UNIVERSITÀ DEGLI STUDI DI MILANO

CONCORSO PUBBLICO, PER TITOLI ED ESAMI, A N. 1 POSTO DI CATEGORIA C - AREA TECNICA, TECNICO-SCIENTIFICA ED ELABORAZIONE DATI, COMPONENTE DEL TEAM PER LA "PROTEZIONE, INFRASTRUTTURE, SISTEMI, SERVIZI" DELL'UFFICIO DI STAFF SICUREZZA ICT, CON RAPPORTO DI LAVORO SUBORDINATO A TEMPO INDETERMINATO, PRESSO LA DIREZIONE GENERALE, UFFICIO DI STAFF SICUREZZA ICT - BANDITO CON DETERMINA NR. 10632/2019 DEL 20/06/2019 E PUBBLICATO SULLA G.U. NR. 51 DEL 28/06/2019 - CODICE 20145

La Commissione giudicatrice del concorso, nominata con determina n. 13585/2019 dell'1/08/2019 e così composta:

DOTT.SSA DIOMEDE NICLA IVANA - PRESIDENTE

DOTT.SSA ZANARDINI FEDERICA - COMPONENTE

DOTT. DE VARDA MICHELE - COMPONENTE

DOTT. FERRARO DOMENICO - SEGRETARIO

comunica le tracce relative alla prova scritta:

TEMA n. 1

1) Una rete universitaria eroga tutti i servizi informatici centralmente con le seguenti modalità:
- alcuni servizi come ad esempio il portale di Ateneo devono essere raggiungibili da ovunque;
- alcuni servizi devono essere accessibili da tutto il personale solo dalla Intranet di Ateneo;
- i server devono essere gestiti solo dal personale dell'IT e sono ospitati in due siti geograficamente separati e configurati in modalità di alta affidabilità.

Si fornisca uno schema logico di sicurezza di una possibile implementazione di tale richiesta soffermandosi sulle componenti tecnologiche da utilizzare per la protezione dei server.

2) La struttura centrale che si occupa della sicurezza informatica di un ateneo deve effettuare l'attività di analisi e verifica della vulnerabilità su tutti i server centrali ospitati nella server farm di ateneo. Descrivere cosa si intende per vulnerabilty assessment e indicarne le varie fasi.

3) Un docente segnala di aver ricevuto la seguente mail:
"Caro utente, è stato rilevato un problema con il tuo account. Per evitare che il tuo account venga sospeso riconnettiti con questo link"
Il candidato identifichi i principali passi necessari per la verifica della bontà della mail e la procedura da seguire in caso si tratti di campagna malevola.

4) Ti informano del fatto che il sito di un dipartimento realizzato su piattaforma CMS WordPress potrebbe essere vulnerabile ad attacchi di tipo XSS. In cosa consiste questo tipo di minaccia? Quali operazioni effettueresti per verificare se il sito sia effettivamente vulnerabile?

TEMA n. 2

1) Descrivere brevemente le caratteristiche generali di un application Firewall e chiarire i vantaggi che si hanno utilizzando questo tipo di tecnologia per proteggere unaweb farm di Ateneo.

2) Quale può essere lo scopo dell'attività di port scanning su una sottorete di Ateneo? Qual è la principale differenza tra un port scanning TCP rispetto ad uno UDP? Quali sono le possibili risposte di una porta host ad un tentativo di scansione e cosa si può dedurre?

3) Un utente segnala di aver ricevuto una mail contenente un allegato con il seguente testo:
Gentile Cliente,

Le inviamo come da Lei richiesto la fattura del 01.09.2019. Il documento è disponibile in allegato.
Cordiali Saluti
Descrivere le azioni che si devono compiere per assicurarsi dell'attendibilità della fonte e che l'allegato non sia malevolo.

4) Un gruppo di ricerca deve ottenere l'approvazione di fondi europei per un progetto che tratta dati particolarmente sensibili attraverso interviste registrate in formato digitale. Il bando di partecipazione richiede che vengano illustrate le modalità con cui i partecipanti del progetto tutti interni all'Ateneo acquisiranno, memorizzeranno e condivideranno con gli altri partecipanti questi dati. Descrivere brevemente quali modalità proporreste per completare il bando.

TEMA n. 3

1) Data la seguente configurazione dell'interfaccia di un firewall:
interface XYZ
ip address 172.16.30.0
e le seguenti ACL applicate in ingresso sull'interfaccia
access-list XYZ permit tcp any 172.16.30.0 255.255.255.0 eq 80
access-list XYZ permit tcp any 172.16.30.0 255.255.255.0 eq 443
access-list XYZ permit tcp 192.168.10.0 255.255.255.0 172.16.30.0 255.255.255.0 eq 22
access-list XYZ deny ip any any
Descrivere schematicamente quale traffico è permesso e quale viene bloccato dalla ACL e fornire un contesto possibile in cui questa ACL potrebbe essere applicata.

2) Quali sono i principali vantaggi nell'utilizzo di tool automatici di Vulnerability Assessment in una rete vasta ed eterogenea di un contesto Universitario?
Quali sono le modalità per automatizzare l'individuazione di vulnerabilità? Quali sono le modalità per automatizzare l'individuazione degli Asset (server di Ateneo)?

3) Vi è appena arrivata la comunicazione della compromissione di un sito web di Ateneo in cui i contenuti delle pagine sono stati modificati da malintenzionati. Quali sono le attività principali per la corretta gestione dell'incidente?

4) Quali sono le operazioni essenziali da eseguire per mettere in sicurezza un sito web dinamico realizzato con una piattaforma CMS come ad esempio WordPress?
I temi appena formulati vengono chiusi in apposite buste che vengono sigillate, siglate sui lembi di chiusura dai componenti della Commissione e prese in consegna dal Presidente.

LA COMMISSIONE

DOTT.SSA DIOMEDE NICLA IVANA - PRESIDENTE .....

DOTT.SSA ZANARDINI FEDERICA - COMPONENTE .....

DOTT. DE VARDA MICHELE - COMPONENTE .....

DOTT. FERRARO DOMENICO - SEGRETARIO .....