CORSO PENETRATION TESTING CON KALI LINUX

Durata: 4 ore

PROGRAMMA

MODULO 1: APPROCCIO ETICO, METODOLOGIA E L'ECOSISTEMA KALI LINUX

- Cos'è Kali / a cosa serve
- Kali Purple (red+blue, SOC-in-a-box) e form factor attuali (Win-KeX/WSL, NetHunter, cloud)
- Le fasi del pentest ancorate a framework: PTES, Cyber Kill Chain, MITRE ATT&CK, con NIST SP 800-115 come riferimento metodologico
- Struttura di Kali e metapackage;
- Etica e legalità: scope, Rules of Engagement, autorizzazione scritta; lab sicuro (VM isolate, snapshot, firewall)

MODULO 2: RECON, SCANNING E NETWORK DISCOVERY

- Host discovery e network mapping (principi + interpretazione)
- Identificazione servizi/porte (TCP/UDP), OS fingerprinting, flag nmap
- Tooling per scala/velocità: NSE, RustScan/masscan, naabu
- Detection awareness (blue team): come appaiono le scansioni in log/IDS

MODULO 3: FASE DI EXPLOITATION, GESTIONE PASSWORD E CONTROLLO REMOTO

- Metasploit: exploit, payload, sessioni
- Brute-force RDP/SSH/SMB; cracking con hashcat/John
- Cenni su C2 moderni (Sliver/Havoc/Mythic) e perché oggi conta l'evasione EDR

MODULO 4: POST-EXPLOITATION: PRIVILEGE ESCALATION, LATERAL MOVEMENT & PIVOTING

- Privilege escalation: enumerazione automatizzata (linPEAS/winPEAS) e misconfig classiche
- Lateral movement: riuso credenziali, pass-the-hash, esecuzione remota (PsExec/WinRM/WMI)
- Chiusura: cleanup, raccolta evidenze per il report e mitigazioni

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO PENETRATION TESTING CON KALI LINUX

Durata: 4 ore

OVERVIEW DEL CORSO

Comprendere le tecniche d'attacco utilizzate dai cybercriminali è il primo passo fondamentale per strutturare una difesa aziendale efficace. Questo Flash Training offre un percorso verticale e pratico incentrato sull'utilizzo di Kali Linux, la piattaforma standard di riferimento a livello globale per le attività di Ethical Hacking e Vulnerability Assessment.

In sole 4 ore, analizzeremo le metodologie strutturate di analisi seguendo i principali framework internazionali (NIST, MITRE ATT&CK, PTES). Passeremo poi alla fase operativa esplorando i tool più efficaci per il network mapping velocizzato, l'exploitation delle vulnerabilità e le complesse dinamiche di post-exploitation, inclusi i movimenti laterali e i moderni sistemi di Command & Control (C2).

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Sistemisti e amministratori di rete
- Security Analyst
- Ethical Hacker
- IT Auditor e Compliance Specialist

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- A utilizzare l'ecosistema Kali Linux (comprese le estensioni Kali Purple e Win-KeX) all'interno di un framework metodologico standardizzato (NIST SP 800-115, PTES).
- Eseguire attività di network mapping avanzato, host discovery e fingerprinting dei servizi ottimizzando la velocità tramite strumenti come RustScan e Nmap.
- Configurare ed eseguire tentativi di exploitation controllati utilizzando il framework Metasploit.
- Identificare le vulnerabilità di configurazione nei sistemi operativi per implementare tecniche di Privilege Escalation locali (tramite linPEAS/winPEAS).
- Comprendere i meccanismi di persistenza, lateral movement (Pass-the-Hash, PsExec/WMI) e l'impatto dei moderni framework C2 in ottica di evasione EDR.

CONTATTI

info@nexsys.it

www.nexsys.it