ЭТИЧНЫЙ ХАКИНГ

Цель программы — сформировать у слушателей профессиональные знания, умения и практические навыки, необходимые для проведения этичного хакинга в целях обеспечения кибербезопасности объектов информационной инфраструктуры, а также развить способность к комплексному анализу киберинцидентов (далее – КИ) и эффективному реагированию на них в рамках национальной системы обеспечения кибербезопасности.

Выпускники курса получают свидетельство о повышении квалификации в области кибербезопасности государственного образца.

Целевая аудитория:

- руководители структурных подразделений и их заместители, специалисты всех наименований и категорий, обеспечивающие кибербезопасность, а также отвечающие за техническую и (или) криптографическую защиту информации, распространение и (или) предоставление которой ограничено.

Требуемая предварительная подготовка слушателей:

- общие представления об информационных системах, правовых, организационных и технических аспектах обеспечения информационной безопасности компьютерных систем;
- базовые знания по IP-сетям, основным протоколам и службам стека TCP/IP;
- навыки работы в ОС Windows или Linux.

Форма обучения – очная (дневная) + очная с использованием информационно-коммуникационных технологий (дистанционно).

Стоимость обучения одного слушателя – 6500 рублей.

Обучение проводится по адресу: г. Минск, ул. К. Цеткин, 24, 11 этаж в соответствии с графиком учебного процесса.

Продолжительность программы – 168 академических часов.

Учебный план курса

№ п/п	Наименования разделов, модулей, тем
	Модуль 1. Основы этичного хакинга и начальные этапы тестирования на проникновение.
I	**Введение в этичный хакинг.**
1.	Обзор программы.
2.	Обзор информационной безопасности.
3.	Угрозы информационной безопасности и векторы атак.
4.	Концепции этичного хакинга. Концепции тестирования на проникновение.
5.	Управление информационной безопасностью.
6.	Стандарты и законы в области информационной безопасности. Система обеспечения кибербезопасности Республики Беларусь.
7.	Знакомство с операционной системой Kali Linux.
8.	Знакомство с операционной системой Parrot Security.
II	**Сбор информации.**
1.	Концепции рекогносцировки. Методология сбора информации.

№ п/п	Наименования разделов, модулей, тем
2.	Инструменты сбора информации.
3.	Работа с метаданными в PDF-файле.
4.	Использование DarkNet для сбора информации.
5.	Меры противодействия сбору информации.
6.	Применение техник по сбору информации.
III	**Сканирование сети.**
1.	Основы компьютерных сетей.
2.	Концепции сканирования сети.
3.	Техники сканирования сети.
4.	Сканирование сети с помощью инструмента Nmap.
5.	Сканирование портов с помощью RustScan и Naabu.
6.	Техники уклонения от систем обнаружения вторжений.
IV	**Анализ уязвимостей.**
1.	Концепции оценки уязвимостей.
2.	Системы оценки уязвимостей.
3.	Инструменты оценки уязвимостей.
4.	Работа в сканере уязвимостей OpenVAS (GVM).
5.	Работа в сканере уязвимостей Nessus.
6.	Работа в сканере уязвимостей OWASP ZAP.
V	**Хакинг системы.**
1.	Архитектура операционной системы.
2.	Слабые точки операционных систем. Методология хакинга системы.
3.	Основы использования Metasploit Framework.
4.	Получение доступа к системе.
5.	Повышение привилегий.
6.	Извлечение паролей пользователей из памяти Windows с помощью Mimikatz.
7.	Применение техник по повышению привилегий в операционных системах.
	Модуль 2. Инструменты и методы атаки: практика выявления и анализа киберугроз.
VI	**Трояны и другое вредоносное программное обеспечение.**
1.	Обзор вредоносного программного обеспечения.
2.	Компьютерные вирусы и черви.
3.	Трояны.
4.	Меры противодействия. Средства защиты от вредоносного программного обеспечения.
VII	**Снифферы.**
1.	Концепции сниффинга.
2.	Техники активного сниффинга.
3.	Инструменты сниффинга.
4.	ARP-spoofing.
5.	DNS-spoofing.
6.	DHCP-spoofing.
7.	Атака истощения DHCP (DHCP Starvation). Rogue DHCP Server.
8.	Использование атаки CAM Table Overflow.
9.	Меры противодействия сниффингу.
10.	Анализ сетевого трафика с помощью Wireshark.
11.	Анализ неизвестного траффика в Wireshark.

№ п/п	Наименования разделов, модулей, тем
12.	Сканирование периметра с помощью утилиты tcpdump.
VIII	**Социальная инженерия.**
1.	Концепции и методы социальной инженерии.
2.	Инсайдерские угрозы.
3.	Имперсонация в социальных сетях. Кража цифровой личности.
4.	Инструменты социальной инженерии.
5.	Использование MSFVenom.
6.	Применение набора средств социальной инженерии SET из состава Kali Linux.
7.	Работа в программе URLCrazy.
IX	**Отказ в обслуживании.**
1.	Концепции DoS/DDoS атак. Техники DoS/DDoS атак.
2.	Ботнет сети. Инструменты проведения DoS и DDoS атак.
3.	Применение техник проведения DoS атаки для вывода из строя сервисов.
X	**Перехват сеанса.**
1.	Концепции перехвата сеанса.
2.	Техники перехвата сеанса. Инструменты для перехвата сеанса.
3.	Атака Man-in-the-Middle.
4.	Применение техник перехвата сеанса для получения доступа к ресурсам серверов.
XI	**Криптография и стеганография.**
1.	Концепции криптографии.
2.	Стеганография.
3.	Алгоритмы шифрования.
4.	Инфраструктура открытых ключей.
5.	Обзор Secure Sockets Layer (SSL). Создание самоподписанных сертификатов SSL для веб-сервера.
6.	Виртуальные частные сети (VPN). Работа с OpenVPN.
7.	Шифрование почты.
8.	Инструменты шифрования диска.
9.	Криптоанализ. Средства криптоанализа. Брутфорс-атаки.
10.	Разработка простых криптографических алгоритмов на основе метода перестановки.
11.	Разработка простых криптографических алгоритмов на основе метода замены.
12.	Разработка простых криптографических алгоритмов.
13.	Работа с программами для стеганографии.
14.	Работа с программами для брутфорса.
15.	Тестирование на проникновение с помощью утилиты THC-Hydra.
16.	Перебор паролей архивов rar и zip с помощью John the Ripper.
17.	Перебор паролей с помощью John the Ripper.
XII	**Обход систем обнаружения вторжений, фаерволлов и систем-ловушек.**
1.	Концепции IDS, фаерволлов, Honeypot и WAF.
2.	Nmap: обход фаервола и IDS.
3.	Инструменты для определения WAF.
	Модуль 3. Этичный хакинг веб-среды и киберучения.
XIII	**Хакинг веб-серверов.**
1.	Концепции веб-серверов.
2.	Типы атак на веб-серверы. Методология атаки на веб-сервер.
3.	Инструменты взлома веб-серверов. Взлом пароля SSH и FTP с помощью Hydra.

№ п/п	Наименования разделов, модулей, тем
4.	Дефейс веб-сервера посредством эксплуатации уязвимости с помощью Metasploit Framework.
XIV	**Хакинг веб-приложений.**
1.	Концепции веб-приложений.
2.	Угрозы веб-приложениям. Меры противодействия взлому веб-приложений. Классификация OWASP Top 10.
3.	Инструменты взлома веб-приложений.
4.	XXE-атака (XML External Entity).
5.	LFI-атака (Local File Inclusion).
6.	RFI-атака (Remote File Inclusion).
7.	Атака Server Side Template Injection (SSTI) (инъекция шаблона на стороне сервера).
8.	Атака Cross-Site Request Forgery (CSRF) (межсайтовая подделка запросов).
9.	Небезопасная прямая ссылка на объект (Insecure Direct Object References, IDOR).
10.	Небезопасное перенаправление (Open Redirect).
11.	Раскрытие информации (Information Exposure).
12.	Удаленное выполнение кода (Remote Code Execution, RCE).
13.	Уязвимость в механизмах аутентификации (Authentication Bypass).
14.	Path Traversal.
15.	Выполнение отраженной и сохраненной XSS атаки.
XV	**SQL инъекции.**
1.	Концепции SQL инъекции. Меры противодействия SQL инъекции.
2.	Примеры применения SQL инъекций.
3.	Автоматизация SQL инъекций.
4.	Server Side Includes (SSI) уязвимость.
5.	Тестирование на проникновение с помощью инструмента SQLMap.
XVI	**Киберучения.**
1.	Киберучения.