ИНСТИТУТ ЛАЗЕРНЫХ И ПЛАЗМЕННЫХ ТЕХНОЛОГИЙ

КАФЕДРА ПРИКЛАДНОЙ МАТЕМАТИКИ

**ФОНД**

**ОЦЕНОЧНЫХ СРЕДСТВ**

текущего, рубежного и промежуточного контроля успеваемости

**ПО УЧЕБНОЙ ДИСЦИПЛИНЕ**

**СЕТЕВЫЕ ТЕХНОЛОГИИ: ВЕБ-ПУБЛИКАЦИИ, УСТРОЙСТВО И БЕЗОПАСНОСТЬ СЕТЕЙ И КЛАСТЕРОВ**

**1.** **ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ**

**1.1. Область применения**

Фонд оценочных средств (ФОС) *–* является неотъемлемой частью учебно-методического комплекса учебной дисциплины «Сетевые технологии: веб-публикации, устройство и безопасность сетей и кластеров» и предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу данной дисциплины.

**1.2. Цели и задачи фонда оценочных средств**

Целью Фонда оценочных средств является установление соответствия уровня подготовки обучающихся требованиям ОС НИЯУ МИФИ.

Для достижения поставленной цели Фондом оценочных средств по дисциплине «Сетевые технологии: веб-публикации, устройство и безопасность сетей и кластеров» решаются следующие задачи:

– контроль и управление процессом приобретения обучающимися знаний, умений и навыков предусмотренных в рамках данного курса;

– контроль и оценка степени освоения общекультурных, общепрофессиональных и профессиональных компетенций предусмотренных в рамках данного курса;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс в рамках данного курса.

**1.3. Контролируемые компетенции**

ОС НИЯУ МИФИ по направлению подготовки 01.04.02 «Прикладная математика и информатика» и рабочая программа дисциплины «Сетевые технологии: веб-публикации, устройство и безопасность сетей и кластеров» магистерской программы «Математическая физика, математическое моделирование, анализ и обработка данных» в рамках профиля «Математическое моделирование физических процессов» предусмотрено формирование следующих общекультурных, общепрофессиональных и профессиональных компетенций:

|  |  |
| --- | --- |
| **Код компетенций** | **Компетенция** |
| ОПК-4 | способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности |
| ПК-1 | способен проводить научные исследования и получать новые научные и прикладные результаты самостоятельно и в составе научного коллектива |
| ПК-2 | способен к разработке и внедрению наукоемкого программного обеспечения, способствующего решению передовых задач науки и техники на основе современных математических методов и алгоритмов |
| ПК-6 | способен к проектированию и разработке наукоемкого программного обеспечения на основе технического задания |
| ПК-8 | способен разрабатывать корпоративные стандарты и профили функциональной стандартизации приложений, систем, информационной инфраструктуры |

**1.4 Планируемые результаты обучения**

Поскольку перечисленные компетенции носят интегральный характер, для разработки оценочных средств целесообразно выделить планируемые результаты обучения – знания, умения и навыки, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения образовательной программы. Таким образом, в результате освоения дисциплины «Сетевые технологии: веб-публикации, устройство и безопасность сетей и кластеров» студенты должны:

*Знать:*

|  |  |  |
| --- | --- | --- |
| **Код** | **Результаты обучения** | **Показатели оценки результатов** |
| З1 | основы построения и функционирования сетей передачи данных, системы управления сети передачи данных | * протокол сетевого уровня: IP * протоколы транспортного уровня: TCP, UDP * протокол канального уровня: Ethernet |
| З2 | систему управления безопасностью сети | * ARP-spoofing и защита от него * DHCP-spoofing и защита от него |
| З3 | аппаратурный состав коммуникационного оборудования сети | * отличия и особенности работы свитча, хаба и коммутатора * принцип работы маршрутизатора |

*Уметь:*

|  |  |  |
| --- | --- | --- |
| **Код** | **Результаты обучения** | **Показатели оценки результатов** |
| У1 | системно мыслить, диагностировать и структурировать проблемы организации процессов обработки данных | * распределять нагрузку между маршрутизаторами * находить и устранять неисправности сетевого оборудования * корректно настраивать роутинг |
| У2 | анализировать процессы обработки данных, интерпретировать получаемые результаты с целью выработки предложений по совершенствованию технологии функционирования сетей | * находить и устранять уязвимости в настройках сетевого оборудования * настраивать NAT, PAT и прокси-сервера * настраивать беспроводную сеть |

*Владеть:*

|  |  |  |
| --- | --- | --- |
| **Код** | **Результаты обучения** | **Показатели оценки результатов** |
| В1 | навыками постановки и решения производственных проблем с позиций системного подхода | * пользоваться доступными способами поиска информационных источников с использование современных Интернет технологий * критически мыслить, оценивать и анализировать преимущества и недостатки существующих программных и аппаратных средств |
| В2 | навыками построения и использования компьютерных сетей различного масштаба | * использовать современные пакеты прикладного программного обеспечения для решения задач, в частности для администрирования и поиска уязвимостей сетевого оборудования |
| В3 | способами оценки возможностей реализации компьютерных сетей на основе базовых технологий и стандартов | * демонстрация навыков быстрого развертывания проводных и беспроводных сетей |

**1.5 Промежуточная аттестация по дисциплине**

Формой промежуточной аттестации по дисциплине «Сетевые технологии: веб-публикации, устройство и безопасность сетей и кластеров» является:

1 семестр – зачет

**1.6 Перечень оценочных средств используемых для текущей аттестации**

|  |  |  |  |
| --- | --- | --- | --- |
| **Код**  **задания** | **Наименование оценочного средства** | **Краткая характеристика оценочного средства** | **Представление оценочного средства в фонде** |
| ЛР1 | Лабораторная работа №1 | Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу | Комплект контрольных заданий по вариантам |
| ЛР2 | Лабораторная работа №2 |
| ЛР3 | Лабораторная работа №3 |
| ЛР4 | Лабораторная работа №4 |
| ЛР5 | Лабораторная работа №5 |
| ЛР6 | Лабораторная работа №6 |
| ЛР7 | Лабораторная работа №7 |
| ЛР8 | Лабораторная работа №8 |
| ЛР9 | Лабораторная работа №9 |

**1.7 Расшифровка компетенций через планируемые результаты обучения**

Связь между формируемыми компетенциями и планируемыми результатами обучения представлена в следующей таблице:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Код** | **Проектируемые результаты освоения дисциплины**  **и индикаторы формирования компетенций** | | | **Средства и технологии оценки** |
| **Знать (З)** | **Уметь (У)** | **Владеть (В)** |
| ОПК-4 | З1, З2, З3 | У1, У2 | В1, В2, В3 | ЛР1, ЛР2, ЛР3, ЛР4, ЛР5, ЛР6, ЛР7, ЛР8, ЛР9, З |
| ПК-1 | З1, З2, З3 | У1, У2 | В1, В3 | ЛР1, ЛР2, ЛР3, ЛР4, ЛР5, ЛР6, ЛР7, ЛР8, ЛР9, З |
| ПК-2 | З1, З2, З3 | У1, У2 | В1, В2, В3 | ЛР3, ЛР4, ЛР5, ЛР6, ЛР7, ЛР8, ЛР9, З |
| ПК-6 | З1, З2, З3 | У1, У2 | В1, В2, В3 | ЛР3, ЛР4, ЛР5, ЛР6, ЛР7, ЛР8, ЛР9, З |
| ПК-8 | З1, З2, З3 | У1, У2 | В1, В2, В3 | ЛР3, ЛР4, ЛР5, ЛР6, ЛР7, ЛР8, ЛР9, З |

**1.8 Этапы формирования компетенций**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Раздел** | **Темы занятий** | **Коды**  **компетенций** | **Знания, умения и навыки** | **Виды аттестации** | | |
| **Текущий контроль –**  **неделя** | **Рубежный контроль – неделя** | **Промежуточная**  **аттестация** |
| Раздел 1 | Тема 1.  Основы сетей передачи данных | ОПК-4 | З1,З3,  У1,У2,  В1,В3 | ЛР1 | КИ-8 | зачет |
| Тема 2.  Протокол транспортного уровня UDP | ОПК-4,  ПК-1,  ПК-2,  ПК-6,  ПК-8 | З1,У1,  У2,В1,  В3 | ЛР2 |
| Тема 3.  Протокол транспортного уровня TCP | З1,У1,  У2,В1,  В2,В3 | ЛР3 |
| Тема 4.  Протоколы прикладного уровня: FTP, SMTP, POP3 и IMAP | З1,З2,  З3,У1,  У2,В1,  В2,В3 | ЛР4 |
| Тема 5. Протокол HTTP. Прокси-сервера | З1,З2,  З3,У1,  У2,В1,  В2,В3 | ЛР5 |
| Раздел 2 | Тема 6.  Разработка клиент-серверных приложений | ОПК-4,  ПК-1,  ПК-2,  ПК-6,  ПК-8 | З1,З2,  У1,У2,  В1,В3 | ЛР6 | КИ-16 |
| Тема 7.  Wi-Fi сети. Открытые сети и сети с WEP-шифрованием | З1,З2,  У1,У2,  В1,В3 | ЛР7 |
| Тема 8.  Wi-Fi сети. Сети с WPA и WPA2-шифрованием | З1,З2,  У1,У2,  В1,В3 | ЛР8 |
| Тема 9.  Атаки и защита беспроводного оборудования | З1,З2,  З3,У1,У2,У3,  В1,В2,  В3 | ЛР9 |

**1.9 Шкала оценки образовательных достижений**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Код** | **Вид оценочного**  **средства** | **Критерии** | **Балл** | **Макс. балл– мин. балл** |
| ЛР1 | Лабораторная работа №1 | выставляется студенту при условии выполнения всех заданий лабораторной работы | 5 | **3 – 5** |
| выставляется в случае, если студент смог защитить компьютер от атак типа ARP-spoofing, но не смог сам провести указанную атаку. | 3 |
| при невыполнении заданий лабораторная работа не зачитывается и у студента образуется долг, который должен быть закрыт в течении семестра или на зачетной неделе | н/з |
| ЛР2 | Лабораторная работа №2 | выставляется студенту при условии выполнения всех заданий лабораторной работы | 5 | **3 – 5** |
| выставляется в случае, если студент смог защитить компьютер от атак типа DHCP-spoofing, но не смог сам провести указанную атаку. | 3 |
| при невыполнении заданий лабораторная работа не зачитывается и у студента образуется долг, который должен быть закрыт в течении семестра или на зачетной неделе | н/з |
| ЛР3 | Лабораторная работа №3 | выставляется студенту при условии выполнения всех заданий лабораторной работы | 5 | **3 – 5** |
| выставляется в случае, если студент смог скачать файл с telnet-сервера, но не смог на него загрузить свой файл. | 3 |
| при невыполнении заданий лабораторная работа не зачитывается и у студента образуется долг, который должен быть закрыт в течении семестра или на зачетной неделе | н/з |
| ЛР4 | Лабораторная работа №4 | выставляется студенту при условии выполнения всех заданий лабораторной работы | 5 | **3 – 5** |
| выставляется в случае, если студент смог скачать и загрузить файл на FTP-сервер, но не смог провести атаку на активный или пассивный режим работы FTP-сервера. | 3 |
| при невыполнении заданий лабораторная работа не зачитывается и у студента образуется долг, который должен быть закрыт в течении семестра или на зачетной неделе | н/з |
| ЛР5 | Лабораторная работа №5 | выставляется студенту при условии выполнения всех заданий лабораторной работы | 5 | **3 – 5** |
| выставляется в случае, если студент смог отправить требуемый запрос на web-сайт, но не смог самостоятельно найти подходящий прокси-сервер или данные для входа на сайт. | 3 |
| при невыполнении заданий лабораторная работа не зачитывается и у студента образуется долг, который должен быть закрыт в течении семестра или на зачетной неделе | н/з |
| ЛР6 | Лабораторная работа №6 | выставляется студенту при условии выполнения всех заданий лабораторной работы | 6 | **3 – 6** |
| выставляется в случае, если студень смог разработать серверную часть приложения, но в качестве клиентской части использовался веб-браузер или утилиты telnet (netcat) | 3 |
| при невыполнении заданий лабораторная работа не зачитывается и у студента образуется долг, который должен быть закрыт в течении семестра или на зачетной неделе | н/з |
| ЛР7 | Лабораторная работа №7 | выставляется студенту при условии выполнения всех заданий лабораторной работы | 6 | **4 – 6** |
| выставляется в случае, если студент смог подобрать пароль к WiFi-сети и записать интернет-трафик других пользователей, но не смог расшифровать перехваченные данные или найти в них пароль. | 4 |
| при невыполнении заданий лабораторная работа не зачитывается и у студента образуется долг, который должен быть закрыт в течении семестра или на зачетной неделе | н/з |
| ЛР8 | Лабораторная работа №8 | выставляется студенту при условии выполнения всех заданий лабораторной работы | 6 | **4 – 6** |
| выставляется в случае, если студент смог подобрать пароль к WiFi-сети и записать интернет-трафик других пользователей, но не смог расшифровать перехваченные данные или найти в них пароль. | 4 |
| при невыполнении заданий лабораторная работа не зачитывается и у студента образуется долг, который должен быть закрыт в течении семестра или на зачетной неделе | н/з |
| ЛР9 | Лабораторная работа №9 | выставляется студенту при условии выполнения всех заданий лабораторной работы | 7 | **4 – 7** |
| выставляется в случае, если студент смог найти в прошивке роутера исполняемый файл, отвечающий за генерацию стандартного пароля, но не смог восстановить алгоритм генерации | 4 |
| при невыполнении заданий лабораторная работа не зачитывается и у студента образуется долг, который должен быть закрыт в течении семестра или на зачетной неделе | н/з |
| З | Зачет | при полностью правильно написанных вопросах и при ответе на все дополнительные вопросы по курсу с незначительными неточностями, которые студент должен устранить в процессе беседы с преподавателем, в рамках которой он демонстрирует углубленное понимание предмета и владение ключевыми знаниями, умениями и навыками, предусмотренными данной дисциплиной | 40-50 | **30 – 50** |
| при полностью правильно написанных вопросах и при ответе на часть дополнительных вопросов по курсу с демонстраций базовых знаний, умений и навыков, предусмотренных данной дисциплиной | 35-39 |
| при написанных ответах на вопросы (допускается содержание некоторых неточностей) и демонстрации базовых знаний, умений и навыков по данной дисциплине | 30-34 |
| если студент не написал ответ хотя бы на один из вопросов и не может ответить на дополнительные компетентностно–ориентированные вопросы | н/з |

Итоговая оценка представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля, и выставляется в соответствии с Положением о кредитно-модульной системе в соответствии со следующей шкалой:

|  |  |  |
| --- | --- | --- |
| Оценка по 5-балльной шкале | Сумма баллов за разделы | Оценка ECTS |
| 5 – *«отлично»* | 90-100 | А |
| 4 – «*хорошо*» | 85-89 | В |
| 75-84 | С |
| 70-74 | D |
| 3 – «*удовлетворительно*» | 65-69 |
| 60-64 | Е |
| 2 – «*неудовлетворительно*» | Ниже 60 | F |

Расшифровка уровня знаний, соответствующего полученным баллам, дается в таблице указанной ниже

|  |  |  |
| --- | --- | --- |
| **Оценка по 5-балльной шкале – оценка по ECTS** | **Сумма баллов за разделы** | **Требования к знаниям на устном зачёте** |
| *«отлично»*  *–*  *А* | 90 ÷ 100 | Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы. |
| *«хорошо»*  *–*  *D, C, B* | 70 ÷ 89 | Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос. |
| *«удовлетворительно»*  *–*  *E, D* | 60 ÷ 69 | Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала. |
| *«неудовлетворительно»*  *–*  *F* | менее 60 | Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине. |

**2.** **ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ**

**для оценки знаний (3), умений (У) и навыков (В)**

**2.1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ**

Ниже приведен перечень оценочных средств используемых при проведении текущего контроля успеваемости студентов.

**2.1.1 ЛАБОРАТОРНАЯ РАБОТА №1 (ЛР1)**

Провести атаку ARP-spoofing на лабораторный компьютер и перехватить пароль. Защитить лабораторный компьютер от атак ARP-spoofing.

**Вариант 1**

Перехватить HTTP-трафик с помощью Kali Linux.

**Вариант 2**

Перехватить HTTP-трафик с помощью Сканер-ВС.

**Вариант 3**

Перехватить FTP-трафик с помощью Kali Linux.

**Вариант 4**

Перехватить FTP-трафик с помощью Сканер-ВС.

**Вариант 5**

Перехватить SMB-трафик с помощью Kali Linux.

**Вариант 6**

Перехватить SMB-трафик с помощью Сканер-ВС.

**2.1.2 ЛАБОРАТОРНАЯ РАБОТА №2 (ЛР2)**

Провести атаку DHCP-spoofing на лабораторный компьютер и перехватить пароль. Защитить лабораторный компьютер от атак DHCP-spoofing.

**Вариант 1**

Перехватить HTTP-трафик с помощью Kali Linux.

**Вариант 2**

Перехватить HTTP-трафик с помощью Сканер-ВС.

**Вариант 3**

Перехватить FTP-трафик с помощью Kali Linux.

**Вариант 4**

Перехватить FTP-трафик с помощью Сканер-ВС.

**Вариант 5**

Перехватить SMB-трафик с помощью Kali Linux.

**Вариант 6**

Перехватить SMB-трафик с помощью Сканер-ВС.

**2.1.3 ЛАБОРАТОРНАЯ РАБОТА №3 (ЛР3)**

Подключиться к telnet-серверу с помощью утилиты telnet или netcat, создать на удаленном сервере текстовый файл, содержащий ФИО студента, а также найти и скачать с удаленного сервера файл с паролем.

**Вариант 1**

Telnet-сервер работает под управлением ОС Windows и не требует авторизации.

**Вариант 2**

Telnet -сервер работает под управлением ОС Linix и не требует авторизации.

**Вариант 3**

Telnet -сервер работает под управлением ОС Windows, студенту заранее известны данные для авторизации на сервере.

**Вариант 4**

Telnet -сервер работает под управлением ОС Linux, студенту заранее известны данные для авторизации на сервере.

**Вариант 5**

Telnet -сервер работает под управлением ОС Windows, студенту требуется подобрать логин и пароль от сервера по словарю.

**Вариант 6**

Telnet -сервер работает под управлением ОС, студенту требуется подобрать логин и пароль от сервера по словарю.

**2.1.4 ЛАБОРАТОРНАЯ РАБОТА №4 (ЛР4)**

Требуется закачать на FTP-сервер текстовый файл, содержащий ФИО студента, найти и скачать с FTP-сервера файл с паролем, а также провести на FTP-сервер указанную атаку. Защитить сервер от наиболее распространенных типов атак.

**Вариант 1**

Провести атаку на FTP-сервер в активном режиме, заставив его отправить запрос на указанный сайт с использованием утилиты telnet или netcat.

**Вариант 2**

Провести атаку на FTP-сервер в активном режиме, заставив его отправить запрос на указанный сайт с использованием утилиты ftp.

**Вариант 3**

Провести атаку на FTP-сервера в активном режиме, заставив его отправить запрос на указанный сайт с использованием любого GUI-клиента.

**Вариант 4**

Провести атаку на FTP-сервер в пассивном режиме, украв файл другого пользователя с использованием утилиты telnet или netcat.

**Вариант 5**

Провести атаку на FTP-сервер в пассивном режиме, украв файл другого пользователя с использованием утилиты ftp.

**Вариант 6**

Провести атаку на FTP-сервер в пассивном режиме, украв файл другого пользователя с использованием любого GUI-клиента.

**2.1.5 ЛАБОРАТОРНАЯ РАБОТА №5 (ЛР5)**

Требуется отправить запрос на web-сайт c авторизацией с помощью указанных утилит.

**Вариант 1**

Использовать HTTP Basic-авторизацию и утилиту telnet или netcat.

**Вариант 2**

Использовать HTTP Basic-авторизацию и интернет-браузер.

**Вариант 3**

Использовать HTTP Digest-авторизацию и утилиту telnet или netcat.

**Вариант 4**

Использовать HTTP Digest -авторизацию и интернет-браузер.

**Вариант 5**

Использовать HTTP и SOCKS прокси-сервер и утилиту telnet или netcat.

**Вариант 6**

Использовать HTTP и SOCKS прокси-сервер и интернет-браузер.

**2.1.6 ЛАБОРАТОРНАЯ РАБОТА №6 (ЛР6)**

Требуется разработать программный комплекс, состоящий из серверной части с веб-интерфейсом и клиентской части. Если в качестве клиентской части будет использован веб-браузер или утилиты netcat или telnet, то оценка будет понижена.

**Вариант 1**

Сервервая часть должна быть написана на языке PHP, клиентская должна работать под ОС Windows.

**Вариант 2**

Сервервая часть должна быть написана на языке С/С++ (cgi-приложение), клиентская должна работать под ОС Windows.

**Вариант 3**

Сервервая часть должна быть написана на языке PHP, клиентская должна работать под ОС Linux / MacOS.

**Вариант 4**

Сервервая часть должна быть написана на языке С/С++ (cgi-приложение), клиентская должна работать под ОС Linux / MacOS.

**Вариант 5**

Сервервая часть должна быть написана на языке PHP, клиентская должна работать под ОС Android / iOS.

**Вариант 6**

Сервервая часть должна быть написана на языке С/С++ (cgi-приложение), клиентская должна работать под ОС Android / iOS.

**2.1.7 ЛАБОРАТОРНАЯ РАБОТА №7 (ЛР7)**

Требуется вычислить пароль от WiFi-сети с указанным типом шифрования (при необходимости), перехватить интернет-трафик других пользователей, расшифровать его (при необходимости), найти в расшифрованном трафике пароль,, а также отключить других пользователей от WiFi-сети.

**Вариант 1**

WiFi-сеть без шифрования, использовать дистрибутив Kali Linux.

**Вариант 2**

WiFi-сеть без шифрования, использовать дистрибутив Сканер-ВС.

**Вариант 3**

WiFi-сеть с WEP-шифрованием, вычислить пароль с помощью утилиты aircrack-ng, использовать дистрибутив Kali Linux.

**Вариант 4**

WiFi-сеть с WEP-шифрованием, вычислить пароль с помощью утилиты aircrack-ng, использовать дистрибутив Сканер-ВС.

**Вариант 5**

WiFi-сеть с WEP-шифрованием, вычислить пароль с помощью утилиты fern-wifi-cracker, использовать дистрибутив Kali Linux.

**Вариант 6**

WiFi-сеть с WEP-шифрованием, вычислить пароль с помощью утилиты fern-wifi-cracker, использовать дистрибутив Сканер-ВС.

**2.1.8 ЛАБОРАТОРНАЯ РАБОТА №8 (ЛР8)**

Требуется вычислить пароль от WiFi-сети с указанным типом шифрования (при необходимости), перехватить интернет-трафик других пользователей, расшифровать его (при необходимости), найти в расшифрованном трафике пароль,, а также отключить других пользователей от WiFi-сети.

**Вариант 1**

WiFi-сеть с WPA/WPA2-шифрованием, узнать пароль через WPS, использовать дистрибутив Kali Linux и утилиту reaver.

**Вариант 2**

WiFi-сеть с WPA/WPA2-шифрованием, узнать пароль через WPS, использовать дистрибутив Сканер-ВС и утилиту reaver.

**Вариант 3**

WiFi-сеть с WPA/WPA2-шифрованием, подобрать пароль по словарю, использовать дистрибутив Kali Linux и утилиту fern-wifi-cracker.

**Вариант 4**

WiFi-сеть с WPA/WPA2-шифрованием, подобрать пароль по словарю, использовать дистрибутив Сканер-ВС и утилиту fern-wifi-cracker.

**Вариант 5**

WiFi-сеть с WPA/WPA2-шифрованием, подобрать пароль по словарю, использовать дистрибутив Kali Linux и утилиту aircrack-ng.

**Вариант 6**

WiFi-сеть с WPA/WPA2-шифрованием, подобрать пароль по словарю, использовать дистрибутив Сканер-ВС и утилиту aircrack-ng.

**2.1.9 ЛАБОРАТОРНАЯ РАБОТА №9 (ЛР9)**

Требуется найти в прошивке роутера исполняемый файл, отвечающий за генерацию стандартного пароля WiFi и восстановить логику работы алгоритма генерации.

**Вариант 1**

Роутер TP-Link.

**Вариант 2**

Роутер D-Link.

**Вариант 3**

Роутер ZyXEL.

**Вариант 4**

Роутер ZTE.

**Вариант 5**

Роутер Huawei.

**Вариант 6**

Роутер Linksys.

**2.2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ РУБЕЖНОГО КОНТРОЛЯ**

В рамках дисциплины «Современные компьютерные технологии (сетевые технологии)» предусмотрено проведение рубежного контроля успеваемости студентов на 8 и 16 неделе.

В качестве оценочного средства при проведении рубежного контроля на 8 неделе используется, так называемый, Контроль по итогам (КИ), минимальная положительная оценка за который подразумевает усвоение студентом необходимого минимума материала, относящегося к Разделу 1 дисциплины. Баллы, за проводящийся на 8 неделе контроль по итогам, выставляются в соответствии со следующей таблицей

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Код оценочного средства – неделя | Вид контроля | Неделя контроля | Минимальный балл | Максимальный бал |
| ЛР1 | Лабораторная работа №1 | 1 | 2 | 5 |
| ЛР2 | Лабораторная работа №2 | 2 | 3 | 5 |
| ЛР3 | Лабораторная работа №3 | 3 | 2 | 5 |
| ЛР4 | Лабораторная работа №4 | 4 | 3 | 5 |
| ЛР5 | Лабораторная работа №5 | 6 | 2 | 5 |
| **КИ** | **Контроль по Итогам** | **8** | **12** | **25** |

Рубежный контроль на 16 неделе проводится аналогично рубежному контролю на 8 неделе и оценивает уровень знаний, полученных студентом в Разделе 2 дисциплинам, выставляется в соответствии с таблицей

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Код оценочного средства – неделя | Вид контроля | Неделя контроля | Минимальный балл | Максимальный бал |
| ЛР6 | Лабораторная работа №6 | 9 | 3 | 6 |
| ЛР7 | Лабораторная работа №7 | 10 | 3 | 6 |
| ЛР8 | Лабораторная работа №8 | 12 | 3 | 6 |
| ЛР9 | Лабораторная работа №9 | 15 | 4 | 7 |
| **КИ** | **Контроль по Итогам** | **16** | **13** | **25** |

**2.3 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

**2.3.1. ВОПРОСЫ К ЗАЧЕТУ**

1. 7 уровней модели OSI.
2. Протокол канального уровня Ethernet. MAC-адрес.
3. Протокол сетевого уровня IP.
4. ARP и RARP запросы и ответы.
5. ARP-spoofing и способы защиты от него.
6. Сетевой мост, свитч и хаб.
7. Протокол сообщений об ошибках ICMP. Ping-запросы и отклики.
8. Протокол UDP.
9. Протоколы BOOTP и DHCP.
10. DHCP-spoofing и способы защиты от него.
11. Протокол передачи данных TFTP.
12. Протокол TCP. Установка и разрыв соединения.
13. Протокол TCP. Интерактивный и неинтерактивный поток данных.
14. Протокол TCP. Алгоритм Нагла.
15. Утилиты telnet, netcat и rlogin.
16. Таблица маршрутизации.
17. Технологии NAT и PAT.
18. Утилиты для управления таблицами маршрутизации.
19. Безопасность маршрутизации.
20. Протокол передачи данных FTP: команды и отклики сервера.
21. Протокол передачи данных FTP: Пассивный и активный режим передачи данных.
22. Атаки на протокол FTP и способы защиты от них.
23. Кодировка данных Base64.
24. Протокол электронной почты SMTP: аутентификация и отправка писем.
25. Протокол электронной почты POP3: аутентификация и получение писем.
26. Протокол электронной почты IMAP: аутентификация, отпрвка и получение писем.
27. Протокол HTTP. GET, POST и другие виды запросов.
28. Протокол HTTP. Заголовки запроса клиента и ответа сервера.
29. Протокол HTTP. Basic и Digest аутентификация.
30. Технология прокси: HTTP, HTTPS, SOCKS4 и SOCKS5 прокси-сервера.
31. Анонимность прокси-серверов.
32. WiFi-Сети. Типы шифрования и аутентификация. Атаки на беспроводные сети и способы защиты от них.
33. WiFi-Сеть без шифрования. Подключение и обмен данными.
34. WiFi-Сеть с WEP-шифрованием. Подключение и обмен данными.
35. WiFi-Сеть с WPA/WPA2-шифрованием. Подключение и обмен данными.
36. Настройка веб-северов Apache, nginx, lighthttpd, Microsoft IIS
37. Настройка php и cgi-приложение на веб-сервере
38. Создание клиентских приложений под ОС Windows, работа с сетью.
39. Создание клиентских приложений под ОС Linux / MacOS, работа с сетью.
40. Создание клиентских приложений под ОС Android / iOS, работа с сетью.