Security+ Acronym + Ports Study Guide

Written By: Raza Tahir

This document provides definitions and explanations of acronyms and essential network ports relevant to the CompTIA Security+ SY0-701 exam as shown on the official guide. It is intended to support exam preparation by helping candidates understand and review key terminology.

If you'd like to test your knowledge on acronyms, use this short guide for active recall practice.

Near the end of this section includes a brief overview of Incident Response.

Additionally, the final sections of this document covers critical network ports, including mnemonics to help you remember protocol numbers and services. Once reviewed, use this section as a quick self-test to check your knowledge.

A

AAA (Authentication, Authorization, and Accounting): A security framework for verifying identities, granting permissions, and recording resource usage. Further breakdown:

- Authentication: Verifies the identity of users through passwords, biometrics, or tokens, and verifies systems using digital certificates or keys.
- Authorization: Defines permissions with authorization models e.g. RBAC & MAC.
- Accounting: Tracks user actions, logs their activities, and generates reports.

ACL (Access Control List): A table that specifies which users or groups can access a resource (e.g., a file) and their permitted actions.

[Link](https://firewalltimes.com/access-control-list/)

[Link](https://learn.microsoft.com/en-us/windows/win32/secauthz/access-control-lists)

AES (Advanced Encryption Standard): A widely adopted symmetric encryption algorithm that protects data with a single key used for both encryption and decryption.

Helpful Video: https://www.youtube.com/watch?v=C4ATDMIz5wc

AES-256: A type of AES encryption using a 256-bit key for strong protection against brute-force attacks. AES-256 is the industry gold standard and best algorithm for protecting data at rest.

https://www.splunk.com/en_us/blog/learn/data-encryption-methods-types.html

AH (Authentication Header): A component of the IPsec protocol that authenticates packet origins and integrity without encrypting payloads.

AI (Artificial Intelligence): The technology that enables machines to perform tasks with humanlike intelligence, reasoning and learning.

AIS (Automated Indicator Sharing): A system for sharing cyber threat indicators between public and private sectors, and acts like a neighborhood watch for computers by enabling rapid response. In maritime operations, if a ship's transponder fails, its last known location freezes or disappears from other vessels' electronic charts.

ALE (Annualized Loss Expectancy): expected financial loss from a specific risk in one year.

Formula:

ALE = Cost per incident (SLE, Single Loss Expectancy) × Expected number of incidents per year (ARO, Annualized Rate of Occurrence)

AP ([Wireless] Access Point): A hardware device that provides wireless connectivity to clients.

Example: When my phone provides a hotspot for my laptop, it acts as a **Wireless Access Point (AP)** that allows my laptop to connect to the internet through the phone.

API (Application Programming Interface): A set of functions and rules that allow two software applications to communicate with each other.

APT (Advanced Persistent Threat): A long-term, targeted cyberattack designed to infiltrate an organization's network and remain undetected for as long as possible.

Example:

Nation-State-sponsored cyber threat actors often use Advanced Persistent Threat (APT) methodology to conduct well-funded, long-term, and covert operations for geopolitical, military, or economic objectives

[Link] (https://www.microsoft.com/en-us/security/business/security-101/what-is-advanced-persistent-threat-apt)

[Link](https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors)

ARO (Annualized Rate of Occurrence): The estimated number of times a risk is expected to happen in one year.

ARP (Address Resolution Protocol): A communication network protocol that maps IPv4 addresses to a MAC address on a local network.

ASLR (Address Space Layout Randomization): A computer security technique that randomizes memory locations every time it runs so that hackers can't exploit memory vulnerabilities.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge): A knowledge base maintained by the non-profit MITRE for listing and explaining adversary tactics and techniques from observed cyberattacks.

AUP (Acceptable Use Policy): A document that explains the rules and permissions people must follow when using an organization's technology and information systems.

Example: https://workspace.google.com/terms/use_policy/

AV (Antivirus): Software that identifies, blocks, and removes malicious programs.

B

BASH (Bourne Again Shell): A free, open-source Unix shell and command-language interpreter for interactive use and scripting. Bash lets users type commands to control their computer and write scripts to automate tasks. Bash is commonly used on Linux and macOS, and it is also available on Windows through tools such as Git Bash!

BCP (Business Continuity Planning): A broad, organization-wide strategy that provides teams with an action plan to maintain essential operations, recover from disruptions, and minimize the impact of unexpected incidents. Unlike a Disaster Recovery Plan (DRP), which focuses primarily on restoring IT systems, infrastructure, and data, a BCP addresses how to keep the entire business operating during a crisis, including staffing, physical facilities, communications, vendors, and customer service.

[Link](https://www.datto.com/blog/what-is-a-business-continuity-plan/)

BGP (Border Gateway Protocol): The protocol used to exchange routing information between autonomous systems across the internet.

BIA (Business Impact Analysis): A proactive assessment that evaluates how disruptions/crises can impact on critical business functions and establishes recovery priorities that helps the business decide what to recover first and what resources are needed.

> BIA also can set time limits, such as how quickly systems must be restored (RTO), how much data loss can be tolerated (RPO), and the maximum downtime the business can tolerate (MTD), helping it determine what to fix first during a crisis.

BIOS (Basic Input/Output System): Firmware used to initialize hardware and start the operating system during boot. It checks hardware components (CPU, RAM, storage, keyboard) for errors.

BPA (Business Partners Agreement): Think: Big Picture Partnership**.**

A foundational contract that establishes the formal terms of a business collaboration, defining governance, rights, obligations, and the allocation of resources and risk. By comparison, while a Memorandum of Understanding (MOU) typically signals a mutual intent to cooperate, and a Memorandum of Agreement (MOA) often outlines specific operational commitments, the legal binding power of any such document ultimately depends on its specific language, the applicable law and mutual intent rather than its title alone.

For example:

- **BPA:** They agree on how to share profits, expenses, and business risks.
- **MOA:** They agree that Company A develops the software by June, while Company B tests it by July.

[Read More](https://www.adobe.com/acrobat/business/resources/business-partnership-agreement.html)

BPDU (Bridge Protocol Data Unit): A type of switch message that is transmitted by a local area network (LAN) bridge.

BYOD (Bring Your Own Device): A policy model that allows employees to use their personal devices for work, allowing access to company systems under established security rules.

- **BYOD** (Bring Your Own Device) is a separate mobile device management (MDM) approach from **CYOD** (Choose Your Own Device) and **COPE** (Corporate-Owned, Personally Enabled).

Link: https://www.comptia.org/en-us/blog/corporate-acceptable-use-policy-a-key-part-of-security-awareness-training/

C

CA (Certificate Authority): A trusted entity that issues and validates digital certificates.

CAPTCHA: A type of challenge designed to distinguish human users from automated programs.

CAR (Corrective Action Report): A Quality Management report that documents the problem, its root cause, the corrective actions required to resolve it, and the completion status.

CASB (Cloud Access Security Broker): A software that enforces security policies and protects data between users and CSP. CASB was originally designed to handle "Shadow IT".

Link: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cloud-access-security-broker-casb

CBC (Cipher Block Chaining): A mode of operation for a block cipher; it provides a method of encrypting data (whether read from a database or captured from a network) by dividing data into fixed-size blocks in memory. It then applies a mixing process: the first block is combined with an initialization vector (IV), and each subsequent block is mixed with the previous ciphertext block before encryption. This hides underlying patterns, and the final encrypted result is either saved to disk or sent across the network. This method provides confidentiality but not message integrity.

CCMP (Counter Mode/CBC-MAC Protocol): A Wi-Fi security protocol combining AES counter-mode encryption with integrity protection.

CCTV (Closed-Circuit Television): A private video surveillance system used for monitoring and surveillance.

CERT (Computer Emergency Response/Readiness Team): A broad cybersecurity response and coordination team.

CFB (Cipher Feedback): A mode of operation for a block cipher; this produces stream-like encryption through feedback from prior ciphertext.

CHAP (Challenge Handshake Authentication Protocol): A type of security authentication protocol that authenticates clients (verifies their identity) through challenge-response exchanges without transmitting their actual passwords over the network.

CIA Triad: A security model prioritizing confidentiality, integrity, and availability.

CIO (Chief Information Officer): An executive overseeing information technology strategy and alignment with organizational goals.

CIRT (Computer Incident Response Team): An internal response team that investigates, contains, and recovers from computer security incidents.

[Link](https://www.microsoft.com/en-us/security/business/security-101/what-is-incident-response)

CMS (Content Management System): Software that simplifies website content creation, organization, and publishing. E.g. WordPress, Squarespace.

COOP (Continuity of Operations Planning): A process by government agencies to ensure essential government functions continue throughout emergencies.

COPE (Corporate Owned, Personally Enabled): A policy model in which an organization provides an employee with a company-owned device for work and limited personal use.

CP (Contingency Planning): A plan that defines responses for significant events that could disrupt operations. Think: Batman.

CRC (Cyclic Redundancy Check): Code that detects accidental data corruption during storage or transmission.

CRL (Certificate Revocation List): A digitally signed file published by a Certificate Authority (CA) that lists the serial numbers of digital certificates revoked before their scheduled expiration dates.

Link: https://securew2.com/blog/certificate-revocation-crl-explained

CSO (Chief Security Officer): An executive responsible for protecting organizational people, information, and physical assets.

CSP (Cloud Service Provider): Vendor delivering cloud-based infrastructure, platforms, or software services. The big 3 are AWS, Azure & Google Cloud Platform (GCP).

CSR (Certificate Signing Request): An encoded message request (sent from an applicant) that contains information needed by a CA to issue a certificate.

CSRF (Cross-Site Request Forgery): A type of malicious exploit in which a website tricks authenticated browsers into submitting unauthorized requests to trusted applications

Example:

1. Alice logs into her bank. The bank stores an authentication cookie in her browser.
2. On the same window, Alice opens a new tab and visits a malicious website.
3. The malicious website tricks her browser into sending a request to her bank and may automatically attach the bank's authentication cookie to that request.
4. If the bank lacks proper CSRF protection, it might accept the unauthorized request.

CSU (Channel Service Unit): A device that connects digital terminal equipment to a telecommunications circuit.

CTM (Counter Mode): A mode of operation that encrypts data using a block cipher, but it works like a stream cipher.

CTO (Chief Technology Officer): An executive directing technological strategy, development, and innovation.

CVE (Common Vulnerability Enumeration a.k.a. Common Vulnerabilities and Exposures): A serial number that names and identifies a specific security flaw/weakness.

Example:

CVE-2017-5638 identifies a critical vulnerability in the Apache Struts 2 web application framework that was exploited in the 2017 Equifax data breach.

CVSS (Common Vulnerability Scoring System): A framework for rating the severity of software vulnerabilities [Link](https://www.first.org/cvss/)

CYOD (Choose Your Own Device): A policy model that lets employees select work devices from a pre-approved list.

D

DAC (Discretionary Access Control): An access control model in which a resource owner, subject to the system's security policies, has the authority to grant, modify, or revoke other users' access permissions to that

resource. These permissions can be implemented using Access Control Lists (ACLs). It is widely recognized as one of the core access control models (alongside MAC and RBAC).

Example:

On a Windows computer, right-click a file, selecting Properties → Security, and changing its access permissions is an example of Discretionary Access Control (DAC).

DBA (Database Administrator): A specialist maintaining database availability, security, performance, and integrity.

DDoS (Distributed Denial-of-Service): A type of cyberattack in which many compromised systems overwhelm a targets server and cause a denial of service that prevents legitimate users from accessing the targeted resource, often resulting in unresponsive services or slow response times.

TL;DR: This attack floods a server with bot traffic to disrupt availability.

[Link: https://www.splunk.com/en_us/blog/learn/ddos-attacks.html]

DEP (Data Execution Prevention): A security feature in an OS that blocks code execution in protected memory regions to reduce exploitation.

[Link](https://learn.microsoft.com/en-us/windows/win32/memory/data-execution-prevention)

DES (Data Encryption Standard): An old & obsolete symmetric block cipher that encrypts data in 64-bit blocks using a 56-bit secret key. It is considered insecure because its short key length makes it vulnerable to brute-force attacks that use modern computing power. AES is more widely used today.

[Link](https://www.nist.gov/blogs/cybersecurity-insights/cornerstone-cybersecurity-cryptographic-standards-and-50-year-evolution)

DHCP (Dynamic Host Configuration Protocol): A network protocol that automatically assigns IP addresses and network configuration settings (e.g. subnet masks) to devices on a network.

Run **ipconfig /all** on Windows to view your server.

DHE (Diffie-Hellman Ephemeral): A key-agreement method that allows two parties to establish a shared secret over an insecure channel using temporary key pairs. Each party exchanges a public key share and independently computes the same shared secret, which can be used to derive session keys.

https://www.youtube.com/watch?v=85oMrKd8afY

DKIM (DomainKeys Identified Mail): An invisible cryptographic signature on an email that verifies the email was signed by the domain and left unaltered. Contrast this with SPF that checks the sending server's authorization (Is this computer/server allowed to send mail for this domain?) versus DMARC that helps verify that authentication matches the domain the sender claims to represent.

DLL (Dynamic Link Library): A library file stored on a computer that provides reusable code and functions to multiple software programs. Windows OS primarily uses the '.dll' extension for DLL files, alongside related extensions like .ocx, .drv, and .sys.

Example:

Windows Media Player is the default application on a Windows computer that uses **winmm.dll**. This shared Windows library can be used by multiple programs (e.g. music or game software) to access multimedia functionality.

[Link](https://learn.microsoft.com/en-us/troubleshoot/windows-client/setup-upgrade-and-drivers/dynamic-link-library)

[Link](https://www.lenovo.com/us/en/glossary/dynamic-link-library/)

DLP (Data Loss Prevention): A system (i.e. a set of technologies and processes) that focuses on (and if needed blocks) how sensitive data is shared, copied, downloaded, accessed without authorization or transferred improperly. DLP protects against both accidental errors (e.g. sending a file to the wrong person) and intentional insider threats (like malicious data exfiltration).

DLP can work with CASB, IAMs, EDRs and IDS.

[Link](https://www.microsoft.com/en-us/security/business/security-101/what-is-data-loss-prevention-dlp)

DMARC (Domain Message Authentication Reporting and Conformance): An email authentication protocol to protect email domains from email domain spoofing by checking SPF and DKIM results.

DNAT (Destination Network Address Translation): A technique that changes packet destination addresses, commonly forwarding traffic to internal hosts.

DNS (Domain Name System): A naming system that translates domain names into IP addresses and other resource records. By default, Port 53 is the default port for DNS.

DoS (Denial-of-Service): A type of cyberattack that disrupts a system or service for legitimate users by flooding or overwhelming a host connected to the internet from a single source or device.

DPO (Data Protection Officer): An executive that oversees privacy compliance, regulations such as GDPR, and organizational protection of personal data.

DRP (Disaster Recovery Plan): A plan that offers procedures for recovering vital systems and data following disruption.

DSA (Digital Signature Algorithm): An asymmetric cryptographic algorithm that is standard for creating and verifying digital signatures. It uses a private key to sign, and a public key to verify. Examples can include RSA and ECDSA.

DSL (Digital Subscriber Line): A broadband internet technology that provides internet through existing telephone wiring. Talking on a landline phone can affect a DSL internet connection.

E

EAP (Extensible Authentication Protocol): An authentication framework that supports multiple methods for network access e.g. wireless networks and Point-to-Point connections.

[Link](https://learn.microsoft.com/en-us/windows-server/networking/technologies/extensible-authentication-protocol/network-access?tabs=eap-tls%2Cserveruserprompt-eap-tls%2Ceap-sim)

ECB (Electronic Codebook): A mode of operation for a block cipher that encrypts plaintext blocks into corresponding ciphertext blocks.

ECC (Elliptic Curve Cryptography): An approach to the asymmetric public-key cryptography system that is based on the algebraic structure of elliptic curves over finite fields. It offers strong security with comparatively small keys and can be used for encryption, key exchanges (e.g. ECDH), and digital signatures (e.g. ECDSA or EdDSA).

ECDHE (Elliptic Curve Diffie-Hellman Ephemeral): A variant of the Diffie-Hellman algorithm that uses elliptic-curve key exchange using temporary keys to provide forward secrecy.

ECDSA (Elliptic Curve Digital Signature Algorithm): A cryptographic public-key algorithm that is used for generating and verifying digital signatures.

> Example:
>
> Bitcoin relies on the ECDSA as its foundational cryptographic system to prove ownership and authorize transactions

EDR (Endpoint Detection and Response): A cybersecurity technology that continuously monitors endpoints to detect, investigate, and respond to threats. EDR can work with SIEM to centralize threat log data, SOAR to automate response actions, and IAM to connect endpoint activity with user identities and access permissions.

[Link](https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response)

EFS (Encrypting File System): A built-in Windows feature that encrypts files and folders on NTFS volumes.

ERP (Enterprise Resource Planning): "A software system that helps organizations streamline their core business processes—including finance, HR, manufacturing, supply chain, sales, and procurement—with a unified view of activity and provides a single source of truth."
(SAP, 2026, [Link](https://www.sap.com/resources/what-is-erp))

ESN (Electronic Serial Number): A unique identification number that's assigned by manufacturers to certain cellular devices.

ESP (Encapsulating Security Payload): A component of IPsec protocol that provides confidentiality, along with some authentication and integrity to data.

F

FACL (File System Access Control List): A type of ACL (Access Control List) that defines user and group permissions for files and directories.

FDE (Full-Disk Encryption): A method of encryption that converts entire storage drives data into unreadable ciphertext. The data remains locked and scrambled even when powered off.

> EX: BitLocker is useful for encrypting the laptop.

FIM (File Integrity Monitoring/Management): A technology that detects and reports unauthorized or unexpected file changes.

> Example:
>
> https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-overview

FPGA (Field-Programmable Gate Array): A chip that contains configurable digital circuits that are configurable after manufacturing for specialized processing tasks by a customer.

> Example:
>
> Emulation developers can program an FPGA chip to replicate the hardware of different gaming consoles, such as Sega systems and the Nintendo 64. The FPGA can then be integrated into a physical FPGA-based gaming system, with a compatible board providing the supporting components and interfaces (e.g. sound, memory, controller, graphics, etc.) needed to run the implementations.
>
> Common Example: https://retrorgb.com/mister.html

FRR (False Rejection Rate): Percentage of a biometric or authentication system incorrectly denies access to a legitimate, authorized user

FTP (File Transfer Protocol): A network protocol that transfers files between networked clients and servers without native encryption. By default, Port 21 is the default port for FTP.

FTPS (FTP Secure): An extension of FTP that secures FTP connections using TLS encryption. By default, implicit FTPS commonly uses port 990, while explicit FTPS by default commonly uses port 21.

G

GCM (Galois/Counter Mode): An efficient mode for operation for symmetric key cryptographic encryption that provides confidentiality and integrity and commonly used with AES.

GDPR (General Data Protection Regulation): A regulation within the European Union that governs personal-data privacy, processing, and protection.

[Link](https://gdpr.eu/what-is-gdpr/)

GPG (GNU Privacy Guard): A free software implementation of OpenPGP used to encrypt, decrypt, and digitally sign information.

[Link](https://www.gnupg.org/)

GPO (Group Policy Object): A feature that centrally configures Windows users, applications and computers within Active Directory.

[Link](https://www.lenovo.com/us/en/glossary/what-is-gpo/?orgRef=https%253A%252F%252Fwww.google.com%252F&srsltid=AU7gw4Vp-hM7eGuX4GGk0Qg3apxUqUXeANT5dsJq1mKX7xUTEySDC7_a)

GPS (Global Positioning System): A free service that utilizes a satellite-based system to provide location, navigation, and precise timing. Owned by the United States government, the GPS was originally developed for military navigation and operations. However, after a Korean passenger plane was accidentally shot down after straying into restricted Soviet airspace, U.S. President Reagan announced that GPS would be made available for civilian use.

[Link](https://www.gps.gov/)

GPU (Graphics Processing Unit): A processor optimized for parallel calculations, graphics rendering, and accelerated computing.

GRE (Generic Routing Encapsulation): A tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network-layer protocols without providing encryption.

H

HA (High Availability): A design approach that keeps a system running despite failures by minimizing downtime through redundancy and fault tolerance.

HDD (Hard Disk Drive): A magnetic data storage device that uses spinning platters coated with magnetic material to store digital data. The data is retained in a non-volatile manner (meaning it stays saved even when the computer is turned off).

HIDS (Host-Based Intrusion Detection System): A system that monitors an OS host for suspicious activity and unauthorized changes. HIDS is installed on individual devices connected to the internet or an organization's internal network and detects malicious activity e.g. threats coming from inside the organization. It can also identify infected devices that may spread malware to other systems.

Example:

https://www.ossec.net/ossec-development-timeline/

HIPS (Host-Based Intrusion Prevention System): A software package that detects and blocks suspicious activity occurring on an individual endpoint.

HMAC (Hashed Message Authentication Code): A type of message authentication code that verifies message integrity for blocks that were sent and authenticity using a secret key and hash function (such as SHA-256 or MD5).

Example: Both SSH and IPsec can use HMAC

HOTP (HMAC-based One-Time Password): A password algorithm that generates one-time passwords using HMAC and an incrementing counter.

HSM (Hardware Security Module): A physical tamper-resistant device that generates, protects, and uses cryptographic keys.

HTML: The standard markup language that structures content displayed by web browsers.

HTTP: An application protocol that transfers web resources between clients and servers. By default, Port 80 is for HTTP; Pneumonic: Around the World in 80 Days

HTTPS: An extension of HTTP that's protected by TLS for encrypted, authenticated web communication. By default, Port 443 is for HTTPS.

HVAC: Technology systems that control indoor heating, cooling, ventilation, and air quality.

I

IaaS (Infrastructure as a Service): A cloud model that provides virtualized computing, storage, and networking resources.

IaC (Infrastructure as Code): The process of provisioning and managing infrastructure through version-controlled configuration files rather than manual processes or interactive interfaces.

[Link](https://www.microsoft.com/en-us/security/business/security-101/what-is-infrastructure-as-code-iac-security)

IAM (Identity and Access Management): A framework for verifying users by managing digital identities, authentication e.g. MFA, authorization, policies and access lifecycles.

Note that IAM helps prevent unauthorized access and DLP helps prevent unauthorized data sharing/loss.

> **Example:**
>
> An employee has permission to access customer records through IAM.
> If they try to email those records to a personal email address, DLP can detect and block the transfer.

[Link](https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam)

ICMP (Internet Control Message Protocol): A network protocol that reports network errors (e.g. Destination Unreachable or Time Exceeded Pings) and operational status between IP devices. It works along IP to help devices and network equipment identify problems with data delivery. A ping command uses ICMP.

ICS (Industrial Control Systems): A broad umbrella term for computer systems that control, monitor and automate the hard and software of industrial equipment, such as factory machinery and power plants. ICS is the general category that includes SCADA, controllers, sensors, communication networks, and industrial equipment. They are prime targets for nation-state adversaries.

> Example:
>
> A water tank has a sensor that measures the water level. The ICS monitors and controls the pump, while the ICS uses SCADA to display the water level and pump status on the operator's screen. If configured and permitted, the operator can use SCADA to start or stop the pump remotely.

[Link](https://www.cisa.gov/topics/industrial-control-systems)

IDEA (International Data Encryption Algorithm): A symmetric key block cipher using a 128-bit key.

IDF (Intermediate Distribution Frame): A cable rack/telecommunications room that connects horizontal cabling from end-user devices to the MDF (main distribution frame).

IdP (Identity Provider): A service that authenticates users and confirms it to other services.

IDS (Intrusion Detection System): A device or software that monitors systems or network traffic to alert suspicious activity or possible intrusions. Common types of IDS are: HIDS, NIDS, and WIDS.

IEEE (Institute of Electrical and Electronics Engineers): A professional organization that develops widely adopted technical standards.

- For example, IEEE 802.1X enforces robust authentication for devices attempting to connect to a network and utilizes central authentication servers (like RADIUS) to authenticate users and devices, validate credentials, and enforce centralized access control before granting network access.

[Link](https://www.ieee.org/)

IKE (Internet Key Exchange): A protocol that negotiates IPsec security associations and cryptographic keys.

IM (Instant Messaging): A type of online chat that enables real-time text communication between users over networks. E.G. AOL Instant Messenger

IMAP (Internet Message Access Protocol): A common Internet protocol that stores emails on a remote server without downloading them to a client, which allows users to access the same messages across multiple devices. Emails remain on the server until deleted by the user.

> Example:
>
> An employee checks their email on their phone, then opens the same inbox on their computer. IMAP keeps the emails synchronized across both devices.

By default, IMAP uses Port 143 for unencrypted (plaintext) connections (can be upgraded to a secure session using the STARTTLS command) and Port 993 for encrypted connections over SSL/TLS.

IoC (Indicator of Compromise): Actual evidence suggesting that a system or network may have been breached, such as a malicious IP address, or unusual activity (e.g. an unauthorized login attempt).

> Example:
>
> If an attacker uses a stolen password to access an email account without permission, the security team can confirm the unauthorized login through logs showing the attacker's IP address and login activity. These logs provide evidence of the compromise, while specific details, such as a malicious IP address, can serve as IoCs.

[Link](https://www.microsoft.com/en-us/security/business/security-101/what-are-indicators-of-compromise-ioc)

IoT (Internet of Things): A physical device (e.g., an appliance) embedded with software, electronics, and network connectivity to collect, exchange, or act upon data.

IP (Internet Protocol): Addresses and routes packets across interconnected networks.

Run the command 'ipconfig' on Windows PowerShell to find your local (private) IP address.

> IPv6 is newer, has tons of address space & doesn't use NAT. This matters because far more devices connect to the internet today than when it first began.

[Link](https://www.geeksforgeeks.org/computer-networks/what-is-internet-protocol-ip/)

IPS (Intrusion Prevention System): A technology that detects and automatically blocks malicious network or system activity. Example: HIPS, NIPS.

IPsec (Internet Protocol Security): A secure network protocol suite that authenticates and encrypts IP network traffic e.g. VPN.

IR (Incident Response): An **overall** approach that defines roles and responsibilities and includes the steps needed to properly resolve, document, and communicate about an incident during/after it has occurred.

The general steps for incident response are:

1. Preparation
2. Detection | Identification
3. Analysis | "Is it a real threat?"

4. Containment | Isolation

5. Eradication

6. Recovery

7. Lessons learned | Report

[Link](https://www.microsoft.com/en-us/security/business/security-101/what-is-incident-response)

[Link](https://www.comptia.org/en/blog/what-is-an-incident-response-plan-and-how-to-create-one/)

IRC (Internet Relay Chat): An application layer protocol that supports real-time text conversations through channels or direct messages.

IRP (Incident Response Plan): A formal document that describes instructions for preparing, detecting, responding to, and recovering from incidents.

ISO: An international organization creating voluntary standards across industries and technologies. For example, ISO/IEC 27001 is an international standard for managing information risk and security.

ISP (Internet Service Provider): A company that provides customers with internet connectivity and related services.

ISSO: An individual maintaining an information system's operational security posture and compliance.

IV (Initialization Vector): A fixed, non-secret value used in encryption to ensure that the same data produces different encrypted results each time.

J

No J terms were included in the supplied material.

K

KDC (Key Distribution Center): A trusted server that issues session keys for secure communications.

KEK (Key Encryption Key): A cryptographic key used to encrypt and protect other keys.

L

L2TP (Layer 2 Tunneling Protocol): A tunneling protocol used to create secure VPN connections, but it requires pairing with another protocol for encryption (e.g. IPsec).

LAN (Local Area Network): A network that connects devices across a limited geographic area. E.G. LAN Party

LDAP (Lightweight Directory Access Protocol): A protocol for accessing, querying and managing distributed directory information over an IP network. By default, Port 389 is the default port for LDAP to use for directory services, like user authentication.

Example:

Stanford University uses OpenLDAP software running on Debian Linux servers to power its central LDAP directory service

[Link](https://uit.stanford.edu/service/directory)

LEAP (Lightweight Extensible Authentication Protocol): A legacy and proprietary Cisco wireless authentication protocol that authenticates users through their credentials to grant them network access. It relies on a modified version of MS-CHAP and it is vulnerable to offline dictionary password attacks. It has well known security weaknesses and should be replaced with newer, secure methods such as EAP-TLS and PEAP to overcome LEAP's restrictions.

Link:
https://securew2.com/blog/leap-authentication-and-how-it-works

M

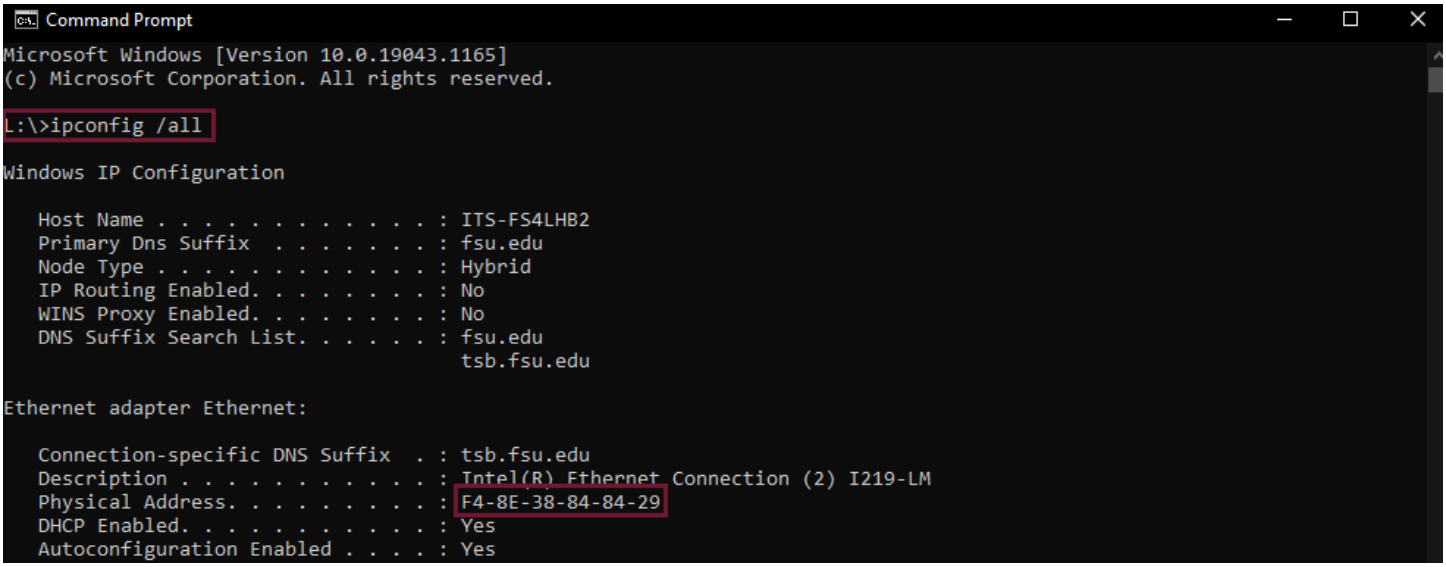
MaaS (Monitoring as a Service): A cloud service that remotely observes a companies infrastructure, applications, servers and services. Not to be confused with Model as a Service.

MAC (Mandatory Access Control): An access control model where access is determined by centrally enforced security policies (e.g. operating system constrains), often using classifications, security labels and user clearances.

Example: A user without the required clearance cannot access a classified document, even if its owner wants to share it.

MAC (Media Access Control): A unique physical address (identifier) used for local network interface communication (e.g. a Wi-Fi adapter can use MAC). MAC ensures that multiple devices can share a network connection equally and in an organized and efficient way.

You can find the MAC physical address by opening the Windows Command Prompt, typing **getmac** OR **ipconfig /all**, and looking for the **Physical Address**.



[Link](https://servicecenter.fsu.edu/s/article/How-do-I-find-the-MAC-address-on-my-computer-1600352497612)

Note: MAC filters can easily be spoofed.

Example: A Wi-Fi router only allows these MAC addresses:

- AA:BB:CC:11:22:33 - Approved laptop
- DD:EE:FF:44:55:66 - Approved phone

If the attacker discovers the laptop's MAC address, the attacker can then spoof (change) their own MAC address to AA:BB:CC:11:22:33, thereby making the router now allow the attacker's device onto the network.

MAC (Message Authentication Code): A cryptographic value that verifies message authenticity and integrity.

MAN (Metropolitan Area Network): A network that connects networks (LANS) across a city or metropolitan region.

MBR (Master Boot Record): A legacy disk sector containing boot code and partition information. Traditionally, when you used to turn on a computer:

1. BIOS checks that the essential hardware is present and working before starting the operating system.
2. BIOS reads the MBR, which helps the computer find the partition where the operating system is located.
3. The MBR examines the partition table to find the active (bootable) partition and executes its boot code.
4. The operating system then uses that partition and begins loading it into memory.

MD5: A broken 128-bit hashing algorithm that is considered insecure because attackers can create two different inputs (e.g. text strings) that produce the same hash, thereby causing a collision.

MDF (Main Distribution Frame): A central telecommunications point that connects external provider lines (e.g. internet or telephone service lines) with internal network cabling. The main idea is to make cable changes quick and easy without rewiring the building e.g. if you're switching to a new internet provider, you can set up and test the new connection first, then switch to a patch cable to make the change in seconds.

MDM (Mobile Device Management): A general IT process *and* a type of security software that manages and secures devices to achieve endpoint security.

Example:

An example of an MDM policy is where an IT team decides that every company laptop must use encryption.

An example of MDM software is a team configuring Microsoft Intune to configure, deploy and enforce the encryption requirement across devices to support the MDM process.

MFA (Multifactor Authentication): An electronic authentication method that requires two or more different types of verification to confirm a user's identity before granting access.

MFD (Multifunction Device): A single machine that combines several functions within one device e.g. MFP

MFP (Multifunction Printer): A printer that combines capabilities such as scanning, copying, and faxing.

[Link](https://www.ricoh-usa.com/en/glossary/multifunction-printer)

ML (Machine Learning): An AI method that enables systems to learn patterns and make predictions from data.

MMS (Multimedia Messaging Service): An extension of standard text messaging that sends multimedia messages (e.g. pics, gifs, etc) across cellular networks.

[Link](https://en.wikipedia.org/wiki/Multimedia_Messaging_Service)

MOA (Memorandum of Agreement): A formal document that defines cooperative responsibilities toward a shared objective.

MOU (Memorandum of Understanding): A high-level document that describes mutual intentions between parties, often without contractual commitment. An MOU is often signed before a Memorandum of Agreement (MOA). Note of course that every business/organization is different, and parties can move straight to a formal MOA contract/definitive agreement without ever drafting or signing an MOU.

> Generally, the process is:
>
> 1. MOU - First, both companies express their intention to work together.
> 2. BPA - Next, they establish the business partnership and its terms.
> 3. MOA - Finally, they outline specific responsibilities for a particular project.

MPLS (Multi-Protocol Label Switching): A networking technology that efficiently forwards network traffic using short path labels instead of reading complex IP addresses.

MSA (Master Service Agreement): A legal contract between a client and a vendor that establishes baselines used to speed up future contract negotiations e.g. services, payment terms, responsibilities, & governing law.

[Link](https://www.docusign.com/blog/master-service-agreements-msas)

MSCHAP: A Microsoft proprietary authentication protocol derived from CHAP.

MSP (Managed Service Provider): A third party (e.g. an outside IT company) under a service agreement that manages a company's IT services such as IT infrastructure, end-user systems, network monitoring, cloud services, and security management.

> Example:
> Infosys, Accenture, Tata Consultancy Services

It is always a good idea to vet MSPs to ensure they follow strong security practices and comply with relevant standards, such as ISO/IEC 27001.

MSSP (Managed Security Service Provider): A third-party company that focuses exclusively or primarily on cybersecurity defense, threat monitoring, and compliance as an IT service, typically through a Security Operations Center (SOC).

MTBF (Mean Time Between Failures): The average time a system or component operates normally between unexpected breakdowns.

MTTF (Mean Time to Failure): The average amount of time that a system will operate before it fails.

[Link](https://www.ibm.com/think/topics/mttr)

MTTR (Mean Time to Recover): The average time required to restore service after failure.

$$\text{MTTR} = \frac{\text{Total Downtime (or Restoration Time)}}{\text{Number of Incidents}}$$

MTU (Maximum Transmission Unit): The size of the largest packet a network interface can transmit without fragmentation.

N

NAC (Network Access Control): A process that supports confidentially by evaluating devices policies and restricting unauthorized devices. It enforces policy before or during network access.

NAT (Network Address Translation): A method of rewriting IP addresses as traffic passes through a network device. IPv6 doesn't use NAT.

NDA (Non-Disclosure Agreement): A contract that requires parties to protect specified private information.

NFC (Near-Field Communication): A subset of RFID technology that enables short-range wireless communication between nearby compatible devices. RFID on the other hand can be used over longer distances and is often used for tracking and identification purposes.

NFC is the ideal technology for smartphone taps, digital wallets, and access cards

[Link](https://www.t-mobile.com/dialed-in/tips-tricks/what-is-nfc)

NGFW (Next-Generation Firewall): A security device that combines traditional filtering with other advanced security features e.g. application awareness and advanced threat prevention.

NIDS (Network-Based Intrusion Detection System): A specific type of IDS that monitors incoming network traffic and alerts suspicious activity across entire network segments.

NIPS (Network-Based Intrusion Prevention System): A specific type of IPS that monitors network traffic and automatically blocks detected threats.

NIST (National Institute of Standards and Technology): A U.S. agency that develops measurement standards and cybersecurity guidance.

> Example: Follow **NIST SP 800-53** guidelines for risk management.

NTFS (New Technology File System): The default Microsoft file system for Windows OS that supports permissions, journaling, encryption, and large volumes.

NTLM (New Technology LAN Manager): A family of legacy Microsoft authentication protocols that use challenge-response mechanisms to prove a client's identity.

NTP (Network Time Protocol): A networking protocol that synchronizes computers and devices to the correct time using time servers. By default, Port 123 is used for NTP; pneumonic: 123 NTP

O

OAuth (Open Authorization): An open standard for letting applications access user information without receiving the user's password.

OCSP (Online Certificate Status Protocol): An internet protocol that checks an X.509 digital certificate's revocation status.

OID (Object Identifier): A unique dotted numeric string (such as 1.3.6.1.2.1.1.5.0 to identify sysname or 1.3.6.1.2.1.1.1.0 that returns the system description of a network device) that is used to retrieve all attributes, variables, objectClasses or system settings from devices like routers, switches, and servers. OIDs can be used within a SNMP command inside a terminal to retrieve specific information.

Example command used in the Net-SNMP suite to retrieve the device's uptime:

snmpget -v 2c -c public 192.168.1.1 1.3.6.1.2.1.1.3.0

Example Output:

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8640000) 1 day, 0:00:00.00

[Link](https://uit.stanford.edu/service/directory/datadefs/objectidentifiers)

OS (Operating System): Software that manages computer hardware, resources, applications, and common program services.

OSINT (Open-Source Intelligence): Intelligence collected and analyzed from publicly available sources.

OSPF (Open Shortest Path First): A routing protocol that helps routers find the best path to send data within an IP network by using Dijkstra's Shortest Path First algorithm.

OT (Operational Technology): Hardware and software that monitors or controls physical devices, processes, and enterprise events e.g. factory equipment, power plants, water treatment systems. Usually, IT teams sit in the office managing data, while OT teams sit on the factory or plant floor managing physical machines.

OTA (Over the Air): Wireless transmission of data, configurations, or software updates to devices such as Wi-Fi and cellular networks (4G/5G)

OVAL (Open Vulnerability Assessment Language): An XML-based standard for cybersecurity tools to describe, test and share vulnerabilities by sharing machine-readable information. It serves as a core standard within SCAP, working alongside CVE and CVSS.

P

P12 (PKCS #12): A portable format for storing or transporting private keys, certificates, and related secrets.

P2P (Peer to Peer): A decentralized model where equal participants can each initiate communication and share resources e.g. Bitcoin, BitTorrent.

PaaS (Platform as a Service): Cloud platform for developing, running, and managing applications without maintaining underlying infrastructure.

PAC (Proxy Auto Configuration): A file which contains rules that tells a web browser to connect directly to a destination or route through a specific proxy server based on the requested URL and host.

PAM (Privileged Access Management): An approach that controls and monitors privileged access to critical systems and assets.

PAM (Pluggable Authentication Modules): A framework that integrates multiple authentication methods through a common API.

PAP (Password Authentication Protocol): A simple authentication protocol that transmits usernames and passwords in plaintext.

PAT (Port Address Translation): (a.k.a. NAT Overload) A specific type of NAT that uses port overloading to translate TCP or UDP connections between private hosts and public networks using port numbers.

PBKDF2 (Password-Based Key Derivation Function 2): A key derivation function that strengthens passwords through salting and repeated computation.

PBX (Private Branch Exchange): A private telephone network used inside a company or organization.

PCAP (Packet Capture): The process of capturing data packets across a network segment.

PCI DSS (Payment Card Industry Data Security Standard): A set of security requirements for organizations handling payment-card information.

PDU (Power Distribution Unit): A device that distributes electrical power to multiple computers or network components, especially in racks.

PEAP (Protected Extensible Authentication Protocol): An extension of EAP that protects authentication exchanges, including passwords, within an encrypted tunnel.

PED (Personal Electronic Device): A small electronic device used for personal communication, data management, or recreation e.g. smartphones.

PEM (Privacy Enhanced Mail): A text-based format that is commonly used to store and translate certificates, and cryptographic keys (whether public or private). PEM is a packaging format that can contain CSRs and is not a security algorithm (e.g. RSA).

PFS (Perfect Forward Secrecy): A security feature that ensures compromised long-term keys cannot be decrypted later.

PGP (Pretty Good Privacy): A data encryption program that provides digital signatures, privacy, and authentication for data communications (e.g. emails, files, and text messages).

> Example:
>
> Edward Snowden secretly communicated his surveillance revelations to journalists in 2013 via PGP encryption.
>
> Proton Mail uses PGP for their end-to-end encryption.

[Link](https://proton.me/blog/what-is-pgp-encryption)

PHI (Personal Health Information): Health information that identifies individuals e.g. health status, healthcare delivery, or healthcare payment.

PII (Personally Identifiable Information): Personal information that is usable alone or with other data to identify, contact, or locate someone. Example: Social Security Number.

PIV (Personal Identity Verification): The U.S. federal standard for reliable identification and access-control credentials.

PKCS (Public Key Cryptography Standards): RSA-established standards that cover public-key cryptography formats and operations.

PKI (Public Key Infrastructure): The framework (e.g. roles, policies, technologies, and procedures) that manages digital certificates and public-key encryption.

ELI5: The main purpose of PKI is to manage digital certificates to secure communications and verify identities.

POP (Post Office Protocol): An older Internet protocol that lets local email clients (e.g. Outlook) retrieve/download messages from remote servers. By default, Port 110 is the standard default port for unencrypted POP3.

For example:

1. Someone sends you an email.
2. The email is stored on your mail server.
3. Your email application uses POP3 to download the email to your computer.

[Link](https://support.microsoft.com/en-us/outlook/what-is-the-difference-between-pop-and-imap)

POTS (Plain Old Telephone Service): Traditional voice-grade residential and small-business telephone service.

PPP (Point-to-Point Protocol): A data-link protocol that establishes direct connections between two network nodes.

PPTP (Point-to-Point Tunneling Protocol): One of the oldest VPN protocols that relies on GRE.

PSK (Pre-Shared Key): A secret password or key that is known between devices before communication or a connection has been established.

PTZ (Pan-Tilt-Zoom): A motorized camera that allows remote control of its viewing direction and magnification. PTZ cameras are commonly used in security buildings, such as office complexes, and are particularly useful for monitoring large areas, entrances, parking lots, and building perimeters.

PUP (Potentially Unwanted Program): A security classification used by cybersecurity software to flag programs that are not outright malicious (e.g., ransomware or Trojans) but rather considered undesirable because of their behavior or effects.

> Example:
>
> Downloading a program that comes bundled with PUPs that changes the browser settings or slows down the computer.

R

RA (Recovery Agent): Entity authorized to recover cryptographic keys, certificates, or encrypted data.

RA (Registration Authority): Verifies certificate requests and authorizes a Certificate Authority to issue certificates.

RACE (Research and Development in Advanced Communications Technologies in Europe): Former European program researching advanced telecommunications networks.

RAD (Rapid Application Development): Software methodology prioritizing rapid prototypes, user feedback, and iterative releases.

RADIUS (Remote Authentication Dial-In User Service): A protocol used for controlling, logging and centralizing network AAA (Authentication, Authorization, and Accounting). By default, Port 1812/1813 is used for RADIUS.

RAID (Redundant Array of Inexpensive Disks): Combines drives into one logical unit for redundancy or improved performance.

RAS (Remote Access Server): Server providing remote users or computers access to network resources.

RAT (Remote Access Trojan): Malware providing attackers a backdoor for remote administrative control.

RBAC (Role-Based Access Control): An access control model that restricts system access according to authorized users' organizational roles.

Example:

An HR employee can access personnel records because their role grants that permission.

RBAC (Rule-Based Access Control): A type of an access control model that grants or denies access according to predefined rules, conditions, and contextual policies.

Example:

A rule might block all access to a server room outside of normal 9:00 AM to 5:00 PM working hours, even for IT staff

RC4 (Rivest Cipher Version 4): Fast stream cipher now considered insecure because of serious vulnerabilities.

RDP (Remote Desktop Protocol): Microsoft protocol providing graphical remote access to another networked computer. By default, Port 3389 is used for RDP.

RFID (Radio Frequency Identifier): A technology used to identify and track tags attached to objects automatically. It can span low, high, and ultra-high frequencies unlike Near Field Communication (NFC) that operates strictly at a single high frequency.

Example: A clothing store can use RFID tags on shirts. An employee scans a whole rack with an RFID reader to count the shirts quickly, instead of scanning each barcode one by one.

RFID Cloning can allow someone to impersonate or copy a tag/a badge onto another blank tag, potentially leading to theft, false inventory records, or unauthorized access.

RIPEMD (RACE Integrity Primitives Evaluation Message Digest): Family of cryptographic hash functions developed in Belgium.

ROI (Return on Investment): Measure comparing an investment's financial benefit with its cost.

RPO (Recovery Point Objective): The maximum acceptable data loss measured backward in time from disruption.

RSA (Rivest, Shamir, and Adleman): Public-key cryptosystem widely used for encryption, key exchange, and digital signatures.

RTBH (Remotely Triggered Black Hole): Routing technique discarding malicious traffic to mitigate denial-of-service attacks.

RTO (Recovery Time Objective): Targeted maximum duration for restoring a business process after disruption.

RTOS (Real-Time Operating System): Operating system processing time-sensitive data with predictable, minimal delays.

RTP (Real-Time Transport Protocol): Network protocol delivering audio and video across IP networks.

S

S/MIME (Secure/Multipurpose Internet Mail Extensions): Standard providing public-key encryption and digital signatures for MIME email.

SaaS (Software as a Service): Provider-hosted applications delivered to customers over the internet.

SAE (Simultaneous Authentication of Equals): A secure wi-fi password-authentication protocol used by WPA3 wireless networks.

SAML (Security Assertions Markup Language): A standard for exchanging authentication and authorization data between identity (IdP) and service providers.

SAN (Storage Area Network): Dedicated network providing consolidated block-level storage access.

SAN (Subject Alternative Name): X.509 extension listing additional hostnames or identities protected by one certificate.

SASE (Secure Access Service Edge): Architecture combining wide-area networking with cloud-delivered security functions.

SCADA (Supervisory Control and Data Acquisition): A subset of ICS, architecture monitoring and controlling industrial processes through computers and networked communications.

SCAP (Security Content Automation Protocol): Standards enabling automated vulnerability management, measurement, and policy-compliance evaluation.

SCEP (Simple Certificate Enrollment Protocol): Protocol automating secure digital-certificate enrollment and issuance.

SD-WAN (Software-Defined Wide Area Network): Software-controlled WAN that optimizes traffic routing across remote locations.

SDK (Software Development Kit): Packaged collection of tools and resources for developing software.

SDLC (Software Development Lifecycle): Process for planning, creating, testing, deploying, and maintaining information systems.

SDLM (Software Development Lifecycle Methodology): Framework defining software-development stages from feasibility through maintenance.

SDN (Software-Defined Networking): A network architecture that uses software controllers or APIs to direct network traffic and manage hardware.

SE Linux (Security-Enhanced Linux): Linux security framework enforcing mandatory access-control policies.

SED (Self-Encrypting Drives): A storage device that automatically and continuously encrypts stored data without user interaction.

SEH (Structured Exception Handler): Windows mechanism handling hardware and software exceptions.

SFTP (Secured File Transfer Protocol): Secure file-transfer method using SSH to encrypt network data.

SHA (Secure Hashing Algorithm): NIST-published family of cryptographic hash functions producing fixed-length message digests. For instance, the 2011 NIST guidance formally deprecated SHA-1 for digital signatures.

SHTTP (Secure Hypertext Transfer Protocol): Obsolete alternative to HTTPS for encrypting HTTP web communications.

SIEM (Security Information and Event Management): A software that monitors and analyzes security logs, events and alerts from applications and network hardware in real-time.

[Link](https://www.microsoft.com/en-us/security/business/security-101/what-is-siem)

SIM (Subscriber Identity Module): Smart card securely storing information identifying a mobile-service subscriber.

SLA (Service-Level Agreement): A contract between a provider and client that defines service quality, availability, response times, responsibilities, and performance expectations.

SLE (Single Loss Expectancy): Expected monetary loss from one occurrence of a risk affecting an asset.

SMS (Short Message Service): Text-messaging service used by telephone, internet, and mobile-device systems.

SMTP (Simple Mail Transfer Protocol): An internet standard transmitting email across IP networks. By default, Port 25 is used for SMTP.

SMTPS (Simple Mail Transfer Protocol Secure): Secures SMTP using TLS for authentication, integrity, and confidentiality.

SNMP (Simple Network Management Protocol): Collects, organizes, and modifies information about managed IP network devices. By default, Port 161/162 is used for SNMP.

Example: https://www.net-snmp.org/

SOAP (Simple Object Access Protocol): Messaging specification for exchanging structured information between web services.

SOAR (Security Orchestration, Automation, and Response): A collection of software tools and solutions that connect security systems via APIs and automate incident response with standardized playbooks. They provide centralized case management to help SOC (Security Operations Center) analysts investigate and remediate threats faster.

[Link](https://www.microsoft.com/en-us/security/business/security-101/what-is-soar)

Scenario:

1. SOAR is proactively configured to receive an alert through an integration, API, or event mechanism.
2. Sometime later, an email security tool detects a suspicious phishing email and sends an alert to the SOAR platform.
3. **Upon receiving the alert, SOAR** triggers the predefined workflow. SOAR queries the SIEM, threat intelligence tools, and email security systems to gather relevant information, assess the threat, and determine the appropriate response actions from a **playbook containing a** predefined set of instructions or rules. The playbook tells the system what steps to perform (e.g., quarantine the email, block malicious indicators, and initiate account-protection actions).

4. SOAR records the incident, evidence, actions taken, and results for the SOC analyst to review.

SoC (System on Chip): Integrated circuit combining major computer or electronic-system components on one chip.

SOC (Security Operations Center): Centralized team monitoring and addressing organizational and technical security issues.

[Link](https://www.microsoft.com/en-us/security/business/security-101/what-is-a-security-operations-center-soc)

SOW (Statement of Work): Project document defining vendor activities, deliverables, responsibilities, and timelines.

SPF (Sender Policy Framework): An email authentication method detecting forged sender addresses during delivery.

SPIM (Spam over Internet Messaging): Unsolicited messages distributed through instant-messaging systems.

SQL (Structured Query Language): Language designed to create, query, and manage relational database data.

SQLi (SQL Injection): Attack inserting malicious SQL statements into application inputs for execution.

SRTP (Secure Real-Time Protocol): Protects RTP traffic with encryption, authentication, integrity, and replay prevention.

SSD (Solid State Drive): Fast storage device using nonvolatile flash memory instead of mechanical disks.

SSH (Secure Shell): Cryptographic protocol securely operating network services across unsecured networks. By default, SSH uses Port 22. The designer chose 22 because it was available and sat perfectly between the two insecure protocols he designed SSH to replace: FTP (port 21) and Telnet (port 23)

SSL (Secure Sockets Layer): Legacy technology used for encrypting online communication.

SSO (Single Sign-On): A system that lets users access multiple applications after one authentication.

STIX (Structured Threat Information eXchange): A standard for exchanging cyber-threat intelligence and is used to describe threats and indicators (e.g. uses specific Language and serialization format?).

SWG (Secure Web Gateway): Filters malicious web traffic and enforces organizational or regulatory browsing policies.

T

TACACS+ (Terminal Access Controller Access Control System): Centralizes validation of users accessing routers or network-access servers.

TAXII (Trusted Automated eXchange of Indicator Information): Application-layer protocol for simple, scalable cyber-threat information exchange.

TCP/IP (Transmission Control Protocol/Internet Protocol): A Communications protocol that connects devices across networks and the internet.

TGT (Ticket Granting Ticket): Kerberos credential used to request service tickets without resubmitting user credentials.

TKIP (Temporal Key Integrity Protocol): Legacy IEEE 802.11 wireless security protocol introduced to improve WEP.s

TLS (Transport Layer Security): A protocol that secures internet connections (e.g. HTTPS uses TLS) and succeeds SSL

TOC (Time-of-Check): Moment a system verifies a resource's state before later use.

TOTP (Time-Based One-Time Password): Algorithm generating temporary passwords valid for short time periods.

TOU (Time-of-Use): Moment a previously checked resource is accessed, when its state may have changed.

TPM (Trusted Platform Module): A hardware chip used to store cryptographic keys and supporting hardware authentication e.g. Bitlocker.

[Link](https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/)

TTP (Tactics, Techniques, and Procedures): Methods and strategies that describes attackers' strategic goals, methods, and operational steps.

TSIG (Transaction Signature): Shared-secret protocol authenticating DNS messages and updates.

U

UAT (User Acceptance Testing): The final software testing phase where users verify that the software handles required real-world tasks.

UAV (Unmanned Aerial Vehicle): A type of aircraft that operates without a human pilot a.k.a. a drone.

UDP (User Datagram Protocol): A connectionless protocol that prioritizes speed. It exchanges time-sensitive messages without guaranteed delivery and is used for time-sensitive transmissions where minor data loss is acceptable in exchange for speed, e.g. VoIP (Voice over IP), online gaming and DNS lookups.

[Link](https://www.lenovo.com/us/en/glossary/what-is-udp)

UEFI (Unified Extensible Firmware Interface): A modern firmware interface designed to replace BIOS; it connects computer hardware to the operating system.

UEM (Unified Endpoint Management): Software that enables IT and security teams to manage, monitor, and secure all organizational devices (e.g., mobile devices, desktops, and other endpoints) through a single tool, regardless of operating system or location. UEM combines mobile management tools (e.g. MDM) with solutions for managing on-premises and remote PCs.

[Link](https://www.ibm.com/think/topics/uem)

UPS (Uninterruptible Power Supply): A battery backup device that provides temporary power when the primary source fails.

URI (Uniform Resource Identifier): A unique character string that identifies a name or resource on the internet.

URL (Uniform Resource Locator): A type of URI that points to a resource on a computer network and provides the mechanism (such as http, https, or ftp) to retrieve it.

[Link](https://en.wikipedia.org/wiki/URL)

USB (Universal Serial Bus): A standard for digital data transmission and power delivery between many types of electronics.

[Link](https://en.wikipedia.org/wiki/USB)

USB OTG (USB On-The-Go): A standard that allows compatible mobile devices to act as USB host and connect directly to other devices without a computer.

UTM (Unified Threat Management): A single security product that combines multiple functions (traditionally provided by separate tools) into one system.

UTP (Unshielded Twisted Pair): A common type of copper cable that uses twisted wire pairs for network communications.

V

VBA (Visual Basic for Applications): A Microsoft event-driven programming language embedded within applications for automation. For example, macros in Microsoft Office applications are created using VBA.

VDE (Virtual Desktop Environment): A virtual machine that provides a graphical experience similar to a physical desktop.

VDI (Virtual Desktop Infrastructure): The technology that hosts desktop operating systems centrally on a server and delivers them to users remotely.

[Link](https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-virtual-desktop-infrastructure-vdi)

VLAN (Virtual Local Area Network): A group of devices across LAN segments to communicate as one network.

VLSM (Variable Length Subnet Masking): A technique that divides an IP address space into differently sized subnets rather than uniform, equal sizes.

VM (Virtual Machine): An emulated computer system that provides functionality comparable to physical hardware.

VoIP (Voice over Internet Protocol): Technologies that deliver voice and multimedia communications across IP networks.

VPC (Virtual Private Cloud): A secure, isolated private-cloud environment hosted within a public cloud.

[Link](https://cloud.google.com/discover/virtual-private-cloud-vpc)

VPN (Virtual Private Network): A secure, encrypted connection to secure remote access across a less secure network e.g. the internet.

VTC (Video Teleconferencing): A technology that enables people in different locations to hold face-to-face meetings remotely.

W

WAF (Web Application Firewall): A firewall that protects web applications by filtering, monitoring, and blocking HTTP(S) traffic to and from web services. It operates on the application layer (Layer 7).

> Link: https://www.cisco.com/site/us/en/learn/topics/security/what-is-web-application-firewall-waf.html

WAP (Wireless Access Point): A networking device that connects Wi-Fi clients to a wired network.

WEP (Wired Equivalent Privacy): An obsolete wireless-network security protocol that is now considered insecure.

WIDS (Wireless Intrusion Detection System): A type of IDS system that detects and alerts administrators to suspicious activity on wireless networks. Some examples include suspected MAC spoofing and Brute-Force Anomalies.

WIPS (Wireless Intrusion Prevention System): A type of IPS that monitors wireless networks and automatically blocks detected threats, rogue access points, and unauthorized devices.

WO (Work Order): A document that authorizes and describes maintenance, repair, installation, or other work to be completed. Examples can include WOs for electric outage, gas leakage, etc.

WPA (Wi-Fi Protected Access): A wireless security standard that improved WEP through stronger encryption and authentication.

WTLS (Wireless TLS): A legacy security protocol that provides privacy, integrity, and authentication for Wireless Application Protocol communications.

X

XDR (Extended Detection and Response): A security platform that integrates security data across multiple sources (e.g. endpoints, networks, email, and cloud systems) to detect and respond to threats. XDR integrates with SIEM, EDR, and SOAR to strengthen cybersecurity.

[Link](https://www.microsoft.com/en-us/security/business/security-101/what-is-xdr)

XML (Extensible Markup Language): A text-based language for structuring, storing, and exchanging data using customizable tags and attributes. XML requires opening and closing tags (e.g. <item> value </item>)

[Link](https://aws.amazon.com/compare/the-difference-between-json-xml/)

XOR (Exclusive OR): A logical operation that:

- returns true when the inputs are different from each other
- returns false when the inputs match.

XSRF (Cross-Site Request Forgery): Another name for CSRF, an attack that tricks authenticated browsers into sending unauthorized requests.

XSS (Cross-Site Scripting): An attack that injects malicious scripts into trusted websites in users' browsers.

Incident Response Process

The Incident Response (IR) process is a step-by-step approach organizations follow to identify, detect, analyze, contain, eliminate, and recover from security incidents while improving responses to future threats.

In simple terms:

1. **Prepare**: Plan and be ready before a security incident can occur.
2. **Detect**: Use tools to identify suspicious activity.
3. **Analyze**: Investigate and assess whether the incident is an actual threat.
4. **Contain**: Isolate the affected systems to stop the incident from spreading.
5. **Eradicate**: Remove threats, malware and vulnerabilities.
6. **Recover**: Restore systems and return to normal operations.
7. **Lessons Learned**: Document the incident, publish reports and improve future security practices.

In long terms:

1. **Preparation: Get Ready Before an Incident**

   Purpose: Prevention is always better than a cure. Establish everything (e.g. planning, training, policies, and tools) needed to respond to a security incident before one occurs.

   - Develop an Incident Response Plan (IRP) that defines roles, responsibilities, and procedures.
   - Train employees and conduct tabletop exercises.
   - Implement security tools such as SIEM, IDS/IPS, and endpoint monitoring.
   - Maintain asset inventories, policies, and communication plans.

2. **Detection: Identify the Incident**

   Purpose: Detect suspicious activity or security events that may indicate an incident. This can include viewing alerts, logs, monitoring, and suspicious emails.

   - Monitor systems using SIEM, IDS/IPS, and security alerts.
   - Review logs for unusual activity, such as repeated failed login attempts.
   - Identify suspicious network traffic or unexpected system behavior.
   - Encourage users to report phishing emails and suspicious activity.

3. **Analysis: Determine If It Is a Real Threat**

   Purpose: Assess the event to determine whether a security incident has occurred and how serious it is.

   Think analysis-type questions such as: Is this a real incident? What happened? How bad is it?

   - Validate alerts to determine whether they are true positives or false positives.

- Identify the attack type, affected systems, and scope of the incident.
- Determine the potential impact and severity.
- Collect and preserve evidence while maintaining the chain of custody.

4. **Containment: Isolate infected system to stop the spread**

   Purpose: Prevent the incident from spreading to other systems and/or causing further damage.

   - Isolate compromised computers or devices from the network.
   - Disable affected accounts if necessary.
   - Use network segmentation to limit access to other systems.
   - Preserve evidence before making changes to affected systems.

5. **Eradication: Remove the Threat Completely [5th Letter of Alphabet = 5th Step in IR Process]**

   Purpose: Eliminate the cause of the incident from the environment.

   - Remove malware, malicious files, and unauthorized software.
   - Patch vulnerabilities that allowed the attack.
   - Reset compromised passwords and credentials.
   - Rebuild compromised systems from known-clean backups when necessary.

6. **Recovery: Restore Normal Operations**

Purpose: Safely return systems & services to normal operation. Restore, test, reconnect, and monitor.

- Restore systems and data from clean backups.
- Test systems to confirm they are functioning properly.
- Reconnect systems to the network after verifying they are secure.
- Implement additional security controls, such as MFA.
- Monitor systems for signs of recurring attacks or reinfection.

7. **Lessons Learned: Document and Improve**

Purpose: Review the incident and improve security to prevent similar incidents in the future. Lessons Learned means review, document, update, report, and improve.

- Conduct a post-incident review to determine what happened.
- Document findings and create an incident report to identify what worked & what needs improvement.
- Update security policies, procedures, and the Incident Response Plan.
- Communicate findings to management and relevant stakeholders.

Ports - Explained

This section covers essential network ports, protocols, and their functions.

20/21 (FTP): File Transfer Protocol.

Port 20 for data transfer, Port 21 for control connections of file transfers, but unencrypted (less secure).

22 (SSH): Secure Shell.

Used for secure remote access to servers & command-line systems (encrypted connection)

23 (Telnet): Unencrypted remote access protocol.

Rarely used due to security risks but may appear in legacy systems.

25 (SMTP): Simple Mail Transfer Protocol.

Used for sending emails b/w email servers, often paired with SMTPS for secure transmission.

53 (DNS): Domain Name System.

Resolves domain names (e.g., google.com) to IP addresses. Uses UDP and TCP & is critical.

80 (HTTP): Hypertext Transfer Protocol.

Used for standard unencrypted web traffic (vulnerable to interception). Port 443 is secure.

110 (POP3): Post Office Protocol v3.

Retrieves & downloads emails , typically unencrypted unless paired with SSL/TLS. Port 995 is secure.

123 (NTP): Network Time Protocol.

Synchronizes clocks across systems, critical for time-sensitive operations (e.g. logging).

137–139 (NetBIOS): Network Basic Input/Output System.

Used for legacy Windows networking services, such as file and printer sharing.

143 (IMAP): Internet Message Access Protocol.

Accesses emails stored on a mail server and supports folder synchronization. Port 993 is secure.

161/162 (SNMP): Simple Network Management Protocol.

Used for monitoring and managing network devices;

Port 161 handles queries, and Port 162 handles traps.

389 (LDAP): Lightweight Directory Access Protocol.

Manages directory services, such as user authentication in Active Directory. Port 636 is secure.

443 (HTTPS): HTTP Secure.

Used for secure (encrypted) web traffic that utilizes SSL/TLS; this is the standard for secure websites.

445 (SMB): Server Message Block.

Used for Windows file and printer sharing and is often targeted by attacks.

636 (LDAPS): LDAP Secure.

Encrypted version of LDAP using SSL/TLS for secure directory access.

993 (IMAPS): IMAP Secure.

Encrypted version of IMAP for email retrieval using SSL/TLS for secure access to mail servers.

995 (POP3S): POP3 Secure.

Encrypted version of POP email retrieval using SSL/TLS, enhancing security for email access.

1812/1813 (RADIUS): Remote Authentication Dial-In User Service.

Used for triple A (authentication, authorization, and accounting) in network access.

3389 (RDP): Remote Desktop Protocol.

Enables remote Windows access and requires strong security to prevent unauthorized access.

Ports - Mnemonics

This section covers mnemonics that will help you remember essential network ports, protocols, and their functions.

Port 20 & 21: FTP

Mnemonic: Sorry, I F'd up the file transfer.

Port 22: SSH

Mnemonic: Shhh.

Port 23: Telnet

Mnemonic: Tell No One.

Port 25: SMTP (Simple Mail Transfer Protocol)

Mnemonic: "Santa Mail" protocol that transfers simple mail on Dec 25th.

Port 53: DNS (Domain Name System)

Mnemonic: Dad! No Salt! You're 53.

Port 67(server), 68(client): DHCP (Dynamic Host Configuration Protocol)

Mnemonic: Downtown Has Cheese Pizza where 67th Street and 68th Cross.

Port 80: HTTP (Hypertext Transfer Protocol)

Mnemonic: Around the World in 80 Days

Port 110: POP (Post Office Protocol)

Mnemonic: The Post Office Pension is 110K.

Port 123: NTP (Network Time Protocol)

Mnemonic: Time is ticking as easy as 123

Port 137-139: NetBIOS

Mnemonic: I caught 137-139 fish in a net!

Port 143: IMAP (Internet Message Access Protocol)

Mnemonic: 143 is a numeric shorthand meaning "I love you".

Did you see my email? I mapped out 143 (my love).

https://www.youtube.com/watch?v=ox8atHI_NH0

Port 161/162: SNTP (Simple Network Management Protocol)

Mnemonic: Our simple HOA network manages houses 161 and 162.

Port 389: LDAP (Lightweight Directory Access Protocol)

Mnemonic: Our lightweight employee directory is only 389 entries long!

Port 443: HTTPS (HTTP Secure)

Mnemonic: 4x4 safe with 3 being the key.

OR don't visit https://www.443.com

Port 445: SMB (Server Message Block)

Mnemonic: Whenever you're ready to share Windows files, call the number 445.

Port 636: LDAPS (LDAP Secure)

Mnemonic: Our specific computer, PC-636, uses LDAPS to securely access directory information (e.g. account details)

Example scenario:

1. At work, the supervisor turns on PC-636.
2. PC-636 needs to verify the employee's account details to verify if they're authorized to access company resources.
3. It securely contacts the company's directory server using LDAPS.
4. The server checks the account information and sends a response over an encrypted connection.

Port 993: IMAPS (IMAP Secure)

Mnemonic: When an employee deletes an email labeled "I ❤️ Imaps 993" on their phone, the email client then updates the server.

Port 995: POP3S (POP3 Secure)

Mnemonic: An employee downloads an email labeled "I HATE POP3S 995" from the mail server to their computer using POP3, allowing them to read it locally.

Port 1812/1813: RADIUS (Remote Authentication Dial-In User Service)

Mnemonic: War of 1812 caused the RADIUS of the dial-in line to remotely be about 1812/1813.

Port 3389: RDP (Remote Desktop Protocol)

Mnemonic:

Many applications use RDP (e.g. MS Remote Help) to remotely access & control computers.

In one case, the user who needs help opens the app and entered the helper's session code '3389' to start the remote session.

Ports - Knowledge Check #1

This section covers a list of key network ports to test your memory. Go through each port number and try to recall its protocol and primary use before checking the answer.

=== === Never give up. Trust your instincts. === ==

Port 21

Port 22

Port 23

Port 25

Port 53

Port 67/68

Port 80

Port 110

Port 123

Port 137–139

Port 143

Port 161/162

Port 389

Port 443

Port 445

Port 636

Port 993

Port 995

Port 1812/1813

Port 3389

Ports - Knowledge Check #2

=== === Never give up. Trust your instincts. === ==

DHCP (Dynamic Host Configuration Protocol)

DNS (Domain Name System)

FTP

HTTP (Hypertext Transfer Protocol)

HTTPS (HTTP Secure)

IMAP (Internet Message Access Protocol)

IMAPS (IMAP Secure)

LDAP (Lightweight Directory Access Protocol)

LDAPS (LDAP Secure)

NetBIOS

NTP (Network Time Protocol)

POP (Post Office Protocol)

POP3S (POP3 Secure)

RADIUS (Remote Authentication Dial-In User Service)

RDP (Remote Desktop Protocol)

SMB (Server Message Block)

SMTP (Simple Mail Transfer Protocol)

SNTP (Simple Network Management Protocol)

SSH

Telnet

References

https://www.oppc.us/secplus/acronyms.html

https://www.oppc.us/secplus/ports.html