Анонс курсів

вересень – грудень 2021

ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ СПЕЦІАЛІСТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

КАЛЕНДАР КУРСІВ (з посиланнями на детальний опис)

ВЕРЕСЕНЬ 2021

- 13-14 вересня: **I-CSE – Cybersecurity Essentials** (набір завершено)
- 15-17 вересня: **I-CSO – Cybersecuritry Operations** (набір завершено)
- 20-21 вересня: **SSS – SOC Survival Skills** (набір завершено)
- 22-24 вересня: **Спеціаліст та внутрішній аудитор СУІБ на основі стандарту ISO / IEC 27001** (набір завершено)

ЖОВТЕНЬ 2021

- 4-5 жовтня: **I-CSE – Cybersecurity Essentials**
- 6-8 жовтня: **I-CSO – Cybersecuritry Operations**
- 11-13 жовтня: **Спеціаліст та внутрішній аудитор СУІБ на основі стандарту ISO / IEC 27001**
- 18-22 жовтня: **CND – Certified Network Defender**
- 25-28 жовтня: **CISM – Certified Information Security Manager** (набір завершено)

ЛИСТОПАД 2021

- 8-12 листопада: **CISA – Certified Information Systems Auditor**
- 22-26 листопада: **CEH – Certified Ethical Hacker** (набір завершено)
- 29 листопада – 3 грудня: **CISSP – Certified Information Systems Security Professional** (набір завершено)

ГРУДЕНЬ 2021

- 6-8 грудня: **I-OSINT – Open-Source Intelligence (Introductory course)** (набір завершено)
- 9-10 грудня: **I-CSE – Cybersecurity Essentials**
- 15-17 грудня: **I-CSO – Cybersecuritry Operations**

Просимо звернути увагу: Учасник може зареєструватись тільки на 1 курс

I-CSE – Cybersecurity Essentials

Дати проведення: 13-14 вересня; 4-5 жовтня; 9-10 грудня 2021

Місце проведення: ISSP Training Center, м. Київ, вул. Радищева 10/14

Тривалість: 2 дні з 10:00 до 18:00 з перервами на обід та кава-паузи

Мова викладання: українська / російська

ПРО КУРС

Курс **Основи кібербезпеки** охоплює основні знання і навички у всіх областях безпеки в кіберпросторі - інформаційна безпека, системна безпека, мережна безпека, мобільна безпека, фізична безпека, етика і закони, пов'язані технології, використання технологій захисту і пом'якшення у захисті бізнесу.

Після закінчення курсу **Основи кібербезпеки** слухачі зможуть виконувати наступні задачі:

- описати характеристики злочинців і героїв в сфері кібербезпеки;
- описати, як принципи конфіденційності, цілісності і доступності, пов'язані зі станом даних і контрзаходами щодо кібербезпеки;
- описати тактику, методи та процедури, які використовуються кіберзлочинцями;
- описати, як та які технології, продукти і процедури використовуються для захисту конфіденційності та для забезпечення цілісності і високої доступності;
- пояснити, як професіонали кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережі;
- пояснити мету законів, пов'язаних з кібербезпекою.

ДЛЯ КОГО

Тренінг адаптовано для широкої аудиторії з **базовим** рівнем підготовки.

ПРОГРАМА КУРСУ

1. Кібербезпека – світ експертів та злочинців
2. Куб кібербезпеки
3. Кібербезпека – загрози, вразливості та атаки
4. Мистецтво захисту таємниць
5. Мистецтво забезпечення цілісності
6. Концепція п`яти дев`яток
7. Захист домену кібербезпеки
8. Як стати спеціалістом з кібербезпеки

Зареєструватись

I-CSO – CyberSecurity Operations

Дати проведення: 15-17 вересня; 6-8 жовтня; 15-17 грудня 2021

Місце проведення: ISSP Training Center, м. Київ, вул. Радищева 10/14

Тривалість: 3 дні з 10:00 до 18:00 з перервами на обід та кава-паузи

Мова викладання: українська / російська

ПРО КУРС

Курс охоплює знання та навички, необхідні для успішного виконання завдань та обов'язків молодшого рівня аналітики безпеки в Центрі моніторингу та управління безпекою (SOC), а саме: підготовка безпечного середовища для діяльності та аналізу кібербезпеки; аналіз мережевих протоколів і служб; надавати пояснення, як працює мережева інфраструктура; класифікувати різні типи мережевих атак Використовувати засоби моніторингу мережі для виявлення атак на мережні протоколи та служби. Застосування різних способів запобігання несанкціонованого доступу до комп'ютерних мереж, хостів і даних Проводити оцінювання попереджень про безпеку мережі Аналіз мережевого вторгнення, з метою виявлення скомпрометованих хостів та вразливостей. Застосування моделей реагування для вирішення інцидентів безпеки

ДЛЯ КОГО

Даний курс орієнтовано на підготовку IT-фахівців для роботи аналітиками з кібербезпеки в Центрах моніторингу та управління безпекою (SOC)

Слухачам потрібно мати такі знання та навички:

- Базові знання про Windows і Linux
- Основні принципи роботи в мережі
- Загальні відомості про двійкові та 16-річні числові системи
- Знання основних принципів програмування
- Базові навички роботи з запитами SQL

ПРОГРАМА КУРСУ

1. Кібербезпека та SOC
2. OS Windows
3. OS Linux
4. Принципи забезпечення мережної безпеки
5. Детальний аналіз мережевої атаки
6. Захист мережі
7. Криптографія та PKI
8. Захист та аналіз кінцевих пристроїв
9. Моніторинг безпеки
10. Аналіз інформації про вторгнення
11. Реагування на інциденти та їх обробка.

Окрім заповнення реєстраційної форми - будь ласка, пройдіть вхідне тестування за посиланням:
https://forms.office.com/Pages/ResponsePage.aspx?id=JxYh3iVPD0O9ljwVuWV2PRcCeVn7hdJJtzQbWrzhIBxUMDFDOEc2QkxJMFQ4UlNRUDYwQ0xRNVVYNS4u

Зареєструватись

SSS – SOC Survival Skills

Дати проведення: 20-21 вересня 2021
Місце проведення: ISSP Training Center, м. Київ, вул. Радищева 10/14
Тривалість: 2 дні з 10:00 до 18:00 з перервами на обід та кава-паузи
Мова викладання: російська

ПРО КУРС

Курс охоплює основи для спеціалістів Операційного центру безпеки (SOC), та охоплює основні навички безпеки для аналітиків SOC

ДЛЯ КОГО

- Адміністратор мережі
- Інженер мережі
- Адміністратор/Інженер/Аналітик із мережевої безпеки
- Аналітик/Оператор з безпеки
- Технік захисту мережі

Учасникам потрібно знати:
- Основи мережевих технологій, модель OSI, модель TCP/IP
- Основи Powershell Scripting (базове використання)
- Основи Linux Bash Scripting (будь-який дистрибутив)
- Знання Active Directory
- Досвід та участь у реагування на більше 100 інцидентів

ПРОГРАМА КУРСУ

1. Endpoint Analysis
- Windows Fundamental
  - Friendship with Powershell
  - Core Windows network commands to know
  - Windows Processes
  - DeepBlue CLI/DeepWhite CLI
- Linux Fundamental
  - Linux Filesystem
  - Users and Privileges
  - Linux CLI and Scripting
  - Processes in Linux
  - Networking in Linux
  - Using and understanding the power of Nmap

2. Server Analysis
- Access to logs
- Getting align with CIS Benchmarks
- Config Files, Port and Services

3. Networking & TCP/IP
- Headers and RFCs
- Shodan Search Engine
- Art of using tcpdump & Wireshark
- Packet Analysis

4. Memory Forensics
- Say hello to Volatility
- Memory Analysis: Network
- Memory Analysis: Process
- Memory Analysis: DLL and CLI

5. Egress Traffic Analysis
- MITRE & Egress
- Real Intelligence Threat Analytics
- Get into Rita
- User agents, JA3, …
- ELK / Security Onion

6. User Entity Behavior Analytics
- MITRE and UEBA
- Log Analysis
  - AD Logs
  - Log Tracer
  - Log Anomalies
  - Which Logs are important to Collect/Check
  - Sysmon
- Certificate Analysis
- Lateral Movement

7. Endpoint Protection Analysis
- EDR

8. Internal Segmentation and Isolation

9. Vulnerability Management

10. Using Tools
- Burp
- ZAP
- Security Scanners like Nessus

Зареєструватись

Спеціаліст та внутрішній аудитор з СУІБ (Система управління інформаційною безпекою) на основі стандарту ISO / IEC 27001

Дати проведення: 22-24 вересня; 11-13 жовтня 2021

Місце проведення: ISSP Training Center, м. Київ, вул. Радищева 10/14

Тривалість: 3 дні з 10:00 до 18:00 з перервами на обід та кава-паузи

Мова викладання: українська / російська

ДЛЯ КОГО

- Фахівці з інформаційної безпеки;
- IT-фахівці, які бажають отримати глибокі знання основних процесів в системі управління інформаційною безпекою (СУІБ);
- Співробітники, залучені до впровадження стандарту ISO 27001;
- Технічні фахівці, які беруть участь в процесах, пов'язаних з СУІБ;
- Аудитори;
- Керівники і старші менеджери, відповідальні за IT-управління та управління ризиками підприємства.

ДАНИЙ КУРС ДОПОМОЖЕ

- Впорядкувати знання про те, які елементи системи інформаційної безпеки потрібно впроваджувати і як робити це без помилок.
- Доповнити існуючі знання і скласти їх в органічну систему, зручну для використання в довгостроковому плануванні та щоденній роботі.
- Навчитися впроваджувати комплексну систему управління інформаційною безпекою на підприємстві.
- Обговорити практичні кейси, і проаналізувати можливі помилки та нюанси, які можуть відігравати вирішальну роль.
- Будувати і розвивати стосунки з професіоналами, які щодня захищають IT-системи різних підприємств від нових загроз, обмінюватися інформацією про нові загрози і методи боротьби з ними.
- Організувати процеси проведення внутрішніх аудитів в межах функціонування СУІБ.

ПРОГРАМА КУРСУ

1. Міжнародна організація по стандартизації ISO
   - Загальна інформація
   - Принципи
   - Організаційна структура
   - Цикл розробки стандарту
2. Сертифікація
   - Терміни
   - Схема
   - Взаємне визнання результатів
3. Серія стандартів 27000
4. Загальні відомості про Стандарт
   - Загальні відомості
   - Завдання, що вирішуються
   - Перелік доменів безпеки
   - Мета та принципи Стандарту
   - Цикл PDCA
   - Виклики під час впровадження
5. Огляд вимог основної частини Стандарту
   - Структура
   - Контекст
   - Лідерство
   - Планування
   - Керування ризиками інформаційної безпеки (детальний огляд процедури)
   - Підтримка
   - Експлуатація
   - Оцінка результативності
   - Вдосконалення
6. Додаток А. Каталог цілей управління і елементів управління
7. Аудит СУІБ
   - Стандарти
   - Терміни та визначення
   - Завдання
   - Види аудиту
   - Учасники аудиту
   - Принципи
   - Етапи
   - Аналіз документації
   - Підготовка плану проведення
   - Збір та верифікація інформації
   - Результати
   - Висновки аудиту
   - Підготовка звіту
8. Етапність впровадження СУІБ
9. Огляд документації СУІБ

Зареєструватись

CND – Certified Network Defender

Дати проведення: 27 вересня – 1 жовтня 2021

Місце проведення: ISSP Training Center, м. Київ, вул. Радищева 10/14

Тривалість: 5 днів з 10:00 до 18:00 з перервами на обід та кава-паузи

Мова викладання: українська / російська

Навчальний комплект включає в себе:
- офіційні навчальні матеріали в електронному вигляді від EC-Council – англійською мовою (доступ на 12 місяців);
- доступ до лабораторного середовища iLabs (строком на 6 місяців);
- ваучер для складання іспиту (дійсний протягом 12 місяців).

ПРО КУРС

Курс CND орієнтований навчити Адміністраторів мереж захищати, виявляти, реагувати та прогнозувати загрози в мережі. Це вдається досягти завдяки знанням та навичкам, пов'язаних з компонентами мережі, трафіком, продуктивністю і використанням, топологією мережі, розташуванням системи та політик безпеки.

ДЛЯ КОГО

- Адміністратори / інженери мережі
- Адміністратори / інженери / аналітики мережевої безпеки
- Інженери з кібербезпеки
- Аналітики безпеки
- Техніки захисту мережі
- Оператори безпеки
- Спеціалісти з CybersecurityOperations, а також ті, хто прагне будувати кар'єру в галузі кібербезпеки

УВАГА: Обов'язкове знання англійської мови на рівні не нижче intermediate (всі навчальні матеріали надаються англійською)

ПРОГРАМА КУРСУ

1. Атаки на мережу та стратегії оборони
2. Адміністративна безпека мережі
3. Технічна безпека мережі
4. Безпека периметру мережі
5. Ендпоінт-безпека - системи Windows
6. Ендпоінт-безпека - системи Linux
7. Ендпоінт-безпека - мобільні пристрої
8. Ендпоінт-безпека - Пристрої IoT
9. Безпека адміністративних додатків
10. Захист даних
11. Безпека віртуальної мережі підприємства
12. Безпека хмарної мережі підприємства
13. Безпека бездротової мережі підприємства
14. Моніторинг та аналіз мережевого трафіку
15. Моніторинг та аналіз журналів мережі
16. Реагування на інциденти та розслідування
17. Безперервність бізнесу та відновлення після катастроф
18. Передбачення ризику з управлінням ризиками
19. Оцінювання вразливостей за допомогою аналізу поверхні атаки
20. Прогнозування загроз за допомогою розвідки кібервразливостей

ДАНИЙ КУРС ДОПОМОЖЕ

- Розуміти управління безпекою мережі
- Встановлювати політики та процедури безпеки мережі
- Адмініструвати безпеки Windows і Linux
- Налаштовувати безпеку мобільних пристроїв та пристроїв IoT
- Впроваджувати методи захисту даних у мережах
- Вбудовувати безпеку технологій віртуалізації
- Визначати хмарну та бездротову безпеки
- Розгортати та використовувати інструменти оцінки ризику
- Вивчити основи первинної відповіді та форенсіки.
- Розуміти показники компрометації, атаки та впливу (IoC, IoA, IoE)
- Нарощувати можливості розвідки загроз.
- Виконувати встановлення та моніторинг системи управління журналюванням.
- Впроваджувати безпеку кінцевих пристроїв.
- Налаштовувати оптимальні рішення брандмауера
- Розуміти та використовувати технології IDS / IPS
- Імплементувати систему AAA (автентифікація, авторизація та облік)

Зареєструватись

CISM – Certified Information Security Manager

Вимоги до учасників:
- знання англійської мови на рівні не нижче intermediate (всі навчальні матеріали надаються англійською)

Дати проведення: 25-28 жовтня 2021

Місце проведення: ISSP Training Center, м. Київ, вул. Радищева 10/14

Тривалість: 4 дні з 10:00 до 18:00 з перервами на обід та кава-паузи

Мова викладання: українська / російська

Навчальний комплект включає в себе:
- офіційні навчальні матеріали в електронному вигляді від ISACA – англійською мовою;
- ваучер для складання іспиту

ДЛЯ КОГО

- Професіонали, які готуються стати сертифікованими CISM
- Спеціалісти з сертифікацією CISA або CISSP, які прагнуть перейти до управління інформаційною безпекою
- Фахівці з загального управління безпекою, які прагнуть перейти до інформаційної безпеки
- Менеджери з інформаційної безпеки
- Фахівці Middle рівня, які змінюють кар'єру

ДАНИЙ КУРС ДОПОМОЖЕ

- Встановлювати та/або підтримувати фреймворк управління інформаційною безпекою та допоміжними процесами для забезпечення відповідності стратегії інформаційної безпеки згідно організаційних цілей та завдань.
- Керувати інформаційними ризиками до прийнятного рівня на основі схильностей до ризику з метою досягнення цілей та завдань організації.
- Розробляти та підтримувати програму інформаційної безпеки, яка визначає, управляє та захищає активи організації, узгоджено зі стратегією інформаційної безпеки та бізнес -цілями, підтримуючи тим самим стан безпеки організації.
- Планувати, встановлювати та керувати здатністю виявляти, досліджувати, реагувати та відновлюватися після інцидентів інформаційної безпеки, щоб мінімізувати вплив на бізнес.

ПРОГРАМА КУРСУ

Домен 1 - Управління інформаційною безпекою
- Пояснення необхідності та бажаними результатами ефективної стратегії інформаційної безпеки
- Створення стратегії інформаційної безпеки, узгодженої з цілями та завданнями організації
- Отримання підтримки зацікавлених сторін, з використанням бізнес-кейсів
- Визначення ключових ролей та відповідальності, необхідних для виконання плану дій
- Встановлення метрики для вимірювання та моніторингу ефективності управління безпекою

Домен 2 - Управління інформаційними ризиками
- Пояснення важливості управління ризиками як інструменту задоволення потреб бізнесу та розробка програми управління безпекою для підтримки цих потреб
- Визначення, оцінка та реагування на ризик відповідним способом, визначеним організаційними директивами
- Оцінювання доцільності та ефективності засобів контролю інформаційної безпеки
- Організація ефективного повідомлення про ризик інформаційної безпеки

Домен 3 - Розробка та управління програмами інформаційної безпеки
- Вирівнювання вимог програми захисту інформації згідно вимог інших функцій бізнесу
- Управління ресурсами програми захисту інформації
- Розробка та впровадження засобів захисту інформації
- Включення вимог безпеки інформації до контрактів, угод та зовнішніх управлінських процесів

Домен 4 - Управління інцидентами з інформаційної безпеки
- Розуміння концепції та практики управління інцидентами
- Визначення складових Плану реагування на інциденти та оцінювання його ефективності
- Розуміння ключових концепцій планування безперервності бізнесу, та Плану ліквідації наслідків катастроф
- Ознайомлення із методами, які зазвичай використовуються для перевірки можливостей реагування на інциденти

Зареєструватись

CISA – Certified Information Systems Auditor

Вимоги до учасників:
- знання англійської мови на рівні не нижче intermediate (всі навчальні матеріали надаються англійською)

Дати проведення: 8-12 листопада 2021

Місце проведення: ISSP Training Center, м. Київ, вул. Радищева 10/14

Тривалість: 5 днів з 10:00 до 18:00 з перервами на обід та кава-паузи

Мова викладання: українська / російська

Навчальний комплект включає в себе:
- офіційні навчальні матеріали в електронному вигляді від ISACA – англійською мовою;
- ваучер для складання іспиту

ДЛЯ КОГО

- Професіонали, які готуються стати сертифікованими CISA
- Фінансові аудитори, які переходять на IT -аудит
- IT-спеціалісти, які переходять на IT-аудит
- Фахівці Middle рівня, які змінюють кар'єру

ДАНИЙ КУРС ДОПОМОЖЕ

- Отримати краще розуміння проведення аудиту ІБ та керівних принципів і стандартів ІБ
- Розвивати практичні знання з п'яти доменів CISA.

Зареєструватись

ПРОГРАМА КУРСУ

Домен 1 - Процес аудиту інформаційної системи
1. Планування аудиту, щоб визначити захищеність та контрольовані інформаційні системи, та чи забезпечують вони цінність для організації.
2. Проведення аудиту відповідно до стандартів аудиту ІБ та стратегії аудиту ІБ на основі ризиків.
3. Комунікації з зацікавленими сторонами про прогрес аудиту, висновки, результати та рекомендації.
4. Проведення контролю аудиту, з метою оцінки якості пропрацювання ризиків.
5. Оцінювання управління IT та моніторинг контролів.
6. Використання інструментів аналізу даних з метою спрощення процесів аудиту.
7. Забезпечення консультаційних послуг та вказівок для організації з метою покращення якості та контролю інформаційних систем.
8. Визначення можливостей для процесних удосконалень IT -політик та практик.

Домен 2 - Загальне управління та менеджмент IT
1. Оцінювання стратегії IT для узгодження зі стратегіями та цілями організації.
2. Оцінювання ефективності структури управління IT та організаційної структури IT.
3. Оцінювання управління IT-політикою та практиками.
4. Оцінювання політики та практики IT організації на відповідність нормативним та правовим вимогам.
5. Оцінювання управління IT -ресурсами та портфоліо для узгодження зі стратегією та цілями організації.
6. Оцінювання політики та практики управління ризиками в організації.
7. Оцінювання управління IT та моніторинг контролів.
8. Оцінювання моніторингу та звітність за ключовими показниками ефективності IT (KPI).
9. Оцінювання відповідності вимогам бізнесу процесів відбору IT - постачальників та управління контрактами.
10. Оцінювання практики управління IT-сервісами відповідно бізнес-вимог.
11. Проведення періодичного огляду інформаційних систем та архітектури підприємства.
12. Оцінювання політики та практики управління даними.
13. Оцінювання програми інформаційної безпеки, з метою визначення її ефективності та відповідності стратегії і цілям організації.
14. Оцінювання потенційних можливостей та загроз, пов'язаних з новими технологіями, нормативними актами та галузевими практиками.

Домен 3 - Отримання, розробка та впровадження інформаційних систем
1. Оцінка відповідності бізнес-критеріїв та запропонованих змін у інформаційних системах з цілями бізнесу.
2. Оцінювання політики та практик управління проектами в організації.
3. Оцінювання контролів на всіх етапах життєвого циклу розробки інформаційних систем.
4. Оцінювання готовності інформаційних систем до впровадження та міграції у виробництво.
5. Проведення огляду систем після впровадження, з метою визначення відповідності результатів проекту, контролів та вимог.
6. Оцінювання політики та практик управління змінами, конфігурацією, релізами та патчами.

Домен 4 - Операції інформаційних систем та стійкість бізнесу
1. Оцінювання здатності організації продовжувати свою діяльність.
2. Оцінювання відповідності вимогам бізнесу практик управління IT-сервісами.
3. Проведення періодичного огляду інформаційних систем та архітектури підприємства.
4. Оцінювання IT-операцій з метою визначення ефективності їх контролю та їх можливість підтримувати цілі організації.
5. Оцінювання практик підтримки IT, з метою визначення ефективності їх контролю та їх можливість підтримувати цілі організації.
6. Оцінювання практики управління базами даних.
7. Оцінювання політики та практики управління даними.
8. Оцінювання політики та практики управління проблемами та інцидентами.
9. Оцінювання політики та практики управління змінами, конфігурацією, релізами та патчами.
10. Оцінювання обчислення кінцевого користувача, з метою визначення ефективності контролю процесів.

Домен 5 - Захист інформаційних активів
1. Проведення аудиту відповідно до стандартів аудиту ІБ та стратегії аудиту ІБ на основі ризиків.
2. Оцінювання політики та практики управління проблемами та інцидентами.
3. Оцінювання політики та практики інформаційної безпеки та конфіденційності в організації.
4. Оцінювання контролів доступу, з метою визначення відповідності заходів охорони інформаційних активів.
5. Оцінювання контролів логічної безпеки для перевірки конфіденційності, цілісності та доступності інформації.
6. Оцінювання практики класифікації даних для узгодження з політиками організації та зовнішніми вимогами.
7. Оцінювання політики та практики, пов'язаних з управлінням життєвим циклом активів.
8. Оцінювання програми інформаційної безпеки, з метою визначення її ефективності та відповідності стратегії і цілям організації.
9. Тестування технічної безпеки з метою виявлення потенційних загроз та вразливостей.
10. Оцінювання потенційних можливостей та загроз, що пов'язані з новими технологіями, нормативними актами та галузевими практиками.

CEH – Certified Ethical Hacker

Дати проведення: 22-26 листопада 2021

Місце проведення: ISSP Training Center, м. Київ, вул. Радищева 10/14

Тривалість: 5 днів з 10:00 до 18:00 з перервами на обід та кава-паузи

Мова викладання: українська / російська

Навчальний комплект включає в себе:
- офіційні навчальні матеріали в електронному вигляді від EC-Council – англійською мовою (доступ на 12 місяців);
- доступ до лабораторного середовища iLabs (строком на 6 місяців);
- ваучер для складання іспиту (дійсний протягом 12 місяців).

ПРО КУРС

CEH – провідна навчальна і сертифікаційна програма з етичного хакінгу в галузі кібербезпеки. Учасники курсу перевіряють систему на наявність слабких місць і вразливостей, використовуючи ті ж самі інструменти та експлойти, що і зловмисні хакери. Даний курс вчить, як хакери думають і діють - щоб ви навчилися краще налаштовувати інфраструктуру безпеки вашої організації та захищатись від майбутніх атак.

ДЛЯ КОГО

- Аналітики/адміністратори інформаційної безпеки
- Співробітники служби захисту інформації (IA)
- Менеджери/спеціалісти з інформаційної безпеки
- Інженери/менеджери з безпеки інформаційних систем
- Фахівці/спеціалісти з інформаційної безпеки
- Аудитори інформаційної безпеки та IT
- Аналітики вразливостей, ризиків і загроз
- Системні адміністратори
- Мережеві адміністратори та інженери

УВАГА: Обов'язкове знання англійської мови на рівні не нижче intermediate (всі навчальні матеріали надаються англійською)

ПРОГРАМА КУРСУ

1. Вступ до етичного хакінгу
2. Футпринтинг (відбитки) та розвідка
3. Сканування мереж
4. Енумерація (деталізація)
5. Аналіз вразливостей
6. Системний хакінг
7. Загрози зловмисного коду
8. Сніффінг
9. Соціальна інженерія
10. Відмова в обслуговуванні (DoS)
11. Перехоплення сесії
12. Методи ухилення від IDS, брандмауерів та honeypots
13. Хакінг веб-серверів
14. Хакінг веб-додатків
15. Хакінг SQL
16. Хакінг бездротових мереж
17. Хакінг мобільних платформ
18. Хакінг IoT та OT
19. Хмарні обчислення
20. Криптографія

ДАНИЙ КУРС ДОПОМОЖЕ

- Будова світу інформаційної безпеки, етичний хакінг, контролі інформаційної безпеки, стандарти та закони, що стосуються інформаційної безпеки.
- Методологія системного хакінгу, стеганографії, атаки з використанням стеганалізу, “замітання слідів”, які спрямовані на розкриття системних та мережних вразливостей.
- Типи шкідливих програм (троянські програми, віруси, хробаки тощо), аудит системи на наявність шкідливих програм, аналіз шкідливого коду та відповідні контрзаходи.
- Методи ідентифікації атак соціальної інженерії, проведення аудиту вразливостей користувачів, впровадження заходів протидії соціальній інженерії.
- Методи та інструменти DoS / DDoS-атаки, спрямовані на перевірку цілі, заходи протидії DoS / DDoS.
- Техніки атак SQL-injection, інструменти для визначення таких атак та заходи протидії їм.
- Бездротове шифрування, методологія та інструменти бездротового хакінгу, інструментарій бездротового захисту.
- Вектор атаки мобільних платформ, використання вразливостей Android,принципи та інструменти мобільної безпеки.
- Методи обходу фаєрволів, IDS та honeypot, інструменти та методи обходу - для аудиту периметру мережі на наявність слабких місць та відповідні контрзаходи.
- Вразливості IoT та OT, організація захисту пристроїв IoT та OT.
- Криптографічні шифри, інфраструктура відкритих ключів (PKI), криптографічні атаки та інструменти криптоаналізу.

Зареєструватись

I-OSINT – Open-Source Intelligence (Вступний курс)

ПРО КУРС

Розвідка на основі відкритих джерел Open Source Intelligence, OSINT) дисципліна, що включає в себе пошук, збір та аналіз інформації з відкритих ресурсів, без порушення законів.

Тренінг «Вступ до OSINT» дозволить учасникам отримати широкий набір знань для проведення такої розвідки, обробки отриманих даних та складання звітів відповідно до цілей.

Окрім знань, ви також отримаєте необхідні для вирішення
цих завдань навички, серед яких:

- збереження вашої анонімності
- профілювання зловмисників
- аналіз метаданих
- автоматичний збір даних
- лог аналіз і кореляція

Курс містить багато практичного матеріалу та вправ.

ДЛЯ КОГО

Тренінг адаптовано для широкої аудиторії з базовим рівнем підготовки.

Дати проведення: 6-8 грудня 2021

Місце проведення: ISSP Training Center, м. Київ, вул. Радищева 10/14

Тривалість: 3 дні з 10:00 до 18:00 з перервами на обід та кава-паузи

Мова викладання: українська / російська

ПРОГРАМА КУРСУ

01. Ресурси для OSINT

- OSINT framework
- awesome OSINT

02. Анонімність табезпекаонлайн

- Virtual machines (Vmwareplayer, Virtualbox).
- Snapshots of virtual machines.
- Linux LiveCDs(Tails). Kali Linux
- Tor, Tor browser
- proxychains, socksify.
- VPN, Double-VPN.
- Proxy servers
- I2P
- Bitcoin
- Firewalls.
- Custom user agents.
- Browser protected mode.
- NoScript.
- Disable browser plugins/extensions/addons.
- Dekloaking(WebRTC-STUN leak, DNS leak, User-agent and device properties leak, Sticky cookies).
- Screenshot anonymization.
- Document metadata anonymization, exiftool.
- Virustotaland public sandbox precaution measures.
- Privnote, anonymous chats
- Precation measures with office and pdf documents.

03. Профайлінг

- Google search. Advanced Google search. Google dorks
- Yandex search. Advanced Yandex search
- Bing search. Advanced Bing search
- Other search engines (yahoo, baidu, duckduck)
- IP address
- AS and BGP, looking glass
- Whois. Domain names and DNS.
- Dig/nslookup
- viewdns.info. dnsdumpster. Dnsrecon.
- www.tcpiputils.com
- MaxMindgeoip, IP2location
- Shodan
- image search engines (google image, tineye, etc.)
- Google translate
- Facebook; LinkedIn; Vkontakte; Odnoklasniki; Google+; Instagram; Twitter
- CheckUserNames.com
- Pastebin
- Virustotal
- State registers
- State databases
- HTML comments
- X509 certificate analysis
- Email headers analysis
- Crimeflareand real IP detection, cloudfailtool.
- Short link expanders
- Webarchives(archive.org)
- Blockchain.info
- Video collection (download helper)
- Desktop screen capture
- Keepnote

04. Аналіз журналу

- grep
- file
- binwalk
- sed and awk
- radare2
- log2timeline
- catdoc

05. Аналіз метаданих

- exiftool
- executable files metadata (PE/ELF)
- FOCA
- Metagoofil

06. Автоматичний пошук

- Python scripting
- Shell scripting
- wget
- curl
- httrack
- Google alerts
- recon-ng
- theharvester
- Maltego
- Twitter python API.
- Spiderfoot
- OSINT Opsectool
- IBM i2
- GeoCreepy
- dataspoit

07. Взаємодії

- Account recovery tricks (partial data display)
- Password reset questions (e.g. phone number, etc.)
- Out of office messages
- Contact forms for confirmation email and its headers
- Social engineering, pretext
- cracking password hashes (john, google search, crackstation, hashcat, custom john rules, cewl, crunch)
- Web bugs
- Trojanizedbinaries, RATs
- Packers/cryptors, AV evasion
- Exploits in documents (Office, PDF)
- Macros in the documents
- Java exploits
- Browser exploits
- User enumeration exploits
- Dekloaking
- XSS and Beef
- DOS on hacker resources

Зареєструватись

CISSP – Certified Information Systems Security Professional

Вимоги до учасників:
- досвід у принаймні 2 з 8 доменів CISSP (див. перелік в програмі курсу)
- знання англійської мови на рівні не нижче intermediate (всі навчальні матеріали надаються англійською)

Дати проведення: 29 листопада – 3 грудня 2021

Місце проведення: ISSP Training Center, м. Київ, вул. Радищева 10/14

Тривалість: 5 днів з 10:00 до 18:00 з перервами на обід та кава-паузи

Мова викладання: українська / російська

Навчальний комплект включає в себе:
- офіційні навчальні матеріали в електронному вигляді від ISC2 – англійською мовою (доступ на 12 місяців);

ПРО КУРС

CISSP – це найбільш всесвітньо-визнана сертифікація у сфері кібербезпеки. Сертифікація CISSP підтверджує професійний рівень у галузі інформаційної безпеки, а також високий технічний та управлінський рівень знань, досвіду, що дозволяє проектувати, впроваджувати та контролювати стан безпеки організації.

ДЛЯ КОГО

- Консультанти з питань безпеки
- Менеджери безпеки
- IT-директори / менеджери
- Архітектори мережі
- Аудитори безпеки
- Архітектори безпеки
- Аналітики з питань безпеки
- Інженери систем безпеки
- Директори з інформаційної безпеки
- Директори з безпеки
- Архітектори мережі

ПРОГРАМА КУРСУ РОЗКРИВАЄ ТЕМИ:

1. Середовище інформаційної безпеки
2. Захист інформаційних активів
3. Управління ідентифікацією та доступом
4. Архітектура та інженерія безпеки
5. Безпека зв'язку та мережі
6. Безпека розробки програмного забезпечення
7. Аналіз та тестування безпеки
8. Операційна безпека
9. Давайте все поєднаємо
10. Інформація про сертифікацію CISSP

ДАНИЙ КУРС ДОПОМОЖЕ

- Розуміти та застосовувати основні концепції та методи, що стосуються галузей інформаційних технологій та безпеки
- Узгоджувати операційні цілі організації із функціями та впровадженнями безпеки
- Розуміти, як захистити активи організації під час їхнього життєвого циклу
- Розуміти концепції, принципи структуру та стандарти для використання при проектуванні, організації впровадження, моніторингу та захисту операційних систем, обладнання, мереж, програм і засобів управління конфіденційністю, цілісністю та доступністю.
- Впроваджувати безпеку системи шляхом застосування принципів проектування безпеки та застосування відповідних заходів захисту від вразливостей загальних типів, що існують в інформаційних системах.
- Розуміти важливість криптографії та функцій безпеки, які вона може забезпечити у сучасному цифровому та інформаційному світі.
- Розуміти вплив елементів фізичної безпеки на безпеку інформаційної системи та застосовувати принципи безпечного проектування, щоб оцінити або рекомендувати відповідні засоби фізичного захисту
- Зрозуміти складові безпеки комунікацій та мереж, вміти надавати детальний опис функціонування комунікацій та мереж.
- Знати концепцію та архітектуру, пов'язані технології, системи і протоколи у відповідності з кожним рівнем моделі Open System Interconnection (OSI).
- Визначати, відповідно до практики безпеки середовищ, стандартні умови для застосування фізичного та логічного контролю доступу до таких середовищ
- Надавати оцінку різним моделям контролю доступу на основі відповідності вимогам безпеки бізнесу.
- Знати основні методи розробки та перевірки стратегій аудиту і тестування, згідно вимог бізнесу..
- Посилити та оптимізувати операційні функції та спроможності організації, застосовуючи відповідні засоби контролю та контрзаходи
- Розпізнавати ризики для діяльності організації та аналізувати нестандартні загрози, вразливості і відповідні сповіщення.
- Розуміти життєвий цикл системи (SLC), життєвий цикл розробки програмного забезпечення (SDLC) та способи застосування захисту до них; визначити, які засоби безпеки відповідають середовищу розробки; надавати оцінку ефективності програмного забезпечення

Зареєструватись

Реєстрація та контакти

Реєстрація за посиланням:
https://form.collect.dai.com/x/TEKr1ulA

За додатковою інформацією звертатись:
Кирило Кулаковський +380 44 594 80 18 kkulakovskyi@issp.com

ISSP Training center на мапі:

https://goo.gl/maps/YV1qqDGUK4aHAhVX8

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ