**Санкт-Петербургский государственный университет**

**Р А Б О Ч А Я П Р О Г Р А М М А**

**УЧЕБНОЙ ДИСЦИПЛИНЫ**

Основы компьютерной безопасности

Fundamentals of Computer Security

**Язык(и) обучения**

русский

Трудоемкость в зачетных единицах: 4

Регистрационный номер рабочей программы: 049260

Санкт-Петербург

2020

**Раздел 1. Характеристики учебных занятий**

**1.1. Цели и задачи учебных занятий**

Цель курса — научить обучающихся понимать основные этапы тестирования безопасности корпоративных компьютерных сетей, знание основных типов уязвимостей в программном обеспечении и способов защиты от них.

**1.2. Требования подготовленности обучающегося к освоению содержания учебных занятий (пререквизиты)**

Знание основ информатики, программирования и математики в пределах бакалаврской подготовки.

**1.3. Перечень результатов обучения (learning outcomes)**

В процессе изучения дисциплины «Основы компьютерной безопасности» обучаемые приобретают следующие

***знания:***

* понятия компьютерной безопасности – доступность, целостность, конфиденциальность;
* историю и современные тенденции построения безопасных систем;
* подходы и методы поиска уязвимостей и способы их устранения;
* организация безопасности на уровне операционных систем и сетевых сервисов;

***умения:***

* работать с компьютером как средством управления информацией, в том числе в глобальных компьютерных сетях;
* соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны;
* реализовывать решения, направленные на защиту сетевых сервисов и обнаружения вероятной атаки;
* использовать готовые утилиты для проведения аудита безопасности компьютерных систем.
* использовать в научной и познавательной деятельности,  
  а также в социальной сфере профессиональные навыки работы с информационными и компьютерными технологиями;
* использовать нормативные правовые документы в своей деятельности, действовать в условиях гражданского общества;
* критически переосмысливать свой опыт, адаптироваться к различным ситуациям, проявлять творческий подход, инициативу и настойчивость в достижении целей профессиональной деятельности;
* производить анализ и грамотную оценку эффективности разрабатываемых методов защиты.

***навыки:***

* работы с информацией из различных источников, включая сетевые ресурсы сети Интернет, для решения профессиональных задач;
* осуществления целенаправленного поиска информации о технологических достижениях в сети Интернет и из других источников;
* применения в профессиональной деятельности современных средств защиты компьютерных систем.

Знать содержание дисциплины «Основы компьютерной безопасности», в частности, иметь базовые представления о системах безопасности, методах взлома, вероятных векторов атак, организация сложной многоуровневой защиты.

Уметь формализовывать поставленные задачи и реализовывать сложные программные комплексы защиты с точки зрения грамотной профессиональной разработки различного рода проектов.

Дисциплина развивает следующие компетенции:

* ОПК-1 – способен находить, формулировать и решать актуальные проблемы фундаментальной и прикладной информатики и информационных технологий;
* ПКА-1 – способен находить, формулировать и решать актуальные проблемы фундаментальной и прикладной информатики и информационных технологий;
* ПКП-1 – способен демонстрировать фундаментальные знания математических и естественных наук, программирования и информационных технологий;
* ПКП-7 – способен использовать знания направлений развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств: операционных систем, операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности;
* ПКП-8 – способен использовать основные концептуальные положения функционального, логического, объектно-ориентированного и визуального направлений программирования, методы, способы и средства разработки программ в рамках этих направлений.

**1.4. Перечень и объём активных и интерактивных форм учебных занятий**

В качестве основных интерактивных форм (общее количество 10 часов) предполагаются практические занятия для обеспечения получения умений и навыков защиты, поиска уязвимостей, настройки продуктов для обеспечения безопасности.

**Раздел 2. Организация, структура и содержание учебных занятий**

**2.1. Организация учебных занятий**

**2.1.1 Основной курс**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Трудоёмкость, объёмы учебной работы и наполняемость групп обучающихся | | | | | | | | | | | | | | | | | | |
| Код модуля в составе дисциплины,  практики и т.п. | Контактная работа обучающихся с преподавателем | | | | | | | | | | | | Самостоятельная работа | | | | Объём активных и интерактивных  форм учебных занятий | Трудоёмкость |
| лекции | семинары | консультации | практические  занятия | лабораторные работы | контрольные работы | коллоквиумы | текущий контроль | промежуточная  аттестация | итоговая аттестация | под руководством преподавателя | в присутствии  преподавателя | сам. раб. с использованием  методических материалов | текущий контроль (сам.раб.) | промежуточная аттестация (сам.раб.) | итоговая аттестация  (сам.раб.) |
| ОСНОВНАЯ ТРАЕКТОРИЯ | | | | | | | | | | | | | | | | | | |
| Форма обучения: очная | | | | | | | | | | | | | | | | | | |
| Семестр 1 | 30 |  | 2 | 15 |  |  |  |  | 2 |  |  |  | 58 |  | 37 |  | 10 | 4 |
|  | 2-30 |  | 2-30 | 2-30 |  |  |  |  | 1-30 |  |  |  | 1-1 |  | 1-1 |  |  |  |
| ИТОГО | 30 |  | 2 | 15 |  |  |  |  | 2 |  |  |  | 58 |  | 37 |  |  | 4 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Виды, формы и сроки текущего контроля успеваемости и промежуточной аттестации | | | | | | |
| Код модуля в составе дисциплины, практики и т.п. | Формы текущего контроля успеваемости | | Виды промежуточной аттестации | | Виды итоговой аттестации  (только для программ итоговой аттестации и дополнительных образовательных программ) | |
| Формы | Сроки | Виды | Сроки | Виды | Сроки |
| ОСНОВНАЯ ТРАЕКТОРИЯ | | | | | | |
| Форма обучения: очная | | | | | | |
| Семестр 1 |  |  | экзамен, устно, традиционная форма | по графику промежуточной аттестации |  |  |

**2.2. Структура и содержание учебных занятий**

Период обучения: **Семестр 1**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п.п.** | **Наименование темы (раздела, части)** | **Вид учебных занятий** | **Кол-во часов** |
| 1 | Раздел 1. Основные понятия в области тестирования на проникновение  Тема 1.1. Стандарт по тестированию на проникновение OSSTMM  Тема 1.2 .Калькулятор опасности уязвимостей CVSS  Тема 1.3. Базы данных уязвимостей (CVE, MS)  Тема 1.4. Основные средства защиты корпоративных сетей и сетевых устройств | лекции | 15 |
| практические занятия | 7 |
| по методическим материалам | 29 |
| 2 | Раздел 2. Вредоносные программы  Тема 2.1 История развития вредоносных программ  Тема 2.2 Основные алгоритмы заражения  Тема 2.3 Устройство ботнетов  Тема 2.4 Анализ работы ботнета на примере Zeus | лекции | 15 |
| практические занятия | 8 |
| по методическим материалам | 29 |
| 3 | Промежуточная аттестация | самостоятельная работа | 37 |
| консультации | 2 |
| экзамен | 2 |
| **Итого** | | | **144** |

**Раздел 1. Основные понятия в области тестирования на проникновение**

Тема 1.1. Стандарт по тестированию на проникновение OSSTMM

* Стандарт OSSTMM, понятие вектора атаки, плоскости атаки. типы тестирования на проникновение: тандем, красная команда, тестирование «белого ящика», тестирование «черного ящика», тестирование «серого ящика».

Тема 1.2. Калькулятор опасности уязвимостей CVSS.

* Базовые метрики уязвимостей. Временные метрики уязвимостей. Разбор нескольких уязвимостей по метрике CVSS. Понятия целевого и уязвимого компонента.

Тема 1.3. Базы данных уязвимостей (CVE, MS)

* Порядок регистрации CVE, иерархия CNA, база данных типов уязвимостей CWE

Тема 1.4. Основные средства защиты корпоративных сетей и сетевых устройств.

* Антивирусное ПО, сетевые средства защиты, понятие сигнатурного и аномального обнаружения. ПО для расследования инцидентов.

**Раздел 2. Вредоносные программы**

Тема 2.1. История развития вредоносных программ

* Основные предпосылки возникновения вредоносных программ. Появление компьютерных вирусов в 80-е годы. Развитие вредоносного ПО до 2008 года. Malware2.0, становление индустрии. Понятие 0/1-day уязвимостей. Основные APT-угрозы.

Тема 2.2. Основные алгоритмы заражения

* Классификация вредоносного ПО. Отличие червя от вируса. Алгоритмы заражения исполняемых файлов. Сокрытие сигнатур через упаковку. Инжектирование в процессы, основные способы записи вируса в автозапуск. «Полезная нагрузка» вируса и ее устройство.

Тема 2.3. Устройство ботнетов

* Централизованные и децентрализованные ботнеты. Этапы заражения ботом. Противодействие ботнету. Понятие DGA. Алгоритмы анализа траффика для поиска ботнета.

Тема 2.4. Анализ работы ботнета на примере Zeus.

* Три уровня протокола Zeus. Алгоритмы поддержания связи. Распространение команд по ботнету. Обфускация траффика. Виды «полезных нагрузок». Противостояние ботнету.

**Раздел 3. Обеспечение учебных занятий**

**3.1. Методическое обеспечение**

**3.1.1 Методические указания по освоению дисциплины**

Успешное освоение дисциплины возможно благодаря посещению лекций, участию в обсуждении вопросов, подготовленных к занятию, самостоятельной работе, включающей в себя чтение специальной литературы по разделам темы, подготовка презентаций по тематике курса.

**3.1.2 Методическое обеспечение самостоятельной работы**

Самостоятельная работа обучающихся в рамках данной дисциплины является важным компонентом обучения, предусмотренным компетентностно-ориентированным учебным планом и рабочей программой учебной дисциплины.   
Настоящей программой предусмотрены формы самостоятельной работы с использованием методических материалов.

**3.1.3 Методика проведения текущего контроля успеваемости и промежуточной аттестации и критерии оценивания**

Промежуточная аттестация состоит из устного экзамена и сдачи лабораторных работ, выдающихся в течение семестра.

Экзамен проводится в устной форме. Билет содержит два вопроса, на подготовку к ответу в аудитории отводится не менее одного академического часа.

После ответа на вопросы билета, преподаватель вправе задать дополнительные вопросы по любой теме из списка вопросов, вынесенных на экзамен. В качестве дополнительных используются вопросы, не требующие длительного вывода и трудоемких вычислений, в том числе основные определения, примеры и логические связи, содержащиеся в курсе.

По совокупности ответов экзаменуемого выставляются оценки по следующим критериям:

* **А** («отлично») — сдано пять лабораторных, либо сдано три из пяти лабораторных и отвечено на два вопроса по теории на А;
* **B** («хорошо») — сдано четыре лабораторных, либо сдано три лабораторных и отвечено на два вопроса по теории как минимум на B;
* **C** («хорошо») — сдано три лабораторных и отвечено на два вопроса по теории как минимум на C;
* **D** («удовлетворительно») — сдана одна лабораторная и отвечено на два вопроса по теории как минимум на D;
* **E** («удовлетворительно») — отвечено на 2 вопроса по теории как минимум на E;
* **F** («неудовлетворительно») — во всех остальных случаях.

**3.1.4 Методические материалы для проведения текущего контроля успеваемости и промежуточной аттестации (контрольно-измерительные материалы, оценочные средства)**

***Примерный краткий перечень вопросов к зачету.***

*По первому разделу:*

1. Понятие вектора атаки, плоскости атаки. типы тестирования на проникновение. Примеры
2. Основные этапы тестирования на проникновение. Утилиты для проведения анализа безопасности.
3. Калькулятор опасности уязвимостей CVSS. Понятия целевого и уязвимого компонента. Примеры
4. Базы данных уязвимостей (CVE, MS). Порядок регистрации CVE, иерархия CNA, база данных типов уязвимостей CWE. Примеры уязвимостей в бинарных программах
5. Базы данных уязвимостей (CVE, MS). Порядок регистрации CVE, иерархия CNA, база данных типов уязвимостей CWE. Примеры WEB-уязвимостей
6. Основные средства защиты корпоративных сетей и сетевых устройств. Принципы работы, примеры продуктов.

*По второму разделу:*

1. Основные предпосылки возникновения вредоносных программ. Появление компьютерных вирусов в 80-е годы. Развитие вредоносного ПО до 2008 года
2. Malware2.0, становление индустрии. Понятие 0/1-day уязвимостей. Основные APT-угрозы.
3. Основные алгоритмы заражения исполняемых файлов. Троян-дроппер, троян-инжектор. Восстановление импортов. Технологии антиэмуляции
4. Классификация вредоносного ПО. Отличие червя от вируса. Сокрытие сигнатур через упаковку. Основные способы записи вируса в автозапуск. «Полезная нагрузка» вируса и ее устройство.
5. Централизованные и децентрализованные ботнеты. Этапы заражения ботом. Противодействие ботнету. Понятие DGA. Алгоритмы анализа траффика для поиска ботнета.
6. Анализ работы ботнета на примере Zeus.Три уровня протокола Zeus. Алгоритмы поддержания связи. Распространение команд по ботнету. Обфускация траффика. Виды «полезных нагрузок». Противостояние ботнету.

***Задания лабораторных работ:***

1. Взлом сайта
   1. Перебрать пароль с помощью утилиты patator с предзапросом CSRF-токена
   2. Найти на сайте уязвимость RCE
   3. Запустить непрерывный tcp-шелл на php
   4. Запустить эксплойт типа LPE под названием dirty-cow-vdso
2. MITM-атака
   1. Провести отравление arp-кеша утилитой arpspoof
   2. Запустить утилиту mitmproxy и заставить ее работать с arpspoof, перехватить траффик бота ходящего на instagram и показать расшифрованный пакет ssl с паролем
   3. Провести xss-атаку на страницу instagramm
   4. Выключить цели интернет
3. Туннелирование
   1. Запустить SSH-туннель типа NfR или NfL, через него зайти в веб-страницу, поднятую командой python -mSimpleHTTPServer
   2. Запустить socks5-прокси в 2 экземплярах с помощью команды NfD и прописать их в proxychains, запустить через него программу curl и убедиться, что соединение прошло через два промежуточных хоста
   3. Запустить dnscat2-туннель и в нем запустить обычный шелл
4. На выбор
   1. AFL-фазер
      1. Запустить AFL-фазер и найти уязвимость типа переполнение буфера или UAF в написанном коде на си
      2. Запустить AFL и найти уже существующую уязвимость в одной из библиотек (например, в libcurl)
   2. SMB-Relay
      1. Запустить утилиту Responder — активный снифер и с его помощью провести атаку SMB-Relay, перехватить NTLM2 хеш пароля и расшифровать его утилитой hashcat или johntheripper
5. Взлом сайта 2
   1. Найти дефолтный пароль от движка
   2. Поиск sql-инъекции на сайте
   3. Открытие reverse-shell
   4. Поиск уязвимости типа LPE через уязвимый бинарный файл с правами suid
   5. Запуск утилиты удаленного управления puppy

**3.1.5 Методические материалы для оценки обучающимися содержания и качества учебного процесса**

Для оценки обучающимися содержания и качества учебного процесса применяется анкетирование в соответствии с методикой и графиком, утвержденными в установленном порядке.

**3.2. Кадровое обеспечение**

**3.2.1 Образование и (или) квалификация штатных преподавателей и иных лиц, допущенных к проведению учебных занятий**

К чтению лекций привлекаются преподаватели, имеющие базовое образование и/или ученую степень, соответствующую профилю преподаваемой дисциплины.

**3.2.2 Обеспечение учебно-вспомогательным и (или) иным персоналом**

Не требуется.

**3.3. Материально-техническое обеспечение**

**3.3.1 Характеристики аудиторий (помещений, мест) для проведения занятий**

Стандартно оборудованные лекционные аудитории для проведения интерактивных лекций: видеопроектор, экран.

**3.3.2 Характеристики аудиторного оборудования, в том числе неспециализированного компьютерного оборудования и программного обеспечения общего пользования**

Не требуется.

**3.3.3 Характеристики специализированного оборудования**

Не предусмотрено.

**3.3.4 Характеристики специализированного программного обеспечения**

Не предусмотрено.

**3.3.5 Перечень и объёмы требуемых расходных материалов**

Фломастеры цветные, губки, канцелярские товары в объеме, необходимом для организации и проведения занятий по заявкам преподавателей, подаваемым в установленные сроки, доступ преподавателя и обучающихся к в компьютерные классы.

**3.4. Информационное обеспечение**

**3.4.1 Список обязательной литературы**

1. Информационная безопасность и защита информации [Текст] : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А Клейменов. - 5-е изд., стер. - М. : Академия, 2011. - 331 с.
2. Крук, Е. А., Линский Е.М. Криптография с открытым ключом. Кодовые системы: Учебное пособие. СПб.: РИО ГУАП, 2004. - 52 с..
3. Шнайер, Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. - 815 с.
4. Чмора, А. Л. Современная прикладная криптография. М.: Гелиос АРВ, 2002. 244 с.
5. Виноградов И.М. Основы теории чисел. Лань, 2009. <http://e.lanbook.com/view/book/46/>
6. Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии. Лань, 2011. <http://e.lanbook.com/view/book/1540/>

**3.4.2 Список дополнительной литературы**

Не требуется.

**3.4.3 Перечень иных информационных источников**

1. Стандарт OSSTMM3 (<https://www.isecom.org/OSSTMM.3.pdf,2020> г.)
2. Стандарт OWASP Web security testing guide (<https://github.com/OWASP/wstg/tree/master/document>)
3. Linux Hardening in Hostile Networks. Server Security from TLS to Tor, Kyle Rankin, 2017, ISBN-10: 0-13-417326-0, ISBN-13: 978-0-13-417326-9
4. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, By Michael Sikorski, Andrew Honig, Year 2012, Publisher No Starch Press,ISBN978-1593272906
5. Art of Computer Virus Research and Defense, Peter Szor, 2005, ISBN-13: 978-0321304544, ISBN-10: 9780321304544

**Раздел 4. Разработчики программы**

Ханов Артур Рафаэльевич, старший преподаватель кафедры системного программирования СПбГУ, [st036451@student.spbu.ru](mailto:st036451@student.spbu.ru).