EUCIP
European Certification of
Informatics Professionals

EUCIP IT Administrator - Modulo 4
IT Security

Syllabus Version 3.0

La versione ufficiale in lingua inglese del syllabus EUCIP *IT Administrator – Modulo 4 – IT Security* è quella pubblicata sul sito web della Fondazione ECDL che si trova all'indirizzo www.eucip.org. La presente versione italiana è stata tradotta a cura di AICA e rilasciata nel mese di dicembre 2014.

EUCIP
European Certification of Informatics Professionals

EUCIP IT Administrator – IT Security

Questo documento presenta il syllabus di *EUCIP IT Administrator – IT Security*. Il syllabus descrive, attraverso i risultati del processo di apprendimento, la conoscenza e le capacità di un candidato che affronti il test per *EUCIP IT Administrator – IT Security*. Il syllabus fornisce inoltre le basi per il test teorico e pratico relativo a questo modulo.

Scopi del modulo

EUCIP IT Administrator – IT Security richiede che il candidato abbia un'ampia comprensione dei concetti relativi alla sicurezza informatica e sia in grado di implementare le misure di sicurezza necessarie ad una rete.

Il candidato dovrà essere in grado di:

- Riconoscere i principali rischi e i principi di gestione della sicurezza; dovrà inoltre conoscere gli standard relativi.
- Riconoscere comuni metodi di cifratura ed essere in grado di applicare i relativi protocolli di crittografia.
- Comprendere i principi di autenticazione a chiave e di controllo di accesso.
- Conoscere i concetti di disponibilità legati alla resilienza e sapere come implementare procedure di copie di sicurezza.
- Comprendere i tipi principali di codice maligno e le minacce; dovrà inoltre essere in grado di proteggere un sistema dagli attacchi.
- Conoscere l'infrastruttura a chiave pubblica e saper applicare i relativi principi.
- Comprendere gli aspetti chiave della sicurezza di rete ed essere in grado di usare firewall, controlli di accesso e gestione dei log.
- Conoscere i principali aspetti sociali, etici e legali della sicurezza informatica.

CATEGORIA	AREA	RIF.	ARGOMENTO
4.1 Gestione della sicurezza	*4.1.1 Concetti fondamentali*	4.1.1.1	Descrivere i principali aspetti della sicurezza dell'informazione: confidenzialità, integrità, disponibilità.
		4.1.1.2	Definire i termini autenticazione e non ripudio.
	4.1.2 Gestione del rischio	4.1.2.1	Riconoscere i principali problemi nell'ambito della valutazione del rischio, quali valore dell'informazione, vulnerabilità, minacce, pericoli, violazioni, impatti, livello di rischio.
		4.1.2.2	Descrivere la relazione tra processi/obiettivi aziendali e gestione del rischio IT; sapere qual è il ruolo della sicurezza IT nella riduzione del rischio.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.1.2.3	Descrivere le funzioni più comuni della sicurezza ad alto livello, quali identificazione e autenticazione, controllo di accesso, responsabilità, ispezioni, riuso degli oggetti, accuratezza, affidabilità del servizio, scambio sicuro di dati.
		4.1.2.4	Saper distinguere tra funzionalità e garanzia, riconoscere l'importanza di raggiungerle entrambe per poter controllare i rischi di sicurezza IT.
	4.1.3 Gestione della sicurezza dell'informazione	4.1.3.1	Descrivere il ruolo di una policy di sicurezza nella conduzione della gestione della sicurezza IT.
		4.1.3.2	Conoscere i processi chiave da implementare in una organizzazione per migliorare la sicurezza dell'informazione, quali ISO/IEC 17799, BS 7799.
		4.1.3.3	Comprendere la necessità per un'organizzazione di pianificare soluzioni di disaster recovery e business continuity.
		4.1.3.4	Definire le responsabilità chiave del personale di un'organizzazione, quali responsabili della sicurezza, amministratori di sistema, normali utenti.
		4.1.3.5	Sapere come partecipare ad un Computer Security Incident Response Team (CSIRT).
	4.1.4 Standard ed enti di normazione	4.1.4.1	Riconoscere i principali enti di normalizzazione e comprendere qual è il loro ruolo.
		4.1.4.2	Riconoscere le metodologie che permettono di valutare i diversi livelli di garanzia (ITSEC, ISO/IEC 15408 - Common Criteria).
		4.1.4.3	Conoscere gli elementi chiave delle norme pubblicate relative all'infrastruttura per la gestione della sicurezza in un'organizzazione, quali ISO/IEC 17799, BS 7799 parte 2.
4.2 Crittografia	*4.2.1 Concetti generali*	4.2.1.1	Comprendere i concetti fondamentali della crittografia, quali testo in chiaro, testo cifrato, algoritmi crittografici.

CATEGORIA	AREA	RIF.	ARGOMENTO
	4.2.2 Cifratura simmetrica	4.2.2.1	Comprendere i principi fondamentali della cifratura simmetrica, quali chiave segreta comune, algoritmi.
		4.2.2.2	Saper distinguere tra i principali standard di cifratura simmetrica, quali DES, 3DES, AES.
	4.2.3 Cifratura asimmetrica	4.2.3.1	Definire i principi fondamentali della cifratura asimmetrica.
		4.2.3.2	Conoscere i principali standard relativi alla chiave pubblica, quali Public Key Cryptography Standard (PKCS) #1, PKCS #7.
	4.2.4 Funzioni di hash e digest	4.2.4.1	Definire i principi fondamentali delle funzioni di hash e digest.
		4.2.4.2	Conoscere i principali standard relativi alle funzioni di hash, quali MD5, SHA1.
	4.2.5 Confronto tra metodi di cifratura	4.2.5.1	Conoscere i vantaggi e gli svantaggi della cifratura simmetrica e asimmetrica.
		4.2.5.2	Comprendere la forza dei diversi metodi di cifratura, sia asimmetrica che simmetrica. Essere consapevoli del concetto di “spazio delle chiavi”.
		4.2.5.3	Comprendere il problema della distribuzione delle chiavi nella crittografia simmetrica e asimmetrica.
		4.2.5.4	Descrivere il ruolo del principio di Kerckhoffs e dell’open source nell’applicazione della disponibilità e robustezza della crittografia.
	4.2.6 Uso	4.2.6.1	Descrivere l’uso dei meccanismi di cifratura, quali le firme digitali per risalire all’autenticità.
		4.2.6.2	Saper distinguere tra la sicurezza di un algoritmo e la sicurezza di un protocollo crittografico.
		4.2.6.3	Descrivere l’uso di hash e digest per ottenere integrità e autenticazione.
		4.2.6.4	Sapere come una firma elettronica implementa il non ripudio e l’autenticazione.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.2.6.5	Comprendere i principi e le caratteristiche fondamentali della cifratura necessari a ottenere la confidenzialità.
	4.2.7 Applicazioni	4.2.7.1	Saper descrivere come si usa la crittografia per proteggere i dati nelle transazioni online.
		4.2.7.2	Installare e impostare il software che gestisce il protocollo PGP.
		4.2.7.3	Comprendere i principi fondamentali di SSH.
		4.2.7.4	Installare e impostare il software che gestisce il protocollo SSH.
		4.2.7.5	Comprendere i principi fondamentali di S/MIME.
		4.2.7.6	Comprendere i principi fondamentali di TLS/SSL.
		4.2.7.7	Comprendere come vengono utilizzate le smartcard.
4.3 Autenticazione e controllo di accesso	*4.3.1 Concetti di autenticazione*	4.3.1.1	Descrivere differenti schemi di autenticazione, quali PAP, CHAP, Kerberos.
		4.3.1.2	Comprendere i principi fondamentali della gestione delle password, quali complessità, memorizzazione, modifiche periodiche.
		4.3.1.3	Descrivere il funzionamento principale dell'autenticazione mediante token.
		4.3.1.4	Saper riconoscere diversi schemi di autenticazione biometrica, quali impronte digitali, scansione dell'iride, riconoscimento vocale.
	4.3.2 Autenticazione di rete	4.3.2.1	Identificare i diversi requisiti per l'autenticazione di rete e su host.
		4.3.2.2	Identificare i diversi schemi di autenticazione via Wi-Fi, quali WEP, WPA e le relative limitazioni.
		4.3.2.3	Identificare diversi protocolli di rete per l'autenticazione di processi distribuiti, quali Kerberos.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.3.2.4	Descrivere la complessità delle architetture ad autenticazione centralizzata (“single sign-on”).
		4.3.2.5	Descrivere i principi fondamentali di funzionamento di Kerberos, quali lo scambio di ticket.
		4.3.2.6	Descrivere il protocollo WSS (Web services-security), lo standard XML-Encryption ed e-Signature.
	4.3.3 Controllo di accesso	4.3.3.1	Conoscere i principali approcci nel controllo di accesso: MAC, DAC, RBAC.
		4.3.3.2	Descrivere cosa sono una Lista di controllo degli accessi (ACL – Access Control List) e un elenco di capacità.
		4.3.3.3	Descrivere come gestire il controllo di accesso nei comuni file system.
		4.3.3.4	Descrivere come gestire il controllo di accesso in un RDBMS (Relational Database Management System).
4.4 Disponibilità	*4.4.1 Concetti di disponibilità*	4.4.1.1	Riconoscere diversi tipi di requisiti relativi alla disponibilità dell’informazione.
		4.4.1.2	Conoscere diversi tipi di requisiti necessari ad una infrastruttura ICT, quali UPS, aria condizionata, cablaggio.
	4.4.2 Resilienza	4.4.2.1	Conoscere diversi tipi di meccanismi di duplicazione di dischi fissi, quali RAID.
		4.4.2.2	Descrivere diversi tipi di duplicazione di host e meccanismi di distribuzione del carico.
		4.4.2.3	Conoscere diversi tipi di infrastrutture per la disponibilità di reti LAN, WAN, WLAN.
	4.4.3 Copie di sicurezza	4.4.3.1	Implementare procedure efficaci di copie di sicurezza locali e di rete.
		4.4.3.2	Verificare una copia di sicurezza e implementare un recupero.

CATEGORIA	AREA	RIF.	ARGOMENTO
4.5 Codice maligno	*4.5.1 Programmi*	4.5.1.1	Sapere come viene operato un computer: sistema operativo, programmi, shell, macro.
		4.5.1.2	Descrivere i requisiti di convalida dell'ingresso dal punto di vista della sicurezza.
		4.5.1.3	Conoscere diversi tipi di overflow e descrivere come possono essere sfruttati per eseguire del codice.
		4.5.1.4	Descrivere i diversi tipi di attacchi nell'interazione browser/webserver, quali cross site scripting.
		4.5.1.5	Descrivere l'attacco di tipo Denial of Service e le modalità con cui può influenzare ambienti e risorse.
		4.5.1.6	Descrivere i diversi metodi di attacco a un computer, quali CD-Rom, messaggi di posta elettronica, navigazione web, client di chat.
		4.5.1.7	Conoscere le modalità corrette per accedere a Internet.
		4.5.1.8	Descrivere i rischi di adware e spyware.
	4.5.2 Gestione automatica dei tipi di file	4.5.2.1	Descrivere come una GUI riconosce quale azione eseguire su un allegato di posta elettronica usando il tipo MIME e l'estensione.
		4.5.2.2	Descrivere come i programmi di posta elettronica riconoscono quale azione eseguire su un allegato di un messaggio usando il tipo MIME e l'estensione.
	4.5.3 Codice scaricabile	4.5.3.1	Descrivere come i tipi MIME possono essere usati in modo doloso e come è possibile difendere un PC da simili attacchi.
		4.5.3.2	Descrivere come le macro possono essere usate in modo doloso e come è possibile difendere un PC da simili attacchi.
		4.5.3.3	Descrivere come le applet possono essere usate in modo doloso e come è possibile difendere un PC da simili attacchi.

CATEGORIA	AREA	RIF.	ARGOMENTO
	4.5.4 Software virale, virus e malware	4.5.4.1	Riconoscere le principali categorie di codici virali, quali trojan, virus, worm.
		4.5.4.2	Comprendere come funziona un programma antivirus.
		4.5.4.3	Descrivere i diversi strumenti che possono essere usati per la protezione contro il malware: antispyware, firewall personali.
		4.5.4.4	Comprendere scopi e limitazioni dei programmi antivirus.
		4.5.4.5	Installare, impostare e aggiornare un programma anti-malware.
4.6 Infrastruttura a chiave pubblica	*4.6.1 Uso della PKI*	4.6.1.1	Essere consapevoli dei problemi di distribuzione della chiave pubblica, quali l'identificazione del proprietario.
		4.6.1.2	Comprendere lo scopo dei Certificati e delle Liste di revoca (CRL – Certificate Revocation Lists).
		4.6.1.3	Descrivere i certificati X.509.V3.
		4.6.1.4	Comprendere l'infrastruttura a chiave pubblica (PKI) e le sue componenti principali: Registration Authority e Certification Authority.
		4.6.1.5	Usare un browser per generare le chiavi e le richieste di certificazione nei confronti di una Certification Authority.
		4.6.1.6	Importare ed esportare un certificato in un browser.
		4.6.1.7	Accedere a una CRL e importarla in un browser.
		4.6.1.8	Usare il protocollo OCSP (Online Certificate Status Protocol).
		4.6.1.9	Saper riconoscere le diverse segnalazioni acustiche e avvertimenti forniti dai browser quando devono mettere in guardia l'utente sulla validità di un certificato.
	4.6.2 Servizi di elenco (Directory)	4.6.2.1	Saper riconoscere il protocollo LDAP (Lightweight Directory Access Protocol).

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.6.2.2	Usare un browser per interrogare un server LDAP per ottenere i dati relativi a un particolare Distinguished Name.
		4.6.2.3	Definire i termini “Common Name”, “Distinguished Name” e “Attributo”.
		4.6.2.4	Descrivere lo stardard X.509 in termini di Certification Authority, struttura del certificato ed estensioni del certificato.
		4.6.2.5	Descrivere come è possibile usare i server LDAP per supportare la gestione del profilo utente e l’autenticazione.
4.7 Sicurezza di rete	*4.7.1 Concetti di telecomunicazione*	4.7.1.1	Comprendere le modalità operative di Ethernet dal punto di vista dell’indirizzo MAC, CSMA/CD.
		4.7.1.2	Comprendere gli aspetti principali del TCP/IP: indirizzi, numeri di porta, flusso principale delle operazioni.
		4.7.1.3	Descrivere l’incapsulamento di TCP/IP in Ethernet.
		4.7.1.4	Descrivere i servizi di rete nell’ambiente TCP/IP.
		4.7.1.5	Installare e gestire un analizzatore di rete.
		4.7.1.6	Descrivere delle principali tipologie di attacco allo stack TCP/IP, quali “sniffing di pacchetti”, “IP spoofing”, “rerouting”, “connection hijacking”, “(distributed) denial of service”.
		4.7.1.7	Descrivere come si possono usare switch e VLAN per organizzare la sicurezza di una LAN.
	4.7.2 Reti wireless	4.7.2.1	Conoscere le principali tecnologie wireless, quali WiFi, Bluetooth, Home Wireless.
		4.7.2.2	Comprendere i problemi di sicurezza relativi alle reti wireless e quali possono essere le possibili soluzioni.
	4.7.3 Servizi	4.7.3.1	Comprendere il concetto di servizi quali punti di accesso ai server.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.7.3.2	Essere a conoscenza degli impieghi illeciti dei servizi, quali utilizzi abusivi, denial of service, contraffazione dei dati.
		4.7.3.3	Essere consapevoli dei rischi legati all'utilizzo fraudolento di DNS.
		4.7.3.4	Essere consapevoli dei principali schemi di autenticazione e delle rispettive vulnerabilità.
		4.7.3.5	Essere consapevoli che debolezze dei protocolli o vulnerabilità nel software possono essere sfruttate per attaccare un server in rete.
		4.7.3.6	Essere consapevoli che i client possono essere vulnerabili quanto i server.
		4.7.3.7	Essere consapevoli dei rischi associati alle tecnologie e ai programmi di tipo peer-to-peer.
	4.7.4 Controllo di accesso	4.7.4.1	Essere consapevoli di come opera l'autenticazione di rete e come viene gestita.
		4.7.4.2	Essere consapevoli di come opera l'autenticazione di rete basata su chiave crittografica e come viene gestita.
		4.7.4.3	Essere consapevoli di come opera l'autenticazione basata su dominio in sistemi di tipo Windows.
	4.7.5 Gestione dei log	4.7.5.1	Riconoscere le informazioni rilevanti per la sicurezza che possono essere ricavate dai log di sistema.
		4.7.5.2	Impostare la registrazione dei log delle applicazioni.
		4.7.5.3	Impostare un servizio centralizzato di registrazione dei log.
		4.7.5.4	Essere consapevoli di come proteggere i log dalle manomissioni.
	4.7.6 Controllo di accesso ai servizi HTTP	4.7.6.1	Comprendere la differenza fra siti web HTTP e HTTPS.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.7.6.2	Comprendere come l'interazione tra il servizio web e gli altri componenti del sistema possa influenzare la sicurezza.
		4.7.6.3	Implementare una versione sicura di un sito web non sicuro, generando chiavi e richieste di certificati; importare chiavi e certificati.
		4.7.6.4	Configurare un sito web in modo che l'identificazione e l'autorizzazione del client avvenga utilizzando password in testo normale.
		4.7.6.5	Configurare un sito web in modo che l'identificazione e l'autorizzazione del client avvenga utilizzando dei certificati, quali SSL V.3.
		4.7.6.6	Riconoscere quali tipi di accessi agli oggetti di una directory possono essere limitati nei siti web.
		4.7.6.7	Applicare le corrette limitazioni di accesso a una specifica directory di un sito web.
	4.7.7 Controllo di accesso ai servizi di posta elettronica	4.7.7.1	Comprendere che è possibile contraffare il mittente ed altre informazioni relative ad un messaggio di posta elettronica.
		4.7.7.2	Impostare un semplice accesso con autenticazione via password sui servizi POP e IMAP.
		4.7.7.3	Impostare un accesso con autenticazione via certificato crittografico sui servizi POP e IMAP.
		4.7.7.4	Impostare l'autenticazione basata su SASL (Simple Authentication and Security Layer) per il servizio SMTP.
		4.7.7.5	Impostare un accesso via tunnel cifrato ai servizi POP e IMAP.
		4.7.7.6	Definire il termine "spam". Illustrare le possibili contromisure.
	4.7.8 Firewall	4.7.8.1	Definire il termine "firewall". Conoscere i limiti e il potenziale di un firewall e saper riconoscere le diverse architetture di firewall, quali gateway, circuiti.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.7.8.2	Definire il termine DMZ (De-Militarized Zone).
		4.7.8.3	Descrivere cosa è un proxy e quali sono le sue modalità operative.
		4.7.8.4	Comprendere come usare un proxy per ridurre il numero di indirizzi IP utilizzati e proteggere una rete interna.
		4.7.8.5	Descrivere cosa è un NAT (Network/Port Address Translation) e in quale modo contribuisce alla sicurezza.
		4.7.8.6	Comprendere i principi di funzionamento dei firewall IP per limitare l'accesso ai servizi IP.
		4.7.8.7	Comprendere i principi di funzionamento dei firewall proxy per limitare e rendere sicura la gestione dei protocolli.
		4.7.8.8	Installare un firewall e un server proxy; implementare una policy di sicurezza.
		4.7.8.9	Nascondere gli indirizzi IP utilizzando un firewall.
		4.7.8.10	Impostare NAT su un firewall.
		4.7.8.11	Impostare le regole di controllo degli accessi su un firewall.
	4.7.9 Intrusion detection	4.7.9.1	Conoscere le categorie fondamentali dei sistemi di rilevamento dei tentativi di intrusione (IDS – Intrusion detection systems) quali IDS di rete, IDS basati su host.
		4.7.9.2	Controllare i log e gli eventi relativi alla sicurezza.
		4.7.9.3	Conoscere i sistemi IPS (Intrusion Prevention Systems) quali IPS di rete, IPS wireless, IPS basati su host.
		4.7.9.4	Installare ed eseguire una configurazione di base di un IDS (Intrusion Detection System).
	4.7.10 Reti private virtuali (VPN)	4.7.10.1	Descrivere i principi dei protocolli IPSEC/IKE.

CATEGORIA	AREA	RIF.	ARGOMENTO
		4.7.10.2	Descrivere le proprietà di sicurezza della separazione del traffico in base a circuito (MPLS).
		4.7.10.3	Descrivere quali livelli di sicurezza possono essere forniti da diverse tecnologie, quali SSL, IPSEC.
		4.7.10.4	Installare un client VPN.
4.8 Aspetti sociali, etici, legali della sicurezza informatica	*4.8.1 Concetti fondamentali*	4.8.1.1	Comprendere i termini “riservatezza” (privacy), “anonimato”, “uso di pseudonimi”.
	4.8.2 Tecnologie di rinforzo alla privacy	4.8.2.1	Riconoscere l’esistenza di un bilanciamento tra autenticazione e privacy.
		4.8.2.2	Comprendere le problematiche etiche legate a tracciamento e sorveglianza sui luoghi di lavoro.
		4.8.2.3	Descrivere gli aspetti principali dei codici deontologici ed etici.
		4.8.2.4	Descrivere gli aspetti principali dell’etica hacker.
		4.8.2.5	Riconoscere le principali forme di crimini informatici, quali cracking, furto d’identità, furto di dati, accessi fraudolenti.
		4.8.2.6	Comprendere i problemi etici e di privacy legati alla biometria.
	4.8.3 Legislazione europea	4.8.3.1	Essere a conoscenza degli aspetti legali della firma digitale e del framework Comunitario relativo alla firma elettronica.
		4.8.3.2	Essere a conoscenza della legge a tutela dei dati personali (Direttiva Europea 95/46) e comprenderne le implicazioni relative al trattamento dei dati personali.
		4.8.3.3	Essere a conoscenza delle principali considerazioni relative all’informatica forense e alla raccolta di prove.