Quiz 1-2

Social engineering factors:

* Authority
* Familiarity
* Urgency
* Consensus
* Scarcity
* Trust

Quiz 3

KPA: Known Plaintext Attack: having the cleartext and encrypted text.

Bluesnarfing: gaining control of a Bluetooth device

Bluejacking: sending unsolicited data over Bluetooth

Padding Oracle On Downgraded Legacy Encryption “POODLE” is an example of a cryptographic downgrade attack.

Quiz 4: 91.89%

Types of threats:

* Script kiddie
* APT (Advanced Persistent Threat)
* Nation states
* Organized crime
* Hacktivist
* Inside job
* Competitors

OSINT: Open-source Intelligence

Quiz 5: 85.71%

“System sprawl”

Tunnel mode: IPsec mode providing complete packet encryption

Transport mode: IPsec provides encryption of payload only

[Quiz 6](https://www.examcompass.com/comptia-security-plus-practice-test-6-exam-sy0-501): 88.89%

NIPS: network security solution inspects network traffic in real-time and has the capability to stop the ongoing attack

NIDS:

IEEE802.1X: an Ethernet switch acts as an authenticator for devices that intend to connect to a network through one of its ports

RSTP: Rapid Spanning Tree Protocol (RSTP) is a network protocol that ensures a loop-free topology for Ethernet networks. This protocol is incorporated into IEEE 802.1Q-2014.

[Quiz 7](https://www.examcompass.com/comptia-security-plus-practice-test-7-exam-sy0-501): 89.29%

Load balancing methods:

* Round-robin method: each consecutive request is handled by next server in a cluster
* Weighted round-robin: each consecutive request is handled in a rotational fashion, but servers with higher specs are designated to process more workload
* Session affinity: ignores the load balancing algorithm by consistently passing requests from a given client to the same server
* Active-active method: load balancers distribute network traffic across all servers
* Active-passive method: load balancers distribute network traffic across servers marked as active
* Least configuration method

LACP: Link aggregation control protocol (Ethernet 802.3ad)

DSCP: Differentiated Services Code Point (DSCP) is a means of classifying and managing network traffic and of providing quality of service (QoS) in modern Layer 3 IP networks. It uses the 6-bit Differentiated Services (DS) field in the IP header for the purpose of packet classification.

* SIEM: A technology that allows for real-time analysis of security alerts generated by network hardware and applications

LWAPP: Lightweight Access Point Protocol (LWAPP) is the name of a protocol that can control multiple Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring or troubleshooting a large network. The system will also allow network administrators to closely analyze the network.

[Quiz 8](https://www.examcompass.com/comptia-security-plus-practice-test-8-exam-sy0-501): 75% (retake: 100%)

DLP: Data Loss Prevention, the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data. Organizations use DLP to protect and secure their data and comply with regulations. Can implement USB blocking, email monitoring, cloud-based security.

pfSense

John the Ripper, Cain & Abel: password cracking software

OpenVAS: offers the functionality of a vulnerability scanner

Nessus: the functionality of a configuration compliance scanner

[Quiz 9](https://www.examcompass.com/comptia-security-plus-practice-test-9-exam-sy0-501): 92.59%

Zenmap: the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application.

Nmap: command-line tool is used for discovering hosts and services on a network

[Quiz 10](https://www.examcompass.com/comptia-security-plus-practice-test-10-exam-sy0-501): 93.94%

UTM: Unified threat management, commonly abbreviated as UTM, is an information security term that refers to a single security solution, and usually a single security appliance, that provides multiple security functions at a single point on the network.

WAF: A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.

[Quiz 11](https://www.examcompass.com/comptia-security-plus-practice-test-11-exam-sy0-501): 92%

In the context of MDM, the isolation of corporate applications and data from other parts of the mobile device is known as containerization.

A mobile security solution that enables separate controls over the user and enterprise data is called storage segmentation.

[Quiz 12](https://www.examcompass.com/comptia-security-plus-practice-test-12-exam-sy0-501): 89.19%

SRTP: enables secure, real-time delivery of audio and video over an IP network

POP3S: TCP port 995

Secure IMAP: TCP 993

SMTPS: refers to a deprecated TLS-based method for securing SMTP

[Quiz 13](https://www.examcompass.com/comptia-security-plus-practice-test-13-exam-sy0-501): 100% - Fátima!

[Quiz 14](https://www.examcompass.com/comptia-security-plus-practice-test-14-exam-sy0-501): 88.89%

SDN: a technology designed to simplify network infrastructure management

SSP:  
SEH:

FDE: a software technology designed to provide confidentiality for an entire data storage device

SED: a data storage device equipped with a hardware-level encryption functionality

[Quiz 15](https://www.examcompass.com/comptia-security-plus-practice-test-15-exam-sy0-501): 86.67%

Protect against SQL injection attacks with input validation and stored procedures.

[Quiz 16](https://www.examcompass.com/comptia-security-plus-practice-test-16-exam-sy0-501): 90.32%

PaaS: the best solution for a web developer intending to create a web app. Platform as a service (PaaS) is a cloud computing model in which a third-party provider delivers hardware and software tools -- usually those needed for application development -- to users over the internet. A PaaS provider hosts the hardware and software on its own infrastructure.

CASB: a security policy enforcement software tool or service placed between cloud service users and cloud applications

[Quiz 17](https://www.examcompass.com/comptia-security-plus-practice-test-17-exam-sy0-501): 87.88%

[Quiz 18](https://www.examcompass.com/comptia-security-plus-practice-test-18-exam-sy0-501): 90.63%

RADIUS: Combines authentication and authorization, Primarily used for network access, Encrypts only the password in the access-request packet.

OAuth is an open standard for authorization.

Shibboleth: SAML-based Single Sign-On (SSO) system

[Quiz 19](https://www.examcompass.com/comptia-security-plus-practice-test-19-exam-sy0-501): 77.78%

**FALSE**: Higher CER values are characteristic features of more accurate biometric security systems

Examples of implementation methods for certificate-based authentication include:

* PIV card
* CAC: A Common Access Card (CAC) is a smart card used for identification of active-duty military personnel, selected reserve, US Department of Defence (DoD) civilian employees and eligible contractor personnel.
* IEEE 802.1X

BPA: a key document governing the relationship between two business organizations

ISA: A type of agreement that documents technical and security requirements of the interconnection between the organizations that own and operate connected IT systems

A general document established between two or more parties to define their respective responsibilities and expectations in accomplishing a particular goal or mission:

* MOU: A memorandum of understanding is a type of agreement between two or more parties. It expresses a convergence of will between the parties, indicating an intended common line of action.
* MOA: A Memorandum of Agreement (MOA) is a written document describing a cooperative relationship between two parties wishing to work together on a project or to meet an agreed upon objective. An MOA serves as a legal document and describes the terms and details of the partnership agreement.

[Quiz 20](https://www.examcompass.com/comptia-security-plus-practice-test-20-exam-sy0-501): 84%

RTO: Recovery Time Objective: a maximum tolerable period of time required for restoring business functions after a failure or disaster

RPO: Recovery Point Objective: In business continuity planning, the maximum tolerable point in time to which systems and data must be recovered after an outage

ARO: Acceptable Risk of Overreliance: In quantitative risk assessment, this term is used for estimating the likelihood of occurrence of a future threat.

MTO: Maximum Tolerable Outage

[Quiz 21](https://www.examcompass.com/comptia-security-plus-practice-test-21-exam-sy0-501): 90.7%

ECB: block cipher mode is the simplest/weakest and therefore not recommended for use.

[Quiz 22](https://www.examcompass.com/comptia-security-plus-practice-test-22-exam-sy0-501): 82.5%

Confusion: used in conjunction with the assumption that the output of a cryptographic function should be considerably different from the corresponding plaintext input

PFS: Perfect Forward Secrecy (PFS), 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.

[Quiz 23](https://www.examcompass.com/comptia-security-plus-practice-test-23-exam-sy0-501): 63.64%

Examples of key stretching algorithms: Bcrypt, PBKDF2

CCMP: AES-based encryption mode implemented in WPA2

TKIP: A security protocol designed to strengthen WEP implementations

[Quiz 24](https://www.examcompass.com/comptia-security-plus-practice-test-24-exam-sy0-501): 82.35%

DER: used to store a binary representation of a digital certificate

PFX, P12: digital certificate formats commonly used to store private keys