CORSO ETHICAL HACKING

Durata: 3 giorni

NEXSYS
LEARN IT, TRANSFORM IT

PROGRAMMA

MODULO 1: PERIMETRO, REGOLE D'INGAGGIO E RESPONSABILITÀ

- Tipologie di attività: vulnerability assessment, penetration test, red teaming
- Definizione dello scope e degli obiettivi insieme al committente
- Autorizzazione scritta, finestre operative e limiti da concordare
- Quadro normativo italiano: accesso abusivo a sistema informatico, trattamento dei dati, obblighi del D.Lgs. 138/2024
- Raccolta, marcatura e conservazione delle evidenze
- Errori tipici che invalidano un ingaggio o espongono chi lo esegue

MODULO 2: METODOLOGIA E ANATOMIA DI UN ATTACCO

- Le fasi di un'intrusione reale, dalla ricognizione all'obiettivo finale
- Standard di riferimento: OWASP, NIST SP 800-115, PTES
- Mappatura delle tecniche osservate con MITRE ATT&CK
- Profili, motivazioni e capacità degli attaccanti
- Controlli di sicurezza aziendali e loro copertura reale
- Allestimento della postazione e del laboratorio di lavoro

MODULO 3: INTELLIGENCE SU FONTI APERTE

- L'impronta digitale di un'organizzazione
- Domini, sottodomini, record DNS e trasparenza dei certificati
- Dati esposti: repository di codice, documenti pubblicati, metadati
- Le persone come vettore: profili pubblici, schemi di posta, credenziali trapelate
- Strumenti di raccolta e automazione della ricerca
- Ridurre la propria esposizione: contromisure applicabili lato azienda

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO ETHICAL HACKING

Durata: 3 giorni

NEXSYS
LEARN IT, TRANSFORM IT

MODULO 4: SCANSIONE DI RETI E SERVIZI

- Individuazione degli host attivi e delle porte in ascolto
- Tecniche di scansione e loro impronta sul bersaglio
- Riconoscimento di servizi, versioni e sistemi operativi
- Ricostruzione della topologia rilevata
- Elusione dei controlli durante la fase di scansione
- Rilevare e limitare le scansioni dal lato di chi difende

MODULO 5: ENUMERAZIONE E RACCOLTA DI DETTAGLIO

- Cosa si ricava dai servizi di rete senza credenziali
- Enumerazione delle directory aziendali e dei servizi di dominio
- Condivisioni, utenze, gruppi e criteri
- Servizi di posta, nomi e sincronizzazione oraria come fonti
- Dal rumore al bersaglio: criteri per scegliere dove insistere
- Irrigidire i servizi per ridurre ciò che rivelano

MODULO 6: SIMULAZIONE DI PHISHING SUI BERSAGLI INDIVIDUATI

- Dalla ricognizione alla lista bersaglio: usare quello che hai già raccolto
- Leve psicologiche e costruzione di un pretesto credibile
- Realizzazione della campagna e delle pagine di raccolta
- Aspetti etici, sindacali e di trattamento dei dati nelle simulazioni
- Misurare i risultati: tasso di click, tempo medio di segnalazione, copertura
- Dalla singola campagna a un programma di awareness continuativo

MODULO 7: COMPROMISSIONE TECNICA

- Finalità e limiti del vulnerability assessment
- Classificazione delle vulnerabilità e fonti di riferimento affidabili
- Strumenti di assessment e configurazione delle scansioni
- Lettura critica dei risultati e riconoscimento dei falsi positivi
- Verifica manuale di una vulnerabilità segnalata
- Struttura di un report di assessment

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO ETHICAL HACKING

Durata: 3 giorni

NEXSYS
LEARN IT, TRANSFORM IT

MODULO 8: ATTACCO AL SISTEMA: ACCESSO, ESCALATION, PERSISTENZA

- Fasi dell'attacco a un singolo sistema
- Selezione, verifica e adattamento di un exploit
- Attacchi alle credenziali e alle password
- Escalation dei privilegi su ambienti Windows e Linux
- Persistenza, tecniche fileless e abuso di strumenti legittimi di sistema
- Tracce lasciate sul sistema e loro gestion

MODULO 9: ATTACCHI SU RETE: INTERCETTAZIONE E AVVELENAMENTO

- Intercettazione del traffico e protocolli ancora in chiaro
- Attacchi basati sugli indirizzi MAC e al protocollo DHCP
- Avvelenamento ARP e DNS
- Tecniche di spoofing
- Dove la cifratura del traffico chiude il problema e dove no
- Segmentazione e controlli che interrompono la catena

MODULO 10: IDENTITÀ, SESSIONI E MOVIMENTO LATERALE

- Gestione delle sessioni e punti deboli ricorrenti
- Dirottamento di sessione a livello di rete e applicativo
- Furto e riutilizzo delle credenziali
- Movimento laterale all'interno di un dominio aziendale
- Abuso di deleghe, permessi e relazioni di fiducia
- Modello a livelli e protezione delle identità privilegiate

MODULO 11: APPLICAZIONI WEB, API E INIEZIONI

- Architettura delle applicazioni moderne e superficie realmente esposta
- Vulnerabilità dei server web e ciclo di patch management
- Iniezioni: SQL, tipologie, metodologia e strumenti automatizzati
- Tecniche di evasione dei filtri e prevenzione strutturale
- Difetti di autenticazione, gestione della sessione e autorizzazione
- API, webhook e web shell: dove si concentra il rischio oggi

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO ETHICAL HACKING

Durata: 3 giorni

MODULO 12: RETI WIRELESS E DISPOSITIVI MOBILI

- Basi delle reti wireless e debolezze della crittografia
- Metodologia di attacco a una rete Wi-Fi aziendale
- Bluetooth e protocolli a corto raggio
- Vettori di attacco su Android e iOS
- Gestione dei dispositivi (MDM) e criteri aziendali
- Difesa delle reti wireless e delle flotte mobil

MODULO 13: CLOUD, CONTAINER, IOT E OT

- Modello di responsabilità condivisa e configurazioni errate ricorrenti
- Identità e permessi eccessivi negli ambienti cloud
- Container e workload serverless: rischi specifici
- Dispositivi IoT: interfacce di gestione, firmware, protocolli
- Ambienti OT e industriali: vincoli e cautele obbligatorie nei test
- Buone pratiche di irrobustimento per ciascuna superficie

MODULO 14: DIFESE PERIMETRALI, EVASIONE E DISPONIBILITÀ DEL SERVIZIO

- Come funzionano firewall, IDS/IPS, EDR e honeypot
- Tecniche di evasione e loro limiti reali
- Elusione delle soluzioni endpoint, letta dal lato di chi difende
- Rilevamento degli honeypot
- Indisponibilità di servizio: DoS, DDoS, botnet e mitigazione
- Configurazioni che chiudono le strade percorse nei moduli precedenti

MODULO 15: PRIORITIZZAZIONE E REPORTING

- Da evidenza a finding: cosa si scrive, cosa si omette, come si documenta
- Valutazione della gravità e del rischio nel contesto specifico del cliente
- Struttura del report: sintesi per la direzione e dettaglio tecnico
- Piano di remediation con priorità e tempi realistici
- Presentazione dei risultati e gestione delle obiezioni
- Retest e chiusura formale dell'ingaggio

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO ETHICAL HACKING

Durata: 3 giorni

OVERVIEW DEL CORSO

Il Corso Ethical Hacking di Nexsys insegna a condurre un'attività di sicurezza offensiva dall'inizio alla fine: definire il perimetro e le autorizzazioni, raccogliere informazioni, sfruttare le vulnerabilità e — soprattutto — trasformare quello che hai trovato in un documento che l'azienda può davvero usare per rimediare.
È un percorso progettato internamente dai consulenti che eseguono penetration test e assessment per i nostri clienti. La struttura segue il ciclo reale di un ingaggio: cinque blocchi, quindici moduli, laboratori in ambienti virtuali isolati e un modulo finale dedicato al reporting, la parte che nella pratica distingue un test utile da un elenco di alert.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a IT manager, CIO, Professionisti IT, System Administrator, Responsabili della sicurezza informatica

COSA SAPRAI FARE ALLA FINE DEL CORSO?

- Definire perimetro, regole d'ingaggio e autorizzazioni prima di toccare un sistema, con il quadro normativo italiano di riferimento
- Ricostruire la superficie d'attacco di un'organizzazione partendo da fonti pubbliche, dati esposti e persone
- Passare dalla scansione all'enumerazione mirata, distinguendo il rumore dai servizi su cui vale la pena insistere
- Progettare, lanciare e misurare una campagna di phishing simulato sui bersagli individuati in ricognizione
- Portare una vulnerabilità fino all'accesso, all'escalation dei privilegi e alla persistenza, in laboratorio controllato
- Attaccare applicazioni web e API moderne, dalle iniezioni ai difetti di autenticazione e autorizzazione
- Muoverti lateralmente su reti e identità aziendali sfruttando credenziali, protocolli deboli e configurazioni errate
- Valutare le superfici estese (wireless, mobile, cloud, container, IoT e OT) con il metodo adatto a ciascuna
- Riconoscere come i controlli difensivi vedono le tue azioni, e cosa serve per chiudere le strade che hai percorso
- Prioritizzare i risultati e scrivere un report che la direzione legge e il team IT riesce effettivamente a chiudere

CONTATTI

info@nexsys.it

www.nexsys.it