Бауманский учебный центр «Специалист»

Программа курса Применение техник этичного хакинга. Лабораторный практикум

Код курса: **ПРАКСЕН**

Тема	Ак. часов
Модуль 1. Подготовка лаборатории и знакомство с окружением • Знакомство с предустановленным программным обеспечением • Знакомство с материалами практикума • Знакомство с основными и дополнительными инструментами • Настройка и запуск виртуальных машин • Знакомство с доменным окружением Active Directory • Знакомство с учебными веб-сайтами в среде IIS, WAMP, Apache Linux • Подготовка лаборатории к выполнению практических заданий	**0.5**
Модуль 2. Сбор информации • Использование **утилит** командной строки Windows для сбора информации • Нахождение поддоменов компании с использованием **Sublist3r** • Сбор личной информации с помощью **онлайн-сервисов** поиска людей • Сбор личной информации с помощью **утилит** и **скриптов** • Сбор информации о целевом сайте с помощью **Firebug** • Извлечение данных компании с использованием **Web Data Extractor** • Зеркалирование сайта с помощью **HTTrack Web Site Copier** • Сбор информации о цели путем отслеживания **электронных писем** • Сбор информации об IP и именах доменов с помощью запросов **Whois** • Расширенная трассировка с использованием **Path Analyzer Pro** • Сбор данных об организации с использованием фреймворка **Maltego** • Выполнение автоматической рекогносцировки сети с использованием **Recon-NG** из состава **Kali Linux** • Использование **Recon-NG** для сбора персональной информации • Сбор информации из социальных сетей, используя Recon-NG **Pushpin** • Автоматизированный сбор сведений об организации с помощью **FOCA** • Интеллектуальный сбор данных с использованием **OSRFramework** • Сбор информации с использованием **Metasploit Framework** • Сбор информации с использованием **theHarvester**	**3**

Модуль 3. Сканирование • Обнаружение хостов с помощью **Colasoft Packet Builder** • Техники создания UDP и TCP пакетов, с использованием **hping3** из состава **Kali Linux** • Обнаружение хостов и сканирование портов с использованием **MegaPing** • Сетевое сканирование с использованием **NMap** • Сканирование сети с помощью **NetScan Tools Pro** • Сканирование с использованием **IP-Tools** • Нахождение компьютеров с использованием **Angry IP Scanner** • Изучение различных методов сетевого сканирования • Выполнение ICMP сканирования с помощью **ping/traceroute** • **Уклонение** от систем обнаружения с помощью использования отвлекающих IP адресов • Организация прокси подключения с помощью **Proxy Workbench** • Анонимный браузинг с использованием **Proxy Switcher** • Анонимный браузинг с использованием **CyberGhost** • Идентификация ОС с использованием **Wireshark** • Построение сетевой диаграммы с использованием **SolarWinds Network Topology Mapper**	**3**
Модуль 4. Перечисление • Перечисление NetBIOS с использованием **Global Network Inventory** • Перечисление сетевых ресурсов с использованием **Advanced IP Scanner** • Выполнение сетевого перечисления с использованием **SuperScan** • Перечисление ресурсов локальной машины с использованием **Hyena** • Выполнение сетевого перечисления используя **NetBIOS Enumerator** • Сетевое перечисление с помощью **SoftPerfect Network Scanner** • Перечисление целевой сети с использованием **NMap** и **Net Use** • Перечисление служб на целевой машине с помощью **NMap** • SNMP перечисление с помощью **snmp_enum** • LDAP перечисление с помощью **ADExplorer** • Сетевое перечисление с помощью различных инструментов **Kali Linux** для выполнения DNS запросов	**1**
Модуль 5. Анализ уязвимостей • Анализ уязвимостей с использованием **Nessus** • Сканирование на наличие уязвимостей в сети с использованием **GFI LANguard** • CGI сканирование с помощью **Nikto**	**1**

Модуль 6. Хакинг системы • Активная онлайн атака с использованием **Responder** • Снятие и взлом хэшей SAM для извлечения паролей с использованием **pwdump7** и **Ophcrack** • Создание и использование радужных таблиц с помощью **Winrtgen** и **RainbowCrack** • Аудит системы паролей с использованием **L0phtCrack** • Эксплуатация уязвимости и создание VNC сессии на Windows 10 с помощью **Metasploit Framework** из состава Kali Linux • Повышение привилегий за счет эксплуатации уязвимости в Windows 10 с помощью **Metasploit Framework** из состава Kali Linux • Взлом Windows Server 2012 с помощью документа MS Office с использованием **TheFatRat** • Получение реверсного Meterpreter шелла и пост-эксплуатация Windows 10 с помощью **Metasploit Framework** из состава Kali Linux • Удаленный мониторинг действий пользователя с использованием **Spytech SpyAgent** • Удаленный мониторинг и запись веб-активности удаленного пользователя с помощью **Power Spy** • Скрытие файлов с помощью NTFS потоков • Скрытие данных с использованием техники стеганографии **White Space** и утилиты snow • Стеганография в изображениях с использованием **OpenStego** • Стеганография в изображениях с использованием **QuickStego** • Построение скрытых каналов с помощью **Covert_TCP** • Просмотр и выключение политик аудита с использованием **auditpol**	**2**
Модуль 7. Трояны и другое вредоносное ПО • Получение контроля над машиной жертвы с помощью **njRAT** • Обфускация трояна с помощью **SwayzCryptor**, чтобы сделать его незаметным для различных антивирусных программ • Создание трояна с помощью **MoSucker** • Создание трояна с помощью **ProRat** • Создание трояна с помощью **Theef** • Создание HTTP трояна и удаленное управление целевой машиной с помощью **HTTP RAT** • Изучение средства создания вирусов **JPS Virus Maker Tool** • Изучение средства создание червя **Internet Worm Maker Thing** • Анализ вируса с помощью **Virus Total** • Анализ вируса с помощью **IDA Pro** • Анализ вируса с использованием **OllyDbg** • Мониторинг TCP/IP соединения с помощью **CurrPorts** • Мониторинг записей реестра с помощью **Regshot** • Мониторинг программ автозагрузки с помощью **WinPatrol** • Мониторинг драйверов устройств с помощью **Driver Booster** • Обнаружение троянов с помощью средств **динамического анализа** • Удаление вредоносного ПО с использованием **ClamWin**	**1**
Модуль 8. Снифферы • Выполнение атаки "Человек посередине" с использованием **Cain & Abel** • Спуфинг **MAC**-адрес с помощью **SMAC** • Сниффинг паролей с использованием **Wireshark** • Анализ использования сети с помощью **Capsa Network Analyzer** • Сниффинг сети с помощью **OmniPeek Network Analyzer** • Обнаружение отравления **ARP** кеша с помощью **Wireshark** • Обнаружение **ARP** атак с помощью **XArp**	**1**

Модуль 9. Социальная инженерия • Обнаружение фишинга с помощью **Netcraft** • Обнаружение фишинга с помощью **PhishTank** • Сниффинг паролей Facebook с использованием **Social Engineering Toolkit** из состава Kali Linux • Сниффинг паролей MS Office 365 с использованием **SpeedPhish Framework в Kali Linux**	**0.5**
Модуль 10. Отказ в обслуживании • SYN флуд целевого хоста с использованием **Metasploit** из **Kali Linux** • SYN флуд целевого хоста с использованием **hping3** • Выполнение распределенной DoS атаки с использованием **HOIC** • Обнаружение и анализ DoS атаки с помощью **KFSensor** и **Wireshark**	**1**
Модуль 11. Перехват сеанса • Перехват сеанса с использованием **Zed Attack Proxy** • Выполнение атаки **sslstrip** и перехват HTTP траффика с помощью **BetterCAP** в **Kali Linux**	**0.5**
Модуль 12. Обход систем обнаружения вторжений, фаерволлов и Honey Pot • Обнаружение вторжений с использованием **Snort** • Обнаружение вредоносного сетевого трафика с помощью **HoneyBot** • Обнаружение хакеров и червей с использованием **KFSensor** • Обход фаерволла Windows с использованием техник уклонения **NMap** • Обход правил фаерволла с использованием **HTTP туннеля** • Обход фаерволла Windows с использованием **Metasploit Framework** из состава **Kali Linux**	**2**
Модуль 13. Хакинг веб-серверов • Выполнение рекогносцировки веб-сервера с использованием инструмента **Skipfish** из состава **Kali Linux** • Сбор сведений о веб-сервере с использованием **httprecon** • Сбор сведений о веб-сервере с использованием **ID Serve** • Сбор сведений о веб-сервере с использованием **Uniscan** из состава **Kali Linux** • Взлом FTP паролей с использованием атаки по словарю с помощью **Hydra**	**1**
Модуль 14. Хакинг веб-приложений • Манипуляция параметрами и эксплуатация **XSS** уязвимости • Выполнение атаки на межсайтовую подделку запросов (**CSRF**) • Перечисление и взлом сайта на WordPress с использованием **WPScan** и **Metasploit** из состава **Kali Linux** • Эксплуатация уязвимости удаленного выполнения команд в **DVWA** для компрометации целевого веб-сервера • Эксплуатация уязвимости загрузки файла в **DVW**A на разных уровнях сложности • Сканирование сайта на наличие уязвимостей с помощью **Acunetix WVS** • Аудит сайта с использование фреймворка **VEGA** из состава **Kali Linux**	**1**
Модуль 15. SQL инъекции • Атаки с помощью SQL инъекций на **MS SQL** • Выполнение атаки с помощью SQL инъекции для извлечения баз данных и открытия шелла с помощью **SQLMAP** • Тестирование на SQL-инъекции с использованием **IBM Security AppScan** • Сканирование веб-приложений с использованием **N-Stalker**	**1**

Модуль 16. Хакинг беспроводных сетей • Сниффинг беспроводной сети с помощью **Wireshark** • Взлом шифрования WEP с помощью **Aircrack-ng** • Взлом шифрования WPA с помощью **Aircrack-ng**	**0.5**
Модуль 17. Хакинг мобильных платформ • Создание реверсного трояна для взлома **Android** с помощью **Kali Linux** • Сбор паролей пользователей мобильных устройств с использованием **Social Engineering Toolkit** • Использование мобильных платформ для проведения **DoS** атаки • Взлом мобильного устройства под управлением Android с использованием **TheFatRat** • **Защита Android** устройств от вредоносных приложений	**1**
Модуль 18. Облачные вычисления • Построение частного облака с использованием **ownCloud** и **WampServer** • Защита частного облака с помощью **ClamAV** • Обход **CalmAV** и взлом хоста для доступа к облачным данным с использованием **Kali Linux** • Выполнение DoS атаки на **Linux Cloud Server** с использованием **Slowloris**	**1**
Модуль 19. Криптография • Расчет хэшей с использованием **HashCalc** • Расчет хэшей и проверка целостности файлов с помощью **MD5 Calculator** • Изучение возможностей шифрования файлов и текста с использованием **CryptoForge** • Шифрование данных с помощью **Advanced Encryption Package** • Шифрование и дешифрование данных с помощью **BCTextEncoder** • Создание и использование самоподписанных **сертификатов** • Шифрование диска с помощью **VeraCrypt** • Шифрование диска с помощью **Rohos Disk Encryption** • Шифрование данных с помощью **CrypTool**	**1**
Модуль 20. Контрольная работа • Выполнение **самостоятельной** практической работы по применению техник этичного хакинга для взлома учебных серверов • Обсуждение **результатов** выполнения контрольной работы • Подведение **итогов** практикума	**1**
Аудиторная нагрузка в классе с преподавателем	**24 ак.ч. + 24 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru