OSCS-9 - SICUREZZA DI RETE E MONITORAGGIO CON TOOL OPEN SOURCE

Categoria: **Cyber Security**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
5 Giorni	Cyber Security	Docente Senior (min. 5 anni)	Professionista IT	PCSNET

OBIETTIVI

-Acquisire competenze di base per lavorare su Linux e FreeBSD.
-Saper configurare rete, utenti e servizi, e analizzare i log.
-Configurare pfSense come firewall, router e gateway VPN.
-Riconoscere, configurare e ottimizzare IDS/IPS open source.
-Centralizzare i log e creare regole di rilevamento personalizzate.
-Analizzare pacchetti e sessioni di rete in profondità.
-Monitorare server e apparati di rete in tempo reale.
-Creare una piattaforma SOC completa.
-Implementare ticketing e gestione asset.

PREREQUISITI

-Conoscenza base di reti TCP/IP (modello OSI, routing, subnetting, DNS, DHCP).
-Concetti di cybersecurity: differenza tra IDS, IPS, SIEM, firewall.
-Conoscenza di base di sistemi Linux.

CONTENUTI

Modulo 1 - Fondamenti di Linux e FreeBSD Linux

Introduzione a Unix/Linux/FreeBSD

-Differenze tra Linux e FreeBSD.
-Struttura del file system (/etc, /var/log, /usr/local).
-Filosofia "tutto è un file".

Comandi di base

-Navigazione (ls, cd, find).
-Manipolazione file (cat, less, head, tail).
-Permessi e sicurezza (chmod, chown, umask).

Gestione pacchetti

-apt (Debian/Ubuntu), pkg (FreeBSD).

Rete

-Configurazione IP (ifconfig, ip addr).
-DNS e routing (route, ip route).
-Firewall di base: iptables, pf.

Gestione servizi

-systemctl, service.
-Avvio automatico.

Logging

-Journalctl.
-/var/log (syslog, auth.log, messages).

Modulo 2 - pfSense (Firewall & Routing)

Installazione pfSense

-Scaricare ISO ufficiale.
-Installazione su VirtualBox con due schede di rete (WAN e LAN).

Primo avvio

-Assegnazione interfacce.
-Configurazione IP iniziale.

Interfaccia web

-Dashboard overview.
-Aggiornamento firmware e pacchetti.

Regole firewall

-Creazione e testing regole di filtraggio.
-NAT (Port Forwarding e Outbound NAT).

VPN

-Creazione di una VPN base con OpenVPN.

Monitoraggio

-Stati connessioni, traffico, log.

Backup e restore configurazione

Laboratorio

-Creazione di una rete isolata con pfSense come firewall principale.
-Configurazione di regole per segmentare traffico LAN/DMZ/WAN.
-Simulazione di attacco bloccato da regola firewall.

Modulo 3 - Snort e Suricata (IDS/IPS)

Teoria IDS/IPS

-Differenza tra rilevamento e prevenzione.

-Flusso di lavoro IDS.

Installazione Snort

-Installazione su Linux.
-Struttura directory e configurazioni.

Regole

-Formato regole Snort.
-Aggiornamento regole (Snort.org).

Suricata

-Differenze rispetto a Snort (multi-threading, prestazioni).
-Integrazione con pfSense.

Analisi eventi

-Lettura log (/var/log/snort/alert).
-Testing con attacchi simulati (es. scansione nmap).

Laboratorio

-Configurazione IDS su pfSense.
-Creazione regola personalizzata per rilevare traffico malevolo.
-Simulazione DoS e rilevamento tramite Snort.

Modulo 4 - Wazuh (SIEM e Log Management)

Concetti di SIEM

-Cos'è un SIEM e differenza rispetto a un semplice syslog server.

Architettura Wazuh

-Server, agent, dashboard Kibana.

Installazione

-Server Wazuh su Linux.
-Configurazione agenti su endpoint.

Creazione regole di sicurezza

Integrazione con Snort/Suricata

Laboratorio

-Configurazione di un server Wazuh.
-Integrazione con un server Linux e pfSense.
-Creazione di una regola per alert su login sospetti.

Modulo 5 - Zeek (Network Analysis)

Introduzione a Zeek

-Differenza tra IDS e Network Analysis.

Installazione

-Setup base su Linux.

Analisi traffico

- -Sessioni HTTP, SSH, DNS.
- -Generazione log dettagliati.

Scripting base Zeek

Laboratorio

- -Cattura pacchetti da pfSense.
- -Analisi traffico sospetto.
- -Creazione script per rilevare anomalie.

Modulo 6 - Zabbix (Network & Host Monitoring)

Architettura Zabbix

Installazione Zabbix Server

Configurazione agenti

Creazione dashboard e alerting

Laboratorio

- -Monitoraggio di un server Linux.
- -Creazione trigger per downtime e performance.

Modulo 7 - Security Onion

Introduzione a Security Onion

Installazione rapida su VM

Integrazione automatica con Suricata, Zeek, Wazuh

Uso dashboard Kibana per incident response

Laboratorio

- -Analisi di un attacco reale simulato.
- -Creazione timeline incidente.

Modulo 8 - iTop (IT Service Management)

ITIL e CMDB: concetti base

Installazione iTop

Gestione asset e ticket

INFO

Materiale didattico: Materiale didattico e relativo prezzo da concordare

Costo materiale didattico: NON incluso nel prezzo del corso
Natura del corso: Operativo (previsti lab su PC)