Безопасность информационных систем

IT-специалисты погрузятся в мир ИБ: безопасность сетей, сред виртуализации, браузеров, операционных систем. Курс рассчитан на Junior и Middle разработчиков, администраторов, специалистов по информационной безопасности, DevOps специалистов

Длительность курса: 142 академических часа

1 Основы создания виртуализированных сред для проведения тестирования PoC уязвимостей и исследования программного обеспечения

1	**Введение**	Практика не предусматривается, студенты получают обзорное занятие по курсу вцелом и набор блогов и ресурсов для изучения. Домашние задания 1 Подготовка виртуальных машин для практики 1) Скачивание файлов, которые представляют собой виртуальные машины, для создания окружения для проведения практик. 2) Чтение документации, изучение структуры

сред виртуализации

2 Материалы для изучения

Последовательность изучения материала:
Windows:
1) https://www.amazon.com/Windows-Internals-Part-architecture-management/dp/0735684189
Главы для изучения:
Processes
Threads
Virtual Memory
Kernel mode vs User mode
2) https://docs.microsoft.com/en-us/windows/desktop/memory/about-memory-management

Linux:
1) https://www.amazon.com/UNIX-Linux-System-Administration-Handbook/dp/0134277554
Главы для изучения:
Chapter #4,5
2) https://github.com/proninyaroslav/linux-insides-ru
https://github.com/proninyaroslav/linux-insides-ru/tree/master/MM - или раздел книги Memory Management

Android:
Разделы для изучения:
https://developer.android.com/guide/platform - архитектура и подсистемы
https://developer.android.com/guide/components/processes-and-threads - потоки и процессы

2 **Что такое виртуализация**

Установка необходимого программного обеспечения: VBox, Docker. Знакомство с основными командами для управления системами.

Домашние задания

1 Работа с системой Docker на базе Linux

Домашнее задание направлено на закрепление знаний полученных на занятии.
Список тем для закрепления:
1. Создание Dockerfile сценария для сборки тестового image (в минимально возможном исполнении. image должен содержать утилиты для тестирования сети)
2. Отработка использования команд для управления состоянием контейнера и image. (Набор команд будет продемонстрирован на занятии)
3. Создание тестовой сети внутри Docker

3 **OS Internals**

Структура операционных систем и основные механизмы, которые нужно знать для успешного прохождения курса.

Домашние задания

1 Изучение команд Windbg

Настроить Windbg для отладки в Windows 7 и Windows 10
Для настройки использовать pdf из материалов.

Научиться просматривать память приложения:
1) Просмотреть заголовок исполняемого файла
2) Исследовать список символов для notepad.exe (команда x)
3) Найти имена функций импортов
4) Изучить команды установки точек останова. (breakpoints).
5) Изучить команды для исследования кучи.
6) Изучить написание скриптов для исследования структуры файла.
7) Изучить команду для просмотра стека всех потоков

4 **OS Internals**

Структура операционных систем и основные механизмы, которые нужно знать для успешного прохождения курса.

Домашние задания

1 Отладка в Linux и настройка окружения для Android

a)Проанализировать файлы по ссылкам:
1. https://pwnable.tw/static/chall/start
2. http://pwnable.kr/bin/bof
b) Установить Android Studio
c) Настроить Эмуляторы согласно инструкции в материалах.
d) Описать работу файлов Android из материалов. (Основная идея проверки ключа.)

---

5 **JavaScript Engine Internals**

Особенности работы Движков JavaScript

Домашние задания

1 Изучение структур данных в памяти

1) Исследовать элементарные типы данных SpiderMonkey
a) Целые числа
b) Массив однотипных значений
c) Массив разнотипных значений (строки, целочисленные значения, объекты).
2) Исследовать элементарные типы данных V8
a) Целые числа
b) Массив однотипных значений
c) Массив разнотипных значений (строки, целочисленные значения, объекты).

---

6 **Анализ программного обеспечения с/без исходных кодов.**

Исследование ПО методами: динамическим и статическим.

Домашние задания

1 Поиск адреса массива на куче в движке Spider Monkey

1. Взять черновой скрипт из материалов занятия
2. Скопировать его на тестовую систему Windows 10 x64.
3. Запустить скрипт под отладчиком в release версии js.exe
4. Найти объект в памяти (Полезны будут команды: s, dqs)

7 **Анализ программного обеспечения с/без исходных кодов.**

Исследование ПО методами: динамическим и статическим.

Домашние задания

1 Исследование приложений

Цель: Необходимо исследовать оставшиеся файлы, которые представляют собой задачи CrackME. Это необходимо для того чтобы получить первичное представление как фильтровать стандартные функции и функции написанные автором приложения. Так же необходимо доанализировать скрипт, который писали сегодня на занятии.

1)
a. Скачать и проанализировать приложения с использованием утилит: r2(Cutter), IDA Pro, шестнадцатеричный редактор
b.Предоставить ключи для успешного прохождения задания.
2)
a. Найти базовый адрес js.exe. и показать его на экране средствами JS.
b. Написать скрипт, который заставит js.exe упасть с ошибкой и в регистре rax будет содержаться '0xdeadbeefbaadcode'

8 **Безопасность виртуальных решений на примере Docker и VBox**

Исследование атак, которые связаны с побегом из виртуальной машины, контейнера

Домашние задания

1 Исследование CVE для VBox

Цель: Собрать максимальное количество информации об уязвимостях платформы VBox. Необходимо научиться агрегировать информацию из сети для составления PoC.

Необходимо найти все упоминания следующих уязвимостей:
• CVE-2018-2860
• CVE-2018-2698
• CVE-2018-3055
• CVE-2018-3085

2 Сетевая безопасность

1 Основные сетевые протоколы. Разбор трафика

Разбор основных протоколов на примере записанных трафиков.

Домашние задания

1 Разбор трафика

Цель: Приобретение навыков использования снифера WireShark. Перед студентом стоит задача - определить что утекло в сеть.

ВНИМАНИЕ: НЕ ЗАПУСКАТЬ ФАЙЛЫ ВНЕ ВИРТУАЛЬНОЙ МАШИНЫ!
1. Загрузить графики на виртуальную машину
2. Проанализировать сетевое взаимодействие и определить:
а) Имя скомпрометированной машины
б) Список файлов, который попал в сеть
в) Идентифицировать вредоносные файлы, если они есть.

---

2 Модификация пакетов и работа с их структурой. Основные приемы при исследовании сетевого трафика

Использование Scapy для модификации и создание пакетов заданных протоколов.

Домашние задания

1 Модификация трафика

Цель: Получит навыки модификации и анализа трафика.

1. Проанализировать новые задания по графикам и ответить на списки вопросов.
2. Написать мини-скрипт для отправки данных по протоколам: ICMP, UDP, DNS

3	**Сетевая подсистема Windows**	Разбор функционала подсистемы с использованием обратной разработки Домашние задания 1 Создание пакета SMB Цель: Получение навыков воспроизведения пакетов, которые пересылаются по сети. 1. Создать пакет SMB с помощью scapy и отправить в сеть. 2. Ответить на вопрос: какие команды используются для поиска хостов в протоколе NetBIOS?
4	**Сетевая подсистема Linux**	Разбор функционала подсистемы с использованием обратной разработки.
5	**Сетевая подсистема Android**	Разбор функционала подсистемы с использованием обратной разработки. Домашние задания 1 Работа с сетевыми подсистемами Цель: Настроит и запустит виртуальное устройство. Получит опыт использования отладочного окружения операционной системы Android. 1. Выполнить все операции, описанные в презентации 2. Прислать скрин работающего эмулятора и командной строки.

6	**Основные методы модификации трафика**	Подмена трафика с использованием EttherCap
7	**Атаки на сетевое взаимодействие**	Настройка ПО для сетевых атак и их моделирование. Например DDos, MitM Домашние задания 1 Проведение Атак на сетевые взаимодействия Цель: Студент получит практические навыки проведения атак. Полученные навыки помогут в дальнейшем понимать как действует злоумышленник при попадании в сеть. 1. Провести атаку на хост с помощью BetterCap a. Подменить содержание ресурса на собственные данные - удалить Тег body 2. Настроить контейнеры и провести атаку на хост через DNS
8	**Исследование возможностей стандартных файрволов операционных систем Linux, Windows**	Создание правил блокирования и фильтрации трафика.

3 Безопасность операционных систем

1	**Основные угрозы (Worms, Trojans, Exploits) в контексте операционных систем Windows, Linux**	Исследование вредоносных программ для различных операционных систем.
2	**Особенности атак на операционную систему Windows**	Проведение атак из матрицы Mitre.
3	**Особенности атак на операционную систему Linux**	Проведение атак из матрицы Mitre.
4	**Особенности атак на операционную систему Android**	Проведение атак из матрицы Mitre.
5	**Настройка подсистем защиты для операционной системы Windows**	Настройка подсистемы защиты операционной системы

6	**Обзор подсистем защиты для операционной системы Linux**	Настройка подсистемы защиты операционной системы
7	**Обзор подсистем защиты для операционной системы Android**	Настройка подсистемы защиты операционной системы
8	**Обзор патчей Windows, Linux, Android**	Исследование патчей для операционных систем.

4 Разбор уязвимостей и эксплойтов для операционных систем Windows, Linux, Android, IoT устройств

1	**Основы безопасности браузеров**	Сборка, компиляция отдельных модулей браузера. В частности - модуль интерпретации языка javascript. Отладка и исследование методов эксплуатации
2	**Основы безопасности браузеров Сборка, компиляция**	Сборка, компиляция отдельных модулей браузера. В частности - модуль интерпретации языка javascript. Отладка и исследование методов эксплуатации.
3	**Архитектура браузера Chrome. Анализ безопасности.**	Сборка, компиляция отдельных модулей браузера. В частности - модуль интерпретации языка javascript. Отладка и исследование методов эксплуатации.
4	**Архитектура браузера FireFox. Анализ безопасности.**	Сборка, компиляция отдельных модулей браузера. В частности - модуль интерпретации языка javascript. Отладка и исследование методов эксплуатации.
5	**Архитектура браузера MS Edge. Анализ безопасности.**	Анализ патчей и поиск уязвимых мест приложения.

6 **Архитектура браузера IE. Анализ безопасности.**

Анализ патчей и поиск уязвимых мест приложения.

Домашние задания

1 Исследование уязвимости

Цель: ДЗ направлено на прокачку навыков, которые могут помочь при анализе безопасности ПО. Параллельно с поиском информации по уязвимости студент будет получать дополнительные материалы, которые описывают большое количество подходов к эксплуатации уязвимостей в современном ПО.

1. Найти всю доступную информацию по уязвимости: CVE-2016-7288
2. Убедиться что версия браузера MS Edge действительно уязвима.
3. На основании полученных PoC создать свой, который будет отрабатывать (для уязвимой версии)

---

7 **Анализ и разбор PoC для MS Office**

Разбор уже известных уязвимостей.

---

8 **Анализ и разбор PoC для Adobe Flash**

Разбор уже известных уязвимостей.

5 Проектная работа

1 **Консультации и обсуждения проектной работы**

Домашние задания

1 Проектная работа

Собрать свое окружение для исследования безопасности информационных систем на базе Linux или Windows виртуальной машины. Предоставить описание того как было собрано окружение и для чего будет использоваться его программное обеспечение.

Предоставить проверочные ключи для сдачи каждого из заданий. (Для каждого студента ключи формируется индивидуально)

Каждый ключ сопровождается отчетом о найденной уязвимости и использованном методе эксплуатации в виде отчета.