and when an activation trigger occurs**, it will deliver the objective, which is usually malicious.
* Email is the most popular method used to spread viruses.

# Polymorphic Viruses

* A polymorphic virus is a shape-shifting virus.
* Create modified, self-encrypting versions of itself to avoid virus definition detection.

# Worms

* Malicious software that travels throughout a network **without the assistance of a host application or user interaction**.
* One of the significant problems caused by worms is that they **consume network bandwidth**.

# Trojan Horse

* A Trojan horse is a program that **looks like something desirable**, such as a screen saver, but includes other malicious code.
* It deceives users into executing it and installing malware onto their computer:
  + Free Anti-virus software
  + Free Computer Cleanup software

# Spyware

* Spyware is malware that’s installed on a user’s system **without your awareness or consent**.
* It runs quietly in the background, collecting information or monitoring your activities, such as:
  + Keystrokes
  + Screenshots
  + Authentication Credentials
  + Personally Identifiable Information
  + Web Form Data

# Adware

* **Adware** is unwanted software that’s designed to show advertisements or collect marketing-type data about you.
* Just like spyware, you typically won’t know adware is running on your computer until you notice unusual advertising pop-ups.

# Rootkit

* Malware that is designed to gain root (administrative) access on a system by exploiting known vulnerabilities that enable privilege escalation.
* Modify core system files and be invisible to the operating system so they can persist without detection:
  + Governmental organization spying on another government
  + Corporate espionage
  + Hacker(s) stealing customer data

# Zero Day Attacks

* Zero-day attacks are cyber attacks against software flaws that are unknown and have no patch or fix.
* Occurs on the same day a weakness is discovered and it's exploited before a fix becomes available from its creator.
* A **bug bounty** programs are offered by software developers by which individuals can receive recognition and compensation for reporting **bugs**, especially those pertaining to exploits and vulnerabilities.

# Hardware Firewalls

* Firewalls are the foundation of a defense-in-depth network security strategy.
* They’re designed to protect organizations from network-based attacks.
* Firewalls do this by filtering data packets that go through them.
* They can be a standalone network device or software on a computer system, meaning **network-based** (**hardware**) or **host-based** (**software**).

# Packet Filtering Firewalls

* 1st generation and most basic type of firewall.
* They inspect all data packets that attempt to traverse it, and based on pre-defined rules, packets are either allowed or denied.
* These predefined rules are commonly called an Access Control List (ACL).
* Considered Stateless Firewalls.

# Circuit-Level Firewalls

* Considered 2nd generation firewalls.
* They operate at the Transport Layer of the OSI Model (Layer 4) and monitor TCP/IP sessions.
* Instead of analyzing each individual packet, they monitor the TCP handshake.
* Valid TCP sessions are allowed to pass, while invalid and terminated sessions are not.

# Application-Level Firewalls

Also known as **proxy servers**, these firewalls operate at the Application Layer of the OSI Model (Layer 7).

Specifically, proxy servers can provide the following services:

* **Filter**: Filters packets based on an application or service (FTP, SMTP, etc.).
* **Caching**: Provides caching services, for example:
* **Logging**: Has the ability to log user activity for auditing purposes.

# Stateful Multilayer Inspection Firewalls

* Provide the functionality of **packet filtering, circuit-level** and **application-level** firewalls combined.
* Can filter traffic at the OSI Network Layer with ACLs.
* Can filter traffic at the OSI Transport Layer by monitoring TCP sessions.
* Can also filter traffic at the OSI Application Layer based on an application or service (FTP, DNS, HTTP, etc.).
* They are also the most expensive type of network firewall.

# Stateless Firewalls

* **Packet Filtering** 1st Generation Firewalls that utilize ACLs based on IP addresses and port numbers.
* Commonly used for internal network boundaries, where to internal networks connect together.

# Stateful Firewalls

* **Circuit-Level**, **Application-Level**, and **Stateful Multilayer Inspection** firewalls.
* Firewalls that inspect the state of packets, i.e. TCP sessions, as well as deep packet protocol inspection (HTTP, DNS, etc.).
* Commonly used perimeter network protection.

# Hardware (Network-Based) Firewalls

Used to protect networks.

* **Pros**
  + Reliable and Dedicated Protection
  + Excellent Protection
* **Cons**
  + Expensive
  + Can be Complex to Configure

# Software (Host-Based) Firewalls

Used to protect individual hosts.

Windows Defender Firewall.

* **Pros**
  + Tailored to Suit Individual Hosts
  + Inexpensive
* **Cons**
  + Less Secure than Hardware Firewalls
  + Can Be Resource Intensive

# Network Isolation

* Network isolation, commonly referred to as network segmentation, is the process of breaking a large network up into separate smaller network segments.
* The goal is to be able to provide granular access control for each segment.
* We can accomplish this with:
  + Routers
  + Switch VLANs
  + Perimeter Networks
  + And Additional Measures…

# Perimeter Network: DMZ

* A small network designed to be securely separated from an organization’s intranet.
* It’s commonly called a DMZ (demilitarized zone).
* Allows untrusted users outside an organization’s LAN (intranet) to access specific services located within the DMZ.
* Also blocks such users from gaining access to the organization’s intranet.

# Virtual LANs (VLANs)

* Essential LANs within a LAN
* Break up a large “physical” LAN into several smaller “logical” LANs.
* Accomplished with managed switches.
* Assign specific switch interfaces (ports) to specific virtual LANs.

# Basic Router

* Used to Connect Different Networks Together
* Routes Traffic Between Networks using **IP Addresses**
* Uses Intelligent Decisions (Routing Protocols) to Find the Best Way to Get a Packet of Information from One Network to Another.
* OSI Layer 3 Device
  + Layer 3 = Router
  + Layer 2 = Switch
  + Layer 1 = Hub

# Honeypot

* A honeypot are decoy server(s) typically placed in a DMZ designed to entice malicious users to attack them.
* They look like live production servers and are poorly configured to make them easier to exploit.
* Provide a two-fold purpose:
  + Lure hackers away from the real network.
  + Allow IT security personnel to observe and learn how hackers are attacking their system(s).

# Network Address Translation (NAT)

* NAT translates private IP addresses to public IP addresses, allowing us to map multiple private IP addresses to a single public IP.
* NAT makes it harder for hackers to penetrate our internal private network because our private IP address stay hidden from other networks.
* The only visible IP addresses hackers see are the public NAT addresses.

# Virtual Private Network (VPN)

* A **virtual private network (VPN)** allows you to connect to a private network over a public network in a secure, encrypted manner.
* Once connected to the Internet with a public IP address, a tunneling protocol is used to create a protected tunnel through the Internet to the VPN server.
* Tunneling basically means encapsulating one protocol within another to ensure that a transmission is secure.

# Types of VPN

* **Remote Access VPNs**:
  + Allows remote users such to securely access an organization’s internal network (intranet) wherever and whenever they need to.
* **Site-to-Site VPNs (Intranet VPNs)**:
  + Allows an organization to connect its remotes sites to the corporate office securely over the Internet.

# VPN Tunneling Protocols: PPTP

* **Point-to-Point Tunneling Protocol (PPTP)**
  + PPTP has known vulnerabilities, so it is falling into disuse in favor of L2TP.
  + Was commonly used by Microsoft and encrypted via Microsoft’s Point-to-Point encryption.
  + Uses TCP port 1723.

# VPN Tunneling Protocols: L2TP

* **Layer 2 Tunneling Protocol (L2TP)**
  + The most commonly tunneling protocol today.
  + Doesn’t encrypt data itself, but relies on IPSec to encrypt data.
  + A downside to IPSec is that it cannot traverse NAT.
  + Uses UDP Port 1701.

# VPN Tunneling Protocols: SSTP

* **Secure Socket Tunneling Protocol (SSTP)**
  + Used to encrypt PPTP or L2TP traffic using SSL over port 443.
  + Was developed to overcome IPSec’s incompatibility with NAT.

# Internet Protocol Security (IPSec)

* IPSec is a protocol that authenticates and encrypts packets sent over an IP network.
* Two Primary Components:
  + **Authentication Header (AH)** 
    - Provides a mechanism for authentication-only; not encryption.
  + **Encapsulating Security Payload (ESP)**
    - Provides a mechanism for both authentication and encryption.

# IPSec Tunnel Mode

* **Tunnel Mode**
  + The entire IP packet is encapsulated and encrypted by IPSec. This protects the internal routing information by encrypting the IP header of the original packet.
  + Commonly used for site-to-site VPNs.
  + NAT is supported with the tunnel mode.

# IPSec Transport Mode

* **Transport Mode**
  + Only encrypts the payload (data) and ESP trailer. The IP header of the original packet is NOT encrypted.
  + Commonly used for client-to-site VPN connections.
  + NAT is NOT supported in Transport Mode.

# Protocol Spoofing

* Protocol spoofing is the misuse of a network protocol to initiate an attack on a host or network device.
* There are three common types of protocol spoofing:
  + ARP Spoofing (ARP Poisoning)
  + DNS Spoofing
  + IP Address Spoofing

# ARP Spoofing (ARP Poisoning)

* Address resolution protocol maps IP addresses to MAC addresses.
* ARP poisoning modifies the network’s ARP cache to take over a victim’s IP address.
* This allows attacker to receive any data intended for the victim.

# DNS Spoofing

* Domain name service (DNS) translates domain names into IP addresses.
* DNS spoofing is when an attacker alters the DNS records to redirect traffic to a fraudulent website, where further attacks can occur.

# IP Address Spoofing

* IP address spoofing is an attack where a malicious user forges a packet’s source IP address.
* By doing so, the malicious user can impersonating the sending computer.

# DoS and DDoS Attacks

**Denial of Service (DoS) Attack**

* A DoS attack is when a malicious user attempts to make a server or other network device unavailable by flooding it with requests.
* This overwhelms the server’s resources so that it can’t respond to service requests.

**Distributed Denial of Service (DDoS) Attack**

* A DDoS attack is a DoS attack that is launched from a large number of malicious machines.

# Back Door Attacks

When someone creates an alternative way into a system that bypasses its security controls.

# Replay Attacks

* Similar to a man in the middle attack, but with a replay attack, the attacker will capture a message sent from a network device to the server.
* Later, the attack will send the original, unmodified message to the server, hoping the server responds thinking the attacker is a valid device.
* If it does, the attacker has successful created a “trusted” relationship with the server.

# Weak Encryption Key & Software Vulnerability Attacks

**Weak Encryption Key**

* Occurs when enough network traffic is captured to allow the key to be broken. An example is WEP encryption.

**Software Vulnerability Attack**

* The exploitation of known software/application vulnerabilities for malicious purposes.

# Remote Code Execution Attack

* Commonly used against web applications.
* When web applications are improperly coded, attackers can run system-level code for malicious purposes.

# SQL Injection Attack

* Occurs when a malicious user manipulates web-based input forms to pass unauthorized SQL to the SQL server database.
* This can allow the attacker to retrieve information, delete information, and even drop tables from the database.

# Cross-Site Scripting Attack (XSS Attack)

* Occurs when a malicious user embed malicious client-side HTML or JavaScript code into a web site’s code, where the code then executes when a user visits the site.
* The attacker can then obtain sensitive page content, session cookies, and other info.

# DNS Security Extensions (DNSsec)

* DNS traffic is not encrypted, so it can potentially be modified if you’re not using IPSec or a VPN.
* DNSsec secures DNS by adding cryptographic digital signatures to existing DNS records.
* By checking a DNS record’s digital signature, you can verify that a requested DNS record came from its authoritative name server.
* DNS records are also hashed, allow a requestor to verify it hasn’t been modified.

# Windows User Account Control (UAC)

* User Account Control (UAC) is a security feature of Windows which helps prevent unauthorized changes to the operating system.
* It helps prevent malware from damaging a PC by always running applications and tasks in a non-administrator account unless an administrator authorizes administrator-level access via UAC.

# How Does UAC Work?

* In Windows, applications run by default without administrator-level privileges.
  + They can’t make changes to the operating system, its system files or registry settings.
* When an application wants to make a system change, the UAC prompt is shown to the user, asking for permission.
* An user with administrative-level access must approve of the UAC to allow the application to make the changes.

# What Can Trigger UAC?

* Below is a sample of items that can trigger UAC:
  + Changes to system-wide settings or files in the Windows or Program Files folders
  + Installing and uninstalling drivers & applications
  + Viewing or changing another user's folders and files
  + Adding or removing user accounts
  + Configuring Windows Update
  + Changing settings to the Windows Firewall
  + Changing UAC settings

# Windows Update Overview

* Windows Update is the means in which we can update our Windows Operating System and associated Microsoft software with fixes, security patches, and services packs.
* Can be manage on individual PCs or at the Active Directory Level with **Windows Server Update Service (WSUS)** or **System Center Configuration Manager (SSCM).**
* WSUS and SSCM allow admins to test, schedule and prioritize updates to large numbers of systems.

# Windows Update Classifications

**Important Updates:** Offer significant benefits, such as improved security, privacy, and reliability. They should be installed as they become available.

**Recommended Updates:** Address non-critical problems or help enhance your computing experience.

**Optional Updates:** Can include updates, drivers, or new software from Microsoft to enhance your computing experience. You can only install these manually.

# Windows Update Categories

**Security Updates:** Updates that address security-related issues in an operating system.

**Critical Updates:** A worldwide release update for any specific issue that is not related to the security that the operating system offers; such updates are released to address a critical but non-security issues.

**Service Packs:** An cumulative set of all hotfixes, security updates, critical updates, fixes, and updates.

# Spam Email

* **Spam email** is unsolicited emails, commonly advertising emails, but sometimes phishing and scamming attempts.
* Such email can clutter our inbox, getting in the way of emails that matter, as well as potentially carry malware.

# Spoofed Emails

* **Email spoofing** is the forgery of an **email header** so that the email seems to have originated from someone or somewhere other than the actual source.
* It’s used in **phishing, pharming** and **spam campaigns** because people are more likely to open an **email** when they think it has been sent by a legitimate source.

# Email Phishing

* **Phishing** is the practice of sending unwanted email to users with the purpose of tricking them into revealing personal information (such as bank account information) or clicking on a link.
* It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email.
* Their goal is to get you to share valuable personal information – such as account numbers, Social Security numbers, or your login IDs and passwords.

# Email Pharming

* **Pharming attacks** redirect users from legitimate websites to fraudulent fake websites.
* With **email pharming**, a user will open up an email with malware, which then installs malicious code on the user’s PC.
* In one form of pharming attack, code sent in an e-mail modifies local hosts file on a personal computer.
* This code then redirects URL clicks to a fraudulent website without your knowledge or consent.

# Spam Filters

* A spam filter is typically a dedicated server or network appliance that filters out spam emails.
* You have your DNS mail exchanger (MX) record point to your spam filter.
* This way your spam filter will filter emails before they are sent to your internal email servers.
* Spam filters can utilize multiple criteria for filter email:
  + Email Addresses, IP Address Ranges, and Keywords
* This information is placed in a Blacklist is blocked.

# Spam Filter Real-Time Blackhole Lists

* Spam filters can also use real-time Blackhole Lists (RBL) and DNS-based blackhole lists (DNSBL).
* These lists are managed by a third party and are continually updated with known spammers.

# PTR Records & Filtering Spam

* **Pointer (PTR) records** are used for Reverse DNS lookups:
  + Allows someone to determine your domain name based on your IP address.
* PTR records play an important role in spam filtering.
* Spam filters and incoming mail servers can be configured to reject emails that do not have a valid PTR record.
* Why? Domain names without a PTR record are often associated with spammers because spammers are more likely to use fake domain names.

# Sender Policy Framework (SPF)

* **Sender Policy Framework (SPF)** is an email authentication protocol that allows the owner of a domain to specify which mail servers they use to send mail from that domain.
* Admins specify **SPF records in DNS**. These records list which IP addresses are authorized to send email on behalf of the domain.
* When receiving an email, the email server with verify the sending email server is listed in the SPF records. If it’s not, it’s considered spam and blocked.

# Anti-Virus

When a malicious email gets past our spam filter(s), blackhole lists, and a sender policy framework, anti-virus provides protection against malware.

# Email Client & Server Protection

**Client:**

* Anti-Virus Software
* Using Encryption and Digital Signatures
* User Education & Awareness

**Server**:

* Spam Filtering
* Blacklisting & Real-Time Blackhole Lists
* Sender Policy Framework (SPF)
* Utilizing PTR Records

# Server Hardening

* Server hardening is the process of reducing the attack surface of server.
* The smaller the attack surface, the less vulnerable the server is to potentially attacks.

# Separation of Services

* Separation of Services is the strategy of placing critical services (Windows Server Roles and Features) on separate physical servers to mitigate the effect of server failures:
  + Hardware Failure
  + Software Failure
  + Exploited / Hacked

# Keeping Servers Updated

* Just like client PCs, Windows Servers should also be kept up-to-date with Windows Updates.
* Ideally should be managed with **Windows Server Update Service (WSUS)** or **System Center Configuration Manager (SSCM).**
* Prior to updating production servers, it’s good practice to test updates, patches and hot fixes on test servers in non-production environments.

# Secure Dynamic DNS

* Windows Server supports **Dynamic DNS updates**, which is where dynamic DNS records are created by computers, rather than manually by an administrator.
* This cuts down the administrative load because admins no longer have to manually manage DNS records.
* If Dynamic DNS updates are enabled, they should be in “**Secure only**” mode. This ensures that only computers that are a member of an Active Directory Domain can create DNS records on the DNS server.

# Disabling Unsecure Authentication Protocols

As part of the server hardening process, unsecure authentication protocols should be disabled. Only secure authentication protocols should be used;

* Use Secure Shell (SSH) instead of Telnet
* Use Secure File Transfer Protocol (SFTP) instead of FTP
* Use Hypertext Transfer Protocol Secure (HTTPS) instead of HTTP

# Read-Only Domain Controllers

**Read-Only Domain Controllers (RODC)** hold a read-only, non-writable copy of the Active Directory Domain Services (AD DS) database. RODCs designed to be utilized in branch offices the following scenarios:

* Physical security isn’t guaranteed. A lack of well-trained IT staff in branch offices. Branch offices have poor network connectivity with the HQ office.

RODCs support unidirectional replication, meaning any erroneous or malicious changes made to the RODC aren’t replicated to the rest of the domain.