CompTIA Security+ SY0-601 Notes

@edoardottt

Thanks reddit.com/user/Average_Down for original notes

1.1 - Compare and contrast different types of social engineering techniques

- **Typosquatting** - URL Hijacking eg: google.com vs g00gle.com
- **Pretexting** - Lying to get your info; actor and a story
- **Pharming** - Poisoned DNS server, redirects a legit website to a bogus site
- **Vishing** - Voice phishing, often spoofed numbers
- **Smishing** - SMS phishing, spoofing here too (text messages)
- **Spear Phishing** - Targeted phishing
- **Whaling** - Spear phishing the CEO or other "large catch" (C level)
- **Eliciting Information** - Extracting information from the victim, often used with vishing
- **Computer Hoaxes** - A threat that doesn't exist
- **Watering Hole Attack** - It targets groups of users by infecting websites that they commonly visit
- **Defense in Depth** - Layered defense
- **Spam** - Unsolicited messages
- **Spim** - Spam over instant messaging
- **Mail Gateway** - On-site or cloud-based filter for unsolicited email
- **Tarpitting** - Slow down the server conversation intentionally
- **Credential Harvesting** - Attacker collects usernames and passwords

Social Engineering principles: Authority, Intimidation, Social proof/Consensus, Scarcity, Urgency, Familiarity/Liking, Trust

1.2 - Given a scenario, analyze potential indicators to determine the type of attack

- **Malware** - Malicious software, gathers information ie: keystrokes, controlled over a botnet, show advertisements, viruses or worms with malware, your computer must run a program, use links or pop-ups
- **Virus** - Malware that reproduces itself, needs a user to start the process, reproduces through file systems or the network, and may or may not cause problems.
- **Virus types**:

    - program viruses (part of an application)
    - boot sector viruses (starts in the boot sector of OS)
    - script viruses (operating system and browser-based)
    - macro viruses (common in Microsoft Office, similar to script virus)
    - fileless virus - a stealth attack, doesn't install or save on the system, good for avoiding anti-virus detection, operates in the memory could be in the registry
- **Worms** - Malware that self-replicates, doesn't need you to do anything, uses network as transmission medium, spreads quickly, signatures can be stopped at the IDS/IPS or Firewall
- **Wannacry worm** - 2017, installed crypto-malware, smbV1 used to infect vulnerable systems and installed double pulsar to encrypt user data
- **Crypto-malware** - A new generation of ransomware, malware encrypts the data files
- **Protect against ransomware** - Always have a backup, offline and not on the same system
- **Trojan Horse** - Software that pretends to be something else, doesn't replicate, circumvents anti-virus
- **PUP** - Potentially Unwanted Program, undesired program often installed along with other software, can hijack your browser
- **RAT** - Remote Administration Tool or Remote Access Trojan, controls the device (ie: DarkComet RAT)
- **Rootkit** - Originally a Unix technique, modifies core system files in part of the kernel, invisible to antivirus software
- **Zeus/Zbot malware** - Kernel driver famous for cleaning out bank accounts, combined with Necurs rootkit, Necurs ensures Zbot can't be deleted and denies any termination process
- **Secure boot with UEFI** - Protects against rootkits in the BIOS
- **Adware** - Pop-up ads everywhere, cause performance issues
- **Spyware** - Malware that spies on you; advertising, identity theft, and affiliate fraud; often a trojan, can capture browser surfing habits, keylogger
- **Logic Bomb** - Often used by someone with a grudge; time bombs, user event, difficult to identify, many logic bombs delete themselves
- **Spraying Attack** - Common passwords, used only a few times to prevent lockout before moving to the next account; hidden from alarms and detection
- **Brute Force** - Every possible password combination until the hash is matched, can take some time, a strong hash algorithm slows things down, most accounts will lockout, more common for an attacker to check for the hash offline
- **Dictionary attack** - Using common words, password crackers can substitute letters
- **Rainbow tables** - Pre-built set of hashes, contains pre-calculated hash chains, speed increased over previous password attacks, rainbow tables are application or OS-specific
- **Salt** - Random data added to a password before hashing takes place
- **Birthday attack** - 23 students have 50% of 2 students having the same birthday, for 30 there's a 70% chance, hash collisions happen when different input gives an output that uses the same hash.
- **MD5 hash** - Has hashing collisions.

- **Downgrade Attack** - Force the system to use a weaker encryption method

1.3 - Given a scenario, analyze potential indicators associated with application attacks

- **XSS (cross-site scripting)** - Originally called cross-site because of browser security flaws, info from one site could be shared with another, very common; malware that uses javascript
- **Non-persistent (reflected) XSS** - Website allows javascript to run in user input fields,
- **Persistent (stored) XSS** - Stored permanently on the website via a post, no specific targets
- **Code injection attack** - Code added into a data stream, enabled because of bad programming;
- **SQL injection** - Uses SQL to access, add, or remove info from a DataBase
- **XML injection** - Modify XML requests
- **LDAP attack** - Manipulates LDAP databases
- **DLL injection** - Injects code into applications and uses the app to run the DLL inside a new process
- **Buffer overflows** - Overwriting a buffer of memory; developers should perform bounds checking, not easy to exploit
- **Pass the Hash** - A replay attack that lets the attacker intercept a hash and replay it back to the server to authenticate, use SSL/TLS to encrypt the hash and stop this attack

1.4 - Given a scenario, analyze potential indicators associated with network attacks

- **Bluejacking** - Sending unsolicited messages over Bluetooth
- **Bluesnarfing** - Access data on a mobile device over Bluetooth

1.5 - Explain different threat actors, vectors, and intelligence sources

1.6 - Explain the security concerns associated with various types of vulnerabilities

1.7 - Summarize the techniques used in security assessments

- **Syslog** - Standard for centralized logging
- **UEBA (User and Entity Behavior Analytics)** - Examine how people are using the network
- **Sentiment Analysis** - Measure how your organization is viewed from the outside
- **SOAR (Security Orchestration, Automation and Response)** - Automate routines, tedious and time invasive activities

1.8 - Explain the techniques used in penetration testing

- **Rules of Engagement** - Defines purpose and scope of a penetration test
- **Wardriving / Warflying** - Search WiFi access points with your car or with a drone

2.1 - Explain the importance of security concepts in an enterprise environment

- **Network Diagrams** - Document physical wire and device
- **IP schema** - IP address plan; number of subnets, hosts, and ranges
- **Data masking** - Hide some of the original data; obfuscating, i.e. ***-**-5555
- **Data encryption** - Encode information into unreadable data; plain text to cipher text
- **Diffusion** - Changing even 1 character results in a completely different output
- **Data at-rest** - The data in on a storage device
- **Data in-transit** - Data moving over the network
- **Data in-use** - Typically decrypted to be used by humans, very attractive to attackers
- **Tokenization** - Replace sensitive data with non-sensitive data; used in NFC with mobile phone credit cards
- **IRM** - Information Rights Management; prevents certain document functions or changes e.g. copy and paste
- **DLP** - Data Loss Prevention is a system that prevents leaking sensitive information

- **SSL/TLS inspection** - Often attacks use TLS to encrypt their malicious site; this inspection gets between the endpoints to determine if the signature is trusted by a Certificate Authority (CA)
- **SSL/TLS Proxy** - Often starts with a firewall, contains an internal CA certificate
- **Hashing** - Message digest as a short string; one-way trip, impossible to recover the original message (verify downloads by comparing hashes; used with digital signatures providing non-repudiation)
- **Hashing collision** - Multiple messages can have the same hash if there is a "collision"; hashing algorithms that have collisions should not be used
- **SHA256** - 256 bits / 64 hexadecimal characters
- **API** - Application programming interfaces; control software or hardware programmatically; secure and harden a login page
- **On-Path attack** - Intercept and modify API messages or replay API commands
- **API injection** - Inject data into an API message
- **API security** - Authentication, limit API access to legitimate users over secure protocols; authorization, API should not allow extended access, each user has limited roles
- **WAF** - Web Application Firewall, apply rules to Web/API communication
- **Hot site** - Constantly updated replica of your production network
- **Cold site** - The complete opposite of a hot site, no data, no applications, no people, only access to power and a network
- **Warm site** - Somewhere in the middle, racks and some equipment, quicker to get ready than a cold site, just bring your software and data
- **Honeypot** - Very attractive (for attackers) fake system to get information about attackers
- **Honeyfile** - File with fake sensitive data (e.g. passwords.txt)
- **DNS Sinkhole** - A DNS that hands out incorrect IP address

2.2 - Summarize virtualization and cloud computing concepts

- **Edge Computing** - Process application data on an edge server close to the user (the local IoT device, often processing on the device itself). No latency, no network requirement; processes data on the device, not the cloud
- **Fog Computing** - A cloud that's close to your data; cloud and IoT combined, extends the cloud
- **Thin Client** - Basic application using VDI or DaaS; local device using a keyboard, mouse, and screen; no huge memory or CPU needs
- **Virtualization** - Run many different OSes on the bare-metal hardware (needs Hypervisor)
- **Containerization** - A container that contains everything you need to run an application; isolated processes in a sandbox, self-contained, apps don't interact with each other. No OS is needed, using the Kernel of the current OS.

- **APIs** - Break up an application into microservices; APIs are resilient and scalable; more secure than a monolithic application
- **Serverless architecture** - Function as a Service (FaaS); stateless compute containers, quick launch servers that are ephemeral (temporary), managed by a third party (Pay as you use)
- **VPC** - Virtual Private Cloud; pool of applications
- **Transit gateway** - Provides cloud routing to VPC often through a VPN

2.3 - Summarize secure application development, deployment, and automation concepts

- **SDN (Software Defined Networking)** - Two planes of operation (Control and Data), programmable networks
- **VM sprawl** - Uncontrolled growth of VMs within an environment; administrators can no longer manage them effectively
- **Sandboxing** - Isolated testing environment
- **Elasticity** - Increase the amount of app instances (horizontal scaling)
- **Scalability** - Increase the hardware capability (resources) of VMs (vertical scaling)
- **Orchestration** - Automation for deploying cloud components
- **Stored Procedure** - Prevent SQL injection
- **Obfuscation** - Turn readable code into unreadable code
- **Software Diversity** - Alternative compiler paths would result in a different binary each time (minimize the attack surface)
- **Continuous Integration (CI)** - Code is constantly written and merged into a central repository
- **Continuous Delivery/Deployment (CD)** - Automates the process for testing and then release without human intervention

2.4 - Summarize authentication and authorization design concepts

- **Directory Service** - Single database with all usernames and passwords for an organization (e.g. Microsoft Active Directory)
- **Federation** - Provides network access to others (other organization)
- **Attestation** - Prove the hardware is yours; a system you can trust. Remote attestation uses TPM and unique hardware identifiers (e.g. IMEI)
- **TOTP** - Time-Based One-Time Password algorithm
- **HTOP** - HMAC-Based One-Time Password algorithm (no short time limit)
- **Retinal Scanner** - Unique capillary structure in the back of the eye

- **Iris Scanner** - Texture, color
- **Facial recognition** - Shape of the face and features
- **Gait Analysis** - Identify a person on how they walk
- **Vascular scanner** - Match the blood vessels visible from the skin
- **False Acceptance Rate (FAR)** - Likelihood an *unauthorized* user will be *accepted*
- **False Rejection Rate (FRR)** - Likelihood an *authorized* user will be *rejected*
- **Crossover Error Rate (CER)** - Defines the overall accuracy of a biometric system (FAR=FRR)

2.5 - Given a scenario, implement cybersecurity resilience

- **RAID (Redundant Array of Independent Disks)**:
    - **RAID 0** - Striping without parity: High performance, no fault tolerance
    - **RAID 1** - Mirroring: Fault tolerant, requires twice the disk space
    - **RAID 5** - Striping with parity: Fault tolerant, additional disk for redundancy
    - **Combinations of items above**
- **NIC Teaming** - Aggregate bandwidth using multiple NICs (fail over on other NICs)
- **SAN Replication** - A specialized high-performance network of storage devices; can replicate between SANs, share data between different devices
- **Full Backup** - Backup everything
- **Incremental Backup** - Backup since the last incremental backup; starts with the first incremental backup after the initial full backup. Must use all incremental backups and initial full backup to restore data.
- **Differential Backup** - Backup since the last full backup; this includes the information in the previous differential backup. Only one full backup and the last differential needed to restore the data.
- **NAS** - Network Attached Storage; file-level access, must overwrite the entire data to add changes
- **SAN** - Storage Area Network; block-level access, can add to the files

2.6 - Explain the security implications of embedded and specialized systems

- **Embedded System** - Hardware and software designed for a specific function (e.g. traffic light controllers, digital watches, medical imaging systems)
- **SoC (system on a chip)** - Multiple components running on a single chip, common with embedded systems; small form factor, low power consumption.

- **Field-programmable gate array (FPGA)** - Integrated circuit that can be configured after manufacturing (new software can be pushed to the device)
- **SCADA/ICS** - Supervisory Control And Data Acquisition, large-scale multi-site Industrial Control Systems (ICS). Requires extensive segmentation
- **HVAC** - Heating, Ventilation and Air Conditioning (traditionally not built with security in mind)
- **RTOS (Real-Time Operating System)** - Operating system with a deterministic processing schedule. No time to wait for other processes (e.g. anti-lock brakes)
- **SIM Card** - Subscriber Identity Module; A universal integrated circuit card, contains mobile details like IMSI
- **Narrowband** - Narrow range of frequency that can transmit over long distances (opposite of broadband)
- **Baseband** - The communication signal uses all of the bandwidth (uses single frequency)
- **Zigbee** - IoT networking IEEE 802.15.4 PAN, an alternative to WiFi; less power used and lets you mesh your IoT network. Uses ISM band (Industrial, Scientific, and Medical band)

2.7 - Explain the importance of physical security controls

- **USB Data Blocker** - Don’t connect to unknown interfaces (Allow the voltage, reject the data)
- **Juice Jacking** - USB data theft through unknown USB jacks ie: phone charger at an airport
- **FM-200** - Fire suppressor avoiding data center destruction
- **Screened Subnet** - Or DMZ, an additional layer of security between the Internet and internal network
- **PDS (Protected Distribution System)** - Physically secure cabled network
- **Air-Gap** - Physical separation between networks; not able to access the separated network devices
- **Shredder/Pulverizer/Hammer/Drill** - Destruct the storage device
- **Degaussing** - Drive unusable using electromagnetic fields
- **Purge** - Only delete some of the data
- **Wipe** - Unrecoverable removal of data; usually overwrites the data, useful for reusing the drives
- **Sdelete** - Windows sysinternals; file level overwriting
- **DBAN** - Darik's Boot and Nuke; whole drive wipe secure data removal

2.8 - Summarize the basics of cryptographic concepts

- **Key Stretching** - Hashing a hash
- **Bcrypt** - Key stretching library; uses blowfish cipher to perform multiple rounds of hashing on passwords
- **PBKDF2** - Password-Based Key Derivation Function 2; part of RSA public key cryptography standards (PKCS #5, RFC 2898)
- **Lightweight cryptography** - IoT devices have less power (compute or otherwise); NIST leads the effort, providing powerful encryption at low cost
- **Homomorphic encryption (HE)** - Performs the calculation while the data stays encrypted and saves the decrypted data to be only viewed with the encryption key
- **Symmetric encryption** - Only uses a single key to encrypt and decrypt; "a shared secret", doesn't scale well. Very fast to use, less overhead than asymmetric encryption (about 128-bits or larger)
- **Asymmetric encryption** - Multiple keys; public key cryptography, the private key is not shared while the public key is shared, the private key is the only key that can decrypt the data encrypted by the public key
- **Diffie-Hellman key exchange** - Taking user1 private key and user2 public key to create a symmetric key that can only be deciphered with both user1 and user2 public/private keys.
- **ECC** - Elliptic Curve Cryptography; used by mobile and IoT devices, uses curves to make smaller keys than other asymmetric encryption methods
- **Key strength**: Larger keys tend to be more secure
- **Key exchange**:
    - out-of-band key exchange - doesn't send symmetric key over the network
    - in-band key exchange - sending it on the network using another encryption method
- **Session keys** - Ephemeral keys (not reusable) need to be unpredictable; session keys are made from in-band key exchange
- **RSA key pair** - SSL/TLS encryption key pair
- **Perfect Forward Secrecy (PFS)** - Change the method of key exchange; *elliptic curve or Diffie-hellman ephemeral*; session keys that change, PFS requires more computing power not all servers can choose PFS and not all browsers can use PFS
- **Quantum Computing** - Uses qubits instead of classical binary; qubits represent both 0 and 1 simultaneously; it breaks our existing encryption mechanisms by quickly factoring prime numbers
- **NTRU** - Cryptosystem using lattice theory; "closest-vector" problem instead of prime numbers; not vulnerable to quantum computing
- Quantum communication protects against eavesdropping; once a QKD (quantum key distribution) is viewed it will change the key

- **Stream cipher** - Encryption is done one bit or byte at a time; high speed, low hardware complexity, used with symmetric encryption not commonly used with asymmetric encryption, the key is often combined with an initialization vector (IV)
- **Block cipher** - Encrypt a fixed-length group; often 64-bit or 128-bit blocks
- **ECB** - Electronic Code Book; block encryption without salt that can give an idea as to what the data was before masking, not ideal
- **CBC** - Cipher Block Chaining; easy to implement, each plaintext block is XORed with the previous ciphertext block; adds additional randomization, uses an IV for the first block
- **XOR** - Exclusive OR; 2 identical inputs are a zero and 2 different inputs are a one
- **CTR** - Counter; acts like a stream cipher, encrypts successive values of a "counter", plaintext can be any size since it's part of the XOR.
- **GCM** - Galois/Counter Mode; encrypts quickly and authenticates where it came from, SSH or TLS
- weak IV in RC4 resulted in the WEP security issue
- **DES** - Created in 1977 and able to be decrypted

3.1 - Given a scenario, implement secure protocols

- **SRTP** - Secure Real-time Transport Protocol; keeps VoIP conversations private; uses AES, uses HMAC-SHA1 for authentication, integrity, and replay protection
- **NTP** - Network Time Protocol, it has no security features and is used to amplify DDoS attacks
- **NTPsec** - Secure Network Time Protocol
- **S/MIME** - Secure/Multipurpose Internet Mail Extension; uses PKI
- **IPSec** - Authentication and Encryption for every packet; Security for OSI layer 3; an encrypted tunnel that uses packet signing. Uses Authentication Header (AH) and Encapsulation Security Payload (ESP)
- **FTPS** - FTP over SSL
- **SFTP** - SSH File Transfer Protocol; more advanced capabilities
- **LDAP** - Lightweight Directory Access Protocol; protocol for reading and writing directories over an IP network
- **LDAPS** - LDAP over SSL
- **SASL** - Simple Authentication and Security Layer; Provides authentication using many different methods
- **DNS** - Domain Name System, no security features
- **DNSSEC** - Domain Name System security extensions; validates DNS responses with public key cryptography
- **SNMPv3** - Simple Network Management Protocol v3 (All three of CIA triad)
- **DHCP** - Dynamic Host Configuration Protocol; no security (starvation attack or dhcp snooping)

3.2 - Given a scenario, implement host or application security solutions

- **EDR** - Endpoint Detection and Response; detects threats based on behavior and process monitoring and not just malware signatures, uses root cause analysis and responds.
- **NGFW** - Next-Generation Firewall; identifies the applications on the internet not just the IP or protocol, also called application layer gateway, stateful multilayer inspection, or deep packet inspection. Examines encrypted data before sending it to the destination.
- **HIDS** - Host-based Intrusion Detection System
- **HIPS** - Host-based Intrusion Prevention System
- **TPM** - Trusted Platform Module; cryptographic functions, persistent memory, uses anti-brute force technology
- **Secure Boot** - BIOS includes the manufacturer's public key, and secure boot verifies the bootloader (prevents unauthorized writes to the flash memory).
- **Trusted Boot** - Bootloader verifies the digital signature of the OS kernel; the kernel verifies other startup components. Just before loading the drivers, ELAM (Early Launch Anti-Malware) starts and checks every driver for trust. Windows won't load an untrusted driver
- **Measured Boot** - UEFI stores a hash of the firmware, boot drivers, and everything else. This hash is stored on the TPM.
- **Remote Attestation** - Device provides an operational report to a verification server. Encrypted and digitally signed with the TPM
- **Fuzzing** - Sending random input into applications to find a crash/panic
- **CERT** - Computer Emergency Response Team; Carnegie Mellon CERT created Basic Fuzzing Framework (BFF)
- **SAST** - Static Application Security Testing; finds security vulnerabilities with automation, not everything can be identified through analysis. false positives are an issue and will need to be verified.
- **FDE** - Full Disk Encryption
- **SED** - Self-Encrypting Drive; uses the Opal storage specification as a standard for SEDs

3.3 - Given a scenario, implement secure network designs

- **SSL Offloading** - SSL Encryption/Decryption
- **Round Robin** - each new user is moved to the next server to give the same amount of load to each server; weighted round robin can prioritize a server for use, dynamic round robin will monitor the server load and distribute to the server with the lowest use. this is used with Active/Active load balancing

- **Affinity** - A user will always be distributed to the same server; users tracked with IP or session IDs.
- **Active/Active** - All servers are active
- **Active/Passive** - If an active server fails, the passive server takes its place
- **Air-Gap** - Physical segmentation
- **VLAN** - Logical segmentation (Virtual Local Area Networks)
- **Extranet** - A private network for partners; doesn't allow full access to the intranet, different from a DMZ
- **Intranet** - Internal Private Network
- **Zero Trust** - A holistic approach to network security; every device, every process, and every person need to be verified
- **SSL VPN** - Uses TCP/443 to authenticate users. Can be run from a browser
- **HTML5 VPN** - Create a VPN tunnel without a separate VPN application (using a browser)
- **Full Tunnel** - All encrypted data is passing through the VPN Server
- **Split Tunnel** - Only a subset of connections pass through the VPN Server
- **L2TP** - Layer 2 tunneling protocol; connecting sites over layer 3 network as if they were connected at layer 2, commonly implemented with IPsec (broadcast storm control via switch)
- **Broadcast Storm Control** - Limit the number of broadcast messages per second
- **Loop Protection** - IEEE standard 802.1D prevents loops via STP (Spanning Tree Protocol)
- **BPDU Guard** - Bridge Protocol Data Unit Guard; If a BPDU frame is seen on a PortFast interface, shut down the interface
- **DHCP snooping** - IP tracking on a layer 2 device; the switch becomes a rogue DHCP firewall
- **MAC Filtering** - Limit access through the physical hardware access (beware MAC addresses can be spoofed)
- **DNS Sinkhole** - Redirect users to internal location for known bad domains
- **FIM** - File Integrity Monitoring; Be notified when some files that shouldn’t change are modified (e.g. Tripwire on Linux)
- **Stateless Firewall** - Does not keep track of traffic flows; rule base will cover communication in both directions
- **Stateful Firewall** - Keeps track of traffic flows; create a session table for each flow
- **UTM** - Unified Threat Management (web security gateway); router, firewall, IDS/IPS, spam filter, etc.
- **Jump Server** - Provides an access mechanism to a protected network (highly secured device, but a significant security concern)
- **HSM** - Hardware Security Module; used in large environments with clusters and redundant power. High-end Cryptographic Hardware that is a plug-in card or separate hardware device. keeps overhead away from the server.

3.4 - Given a scenario, install and configure wireless security settings

- **WPA2** - Uses CCMP block cipher mode; data confidentiality with AES and CBC-MAC for MIC, PSK (pre-shared key aka password) brute-force is a problem.
- **WPA3** - Uses GCMP block cipher mode; Galois/Counter Mode protocol; uses AES and GMAC
- **SAE** - Simultaneous Authentication of Equals; WPA3 uses a shared session key, no more hand-shakes. Adds Perfect Forward Secrecy. IEEE standard is known as the "dragonfly handshake"
- **802.1x** - Centralized authentication for wireless networks using login credentials; also referred to as port-based network access control (NAC); uses RADIUS, LDAP, or TACACS+ as an access database
- **WPS** - Wi-Fi Protected Setup; Allows “easy” setup of mobile device (PIN, Push a button, NFC); Absolutely insecure, disable it!
- **EAP** - Extensible Authentication Protocol; an authentication framework for wireless networks, many ways to authenticate based on RFC standards
- **EAP-FAST** - EAP Flexible Authentication via Secure Tunneling; Authentication Server (AS) and supplicant (client) share a protected access credential (PAC) (shared secret) over TLS tunnel; needs a RADIUS server
- **PEAP** - Protected Extensible Authentication Protocol; created by Cisco, Microsoft, and RSA Security; encapsulates EAP in a TLS tunnel, AS uses a digital certificate instead of a PAC. Client doesn't use a certificate. Microsoft uses PEAP with MSCHAPv2, can also be used with GTC (generic token card) or hardware token generator.
- **EAP-TLS** - EAP Transport Layer Security; strong security, wide adoption, and support from most of the industry; Requires digital certificates on the AS and all other devices. AS and supplicant exchange certificates for mutual authentication. TLS tunnel is then built for the user authentication process. Complex implementation; needs PKI (public key infrastructure), all wireless clients need certificates managed and deployed. Not all devices support digital certificates.
- **EAP-TTLS** - EAP Tunneled TLS; supports other authentication protocols in a TLS tunnel; requires a digital certificate on the AS, does not require digital certificates on every device. Builds a TLS tunnel using this digital certificate. Can use other types of EAP, MSCHAPv2, or anything else
- **RADIUS Federation** - Members of one organization can authenticate to the network of another organization using their normal credentials; use 802.1x as the authentication method and RADIUS on the backend. EAP to authenticate.

3.5 - Given a scenario, implement secure mobile solutions

- **Geofencing** - Restrict or allow features when the device is in a particular area
- **Containerization** - Separate enterprise mobile apps and data from a user-owned device.
- **MicroSD HSM** - Same as Hardware Security Module but much smaller and used on a mobile device
- **UEM** - Unified Endpoint Management; Manage mobile and non-mobile devices; end users use different types of devices
- **MAM** - Mobile Application Management; Provision, update and remove apps; Create an enterprise app catalog
- **SEAndroid** - SELinux (Security-Enhanced Linux) on Android OS
- **Geotagging** - Adds location to document metadata
- **BYOD** - Bring Your Own Device; Need to meet the company's requirements
- **COPE** - Corporate-Owned, Personally Enabled; Company buys the device
- **CYOD** - Choose Your Own Device; similar to COPE, but with the user's choice
- **Corporate-Owned** - The company owns the device and controls the content

3.6 - Given a scenario, apply cybersecurity solutions to the cloud

- **AZ** - Availability Zones; Isolated locations with a cloud region; has independent power, HVAC and networking
- **IAM** - Identity and Access Management; who gets access to a cloud resource, maps job functions to roles
- **Compute cloud instances**:
    - Amazon Elastic Compute Cloud (EC2)
    - Google Compute Engine (GCE)
    - Microsoft Azure Virtual Machines
- **CASB** - Cloud Access Security Broker; makes your security policies work in the cloud, determines what apps are in use and if users are authorized (Visibility), Compliance, Threat Prevention, and Data Security
- **SWG** - Next-Gen Secure Web Gateway; Monitor APIs, make policies; protect users and devices. Can apply different policies to different resources

3.7 - Given a scenario, implement identity and account management controls

- **Identity Provider (IdP)** - Authentication as a service; commonly used with SSO applications. Uses standard authentication methods ie. SAML, OAuth, OpenID Connect, etc.
- **ssh-keygen** - A command to create public/private key pairs on Linux and macOS. Use the *ssh-copy-id* command to apply the public key to the server.
- **Service Accounts** - Run in the background and exclusively used by services. Access can be defined for a specific service.
- **Password Entropy** - Entropy measures how difficult the password would be to guess.

3.8 - Given a scenario, implement authentication and authorization solutions

- **KBA** - Knowledge-Based Authentication; static (pre-configured shared secrets e.g. question and answer) or dynamic
- **PAP** - Password Authentication Protocol; a basic authentication method, used in legacy operating systems. Sends everything in the clear, non-encrypted.
- **CHAP** - Challenge-Handshake Authentication Protocol; three-way handshake, after a link is established the server sends a challenge message. The client responds with a password hash calculated from the challenge and the password. The server compares the received hash with the stored hash. This occurs periodically during the connection.
- **MS-CHAP** - Microsoft version of CHAP; uses DES, easy to brute force the NTLM hash. DON'T USE MS-CHAP!
- **RADIUS** - Remote Authentication Dial-in User Service; very common AAA protocol. Centralized authentication.
- **TACACS** - Terminal Access Controller Access-Control System; remote authentication protocol; TACACS+ most advanced version (Cisco)
- **Kerberos** - Network Authentication Protocol; auth once, trusted by the system; mutual authentication (secure against MiTM and replay attacks).
- **IEEE 802.1X** - Port-based Network Access Control; you don’t get access to the network until you authenticate
- **SAML** - Security Assertion Markup Language; Open standard for authentication and authorization; not originally built for mobile devices
- **OAuth** - Authorization framework; used with OpenID connect. OAuth determines what can be used by the third-party app and OpenID Connect provides the authentication.
- **MAC** - Mandatory Access Control; every object gets a label and the user gets a minimum access level.
- **DAC** - Discretionary Access Control; the owner picks the control access, and the data owner can change access at any time (used in most OSes).

- **RBAC (Role-Based Access Control)** - You are assigned rights and permissions based on your role.
- **ABAC** - Attribute-Based Access Control; a next-generation authorization model: combines and evaluates multiple parameters ie: IP address, time of day, desired action, etc.
- **RBAC (Rule-Based Access Control)** - System admin makes the rules for the object trying to be accessed ie: only able to access lab resources between 9am-5pm.
- **Privileged access management (PAM)** - Managing superuser access; privileged access is used temporarily.

3.9 - Given a scenario, implement public key infrastructure

- **PKI** - Public Key Infrastructure; digital certificates: create, distribute, manage, store, and revoke.
- **Digital Certificate** - Binds a public key with a digital signature and other details about a key holder
- **RA (Registration Authority)** - The entity requesting the certificate needs to be verified
- **CRL** - Certificate Revocation List; Maintained by the CA, can contain many revocations in a large file.
- **OCSP** - Online Certificate Status Protocol; the status of the certificate is stapled to the SSL/TLS handshake (OCSP stapling)
- **Domain Validation (DV) Certificate** - Owner of the certificate has some control over a DNS domain
- **Extended Validation (EV) Certificate** - Additional checks have verified the certificate owner's identity
- **Subject Alternative Name** - Lists additional identification information
- **Code Signing Certificate** - Applications can be signed by the developer (user has the opportunity to stop the application if some security check is not passed)
- **Self-Signed Certificate** - Internal certificates don't need to be signed by a public CA
- **DER** - Format designed to transfer syntax for data structures (binary format, not human readable)
- **PEM** - Privacy-Enhanced Mail; Base64-encoded DER certificate
- **PKCS #12** - Personal Information Exchange Syntax Standard; Container format for many certificates, often used to transfer a private and public key pair
- **CER** - Windows X.509 file extension; usually contains a public key
- **PKCS #7** - Cryptographic Message Syntax Standard (contains certificates and chain certificates)
- **Pinning** - "Pin" the expected certificate or public key to an application (compiled in the app)
- **Key Escrow** - Hand over your private keys to a 3rd-party

4.1 - Given a scenario, use the appropriate tool to assess organizational security

- **traceroute** - Determine the route a packet takes to a destination (ICMP messages could be filtered by firewalls)
- **nslookup/dig** - DNS lookup
- **ipconfig** - Determine TCP/IP and network adapter information *on Windows*
- **ifconfig** - Determine TCP/IP and network adapter information *on Linux*
- **ping** - Test reachability using ICMP packets
- **pathping** - Windows command that runs traceroute and ping together to display combined output.
- **netstat** - Network Statistics; -a shows all active connections; -b show binaries (windows); -n just IP addresses
- **arp** - Address Resolution Protocol command; -a will show IP with MAC address
- **route** - Windows Device Routing Table;
    - Windows: route print
    - Linux: netstat -r
- **curl** - client URL; grab raw data from sites and display into a terminal
- **hping** - TCP/IP packet assembler/analyzer; can send almost anything modified in the packet.
- **nmap** - network mapper; port scans, operating system scan, service scans, add scripts;
- **theHarvester** - gathers OSINT; scrapes Google or Bing, DNS brute force, and more
- **sn1per** - combines many recon tools into a single framework
- **scanless** - port scan proxy; run port scans from a different host.
- **dnsenum** - enumerate DNS information; view host information from DNS servers
- **Nessus** - Vulnerability Scanner; extensive reporting.
- **Cuckoo** - A sandbox for malwares; test a file in a safe environment. Track and trace executable files
- **cat** - Concatenate files
- **head** - View the first part of a file
- **tail** - View the last part of a file
- **grep** - Find text in a file
- **chmod** - Change mode of a file system object (read/write/execute)
- **logger** - Add information to the syslog file
- **OpenSSL** - Manages SSL/TLS X.509 certificates; encrypt and decrypt also possible
- **Wireshark** - Graphical packet analyzer
- **tcpdump** - Capture packets from the command line; installed in most Linux versions
- **tcpreplay** - A suite of packet replay utilities; great to use for testing your IPS and firewall with malicious packets
- **dd** - Linux command creates a bit-by-bit copy of a drive; used for forensics
    - Create a disk image: *dd if=/dev/sda of=/tmp/out.img*
    - Restore a disk image: *dd if=/tmp/out.img of=/dev/sda*

- **memdump** - Copy system memory (RAM) to the standard output stream; then copy to another host
- **WinHex** - A universal hexadecimal editor; edit disks, files, RAM, and disk cloning on Windows OS
- **FTK imager** - Windows AccessData forensic drive imaging tool; includes file utilities and read-only image mounting. Support for many different file systems and full disk encryption methods, the investigator still needs the password. Can also import other image formats ie: dd, Ghost, Expert Witness, etc
- **Autopsy** - Performs digital forensics of hard drives or smartphones; views many different types of data.

4.2 - Summarize the importance of policies, processes, and procedures for incident response

- **NIST SP 800-61 Revision 2** - Computer Incident Handling Guide
- **PICERL**:
    - **Preparation**: Communication, Resources, Policies
    - **Identification**: Monitoring
    - **Containment**: Isolation, Sandboxes
    - **Eradication**: Remove, Disable, Fix and Patch
    - **Recovery**: Backup
    - **Lessons Learned**: Learn and Improve
- **Tabletop exercise** - Analysis of a potentially real situation in a meeting
- **Walkthrough exercise** - Applies the concepts from the tabletop exercise
- **Simulation** - Test with a simulated event (phishing, breaches…)
- **Communication Plan** - Get your contact list together (internal and external)
- **Disaster Recovery Plan** - Part of Business Continuity Plan; Keep the organization up and running
- **COOP** - Continuity Of Operations Planning; Must be documented and tested before a problem occurs
- **Incident Response Team** - Receives, Review and Responds
- **Retention Policy** - Backup data! Copies, versions of copies, lifecycle of data, purging of data (also for Regulatory Compliance)
- **MITRE ATT&CK Framework** - Determine the actions of an attacker, identify the point of intrusion, understand methods used to move around, and identify potential security techniques to block future attacks.
- **Diamond Model of Intrusion Analysis** - Adversary, Capability, Victim, Infrastructure
- **Cyber Kill Chain**:
    - **Reconnaissance**
    - **Weaponization**
    - **Delivery**
    - **Exploit**

    - **Installation**
    - **Command & Control (C2)**
    - **Actions on objectives**

4.3 - Given an incident, utilize appropriate data sources to support an investigation

- **NVD** - National Vulnerability Database (nvd.nist.gov)
- **False Positive** - A vulnerability is identified that doesn't really exist
- **False Negative** - A vulnerability exist, but you didn't detect it
- **SIEM** - Security Information and Event Management; used for data correlation and forensic analysis
- **Rsyslog** - Rocket-fast System for log processing
- **Syslog-ng** - A popular syslog daemon with additional filtering and storage options
- **NXLog** - Collection for many diverse log types
- **Journalctl** - Method for querying the system journal
- **Metadata** - Data that describes other types of data
- **NetFlow** - Gather traffic statistics from all traffic flows
- **IPFIX** - IP Flow Information Export (newer NetFlow standard)
- **sFlow** - Sampled Flow; Only a portion of the actual network traffic

4.4 - Given an incident, apply mitigation techniques or controls to secure an environment

- **Approved/Allow List** - Nothing runs unless it's approved
- **Block/Deny List** - Nothing on this "bad list" can be executed
- **URL Filter** - Limit access to untrusted / known malicious websites
- **Isolation** - Administratively isolate a compromised device (or process) from everything else
- **Containment** - Run each application in its own sandbox (limit interaction)
- **Segmentation** - Separate the network; Prevent unauthorized movement, limit the scope of a breach
- **Playbook** - Conditional steps to follow (e.g. investigate a data breach, recover from ransomware)

4.5 - Explain the key aspects of digital forensics

- **RFC 3227** - Guidelines for Evidence Collection and Archiving

- **Legal Hold** - A legal technique to preserve information; prepare for impending litigation
- **Admissibility** - Not all data can be used in a court of law
- **Chain of Custody** - Document evidencing that nothing changed from the incident
- **Recording time offsets** - Timezone determines how the time is displayed (FAT/NTFS)
- **Order of Volatility**:
    1. CPU registers, CPU cache
    2. Router table, ARP cache, process table, kernel statistics
    3. RAM
    4. Temporary file systems
    5. Disk
    6. Remote logging and monitoring data
    7. Physical configuration, network topology
    8. Archival media
- **Snapshot** - Backup of a VM, then incremental update
- **Right-to-audit** - A legal agreement to have the option to perform a security audit at any time
- **E-Discovery** - Gathering electronic data required by the legal process
- **Data Recovery** - Extract missing data without affecting the integrity of the data
- **Non-Repudiation** - Proof of data integrity and the origin of the data (MAC or Digital Signature)
- **Strategic CounterIntelligence** - Prevent hostile intelligence operations, discover and disrupt foreign intelligence threats

5.1 - Compare and contrast various types of controls

- **Managerial controls** - Focus on the security design or security policies; Standard Operational Policies
- **Operational controls** - Implemented by people; security guards or awareness programs
- **Technical controls** - Implemented by the system; OS controls, firewalls, or anti-virus
- **Preventive** - Prevents access to an area; firewalls, door locks, security guards
- **Detective** - May not prevent access; identify and record an intrusion; Motion detectors or IDS
- **Corrective** - Designed to mitigate damage; IPS blocking, restore from backup, backup sites
- **Deterrent** - May not directly prevent access; discourages an intrusion attempt; warning signs, login banners, or security lighting
- **Compensating** - Doesn't prevent an attack; attempts to recover
- **Physical** - Fences or door locks

5.2 - Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture

- **GDPR** - General Data Protection Regulation; Controls export of personal data for individuals in the EU (right to be forgotten, privacy policy…)
- **PCI DSS** - Payment Card Industry Data Security Standard
- **CIS** - Center for Internet Security
- **CIS CSC** - Critical security controls for effective cyber defense using 20 key actions (practical information)
- **NIST RMF** - NIST Risk Management Framework; mandatory for US federal agencies;
    - Categorize - Define Environment
    - Select - Pick appropriate controls
    - Implement - Define proper implementation
    - Assess - Determine if controls are working
    - Authorize - Make a decision to authorize a system
    - Monitor - Check for ongoing compliance
- **NIST CSF** - NIST Cybersecurity Framework;
    - Framework Core:
        i. Identity
        ii. Protect
        iii. Detect
        iv. Respond
        v. Recover
    - Framework Implementation Tiers: An organization's view of cybersecurity risk and process to manage the risk
    - Framework Profile: The alignment of standards, guidelines, and practices to the framework core
- **ISO/IEC Frameworks** - International Organization for Standardization / International Electrotechnical Commission;
    - **27001** - Standard for an Information Security Management System (ISMS)
    - **27002** - Code of practice for information security controls
    - **27701** - Privacy information management systems (PIMS)
    - **31000** - International standards for risk management practices
- **SSAE SOC 2 Type I/II** - The American Institute of Certified Public Accountants (AICPA) auditing Standard Statement of Standards for Attestation Engagements number 18 (SSAE 18)
- **SOC 2** - Trust Services Criteria (security controls); firewalls, intrusion detection, and multi-factor authentication
    - Type I - Audit that tests controls in place at a particular point in time
    - Type II - Audit that tests controls over a period of at least 6 months consecutive
- **CSA** - Cloud Security Alliance; security in cloud computing.

- **CCM** - Cloud Controls Matrix, cloud-specific security controls.
- **Web Server Hardening**:
    - Info leak: banner information, disable directory browsing
    - Permissions: run from a non-privileged account, configure file permissions
    - Configure SSL: manage and install certificates
    - Log files: monitor access logs
- **Operating System Hardening**:
    - Updates: OS updates/service packs, security patches
    - User accounts: minimum password length and complexity, account limitations
    - Network access and security: limit network access
    - Monitor and secure: anti-virus, anti-malware
- **Application Server**:
    - Middleware - usually between the web server and the database (programming languages, runtime, libraries, etc)
    - OS patches
    - Limit access from other devices
- **Network Infrastructure devices**:
    - Configure authentication, NO DEFAULTS!
    - Check for security updates from the manufacturer

5.3 - Explain the importance of policies to organizational security

- **AUP** - Acceptable Use Policy; Used by an organization to limit legal liability
- **Job Rotation** - Keep people moving between responsibilities to limit a single person maintains control for long period of time
- **Mandatory Vacations** - Rotate others through the job, limit the ability for one person to commit a type of fraud
- **Separation of Duties**:
    - **Split Knowledge** - No one person has all of the details
    - **Dual Control** - Two people must be present to perform the business function
- **Clean Desk Policy** - When you leave, nothing is on your desk
- **Least Privilege** - No rights beyond job duties, minimal privileges granted
- **Background Check** - Pre-employment screening (verify claims, criminal history…)
- **Adverse Actions** - Not hiring a candidate due to a failed background check
- **NDA** - Non-Disclosure Agreement; confidentiality agreement/legal contract, prevents the use of dissemination of confidential information
- **Social Media Analysis** - Gather data on social media; build a personal profile, used in hiring
- **On-Boarding** - Policy for new hires, IT agreements need to be signed, Provide required IT equipment, create accounts…

- **Off-Boarding** - Policy for people leaving the organization, opposite of on-boarding (delete accounts…)
- **Phishing Simulation** - See which users are susceptible to phishing attacks without being a victim of phishing
- **Role-based Security Awareness Training** - Before providing access, train your users
- **Supply Chain** - The system involved when creating a product
- **SLA** - Service Level Agreement; minimum terms for services provided; uptime, response time agreements
- **MOU** - Memorandum of Understanding; both sides agree on the contents of the memo; usually includes statements of confidentiality, informal letter of intent, *not a signed contract!!!!*
- **MSA** - Measurement System Analysis; used with quality management systems, assess the measurement process
- **BPA** - Business Partnership Agreement; going into business together, owner stake, financial contract
- **EOL** - End Of Life; stops selling a product, but may continue supporting the product
- **EOSL** - End Of Service Life, no longer selling or supporting the device with patches
- **Data Governance** - Rules, processes and accountability associated with an organization's data
- **Data Classification** - Identify data types (personal, public, restricted…); to protect data efficiently
- **Data Retention** - Keep files that change frequently for version control (for legal requirements too!)
- **Change Control** - A formal process for managing change (avoid downtime, confusion and mistakes):
    - Determine the scope of the change
    - Analyze the risk associated with the change
    - Create a plan
    - Get end-user approval
    - Present the proposal to the change control board
    - *Have a backout plan!* if the change doesn't work
    - Document the changes
- **Asset Management** - Identify and track computing assets to respond faster to security problem
- **Data Steward** - Manages the governance process, responsible for data accuracy, privacy, and security; associates sensitivity labels to the data, ensures compliance with any applicable laws and standards

5.4 - Summarize risk management processes and concepts

- **Risk Acceptance** - We'll take the risk

- **Risk Avoidance** - Stop participating in high-risk activity
- **Risk Transference** - Buy some cybersecurity insurance
- **Risk Mitigation** - Decrease the risk level, invest in security systems
- **Inherent Risk** - Risk that exists in the absence of controls; impact + likelihood
- **Residual Risk** - Risk that exists after the controls are considered; inherent risk + control effectiveness
- **Risk Appetite** - The amount of risk an organization is willing to take
- **HIPAA** - Health Insurance Portability and Accountability Act; New storage requirements, network security, protect against threats
- **ARO** - Annualized Rate of Occurrence
- **SLE** - Single Loss Expectancy: What is the monetary loss if a single event occurs?
- **ALE** - Annualized Loss Expectancy: ARO x SLE
- **RTO** - Recovery Time Objective; how long it takes to get back to a particular service level
- **RPO** - Recovery Point Objective; how much data loss is acceptable
- **MTTR** - Mean Time To Repair; time required to fix the issue
- **MTBF** - Mean Time Between Failures: predict the time between outages
- **DRP** - Disaster Recovery Plan: detailed plan for resuming operations after a disaster
- **Mission-Essential Functions** - The most important systems in your organization; identify these critical systems!

5.5 - Explain privacy and sensitive data concepts in relation to security

- **Information Life Cycle**:
    - Creation and Receipt
    - Distribution
    - Use
    - Maintenance
    - Disposition
- **Privacy Impact Assessment (PIA)** - Privacy risk needs to be identified in each initiative; fix the concerns before they become an issue
- **Data Classification**:
    - **Proprietary Data** - Data that's unique to an organization
    - **PII** - Personally Identifiable Information
    - **PHI** - Protected Health Information
    - **Public/Unclassified** - No restrictions on viewing
    - **Private/Classified/Restricted** - Restricted access
    - **Sensitive** - Intellectual Property, PII, PHI
    - **Confidential** - Very sensitive, must be approved to view
    - **Critical** - Data should always be available

- **Tokenization** - Replace sensitive data with a non-sensitive placeholder (SSN 322-09-5366 –> 100-91-7294); this isn't encryption or hashing
- **Minimization** - Only collect and retain necessary data (HIPAA and GDPR rules this)
- **Masking** - Hide some of the original data (e.g. credit card number ****-****-****-5912)
- **Anonymization** - Make it impossible to identify individual data from a dataset; allows for data use without privacy concerns. ie: hashing, masking, etc.; cannot be reversed, no way to associate the data to a user
- **Pseudo-Anonymization** - Replace personal information with pseudonyms, may be reversible, original data is stored in the database.
- **Data Responsibilities**:
    - **Data Owner** - Accountable for specific data, often a senior officer; ie: VP of Sales owns the customer relationship data
    - **Data Controller** - Manages the purpose and means by which personal data is processed
    - **Data Processor** - Process data on behalf of the data controller, often a third-party
    - **Data Custodian/Steward** - Responsible for data accuracy, privacy, and security; labels the data, ensures compliance, and manages access rights
    - **Data Protection Officer (DPO)** - Responsible for the organization's data privacy, sets policies and implements processes and procedures

Acronym List

3DES Triple Data Encryption Standard
AAA Authentication, Authorization, and Accounting
ABAC Attribute-based Access Control
ACL Access Control List
AD Active Directory
AES Advanced Encryption Standard
AES256 Advanced Encryption Standards 256bit
AH Authentication Header
AI Artificial Intelligence
AIS Automated Indicator Sharing
ALE Annualized Loss Expectancy
AP Access Point
API Application Programming Interface
APT Advanced Persistent Threat
ARO Annualized Rate of Occurrence
ARP Address Resolution Protocol
ASLR Address Space Layout Randomization
ASP Active Server Pages
ATT&CK Adversarial Tactics, Techniques, and Common Knowledge
AUP Acceptable Use Policy

AV Antivirus
BASH Bourne Again Shell
BCP Business Continuity Planning
BGP Border Gateway Protocol
BIA Business Impact Analysis
BIOS Basic Input/Output System
BPA Business Partnership Agreement
BPDU Bridge Protocol Data Unit
BSSID Basic Service Set Identifier
BYOD Bring Your Own Device
CA Certificate Authority
CAPTCHA Completely Automated Public Turing Test to Tell Computers and Humans Apart A
CAR Corrective Action Report
CASB Cloud Access Security Broker
CBC Cipher Block Chaining
CBT Computer-based Training
CCMP Counter-Mode/CBC-MAC Protocol
CCTV Closed-Circuit Television
CERT Computer Emergency Response Team
CFB Cipher Feedback
CHAP Challenge-Handshake Authentication Protocol
CIO Chief Information Officer
CIRT Computer Incident Response Team
CIS Center for Internet Security
CMS Content Management System
CN Common Name
COOP Continuity of Operations Planning
COPE Corporate-owned Personally Enabled
CP Contingency Planning
CRC Cyclic Redundancy Check
CRL Certificate Revocation List
CSA Cloud Security Alliance
CSIRT Computer Security Incident Response Team
CSO Chief Security Officer
CSP Cloud Service Provider
CSR Certificate Signing Request
CSRF Cross-Site Request Forgery
CSU Channel Service Unit
CTM Counter-Mode
CTO Chief Technology Officer
CVE Common Vulnerabilities and Exposures
CVSS Common Vulnerability Scoring System
CYOD Choose Your Own Device
DAC Discretionary Access Control

DBA Database Administrator
DDoS Distributed Denial-of-Service
DEP Data Execution Prevention
DER Distinguished Encoding Rules
DES Data Encryption Standard
DHCP Dynamic Host Configuration Protocol
DHE Diffie-Hellman Ephemeral
DKIM Domain Keys Identified Mail
DLL Dynamic-link Library
DLP Data Loss Prevention
DMARC Domain Message Authentication Reporting and Conformance
DNAT Destination Network Address Transaction
DNS Domain Name System
DNSSEC Domain Name System Security Extensions
DoS Denial-of-Service
DPO Data Protection Officer
DRP Disaster Recovery Plan
DSA Digital Signature Algorithm
DSL Digital Subscriber Line
EAP Extensible Authentication Protocol
ECB Electronic Code Book
ECC Elliptic-curve Cryptography
ECDHE Elliptic-curve Diffie-Hellman Ephemeral
ECDSA Elliptic-curve Digital Signature Algorithm
EDR Endpoint Detection and Response
EFS Encrypted File System
EIP Extended Instruction Pointer
EOL End of Life
EOS End of Service
ERP Enterprise Resource Planning
ESN Electronic Serial Number
ESP Encapsulating Security Payload
ESSID Extended Service Set Identifier
FACL File System Access Control List
FDE Full Disk Encryption
FIM File Integrity Monitoring
FPGA Field Programmable Gate Array
FRR False Rejection Rate
FTP File Transfer Protocol
FTPS Secure File Transfer Protocol
GCM Galois/Counter Mode
GDPR General Data Protection Regulation
GPG GNU Privacy Guard
GPO Group Policy Object

GPS Global Positioning System
GPU Graphics Processing Unit
GRE Generic Routing Encapsulation
HA High Availability
HDD Hard Disk Drive
HIDS Host-based Intrusion Detection System
HIPS Host-based Intrusion Prevention System
HMAC Hash-based Message Authentication Code
HOTP HMAC-based One-time Password
HSM Hardware Security Module
HSMaaS Hardware Security Module as a Service
HTML Hypertext Markup Language
HTTP Hypertext Transfer Protocol
HTTPS Hypertext Transfer Protocol Secure
HVAC Heating, Ventilation, Air Conditioning
IaaS Infrastructure as a Service
IAM Identity and Access Management
ICMP Internet Control Message Protocol
ICS Industrial Control Systems
IDEA International Data Encryption Algorithm
IDF Intermediate Distribution Frame
IdP Identity Provider
IDS Intrusion Detection System
IEEE Institute of Electrical and Electronics Engineers
IKE Internet Key Exchange
IM Instant Messaging
IMAP4 Internet Message Access Protocol v4
IoC Indicators of Compromise
IoT Internet of Things
IP Internet Protocol
IPS Intrusion Prevention System
IPSec Internet Protocol Security
IR Incident Response
IRC Internet Relay Chat
IRP Incident Response Plan
ISA Interconnection Security Agreement
ISFW Internal Segmentation Firewall
ISO International Organization for Standardization
ISP Internet Service Provider
ISSO Information Systems Security Officer
ITCP IT Contingency Plan
IV Initialization Vector
KDC Key Distribution Center
KEK Key Encryption Key

L2TP Layer 2 Tunneling Protocol
LAN Local Area Network
LDAP Lightweight Directory Access Protocol
LEAP Lightweight Extensible Authentication Protocol
MaaS Monitoring as a Service
MAC Media Access Control
MAM Mobile Application Management
MAN Metropolitan Area Network
MBR Master Boot Record
MD5 Message Digest 5
MDF Main Distribution Frame
MDM Mobile Device Management
MFA Multi Factor Authentication
MFD Multifunction Device
MFP Multifunction Printer
ML Machine Learning
MMS Multimedia Message Service
MOA Memorandum of Agreement
MOU Memorandum of Understanding
MPLS Multiprotocol Label Switching
MSA Measurement Systems Analysis
MS-CHAP Microsoft Challenge-Handshake Authentication Protocol
MSP Managed Service Provider
MSSP Managed Security Service Provider
MTBF Mean Time Between Failures
MTTF Mean Time to Failure
MTTR Mean Time to Repair
MTU Maximum Transmission Unit
NAC Network Access Control
NAS Network-attached Storage
NAT Network Address Translation
NDA Non-disclosure Agreement
NFC Near-field Communication
NFV Network Function Virtualization
NGFW Next-generation Firewall
NG-SWG Next-generation Secure Web Gateway
NIC Network Interface Card
NIDS Network-based Intrusion Detection System
NIPS Network-based Intrusion Prevention System
NIST National Institute of Standards & Technology
NOC Network Operations Center
NTFS New Technology File System
NTLM New Technology LAN Manager
NTP Network Time Protocol

OCSP Online Certificate Status Protocol
OID Object Identifier
OS Operating System
OSI Open Systems Interconnection
OSINT Open-source Intelligence
OSPF Open Shortest Path First
OT Operational Technology
OTA Over-The-Air
OTG On-The-Go
OVAL Open Vulnerability and Assessment Language
OWASP Open Web Application Security Project
P12 PKCS #12
P2P Peer-to-Peer
PaaS Platform as a Service
PAC Proxy Auto Configuration
PAM Privileged Access Management
PAM Pluggable Authentication Modules
PAP Password Authentication Protocol
PAT Port Address Translation
PBKDF2 Password-based Key Derivation Function 2
PBX Private Branch Exchange
PCAP Packet Capture
PCI-DSS Payment Card Industry Data Security Standard
PDU Power Distribution Unit
PE Portable Executable
PEAP Protected Extensible Authentication Protocol
PED Portable Electronic Device
PEM Privacy Enhanced Mail
PFS Perfect Forward Secrecy
PGP Pretty Good Privacy
PHI Personal Health Information
PII Personally Identifiable Information
PIN Personal Identification Number
PIV Personal Identity Verification
PKCS Public Key Cryptography Standards
PKI Public Key Infrastructure
PoC Proof of Concept
POP Post Office Protocol
POTS Plain Old Telephone Service
PPP Point-to-Point Protocol
PPTP Point-to-Point Tunneling Protocol
PSK Pre Shared Key
PTZ Pan-Tilt-Zoom
PUP Potentially Unwanted Program

QA Quality Assurance
QoS Quality of Service
PUP Potentially Unwanted Program
RA Registration Authority
RAD Rapid Application Development
RADIUS Remote Authentication Dial-in User Service
RAID Redundant Array of Inexpensive Disks
RAM Random Access Memory
RAS Remote Access Server
RAT Remote Access Trojan
RC4 Rivest Cipher version 4
RCS Rich Communication Services
RFC Request for Comments
RFID Radio Frequency Identification
RIPEMD RACE Integrity Primitives Evaluation Message Digest
ROI Return on Investment
RPO Recovery Point Objective
RSA Rivest, Shamir, & Adleman
RTBH Remotely Triggered Black Hole
RTO Recovery Time Objective
RTOS Real-time Operating System
RTP Real-time Transport Protocol
S/MIME Secure/Multipurpose Internet Mail Extensions
SaaS Software as a Service
SAE Simultaneous Authentication of Equals
SAML Security Assertions Markup Language
SCADA Supervisory Control and Data Acquisition
SCAP Security Content Automation Protocol
SCCM Microsoft System Center Configuration Manager
SCEP Simple Certificate Enrollment Protocol
SDK Software Development Kit
SDLC Software Development Life Cycle
SDLM Software Development Life-cycle Methodology
SDN Software-defined Networking
SDP Service Delivery Platform
SDV Software-defined Visibility
SED Self-Encrypting Drives
SEH Structured Exception Handling
SFTP SSH File Transfer Protocol
SHA Secure Hashing Algorithm
SIEM Security Information and Event Management
SIM Subscriber Identity Module
SIP Session Initiation Protocol
SLA Service-level Agreement

SLE Single Loss Expectancy
SMB Server Message Block
SMS Short Message Service
SMTP Simple Mail Transfer Protocol
SMTPS Simple Mail Transfer Protocol Secure
SNMP Simple Network Management Protocol
SOAP Simple Object Access Protocol
SOAR Security Orchestration, Automation, Response
SoC System on Chip
SOC Security Operations Center
SPF Sender Policy Framework
SPIM Spam over Instant Messaging
SQL Structured Query Language
SQLi SQL Injection
SRTP Secure Real-time Transport Protocol
SSD Solid State Drive
SSH Secure Shell
SSID Service Set Identifier
SSL Secure Sockets Layer
SSO Single Sign-on
STIX Structured Threat Information eXpression
STP Shielded Twisted Pair
SWG Secure Web Gateway
TACACS+ Terminal Access Controller Access Control System
TAXII Trusted Automated eXchange of Intelligence Information
TCP/IP Transmission Control Protocol/Internet Protocol
TGT Ticket Granting Ticket
TKIP Temporal Key Integrity Protocol
TLS Transport Layer Security
TOTP Time-based One Time Password
TPM Trusted Platform Module
TSIG Transaction Signature
TTP Tactics, Techniques, and Procedures
UAT User Acceptance Testing
UDP User Datagram Protocol
UEBA User and Entity Behavior Analytics
UEFI Unified Extensible Firmware Interface
UEM Unified Endpoint Management
UPS Uninterruptible Power Supply
URI Uniform Resource Identifier
URL Universal Resource Locator
USB Universal Serial Bus
USB OTG USB On-The-Go
UTM Unified Threat Management

UTP Unshielded Twisted Pair
VBA Visual Basic for Applications
VDE Virtual Desktop Environment
VDI Virtual Desktop Infrastructure
VLAN Virtual Local Area Network
VLSM Variable-length Subnet Masking
VM Virtual Machine Vo
IP Voice over IP
VPC Virtual Private Cloud
VPN Virtual Private Network
VTC Video Teleconferencing
WAF Web Application Firewall
WAP Wireless Access Point
WEP Wired Equivalent Privacy
WIDS Wireless Intrusion Detection System
WIPS Wireless Intrusion Prevention System
WORM Write Once Read Many
WPA WiFi Protected Access
WPS WiFi Protected Setup
XaaS Anything as a Service
XML Extensible Markup Language
XOR Exclusive OR
XSRF Cross-site Request Forgery
XSS Cross-site Scripting