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	5	Differenze tra le distribuzioni Linux
2	5	Utilizzo e comandi del "vi"
3	20	Istallazione e configurazione di base
4	10	Configurazione della connessione SSH, X11 e VNC
5	10	Istallazione e configurazione di Apache
6	10	Crittografia, certificati e HTTPS
7	25	Programmazione bash shell
8	15	Hardening
TOT	**100**	

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

- 100 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 del TCP/IP.

Articolazione del modulo formativo

Unità	Ore	Contenuti
1	20	TCP/IP
2	20	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
3	10	Cenni su protocolli di Routing.
TOT	**50**	

Obiettivi

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

Durata oraria

- 50 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);
- conoscere le nozioni tecniche necessarie per dimensionare correttamente un'architettura di rete locale;
- Applicare soluzioni concordate per il raggiungimento del livello di interoperatibilità previsto tra diversi sistemi e architetture di rete;

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 una rete.

Sussidi didattici

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

Modulo 3
Cyber Security Operations

In questo modulo, gli allievi acquisiranno i fondamenti delle tematiche presenti all'interno di un Security Operations Center e 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, delle tecniche OSINT e fornite basi di Threat Intelligene.

Articolazione del modulo formativo

Unità	Ore	Contenuti
1	1	Differenze tra PT e VA e cenni normativi riguardo il tema
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
2	8	Tipiche fasi di un attacco informatico
3	8	Introduzione a OWASP e le tipologie di attacco informatico
4	7	Introduzione ai tools utilizzati per un Vulnerability Assessment
5	10	Tecniche di exploit
6	3	Analisi dei risultati e stesura della reportistica
7	25	Cyber Security Operation Center
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;
- 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

- 70 ore

Conoscenze

- 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;

- 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;
- 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, 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
- 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 4
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.

Articolazione del modulo formativo

Unità	Ore	Contenuti
1	5	Account ed Identità
2	5	Riconciliazione e Provisioning
3	5	Organizzazioni e Ruoli
5	5	Workflow approvativi
6	10	Access Management
TOT	**30**	

Obiettivi

- Acquisire le basi del Lifecycle degli account;
- Acquisire le basi dell'Access Management;

Durata oraria

- 30 ore

Conoscenze

- Conoscere le basi del LifeCicle degli account;
- Conoscere le basi dell'Access Management;

Competenze da acquisire (sarà in grado di)

- Capire un'analisi di un processo di gestione di un account;
- Capire un'analisi di un processo di Access Management;

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 i principali processi di gestione dell'Access Management

Sussidi didattici

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

Modulo 5
Workshop

In questo modulo, gli allievi parteciperanno a Workshop tenuti dai nostri partner con esperti operativi degli argomenti trattati.

In particolare, saranno tenuti dei Workshop su:

- GDPR
- Blockchain
- Artificial Intelligence
- Machine Learning

Obiettivi
- Affrontare argomenti su Blockchain, Artificial Intelligence e Machine Learning;
- Interagire con figure professionali del mondo del lavoro;

Durata oraria
- T.B.D

Conoscenze
- Conoscere le nozioni e le basi di GDPR, Blockchain, Artificial Intelligence e Machine Learning;

Competenze da acquisire (sarà in grado di)
- Essere in grado di comprendere i principi di GDPR, Blockchain, Artificial Intelligence e Machine Learning alla sicurezza;

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

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