10/14 Volnovaska Str., 03124, Kyiv, Ukraine
Tel.:+380 44 594 80 18; training@issp.com
www.issp.training

I-OSINT CR | Кібер-розвідка

Авторський курс від ISSP

Курс для спеціалістів з технічним досвідом, для поглибленого дослідження цільового об'єкту, з використанням як пасивних, так і активних методів, засобів та інструментів. Основний акценти курсу – це безпека та анонімність розвідника.

Для кого:

- Junior Pentester
- Спеціалісти із захисту мереж
- Системні адміністратори
- Спеціалісти кібер-розвідки військової і цивільної сфери з базовим досвідом в IT

Слухачам потрібно:

- знання в мережевих технологіях
- вміння працювати з терміналом Linux та навички зі скріптингу

Даний курс допоможе:

- Проаналізувати мету розвідки та вимоги її деталізації.
- Навчитись на практиці використовувати алгоритм проведення розвідки Open-source Intelligence: Social Intelligence, Human Intelligence та інших.
- Підготувати безпечний процес для проведення дослідження.
- Протягом курсу здійснити реальний пошук інформації про події, людей та організації (доступ до даних соціальних мереж, пошук об'єктів за геолокацією та картами, онлайн-камерами, метаданими).
- Навчитись збирати дані з Darkweb.
- Навчитись обробляти розрізнену інформацію про об'єкт дослідження.
- Навчитись використовувати інструментарій розвідника.
- Збирати технічну інформацію про ресурси цілі.
- Сформувати якісний звіт про досліджуваний об'єкт (обирається учасником самостійно).

Програма курсу:

1. Загальна інформація про OSINT

- Що таке OSINT?
- Важливість OSINT
- Основні типи OSINT
- Етапи OSINT
- Процес розвідки
- Види OSINT за напрямками
- Нюанси та складності OSINT

10/14 Volnovaska Str., 03124, Kyiv, Ukraine
Tel.:+380 44 594 80 18; training@issp.com
www.issp.training

2. Безпечний OSINT
- Безпека свого комп'ютера
- Ризики дослідника
- Безпечна платформа для OSINT
- Зберігання паролів
- VPN – віртуальна мережа
- VPN та DNS leak
- TOR
- Proxy
- Анонімність платежів
- Віртуалізація
- Linux
- Безпечна платформа для OSINT
- Безпечна комунікація для OSINT

3. Альтернативний профіль для OSINT
- Методи створення альтернативного профілю
- Ризики використання тимчасових адрес і телефонних номерів

4. Документування
- Алгоритм процесу документування матеріалів
- Інструменти для ефективного документування

5. Робота з пошуковими системами
- Пошукові системи
- Фреймворк для OSINT
- Google Dorks
- Розширений пошук
- Реверсивний пошук і дослідження зображень
- Пошук відео
- Метаданні

6. Дослідження людей (people OSINT)
- Розвідка соціальних мереж
- Алгоритм дій
- Інструментарій
- Чек-ліст для розвідки соціальних мереж
- Пошук у Linked.in
- Пошук за реальним іменем
- Пошук за електронною скринькою
- Пошук за нікнеймом
- Пошук за номером телефону

7. Дослідження бізнесу (business OSINT)
- Алгоритм проведення
- Практичний кейс
- Джерела для інформації про компанію

8. Технічні методи розвідки (Reconnaissance)
- Технічні аспекти
- Веб-технології
- Алгоритм розвідки

9. DarkWeb
- Базові поняття
- Джерела інформації

10. Звітність
- Правила ведення звітності

11. Навчальні портали

Формат навчання:
3 дні, з 10:00 до 17:30, з перервами на обід та кава-паузи.

Мова викладання:
Українська.

Тренер курсу
Юрій Самохвалов - інструктор-методолог Тренінгового Центру ISSP, акредитований інструктор EC-Council, Cisco. Сертифікований спеціаліст за напрямками OSINT, етичного хакінгу, аналітики з кібербезпеки, побудови захищеної інфраструктури та розслідування комп'ютерних злочинів, також є автором низки курсів з кібербезпеки, як для початківців, так і для спеціалістів. Досвід Юрія включає проектування, реалізацію та менеджмент мережевої інфраструктури компанії, проектування та реалізація структурних і безпекових проектів для замовників з комерційного та державного секторів.