РАДА НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

вул. Петра Болбочана, 8, м. Київ, 01601, телефон: (044) 255-06-50, телефакс: (044) 255-05-85

_____ № _____

_____

Голові Правління Інтернет Асоціації України (ІнАУ)

САВЧУКУ О.М

вул. О. Гончара, 15/3, офіс 22,
м. Київ, 04053

Щодо проведення кібернавчань

Шановний Олександре Михайловичу!

З метою підвищення кваліфікації фахівців телекомунікаційного сектору Національний координаційний центр кібербезпеки (далі – НКЦК) за підтримки Фонду цивільних досліджень і розвитку США в Україні (CRDF Global) реалізує дев'ятий навчальний захід із серії "Управління вразливостями". Метою навчання є покращення практичних навичок з виявлення вразливостей в інформаційних системах установ та підприємств.

Захід складатиметься з двох етапів. Перший етап проходитиме з 4 до 28 липня 2022 року і включатиме теоретичну складову та практичні заняття з тестування інформаційних систем для виявлення вразливостей, опрацювання взаємодії під час інформування про інциденти та вразливості. Перша частина зазначеного етапу буде онлайн, а друга складатиметься з виконання практичних завдань на об'єкті працевлаштування учасника. Другий етап проходитиме з 29 липня до 9 серпня 2022 року та включатиме перевірку інформаційних систем організації працівника, яка буде проведена фахівцем, залученим до заходу. Після тестування периметра кібербезпеки учасник надає відповідний звіт до НКЦК, який містить інформацію лише про типи виявлених загроз, їхню кількість та кількість ліквідованих загроз під час проведення такого тестування.

Зазначаємо, що детальна програма навчань та формат першого етапу визначені в додатку.

Для зарахування на участь у навчальному заході кандидати (технічні спеціалісти IT-підрозділів та підрозділів з кібербезпеки підприємств, установ і

організацій) повинні зареєструватися за посиланням: https://ok.ncscc.gov.ua/index.php?r=survey/index&sid=9&lang=uk або  та пройти тестування до 24.06.2022 включно.

Про результати тестування кандидатів, які пройшли відбір на навчальну програму з виявлення вразливостей, підприємства, установи і організації буде поінформовано додатково 27.06.2022.

Враховуючи викладене та цільову аудиторію вказаного курсу, просимо Вашого сприяння щодо організації залучення фахівців телекомунікаційного сектору, зокрема операторів електронних комунікацій (перевага надається операторам не вищого рівня).

У разі виникнення інших питань просимо звертатися до координатора проєкту з боку Апарату РНБО України Івахненко Євгенії Володимирівни (тел.: 050 272 5039; електронна адреса: event@ncscc.gov.ua).

Додаток: на 1 арк.

З повагою

Заступник Секретаря РНБО України,
заступник керівника НКЦК **Сергій ДЕМЕДЮК**

Додаток

Програма 9-го тренінгу «Управління вразливостями»

Модуль 1. Networking & Monitoring

Опис та порівняння мережевих моделей ISO/OSI та TCP/IP. Механізм інкапсуляції/декапсуляції даних. Мережеві пристрої та їх робота в моделі TCP/IP. Опис, функції та протоколи кожного з рівнів моделі TCP/IP та порівняння із моделлю ISO/OSI. Структура та характеристики основних мережевих протоколів, атак та методів захисту на кожному рівні моделі TCP/IP. WiFi мережі. Інструменти та методи сканування мереж та аналізу мережевого трафіку. Моніторинг інформаційних систем, централізований збір подій, аналіз подій інформаційної безпеки. Інструменти збору та аналізу подій інформаційної безпеки.

Модуль 2. Compliance & Security Testing

Управління інформаційною безпекою. Методології та стандарти побудови СУІБ. Контролі інформаційної безпеки. Методології управління ризиками. Об’єкти критичної інфраструктури. Оцінка інформаційної безпеки. Аудит інформаційної безпеки. Системи та методології ручного та автоматичного аудиту. Тестування інформаційної безпеки. Тестування безпеки додатків. Методології та стандарти тестування на проникнення. Структура кібератак – моделі та фреймворки. Приклади аналізу інформації з відкритих джерел. Приклади активної та пасивної розвідки.

Модуль 3. Web Security

Архітектура web-додатків. Опис, характеристики та структура HTTP протоколу. Забезпечення конфіденційності з’єднання (TLS). Захист web-додатків. Методологія тестування web-додатків на вразливості. Розширені інструменти браузеру. Методи роботи з інструментом Burp Suite. OWASP Top 10. Атаки на автентифікацію. Атаки типу Cross Site Scripting (XSS). Атаки типу Cross Site Request Forgery (CSRF). Атаки типу Injection (OS Command, SQL). Атаки на стороні серверу (SSRF, SSI, LFI, RFI). Ланцюги вразливостей. Приклади та опис основних типів web-атак.

Модуль 4. Infrastructure Security

Зовнішнє тестування інформаційної безпеки інфраструктури. Аналіз інформації з відкритих джерел для дослідження інфраструктури підприємства. Модель The Cyber Kill Chain: розвідка та озброєння (методи та інструменти). Активна розвідка (методи та інструменти). Модель The Cyber Kill Chain: доставка (методи та інструменти). Модель The Cyber Kill Chain: експлуатація (методи та інструменти). Внутрішнє тестування інформаційної безпеки інфраструктури. Методи та інструменти сканування. Тактики, техніки та процедури. Основи LDAP. Модель The Cyber Kill Chain: експлуатація та інсталяція (методи та інструменти). Модель The Cyber Kill Chain: розширення контролю (методи та інструменти). Модель The Cyber Kill Chain: дії з об’єктами. (методи та інструменти).