Реверс-инжиниринг

Курс рассчитан на разработчиков программного обеспечения, системных программистов, системных аналитиков, вирусных аналитиков, специалистов по информационной безопасности, devops-специалистов

Длительность курса: 118 академических часов

1 Низкоуровневое программирование на ассемблер под x8086/x64

1 **Регистры процессора, работа с памятью**

Домашние задания

1 Установка софта

Необходимо установить следующий софт:
Emu 8086
FASM
x64Dbg
Ida Pro 7
Hiew
Far Manager
ConEmu

2 **Представление данных, кода, опкоды команд.**

Домашние задания

1 Одинаковые команды - разные опкоды

Цель: Неодходимо составить список как можно больших команд, которые будут иметь один и тот же смысл, но разные опкоды. Пример:
xor ax, ax | 33 c0
xor ax, ax | 31 c0

---

3 **Арифметические, логические команды. Команды условного/безусловного перехода**

Домашние задания

1 Написать keygen к программам CRACKME.EXE (66f573036f8b99863d75743eff84f15d)

Необходимо дизассемблировать программу и написать генератор валидных пар login:password.

---

4 **Прерывания BIOS**

2 Низкоуровневое программирование на ассемблер под MIPS

1 **Регистры процессора. Работа с памятью**

Домашние задания

1 Калькулятор суммы

Цель: Написать программу, которая:
1) принимает на вход два слагаемых в виде hex цифр,
2) считает сумму и выводит её не экран тоже, в hex виде.

Пример ввода: Slag1 = 12345 Slag2 = 2
Summa: 12347

---

2 **Арифметические, логические команды. Команды условного/безусловного перехода**

---

3 **Опкоды команд**

3 Защищённый режим процессора

1 Сегментная организация памяти

2 Страничная организация памяти

Домашние задания

1 Билдер дескрипторов памяти

Написать программку (лучше на python, но можно и на других ЯП), которая на вход будет принимать: адрес сегмента, лимит сегмента, права (чтение/запись/исполнение) и будет возвращать сформированный дескриптор сегмента

4 Внутреннее устройство Windows

1 Объекты ядра

Домашние задания

1 Стек в PM

1. Написать программку (лучше на python, но можно и на других ЯП), которая на вход будет принимать: адрес сегмента, лимит сегмента, права (чтение/запись/исполнение) и будет возвращать сформированный дескриптор сегмента
2. Добавить дескриптор сегмента, для стека в segmodel.asm

---

2 Менеджер памяти

Домашние задания

1 Crc32

Цель: Переписать программу с MIPS ассемблера на 8086. Захардкодить рандомную строку в 0x100 байт и от неё считать хеш. Функция, выполняющая расчёты должна быть STDCALL

---

3 Диспетчер ввода-вывода

5 Системное программирование

1 **PE формат**

2 **WinApi функции. Перехваты WinApi функций**

Домашние задания

1 Pe Loader

Реализовать простейший Pe Loader, который будет считывать с диска Pe (exe) из памяти и запускать его.
Pe файл брать тот, который выдаёт MessageBox и скомпилирован на FASME.

3 **Программирование Native приложений**

4 **Способы добавления в автозагрузку**

Домашние задания

1 Сборка Native приложения с помощью WDK

Неодходимо собрать приложение dumpMbr.7z, установить его на виртуальную машину и перезагрузить её.

5 **Программирование служб**

Домашние задания

1 Сборка драйвера и службы

Цель: Задание включает две части:
1. Сборка драйвера, исходники которого прикреплены
2. Сборка службы

Драйвер нужно просто сбилдить утилитой build и прислаить скриншот её вывода и сам полученный sys файл
Службу нужно дописать так, чтобы на момент её загрузки она выполнила какие-то действия, к примеру записала в корень диска C файл serv.log с произвольной информацией.
Служба должна запуститься в контексте процесса svchost. Этот процесс нужно будет сдампить и прислать дамп. Помимо этого нужно прислать исходники и билд самой службы.

---

6 **Настройка рабочей среды для отладки драйверов режима ядра**

6 Написание простейших драйверов

1 Написание кастомного MBR

Домашние задания

1 Кастомный MBR

Цель: Написать свой кастомный загрузочный код от MBR, который при выполнеии будет требовать ввести пароль. В случае, если пароль верен, то ПК должен продолжить загрузки ОС так, как буд-то бы ничего и не было.
В противном случае зациклить запрос на введение пароля. Для простоты допускается использовать виртуальную дискету, с которой ПК будет грузиться первоначально. На проверку прислать код и сомпилированную дискету (ну и сам пароль). Пароль нужно хранить в виде CRC32 хеш суммы.

7 Обратная разработка программ

1	**Динамический анализ кода**	WinDbg, Sysinternels Tools, WireShark
2	**Статический анализ кода**	Ida Pro
3	**Разработка shell кодов**	
4	**Metasploit**	
5	**Внедрение реверс шела в некоторые прошивки роутеров**	
6	**Поиск и эксплуатация уязвимостей Buffer Overflow/UAF**	

8 Проектная работа

1	**Вводное занятие по проектной работе**	Домашние задания 1 Проектная работа
2	**Консультации и обсуждения проектной работы**	
3	**Консультации и обсуждения проектной работы**	
4	**Итоговое занятие. Обсуждение проектной работы**	