# Sec+ Notes

Thanks for supporting my channel! These are my notes that I used to pass the Sec+ Exam on my first try!

Prompt:

I am currently studying to get my CompTIA Security+. I want you to act as if you are my tutor preparing me for the test. I am going to ask you about a bunch of different concepts, I want your answers to include a few things.

1. General overview of the concept
2. What I might need to know about it for the Security+ exam

Answer all of my question in this format, until I say otherwise. Can you do that for me?

Bluesnarfing - exploiting bluetooth devices by establishing an unauthorized connection and retrieving sensitive information from them.

Phishing -

Pharming - redirecting requests to fraudulent websites via DNS spoofing

- DNS cache poisoning / DNS spoofing
- Host file poisoning

Vishing - a form of social engineering that uses VOIP to retrieve personal information from its victims

Watering hole attack - when attackers target a specific group and exploits websites that the group commonly visits by injecting malicious code, users that visit the website will be automatically infected without their knowledge

Pretexting - creating a fake scenario to elicit sensitive information from victims

Prepending - when an attacker manipulates the caller ID to make it seem as if its calling from a trusted entity

Rootkit - a type of malicious software that is installed by attackers to provide persistent and stealthy access to a system, they are used to manipulate system functions, files, intercept network traffic

Fileless virus - malware that resides and executes within a system's memory that does not leave a trace behind

Cryptomalware - malicious software that is used to encrypt files on a user's system, until a ransom is paid to the attacked.

Spyware - malicious software that is used to gather information from a user's device without their knowledge or consent

## Password attacks

- Brute force - straight up guessing passwords using every possible combination of characters, can be automated with scripts
- Dictionary - attempts to guess passwords with commonly used passwords, more effective than brute force
- Rainbow Table - a table with ciphertext and their corresponding plain text values, that is used to compare and match with encrypted passwords
- Credential Stuffing - using previous passwords from other breaches to gain access to other accounts, relying on users that use the same passwords for multiple accounts

- Replay - attackers intercept data packets and retransmits them to gain unauthorized access
- Password Spraying - attempting commonly used passwords multiple times across different accounts, while not triggering account lockouts or detection
- Birthday attack - exploits the probability of two different inputs producing the same hash value

On-path attack/man in the middle attack - when an attacker places them in the middle of communication between two entities and intercepts/alters communication between them

Cross site scripting attack (XSS) - attacker injects a website with malicious code, and when victims visit the website, their browser automatically executes the code

## Application attack - malicious activities or techniques that target web applications

- Injection attacks
- XSS
- Cross site request forgery (XSRF) - when authenticated users unknowingly perform malicious actions by exploiting their session
- DDOS

LDAP Injection

XML Injection

Pointer dereference -

Buffer overflow - when buffer overflows with storage and spills over into other memory locations

SSL Stripping - a form of a MITM attack and downgrade attack in which the attacker places themselves in between a communication and downgrades the secure HTTPS connection to an insecure HTTP connection

Pass the Hash - a hacking technique that uses the hashed value to authenticate

Directory traversal attack (dot-dot-slash attack) - an attack in which they attempt to bypass access restrictions and gain unauthorized access to files or execute commands on the web server

Race condition - when multiple processes share the same resources without proper synchronization, this can lead to data inconsistencies, unexpected program behavior, and security vulnerabilities

Application whitelisting - only approved softwares are allowed to run on a system

Refactoring - improving the internal structure of code without compromising its external behavior

Shimming - a thin layer of code that allows for increased compatibility between different software components

RFC Request for Comment - document series that sets the standards of design, development, and implementation of internet standards

CVE (Common Vulnerabilities and Exposures) - dictionary of unique identifiers assigned to publicly known vulnerabilities in software and hardware systems

NVD (National Vulnerability Database) - government repository of vulnerability management data

TTP (Tactics, Techniques, and Procedures) - the methods and approaches used by attackers to conduct attacks

CVSS (Common Vulnerability Scoring System) - framework that is used to quantify the severity and impact of security vulnerabilities

STIX (Structured Threat Information Expression) - WHAT info is relayed, language and framework to exchange cybersecurity threat intel

TAXII (Trusted Automated Exchange Indicator Information) - HOW the info is relayed

HIPS (Host-based Intrusion Prevention System) - security technology that focuses on protecting hosts from intrusions and malicious activities

SIEM (Security Information and Event Management) - collects log data and takes appropriate action

PCAP (Packet Capture) - software tool that captures and analyzes network traffic

SOAR (Security Orchestration, Automation, and Response) - combines security orchestration and automation with incident response to improve efficiency of security operations

DLP (Data Loss Prevention) - defines how your organization shares and protects data without exposing it to unauthorized users

Hot Site - fully operational and ready to use off-site facility

Warm Site - partially equipped off-site facility

Cold Site - off-site facility that provides physical space, but does not have the necessary technological infrastructure

MSP (Managed Service Provider) - third party company that ensures that your IT systems are operational

MSSP (Managed Security Service Provider) - third party company that ensures that your people and IT operations are secure and reliable

Data sanitization - the erasure of data to ensure that it cannot be recovered from the storage device

Normalization - turning data into a standardized format

Baselining - monitoring network performance by comparing it to its historic performance levels

Code obfuscation - making applications difficult to disassemble or decompile

VM Sprawl - when the number of virtual machines reaches a point in which administrators cannot manage them effectively

VM escape - an attacker runs code on the VM that grants them access to the hypervisor

Normalization - organizes data within a database, allowing it to run smoother

OWASP (Open Worldwide Application Security Project) - online community that provides freely-available resources in the field of web application security

TOTP (Time-based One Time Password) - an algorithm that generates a one time password

FAR (False Acceptance Rate) - the rate in which a biometric security feature will incorrectly allow an unauthorized party to pass

FRR (False Rejection Rate) - the rate in which a biometric security system will reject an authorized user

(CER) - the overall accuracy of the biometric system

RAID (Redundant Array of Independent Disks) - technology that combines multiple physical hard drives into a single unit for improved performance, fault tolerance, and data redundancy

**RAID Levels**

- RAID 0 (Striping) - splits data across multiple drives, more efficient
- RAID 1 (Mirroring) - data redundancy across multiple drives, better fault tolerance too
- RAID 5 - requires minimum of 3 drives, block-level striping with parity across multiple drives
- RAID 6 - similar to RAID 5, but can withstand two drives failing without data loss
- RAID 10 - combines RAID 0 and RAID 1, minimum four drives and provides increased fault tolerance and redundancy

NIC Teaming - grouping physical network adapters to improve performance and redundancy

UPS (Uninterruptible Power Supply) - used for emergency power outages

Restore point - a file-based representation of the current state of a virtual machine

**Backups**

- Incremental backups - backing up only the data that has changed since the last full or incremental backup
- Snapshot backups - point-in-time backups that capture the state of a system at a specific moment
- Differential backups -

SCADA (Supervisory Control and Data Acquisition) - system used to monitor and control industrial processes and infrastructure

ICS (Industrial Control System) - used to control industrial systems, works with SCADA

MFD/MFP (Multi Function Device/Multi Function Printer) - a device that combines that functionality of multiple devices into one

RTOS (Real-time Operating System) - an OS designed for real-time applications when timing is critical

POSIX (Portable Operating System Interface) - standards that define an interface between applications and operating systems

TPM (Trusted Platform Module) - a hardware device that provides a range of security functions and features

- Secure boot
- Remote attestation

- Data sealing

HSM (Hardware Security Module) - a hardware device that is used to secure and protect cryptographic keys and perform cryptographic operations

Zigbee - wireless communication protocol for low-power, low-data rate devices (IoT devices)

ANT+ - wireless communication protocol specifically designed for low-power, low-latency applications in the field of sports/health monitoring

Extranet - an extension of the internal network that authorizes external parties access

Degaussing - permanently erasing data from the magnetic media by disrupting the magnetic patterns that store the data

## Encryption

Key stretching - a technique used to increase the computational effort required to derive keys from a password

- Bcrypt
- PBKDF2

Elliptic Curve Cryptography (ECC) - public-key cryptographic system, asymmetric

PFS (Perfect Forward Secrecy) - ensures that confidentiality of past communication sessions even if the long-term secret keys used in those sessions have been compromised

Ephemeral Key - an asymmetric key that is used for only one session

Static key - a key that is used for a longer duration and sessions

Session key - asymmetric key that is used for encryption and decryption in a single session

ECB - weakest block cipher mode, DES

Homomorphic encryption - encrypted data can still be processed

EFS (Encrypting File System) - file-level encryption within Microsoft Windows

FDE (Full Disk Encryption) - a method of encrypting an entire storage device

## Symmetric Encryption Algorithms

- Advanced Encryption Standard (AES): AES is a widely used symmetric encryption algorithm that supports key sizes of 128, 192, and 256 bits.
- Data Encryption Standard (DES): DES is an older symmetric encryption algorithm that uses a 56-bit key and operates on 64-bit blocks of data.
- Triple Data Encryption Standard (3DES): 3DES is a variant of DES that applies the DES algorithm three times to each block of data, using two or three different keys.
- Blowfish: Blowfish is a symmetric key block cipher that operates on variable-length blocks and supports key sizes from 32 to 448 bits.
- Twofish: Twofish is a symmetric key block cipher that supports key sizes up to 256 bits and operates on 128-bit blocks.

- Serpent: Serpent is a symmetric key block cipher that operates on 128-bit blocks and supports key sizes of 128, 192, and 256 bits.
- Camellia: Camellia is a symmetric key block cipher that operates on 128-bit blocks and supports key sizes of 128, 192, and 256 bits. It is a joint development by NTT and Mitsubishi Electric Corporation.
- IDEA (International Data Encryption Algorithm): IDEA is a symmetric key block cipher that operates on 64-bit blocks and supports key sizes of 128 bits.
- RC4: RC4 is a stream cipher known for its simplicity and speed. It operates on variable-length keys and generates a keystream that is XORed with the plaintext to produce the ciphertext.
- ChaCha20: ChaCha20 is a stream cipher that is widely used in applications such as TLS. It operates on 512-bit blocks and supports key sizes of 128, 256 bits.

## Asymmetric Algorithms

- RSA (Rivest-Shamir-Adleman):
  RSA is one of the most widely used asymmetric encryption algorithms. It relies on the difficulty of factoring large prime numbers. The algorithm generates a public-private key pair, where the public key is used for encryption, and the private key is used for decryption. RSA is often employed in secure email communication, SSL/TLS protocols, digital signatures, and key exchange.
- Diffie-Hellman (DH):
  Diffie-Hellman is a key exchange algorithm that allows two parties to establish a shared secret key over an insecure communication channel. It enables secure communication even if an eavesdropper intercepts the exchange. Diffie-Hellman is used in various protocols such as SSL/TLS, IPsec, and secure email.
- Elliptic Curve Cryptography (ECC):
  ECC is a family of asymmetric algorithms based on the mathematics of elliptic curves over finite fields. ECC provides the same level of security as RSA but with smaller key sizes, making it computationally efficient. It is commonly used in resource-constrained environments such as mobile devices and Internet of

Things (IoT) devices. ECC is utilized in SSL/TLS, digital signatures, and secure key exchange.

- Digital Signature Algorithm (DSA):
  DSA is a widely used algorithm for creating and verifying digital signatures. It provides authentication, integrity, and non-repudiation of digital documents. DSA uses the mathematics of modular exponentiation and discrete logarithms. It is commonly used in digital certificates, secure email, and secure file transfers.
- PGP

DNSSEC - ensures that you are communicating with the correct website or service

## Wireless Network Protocols

1. WEP (Wired Equivalent Privacy): WEP was the original security protocol used for wireless networks. However, it is now considered weak and easily compromised. Its use is strongly discouraged.
2. WPA (Wi-Fi Protected Access): WPA is an improvement over WEP and provides stronger security. It uses TKIP (Temporal Key Integrity Protocol) for encryption and includes authentication mechanisms like WPA-PSK (Pre-Shared Key) and WPA-Enterprise (using an authentication server).
3. WPA2 (Wi-Fi Protected Access 2): WPA2 is the current standard for wireless network security. It uses the AES (Advanced Encryption Standard) algorithm for encryption and offers stronger security than WPA. It supports both WPA2-PSK and WPA2-Enterprise authentication modes.
4. WPA3 (Wi-Fi Protected Access 3): WPA3 is the latest iteration of Wi-Fi security protocols. It enhances security by introducing new features like SAE (Simultaneous Authentication of Equals) and stronger encryption methods. WPA3 is backward compatible with WPA2.
5. EAP (Extensible Authentication Protocol): EAP is an authentication framework used in wireless networks. It allows for different authentication methods to be used, such as EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled TLS),

PEAP (Protected EAP), and EAP-FAST (Flexible Authentication via Secure Tunneling).

## Network Protocols

IPsec - rules or protocols for secure connections over a network

- AH (Authentication Header) - authenticates the origin of packets
- ESP (Encapsulating Security Payload) - provides confidentiality, integrity, and authentication
- Transport mode - only encrypts payload
- Tunnel mode - entire packet encryption

POP3 - one-way incoming mail protocol that downloads emails onto a local device

SNMP (Simple Network Management Protocol) - facilitates the collection of information about devices on a network

- SNMPv1
- SNMPv2
- SNMPv3
- SNMPv4

SMTP - a TCP/IP protocol used in sending and receiving mail

TCP is responsible for delivery, while IP is responsible for the correct address to which the data is sent

MAC (Mandatory Access Control) - high level of access control security that requires all access to be predefined based on system classification, configuration, and authentication

Nessus - vulnerability assessment tool that assesses vulnerabilities in computer networks, systems, and apps

Netcat - networking tool that manages network connections

**Aircrack-ng** - a suite of network security tools for assessing the security of Wi-Fi networks, capturing network packets, and conducting various attacks on Wi=Fi encryption protocols

MD5 and SHA-1 are cryptographic hash functions, which means they take any length input and produce a fixed-size output called a hash value or digest.

WPA (Wi-Fi Protected Access) - wireless security protocol designed to secure Wi-Fi networks, more secure than WEP

tracert - a command line tool that allows you to trace the route a network packet takes from your computer to a destination IP address or hostname

GLBA (Gramm-Leach-Bliley Act) - a U.S. federal law that requires financial institutions to share how they share and protect customer’s private information

SOX (Sarbanes-Oxley) - U.S. federal law that sets requirements for all US public company boards

DHCP scope - the range of IP addresses that are able to be assigned to devices within a network

DHCP snooping - a security feature on network switches that mitigates the risk of rogue DHCP serves and unauthorized network access

EDR (Endpoint Detection and Response) - security solutions designed to detect and respond to threats and malicious activities on endpoints

SWG (Secure Web Gateway) - provides organizations with visibility, control, and protection for web traffic.

CASB (Cloud Access Security Broker) - acts as the middle man between an organization’s on prem infrastructure and cloud, to ensure that both are secure

RADIUS (Remote Authentication Dial-In User Service) - network protocol that focuses on AAA, and managing user access to network resources

Opal - SED (self encrypting drive) technology that provides hardware-based encryption to protect data that is stored on the drive

MTBF (Mean Time Between Failures - measure to estimate the average time between the failures of a system

MTTR (Mean Time To Recovery) - the amount of time it’ll take to repair a system

MTTF (Mean Time to Failure) - the amount of time until a system is expected to fail

RTO (Recovery Time Objective) - the maximum amount of time that is tolerable to have the systems down

DAC (Discretionary Access Control) - access to a resource is outlined by the owner

802.1X - an authentication framework that controls access to a network, ensures that only authorized devices are granted access to the network resources

How to Read Logs

COPE (Corporate Owned Personally-Enabled) - MDM strategy where organizations provide devices, while allowing limited personal use

VDI (Virtual Desktop Infrastructure) - technology that allows OS and apps to be hosted and delivered to end-user devices over a network

DNS Sinkhole - manipulating DNS responses to redirect traffic from malicious domains to a non-existent or controlled destination

Dump - the process of capturing the contents inside of a computer’s RAM at a specific moment

POST (Power-On Self Test) - tests performed by a computer system to verify hardware components are functioning properly during start up

Kerberos - a network authentication protocol that provides secure authentication for client-server applications over an untrusted network, helps prevent eavesdropping, replay attacks, and unauthorized access

HSM (Hardware Security Module) - tamper-resistant hardware device designed for secure key management, used to safeguard sensitive information like cryptography keys, certificates, and other critical data.

Screened subnet or DMZ - a network architecture design that separates the internal network from the internet (like a network air gap)

VPN concentrator or VPN gateway - networking device that enables secure remote access to a private network over the internet

IMAP (Internet Message Access Protocol) - email retrieval protocol that allows clients to manage emails stored on the mail server

S/MIME - a standard for securing email messages with encryption and digital signatures

Data Custodian - a team or individual responsible for the storage, management, and protection of data

ALE - the expected financial impact of a specific risk over one year

SLE (Single Loss Expectancy) - the expected loss of revenue from a specific risk

ARO - the frequency of the specific event occurring within a one-year period

Containerization -

## Types of Booting

- Measured - a process that involves measuring and recording the integrity of various boot components during startup like firmware, bootloader, OS kernel by the TPM
- Trusted - verifies the measured components' integrity against a known set of trusted values
- Secure - security feature that prevents the execution of malicious software during the boot process

# Standards

**GDPR (General Data Protection Regulation) -** data protection and privacy for individuals in the EU

**PCI DSS (Payment Card Industry Data Security Standard) -** a standard for protecting credit cards

**CSA CCM (Cloud Security Alliance Cloud Controls Matrix)** - security controls and best practices frameworks for secure cloud computing environments

**FISMA (Federal Information Security Management Act)** - U.S. federal law framework that protects gov. info, ops, and assets

**GLBA (Gramm-Leach-Bliley Act) -** requires financial institutions to explain how they share and protect their customer's private information

**SOX (Sarbanes-Oxley)** - US federal law that sets requirements for US public company boards, management, and public accounting firms

## ISO

1. ISO/IEC 27001: This standard specifies the requirements for an information security management system (ISMS). It provides a framework for implementing and managing security controls to protect information assets.
2. ISO/IEC 27002: This standard provides a code of practice for information security controls. It offers guidance on selecting, implementing, and managing security controls to address specific risks identified in an organization. **PII**
3. ISO/IEC 27005: This standard focuses on information security risk management. It provides guidelines for identifying, assessing, and treating information security risks in a systematic and consistent manner.
4. ISO/IEC 27017: This standard offers specific guidelines for information security controls in cloud computing environments. It addresses security considerations related to the use of cloud services and provides guidance for both cloud service providers and cloud customers.
5. ISO/IEC 27018: This standard focuses on privacy protection in public cloud computing environments. It provides guidelines for the implementation of

controls to protect personal data in cloud-based services.

6. ISO/IEC 27031: This standard addresses business continuity management for information and communication technology (ICT) systems. It provides guidelines for planning, establishing, implementing, operating, monitoring, reviewing, and maintaining ICT continuity.

## Commands

- tail - command used to display the last part of a file or stream
- openssl - an open source software library all about cryptography
- scanless - tool that performs port scanning or reconnaissance
- grep - a command that is used for searching and filtering text files or streams based on patterns or regular expressions
- Nmap - open source network scanning tool, identifies open ports, and gathers information about hosts and services that are running in a network
- curl - command line tool that is used for making HTTP requests and interacting with web servers, can be used to download files, send data to web servers, and test APIs.
- head - command used to display the first few lines of a file or beginning of a stream
- tracert - command that is used to trace the route a packet takes from the source device to the destination device
- netstat - command used to view active network connections, listening ports, routing tables, network interface stats
- netcat - command that is used to establish and interact with network connections, can be used for data transmission, port scanning, file transfer, and testing
- dig - command used for querying DNS servers to get information about domain names, IP addresses, and more.
- pathping - combines the features of ping and tracert
- hping - used for security auditing and testing of firewalls and networks

- chmod - sets permissions of files or directories

STP frame (Spanning Tree Protocol) - a network protocol used to prevent loops in Ethernet networks

MTU (Maximum Transmission Unit) - the maximum size of a data packet that can be transmitted over a network protocol without fragmentation

BPDU (Bridge Protocol Data Unit) - unit of communication in STP protocol

Jump server - a dedicated system used as an access point for connecting and managing other systems in a network

NAT (Network Address Translation) - process for translating IP address between different network domains, Layer 3, used to overcome IPv4 limitations by allowing multiple devices with private IP address to share a single public IP address

Geofencing - technology that allows the creation of virtual boundaries around real-world geographic areas

OTG (On-the-go) - enables direct USB connection between devices

IdP (Identity Provider) - manages the authentication and authorization process for users within a network

KBA (Knowledge-Based Authentication)

GPO (Group Policy Object) - Windows group policy settings that defines what a system looks like and how it behaves to a group of users

Syslog - centralized log management system

Nessus - vulnerability scanning tool that helps identify vulnerabilities, and take appropriate actions to mitigate them

## Port numbers

1. FTP (File Transfer Protocol): 20 (data), 21 (control)
2. SSH (Secure Shell): 22
3. Telnet: 23
4. SMTP (Simple Mail Transfer Protocol): 25
5. DNS (Domain Name System): 53
6. DHCP (Dynamic Host Configuration Protocol): 67 (server), 68 (client)
7. HTTP (Hypertext Transfer Protocol): 80
8. HTTPS (Hypertext Transfer Protocol Secure): 443
9. RDP (Remote Desktop Protocol): 3389
10. SNMP (Simple Network Management Protocol): 161 (SNMP agent), 162 (SNMP manager)
11. NTP (Network Time Protocol): 123
12. LDAP (Lightweight Directory Access Protocol): 389
13. IMAP (Internet Message Access Protocol): 143
14. POP3 (Post Office Protocol version 3): 110
15. SMB (Server Message Block): 445
16. AFP (Apple Filing Protocol): 548
17. RADIUS (Remote Authentication Dial-In User Service): 1812 (authentication), 1813 (accounting)
18. SIP (Session Initiation Protocol): 5060 (TCP/UDP)

19. FTPS (FTP Secure): 990
20. TFTP (Trivial File Transfer Protocol): 69