PORTS

PORT #	FULL NAME	DESCRIPTION
0-1023	System Ports	
1024-49151	User Ports	
49152-65535	Dynamic and/or Private Ports	
TCP 20	FTP (File Transfer Protocol) - Data Channel	Unsecure
TCP 21	FTP - Control Channel	Unsecure
TCP 21	FTPS	Using TLS (TCP 21 in explicit mode and 990 in implicit mode)
TCP 22	SSH	Secure AF (unless you mishandle keys/passwords)
TCP 23	Telnet	Unsecure
TCP 25	SMTP (Simple Mail Transfer Protocol), sending email	Unsecured, unencrypted. Use Port 587 instead
UDP/TCP 53	DNS	Unsecure, succumbs to DDoS
UDP/TCP 53	DNSSEC	Provides integrity not confidentiality via digital signatures
TCP 80	HTTP	Unsecure, unencrypted
UDP/TCP 110	POP3 (Post Office Protocol Version 3)	First port for sending email. Unsecure, unencrypted, use 995 instead
TCP 143	IMAP (Internet Message Access Protocol)	Send email and more features than POP3 but still unencrypted and unsecured. Use Port 993 instead
UDP/TCP 161	SNMP (Simple Network Management Protocol)	Used for network management, unsecured. SNMPv3 is secure but not by much
TCP 443	HTTPS (Hypertext Transfer Protocol Secure)	Secure and encrypts data between the user's browser and website via TLS
TCP 445	SMB (Server Message Block)	Microsoft's networking port. Should not be open to the public. Allows sharing files and printers over the network. Blocking will prevent file and printer sharing
UDP/TCP 515	LPD (Line Printer Daemon)	Printing port, unsecured
TCP 548	AFP (Apple Filing Protocol)	AppleShare, Personal File Sharing, File services via a networked connection, unsecured - no UN or PWs
TCP 636	LDAPS (Secure Lightweight Directory Access Protocol)	TLS-protected version of LDAP (Lightweight Directory Access Protocol, previously Port 389)
TCP 777	multiling-http	Trojans use this port
TCP 989	FTPS (Implicit) - Data Channel	
TCP 990	FTPS (Implicit) - Control Channel	
TCP 1433	SQL	Microsoft's SQL server, needs to be secured
UDP/TCP 1443	Integrated Engineering Software	
TCP 3389	RDP (Remote Desktop Protocol)	Microsoft's RDP, officially listed as Windows-Based Terminal (WBT)
TCP 5000	UPnP (Universal Plug-in-Play)	Permits networked devices (Computers, printers, Wi-Fi access points) to discover each other's presence and establish a connection
UDP 5004	SRTP (Secure Real-Time Protocol)	Provides audio and video streams via network. A secure alternative to RTP
TCP 5223	Apple's Push Notification Service	Officially listed as "HP Virtual Machine Group Management"

LINUX COMMANDS

COMMAND	FULL NAME	DESCRIPTION
chmod	Change mode	Allows users to change the permissions of files and directories. Syntax: chmod <Operations> <File/Directory Name>
u	user	Grant permission to a user
g	group	grant permission to a group
o	others	grant permissions to others (not in u or g)
r	read	grants read permissions
w	write	grant write permission
x	execute	grant execute permission
+' or '-' operator		indicates adding or removing permissions. example: chmod +r sample.txt --> adds read permissions to the sample.txt file
chown	Change file ownership	
chgrp	Change group ownership	
chroot	Changes root	
ls	List	Lists a directory's content
ln	link	creates a ink to a file
ps	Process Status	report a snapshot of the current processes
date	Prints or sets the system date and time	
pwd	Print Working Directory	Shows the current working directory's path
cd	Change directory	Change the shell working directory
time	time	Report time consumed by pipeline's execution
times	times	display process times
cp	Copy	Copies a file or directory
mv	Move	Moves files or directories from one directory to another
rm	remove	Removes (deletes) files, directories, device nodes and symbolic links
dd	Data duplicator	Copies and converts a file
if	Input file	Specifies the source of data to be copied
of	Output file	Specifies the destination where the output file will be recorded to
cat	Concatenate (to merge things together)	Display file contents on the terminal
ExifTool	Exchangeable Image File Format	Reads metadata for multimedia files
touch	change file timestamps	
locate	Finds files by name	Find a file in the database
uname	Prints system information	Get basic information about the OS
mkdir	Make directory	
rmdir	Remove directory	
sudo	Superuser	Execute commands with administrative privileges
su	Switch user	allows to run commands with a substitute user and group ID
groups	prints groups	Prints the groups of which the user is a member
cksum	Checksums and count the bytes in a file	checksum and count the bytes in a file

CHMOD LINUX COMMANDS

NUMERIC REPRESENTATION	PERMISSION	LETTER REPRESENTATION
0	No permission	- - -
1	Execute	- - x
2	Write	-w-
3	Execute + Write	-wx
4	Read	r--
5	Read + Execute	r-x
6	Read + Write	rw-
7	Read + Write + Execute	rwx

IEEE 802 STANDARDS

STANDARD	FULL NAME	DESCRIPTION
IEEE 802		Collection of networking standards that cover physical and data link layer specifications for technologies such as Ethernet and wireless
802.1X	WPA-2, Standard for NAC	Port-based NAC for wired/wireless networks, RADIUS validates the user
802.1D	Spanning Tree Protocol (STP)	Ethernet MAC bridges standard which includes bridging, Spanning Tree Protocol and others. Loop protection mechanism
802.1Q	Dot1Q	Supports VLAN on IEEE 802.3 Ethernet network
802.11	-	Collection of Wireless LAN & Mesh Wi-Fi
802.11b	Wi-Fi 1	11 Mbit/s, 2.4 GHz
802.11a	Wi-Fi 2	54 Mbit/s, 5 GHz
802.11g	Wi-Fi 3	54 Mbit/s, 2.4 GHz
802.11n	Wi-Fi 4	600 Mbit/s, 2.4 GHz and 5 GHz
802.11ac	Wi-Fi 5	6.9 Gbit/s, 5 GHz
802.11ax	Wi-Fi 6 and Wi-Fi 6E	9.6 Gbit/s, 2.4 GHz, 5 GHz, 6 GHz
802.11be	Wi-Fi 7	Extremely High Throughput (EHT), 40+ Gbit/s, 2.4 GHz, 5 GHz, 6 GHz (adopted 2024)
802.11bn	Wi-Fi 8	Ultra High Reliability (UHR), 100,000 Mbit/s (adopted 2028)
802.15.1	WPAN/Bluetooth	
802.3	Wired Ethernet	Collection of standards defining physical layer and data link layer's MAC of wired Ethernet

CHAPTER 1: TODAY'S SECURITY PROFESSIONAL

ACRONYM	FULL NAME	DESCRIPTION
CIA Triad	Confidentiality, Integrity, Availability (and nonrepudiation)	Describes what cybersecurity professionals seek to continuously protect
DAD Triad	Disclosure, alteration, denial	Describes what threat actors seek
	Confidentiality	Unauthorized individuals are not able to gain access to sensitive info
	Integrity	Ensuring no unauthorized modifications of data
	Availability	Data/systems are readily available
	Nonrepudiation	Digital signature, cannot deny it was sent from you
	Disclosure	Data loss or data exfiltration. The opposite of confidentiality
	Alteration	Unauthorized modification of data. Opposite of integrity
	Denial	Disruption of authorized users to access data. Opposite of availability
	Control objectives	Desired security state
	Security controls	Specific measures to achieve control objectives
	Gap analysis	Examining security controls VS control objectives
	Technical controls	Firewall rules, access control lists, IPS, and encryption
	Operational controls (AKA processes)	Access reviews, log monitoring, vulnerability management
	Managerial control (AKA risk management)	Risk assessments, securing planning exercises, change management
	Physical controls	Fences, lighting, locks, fire suppression, alarms
DLP	Data loss prevention	Via pattern matching, watermarking, or DRM
Agentless (network-based) DLP		Dedicated devices on a network that blocks traffic and auto-applies encryption
DRM	Digital Rights Management	Enforce copyright and data ownership
	Deidentification	Removing the ability to link data back to an identity
	Segmentation	Placing sensitive systems on separate networks
	Isolate	Cutting systems off from access
TLS	Transport Layer Security	cryptographic protocol designed to provide communications security over a computer network
SSL	Secure Sockets Layer	It used the same cryptographic keys for message authentication and encryption
SMTP		an Internet standard communication protocol for electronic mail transmission
PGP	Pretty Good Privacy	popular program used to encrypt and decrypt email over the internet, as well as authenticate messages with digital signatures and encrypted stored files
GPG	Gnu Privacy Guard	a free-software replacement for Symantec's PGP cryptographic software suite
	Gnu Project	a free software, mass collaboration project announced by Richard Stallman on September 27, 1983. Its goal is to give computer users freedom and control in their use of their computers and computing devices by collaboratively developing and publishing software that gives everyone the rights to freely run the software, copy and distribute it, study it, and modify it
SMTPS	Simple Mail Transfer Protocol Suite	It is a way to secure SMTP at the transport layer, by wrapping SMTP inside Transport Layer Security (TLS). Conceptually, it is similar to how HTTPS wraps HTTP inside TLS.
FTP	File Transfer Protocol	network protocol for transmitting files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections. Within the TCP/IP suite, FTP is considered an application layer protocol.
SFTP	Secure File Transfer Protocol	Secure File Transfer Protocol (SFTP) is a network protocol for securely accessing, transferring and managing large files and sensitive data. Designed by the Internet Engineering Task Force as an extension of Secure Shell (SSH), SFTP enables access, transfer and management of files over a network.
SCP	Supply Chain Planning	Supply chain planning (SCP) is the process of anticipating the demand for products and planning their materials and components, production, marketing, distribution and sale. Its overall goal is to balance supply and demand, so sales revenue opportunities are fully exploited in a timely manner and at the
WMIC	Windows Management Instrumentation Command-line	The Windows command wmic extends WMI for operation from several command-line interfaces and through batch scripts without having to rely on any other programming language. The command wmic uses class aliases to query related information.
TCP/IP	Transmission Control Protocol/Internet Protocol	The suite of communications protocols (the main ones being TCP and IP) used to connect hosts on the Internet. TCP/IP is used by the Internet, making it the de facto most widely spread standard for transmitting data over networks. TCP and IP were developed by a DOD (Department of Defense) research project to connect a number different networks designed by different vendors into a network of networks (the Internet).
UDP	User Datagram Protocol	communications protocol, an alternative to TCP (Transmission Control Protocol), and uses the Internet Protocol (IP) to actually get a data units (datagrams) from one network node to another. UDP does not provide the service of dividing a message into packets (unlike TCP) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in.
SCTP	Stream Control Transmission Protocol (AKA "next gen TCP")	a computer networking Transport Layer protocol, serving in a similar role as the popular TCP/UDP protocols. It provides some of the same service features of both, ensuring reliable, in-sequence transport of messages with congestion control. Sometimes referred to as "next generation TCP", SCTP is designed to make it easier to support a telephone connection over the Internet (and specifically to support the telephone system's Signaling System 7 (SS7) on Internet connection). SCTP was defined in 2000 by the IETF Signaling Transport (SIGTRAN) working group in RFC 4960 (RFC 3286 provides an introduction). Defined by RFC 2960 originally, obsoleted by RFC 4960.

CHAPTER 2: CYBERSECURITY THREAT LANDSCAPE

ACRONYM	FULL NAME	DESCRIPTION
	Black Hat	Unauthorized

	Black Hat Briefings	Black Hat Briefings is a computer security conference that provides security consulting, training, and briefings to hackers, corporations, and government agencies around the world.
	Gray Hat	Semi-authorized
	White Hat	Authorized
	Red Hat	Red Hat, Inc. is an American software company that provides open source software products to enterprises and is a subsidiary of IBM. Founded in 1993, Red Hat has its corporate headquarters in Raleigh, North Carolina, with other offices worldwide
	Script Kiddie	Unskilled attacker
	Hacktivist	Ex: Anonymous
	Organized Crime	Ransomware, child sexual abuse material, online fraud, dark web
	Shadow IT	Unapproved IT tech
APT	Advanced Persistent Threat	Usually, nations state attackers
OSINT	Open Source Intelligence	
OWASP	Open Worldwide Application Security Project	hosts community-developed standards/best guides
CISA	Cybersecurity and infrastructure security agency	Founded 2018, "We connect our stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people"
NSA	National Security Agency	
NIST	National Institute of Standards and Technology	Provides standards for many products and standards, makes the NVD
CIS	Center for Internet Security	US 501 nonprofit organization, formed in October 2000. Its mission statement professes that the function of CIS is to " help people, businesses, and governments protect themselves against pervasive cyber threats
IEEE	Institute of Electrical and Electronics Engineers	The Institute of Electrical and Electronics Engineers is an American 501 professional association for electronics engineering, electrical engineering, and other related disciplines. The IEEE has a corporate office in New York City and an operations center in Piscataway, New Jersey.
IETF	Internet Engineering Task Force	The Internet Engineering Task Force is a standards organization for the Internet and is responsible for the technical standards that make up the Internet protocol suite. It has no formal membership roster or requirements and all its participants are volunteers
ISACA	Information Systems Audit and Control Association	Global non-profit to help IT professional audit, cybersecurity, and emerging tech (via certs, publications, etc)
OASIS	Organization for the Advancement of Structured Information Protocol	OASIS Cyber Threat Intelligence (CTI) TC, non-profit that maintains XML & HTML
AIS	Automated Indicator Sharing	?
WHOIS	WHOIS lookup AKA Domain Namelookup	Developed by CISA, DNS lookup gets the IP, WHOIS or Domain Name lookup gets the name
IoC	Indicators of Compromise	Red flags: file signatures, log patterns, file and code repositories
	Threat maps	Geographic view of threat intelligence (unreliable)
STIX	Structured Threat Information of eXpression	XML language describing the attack in a STIX JSON
TAXII	Trusted Automated eXchange of Intelligence Information protocol	Method of transport for STIX, communication via HTTPS
ISAC	Information Sharing and Analysis Center	
RFC	Requests for Comment	Official specification for a technology
TTP	Tactics, techniques, and procedures	
ATT&CK	Adverbial Tactics, Techniques, and Common Knowledge	Developed MITRE, Modern way of looking at cyberattacks
MITRE	The MITRE Corporation	MITRE is a government-funded research organization that provides technical and engineering guidance to the United States Air Force. It was spun off from MIT in 1958, but the name is not an acronym
HTTPS	Hypertext Transport Protocol Secure	
XML	Extensible Markup Language	Allows different apps to exchange and store data in a universal way
HTML	Hypertext Markup Language (current is 5)	Language of the web for displaying content

CHAPTER 3: MALICIOUS CODE

ACRONYM	FULL NAME	DESCRIPTION
	Ransomware	Holding data for ransom
	Trojan	Disguised as legitimate software
	Worm	Self-replicating
	Virus	Requires infection mechanisms and host programs to spread themselves
	Spyware	Stalkerware, associated with identity fraud
	Bloatware	Not necessarily harmful, more applications than you need
PUP	Potentially Unwanted Program	AKA Bloatware
	Honeypot	a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems
	Honeynet	A honeynet is a network set up with intentional vulnerabilities hosted on a decoy server to attract hackers
	Honeyfile	Trap file, prevents ransomeware
	Honeytoken	fictitious words or records that are added to legitimate databases. They allow administrators to track data in situations they wouldn't normally be able to track, such as cloud-based networks. If data is stolen, honey tokens allow administrators to identify who it was stolen from or how it was leaked
	Keylogger	Keeps track of keystrokes and send it to an attacker via C&C (command-and-control) server
	Rootkit	Infects the MBR
	Logic bomb	Malicious code that activates when conditions are met
	Botnet	Network of computer that are infected with malware and controlled by an attacker. Usually for DDoS attacks. Utilizes routers, C&C, HTTP or IRC

CHAPTER 4: SOCIAL ENGINEERING AND PASSWORD ATTACKS

ACRONYM	FULL NAME	DESCRIPTION
	Phising	Fraudulent acquisition of information
	Spear phishing	Targeted phishing
	Whaling	Targeting high-earners/high-rankers
	Vishing, Smishing	Voice and SMS based phishing
BEC	Business Email Compromise	Compromised accounts, spoofed email, typo squatting domain, malware
	Pretexting	Made-up scenario to justify
	Pharming	Redirects victim to lookalike site by attacking system's host file
TRUST	Tell your story, ready your team, Understand and assess MDM, Strategize response, track outcomes	CISA's model for countering phishing
ZTTM 2.0	Zero Trust Maturity Model Version 2.0	The maturity model aims to assist agencies in the development of zero trust strategies and implementation plans and to present ways in which various CISA services can support zero trust solutions across agencies.
	Rainbow table attacks	Creating a hash collision (AKA birthday attack)
	Password spraying	One password, many accounts
	Dictionary attacks	A form of brute force attacks, using list of words for attacks (ex: tool name John The Ripper does this)
JtR	John The Ripper	Helps crack passwords

CHAPTER 5: SECURITY ASSESSMENT AND TESTING

ACRONYM	FULL NAME	DESCRIPTION
NVD	National Vulnerability Database	Lists all of the CVEs

SCAP	Security Content Automation Protocol	Standardized communication approach for security info (created by NIST)
CCE	Common Configuration Enumeration	Systems and configurations issues
CPE	Common Platform Enumeration	Product names and versions
CVE	Common Vulnerability & Exposures	Security flaws
CVSS	Common Vulnerability Scoring System	Measuring and describing severity. 0.1-3.9 (low), 4.0-6.9 (medium), 7.0-8.9 (high), 9.0-10.0 (critical)
XCCDF	Extensible Configuration Checklist Description Format	Reporting checklist results
OVAL	Open Vulnerability and Assessment Language	International community that promotes open and publicly available security content. Taken over by CIS
ASV	Approved Scanning Vendor	Examples: Nessus, Qualys, Rapid7's Expose, OpenVAS
	Static Testing	Analyzing code without executing it
	Dynamic Testing	Executes code as part of test
	Interactive Testing	Combines static and dynamic testing
	Fuzz testing (AKA fuzzing)	Testing codes ability to handle random data
SIEM	Security Incident and Event Management	The main dashboard and tool SOC teams use
SOC	Security Operations Center	
SOAR	Security Orchestration, Automation, and Response	Automating responses, learn of emerging threats, scans.
	Pen Testing	White hat hacker, first-hand knowledge, constructive feedback, focused information on specific attack targets
	Threat Hunting	Looking for attacks hiding in secret
RoE	Rules of Engagement	Defining permitted scope in
	Responsible Disclosure Programs	Bug bounty programs
	Security Assessments	Comprehensive review of a system's security (internal use only)
	Security Audit	Independent authors (potentially public)
	Security Attestation Letter	Formal state that proves the safety and security of a system
COBIT	Control Objectives for Information and related Technologies	Used to develop, implement, monitor, and improve IT structures. Maintained by ISACA

CHAPTER 6: APPLICATION SECURITY

ACRONYM	FULL NAME	DESCRIPTION
SDLC	Software development lifecycle	1-Planning, 2-Requirements, 3-Design, 4-Coding, 5-Testing, 6-Training and Transition, 7-Ongoing Operations, 8-End of Life/Decommissioning
UAT	User acceptance testing (end user)	
	Staging	Transition environment
QA	Quality Assurance (during manufacturing)	Test environment
	DevOps	Software development + IT operations
	DevSecOps	Software development + security + IT operations
CI/CD	Continuous Integration/Continuous Deployment (or Delivery)	Consistently checking code, monitoring
API	Application Programmable Interface	Relies on rate limiting, inputting filtering, appropriate monitoring
	Injection Vulnerabilities	Primary attack for web applications
	Blind SQL Attacks	Asking data database true or false questions
LDAP	Lightweight directory access protocol	Vendor-netural software protocol used to lookup information or devices within a network, supports C and C++
DLL	Dynamic-link library	A DLL is a library that contains code and data that can be used by more than one program at the same time in Windows OS
XSS	Cross-Site Scripting	Web injection attack which malicious scripts are injected into a website. Executes when the victim loads the website
	Non-persistent/Reflected XSS (Type 1 XSS)	Injecting HTML code into error message and the website unknowingly spits it right back
	Stored/Persistent XSS (Type 2 XSS)	Waiting for the site to interact with malicious code (ex: leaving malicious HTML code in blog comments)
	Blind Cross-site Scripting	A form of persistent XSS, sending a hidden payload that collect victims info like cookies, credentials. Hard to confirm but can be done via XSS Hunter
	XSS Hunter	Open source service to find XSS
DOM	Document object model	connects web pages to scripts or programming languages by representing the structure of the document
	DOM-based XSS	Attacker injects a script into a response, written deep in JS code, look for eval() method
	Session Hijacking	Taking over control of a user's web session
	Cookies Theft (AKA cookie hijacking, stealing)	Stealing user's cookie data to access user's accounts
	Session Replay Attack	Attack replays the website's session as the user
NTLM	Windows New Technology LAN Manager	Verifies user's identities and protects confidentiality, integrity
	NTLM pass-the-hash attack	Steals hash and tries to unlock stuff with it, doesn't require the attacker to gain any credentials
IDOR	Insecure Direct Object Reference	When a web app provides direct access to something by modifying the URL (ex: changing the end to 123, 124, 125)
	Directory Traversal (AKA path traversal)	Navigating somewhere else on directory paths (ex: using the ".." In header
CSRF/XSRF	Cross-Site Request Forgery (AKA Sea Surf, Session Riding)	Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website or web application where unauthorized commands are submitted from a user that the web application trusts
SSRF	Server-side request forgery	Tricking a server to visit a URL based on user-supplied input. Possible when web app accepts URLs as input
WAF	Web Application Firewall	Firewall specific to the application layer (OSI L7), sits in front of web server, performs input validation
	Parameters Queries	Sends parameters and not code to databases to prevent injection
	Sandboxing	Controlled test environments
SDK	Software Development Kits	Set of platform-specific building tools for developers
SPOF	Single Point of Failure	
	Scalability	Support demand as needed
	Elasticity	Provision/deprovision resources automatically
	Buffer Overflows	Placing more data into memory are than it can handle
ASLR	Address Space Layout Randomization	memory protection process for OSes that guards against buffer-overflow attacks by randomizing location for executables
PAP	Password Authentication Protocol	password-based authentication protocol used by Point-to-Point Protocol to validate users. PAP is specified in RFC 1334. Almost all network operating systems support PPP with PAP, as do most network access servers. PAP is also used in PPPoE, for authenticating DSL users.
TOC	Time-of-Check	Instance when the system verifies permissions
TOU	Time-of-Use	The moment when system accesses the resource
TOE	Time of Evaluation	Being evaluated for potential vulnerabilities
TOC/TOU	Time of check to time of use	If someone is logged on already and permission is removed…well too bad. They have that resource forever

CHAPTER 7: CRYPTOGRAPHY AND PKI

ACRONYM	FULL NAME	DESCRIPTION
	Encryption	Plaintext → cipher text via encryption key
	Decryption	Cipher text → plaintext via decryption key
	Substitution cipher	Cipher that substitutes one character for another (ex: Julius Caesar's letters)
	Polygraphic Substitution	Shifting letters around even more
	Vigenere Cipher	Keyword to lookup cipher text
	Transposition Ciphers	Scrambling letters in a certain manner
	Steganography	Art of using cryptographic techniques to obscure secret messages in another file
BIOS	Basic Input/Output System	also known as the System BIOS, ROM BIOS, BIOS ROM or PC BIOS) is firmware used to provide runtime services for operating systems and programs and to perform hardware initialization during the booting process (power-on startup).
MBR	Master boot record	contains executable code to function as a loader for the installed operating system
FDE	Full disk encryption	All files on a hard drive are automatically encrypted, except the MBR

EFS	Encryption File System	provides an added layer of protection by encrypting files or folders on various versions of the Microsoft Windows OS
(Amazon) EFS	Amazon Elastic File System	provides flexible storage capacity that scales to accommodate workloads that run on AWS Elastic Compute Cloud (EC2) instances and access files through application programming interface (API) requests.
NTFS	New Technology File System	the file system that the Windows NT operating system (OS) uses for storing and retrieving files on hard disk drives (HDDs) and solid-state drives (SSDs)
SED	Self-Encrypting Drives	type of hard drive that automatically and continuously encrypts the data on the drive without any user interaction
	File-level encryption	Individual files are encrypted
	Volume encryption	Volume on a storage device
IV	Initialization Vector	An initialization vector (IV) or starting variable (SV)[5] is a block of bits that is used by several modes to randomize the encryption and hence to produce distinct ciphertexts even if the same plaintext is encrypted multiple times, without the need for a slower re-keying process.
CBC	Cipher Block Chaining	In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol	uses AES to provide confidentiality. Provides authentication for user and access control capabilities
ECB	Electronic Code Book	Simplest encryption methods, The message is divided into blocks, and each block is encrypted separately.
CFB	Cipher Feeback	The cipher feedback (CFB) mode, in its simplest form uses the entire output of the block cipher. In this variation, it is very similar to CBC, turning a block cipher into a self-synchronizing stream cipher
P	Plaintext	
C	Cipher Text	
	Key Space	range of values that are valid for the key to use for an algorithm AKA all the possibilities
	Key Length	number of binary bits in the key
	Cryptovariables	Another term for cryptographic keys
	Cryptography	Creating and implementing secret codes and ciphers
	Cryptoanalysis	The study of methods to defeat codes and ciphers
	Cryptology	Cryptoanalysis + cryptography
	Cryptosystems	Specific implementation of code or cipher in software
	Cipher suites	Sets of ciphers and key lengths to support a system
	Kerckhoff's Principle/assumption	the enemy knows the system (not security through obscurity)
	Block ciphers	Apply encryption algorithm
	Stream ciphers	One character or a bit at a time (ex: Caesar's cipher)
DES	Data Encryption Standard	56-bit key created decades ago (insecure)
AES	Advanced Encryption Standards	For symmetric keys, current version is 256 bit
	Symmetric Key Algorithms	AKA Secret key cryptography or private key cryptography. The number of keys is calculated by: (n (n-1)) / 2
	Asymmetric Key Algorithms	Public and private key algorithms. Number of keys needed is always 2X the number of users
DH	Diffie-Hellman	Key exchange algorithm
DSA	Digital Signature Algorithm	a public-key cryptosystem and Federal Information Processing Standard for digital signatures, based on the mathematical concept of modular exponentiation and the discrete logarithm problem
KEM	Key Encapsulation Mechanism	used to secure symmetric key material for transmission using asymmetric (public-key) algorithms. It is commonly used in hybrid cryptosystems
RSA		A public-key signature algorithm developed in 1977
ECC	Elliptic Curve Cryptography	Less computation and power than RSA. Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller and more efficient cryptographic keys. ECC is an alternative to the Rivest-Shamir-Adleman (RSA) cryptographic algorithm and is most often used for digital signatures in cryptocurrencies, such as Bitcoin and Ethereum, as well as one-way encryption of emails, data and software.ECC offers several benefits compared to RSA: It operates on devices with low CPU and memory resources. It encrypts and decrypts faster. Larger key sizes can be used without significantly increasing the key size or CPU and memory requirements.
ECDHE	Elliptic Curve Diffie-Hellman Key Exchange	a key agreement protocol that allows two parties, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel
ECDSA	Elliptic Curve Digital Signature Algorithm	offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic-curve cryptography.
SHA	Secure Hash Algorithm	SHA-1, SHA-2, SHA-3 (current)
KEK	Key Encryption Key	Key that encrypts another key
RC4	Rivest Cipher 4	In cryptography, RC4 (Rivest Cipher 4, also known as ARC4 or ARCFOUR, meaning Alleged RC4, see below) is a stream cipher. While it is remarkable for its simplicity and speed in software, multiple vulnerabilities have been discovered in RC4, rendering it insecure.
SHS	Secure Hash Standard	AKA FIPS 180, created by NIST
MD5	Message-Digest Algorithm	public key
	Digital Signatures	Enforce non-repudiation & integrity
HMAC	Hash-Based Message Authentication Code	Partial digital signature → guarantees integrity but not non-repudiation
PKI	Public Key Infrastructure	the underlying framework that enables entities -- users and servers -- to securely exchange information using digital certificates
	Key Escrow	a mechanism that allows authorized parties to access the encryption keys of a system or device in the event that the owner is unable to do so
	public key	AKA Asymmetric key cryptography
	private key	AKA Symmetric key cryptography
CA	Certificate Authority	Issues digital certificates to provide assurance people are who they claim to be
X.509	X.509 Standard (V3)	The current standard for digital certificates
SAN	Subject Alternative Name	A Subject Alternative Name (SAN) is a field in an X.509 certificate that identifies domain names, IP addresses, email addresses, URIs, or UPNs. SANs are used to specify additional hostnames for individual SSL certificates. They are a common practice for SSL certificates and are replacing common names.
	Wildcard Certificate	Designated by the "*" sign, applies to only ONE level of subdomain
RA	Registration Authorities	Help CAs verify identities before digital signing
	Root CAs	Protected by offline CA (like proxy servers)
CSR	Certificate Signing Request	Providing CA with your public key to initiate the CSR
DV	Domain Validation Certificate	CA verifies use subject has control over the domain name
EV	Extended Validation	Higher level of assurance, more security steps for CA
CRLs	Certification Revocation Lists	Newly revoked certificates
OCSP	Online Certification Status Protocol	Faster and real-time verification
DER	Distinguished encoding rules	Binary file stored in .der, .crt, .cer
PEM	Privacy Enhanced Mail	Text-version of DER format. Stored in .pem, or .crt extension
PFX	Personal Information Exchange	password protected file certificate commonly used for code signing your application, Windows systems using .pfx or .p12 file
	Salting	Adding random generated values to each password prior to hashing
	Key Stretching	Housing of iterations of salting and hashing
WEP	Wireless Equivalent Privacy	Uses RC4 encryption algorithm, very insecure

CHAPTER 8: IDENTITY AND ACCESS MANAGEMENT

ACRONYM	FULL NAME	DESCRIPTION
AAA	Authentication, Authorization, and Accounting	Device authentication methods: digital certificate, IP addresses, and MAC addresses. People authentication methods: UN/PW, Biometrics, MFA. TACACS+ and RADIUS also provide AAA functionality
	Traits	Inherent to subject (hair, skin, eye color)
	Attributes	Can be changeable things, like title or address
SSO	Single sign-on	Authentication protocol
OAuth	Open Authorization	Opn standard for authorizing websites via SSO (ex: web conferencing tools using google calendar). Handles authorization of access to protected resources
CHAP	Challenge Handshake Authentication Protocol	Encrypted challenge + 3-way handshake
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol	

802.1X	IEEE Standard for NAC	The IEEE 802.1X standard provides a network access framework for managing wireless LAN usage. But 802.1X is merely an envelope that carries some type of Extensible Authentication Protocol.
NAC	Network Access Control	the process of restricting unauthorized users and devices from gaining access to a corporate or private network.
RADIUS	Remote Authentication Dial-In User Service	Most common AAA systems of networks, system, etc. Sends passwords via shared secret and MD5 hashed passwords
TACACS+	Terminal Access Controller Access Control System Plus	Provides AAA via TCP, allows for individual commands. Designed by Cisco
	Kerberos	Authentication service ticketing request system for between hosts and untrusted networks
SAML	Security Assertion Markup Languages	XML-based open standard for exchanging authentication and authorizing information, used for identity providers
OpenID		Open standard for decentralized authentication (ex: sign in with Google)
IdP	OpenID Identity Providers	Google, Facebook, Amazon, etc
RP	Relying Parties	Redirect it to the IdPs
	Federation	Group of trusted IdPs relaying information. Many CSPs use this
	Principal	User in federation
CSP	Cloud Service Provider	a company that offers components of cloud computing -- typically, infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS).
SP	Service Provider (in Federation)	Provides services to IdPs who have been attested to
	Security Key	Hardware devices
FIDO (1.0)	Fast Identity Online	FIDO Alliance, promoting passkeys instead of passwords
FIDO2		FIDO vs FIDO2 FIDO2 is a more comprehensive and standardized protocol that is supported by all leading browsers and operating systems, including Android, IOS, MacOS and Windows.
CTAP	Client to Authenticator Protocol	Client To Authenticator Protocol (CTAP) is a specification describing how an application (i.e. browser) and operating system establish communications with a compliant authentication device over USB, NFC or BLE communication mediums. The specification is part of the FIDO2 project and W3C WebAuthN specification.
MFA	Multi-Factor Authentication	Something you have, something you are, something you know
OTP	One Time Password	Makes brute force harder, dynamically made
TOTP	Time-based One Time Password	uses algorithms to derive an OTP and then moves on (ex: Authenticator app)
HMAC	Hash-based message authentication codes	
HTOP	HMAC One Time Passwords	generate code token from last known token (ex: SMS code. Susceptible to SIM cloning)
	Static Codes	algorithmically generated, stored in a secure location, but can be compromised
	Biometrics	something you are (physiology) like fingerprints, retina scans, facial recognition, voice recognition, vein recognition, gait analysis (how a person walks)
FRR	False Rejection Rate	FIDO sets their standard for 3% of attempts
FAR	False Acceptance Rate	FIDO sets their standards at 0.01% for FAR
ROC	Receiver Operating Characteristic	The ROC curve can be used to visualize the difference between normal and abnormal test results. It connects points with 1 - specificity (false positive rate) on the x-axis and sensitivity on the y-axis
IAMPR	Imposter Attacker Presentation Match Rate	a metric used in a full-system evaluation
PAM	Privileged Access Management	Tools for ensuring least privilege
JIT	Just-in-time permissions	Permissions granted and revoked when needed
	Password vaulting	Access privileged accounts without knowing the password
	Ephemeral accounts	one-time accounts created on the fly, which are immediately deprovisioned or deleted after use
BASH	Bourne-Again Shell	a Unix shell and command language written by Brian Fox for the GNU Project as a free software replacement for the Bourne shell.[15][16] The shell's name is an acronym for Bourne-Again SHell, a pun on the name of the Bourne shell that it replaces[17] and the notion of being "born again".
CAPTCHA	Completely Automated Turing Test to Tell Computers and Humans Apart	a type of challenge–response test used in computing to determine whether the user is human in order to deter bot attacks and spam.
MAC	Mandatory access controls	OS sets security policy, users cannot change security settings (rare setting, ex: SELinux)
DAC	Discretionary Access Control	More common, access control scheme to control home PCs (ex: Linux file permissions)
RBAC	ROLE-Based Access Control	Roles are matched with privileges, popular with enterprises, dynamic and good for ZTA
RuBAC	RULE-Based Access Control	Set of rules that apply to various objects or resources (ex: firewall ruleset). It is not as dynamic as RBAC
ABAC	Attribute-based Access Control	Policies that are driven by the attributes of the users. Complex to manage

CHAPTER 9: RESILIENCE AND PHYSICAL SECURITY

ACRONYM	FULL NAME	DESCRIPTION
UPS	Uninterruptible Power Supply	Immediate power backup in case of a power outage, not a long-term solution
PDU	Managed Power Distribution Units	Intelligent & remote power management
RAID	Redundant Array of Independent Disks	
RAID 0	Striping	Pros: Exceptional performance due to parallel data access, cost-effective. Cons: 0 redundancy or fault tolerance.
RAID 1	Mirroring	When one drive fails, the other recovers. High reliability, easy setup, fast read performance. But reduced capacity, higher cost
RAID 5	Parity	Pros: Balance between RAID 0 and RAID 1. Efficient storage capacity can withstand the loss of a single drive. Cons: performance is impacted a bit, may fail during rebuild performance
RAID 6		Pros: offers higher fault tolerance than RAID 5. Cons: write performance is impacted
RAID 10	AKA RAID 1+0	Minimum of four disks, both mirrored and stripped. Pros: good performance, fault tolerance, and fast rebuild times. Cons: large # of drives, reduced useable capacity & scalability
RPO	Recovery Point Objective	How much data loss is acceptable
RTO	Recovery Time Objective	How long the recovery can take
	Full Backup	Copies the entire device or storage system
	Differential Backup	All the data that has changed since the last FULL BACKUP
	Incremental Backup	Captures changes since last incremental backup. Pro: fast to recover. Con: slow to backup
	Replication	Synchronous (real-time) or asynchronous (after-the-fact) methods of copying data
	Journaling	Creates a log of changes that can reply if an issue occurs → restoring to a fixed snapshot. Con: The journal also needs to be stored somewhere
	Snapshot	Captures the full state of a system when the backup is completed (common for VMs). Pro: captured live. Con: consumes a lot of storage
	Images	Complete copy of a server or drive down to the bit. Backup method of choice for complex servers
	Gold Master Image	Best and final version of a VDI (virtual desktop infrastructure)
NAS	Network-Attached Storage	
SAN	Storage Area Network	Multiple computers or servers
C2	Command & Control Servers	C2 servers facilitate data exfiltration by instructing the compromised device to send specific data to the server. This data can include stolen credentials, sensitive documents, or other valuable information.
HDD	Hard Disk Drives	
SSD	Solid State Drive	
	Nearline Backups	Not immediately available but can be retrieved. Pro: faster than offsite. Con: slower than onsite. (ex: Amazon's S3, Google's Coldline storage)
DRP	Disaster Recovery Planning	
	Nonpersistance	Ability to have systems or services that are spun up and shut down as needed
	Hot site	Operated full-time
	Warm Site	Have systems but no live data
	Cold Site	Only bare metal infrastructure
	Multi-cloud	Business will continue even if one cloud vendor has a problem
CCTV	Closed-Circuit Television	
RFID	Radio Frequency ID	Uses a tag and a receiver which includes: active tags, semi-active tags, and passive tags

CHAPTER 10: CLOUD AND VIRTUALIZATION SECURITY

ACRONYM	FULL NAME	DESCRIPTION
CSA	Cloud Security Alliance	Defines best practices for securing cloud computing. Made the CCM & STAR system
CCM	Cloud Controls Matrix	Determines appropriate use of cloud security controls
STAR	Security Trust, Assurance, and Risk	Technology-neutral certification. L1: self-assessment. L2: third-party audit. L3: continuous auditing.
	Edge Computing	IoT devices that preprocess data before shipping it back to the cloud
	Fog Computing	IoT sensors in between edge computing and server
IaaS	Infrastructure as a Service	Responsible for Hardware and datacenter
SaaS	Software as a service	Responsible for Hardware, Datacenter, OS, and Application
PaaS	Platform as a service	Responsible for Hardware, Datacenter, and OS
XaaS	Anything as a service	
FaaS	Function as a service	
MSP	Managed Service Provider	Capable of working customer's total environment, on-premises and cloud
MSSP	Managed Security Service Provider	Security monitoring, vulnerability management, incident response, and firewall management
VM	Virutal Machines	
RDP	Remote Desktop Protocol	a secure network communications protocol developed by Microsoft. It enables network administrators to remotely diagnose problems that individual users encounter and gives users remote access to their physical work desktop computers
	Containers	Application-level virtualization (ex: Docker), each instance is the same hardware/OS
SDN	Software-Defined Networking	Allows engineers to interact and modify cloud resources via APIs
SDV	Software-Defined Visibility	Traffic insight on virtual networks
VPC	Virutal Private Cloud	Virtual segmentation for a multi-tenant model, designates subnets as private or public
VLAN	Virtual Local Area Network	Logical overlay network that separates devices that share a physical LAN
CASB	Cloud Access Security Brokers	software tools in-between cloud users and providers
	Inline CASB	Physically inline between users and providers
HSM	Hardware Security Modules	Physical computing devices that are tamper-resistant and hardened. Protect and manage cryptographic keys, digital signatures, perform encryption/decryption, create & verify digital signatures
TPM	Trusted Platform Module	Dedicated computer chipto perform and store cryptographic information
	Secure Enclave	Apple's version of a TPM
	Cloud Bursting	On-demand and temporary use of public cloud when demand exceeds resources
	Monolithic Applications	One app for everything
	Hypervisors	Isolates virtual machines. Type 1: bare-metal hypervisors, operate on the hardware. Type 2: runs on top of OS
	Cloud Instance	Virtual server
	Region	Set of connected data centers
	Availability zone	One or more data centers with independent power & cooling
	Geography	Area of the world containing at least one region —> fault tolerance
	Embedded Systems	electronic product that contains a microprocessors and software design to perform a specific task

CHAPTER 11: ENDPOINT SECURITY

ACRONYM	FULL NAME	DESCRIPTION
EOL	End of life	AKA End of sales
EOSL	End of service life	End of technical support, legacy
EDR	Endpoint detection and response	Behavioral monitor endpoint devices & detect/respond to threats
XDR	Extended detection and response	Holistic approach using AI to monitor and response to threats across the entire enterprise
IPS	Intrusion Prevention System	Could shutdown the whole system
IDS	Intrusion Detection System	Won't shutdown the whole system
NIPS	Netowork-based IPS	Network-based IPS —> monitors the entire network
HIPS	Host-based intrusion prevention system	Monitors a single host ffor malicious activity, analyzes traffic before host can process it. Con: can block legitimate traffic
HIDS	Host-based intrusion detection system	Cannot block, only detect
GPO	Group Policy Objects	Hardening system and domain controls via policy
SCT	Security Compliance Toolkit	Security baseline config
SELinux	Security-Enhanced Linux	Linux kernel based security module that provides more capabilities than a traditional Linux
	Jamf Pro	MDM solution for apple devices
RTOS	Real-time operating system	Ex: car
ICS	Industrial Control Systems	Network and software used to control industrial systems (ex: power plant, water plant, manufacturing)
SCADA	Supervisory Control and Data Acquisition	Large industrial systems (ex: power plants, manufacturing, water plants)
RTU	Remote Telemetry Units	Microprocessors collecting data for SCADA
VoIP	Voice over Internet Protocol	Technology that allows users to make phone calls over a broadband internet connection
MFP	Multifunction peripheral	A device that performs a variety of functions that would be otherwise carried out by seperate devices (ex: printer, scanner, copier, fax machine). Con: can act as reflectors, amplifiers, and pivot points for attackers
IoT	Internet of Things	AKA Embedded Devices
SIM	Subscriber Identity Module	Subkect to SIM cloning, physically removing
SIM	Security Information Management	the practice of collecting, monitoring and analyzing security-related data from computer logs and various other data sources, evolved into SIEM
LTE	Long-Term Evolution	(ex: 4G) wireless broadband communication for mobile devices
Wi-Fi	Wireless Fidelity	
DBAN	Darik's Boot and Nuke	Performs multiple passes over a disk to completely sanitize it

CHAPTER 12: NETWORK SECURITY

ACRONYM	FULL NAME	DESCRIPTION
DID	Defense-in-depth	Multiple controls to prevent SPOF
OSI	Open Systems Interconnection	
L1	Physical Layer	
L2	Data link layer	
L3	Network Layer	Firewalls, IPSec
L4	Transport Layer	
L5	Session Layer	
L6	Presentation layer	
L7	Application Layer	
ZTA	Zero Trust Architecture	Control plane + data plane
	Control Plane	Controls data plane, adaptive identity, leverages context, may request additional info, policy driven
	Data Plane	Implicit trust zones, subject, policy enforcement points
PE	Policy Engines	Makes policy decisions
PA	Policy Administrators	Establish or remove communication between subjects and resources

PEP	Policy Enforcement Points	Communicate with policy admins to forward requests between subjects and receive instructions
PDP	Policy Decision Point	
	Subjects	Users in ZTA
DRA	Data Recovery Agent	Microsoft Windows user account with the ability to decrypt data that was encrypted by other users
FEK	File Encryption Key	
FIM	File Integrity Monitoring	Detects changes made to system/app/files by creating a baseline creation (hash)
PPP	Point-to-Point Protocol	suite of computer communication protocols that provide a standard way to transport multiprotocol data over point-to-point links (outdated)
EAP	Extensible Authentication Protocol	Evolution of PPP, framework that allows for the use of different authentication methods for secure network access technologies
EAPoL	Extensible Authentication Protocol over LAN	EAPOL (Extensible Authentication Protocol over Local Area Network) encapsulates EAP packets within Ethernet frames.
LEAP	Lightweight EAP	Developed by Cisco prior to IEEE ratification of 802.11i security standard (outdated)
PEAP	Protected EAP	authenticates servers using certificates and wraps EAP using TLS tunnel
EAP-TLS	Transport Layer Security	Still considered one of thre most secure EAP standards, implements certificate-based authentication as well as mutual authentication
EAP-TTLS	Tunneled Transport Layer Security	Extends EAP-TLS, does not require client devices to have a certificate to create a secure session by requiring software
EAP-FAST	Flexible Authentication via Secure Tunneling	Replacement for LEAP. FAST provides faster authentication while roaming
CAM	Content-addressable memory	AKA associative memory or associative storage, computer memory used in very high-speed searching applications
HA	High availability	
SD-WAN	Software-defined Wide Area Network	Virtual wide area network design that combines many services for organizations
MPLS	Multi-protocol label switching	SD-WAN, 4G, 5G. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. MPLS can encapsulate packets of various network protocols, hence the multiprotocol component of the name
SASE	Secure Access Service Edge	Private networks + SD-WAN + firewalls + CASBs + ZTA → secure access for devices regardless of location
DMZ	Demilitarized Zone	AKA Permieter zone, no-mans-land in network designed to add security layer by isolating networks (like N/S Korea)
	Intranet	Internal network
MAC Address	Media Access Control	12-character code that identifies a device or network
BPDU	Bridge Protocol Data Unit	Protects STP from sending messages it should not, prevents looping
DHCP	Dynamic Host Configuration Protocol	Network protocol that automatically assigns IP address to devices, currently using IPv6 called DHCPv6
IPv4	Internet Protocol version 4	Most common version of IP, uses 32-bit address space
IPv6	Internet Protocol version 6	hosts automatically generate IP addresses internally using stateless address autoconfiguration (SLAAC)
SLAAC	Stateless Address Autoconfiguration	Includes a "privacy address" or "temporary addresses" for IP address privacy
	DHCP Snooping	Prevents rogue DHCP server from handing out IP addresses
ARP	Address Resolution Protocol	Links MAC addresses with IP addresses
RARP	Reverse Address Resolution Protocol (Obsolete)	Client computer requests its IP address from a network when it has a MAC address, replaced by DHCP
VPN	Virtual Private Network	Virtual network link across a public network
IPSec VPN	Site-to-site VPN	Tunnel or transport mode. For VPNs that need more than web and app traffic
SSL VPN	Technically TLS VPN	Portal-based (HTML 5), tunnel mode, no client installation required
	Jump Servers	(AKA jump boxes) securely operates in two different security zones via SSH or RDP
	Load Balancing	Distribute network traffic to equally across a pool of resources to support an application
NGFW	Next gen firewalls	all-in-one-network security devices (deep packet inspection, IDS/IPS, AV) —> faster than UTMs because focused but more config time
	Stateless Firewalls	(AKA packet filters) Most basic firewall, filters every packet's header
	Stateful Firewalls	(AKA dynamic packet filters) track packets, make smart decisions
WAF	Web Application Firewalls	database queries, APIs, and other web app tools —> firewall + IPS, blocks attacks in real time
UTM	Unified Threat Management	firewall, IDS/IPS, AV, URL/email filtering, DLP, analytics —> “out of the box” solution
	Proxy servers	Accept and forward
	Content Filtering	use of hardware or software to screen and/or restrict access to resources
URL	Uniform Resource Lacator	
ACL	Access Control List	Allow or deny lists (time-based, dynamic)
OOBM	Out of bound management	remotely access and manage devices and infrastructure
DNS	Domain-name system	only tells WHERE to send traffic —> not inherently secure
DNSSEC	DNS System Security Extensions	provides authentications of DNS data
	DNS filtering	blocks malicious domains via lists
MIME	Multipurpose Internet Mail Extensions	It lets users exchange different kinds of data files, including audio, video, images and application programs, over email
S/MIME	Secure/Multipurpose internet Mail Extensions	widely accepted protocol for sending digitally signed and encrypted messages
DKIM	DomainKeys Identified Mail	Signature header to verify email sender and prevent email spoofing
SPF	Sender Policy Framework	Allow list for email domains. If not on the list → rejected
DMARC	Domain-based Message Authentication Reporting and Conformance	determine whether you should refuse or accept email message
	Ephemeral Keys	perfect forward key secrecy —> even if key exchange is compromised, communication will not
SNMP	Simple Network Management Protocol	monitor and manage network devices on a LAN or WAN
SNMPv3	Simple Network Management Protocol version 3	authenticating message sources, message integrity validation, and confidentiality
	SNMP Trap	Message when device encounters an error
MIB	management information base	where a MIB is listed
BGP	Border Gateway Protocol	Enables the internet exchange routing information between autonomous systems (insecure). Susceptible to BGP hijacking
NTP	Network Time Protocol	Synchronizes clocks of computer systems (insecure)
SSH	Secure Shell	Protocol for remote console access to devices. Also tunneling protocol
IPSec	Internet Protocol Security	Entire suite of security protocols, used for VPNs
AH	Authentication Header	hashing + shared secret key = IP payload is secured
ESP	Encapsulating Security Payload	tunnel mode - entire packet secured, transport mode - only payload secured
SA	Security Associations	Bulding block where are the secure communications is built
SPI	Security Paramters Index	an identifier used to uniquely identify both manually and dynamically established IPSec
RTP	Real-time Transport Protocol	network standard designed for transmitting audio or video data that is optimized for consistent delivery of live data. It is used in internet telephony, Voice over IP and video telecommunication. It can be used for one-on-one calls (unicast) or in one-to-many conferences (multicast).
SRTP	Secure Real-time Transport Protocol	an extension to RTP (Real-Time Transport Protocol) that incorporates enhanced security features
IKE	Intenet Key Exchanges	setup using X.509 certificates, standard protocol used to set up a secure and authenticated communication channel between two parties via a virtual private network
ISAKMP	Internet Security Association and Key Management Protocol	for establishing security association (SA) and cryptographic keys in an Internet environment
MITM	Man In The Middle	On-path attacks
MITB/MIB	Man In The Browser	
	Amplified DoS Attacks	taking advantage of small query —> large result (ex: DNS query)
	Reflected DoS Attack	spoofing IP address to conduct an attack
	ICMP Floods	AKA ping floods
	Smurf attacks	spoofed sender address via ICMP broadcast messages

CHAPTER 13: WIRELESS AND MOBILE SECURITY

ACRONYM	FULL NAME	DESCRIPTION
BYOD	Bring your own device	
CYOD	Choose your own device	
COPE	Corporate-owned, personally enabled	
COBO	Corporate Owned Business Only	

MDM	Mobile Device Management	Mobile device management is the administration of mobile devices, such as smartphones, tablet computers, and laptops. MDM is usually implemented with the use of a third-party product that has management features for particular vendors of mobile devices
MAM	Mobile Application Management	software and services responsible for provisioning and controlling access to internally developed and commercially available mobile apps used in business
MCM	Mobile Content Management	Mananing and distributing enterprise files on mobile systems
RCS	Rich Communication Services	new version of SMS, allows for more data connection via text like video, pictures, GIFs, etc
OTA	Over-the-air	wireless delivery of data, software or firmware to mobile devices
SSP	Security Simple Pairing	Security Mode 4 for Bluetooth
GPS	Global Positioning System	uses satellite network (ex: U.S. GPS system, Russian GLONASS) —> used for Geolocation authentication, geofencing
NFC	Near-field communication	very short-range communication (4 inches) between devices (ex: Apply Pay, Google Pay)
	Infrared	only work in line-of-sight (speeds from 115 Kbit/s to 1 Gbit/s)
BIAS	Bluetooth Impersonation AttackS	Exploiting mutual authentication
TKIP	Temporal Key Integrity Protocol	security protocol used in the IEEE 802.11 wireless networking standard. TKIP was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as an interim solution to replace WEP without requiring the replacement of legacy hardware
WPA-2	Wi-Fi Protected Access 2	Security protocol that encyrpts internet traffic on wireless networks, compatible with CCMP
WPA2-PSK	WPA2-Personal	pre-shared key, allows client to authenticate with a server infrastructure
	WPA2-Enterprise	relies on RADIUS as part of 802.1X
WPA-3	Wi-Fi Protected Access 3	SAE, perfect forward secrecy, Optional 192-bit security mode, still uses RADIUS, OWE
SAE	Simultaneous Authentication of Equals (AKA Dragonfly Key Exchange)	requires client/network to validate both sides
PFS	Perfect Forward Secrecy	also known as Forward Secrecy, is an encryption style known for producing temporary private key exchanges between clients and servers. For every individual session initiated by a user, a unique session key is generated. If one of these session keys is compromised, data from any other session will not be affected. Therefore, past sessions and the information within them are protected from any future attacks.
OWE	Opportunistic wireless encryption	provide encrypted Wi-Fi on open networks when possible

CHAPTER 14: MONITORING AND INCIDENT RESPONSE

ACRONYM	FULL NAME	DESCRIPTION
IR	Incident Response	plan, process, team, technology, skills, and training to respond appropriately (ongoing process)
IRP	Incident Response Plan	set of instructions to detect, respond to and limit the effects of an information security event.
CERT	Computer Emergency Response Team	
CIRT	Computer Incident Response Team	
CSIRT	Computer Security Incident Response Team	
	Incident	violation of organizations policies
	Events	observable occurrence
PICERL	Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned	Incident response process by SANS
BC	Business Continuity	making sure business can continue despite the incident, important for larger incidents
sFlow	Sampled Flow	collect IP traffic as it enters or exits interface, developed by Cisco in 1996 —> tracks bandwidth utilization
NetFlow v9		
IPFIX	Internet Protocol Flow Information Export	The IPFIX protocol provides network administrators with access to IP Flow information
RCA	Root Cause Analysis	Ask five why's, event analysis, diagramming cause and effect
CAR	Corrective Action Report	an official document issued when an element of a plan hasn't been implemented or executed properly
	Whitelists	Application allow lists
	Blacklists	Application deny lists
	Containment	Leaves system in place but prevents further actions

CHAPTER 15: DIGITAL FORENSICS

DFIR	Digital Forensics and Incident Response	Finding evidence, removing attacker, assessing damage, lessons learned
	Computer Forensics	Subfield of Digital Forensics
	Artifacts	Pieces of evidence that point to an activity on a system
	E-discovery	Electronic discovery
	Legal Hold	
	DFIR Tools	Eric Zimmerman's Tools KAPE (Knoll Artifact Parser and Extractor): automates artifact collection, creates timeline Autopsy: open source forensic platform Volatility: memory analysis Redline: collecting forensic information Velociraptor: open-source advanced endpoint-monitoring, forensics, and response platform
EDRM	Electronic Discovery Reference Model	Framework for outlining activities for recovering and discovering digital data
	Venue	Location where legal case is heard
	Nexus	A connection or link between things, persons, or events in part of a chain of causation
	Order of Volatility	What data is most likely to be lost to due to normal processes: CPU cache and registers Ephemera data: kernel statistics, ARP cache, process table System memory - RAM Temporary files and swap space Data on the disk OS Devices, IoT devices Firmware Snapshots from VMs Remote logs Backups
SMART		ASR Data's format for their SMART forensic tool
E01	Encase Image File Format	Developed by ASR Data, the Expert Witness file format (aka E01 format aka EnCase file format) is an industry standard format for storing "forensic" images. The format allows a user to access arbitrary offsets in the uncompressed data without requiring decompression of the entire data stream.
AFF	Advanced Forensics Format	The Advanced Forensic Format (AFF) is on-disk format for storing computer forensic information. Critical features of AFF include: AFF allows you to store both computer forensic data and associated metadata in one or more files.

SANS	SANS Institute	The SANS Institute is a private U.S. for-profit company founded in 1989 that specializes in information security, cybersecurity training, and selling certificates. Topics available for training include cyber and network defenses, penetration testing, incident response, digital forensics, and auditing
SANS SIFT	SANS SIFT Workstation	The SIFT Workstation is a collection of free and open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings
	Checksum	Small-sized block of data derived from another block of data to detect errors

CHAPTER 16: SECURITY GOVERNANCE AND COMPLIANCE

ACRONYM	FULL NAME	DESCRIPTION
GRC	Governance, risk, and compliance	
	Governance programs	set of procedures and controls put in place to allow an organization to effectively direct its work
SME	Subject Matter Experts	
CISO	Chief Information Security Officer	
AUP	Acceptable Use Policy	
ISO	International Organization for Standardizations	
ISO 27001		Information security management systems
ISO 27002		Controls implemented to meet cybersecurity objectives
ISO 27701		Standard guidance for managing privacy controls
ISO 31000		Guidelines for risk management
MSA	Master Service Agreements	umbrella contract for the work that a vendor does
SOW	Statement of Work	project-specific details and references to MSAs
SLA	Service Level Agreement	contracts that specify conditions of service will be provided by vendor
MOU	Memorandum of Understanding	informal document laying out relationship with vendor
MOA	memorandum of agreement	formal document outlining the terms between parties, establishing roles and responsibilities. More detailed than MOUs
BPA	Business partner agreements	when two organizations agree to do business together, could potentially specify responsibilities and division of profits
HIPAA	Health Insurance Portability and Accountability Act	Privacy rules for medical industry in the US
PCI DSS	Payment Card Industry Data Security Standards	
PFI	PCI Forensic Investigator	help determine the occurrence of a cardholder data compromise and when and how it may have occurred.
GLBA	Gramm-Leach-Bliley Act	US financial institutions must have security programs
SOX	Sarbanes-Oxley Act	Strong security for publicly traded companies financial records
GDPR	General Data Protection Regulation	Security and privacy requirements for PII in the EU
FERPA	Family Educational Rights and Privacy Act	US student education records privacy
CSF	Cybersecurity Framework	Broad structure for cybersecurity controls in private sector
RMF	Risk Management Framework	formal process for implementing security controls and authorizing system use
	NIST Framework Core	Identify Protect Detect Respond
	NIST Cybersecurity Framework Implementation tiers	Tier 1: Partial Tier 2: Risk Informed Tier 3: Repeatable Tier 4: Adaptive
CBT	Computer Based Training	part of a diversity of a strong security training program

CHAPTER 17: RISK MANAGEMENT AND PRIVACY

ACRONYM	FULL NAME	DESCRIPTION
ERM	Enterprise Risk Management	formal org approach to risk analysis. Identify risks, determine severity
AV	Asset Value	Expressed in dollars
ARO	Annualized Rate of Occurance	ARO 2.0 means 2X per year
EF	Exposure Value	Percentage of expected damage (ex: EF 90%)
SLE	Single Loss Expectancy	AV * EF, amount of financial damage expected from each time risk materializes
ALE	Annualized Loss Expectancy	SLE * ARO, amount of damage expected each year
TCO	Total Cost of Ownership	The mitigation cost: upfront costs + ongoing costs (nromalliy operational)
KRI	Key Risk Indicators	
KPI	Key Performance Indicators	
KRA	Key Results Area	
BIA	Business Impact Analysis	
MTBF	Mean time between failure	Expected time between failures, measures reliability of a system
MTTR	Mean time to repair	Average amount of time to restore
PII	Personal Identifiable Information	
PHI	Personal Health Information	Subject to HIPAA
DPO	Data Protection Officer	Official role required by GDPR (Chief Privacy Officer in US)
	Automation	Achieving outcomes without humans
	Orchestration	Orchestration allows you to share information easily, enabling multiple tools to respond to incidents as a group, even when the data is spread across a large network and multiple systems or devices
IaC	Infrastructure as Code	Using code to manage & provide