CySA + Key Terms

TACACS+ - TACACS+ is an extension to TACACS (Terminal Access Controller Access Control System) and was developed as a proprietary protocol by Cisco.

RADIUS - The Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that operates on port 1812 and provides centralized Authentication, Authorization, and Accounting management for users who connect and use a network service, but Cisco did not develop it.

Kerberos - Kerberos is a network authentication protocol designed to provide strong mutual authentication for client/server applications using secret-key cryptography developed by MIT.

(CHAP) Challenge-Handshake Auth Protocol - CHAP is an authentication protocol but does not provide authorization or accounting services.

(TLS) Transport Layer Security - is a widely adopted security protocol designed to facilitate privacy and data security for communications over the internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website.

SSL - Deprecated. TLS is used, terms are used interchangeably.

OpenSSL 1.0.1g - Patched notorious heartbleed bug.

TOGAF Framework - TOGAF is a prescriptive framework that divides the enterprise architecture into four domains. Technical architecture describes the infrastructure needed to support the other architectural domains. Business architecture defines governance and organization and explains the interaction between enterprise architecture and business strategy. Applications architecture includes the applications and systems an organization deploys, the interactions between those systems, and their relation to the business processes. Data architecture provides the organization’s approach to storing and managing information assets. This question may seem beyond the scope of the exam. Still, the objectives allow for "other examples of technologies, processes, or tasks about each objective may also be included on

the exam although not listed or covered" in the objectives' bulletized lists. The exam tests the equivalent of 4 years of hands-on experience in a technical cybersecurity job role.

Fuzzing - Fuzzing is an automated software assessment technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions (crashes), failing built-in code assertions, or finding potential memory leaks.

Address space layout randomization (ASLR) - makes it harder to buffer overflow.

STIX Protocol - STIX (Structured Threat Information eXpression) is a standardized XML programming language for conveying data about cybersecurity threats in a common language that can be easily understood by humans and security technologies

(CDN) Content Delivery Network - A content delivery network (CDN) is a geographically distributed network of proxy servers and their data centers that provide high availability and performance by distributing the service spatially relative to end-users.

Prowler - is an exploitation framework that is used to test the security configurations of an AWS account.

OpenVAS - OpenVAS is a general-purpose vulnerability scanner but does not deal with cloud-specific issues.

ScoutSuite - is used to audit instances and policies created on multi-cloud platforms.

Port 515, 631, 9100 - ports used for printers.

Formal verification methods - are designed for use in critical software in which corner cases must be eliminated. Single greatest mitigation against a threat.

(SOAR) Security orchestration, automation, and response - is used to facilitate incident response, threat hunting, and security configuration by orchestrating automated runbooks and delivering data enrichment. A SOAR may be implemented as a standalone technology or integrated within a SIEM as a next-gen SIEM.

CVSS Metrics - the base metric is composed of 8 factors: access vector (AV), access complexity (AC), privileges required (PR), user interaction (UI), scope (S), confidentiality (C), integrity (I), and availability (A).

Root Cause Analysis - A root cause analysis provides a deep dive into what allowed the incident to occur, helping to identify vulnerabilities and procedural shortcomings.

Strcopy vulns - C, C++ strcopy command has buffer overflow vulns. Convert os to run ASLR to prevent.

XCCDF (extensible configuration checklist description format) - is a language that is used in creating checklists for reporting results.

What do vuln scanners commonly use? - Service and version identification are often performed by conducting a banner grab or by checking responses for services to known fingerprints for those services. UDP response timing and other TCP/IP stack fingerprinting techniques are used to identify operating systems only. Using nmap -O will conduct an operating system fingerprint scan, but it will not identify the other services being run.

Oauth2 - explicitly designed to auth claims.

OpenID Connect - is an auth protocol that can be implemented with oauth.

Security Assertion Markup Language (SAML) - is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is an XML-based markup language for security assertions.

Jumpbox - single point of entry for administration of servers.

Bastion Host - a special-purpose computer on a network specifically designed and configured to withstand attacks.

Beaconing - Network indicator of compromise.

Drupal 7.58/8.5.1 - patched CVE-2018-7600 or drupalgeddon2.

Infrastructure as Code IaC - IaC is designed with the idea that a well-coded description of the server/network operating environment will produce consistent results across an enterprise and

significantly reduce IT overhead costs through automation while precluding the existence of security vulnerabilities.

(DLP) - Data loss prevention (DLP) software detects potential data breaches/data exfiltration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while in-use, in-motion, and at-rest.

Network Access Control - prevents unauthed users from connecting to a network.