UNIVERSITÀ DEGLI STUDI DI MILANO

CONCORSO PUBBLICO, PER TITOLI ED ESAMI, A N. 1 POSTO DI CATEGORIA D - AREA TECNICA,TECNICO-SCIENTIFICA ED ELABORAZIONE DATI, TEAM PER LA "PROTEZIONE INFRASTRUTTURE, SISTEMI, SERVIZI" CON RAPPORTO DI LAVORO SUBORDINATO A TEMPO INDETERMINATO, PRESSO LA DIREZIONE GENERALE UFFICIO DI STAFF SICUREZZA ICT, , PUBBLICATO SULLA G.U. N. 30 DEL 13.04.2018 - CODICE 19192

La Commissione Giudicatrice del concorso, nominata con decreto n. 6494 del 23.05.2018, composta da:

DOTT.SSA DIOMEDE NICLA IVANA - PRESIDENTE

DOTT.SSA ZANARDINI FEDERICA - COMPONENTE

DOTT. DE VARDA MICHELE - COMPONENTE

DOTT.SSA CORNO ANNALISA - SEGRETARIO

Comunica le tracce relative alla prima prova.

TEMA 1

Descrivere sinteticamente 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.

TEMA 2

Considerare i servizi applicativi di un Ateneo che offre 3 tipologie di servizi verso gli Utenti in cloud interno:

- servizi di e-learning rivolti agli studenti (video lezioni, test on line) e accessibile da Internet.
- Servizi per l'amministrazione (gestione del personale, contabilità e fatturazione, etc) consultabili solo dalla intranet
- Servizi per la ricerca (risorse di calcolo, storage, etc)

Descrivere i principali criteri di sicurezza con cui devono essere sviluppate e mantenute le tre tipologie di applicazioni, i requisiti di sicurezza dei servizi e le modalità per garantire la corretta fruizione e la protezione dei dati e le modalità con cui verificare il livello di sicurezza conseguito.

TEMA 3

Descrivere le possibili soluzioni architetturali, i meccanismi e gli algoritmi/protocolli per la protezione di file con dati ad alto livello di criticità (ad esempio si consideri il caso di dati "sensibili") archiviati in un formato scelto dal Candidato e memorizzato su un server esposto su Internet. Il candidato illustri le soluzioni utili a ridurre il rischio, facendo un'analisi costo benefici.

La Commissione comunica le tracce relative alla seconda prova.

TEMA 1

1. Si consideri un servizio esposto su porta 80. Il candidato descriva lo stato dell'arte delle tecniche che potrebbero essere sfruttate per effettuare il defacement del sito e le relative contromisure.

2. Partendo dal ciclo di vita del software, si illustri l'importanza dal punto di vista della sicurezza dell'utilizzo di tecniche di test e di debug del software e si diano degli esempi.

3. Descrivere sinteticamente come funziona la crittografia simmetrica indicando quali algoritmi sono ad oggi più affidabili, motivando la risposta

.

TEMA 2

1. Definire le procedure e i meccanismi di sicurezza configurabili o supportati in modo nativo dal sistema operativo in un contesto Windows e/o Unix based, e come sfruttare tali meccanismi in modo automatico al fine avere un controllo completo sulla sicurezza del Sistema e fornire un riscontro sul buon funzionamento dello stesso.

2. Descrivere cosa si intende per Security Information and Event Management (SIEM), quali sono le sue caratteristiche, le sue potenzialità e i suoi benefici. Si descriva una possibile architettura SIEM all'interno di una grande rete Universitaria.

3. Spiegare cosa si intende per SQL injection e quali metodi si utilizzano nello sviluppo di codice per prevenirlo.

TEMA 3

1. Definire i sistemi adottabili per la difesa dai malware e quindi utili a controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'Università, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

2. Dato un file di log di un firewall nel formato:

timestamp IP_sorgente IP_destinazione DENY/PERMIT

Scrivere un esempio di codice nel linguaggio desiderato per leggere il file, estrarne data e ora, indirizzo IP sorgente e destinazione. La routine deve mandare un alert, ad esempio una mail, se lo stesso IP sorgente compare più di 5 volte nell'intervallo di 5 minuti in un log di tipo DENY.

3. Descrivere cosa si intende per VPN e descrivere in dettaglio almeno 2 tipologie di VPN facendo riferimento agli algoritmi crittografici in uso.

LA COMMISSIONE

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

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

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

DOTT.SSA CORNO ANNALISA - SEGRETARIO .....