Digital Defense
Corso di Information & Cyber Security

Modulo 1
Linux OS

In questo modulo, gli allievi imparano la conoscenza e l'utilizzo del sistema operativo LINUX. Verranno spiegati ed utilizzati i principali comandi per la gestione del sistema operativo.

Articolazione del modulo formativo

Unità	Ore	Contenuti
1	2	Differenze tra le distribuzioni Linux
2	3	Utilizzo e comandi del "vi"
3	5	TCP/IP base
3	10	Istallazione e configurazione di base
4	10	Configurazione della connessione ssh e X11
5	5	Configurazione di una directory remota in SMB e NFS
5	10	Istallazione e configurazione di Apache
6	25	Programmazione bash shell
TOT	**70**	

Obiettivi

- Acquisire le basi concettuali sistema operativo Linux;
- Acquisire la capacità di gestire del sistema operativo;
- Acquisire la capacità di gestire un servizio erogato da un server linux;
- Acquisire la capacità di utilizzare uno shell script;

Durata oraria

- 70 ore

Conoscenze

- Conoscere le basi concettuali sistema operativo Linux;
- Conoscere la gestione del sistema operativo;
- Conoscere la gestione di un servizio erogato da un server linux;
- Conoscere lo shell scripting;

Competenze da acquisire (sarà in grado di)

- Gestire le principali funzionalità di un sistema operativo Linux;
- Essere in grado di eseguire correttamente un trouble shooting delle attività sistemistiche Linux

Modalità formative

- lezioni frontali, presentazione di casi, ascolto/visione di audiovisivi, hands-on/workshop;

Valutazione dell'apprendimento

- L'efficacia dell'insegnamento impartito verrà valutata attraverso la discussione in aula al termine di ogni unità didattica, tramite test di verifica e/o mediante esecuzione di hands-on/workshop pratici;

Indicatori di padronanza

- Conoscere le principali caratteristiche di un sistema operativo Linux
- Gestire le configurazioni dei servizi erogati da un sistema Linux
- Acquisire la capacità di trouble shooting dei problemi;

Sussidi didattici

- Aula didattica, attrezzature informatiche, software, video proiettore, dispense;

Modulo 2
Network Management

In questo modulo, gli allievi imparano i principi base del TCP/IP.

Articolazione del modulo formativo

Unità	Ore	Contenuti
1	5	Breve storia di Internet. Introduzione alle reti locali. Disegno architetturale di alto livello. Switching: Rete fra 2 hosts. LANs e Hubs, Switches. Switches vs. Routers.
2	25	Configurazione di un Router. Dimensionamento/Subnetting di Reti LAN. Virtual LAN. InterVLAN Routing.
3	25	Protocolli di Routing. Protocolli Distance-Vector. Protocolli Link-State. IGP vs BGP. Routing Information Protocol (RIP); Open Shortest Path First (OSPF); Enhanced Interior Gateway Routing Protocol (EIGRP).
4	15	Configurazione di funzioni di gestione di una rete locale. Dynamic Host Configuration Protocol (DHCP); Network Address Translation (NAT); Access Control List (ACL). Sicurezza nelle reti Ethernet
TOT	**70**	

Obiettivi

- Strutturazione e redazione di progetto tecnico di rete;
- Configurazione e gestione di una infrastruttura di rete;

Durata oraria

- 70 ore

Conoscenze

- Architettura e componenti hardware di PC client e periferiche;
- Nozioni tecniche necessarie per dimensionare correttamente un'architettura di rete locale;
- Dispositivi di networking: server di rete, apparati di rete e cablaggi;
- Concetti relativi alla comunicazione in area LAN, WAN e MAN;
- Elementi base della tecnologia web e dei protocolli di rete cablate e non (TCP/IP ed altri in uso;

Competenze da acquisire (sarà in grado di)

- definire servizi e protocolli di rete da installare, disinstallare, configurare sulle diverse tipologie di apparato;
- identificare tipologia hardware e software di server in relazione alle esigenze del sistema (applicazioni in uso, data base, ecc.);
- tradurre le esigenze di networking in configurazioni della topologia di rete (hardware e software) ed in livelli di servizio (disponibilità, funzionalità, prestazioni, efficacia, efficienza);

- valutare requisiti e funzioni delle di tecnologie di trasmissione e dispositivi di comunicazione (in termini di portata della velocità di trasmissione dati, nodi e lunghezze massime, ecc.) per verificarne potenzialità e limiti;
- conoscere le nozioni tecniche necessarie per dimensionare correttamente un'architettura di rete locale;
- Adottare procedure per ottimizzare la configurazione dell'architettura di rete (interfacce, protocolli e servizi);
- Applicare soluzioni concordate per il raggiungimento del livello di interoperatibilità previsto tra diversi sistemi e architetture di rete;
- Riconoscere e applicare procedure (e programmi) di assemblaggio e installazione delle componenti di rete attive (sistemi operativi, router, switch, modem, hub, ecc) e passive (spina, presa, cavi, rack, ecc.);

Modalità formative

- lezioni frontali, presentazione di casi, ascolto/visione di audiovisivi, hands-on/workshop;

Valutazione dell'apprendimento

- L'efficacia dell'insegnamento impartito verrà valutata attraverso la discussione in aula al termine di ogni unità didattica, tramite test di verifica e/o mediante esecuzione di hands-on/workshop pratici;

Indicatori di padronanza

- Conoscere i principali processi di gestione di un account
- Conoscere la modalità di utilizzo di Oracle OIG 12c

Sussidi didattici

- Aula didattica, attrezzature informatiche, software, video proiettore, dispense;

Modulo 3
Vulnerability Assessment & Penetration Test

In questo modulo, gli allievi imparano l'importanza della sicurezza applicativa. Verranno affrontati temi come le vulnerabilità più note delle applicazioni, le tecniche per eseguire un attacco e quali sono i controlli/soluzioni a queste vulnerabilità. Verrà inoltre illustrata una panoramica del framework di riferimento OWASP.

Articolazione del modulo formativo

Unità	Ore	Contenuti
1	2	Differenze tra PT e VA e cenni normativi riguardo il tema
2	10	Tipiche fasi di un attacco informatico
3	10	Introduzione a OWASP e le tipologie di attacco informatico
4	10	Introduzione ai tools utilizzati per un Vulnerability Assessment
5	10	Tecniche di exploit
6	3	Analisi dei risultati e stesura della reportistica
7	25	Hands-on e workshop pratici
TOT	**70**	

Obiettivi

- Acquisire le basi del framework di riferimento OWASP;
- Acquisire le differenze tra Vulnerability Assessment e Penetration Test, e i rispettivi obiettivi;
- Acquisire le tipologie di attacco più comuni;
- Acquisire le conoscenze di base dei tool più comuni utilizzati in fase di VA e PT;

Durata oraria

- 70 ore

Conoscenze

- Conoscere le basi del framework di riferimento OWASP;
- Conoscere le differenze tra Vulnerability Assessment e Penetration Test, e i rispettivi obiettivi;
- Conoscere le tipologie di attacco più comuni;
- Conoscere i principali tools più comuni utilizzati in fase di VA e PT;

Competenze da acquisire (sarà in grado di)

- Eseguire un’attività di Vulnerability Assessment di livello base;
- Eseguire un’attività di Penetration Test di livello base;
- Produrre un report riepilogativo in merito ad un’attività di VA e PT;

Modalità formative

- lezioni frontali, presentazione di casi, ascolto/visione di audiovisivi, hands-on/workshop;

Valutazione dell'apprendimento

- L'efficacia dell'insegnamento impartito verrà valutata attraverso la discussione in aula al termine di ogni unità didattica, tramite test di verifica e/o mediante esecuzione di hands-on/workshop pratici;

Indicatori di padronanza

- Conoscere le principali "best practices" di OWASP
- Conoscere la modalità di utilizzo dei principali tools di Kali Linux

Sussidi didattici

- Aula didattica, attrezzature informatiche, software, video proiettore, dispense;

Modulo 4
Data & Endpoint Security

Articolazione del modulo formativo

Unità	Ore	Contenuti
1	4	Introduzione alla protezione dei dati e database: CIA + Prevention + Detection
2	4	Data Security: DB firewall, DB Masking/Encryption, Database Monitoring Activity
3	4	Gestione delle utenze privilegiate dei DB Administrators + EUS
4	4	Sicurezza dei dati mediante le soluzioni di EndPoint Security e DLP
5	4	Convergenza delle misure di sicurezza adottate in una realtà enterprise: SIEM, IRP, SOAR, UEBA
TOT	**20**	

Obiettivi

- Acquisire le nozioni di base riguardanti gli aspetti di sicurezza dei dati e dei database;
- Acquisire una conoscenza di alto livello delle soluzioni software più comuni per implementare misure di sicurezza adeguate per la protezione dei dati;
- Acquisire le nozioni di base riguardanti una tipica infrastruttura enterprise per il controllo continuo nel tempo delle misure di sicurezza implementate per la protezione dei dati;

Durata oraria

- 20 ore

Conoscenze

- Conoscere le nozioni di base riguardanti gli aspetti di sicurezza dei dati e dei database;
- Conoscere ad alto livello le soluzioni software più comuni per implementare misure di sicurezza adeguate;
- Conoscere le basi riguardanti una tipica infrastruttura enterprise per il controllo continuo nel tempo delle misure di sicurezza implementate a protezione dei dati;

Competenze da acquisire (sarà in grado di)

- Saper distinguere le misure di sicurezza per i dati strutturati e non strutturati
- Saper identificare la soluzione software adeguata per implementare determinati scenari di messa in sicurezza dei dati e database;
- Saper individuare quali sono le componenti tipiche di un'infrastruttura enterprise per il continuo controllo nel tempo delle misure di sicurezza implementate per la protezione dei dati;

Modalità formative

- lezioni frontali, presentazione di casi, ascolto/visione di audiovisivi

Valutazione dell'apprendimento

- L'efficacia dell'insegnamento impartito verrà valutata attraverso la discussione in aula al termine di ogni unità didattica, tramite test di verifica e/o mediante esecuzione di hands-on/workshop pratici;

Indicatori di padronanza

- Conoscere le modalità più comuni per implementare le misure di sicurezza dei dati;
- Conoscere le soluzioni software più comuni per implementare le misure di sicurezza dei dati;
- Conoscere quali sono e come interagiscono fra loro, i principali componenti di un'infrastruttura enterprise per il continuo controllo delle misure di sicurezza implementate;

Sussidi didattici

- Aula didattica, attrezzature informatiche, software, video proiettore, dispense;

Modulo 5
Identity Access Management & Cloud Security

In questo modulo, gli allievi imparano l'importanza della sicurezza preventiva. Verrà affrontato il tema del life cycle di un account, dalla creazione di un'identità alla cancellazione dell'account quando non più necessario. Verrà inoltre illustrata una panoramica del software di Identity Management Oracle OIG 12c.

Articolazione del modulo formativo

Unità	Ore	Contenuti
1	5	Riconciliazione delle identità
2	5	Provisioning di un account
3	10	Workflow approvativi
4	10	Istallazione di Oracle OIG 12c
5	15	Application Instance, Organizzazioni, Ruoli ed Access Policy
6	20	Api e OIG Plugin
7	5	Scheduled task, Prepopulate e Event handler
TOT	**70**	

Obiettivi

- Acquisire le basi del life cycle degli account;
- Acquisire la capacità di configurare ed utilizzare Oracle OIG 12c;
- Acquisire la capacità di realizzare un plugin per Oracle 12c;

Durata oraria

- 70 ore

Conoscenze

- Conoscere le basi del life cycle degli account;
- Conoscere la configurazione e l'utilizzo di Oracle OIG 12c;
- Conoscere la realizzazione di un plugin per Oracle OIG 12c;

Competenze da acquisire (sarà in grado di)

- Eseguire un'analisi di un processo di gestione di un account;
- Eseguire la configurazione di Oracle OIG 12c;
- Produrre un plugin per Oracle OIG 12c ;

Modalità formative

- lezioni frontali, presentazione di casi, ascolto/visione di audiovisivi, hands-on/workshop;

Valutazione dell'apprendimento

- L'efficacia dell'insegnamento impartito verrà valutata attraverso la discussione in aula al termine di ogni unità didattica, tramite test di verifica e/o mediante esecuzione di hands-on/workshop pratici;

Indicatori di padronanza

- Conoscere i principali processi di gestione di un account
- Conoscere la modalità di utilizzo di Oracle OIG 12c

Sussidi didattici

- Aula didattica, attrezzature informatiche, software, video proiettore, dispense;

Modulo 6
Framework, Best Practices & Standards (Eng)

In questo modulo, gli allievi conosceranno i componenti essenziali ed i concetti relativi alla sicurezza informatica quali Riservatezza, Integrità, Disponibilità (CIA), Autenticazione, Autorizzazione, Vulnerabilità, Minaccia, Rischio, Intrduzione alla protezione dei dati e data base: DB firewall, DB Masking/Encryption, Database Monitoring Activityetc...
Verranno inoltre esplorati gli argomenti riguardanti i framework e agli standard internazionali di riferimento come il NIST, ENISA, GDPR, PCI, etc...

Articolazione del modulo formativo

Unità	Ore	Contenuti
1	3	Overview generale dei framework di riferimento
2	3	Approfondimento riguardo il framework NIST, ENISA e CIA
3	3	Approfondimento riguardo gli standard: ISO 27001/27002, PCI DSS, SOX, CIS
4	3	AgID: "Misure Minime per la PA Italia" + EIDAS + SPID
5	6	Approfondimento riguardo il GDPR
TOT	**18**	

Obiettivi

- Acquisire le nozioni e le basi dei principali framework e standard internazionali di riferimento relativi al settore;
- Acquisire le nozioni per capire come passare dalle linee guida dei framework ad azioni concrete di implementazioni tecnologiche per adeguate misure di sicurezza;

Durata oraria

- 18 ore

Conoscenze

- Conoscere quali sono i principali framework e standard internazionali di riferimento relativi al settore;
- Conoscere quali azioni e tecnologie indirizzano i punti principali dei framework e degli standard internazionali;
- Conoscere quali sono le indicazioni principali per le misure di sicurezza della Pubblica Amministrazione in Italia;

Competenze da acquisire (sarà in grado di)

- Essere in grado di mappare i principali punti dei framework e standard internazionali con le soluzioni tecnologiche più comunemente utilizzate;
- Essere in grado di indicare come indirizzare i principali requisiti di sicurezza dettati dai framework mediante l'utilizzo di soluzioni tecnologiche;

Modalità formative

- lezioni frontali, presentazione di casi, ascolto/visione di audiovisivi

Valutazione dell'apprendimento

- L'efficacia dell'insegnamento impartito verrà valutata attraverso la discussione in aula al termine di ogni unità didattica e/o tramite test di verifica;

Indicatori di padronanza

- Adottare azioni e procedure atte alla prevenzione e/o all'implementazione di adeguate misure di sicurezza;

Sussidi didattici

- Aula didattica, attrezzature informatiche, software, video proiettore, dispense;

Modulo 7
Blockchain, AI & Machine Learning for Security

In questo modulo, gli allievi conosceranno i principi base ed i concetti relativi a Blockchain, Artificial Intelligence e Machine Learning. Verranno inoltre esplorati gli argomenti riguardanti la sicurezza legata ai concetti precedenti.

Articolazione del modulo formativo

Unità	Ore	Contenuti
1	5	Overview generale di una Blockchain
2	5	Overview generale di Artificial Intelligence
3	5	Overview generale di Machine Learning
4	5	Applicazione dei principi di Blockchain, Artificial Intelligence e Machine Learning alla sicurezza
TOT	**20**	

Obiettivi

- Acquisire le nozioni e le basi di Blockchain, Artificial Intelligence e Machine Learning;

Durata oraria

- 20 ore

Conoscenze

- Conoscere le nozioni e le basi di Blockchain, Artificial Intelligence e Machine Learning;
- Conoscere come applicare i principi di Blockchain, Artificial Intelligence e Machine Learning alla sicurezza;

Competenze da acquisire (sarà in grado di)

- Essere in grado di applicare i principi di Blockchain, Artificial Intelligence e Machine Learning alla sicurezza;

Modalità formative

- lezioni frontali, presentazione di casi, ascolto/visione di audiovisivi

Valutazione dell'apprendimento

- L'efficacia dell'insegnamento impartito verrà valutata attraverso la discussione in aula al termine di ogni unità didattica e/o tramite test di verifica;

Indicatori di padronanza

- Adottare azioni e procedure atte alla prevenzione e/o all'implementazione di adeguate misure di sicurezza;

Sussidi didattici

- Aula didattica, attrezzature informatiche, software, video proiettore, dispense;

Modulo 8
Sicurezza sul lavoro - D. Lgs. N. 81/08

In questo modulo, gli allievi conosceranno i principi base ed i concetti relativi la sicurezza su lavoro

Articolazione del modulo formativo

Unità	Ore	Contenuti
1	3	Aspetti generali del D. Lgs. N. 81/08
2	3	I soggetti della prevenzione
3	3	I principali rischi
4	3	Il servizio di prevenzione/protezione
TOT	**12**	

Obiettivi

- Conoscenza delle caratteristiche del posto di lavoro e dei rischi ad esso connessi;
- Rispetto costante delle misure di prevenzione e sicurezza
- Il trattamento dei dati personali
- Rispettare le normative in tema di diritto d'autore, pubblicità ingannevole, proprietà industriale

Durata oraria

- 12 ore

Conoscenze

- I rischi connessi alla propria mansione/posto di lavoro;
- Le procedure riferite alla mansione;
- Le misure di prevenzione presenti sul posto di lavoro
- Normativa a tutela della privacy (trattamento dei dati personali, ecc.)
- Principali riferimenti legislativi e normativi in materia di diritto d'autore, pubblicità ingannevole, proprietà industriale, ecc

Competenze da acquisire (sarà in grado di)

- Utilizzare le procedure atte a svolgere la mansione assegnata nel rispetto delle norme di sicurezza
- Acquisire le competenze di base della normativa vigente necessarie al corretto utilizzo della campagna di comunicazione.
- Rispettare le normative di settore

Modalità formative

- Lezioni frontali, presentazione di casi, ascolto/visione di audiovisivi Indicatori di padronanza
- Acquisire conoscenze giuridiche di base sulle materie trattate

Valutazione dell'apprendimento

- Valutazione in ingresso dei saperi e l'efficacia dell'insegnamento impartito verrà valutata attraverso la discussione in aula al termine del modulo e tramite test formalizzati e/o realizzazione di elaborati di tipo professionale

Sussidi didattici

- Aula didattica, attrezzature informatiche, software, video proiettore, dispense;