Handout 1

CompTIA Security+ Acronyms

3DES	Triple Digital Encryption Standard	Performs encryption in 3 rounds of the same algorithm.
802.1x	Switch authentication	Standard for controlling access to intranet infrastructure devices.
AAA	Authentication Authorization, and Accounting	The principle of verifying identity, capability and use.
ABAC	Attribute-based Access Control	Granting access based upon the characteristic of the subject, such as clearance level.
ACL	Access Control List	Restricting entry, based upon a listing of controls or permissions.
AES	Advanced Encryption Standard	Rijndael was approved by the US government and given this title.
AES256	Advanced Encryption Standards 256bit	The 256 bit version of this algorithm is its highest level and is deemed uncrackable by brute force methods.
AH	Authentication Header	The AH header transmits in clear text but authenticates and integrity checks each packet.
AI	Artificial Intelligence	The simulation of human intelligence and thinking in a machine, including adaptive learning and problem-solving.
AIS	Automatic Indicator Sharing	Automated sharing of threat information between organizations to enhance detection and response.
ALE	Annualized Loss Expectancy	The single loss expectancy times the annualized rate of occurrence.
ALG	Application Layer Gateway	This is a type of firewall able to inspect headers and payload in the upper protocol layers.
AP	Access Point	Infrastructure connection point for most wireless networks.
API	Application Programming Interface	These are development tools used by programmers that have prebuilt functions with desired utility.
APT	Advanced Persistent Threat	Applications with advanced targeting, zero days and exfiltration techniques that are aimed at particular organizations or industries.

Handout 1: CompTIA Security+ Acronyms

ARO	Annualized Rate of Occurrence	Most risk assessments track threats and attacks on an annualized basis.
ARP	Address Resolution Protocol	Given the IP address ARP will locate the MAC address.
ASLR	Address Space Layout Randomization	This randomizes the location of an application in memory making it harder for attackers to successfully perform the buffer overflow.
ASP	Application Service Provider	An organization provides access to its custom developed software, such as accounting or customer management.
Asymmetric key	Public key	The use of complementary values to disguise and then reveal information.
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge	A database of adversarial tactics and techniques that might be used to compromise systems organizations to enhance threat management.
AUP	Acceptable Use Policy	This policy is legally required, if HR wants to fire someone for misuse.
AV	Antivirus	Designed to identify malware, primarily based upon known patterns.
AV	Asset Value	This can be the replacement cost or income derived from something.
AXFR	Zone transfer	The synchronization of name resolution information between a primary and secondary DNS server.
BASH	Bourne again shell	Bash is a UNIX and Linux command interface and language.
BCP	Business Continuity Plan	The orderly planning for and management of threats and incidents to an organization.
BGP	Border Gateway Protocol	Border Gateway Protocol is for routing exterior traffic between autonomous systems/organizations.
BIA	Business Impact Analysis	This is the prerequisite for disaster recovery and continuity planning to identify potential losses.
BIA	Business Impact Analysis	Assessing the criticality of business activities and assets in order to determine the appropriate protection and recovery options.
BIOS	Basic Input/Output System	The now deprecated firmware based initialization code for booting a system.
Bluetooth	802.15	Technology commonly used to communicate with small devices at modest speeds over a short range with low security requirements.
BO	Buffer overflow	The insertion of malicious computer instructions into the RAM of a host to accomplish denial of service or injecting shellcode.
BPA	Business Partners Agreement	This outlines the goals and responsibilities between entities pursuing a common work product.

Handout 1: CompTIA Security+ Acronyms

BPDU	Bridge Protocol Data Unit	Key element in STP to prevent looping.
BPDU	Bridge Protocol Data Unit	This protocol is used to identify efficient paths and loops in a switched network.
Brute force	Brute force attack	Discovers a hash or encrypted secret by attempting all combinations and permutations.
BSSID	Basic Service Set IDentifier	This is the MAC address that a wireless device is attached to.
BYOD	Bring Your Own Device	The organization compensates the individual for use of their phone in organizational activities.
C2	Command and control	Servers that are centrally placed the hold control instructions for illicitly managed hosts.
CA	Certificate Authority	This entity issues certificates. After verifying them, and is the center of trust in PKI.
CAC	Common Access Card	A form of identification with photograph, barcode, RFID and cryptographic storage of private key information.
CAPTCHA	Completely Automated Public Turing to Tell Computers and Humans Apart	This is intended to prevent rogue automated attempts at access.
CAR	Corrective Action Report	A document generated when the defect or error has been detected that has the goal of eliminating a reoccurrence.
CASB	Cloud Access Security Broker	A software resource place between users and cloud applications that monitors and enforces policy-based access to cloud resources.
CBC	Cipher Block Chaining	Each plaintext block is XORed (see XOR) with the immediately previous ciphertext block.
CBT	Computer-Based Training	Courseware or lessons that are delivered via a computer, commonly used for at home and corporate training.
CCMP	Counter-Mode/CBC-Mac Protocol	Each plaintext block is XORed (see XOR) with the immediately previous ciphertext block that includes a message authentication code.
CCTV	Closed-circuit Television	Allows monitoring and recording of activities in an area.
CER	Cross-over Error Rate	The point at which false acceptances are equal to false rejection.
CER	Certificate	A generic term for a document that facilitates authentication.
CERT	Computer Emergency Response Team	A multi-discipline group designated to handle IT incidents.
CFB	Cipher Feedback	A mode of operation for a block cipher.
Chain of custody	Evidence control and management	The documentation of handling and protection of evidence.

Handout 1: CompTIA Security+ Acronyms

CHAP	Challenge Handshake Authentication Protocol	Commonly used by routers and has several derivatives in use by Microsoft for authentication.
CIA	Confidentiality Integrity Availability	The security triad.
CIO	Chief Information Officer	The most senior official in an organization responsible for the information technology and systems that support enterprise.
CIRT	Computer Incident Response Team	A group that investigates and resolves IT security problems.
CIS	Center for Internet Security	Its mission is to identify develop, promote, and lead the world with regard to best practices for cybersecurity solutions.
CMP	Change Management Policy	An organizational process designed to facilitate making changes to organizational resources in such a way that they are identifiable, auditable, and orderly.
CMS	Content Management System	These are applications that facilitate the creation, editing, publishing and archival of web pages and content.
CN	Common Name	An identifying name that may be applied to a directory resource, such as a user, server, or other object.
COOP	Continuity of Operations Plan	Ensuring that vital and primary mission essential functions continue to run, even in the face of emergencies.
COPE	Corporate Owned, Personally Enabled	Smart phones owned by the organization but approved for personal use.
CP	Contingency Planning	Procedures to follow in the event of a catastrophic incident, even though it may be unlikely.
CRC	Cyclical Redundancy Check	An error checking code, used in digital technology primarily to identify accidental changes to data.
Crimeware	Cyber theft	A class of malware that automates malicious activity.
CRL	Certificate Revocation List	This is maintained by a certificate authority to identify certificates associated with compromised or lost private keys.
CSA	Cloud Security Alliance	A nonprofit organization that promotes best practices in security for cloud-based computing.
CSIRT	Computer Security Incident Response Team	Information technology personnel whose purpose is to prevent, manage and coordinate actions about security incidents.
CSO	Chief Security Officer	An executive position in charge of policy and programs to reduce risk in an organization.
CSP	Cloud Service Provider	An organization that provides cloud-based access to infrastructure, storage and/or applications.
CSR	Certificate Signing Request	Created by an applicant seeking to gain a certificate from an authority.

Handout 1: CompTIA Security+ Acronyms

CSRF	Cross-site Request Forgery	An attack wherein a message is spoofed from a user to a trusted site.
CSU	Channel Service Unit	A connecting device used to link an organization to telco-based T-services
CTO	Chief Technology Officer	The executive person tasked with identifying useful technology, IT strategies and partnerships.
CTOS	Centralized terminal operating system.	Legacy management.
CTR	Counter	This form of encryption is used by AES to perform streaming encryption.
CVE	Common Vulnerabilities and Exposures	A database of known and published software flaws that may impact security that is managed by MITRE.
CVSS	Common Vulnerability Scoring System	An empirical scheme for rating vulnerability severity based upon specific aspects of the vulnerability, environment, and nature of threats.
CYOD	Choose Your Own Device	In this mode of control and acquisition, an employee chooses a device from a company provided list. Ownership may be personal or organization.
DAC	Discretionary Access Control	The creator has all control over an asset and access to it. The default form of access for Windows.
Data custodian	Facilitates use	Exemplified by data center personnel who manage and maintain systems.
Data owner	Responsible for use	Determines logical controls, authorizes use and defines required security.
DBA	Database Administrator	This role is filled by personnel capable of managing automated and large information repositories.
DDoS	Distributed Denial of Service	This attack methodology involves a multitude of remotely controlled devices focusing upon a single target.
DEP	Data Execution Prevention	And operating system memory management technique that prevents user data from overlapping into computer instructions.
DER	Distinguished Encoding Rules	A commonly used method of encoding the data that makes up the certificate using ASN.1.
DES	Digital Encryption Standard	The first US government standard for symmetric encryption. It has a 56 bit key.
DHCP	Dynamic Host Configuration Protocol	This is an extension of BOOTP and is used to dynamically allocate IPs.
DHE	Diffie-Hellman Ephemeral	This is a key exchange algorithm that enhances confidentiality by discarding the session keys after use.
Dictionary	Dictionary attack	Performs hashing or encryption on an array of predetermined candidate phrases and compares it to the secret.

Handout 1: CompTIA Security+ Acronyms

Differential BU	Differential backup	It moves files to alternative media that have the archive bit set, and then it does not clear it.
DKIM	Domain Keys Identified Mail	A messaging security standard designed to facilitate non-repudiation between sender and receiver.
DLL	Dynamic Link Library	These files are not directly executed but are called up by an application when certain additional functions or libraries are needed.
DLP	Data Loss Prevention	Strategies and applications that prevent data theft or illicit access.
DMARC	Domain Message Authentication Reporting and Conformance	This is an email security standard designed to allow domains to protect themselves from unauthorized use and spoofing.
DMZ	Demilitarized Zone	The perimeter area where the outside world may access certain services.
DNAT	Destination Network Address Translation	The initial destination of a packet as it enters a NAT system to be redirected to another destination.
DNAT	Destination Network Address Translation	It redirects packets destined for specific IP address or specific port on IP address, on one host simply to a different address mostly on different host.
DNS	Domain Name Service	An application that handles symbolic name to address mappings, as well as the reverse.
DNSSEC	Domain Name System Security Extensions	An array of tools devised by the IETF to secure DNS transactions.
DoS	Denial of Service	A one on one attack that causes access or utility to cease.
DPO	Data Protection Officer	A senior officer responsible for an organization's data protection strategies and compliance.
DRP	Disaster Recovery Plan	The immediate plans for recovery of operations or services in the event of a catastrophic incident.
DSA	Digital Signature Algorithm	An algorithm created by the NSA to implement non-repudiation.
DSL	Digital Subscriber Line	High-speed Internet conductivity based upon existing infrastructure for telephones.
EAP	Extensible Authentication Protocol	A derivative of PPP used by wired and wireless networks to validate connections.
ECB	Electronic Code Book	A mode of symmetric encryption that divides the message into each block and encrypts them separately.
ECC	Elliptic Curve Cryptography	An algorithm commonly used for key exchange that relies upon geometric complexities.
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral	Used to negotiate a temporary shared secret using a public and private key.

Handout 1: CompTIA Security+ Acronyms

ECDSA	Elliptic Curve Digital Signature Algorithm	This signing technique employs the complexities of geometry, instead of factoring prime numbers.
EDR	Endpoint Detection and Response	An intranet technology designed to protect access to the infrastructure, identify threats and quarantine known offenders.
EF	Exposure Factor	Typically referenced as a percentage value indicating value lost from one attack.
EFS	Encrypted File System	A cryptosystem built into Microsoft that allows selective encryption.
EIP	Extended Instruction Pointer	A programming concept that points an application to the bottom or next step in execution.
EMI	Electromagnetic Interference	Typically associated with accidental radiation of signals that interfere with IT systems.
EMP	Electro Magnetic Pulse	Large and significant discharge of signals that can create a denial of service in transmission and storage.
EOL	End of Life	This term identifies when a product has reached the end of its useful life according to the vendor.
EOSL	End of Service Life	This term identifies when a product has reached the end of its useful life and is no longer patched or fixed or maintained.
ERP	Enterprise Resource Planning	Software designed to run and entire organization, including automation, finance, HR and manufacturing.
ERP	Enterprise Resource Planning	Business process management integrated into multiple aspects of an organization, it services, and human resources.
ESN	Electronic Serial Number	An identifying number created by the Federal Communications Commission to uniquely identify mobile devices and radios.
ESP	Encapsulated Security Payload	A header used in IPSEC to create confidentiality.
FACL	File System Access Control List	This is creating filters or restrictions on disk storage.
FAR	False Acceptance Rate	When biometrics malfunction, incorrectly granting permissions.
FDE	Full Disk Encryption	Enforcing confidentiality across the entire storage device.
FIM	File Integrity Monitoring	A defensive control designed to assess or validate the integrity of files, such as Tripwire.
FPGA	Field Programmable Gate Array	An integrated circuit or chip that may be revised or configured after manufacture.
FRR	False Rejection Rate	A biometric measurement, indicating the rate at which authorized personnel are forbidden access.
FTP	File Transfer Protocol	A file management application designed to insecurely upload and download files.

Handout 1: CompTIA Security+ Acronyms

FTPS	File transfer Protocol - Secure	A relative of HTTPS implemented in the same way with certificates and key exchange.
Full BU	Full backup	It moves files to alternative media that regardless of whether the archive bit is set, and then it clears it.
GCM	Galois Counter Mode	Useful for protecting packet data as it has little latency and minimum operation overhead.
GDPR	General Data Protection Regulation	A law from the European Union that directs protection and privacy of personal information.
GPG	Gnu Privacy Guard	The free incarnation of a popular cryptosystem, commonly used to secure email.
GPO	Group Policy Object	A feature of Windows that provides centralized management of configuration and settings.
GPS	Global Positioning System	A satellite-based protocol that can closely identify the location or asset.
GPU	Graphic Processing Unit	These processors have an alternate use in discovering keys and cracking.
GRE	Generic Routing Encapsulation	An old and standard protocol that inserts one packet within another.
HA	High Availability	Ensuring that system uptime extends longer than what it normally would.
HDD	Hard Disk Drive	A mass storage system, typically implemented with spinning platters and heads that perform reading and writing.
HIDS	Host-based Intrusion Detection System	A defensive application that identifies anomalous or malicious activities within a device.
HIPS	Host-based Intrusion Prevention System	A defensive application that prevents anomalous or malicious activities within a device.
HMAC	Hashed Message Authentication Code	Implementing non-repudiation via an exchanged value and hashing.
Honeynet	Honeypot network	A sophisticated system designed to locate, discover, distract and otherwise observe malicious behavior.
Honeypot	Fake target	Used to identify and distract hackers.
Host firewall	Software firewall	The last line of defense for a system against a malicious intranet host.
hosts	Local resolver	This is a file wherein the system manager may define their own names to resolve IP addresses.
HOTP	HMAC-based One-Time Password	Performs authentication by requiring a user to enter a system generated code into a hashing or calculating algorithm that produces a response.
HSM	Hardware Security Module	These key management systems are ideally suited for automated private key transactions that require strong security.
HSMaaS	Hardware Security Module as a Service	A cloud-based service that allows customers to create, manage and implement encryption keys.

Handout 1: CompTIA Security+ Acronyms

HTML	Hypertext Markup Language	The scripting used by browsers to interpret and display content.
HTTP	Hypertext Transfer Protocol	The means by which HTML and images are viewed and accessed by browsers.
HTTPS	Hypertext Transfer Protocol over SSL/TLS	Performing HTTP over an encrypted channel.
HVAC	Heating, Ventilation and Air Conditioning	The heating, cooling and other environmental aspects of a building.
IaaS	Infrastructure as a Service	Implementing cloud-based networks, servers and other infrastructure.
IaC	Infrastructure as Code	Management and provisioning of infrastructure systems and divides by code and settings versus manual and physical means.
IAM	Identity and Access Management	The policies, procedures and technologies that facilitate ensuring that only the appropriate personnel have access to resources in an organization.
ICMP	Internet Control Message Protocol	A multifunctional protocol designed to perform network testing and report errors.
ICS	Industrial Control Systems	Semi-intelligent devices used to control industrial or scientific equipment from central consoles.
IDEA	International Data Encryption Algorithm	This is a symmetric cipher that is block-oriented, with the key size of 128 bits.
IDF	Intermediate Distribution Frame	The wiring panels linked by risers between floors to perform cross-connection.
IdP	Identity Provider	A service that contain subjects and can perform centralized authentication on behalf of service providers.
IDS	Intrusion Detection System	A generic term referring to generating alerts four malicious activity.
IEEE	Institute of Electrical and Electronics Engineers	The mission of the IEEE is to promote and develop technological advances for the benefit of humanity.
IKE	Internet Key Exchange	This is used prior to IPSEC for the negotiation, exchange and management of symmetric key information.
IM	Instant Messaging	A class of online chat that offers real-time transmission of messages over the Internet and local area networks.
Image	Drive cloning	The archival of information, bit by bit, or sector by sector to alternative media.
IMAP4	Internet Message Access Protocol v4	This application listens on TCP/143 and it is clear text form.
Incremental BU	Incremental backup	It moves files to alternative media that have the archive bit set, and then it clears it.
Input validation	Inspection or sanitation	The verification of programmatic input to an application.

Handout 1: CompTIA Security+ Acronyms

IoC	Indicators of Compromise	Artifacts and other forensic data that may be used to identify illicit activity, malware and data breaches.
IoT	Internet of Things	A reference to network devices that typically have little defensive capability.
IP	Internet Protocol	A layer 3 system for addressing, fragmenting, reassembly and delivery of datagrams.
IPS	Intrusion Prevention System	A security measure designed to detect as well as prevent threats from advancing or escalating.
IPSec	Internet Protocol Security	Generally considered the most secure remote access protocol.
IPv6	Internet Protocol version 6	Greatly expands the address in space, provides for simplified headers and has hexadecimal addressing.
IR	Incident Response	A generic reference to steps to be taken after specific adverse events occur.
IRC	Internet Relay Chat	A protocol commonly implemented by helpdesks and Bots.
IRP	Incident Response Plan	Devised plans to be implemented upon the manifestation of a specific threat.
ISA	Interconnection Security Agreement	The agreed-upon measures, settings and protocols taken by two organizations to facilitate communication.
ISFW	Internal Segmentation Firewall	A network firewall placed on the intranet to separate two different security zones.
ISO	International Organization for Standardization	An international nonprofit organization that develops and publishes standards.
ISP	Internet Service Provider	An organization that facilitates access to a worldwide digital network.
ISSO	Information Systems Security Officer	An organizational role charged with developing, implementing, testing and reviewing IT security.
ITCP	IT Contingency Plan	Minimizing risk by identifying threats of the vulnerabilities in the appropriate measures to limit or prevent them.
IV	Initialization Vector	This is a random number that augments a secret key to enhance security for a session.
KDC	Key Distribution Center	The key server in a Kerberos realm that has access to the keys for all principles.
KEK	Key Encryption Key	Protects a private or secret key from unauthorized access or disclosure.
L2 Device	Switch	Filter and forward data at the MAC layer.
L2TP	Layer 2 Tunneling Protocol	Supports VPN site to site connections but does not encrypt.
L3 Device	Router	This is an infrastructure device that interconnects networks and can span different technologies.

Handout 1: CompTIA Security+ Acronyms

LAN	Local Area Network	A network composed of relatively short-range protocols that facilitate swift transfer of information.
LDAP	Lightweight Directory Access Protocol	This is a protocol designed to work with AD or NDS information from a tree.
LEAP	Lightweight Extensible Authentication Protocol	Commonly integrated with Cisco systems to facilitate centralized authentication.
Logic bomb	Insider alteration	A category of malicious activity, wherein an authorized user adds unwanted instructions.
MaaS	Monitoring as a Service	The staging of general purpose or security management systems on the cloud that manage local agent-based systems.
MAC	Media Access Control	This is typified by a network interface card, along with its unique burned in identifying number.
MAC	Mandatory Access Control	A strict form of access control that prevents subjects from accessing objects above their security level.
MAC	Message Authentication Code	A small piece of information sent along with a message that validates the sender.
MAM	Mobile Application Management	Management software designed to allow an enterprise to maintain control over its mobile devices, smart phones and tablets.
MAN	Metropolitan Area Network	A general description of a technology that allows access across entire municipal areas.
Mantrap	Screening area	An access point to a physical organization designed to regulate inbound and outbound access.
MBR	Master Boot Record	A pointer to an area on the disk where initial loading information is stored.
MD5	Message Digest 5	One of the oldest hashing algorithms.
MDF	Main Distribution Frame	This is the centralized connection point between intermediate distribution frames and the outside world.
MDM	Mobile Device Management	Software that centrally controls the security aspects and configuration of smart phones.
MFA	Multi-Factor Authentication	Requiring the use of two or more of location, something you know, have, are or do.
MFD	Multifunction Device	Office equipment, typically a printer, that is able to fax, photocopy and scan documents.
MFP	Multifunction Printer	A printer that can fax, photocopy and scan documents.
MITM	Man-in-the-Middle	An attacker insinuates itself between a client and a server, observing or modifying communication.
MITM	Man in the middle	On-Path attack wherein a node listens to and takes over a conversation by insinuating itself in the stream of communication.

Handout 1: CompTIA Security+ Acronyms

ML	Machine Learning	A component of artificial intelligence that enables a system to learn, adapt and improve based upon inputs without having to be reprogrammed.
MMS	Multimedia Message Service	A protocol intended to facilitate multimedia transfer over SMS.
MOA	Memorandum of Agreement	This is a document that describes the cooperative work to be taken together by two parties toward an objective.
MOU	Memorandum of Understanding	This provides terms and details necessary for two parties to work together.
MPLS	Multi-protocol Label Switching	This is used by WAN providers to quickly forward data using short and discrete labels, rather than complex network addresses.
MSA	Master Service Agreement	An agreement between parties that establishes what terms and conditions will govern a range of activities.
MSCHAP	Microsoft Challenge Handshake Authentication Protocol	Uses an initial handshake to create a nonce added to the hashed ID and secret to create varying outputs.
MSP	Managed Service Provider	A specialty provider of IT services management contracted by a client.
MSSP	Managed Security Service Provider	A contracted service wherein an outside party manages, monitors and maintains security services, including firewalls, intrusion detection, virtual private networks and end point security.
MTBF	Mean Time Between Failures	The estimation as to how often serious errors occur, typically measured in thousands of hours.
MTTF	Mean Time to Failure	Measures the average amount of time an e asset operates before it has a serious failure.
MTTR	Mean Time to Recover or Mean Time to Repair	A standard recovery statistic indicating swiftness of DRP responses.
MTU	Maximum Transmission Unit	The maximum number of bytes allowed within a datalink technology.
NAC	Network Access Control	A technology primarily used for local access control that may involve MAC addresses and 802.1x.
NAS	Network-attached Storage	File oriented storage of computer information across the network on a central device that may be using multiple storage media.
NAT	Network Address Translation	This is commonly implemented by firewalls and is used to remap address space on the inside to one or several addresses on the outside edge.
NDA	Non-disclosure Agreement	A legally binding agreement, compelling parties to not reveal information to others.

Handout 1: CompTIA Security+ Acronyms

NFC	Near Field Communication	This is a short range wireless technology, commonly used for payment systems and person-to-person data exchanges.
NFV	Network Function Virtualization	An architectural concept that utilizes virtual machines and virtual infrastructures to connect and manage networks.
NGFW	Next-generation Firewall	Considered a third-generation technology, this type of firewall implements multiple security measures, such as filtering, VPN, social media monitoring and more to provide protection.
NG-SWG	Next-generation Secure Web Gateway	A cloud-based defensive measure designed to protect users from web-based threats and to provide enforcement of corporate policies.
NIC	Network Interface Card	The layer 2 device that physically connects a system to a network.
NIDS	Network-based Intrusion Detection System	The technology used to scan, packet data for threats and exploits.
NIPS	Network-based Intrusion Prevention System	A technology that identifies and stops attacks by inspecting network information.
NIST	National Institute of Standards & Technology	A government group that publishes recommendations and standards, many related to IT security.
NOC	Network Operations Center	IT network management, monitoring and control are performed here.
NOP	No operation	A common element in memory corruption attacks.
NTFS	New Technology File System	The file system used by Windows that incorporates multilevel security.
NTP	Network Time Protocol	This protocol is necessary to support Kerberos and its requirement for close chronograph management.
OAUTH	Open Authorization	An authentication mechanism that allows secure delegated access.
OCSP	Online Certificate Status Protocol	This protocol is used by the client to validate the status of a received certificate.
OID	Object Identifier	This is a value, commonly associated with SNMP that is used to identify aspects of a managed device or system.
OS	Operating System	The software on a system initially loaded that regulates access to resources and facilitates the execution of applications.
OSI	Open Systems Interconnection	A seven layer scheme that identifies commonly implemented features involved in networked applications and systems.

Handout 1: CompTIA Security+ Acronyms

OSINT	Open-source Intelligence	Accessing data stores of information that enable one to collect, analyze and discern useful information from publicly available resources.
OSPF	Open Shortest Path First	An open standard routing protocol capable of dynamic routing and the secure transfer of routing table information.
OT	Operational Technology	Associated with industrial controls and processes, this refers to systems that identify changes, perform monitoring and control industrial equipment resources.
OTA	Over The Air	A general technology category of systems that use wireless and cellular means to obtain new data or updates.
OTG	On-The-Go	A technical specification for USB devices that allow them to act as hosts and facilitate connections from other USB devices, such as mice and keyboards.
OTP	One-time password	Implement the authentication with a secret that expires upon initial access.
OTP	One-time pad	Involves a key that is as long as the message but may only be used once.
OVAL	Open Vulnerability Assessment Language	A derivative of the SCAP program to automate vulnerability detection and management.
OWASP	Open Web Application Security Project	A nonprofit international organization that facilitates education, secure development, documentation, tools and other technologies to enhance web applications.
P12	PKCS #12	This format allows for the storage of both public and private keys in open or encrypted form.
P2P	Peer to Peer	A headless file sharing system that has no centralized point of control and facilitates wide-open file sharing.
PaaS	Platform as a Service	A form of access that allows an organization to create and run its own applications on the cloud.
PAC	Proxy Auto Configuration	A JavaScript based technology that regulates the configuration of browsers and their use of web proxies.
PAM	Privileged Access Management	The processes and technologies use to secure administrative or privileged accounts.
PAM	Pluggable Authentication Modules	Dynamically, loadable authentication libraries used on Linux.
PAP	Password Authentication Protocol	This is an insecure authentication protocol, sometimes used between routers.
PAT	Port Address Translation	Address translation that multiplexes many internal addresses through one or a few external address, linking connections based upon the source port.

Patch management	Configuration and baseline maintenance	An application designed to identify compliance deviations and variance from a baseline, and then rectify it.
PBKDF2	Password-based Key Derivation Function 2	This cryptographic function, processes, and otherwise insecure secret through repeated rounds of hashing to create a longer key value.
PBX	Private Branch Exchange	The point of interface between the public switched telephone network and an organization's internal telephony.
PCAP	Packet Capture	Sniffing and recording network data into a file for later analysis.
PCI DSS	Payment Card Industry Data Security Standard	A nongovernmental security standard that regulates the implementation and security of web payment gateways.
PDU	Power Distribution Unit	This is a multiple output device that regulates the power supply and its quality to multiple devices within a rack of devices in a data center.
PE	Portable Executable	This is a format for code run by Windows systems and 32 or 64 bit mode.
PEAP	Protected Extensible Authentication Protocol	An EAP form that sends MSCHAP credentials secured within a TLS envelope.
PED	Portable Electronic Device	Small electronics, such as beepers, calendars and note applications used prior to smartphones.
PEM	Privacy-enhanced Electronic Mail	This is one of the oldest formats of certificates and uses Base64.
PFS	Perfect Forward Secrecy	This is the property of Key management where in the loss of one key is not in danger data encrypted with earlier session keys.
PFX	Personal Exchange Format	A binary format for storing or sending server certificates and private keys.
PGP	Pretty Good Privacy	A widely used cryptosystem initially used for securing email by encryption and digital signatures.
PHI	Personal Health Information	Typically sensitive information regarding the health of an individual.
Phishing	Malicious spam	Bogus messaging sent to a wide array of potential targets.
PII	Personally Identifiable Information	This is data or pieces of data that uniquely correspond to or identify one individual and requires special handling.
PIN	Personal Identification Number	Knowledge-based authentication using a single value or number.
PIV	Personal Identity Verification	An identification card that contains a photograph, RFID, barcode, and cryptographically stored PKI information.

Handout 1: CompTIA Security+ Acronyms

Pivot	Staging new attack	Gaining control of one application or host in order to manipulate a secondary target.
PKCS	Public Key Cryptography Standards	Public-key encryption standards developed by RSA Security.
PKI	Public Key Infrastructure	The processes and management associated with the identification and validation of certificates and public keys.
PoC	Proof of Concept	An implementation of an idea or theory that establishes its validity commonly associated with vulnerabilities and exploits.
POODLE	Padding Oracle on Downgrade Legacy Encryption	An attack technique that could subvert confidentiality in an SSL connection.
POP	Post Office Protocol	This protocol listens on TCP/110 and downloads messages from the server.
Port scan	Network mapping and service enumeration	Performing address and host discovery, along with identifying listening applications.
POTS	Plain Old Telephone Service	The old form of telephony that implemented dedicated copper connections vs. packet advised voice transmission.
PPP	Point-to-Point Protocol	This is a layer 2 technology implemented to facilitate communication between endpoints or routers.
PPTP	Point-to-Point Tunneling Protocol	A largely deprecated protocol used for establishing tunnels and securing packet ice communication.
PSK	Pre-shared Key	Managing key establishment and management by using pre-established relationships and non-automatic exchange methods.
PTZ	Pan-Tilt-Zoom	The property of a camera to be able to swivel in various directions on demand.
PUP	Potentially Unwanted Program	Defined by policy, this is software that provides functionality in violation of authorized use.
QA	Quality Assurance	The monitoring and control function an organization that identifies, prevents or corrects errors in processes, procedures or products.
QoS	Quality of Service	A networking function that seeks to reserve bandwidth in order to preserve the timing and availability of communication, especially as it pertains to multimedia.
RA	Recovery Agent	The party in PKI who is capable of obtaining a private key locked away in escrow.
RA	Registration Authority	This is the entry point of a subject into PKI. It is here that a party establishes and verifies identity before obtaining keys.
RACE	Research and Development in Advanced Communications Technologies in Europe	

Handout 1: CompTIA Security+ Acronyms

RAD	Rapid Application Development	A model of application development that very quickly works through the development phases.
RADIUS	Remote Authentication Dial-in User Server	The most common centralized authentication service.
RAID	Redundant Array of Inexpensive Disks	A set of standards that specify varying levels of fault tolerance, performance and system requirements for hard drive data storage.
RAM	Random Access Memory	This is a form of storage that allows specific and independent access to information and does not require a sequential read or write.
Ransomware	Cryptovirology	Requires payment for return of information.
RAS	Remote Access Server	A Microsoft specific term that relates to servers that facilitate modem-based access to an intranet.
RAT	Remote Access Trojan	Software that implements illicit remote control software.
RBAC	Role-based Access Control	A model of access control, typically implemented in an inverted tree, where rights float down.
RBAC	Rule-based Access Control	A model of access regulation commonly used for firewalls and physical controls.
RC4	Rivest Cipher version 4	A now deprecated encryption algorithm used by SSL and WEP.
RCS	Rich Communication Services	This is designed to become a successor to SMS messaging that provides communication between phones and carriers.
RDP	Remote Desktop Protocol	Allows access to a system for remote management and help desk operations.
RFC	Request for Comments	Documents that are largely specifications and definitions for entities on the Internet.
RFID	Radio Frequency Identifier	This is a common choice for tracking small devices and objects, as well as doorway access control.
RIPEMD	RACE Integrity Primitives Evaluation Message Digest	This is a hashing algorithm.
RMF	Risk Management Framework	This risk management paradigm was promulgated by the US government.
ROI	Return on Investment	This is the primary metric to be used when evaluating whether something is worth the time, effort or cost.
Rootkit	Enables and hides access	Implemented by an attacker to prevent discovery or observation of activities.
RPO	Recovery Point Objective	A metric that identifies the number of transactions or quantity of data that can be acceptably lost.
RSA	Rivest, Shamir, & Adleman	This algorithm relies on factoring large prime numbers.

Handout 1: CompTIA Security+ Acronyms

RTBH	Remotely Triggered Black Hole	Cisco term that refers to a filtering technique that dumps unwanted traffic prior to being received in the target network.
RTO	Recovery Time Objective	A metric that identifies the maximum amount of time allowed for an outage.
RTOS	Real-time Operating System	These are operating systems that work in real-time, such as manufacturing and robotics.
RTP	Real-time Transport Protocol	One of several protocols used for telephony/audio/video.
S/MIME	Secure/Multipurpose Internet Mail Extensions	Developed by RSA, this is a formatting standard originally created for implementing digital signatures and encryption with public key infrastructure.
SaaS	Software as a Service	A minimal cloud asset that allows access to one application or port.
SAE	Simultaneous Authentication of Equals	Based upon Dragonfly, this key management system incorporates elements of Diffie Hellman and is a part of WPA3.
SAML	Security Assertions Markup Language	A method of exchanging credentials via a trusted authentication service.
SAN	Storage Area Network	A remote file system access via Internet-based protocols.
SAN	Subject Alternative Name	Embedding multiple names for server within a single certificate.
SASE	Secure Access Service Edge	Technology that delivers network and security controls as a cloud computing service directly to the source of connection rather than a data center.
SCADA	System Control and Data Acquisition	Industrial controls automation the network-based management systems that control many remote, small, embedded devices.
SCAP	Security Content Automation Protocol	This is a framework promoted by the US government to create open standards for the automation of information assurance.
SCEP	Simple Certificate Enrollment Protocol	This is a technology that is highly resistant to dictionary attacks and is designed to replace Pre-shared Keys and WPA2-Personal.
SCP	Secure Copy	A command line application that will securely upload or download files to work from a remote host.
SCSI	Small Computer System Interface	A host bus interface to connect to multiple hard drives.
SDK	Software Development Kit	Tools, APIs and applications created by a vendor to allow development and customization.
SDLC	Software Development Life Cycle	The sequence of processes involved in the creation and management of software.

Handout 1: CompTIA Security+ Acronyms

SDLM	Software Development Life-cycle Methodology	The stages or phases of a software-based application as it goes from inception to maintenance.
SDN	Software Defined Network	Using virtualization to create, manage and secure networks between various systems.
SDP	Service Delivery Platform	The elements that provide service delivery, session management and other key components to a client.
SDV	Software-defined Visibility	The capability implemented with software that allows for the organization to closely inspect network traffic from an array of collectors and sensors.
SE Linux	Security-enhanced Linux	A Linux kernel security module that provides a mechanism for supporting extended access control security policies, such as mandatory access controls (MAC).
SED	Self-Encrypting Drives	Storage devices that are capable of implementing high-grade encryption without additional software or resources.
SFTP	Secured File Transfer Protocol	This application runs over TCP/22 and encrypts control and data functions.
SHA	Secure Hashing Algorithm	A now deprecated hashing algorithm that has been in very common use.
SHE	Structured Exception Handler	This is the facility within Windows that identifies memory corruption and contingencies.
SHTTP	Secure Hypertext Transfer Protocol	An obsolete alternative to the HTTPS protocol.
SIEM	Security Information and Event Management	These servers collect, aggregate and analyze data from multiple sources to identify threats and dangerous trends.
SIM	Subscriber Identity Module	An integrated circuit that identifies a phone and subscriber.
SIP	Session Initiation Protocol	This is used to signal, start up, maintain and terminate real-time communication services between endpoints using Internet protocol.
SLA	Service Level Agreement	An agreement on the characteristics of quality and performance between two parties.
SLE	Single Loss Expectancy	The value of an asset multiplied times the exposure factor.
SMB	Server Message Block	This is a core Microsoft protocol used for general access and authentication.
SMS	Short Message Service	Protocol used by cell phones to exchange brief text-based messages.
SMTP	Simple Mail Transfer Protocol	The vulnerable application responsible for forwarding email to a destination server or receiving it from a sender.
SMTPS	Simple Mail Transfer Protocol Secure	The secured application responsible for forwarding email to a destination server or receiving it from a sender.

Handout 1: CompTIA Security+ Acronyms

SNMP	Simple Network Management Protocol	A network-based application designed to discover device status, change configuration and receive errors and exceptions.
SOAP	Simple Object Access Protocol	The structured markup used to identify components of service oriented architecture messages.
SOAR	Security Orchestration, Automation, Response	A software architecture designed to allow an organization to collect and analyze threat information from numerous sources and inputs, as well as respond to incidents
SoC	System on Chip	The minimization of an application and operating system to a state that will fit on an integrated circuit.
SOC	Security Operations Center	This is a hub of operations and communication that focuses on security incidents and management at a technical level.
SOW	Statement of Work	It is a narrative description of a project's work requirement.
SPF	Sender Policy Framework	An email validation architecture designed to detect and eliminate spoofing and spamming through approved mail exchangers.
SPIM	Spam over Internet Messaging	Chat messages delivered as a hoax were to induce purchase.
SPIT	Spam over Internet Telephony	The use of SMS to deliver unwanted messages.
SPoF	Single Point of Failure	A device, business process or person that is critical to a business and has no redundancy.
SQL	Structured Query Language	An industry-standard mass information repository retrieval system.
SQLi	SQL injection	Manipulation of input to the front end of a server in order to gain access to the data repositories.
SRTP	Secure Real-Time Protocol	A secure form of Internet protocol-based telephony.
SSD	Solid State Drive	Nonvolatile storage using persistent solid-state flash memory to store and retrieve information.
SSH	Secure Shell	This protocol, runs over TCP/22 and encrypts its exchanges.
SSID	Service Set Identifier	An identifier for a wireless network.
SSL	Secure Sockets Layer	A certificate-based authentication and encryption application that would securely process any TCP-based layer 7 protocol.
SSO	Single Sign-on	An authentication architecture that relies on a central system and it's authentication to authorize users for other services using a single set of credentials.
Stego	Stenography	The obfuscation of information within a common looking format that achieves stealth.

Handout 1: CompTIA Security+ Acronyms

STIX	Structured Threat Information eXpression	Developed by OASIS and MITRE, this is an international standard for sharing intelligence and threat information
STP	Shielded Twisted Pair	Four pairs of wires wrapped in foil that is grounded to prevent interference and eavesdropping.
SWG	Secure Web Gateway	A system used by enterprises to protect the intranet from hostile or unsecured traffic, commonly implemented in a cloud-based solution.
Symmetric key	Secret key	The use of a single value to hide and then reveal information.
TACACS+	Terminal Access Controller Access Control System Plus	This was initially used by Cisco as centralized authentication for its routers and switches.
TAXII	Trusted Automated eXchange of Indicator Information	This defines four different services (discovery, collection, inbox and polling) for the purpose of sharing intelligence and threat information between organizations.
TCP	Transmission Control Protocol	An upper layer protocol that requires handshakes, acknowledgments and a graceful close.
TCPDump	Wireshark alternative	It is a command Linux based network analysis tool.
TGT	Ticket Granting Ticket	This is returned after a user successfully. Authenticates to a KDC.
TKIP	Temporal Key Integrity Protocol	A protocol for key management and change used by WPA.
TLS	Transport Layer Security	This is now incorporated into HTTPS and allows for AES and other more recent cryptographic algorithms.
TOC	Time-of-check	The time point when information is tested for validity and later use.
TOTP	Time-based One-time Password	A physical token-based authentication system with an access code that changes regularly.
TOU	Time-of-use	The point in time when information is fetched and employed.
TPM	Trusted Platform Module	A cryptographic chipset that contains key information to allow encryption and ensure device integrity.
Trojan	Trojan horse	This is a methodology of approaching a target by disguising one thing or activity is something trustworthy to achieve insertion.
TSIG	Transaction Signature	The component of the name resolution message that performs authentication in DNSSEC.
TTP	Tactics, Techniques, and Procedures	A reference to the patterns of actions or methods that can be associated with specific threat actors.
UAT	User Acceptance Testing	This is the phase of development wherein the client decides if it is correct.
UAV	Unmanned Aerial Vehicle	Remotely piloted aircraft.

Handout 1: CompTIA Security+ Acronyms

UDP	User Datagram Protocol	A datagram protocol that has no handshake, close or acknowledgment requirement.
UDP	User Datagram Protocol	An upper layer protocol that does not require acknowledgment.
UEBA	User and Entity Behavior Analytics	The tools and resources used to analyze insider threats and to proactively prevent fraud and exfiltration.
UEFI	Unified Extensible Firmware Interface	The modern solution for the boot up environment of computer.
UEM	Unified Endpoint Management	Software that may be implemented to protect devices, servers and other endpoints from a variety of threats that can be managed from a single interface.
UPS	Uninterruptable Power Supply	This is typically a battery-powered device that provides temporary electric support.
URI	Uniform Resource Identifier	This is the file/resource portion of an URL, typically located at the end.
USB	Universal Serial Bus	Multiplatform specification for integrating peripherals into computer systems.
USB OTG	USB On The Go	An extension of the USB specification that allows it to integrate with devices such as tablets and smart phones.
UTM	Unified Threat Management	This is a multifunction firewall system, commonly supporting VPN, NAT, antivirus, spam filtering, intrusion detection and content filtering.
UTP	Unshielded Twisted Pair	Commonly known as four-pair, in ubiquitous use for data networking wired connections.
VA	Vulnerability assessment	An operational defense designed to proactively discover flaws, incorrect configurations and outdated applications.
VBA	Visual Basic	An old Microsoft programming language.
VDE	Virtual Desktop Environment	Hosting a desktop operating system on a centralized server and allowing users to remotely access it.
VDI	Virtual Desktop Infrastructure	Hosting a desktop operating system on a centralized server and allowing users to remotely access it.
VLAN	Virtual Local Area Network	A technology for isolating and nodes attached to switches into various groups to enhance performance and create isolation-based security.
VLSM	Variable-length Subnet Masking	An IP network masking technique that does not require full bytes in each position of the mask.
VM	Virtual Machine	The implementation of an operating system within an application running on top of another host.
VoIP	Voice over IP	Converting analog sound into packet eyes data for efficient transport over the Internet.
VPC	Virtual Private Cloud	An implementation of cloud computing where in the cloud service provider reserves resources for particular group or customer, providing isolation.

Handout 1: CompTIA Security+ Acronyms

VPN	Virtual Private Network	The transmission of information in a protected form over potentially hostile mediums.
VTC	Video Teleconferencing	Video or audio conductivity between remote sites.
WAF	Web Application Firewall	A filtering device designed to perform deep content inspection to identify application threats.
WAP	Wireless Access Point	The hub of communication in a radio-based data network.
WEP	Wired Equivalent Privacy	The now deprecated authentication and confidentiality measures used by 802.11 networks.
WIDS	Wireless Intrusion Detection System	This is an intrusion sensor that looks for 802.11-related threats.
WIPS	Wireless Intrusion Prevention System	This is an intrusion sensor that stops 802.11-related threats.
WO	Work Order	An authorization or request for labor or an operation.
WORM	Write Once Read Many	One-way writing of logs and performance data.
Worm	Massive propagation messages	Self-propagating malicious software that floods a network, causing a denial of service.
WPA	WiFi Protected Access	The predecessor to WPA/2 that implemented TKIP.
WPA2	WiFi Protected Access 2	The successor to WPA that incorporates AES-CCMP.
WPS	WiFi Protected Setup	New clients may gain access by pushing a button.
WTLS	Wireless TLS	A security layer for the Wireless Application Protocol.
x.509v3	Schema of identification document.	Definition and structure for server, host, and personal identification.
XaaS	Anything as a Service	A broad term that refers to accessing any type of service, large or small, via the Internet and it is commonly associated with cloud computing.
XDR	Extended Detection and Response	The purpose of WTLS is to provide privacy, data integrity and authentication with systems communicating using an access point.
XML	Extensible Markup Language	A text-based language that defines the encoding of documents and data so that it is both human readable and machine readable, commonly associated with web services.
XOR	Exclusive Or	A mathematical bit -wise operation, commonly employed in encryption.
XSRF	Cross-site Request Forgery	An attack wherein a message is spoofed from a user to a trusted site.
XSS	Cross-site Scripting	Web application attack that relies on malicious user, script input to steal information from other users.

Handout 1: CompTIA Security+ Acronyms