CertComp

Syllabus

IT - SECURITY

Introduzione alla Certificazione "IT-SECURITY"

Il Corso di Formazione e Certificazione **IT SECURITY** si basa sulle prerogative della sicurezza informatica, sia dei singoli individui che delle organizzazioni. La sicurezza informatica (cyber security o sicurezza digitale) è riferita a tutte le procedure attuabili per proteggere informazioni (ovvero dati di account, file, immagini, etc.) mediante azioni e pratiche di difesa da attacchi e danni informatici.
Il Corso di Formazione e Certificazione **IT SECURITY** si pone l'obiettivo di trasferire le capacità teoriche e pratiche per un'adeguata protezione e gestione di dati e informazioni.

Il Corso di Formazione e Certificazione **IT-SECURITY** ha una durata complessiva di **200 ore**.
Le ore di Corso di Formazione previste per il didattico sono indicative, in quanto variano in funzione delle competenze, abilità e capacità che il Candidato possiede e delle specifiche aree di Skill previste dal relativo didattico. Il totale tiene conto delle ore complessive di formazione date dalla lettura delle dispense, dall'esecuzione delle esercitazioni, dall'approfondimento sui link di riferimento, dall'integrazione delle eventuali richieste di chiarimenti/spiegazioni al Tutor/Docente e dal numero medio di ore necessarie a superare il TEST di Verifica Finale dell'apprendimento.

Al termine del Corso di formazione viene rilasciato al Candidato l'**Attestato di Frequenza al Corso di Formazione IT-SECURITY.**

Syllabus

- ### Definizione dei domini del Syllabus

In ambito informatico il "dominio" di un esame si riferisce all'insieme di competenze che identificano in modo univoco le conoscenze e competenze rispetto ad una particolare tecnologia, prodotto, logica di processo, attività intellettuale o pratica. Il dominio dell'esame TESI su **IT-SECURITY** è composto da vari elementi, differenti tra loro, che identificano parti specifiche per stabilire le conoscenze in modo globale. Per la costruzione della prova d'esame **"IT-SECURITY",** sono stati nel dettaglio identificati i seguenti **domini e sottodomini** per la composizione dell'Esame:

IT - SECURITY	
Dominio	**Sotto-dominio**
1.0 - Che cos'è la sicurezza informatica	
	1.0.1 La scala delle minacce alla sicurezza informatica
	1.0.2 Le sfide della sicurezza informatica
	1.0.3 Sicurezza dell'applicazione
	1.0.4 Sicurezza sul cloud
	1.0.5 Gestione dell'identità e sicurezza dei dati
	1.0.6 Sicurezza mobile
	1.0.7 Sicurezza della rete
	1.0.8 Disaster recovery e pianificazione della continuità operativa
	1.0.9 Formazione degli utenti
	1.0.10 Criminalità informatica
	1.0.11 I vantaggi della sicurezza informatica
	1.0.12 Triade della CIA
	1.0.13 Chi è un esperto di sicurezza informatica?
	1.0.14 Cosa fa un esperto di sicurezza informatica

2.0 - Gli attacchi informatici	
	2.0.1 Principali tipi di attacchi
	2.0.2 Ruoli IT all'interno dell'azienda
	2.0.3 Cos'è l'hacking etico
	2.0.4 Quali sono i diversi tipi di hacker
	2.0.5 White Hat Hacker vs Black Hat Hacker
	2.0.6 Quali sono i ruoli e le responsabilità di un hacker tecnico
	2.0.7 Principali vantaggi dell'hacking etico
	2.0.8 Cos'è il test di penetrazione
	2.0.9 Cos'è Kali Linux
	2.0.10 Aree di penetration test
	2.0.11 Cos'è SQL injection?
	2.0.12 Come funziona SQL in un sito web
3.0 - I firewall	
	3.0.1 Perché i firewall sono importanti
	3.0.2 Usi chiave dei firewall
	3.0.3 Funzioni del firewall
	3.0.4 Come funziona un firewall
	3.0.5 Tipi di firewall
	3.0.6 Livello applicazione e firewall proxy
	3.0.7 L'importanza di NAT e VPN
	3.0.8 VPN (Rete Privata Virtuale)
	3.0.9 Attacchi interni
4.0 - Vulnerabilità	
	4.0.1 Cos'è un attacco ransomwarer
	4.0.2 Come si svolge un attacco ransomware
	4.0.3 Tipi di ransomware
	4.0.4 Come prevenire gli attacchi ransomware
	4.0.5 Attacchi ransomware popolari nella storia
5.0 - Conoscere la rete	
	5.0.1 Cosa sono le reti informatiche
	5.0.2 Cos'è un indirizzo IP
	5.0.3 Perché utilizzare un indirizzo IP
	5.0.4 Funzionamento di un indirizzo IP
	5.0.5 Versioni dell'indirizzo IP
	5.0.6 Tipi di indirizzi IP
6.0 - prevenzione degli attacchi informatici	
	6.0.1 Tipi di attacchi informatici
	6.0.2 Come prevenire gli attacchi informatici