Roma Tre

CONCORSO AM1CTEC24

PROVA 1

Quesito 1

Il candidato descriva l'implementazione di una politica di backup efficace, tenendo conto della sicurezza, della disponibilità e della continuità operativa.

Quesito 2

Il candidato descriva i principali criteri da considerare nella scelta di un'architettura software per un sistema informativo, analizzando aspetti come scalabilità, manutenibilità, sicurezza e interoperabilità.

Quesito 3

Il candidato descriva la figura del dirigente e le principali competenze.

Quesito 4

Leggere e tradurre il seguente testo

Computer security (also cybersecurity, digital security, or information technology (IT) security) is a subdiscipline within the field of information security. It consists of the protection of computer software, systems and networks from threats that can lead to unauthorized information disclosure, theft or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide.

The significance of the field stems from the expanded reliance on computer systems, the Internet, and wireless network standards. Its importance is further amplified by the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity has emerged as one of the most significant new challenges facing the contemporary world, due to both the complexity of information systems and the societies they support. Security is particularly crucial for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance.

Roma Tre

CONCORSO AM1CTEC24

PROVA 2

Quesito 1

Il candidato illustri il ruolo dei log di sistema nella sicurezza informatica. Quali informazioni dovrebbero essere registrate e come andrebbero gestiti per garantire integrità e riservatezza?

Quesito 2

Il candidato descriva le fasi principali del ciclo di vita di un sistema informativo (ad esempio SDLC - System Development Life Cycle) spiegando il ruolo di ciascuna fase e come si integrano tra loro.

Quesito 3

Il candidato descriva le principali funzioni del Senato Accademico dell'Università degli Studi Roma Tre

Quesito 4

Leggere e tradurre il seguente testo

A vulnerability refers to a flaw in the structure, execution, functioning, or internal oversight of a computer or system that compromises its security. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database. An exploitable vulnerability is one for which at least one working attack or exploit exists. Actors maliciously seeking vulnerabilities are known as threats. Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using automated tools or customized scripts.

Various people or parties are vulnerable to cyber attacks; however, different groups are likely to experience different types of attacks more than others.

Roma Tre

CONCORSO AM1CTEC24

PROVA 3

Quesito 1

Il candidato descriva come si può implementare un sistema di backup e disaster recovery in un ambiente virtualizzato. Quali strumenti o strategie possono essere adottati?

Quesito 2

Il candidato spieghi il ruolo dell'analisi dei requisiti nella progettazione di un sistema informativo. Come si raccolgono, documentano e validano i requisiti funzionali e non funzionali?

Quesito 3

Il candidato descriva le principali funzioni del Consiglio di Amministrazione dell'Università degli Studi Roma Tre

Quesito 4

Leggere e tradurre il seguente testo

Man-in-the-middle attacks (MITM) involve a malicious attacker trying to intercept, surveil or modify communications between two parties by spoofing one or both party's identities and injecting themselves in-between. Types of MITM attacks include:

IP address spoofing is where the attacker hijacks routing protocols to reroute the targets traffic to a vulnerable network node for traffic interception or injection.

Message spoofing (via email, SMS or OTT messaging) is where the attacker spoofs the identity or carrier service while the target is using messaging protocols like email, SMS or OTT (IP-based) messaging apps. The attacker can then monitor conversations, launch social attacks or trigger zero-day-vulnerabilities to allow for further attacks.

WiFi SSID spoofing is where the attacker simulates a WIFI base station SSID to capture and modify internet traffic and transactions. The attacker can also use local network addressing and reduced network defenses to penetrate the target's firewall by breaching known vulnerabilities. Sometimes known as a Pineapple attack thanks to a popular device. See also Malicious association.

Roma Tre

CONCORSO AM1CTEC24

PROVA 4 non estratta

Quesito 1

Il candidato descriva i principali vantaggi e svantaggi nell'adozione di un'infrastruttura cloud rispetto a una on-premise.

Quesito 2

Il candidato descriva un sistema XDR (Extended Detection and Response) e in che modo avviene l'integrazione con altri strumenti di sicurezza già presenti in un Ateneo, come firewall, antivirus o sistemi di gestione identità.

Quesito 3

Il candidato descriva quali sono le principali figure di governo dell'Università Roma Tre e quali competenze sono attribuite al Rettore secondo lo Statuto.

Quesito 4

Leggere e tradurre il seguente testo

A backdoor in a computer system, a cryptosystem, or an algorithm is any secret method of bypassing normal authentication or security controls. These weaknesses may exist for many reasons, including original design or poor configuration. Due to the nature of backdoors, they are of greater concern to companies and databases as opposed to individuals.

Backdoors may be added by an authorized party to allow some legitimate access or by an attacker for malicious reasons. Criminals often use malware to install backdoors, giving them remote administrative access to a system. Once they have access, cybercriminals can "modify files, steal personal information, install unwanted software, and even take control of the entire computer."

Roma Tre

CONCORSO AM1CTEC24

PROVA 5 non estratta

Quesito 1

Il candidato descriva quali sono le principali differenze tra un sistema informativo centralizzato e uno distribuito. Quali vantaggi e svantaggi comportano in termini di scalabilità, sicurezza e manutenzione?

Quesito 2

Il candidato descriva un progetto di massima per un'infrastruttura virtualizzata per un'università con 500 utenti attivi specificando le tecnologie utilizzate (es. VMware, Hyper-V, KVM), la configurazione hardware minima e le politiche di backup.

Quesito 3

Il candidato descriva come viene nominato il Direttore Generale e quali sono le sue responsabilità nella gestione amministrativa dell'Ateneo.

Quesito 4

Leggere e tradurre il seguente testo

Denial-of-service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users.

Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim's account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of distributed denial-of-service (DDoS) attacks are possible, where the attack comes from a large number of points.

In this case, defending against these attacks is much more difficult. Such attacks can originate from the zombie computers of a botnet or from a range of other possible techniques, including distributed reflective denial-of-service (DRDoS), where innocent systems are fooled into sending traffic to the victim.

With such attacks, the amplification factor makes the attack easier for the attacker because they have to use little bandwidth themselves. To understand why attackers may carry out these attacks, see the 'attacker motivation' section.

Roma Tre

CONCORSO AM1CTEC24

PROVA 6

Quesito 1

Il candidato descriva il concetto di interoperabilità tra sistemi informativi. Quali standard e protocolli possono essere adottati per favorire lo scambio sicuro e coerente di dati tra enti diversi?

Quesito 2

Il candidato descriva come si gestisce la sicurezza in un ambiente virtualizzato. Discuta in generale delle principali minacce (es. VM escape, attacchi laterali) e delle contromisure adottabili.

Quesito 3

Il candidato descriva qual è la composizione e la funzione del Nucleo di Valutazione di Ateneo secondo lo Statuto.

Quesito 4

Leggere e tradurre il seguente testo

A direct-access attack is when an unauthorized user (an attacker) gains physical access to a computer, most likely to directly copy data from it or steal information. Attackers may also compromise security by making operating system modifications, installing software worms, keyloggers, covert listening devices or using wireless microphones. Even when the system is protected by standard security measures, these may be bypassed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and the Trusted Platform Module standard are designed to prevent these attacks.

Direct service attackers are related in concept to direct memory attacks which allow an attacker to gain direct access to a computer's memory. The attacks "take advantage of a feature of modern computers that allows certain devices, such as external hard drives, graphics cards, or network cards, to access the computer's memory directly."