Програма професійного розвитку в сфері кібербезпеки та реінтеграції для ветеран «Кіберзахисники 2024»

Період навчання	04 березня 2024 – 18 липня 2024 року
Тривалість навчання	До 5 місяців
Цільова група	Ветерани та Ветеранки
Кількість учасників програми	28 ветеранів
Сфера навчання	Кібербезпека
Метод навчання	Лекції, практичні завдання, групова робота
Формат навчання	Онлайн/офлайн
Кількість годин лекційних занять	80 годин
Кількість годин практичних занять	160 годин
Додаткове навчання	Англійська мова від British Council
Закінчення програми	Свідоцтво про підвищення кваліфікації від КПІ ім. Ігоря Сікорського
Міжнародна сертифікація	Тренінг та здобуття сертифікації: - eJPT Certification, JuniorPenetration Tester. - Systems Security Certified Practitioner.

Фонд цивільних досліджень та розвитку США (CRDF Global) імплементували програму професійного розвитку для ветеранів та ветеранок у сфері кібербезпеки та реінтеграції **«Кіберзахисники»**, яка спрямована на забезпечення комплексного навчання у сфері

кіберзахисту та кібеоборони, надання професійного розвитку та успішну реінтеграцію учасників у "цивільне життя".

Метою даної програми є підтримка ветеранів та ветеранок у нових кар'єрних можливостях у сфері кібербезпеки у державному та/або приватному секторах України, а також посилення спроможності ветеранів і ветеранок пристосовуватися до цивільного життя в громаді через формування соціальних компетентностей (знань, навичок, особистісних якостей) у ході менторської підтримки, кар'єрного консультування та психосоціальної підтримки. Програма пропонує ветеранам не лише нові навички та знання, а й можливість зберегти відданість захисту країни в цифровому світі, сприяючи зміцненню систем захисту цифрової інфраструктури в Україні.

Навчальні модулі

Модулі	**Результати**
Теорія Безпеки	Розуміння тріади CIA, моделі сучасних APT-атак та тенденції в кібербезпеці, знання про різні кібератаки та їх наслідки.
Методи та Механізми Безпеки	Вміння ідентифікувати, аутентифікувати, контролювати доступ, аудит, підписувати, шифрувати, захищати від відмови та використовувати антивірусний захист.
Вступ до Криптографії	Симетрична криптографія. - Криптографічні механізми. Модель захищеного каналу зв'язку. Шифр одноразового блокноту. Потокові шифри. Блокові шифри. Геш-функції. Асиметрична криптографія -Алгоритм Діффі-Хеллмана. Асиметричні шифри. RSA. Цифрові підписи. Атака `Man-in-the-Middle`.
Malware	Ідентифікування різних типів зловмисного ПЗ та розуміння принципів і техніки антивірусного захисту.
Network security	Аналізування мережевих пакетів, виконання сканування мережі та зняття трафіку, а також розуміння вразливості мережевих протоколів. Ethernet та Internet Protocol(IP). ACL та Firewall. IDL та IPS. Проблеми протоколів 1.5-3.5 рівнів, інструменти експлуатації від фізичного рівня до ICMP та техніки захисту. Протоколи транспортного та прикладного рівня

Operating systems security	Розуміння роботи, конфігурації та експлуатації Windows та Linux систем
Безпека Веб-Додатків	Протокол HTTP; вразливості веб-додатків; типи атак на веб-додатки: завантаження та виконання довільних файлів, в тому числі локальних, віддалене включення файлів, підробка міжсайтових запитів, міжсайтовий скриптинг; механізми захисту веб-серверів та веб-додатків; виправлення вразливостей у веб-додатках
Penetration Testing	Знання та навички у сфері тестування на проникнення, розуміння процедур відповідального тестування на проникнення, досвід використання інструментів тестування на проникнення. Знання методології тестування на проникнення - Cyber Kill Chain.
Цифрова Криміналістика та Реагування на Інциденти	Розуміння процесу цифрової експертизи. Навички відновлення інформації, збору інформації на низькому рівні, RAM- аналізу
Cloud Fundamentals	Базові концепції хмарних обчислень, моделі надання послуг (IaaS, PaaS, SaaS), типи хмарних розгортань (публічні, приватні, гібридні) та принципи масштабованості, високої доступності та безпеки в хмарі. Основи AWS IAM, Обчислювальні технології та сервіси, Технології та сервіси зберігання, Мережеві технології, Безпека, відповідність та управління AWS.

Отримані Практичні Навички та Інструменти

Під час практичних занять учасники отримали практичний досвід роботи з різними інструментами та техніками кібербезпеки, включаючи:

- **Nmap:** Сканування та цифрова розвідка мережі. Практичне використання nmap скриптів.
- **Hydra:** Робота з інструментом Hydra.
  SMB: Базові принципи роботи SMB протоколу та файлових дистрибуцій. SMB user enumeration. Bruteforce та Dictionary Attacks.
- **CyberChef:** Практичне використання інструменту CyberChef для шифрування, дешифрування, кодування, роботи з хешами та аналізу даних.

- **Hashes:** Принципи роботи хеш-функцій. Ідентифікація різних типів хешування. Hash cracking.
- **Python:** Аналіз коду шифраторів та створення дешифраторів на основі аналізу.
- **Linux:** Адміністрування та конфігурація операційної системи Linux.
- **Hashcat та John the Ripper:** Використання Hashcat та John the Ripper для роботи з паролями.
- **OpenSSL:** Робота з криптографією, генерування ключів та сертифікатів, шифрування та дешифрування даних.
- **Strings:** Аналіз та видобування корисної інформації з файлів шкідливого програмного забезпечення.
- **Virustotal:** Використання для перевірки файлів на наявність вірусів, троянців, червей та іншого шкідливого програмного забезпечення.
- **LOKI, THOR, FENRIR, YAYA, VALHALLA:** Використання для пошуку шкідливого програмного забезпечення та інших підозрілих активностей на хості.
- **YARA rules:** Виявлення та класифікація шкідливого програмного забезпечення.
- **Wireshark:** Аналіз мережевого трафіку та перехоплення мережевих пакетів.
- **Enum4linux**: Використання для переліку та аудиту інформації про SMB/Windows мережі.
- **Crackmapexec:** виконання атак та отримання інформації про мережеві ресурси.
- **BloodHound**: Виявлення шляхів атаки в мережі. Використовується для візуалізації та дослідження взаємозв'язків у доменах AD.
- **SharpHound**: Збір інформації з Active Directory про користувачів, групи, комп'ютери та інші об'єкти.
- **PowerSploit**: Експлуатація вразливостей та виконання атак у середовищі Windows.
- **Windows Fundamentals, Active Directory:** Адміністрування та конфігурація операційної системи Windows. Розуміння принципів роботи Active Directory.
- **Mimikatz:** Екстракція паролів, хешів паролів та Kerberos tickets в системах Windows..
- **BurpSuite:** Практичне тестування безпеки веб-додатків.
- **Cross-Site Scripting (XSS):** Принципи роботи XSS атак. Виявлення та експлуатація XSS-вразливостей.
- **Cross-Site Request Forgery (CSRF):** Принципи роботи CSRF атак. Виявлення та експлуатація CSRF-вразливостей.
- **Beef (Browser Exploitation Framework):** Експлуатація вразливостей браузерів.
- **SQL Injection:** Принципи роботи атаки типу SQL-ін'єкція. Виявлення та експлуатація SQL-ін'єкцій.
- **Directory Traversal:** Принципи роботи атаки типу Directory Traversal. Виявлення вразливостей у веб-додатках, що можуть дозволити доступ до конфіденційної інформації та системних файлів.

- **OS command injection:** Принципи роботи атаки типу OS command injection. Виявлення та експлуатація OS command injection. Використання webshells.
- **SQLmap:** Автоматичне виявлення та експлуатація SQL-ін'єкцій
- **Metasploit:** Використання Metasploit Framework. Практичне налаштування Metasploit Framework. Застосування методології Cyber Kill Chain на практиці. Тестування на проникнення та експлуатація вразливостей.
- **Autopsy:** Аналіз цифрових знімків жорстких дисків.
- **Volatility:** Аналіз цифрового знімку оперативної пам'яті.
- **AWS IAM:** Управління доступом і ідентифікацією в AWS. Використання для безпечного управління доступом до сервісів і ресурсів AWS.
- **AWS EC2:** Обчислювальні ресурси в хмарі. Використання для запуску віртуальних серверів, масштабування обчислювальних потужностей та управління навантаженням.
- **AWS S3:** Об'єктне сховище даних. Використання для зберігання та отримання будь-яких обсягів даних з високою доступністю та безпекою.
- **AWS VPC:** Віртуальна приватна хмара. Використання для запуску ресурсів AWS в ізольованій віртуальній мережі, що забезпечує контроль над мережевим середовищем.
- **AWS Security services:** Комплекс сервісів для забезпечення безпеки в AWS. Огляд та використання інструментів для моніторингу, захисту даних, управління доступом та відповідності вимогам безпеки.

Протягом інтенсивного курсу навчання наші учасники опанували фундаментальні знання з кібербезпеки, що включають як теоретичні аспекти, так і практичні навички. Цей комплексний підхід до навчання дозволяє їм впевнено застосовувати набуті знання на практиці. Завдяки отриманим знанням та вмінням, наші випускники навчальної реінтеграційної програми "Кіберзахисники" готові приєднатися до Вашої команди, забезпечуючи високий рівень захисту та безпеки у вашій організації. Обираючи наших випускників, Ви отримуєте надійних, кваліфікованих фахівців, здатних ефективно реагувати на сучасні кіберзагрози та підтримувати безпеку вашої інформаційної інфраструктури.

Якщо Ваша установа зацікавлена в кваліфікованих кандидатах нашої програми, просимо Вас надати відгук та актуальні вакансії за вказаними нижче контактами. Ваші відгуки та пропозиції будуть ретельно розглянуті, і ми з радістю надамо резюме наших учасників для подальшого обговорення та запрошення на інтерв'ю.

Контакти: cyberdefenders@crdfglobal.org

Кібер Захисники
Програма професійного розвитку в сфері кібербезпеки та реінтеграції для ветеранів