



corvallis



OSINT E SOCIAL ENGINEERING

Se hai bisogno di maggiori informazioni, scrivi a:
formazione@swascan.com

Settembre '24

Descrizione

OSINT è l'acronimo delle parole inglesi Open Source Intelligence e identifica il processo di raccolta delle informazioni attraverso la consultazione delle fonti di pubblico accesso o fonti aperte.

Attraverso il nostro Corso OSINT viaggerete, attraverso la rete, tra motori di ricerca, file multimediali, posta elettronica, social network, imparando ad identificare i numerosi luoghi dove raccogliere informazioni.

Quest'ultime dovranno poi essere vagliate e campionate al fine di selezionare quelle valide, fruibili e probatorie. Impareremo che solo attraverso precisi processi di indagine, adeguate metodologie d'analisi e specifiche attività di filtraggio sarà possibile raggiungere una verificata conoscenza del mondo OSINT.

Un momento importante del Corso sarà dedicato a comprendere come i dati, reperiti attraverso le analisi OSINT, possano essere impiegati dai criminali per strutturare un attacco di ingegneria sociale, mettendo a rischio la sicurezza del perimetro aziendale sfruttando il fattore umano.

Obiettivo

Lo scopo del corso è di fornire gli strumenti tecnici e teorici per lo svolgimento di una ricerca OSINT sulla rete. Alla fine del percorso, i partecipanti saranno in grado di effettuare un'analisi OSINT utilizzando sia tecniche manuali che tool di ricerca nonché di valutare l'attendibilità delle informazioni reperite. Inoltre, i discenti saranno edotti sulle principali tipologie di attacchi di ingegneria sociale che sfruttano il mondo OSINT per portare a segno le proprie aggressioni e apprenderanno come difendersi.



Capture The Flag OSINT

Il Corso terminerà con una "CTF OSINT". Si tratta di una sfida che mette alla prova le abilità dei partecipanti nell'utilizzo delle tecniche di raccolta di informazioni aperte per risolvere problemi e enigmi.

Manuale di istruzioni

- Sarà possibile lavorare in team o singolarmente.
- Qualora il team impiegasse un lasso di tempo eccessivo per risolvere un determinato enigma, potrà chiedere supporto al docente. Quest'ultimo coprirà il ruolo del "suggeritore" e del cosiddetto "aiuto del pubblico". Valutate bene quando consultarlo perchè durante l'intera sfida potrà fornire solo 3 indizi...
- Non ci sono regole; non verranno specificati gli strumenti e le fonti da utilizzare per cui spazio alla fantasia.



Programma didattico



GIORNATA 1

- OSINT: Cos'è e da dove nasce?
- Da chi viene usato ed in che settori può essere estremamente utile?
- Legami OSINT e Sicurezza informatica
- Raccolta dati e reportistica

GIORNATA 2

- Ricerca per immagini e geolocalizzazione
- Google Dorks e motori di ricerca
- Data Breach Search Engine
- Siti web & IOT
- Automazione OSINT (Pro e contro)

GIORNATA 3

- Social Media Intelligence (SOCMINT)
- Potenzialità dell'ingegneria sociale
- Come i dati possono essere usati per strutturare un attacco informatico
- Attacchi basati sull'ingegneria sociale & OSINT

GIORNATA 4

- Capture The Flag
- Conclusioni e saluti

**Segui le lezioni da dove vuoi tu!
Il corso è interamente somministrato
in modalità DAD.**

Destinatari



Questo corso di formazione è destinato a professionisti nel campo della sicurezza informatica, professionisti del settore legale, forze dell'ordine, giornalisti e investigatori privati, analisti di intelligence, tecnici, internal audit e chiunque abbia interesse ad approfondire la materia.



Prerequisiti

Non sono richieste competenze specifiche per la partecipazione al Corso.

Metodologia



Il Corso di Formazione verrà erogato in modalità sincrona attraverso la costituzione di classi virtuali.

Il Corso ha una durata di **16 ore** distribuite in due appuntamenti settimanali della durata di 4 ore ciascuno nella fascia oraria pomeridiana.

Calendario

18 Settembre

20 Settembre

24 Settembre

26 Settembre

Orario: 14:00 – 18:00



Inclusa una copia gratuita dei materiali didattici utilizzati durante il Corso.