

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Дагестанский государственный университет»  
Факультет информатики и информационных технологий

## **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

### **Безопасность вычислительных сетей**

Кафедра информационных технологий и безопасности компьютерных систем

**Образовательная программа бакалавриата**  
10.03.01 Информационная безопасность

**Направленность (профиль) программы:**  
Безопасность компьютерных систем

**Форма обучения**  
Очная

**Статус дисциплины:**  
обязательная часть ОПОП

Махачкала, 2022

Рабочая программа дисциплины «Безопасность вычислительных сетей» составлена в 2022 году в соответствии с требованиями ФГОС ВО- бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность» от «17» ноября 2020 г. №1427.

Разработчик(и): ИТиБКС, Фейламазова С.А.

Рабочая программа дисциплины одобрена:  
на заседании кафедры ИТиБКС от «16» марта 2022г., протокол № 8

Зав. кафедрой  Ахмедова З.Х

на заседании Методической комиссии факультета ИиИТ от «17» марта 2022г.,  
протокол №7.

Председатель  Бакмаев А.Ш.

Рабочая программа дисциплины согласована с учебно-методическим управлением  
«31» марта 2022 г.

Начальник УМУ  Гасангаджиева А.Г.

## Аннотация рабочей программы дисциплины

Дисциплина «Безопасность вычислительных сетей» входит в обязательную часть образовательной программы бакалавриата по направлению 10.03.01 Информационная безопасность.

Дисциплина реализуется на факультете информатики и информационных технологий кафедрой информационных технологий и безопасности компьютерных систем.

Содержание дисциплины охватывает круг вопросов, связанных с изучением основ построения сетей и систем передачи информации, характеристик основных телекоммуникационных систем сигналов и протоколов, применяемых для передачи различных видов сообщений.

Дисциплина нацелена на формирование следующих компетенций выпускника: профессиональных – ПК-4, ПК-7. Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, лабораторные занятия, самостоятельная работа.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме – *устный и письменный опрос*, промежуточный контроль в форме *экзамена*.

Объем дисциплины 4 зачетных единиц, в том числе в академических часах по видам учебных занятий.

Объем дисциплины в очной форме

Семестр	Учебные занятия						СРС, в том числе экза мен	Форма промежуточной аттестации(зачет, дифференцирован- ный зачет, экзамен)
	в том числе							
	Контактная работа обучающихся с преподавателем							
	из них							
Всего	Лекции	Лаборатор- ные занятия	Практи- ческие занятия	КСР	Консуль- тации			
8	144	32	32				80	зачет

### 1. Цели освоения дисциплины.

**Целью освоения дисциплины** «Безопасность вычислительных сетей» является изучение теоретических основ и принципов обеспечения безопасности сетей, сетевых угроз и методов борьбы с ними.

#### Задачи дисциплины:

- дать студентам прочные знания и практические навыки в области, определяемой целями курса;
- изучение основных угроз в сетях ЭВМ и методов противодействия им;
- овладения механизмами построения систем безопасности сетей ЭВМ;
- изучение мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- изучить защищенные протоколы и межсетевые экраны.

### 2. Место дисциплины в структуре ОПОП бакалавриата.

Учебная дисциплина «Безопасность вычислительных сетей» входит в обязательную часть.

Программа базируется на дисциплинах: «Физика», «Информатика», «Сети и системы передачи информации».

Входными знаниями для освоения данной дисциплины являются знания основы сетей передачи данных, полученные при освоении дисциплины «Информатика».

### 3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Код и наименование компетенции из ОПОП	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения	Процедура освоения
ПК 4 Способен проектировать и администрировать телекоммуникационные системы и сети, конфигурировать телекоммуникационное оборудование	ПК 4.1. Знать стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей	Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей	устный и письменный опросы
	ПК 4.2. Уметь проектировать и администрировать локальные и глобальные телекоммуникационные сети	Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей	устный и письменный опросы
	ПК 4.3. Владеть навыками и способами конфигурирования сетей, повышения их надежности и отказоустойчивости	Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей	устный и письменный опросы
ПК-7 Обеспечение функционирования средств связи сетей связи специального назначения	ПК 7.1. Номенклатура, функциональное назначение и основные характеристики средств связи сетей связи специального назначения, включая СКЗИ; ПК 7.2. Проводить проверку комплектности средств связи сетей связи специального назначения, включая СКЗИ; ПК 7.3. Настройкой средств связи сетей связи специального назначения, включая СКЗИ;	Знать: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Уметь: Выполнять настройку и проверку функционирования средств связи сетей связи специального назначения, включая СКЗИ Владеть: Проверкой функционирования средств связи сетей связи специального назначения, включая СКЗИ	устный и письменный опросы

### 4. Объем, структура и содержание дисциплины.

**4.1.** Объем дисциплины составляет 5 зачетных единиц, 180 академических часов

**4.2.** Структура дисциплины.

#### 4.2.1. Объем дисциплины в очной форме.

№ п/п	Названия разделов	Семестр	Неделя	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации
				Лекции	Практические занятия	Лабораторные занятия	Контроль самост. работы		
<b>Модуль I. Основные безопасности сетей</b>									
1	<b>Введение в сетевую безопасность</b>	8		2				6	Устный опрос
2	<b>Протоколы сетевой аутентификации. Модели разграничения доступа. Вредоносное программное обеспечение.</b>	8		2		2		6	Устный опрос
3	<b>Системы обнаружения и предотвращения вторжений (ISD/IPS)</b>	8		2		4		6	Устный опрос
4	<b>Угрозы безопасности на канальном уровне 2</b>	8		4		4		4	
	<b>Итого за модуль:</b>			<b>10</b>		<b>10</b>		<b>22</b>	
<b>Модуль II. Анализ уязвимостей</b>									
5	<b>Уязвимости по приложениям</b>	6		4		4		8	Устный опрос
6	<b>Анализ защищённости веб-приложений</b>	6		4		4		8	Устный опрос
7	<b>Способы обхода авторизации</b>	6		2		2		6	Устный опрос
	<b>Итого за модуль:</b>			<b>10</b>		<b>10</b>		<b>22</b>	
<b>Модуль III. Сетевая операционная система</b>									
8	<b>Методы сканирования и уклонения в Kali Linux</b>	6		2		2		6	Устный опрос
9	<b>Инструменты Kali Linux.</b>	6		2		2		6	

10	<b>Python для тестирования на проникновение</b> 1. Понимание сокетов и создание TCP-сервера 2. Создание TCP-клиента. 3. Разработка сканера Nmap.	6		2		2		6	Устный опрос
11	<b>Исследование сетей с Python</b>			2		2		4	
<b>Итого за модуль:</b>				<b>8</b>		<b>8</b>		<b>22</b>	
<b>Модуль IV. Безопасность беспроводных сетей</b>									
12	<b>Безопасность беспроводных сетей.</b> 1. WEP-атаки на конфиденциальность проводных сетей 2. Протоколы WPA и AES 3. Беспроводные атаки и защита от них 4. Проектирование безопасной сети с помощью беспроводной связи. Создание ширококонтинентального трафика базе ESP8266 для подавления активности беспроводной сети.			<b>4</b>		<b>4</b>		<b>14</b>	
<b>Итого за модуль</b>				<b>4</b>		<b>4</b>		<b>14</b>	
<b>Всего часов</b>				<b>32</b>		<b>32</b>		<b>80</b>	

#### 4.3 Содержание дисциплины, структурированное по темам (разделам).

##### 4.3.1. Содержание лекционных занятий по дисциплине

№ п/п	Наименование темы	Трудоемкость		Формируемые компетенции	Результаты освоения (знает, умеет, владеет)	Технологии обучения
<b>Модуль 1</b>						
1	<b>Введение в сетевую безопасность</b>	2	<p>1. Основные понятия и определения.</p> <p>1. Нейтрализация угроз. Области сетевой безопасности.</p> <p>2. Общие рекомендации по сетевой безопасности.</p> <p>3. Типы атак.</p>	ПК-4	<p>Знает: стек протоколов TCP/IP и модель OSI.</p> <p>Принципы построения локальных и глобальных компьютерных сетей.</p> <p>Знает: стек протоколов TCP/IP и модель OSI.</p> <p>Принципы построения локальных и глобальных</p>	Устный опрос

					компьютерных сетей. Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей	
2	<b>Протоколы сетевой аутентификации. Модели разграничения доступа. Вредоносное программное обеспечение.</b>	2	1. Локальная аутентификация Windows. Протоколы сетевой аутентификации.	ПК-4	Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей. Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей. Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей. Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей.	Устный опрос
3	<b>Системы обнаружения и предотвращения вторжений (ISD/IPS)</b>	2	1. Что такое системы обнаружения вторжений (IDS). 2. Сетевые ISD (NIDS) 3. Проблемы NIDS Системы предотвращения вторжений (IPS).	ПК-4	Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей. Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей. Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей. Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей.	Устный опрос
4	<b>Угрозы безопасности на канальном уровне 2</b>		1. Атака на таблицу MAC. 2. Атаки на сети VLAN.	ПК-4	Знает: стек протоколов TCP/IP и модель OSI. Принципы построения	

			3. Атаки, связанные с DHCP. 4. ARP атаки. Атаки с подменой адреса.		локальных и глобальных компьютерных сетей. Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей. Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей	
--	--	--	--	--	---	--

### Модуль 2

5	Уязвимости по приложения	2	1. SSTI. 2. XXE-атака. 3. XSS-атаки. Снижение риска атак межсайтового скриптинга (XSS) с помощью helmet .xssFilter. 4. Атака на сервер компьютерной сети: SSRF атака.	ПК-4	Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей. Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей. Знает: стек протоколов TCP/IP и модель OSI. Принципы построения локальных и глобальных компьютерных сетей	Устный опрос
6	<b>Анализ защищённости веб-приложений</b>	2	1. Методология тестирования на проникновение: Метод черного ящика (black box), Метод белого ящика (white box), Метод серого ящика (gray box) 2. Анализ защищённости веб-	ПК-7	Знать: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Уметь: Выполнять настройку и проверку функционирования средств связи сетей связи специального назначения, включая СКЗИ Владеть:	Устный опрос



			<p>приложений путём внешних проверок (автоматизированных и ручных).</p> <p>3. Этапы теста на проникновение:</p> <p>4. Тестирование на проникновение с помощью Burp</p> <p>5. Nikto – сканер веб-серверов NSLOOKUP – утилита для поиска DNS-серверов</p>		<p>Проверкой функционирования средств связи сетей связи специального назначения, включая СКЗИ</p>	
7	<b>Способы обхода авторизации</b>	2	<p>1. BruteForce.</p> <p>2. SQL инъекции. Cookie.</p>	ПК-7	<p>Знать: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Уметь: Выполнять настройку и проверку функционирования средств связи сетей связи специального назначения, включая СКЗИ Владеть: Проверкой функционирования средств связи сетей связи специального назначения, включая СКЗИ</p>	Устный опрос
8	<b>Методы сканирования и уклонения в Kali Linux</b>	2	<p>1. Описание метода обнаружения цели.</p> <p>2. Как с помощью инструментов Kali Linux распознать целевую машину.</p> <p>3. Шаги, которые необходимо выполнить для поиска операционных систем целевых машин (получение отпечатков</p>	ПК-7	<p>Знать: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Уметь: Выполнять настройку и проверку функционирования средств связи сетей связи специального назначения, включая СКЗИ Владеть:</p>	Устный опрос

			<p>операционной системы).</p> <p>4. Автоматическое сканирование с помощью Striker.</p> <p>5. Соккрытие с помощью Nipe.</p> <p>6. Сканирование nmap.</p> <p>7. Sql map NetCat</p>		<p>Проверкой функционирования средств связи сетей связи специального назначения, включая СКЗИ</p>	
9	<b>Инструменты Kali Linux.</b>	2	<p>1. Разведка сайтов.</p> <p>Поиск каталогов и файлов. Dirb, Dirhunt, DirBuster</p>	ПК-7	<p>Знать: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Уметь: Выполнять настройку и проверку функционирования средств связи сетей связи специального назначения, включая СКЗИ Владеть: Проверкой функционирования средств связи сетей связи специального назначения, включая СКЗИ</p>	Устный опрос
10	<b>Python для тестирования на проникновение</b>	2	<p>1. Понимание сокетов и создание TCP-сервера</p> <p>2. Создание TCP-клиента.</p> <p>Разработка сканера Nmap.</p>	ПК-7	<p>Знать: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Уметь: Выполнять настройку и проверку функционирования средств связи сетей связи специального назначения, включая СКЗИ Владеть: Проверкой функционирования средств связи сетей связи специального назначения, включая СКЗИ</p>	Устный опрос

11	<b>Исследование сетей с Python</b>		<ol style="list-style-type: none"> <li>1. Сканер сети библиотеки scapy</li> <li>2. Использование веб-библиотек. Взаимодействие с веб-сервисами - библиотека urllib2.</li> <li>3. Форензика с Python</li> <li>4. Библиотека requests</li> <li>5. Пакеты lxml и BeautifulSoup.</li> </ol>	ПК-7	<p>Знать: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации</p> <p>Уметь: Выполнять настройку и проверку функционирования средств связи сетей связи специального назначения, включая СКЗИ</p> <p>Владеть: Проверкой функционирования средств связи сетей связи специального назначения, включая СКЗИ</p>	Устный опрос
12	<b>Безопасность беспроводных сетей.</b>	2	<ol style="list-style-type: none"> <li>1. WEP-атаки на конфиденциальность проводных сетей</li> <li>2. Протоколы WPA и AES</li> <li>3. Беспроводные атаки и защита от них</li> <li>4. Проектирование безопасной сети с помощью беспроводной связи.</li> </ol> <p>Создание широкополосной базы трафика для ESP8266 для подавления активности беспроводной сети.</p>	ПК-7	<p>Знать: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации</p> <p>Уметь: Выполнять настройку и проверку функционирования средств связи сетей связи специального назначения, включая СКЗИ</p> <p>Владеть: Проверкой функционирования средств связи сетей связи специального назначения, включая СКЗИ</p>	Устный опрос

#### 4.3.2. Содержание лабораторных занятий по дисциплине

№ п/п	Наименование темы	Трудоемкость	Содержание	Формируемые компетенции	Результаты освоения	Технологии обучения
1	Аудит информационной	2	Инструментальный анализ	ПК-4	Знает современные инструментальные	Устный опрос

	безопасности.		защищенности. Основные этапы работ при проведении аудита.		средства программного обеспечения. Умеет анализировать и выбирать инструментальные средства программного обеспечения. Владеет навыками использования методов и инструментальных средств исследования программного обеспечения.	
2	Локальная аутентификация Windows.	2	Локальные учетные записи. Создание, удаление.	ПК-4	Знает современные инструментальные средства программного обеспечения. Умеет анализировать и выбирать инструментальные средства программного обеспечения. Владеет навыками использования методов и инструментальных средств исследования программного обеспечения.	Устный опрос
3	DLP-системы. DMZ –системы. DPI- системы. WAF-системы	2	системы защиты	ПК-4	Знает современные инструментальные средства программного обеспечения. Умеет анализировать и выбирать инструментальные средства программного обеспечения. Владеет навыками использования методов и инструментальных средств исследования программного обеспечения.	Устный опрос
4	Mitm атака	2	Разбор атаки «человек по середине»	ПК-4	Знает современные инструментальные средства программного обеспечения. Умеет анализировать и выбирать инструментальные средства программного обеспечения. Владеет навыками использования методов и	Устный опрос

					инструментальных средств исследования программного обеспечения.	
5	Настройка параметров безопасности коммутатора cisco.	2	Пароли. Зашифрованные пароли. Режимы работы.	ПК-4	Знает современные инструментальные средства программного обеспечения. Умеет анализировать и выбирать инструментальные средства программного обеспечения. Владеет навыками использования методов и инструментальных средств исследования программного обеспечения.	Устный опрос
6	Определение пароля WI-FI	2	принципы определения пароля беспроводных сетей.	ПК-5	Знает современные технологии разработки ПО (структурное, объектно-ориентированное) Умеет использовать современные технологии разработки ПО. Имеет навыки использования современных технологий разработки ПО	Устный опрос
7	Межсетевые экраны.	2	настройка межсетевых экранов	ПК-5	Знает современные технологии разработки ПО (структурное, объектно-ориентированное) Умеет использовать современные технологии разработки ПО. Имеет навыки использования современных технологий разработки ПО	Устный опрос
8	Анализатор протоколов Wireshark	4	Анализ сетевого трафика	ПК-7	Знать: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Уметь: Выполнять настройку и проверку	Устный опрос

					функционирования средств связи сетей связи специального назначения, включая СКЗИ Владеть: Проверкой функционирования средств связи сетей связи специального назначения, включая СКЗИ	
9	Утилиты командной строки.	2	работа с утилитами командной строки	ПК-7	Знать: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Уметь: Выполнять настройку и проверку функционирования средств связи сетей связи специального назначения, включая СКЗИ Владеть: Проверкой функционирования средств связи сетей связи специального назначения, включая СКЗИ	Устный опрос
10	Инструменты Kali Linux	12	Burp Suite. WireShark. OWASP Zed. Maltego Metasploit Nmap.	ПК-7	Знать: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Уметь: Выполнять настройку и проверку функционирования средств связи сетей связи специального назначения, включая СКЗИ Владеть: Проверкой функционирования средств связи сетей связи специального назначения, включая СКЗИ	Устный опрос

### Лабораторная работа №1. Man-in-the-middle атака

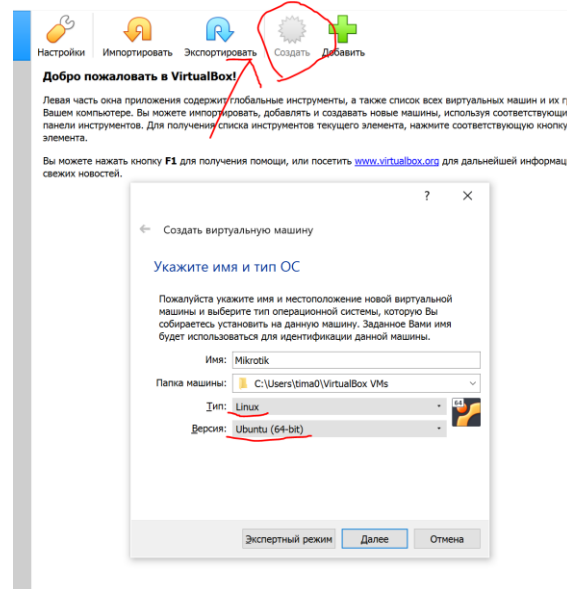
Необходимые файлы

Для проведения атаки нам потребуется:

1. Виртуальная среда VirtualBox
2. Образ маршрутизатора Mikrotik и Winbox
3. Образ Windows 10
4. Образ Kali Linux

## Установка и настройка маршрутизатора Mikro Tik

Открываем VirtualBox и создаем новую виртуальную машину

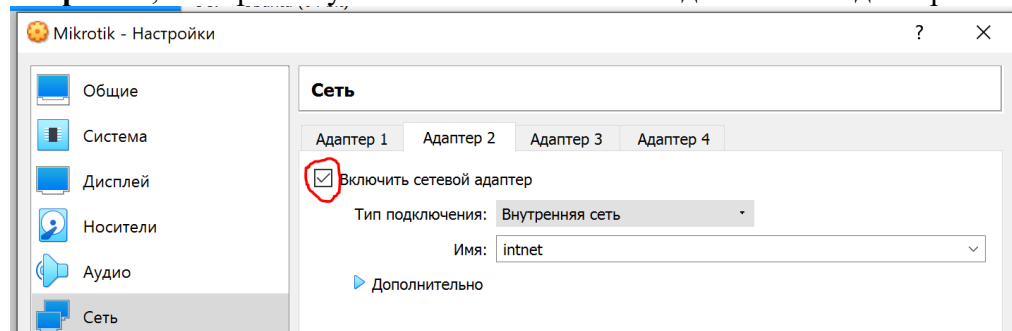


Указываем тип **Linux** и версию **Ubuntu 64**

Файл типа vdi, поэтому **используем существующий виртуальный жесткий диск** и выберем его из файловой системы. Создадим машину.

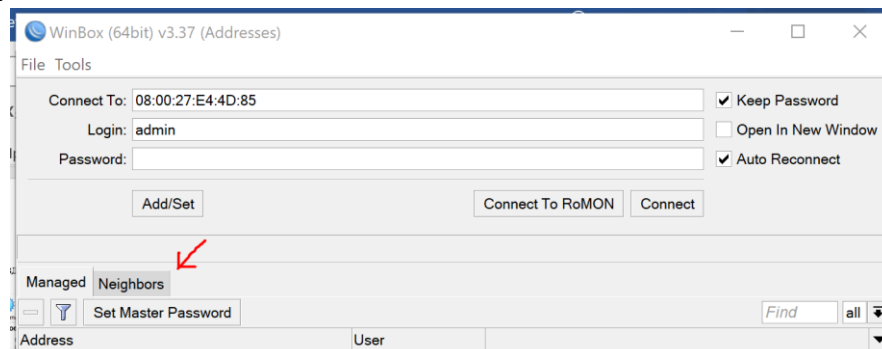
После здания перейдем к настройкам сети Mikrotik.

Переходим в **настройки**, выбираем пункт **сеть**. Меняем тип подключения адаптера 1 на **сетевой мост**.

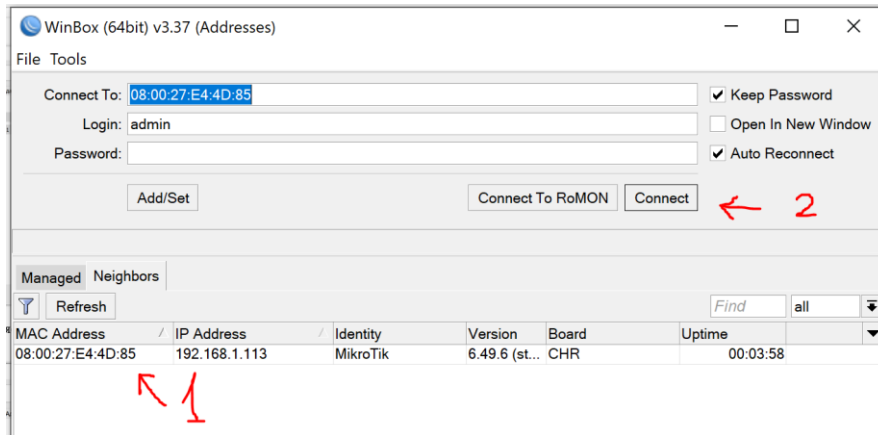


Переходим к адаптеру 2, включаем и выбираем тип подключения **внутренняя сеть**.

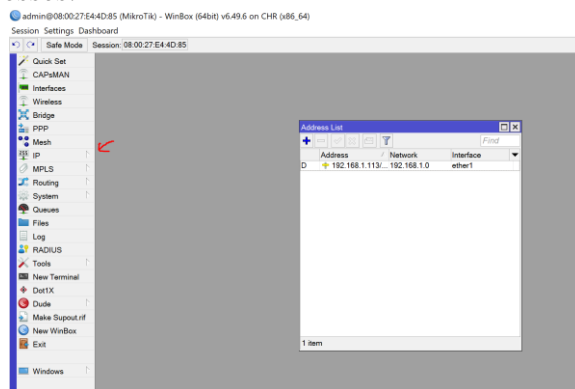
Открываем Winbox



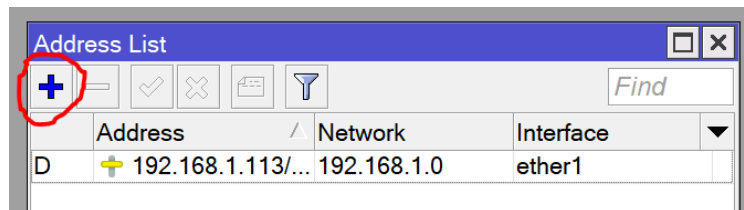
В Winbox'е выбираем **Neighbors**



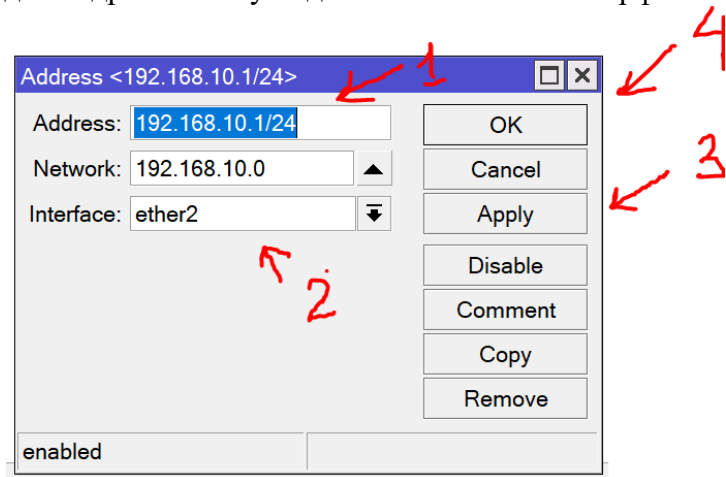
Дважды кликаем на MAC адрес и коннектимся.  
 Логин: admin Пароль: без пароля .  
 Открываем вкладку IP → Addresses.



Жмем на **плюс**



Задаем адрес и маску подсети. Указываем интерфейс №2





Address List			
	Address	Network	Interface
D	192.168.1.113/...	192.168.1.0	ether1
	192.168.10.1/24	192.168.10.0	ether2

Открываем IP → DHCP Server

DHCP Server																		
DHCP	Networks	Leases	Options	Option Sets	Vendor Classes	Alerts												
<table border="1"> <thead> <tr> <th>Name</th> <th>Interface</th> <th>Relay</th> <th>Lease Time</th> <th>Address Pool</th> <th>Add AR...</th> </tr> </thead> <tbody> <tr> <td>dhcp1</td> <td>ether2</td> <td></td> <td>00:10:00</td> <td>dhcp_pool1</td> <td>no</td> </tr> </tbody> </table>							Name	Interface	Relay	Lease Time	Address Pool	Add AR...	dhcp1	ether2		00:10:00	dhcp_pool1	no
Name	Interface	Relay	Lease Time	Address Pool	Add AR...													
dhcp1	ether2		00:10:00	dhcp_pool1	no													

Выбираем DHCP Setup

DHCP Setup

Select interface to run DHCP server on

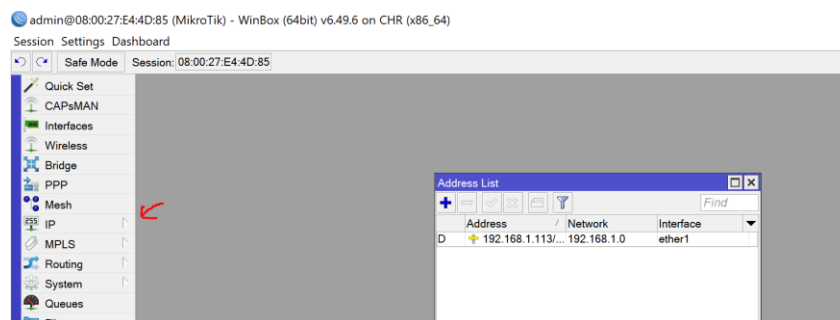
DHCP Server Interface: ether2

Back Next Cancel

Укажем DHCP Сервером **второй интерфейс**, оставшиеся настройки не меняем и жмем next пока окошко не пропадет.

DHCP Server																		
DHCP	Networks	Leases	Options	Option Sets	Vendor Classes	Alerts												
<table border="1"> <thead> <tr> <th>Name</th> <th>Interface</th> <th>Relay</th> <th>Lease Time</th> <th>Address Pool</th> <th>Add AR...</th> </tr> </thead> <tbody> <tr> <td>dhcp1</td> <td>ether2</td> <td></td> <td>00:10:00</td> <td>dhcp_pool1</td> <td>no</td> </tr> </tbody> </table>							Name	Interface	Relay	Lease Time	Address Pool	Add AR...	dhcp1	ether2		00:10:00	dhcp_pool1	no
Name	Interface	Relay	Lease Time	Address Pool	Add AR...													
dhcp1	ether2		00:10:00	dhcp_pool1	no													

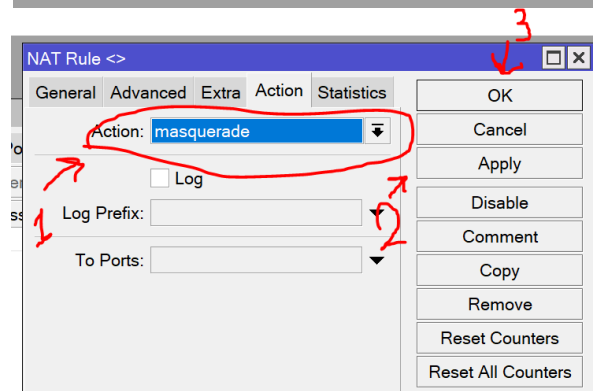
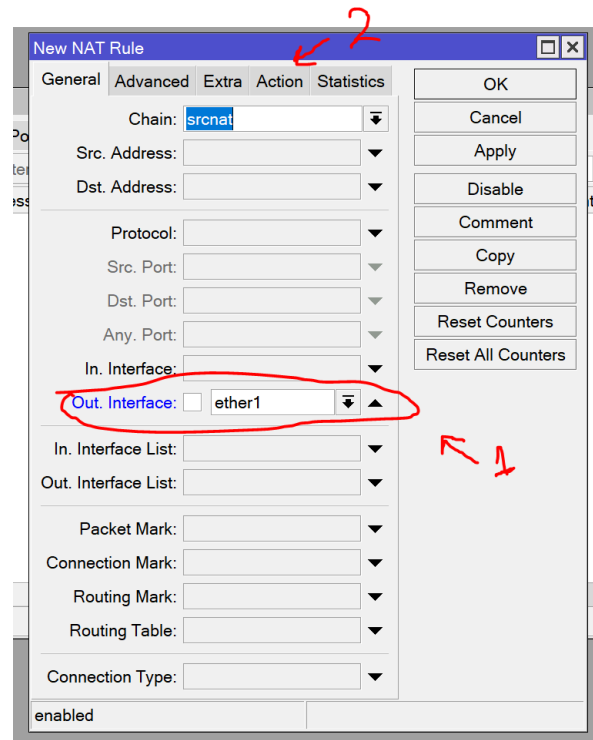
Открываем IP → Firewall



Выбираем вкладку NAT и жмем плюс

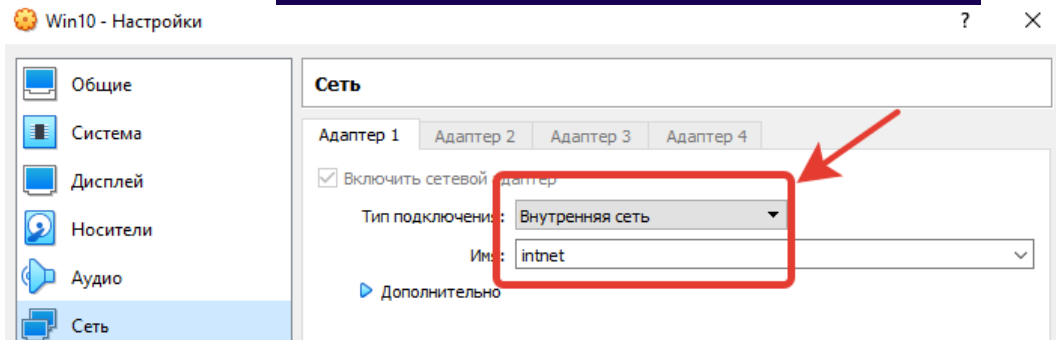
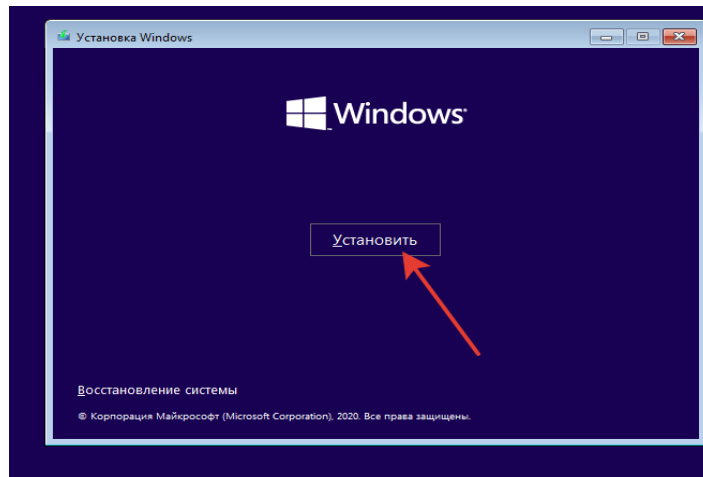
Firewall																																			
Filter Rules	NAT	Mangle	Raw	Service Ports	Connections	Address Lists	Layer7 Protocols																												
<table border="1"> <thead> <tr> <th>#</th> <th>Action</th> <th>Chain</th> <th>Src. Address</th> <th>Dst. Address</th> <th>Proto...</th> <th>Src. Port</th> <th>Dst. Port</th> <th>In. Inter...</th> <th>Out. Int...</th> <th>In. Inter...</th> <th>Out. Ir</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>												#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Ir												
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Ir																								

Настроим nat, чтобы интернет работал и на виртуальных машинах. Выбираем **ether1** и переходим в **Action**



Меняем Action с **accept** на **masquerade**. Жмем apply и ОК.  
На этом настройке маршрутизатора завершена.



## Установка Windows 10



После окончания установки. Отключим Windows и сменим сеть на внутреннюю.

## Установка Kali Linux

Для установки распакуем архив с Kali.

Имя	Дата изменения	Тип	F
 kali-linux-2022.3-virtualbox-amd64.vbox	08.08.2022 13:30	VirtualBox Machine ...	
 kali-linux-2022.3-virtualbox-amd64.vdi	08.08.2022 13:30	Virtual Disk Image	

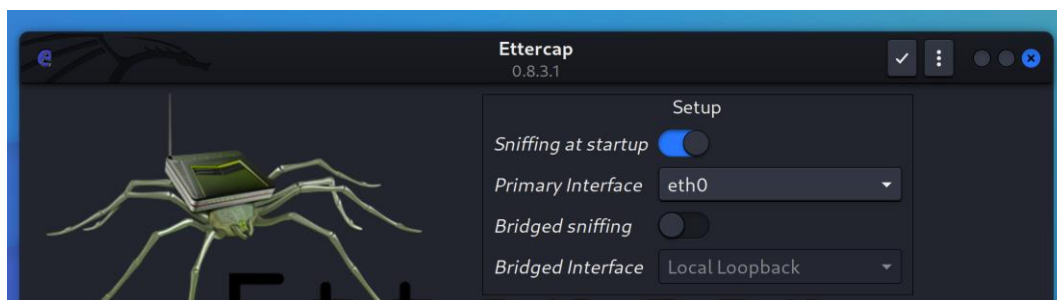
В распакованном архиве дважды нажмем на синий файл vbox и нас перекинет в VirtualBox с уже полностью настроенной машиной.

## Атака



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
└─$ sudo ettercap -G  
[sudo] password for kali:  
  
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

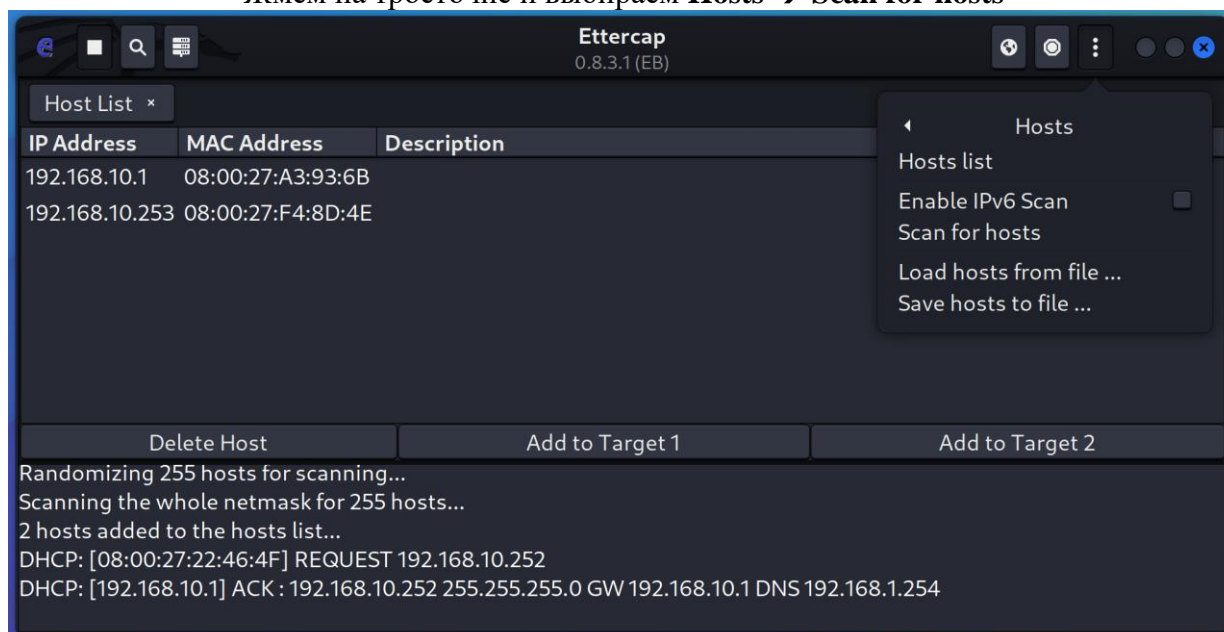
Развернем Ettercap через команду **sudo Ettercap -G**



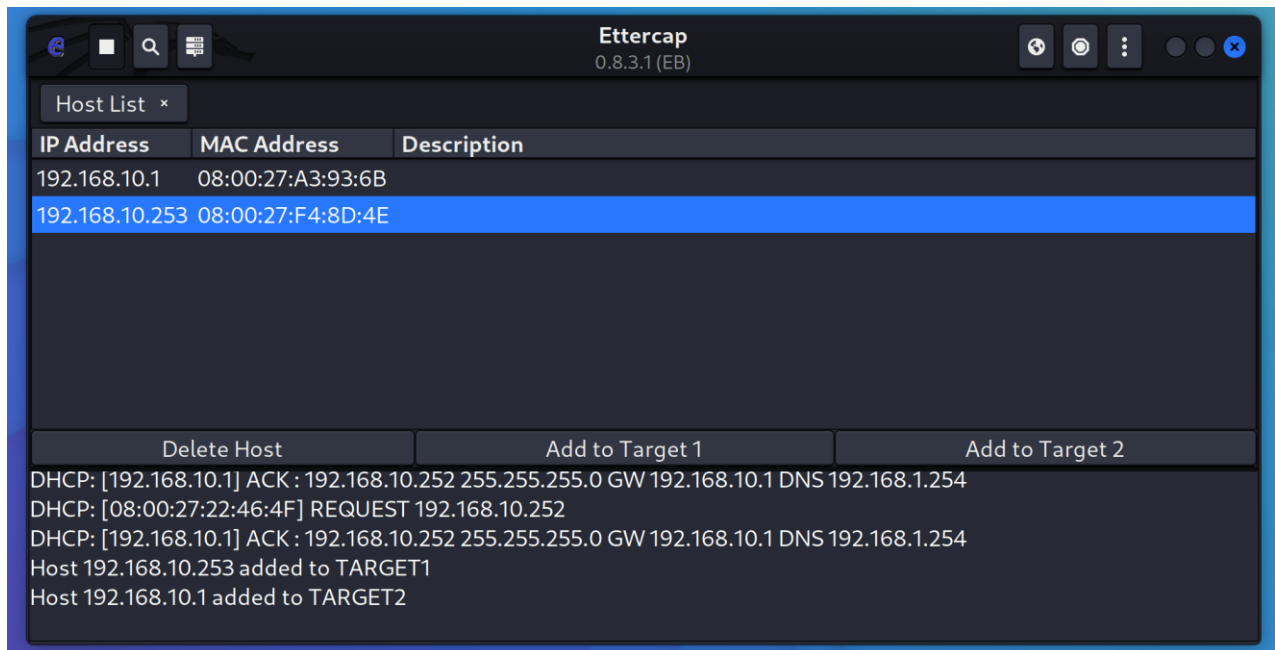
В появившемся окне выбираем интерфейс **eth0** и жмем на галочку



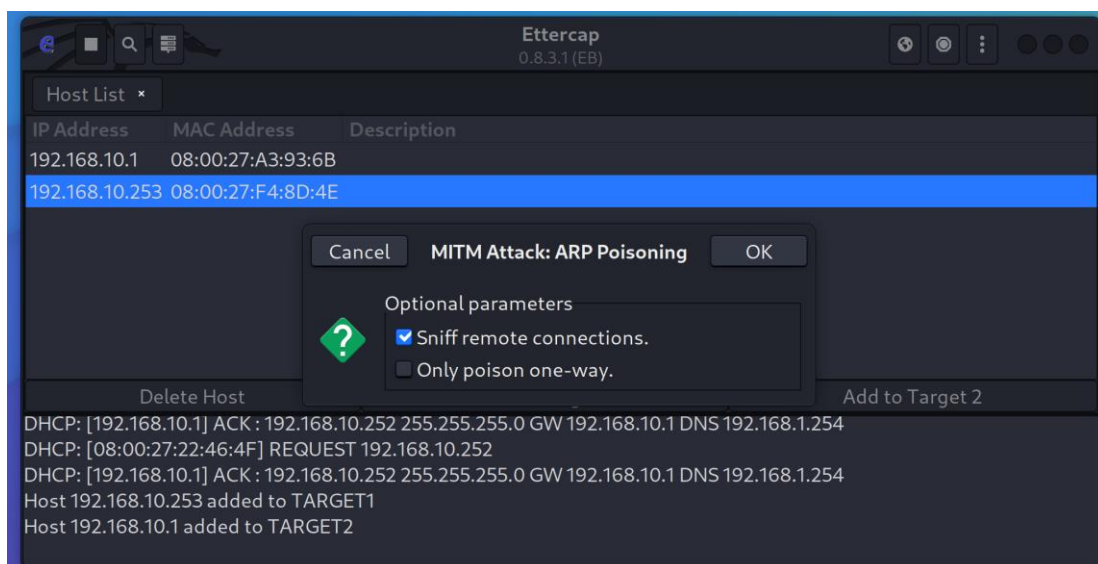
Жмем на трюеточие и выбираем **Hosts → Scan for hosts**



После сканирования переходим в **Hosts → Hosts list** и проверяем есть ли в нашем списке ip-адрес роутера и потенциальный жертвы (если у вас только 1 ip-адрес, повторите верхний пункт со сканированием еще раз)

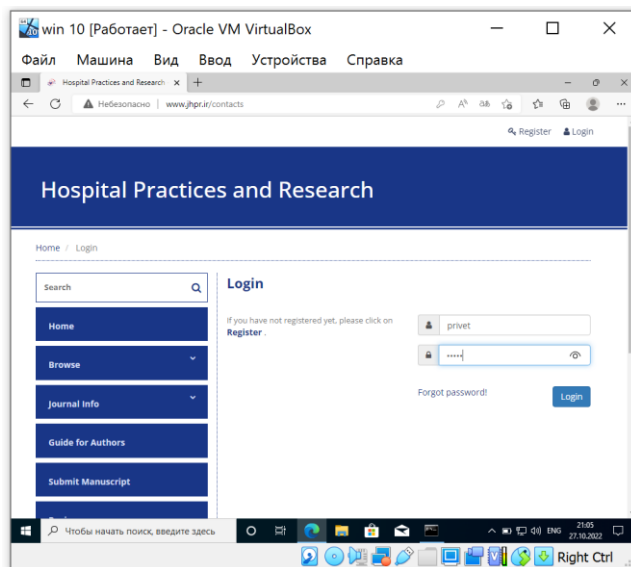


Ip-адрес жертвы(192.168.10.253) определяем как target 1, ip-адрес маршрутизатора(192.168.10.1) определяем как target 2

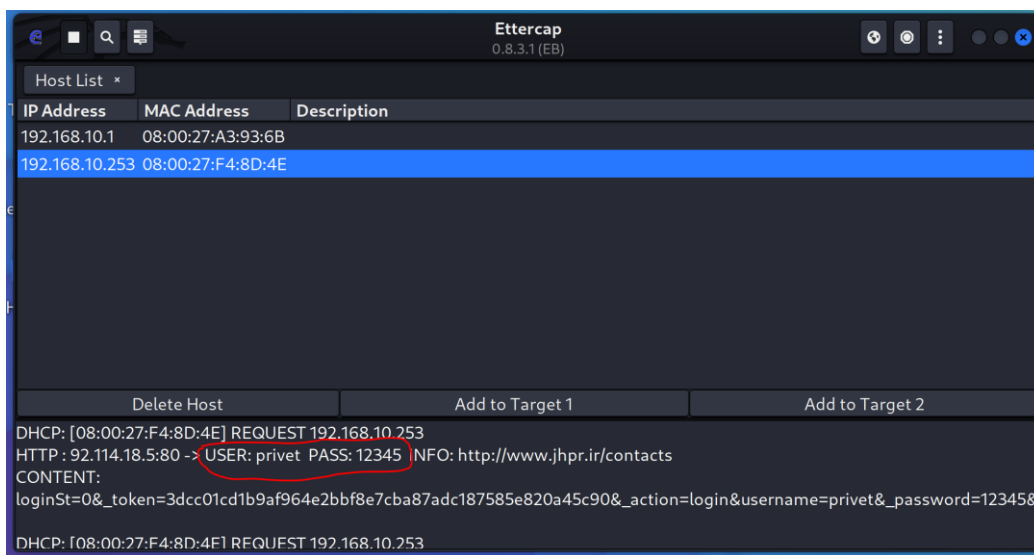


Для проведения атаки ждем на **mitm menu**(глобус) → **Arp poisoning**, в появившемся окне ждем ОК.

Для проверки атаки на компьютере жертвы откроем любой незащищенный сайт и попробуем авторизоваться. Для примера можно использовать использовать эту ссылку [www.jhpr.ir/contacts](http://www.jhpr.ir/contacts)



Заполним фейковыми данными поля для авторизации, нажмем Login и проверим Ettercap на ПК злоумышленника



И как мы видим данные успешно перехвачены.

### Как защититься?

1. Не позволяйте посторонним лицам иметь доступ в вашу сеть.
2. Используйте VPN, эта технология способна решить все проблемы с небезопасными сетями
3. Переходите только по защищенным HTTPS страницам

## 5. Образовательные технологии

Лекционные занятия на курсе проводятся с использованием мультимедийного проектора и в сопровождении с презентациями в формате Power Point. Лабораторные занятия проходят в компьютерных классах, оснащенных персональными компьютерами с ОС Kali Linux

Во время лабораторных занятий студенты активно взаимодействуют с преподавателем, задают вопросы по курсу и лабораторным заданиям, сдают лабораторным заданиям.

## 6. Учебно-методическое обеспечение самостоятельной работы студентов обучающихся по дисциплине

### Форма контроля и критерий оценок

В процессе обучения студентов применяются следующие формы контроля успеваемости:

- посещаемость лекций;
- посещаемость лабораторных занятий;
- выполнение и сдача лабораторных заданий.

## Примерное распределение времени самостоятельной работы студентов

Вид самостоятельной работы	Примерная трудоёмкость	Формируемые компетенции
	очная	
<b>Текущая СРС</b>		
Подготовка к лекции, работа с учебной литературой и электронными источниками	10	ПК-4
Подготовка к практическим, лабораторным занятиям	10	ПК-4, ПК-7
подготовка к контрольным работам	10	ПК-4, ПК-7
выполнение домашних заданий в виде решения отдельных задач, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин	10	ПК-4, ПК-7
самостоятельное изучение разделов дисциплины	10	ПК-7
<b>Творческая проблемно-ориентированная самостоятельная работа</b>		
поиск, изучение и презентация информации по заданной проблеме	10	ПК-4, ПК-7
Подготовка письменных работ (рефератов)	10	ПК-7
исследовательская работа, участие в конференциях, семинарах, олимпиадах	10	ПК-4, ПК-7
Итого СРС	80	

## 7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

### 7.1. Типовые контрольные задания

#### Контрольные вопросы к модулю 1

##### Вариант 1

Задание 1. Основные понятия безопасности сетей

Задание 2. Основные виды аудита безопасности

Задание 3. Протоколы аутентификации

##### Вариант 2

Задание 1. Типы атак.

- Задание 2. Основные функции канального уровня.
- Задание 3. Инструментальный анализ защищенности.

### **Вариант 3**

- Задание 1. DMZ –системы
- Задание 2. Что такое системы обнаружения вторжений (IDS).
- Задание 3. Сетевые ISD (NIDS)

### **Вариант 2**

- Задание 1. DPI- системы
- Задание 2. WAF-системы.
- Задание 3. Протоколы сетевой аутентификации

## **Контрольные вопросы к модулю 2**

### **Вариант 1**

- Задание 1. Вектор сетевых атак. Типы атак.
- Задание 2. Спуфинг ARP.
- Задание 3. Атаки TPC.
- Задание 4. Стандарты WAN.

### **Вариант 2**

- Задание 1. Атаки, связанные с DHCP
- Задание 2. Вредоносное ПО.
- Задание 3. Атаки DNS.
- Задание 4. Режимы беспроводной сети 802.11

### **Вариант 3**

- Задание 1. Защита не используемых портов.
- Задание 2. Нейтрализация атак таблицы MAC-адресов.
- Задание 3. Ограничение и изучение MAC-адресов.
- Задание 4. Режимы нарушения безопасности порта.

### **Вариант 4**

- Задание 1. Защита доступа к устройствам.
- Задание 2. Назначение административных ролей.
- Задание 3. Простой протокол сетевого управления SNMP.
- Задание 4. Определение типов межсетевых экранов.

### **Вариант 5**

- Задание 1. Разработка конфигурации межсетевого экрана.
- Задание 2. Построение набора правил межсетевого экрана.
- Задание 3. Выявление различий между межсетевыми экранами различных типов
- Задание 4. Конечные точки и сетевые диалоги.

## **Контрольные вопросы к 3 модулю**

### **Вариант 1**

- Задание 1 BruteForce.
- Задание 2. Тестирование на проникновение с помощью Burp
- Задание 3. SQL инъекции.
- Задание 4. Cookie.

### **Вариант 2**

- Задание 1. Принцип атаки внедрения SQL.
- Задание 2. Типы SQLi.
- Задание 3. Защита от SQLi.
- Задание 4. Union injection.

### **Вариант 3**

- Задание 1. Разведка сайтов. Поиск каталогов и файлов. Dirb, Dirhunt, DirBuster.
- Задание 2. dirsearch —инструмент командной строки, предназначенный для брут-форса (поиска путём полного перебора) директорий и файлов в веб-сайтах.



Задание 3. DVCS-Ripper

Задание 4. SQLmap

#### Вариант 4

Задание 1. Автоматическое сканирование с помощью Striker.

Задание 2. Соккрытие с помощью Nipe.

Задание 3. Понимание сокетов и создание TCP-сервера

Задание 4 Создание TCP-клиента

Задание 4 Разработка сканера Nmap

#### Вариант 3

Задание 1. WEP-атаки на конфиденциальность проводных сетей

Задание 2. Протоколы WPA и AES

Задание 3. Заблуждения о безопасности беспроводной сети

Задание 4. Беспроводные атаки и защита от них

#### Вопросы к экзамену зачету

1. Нейтрализация атак таблицы MAC-адресов.
2. Ограничение и изучение MAC-адресов.
3. Режимы нарушения безопасности порта.
4. Защита доступа к устройствам.
5. Назначение административных ролей.
6. Простой протокол сетевого управления SNMP.
7. Определение типов межсетевых экранов.
8. Разработка конфигурации межсетевого экрана.
9. Построение набора правил межсетевого экрана.
10. Выявление различий между межсетевыми экранами различных типов
11. Конечные точки и сетевые диалоги.
12. Выявление наиболее активных сетевых узлов с помощью конечных точек и диалогов
13. Общедоступные сайты, которые можно использовать для сбора информации о целевом домене.
14. Анализ DNS.
15. XXE-атака.
16. XSS-атаки.
17. Снижение риска атак межсайтового скриптинга (XSS) с помощью helmet.xssFilter.
18. BruteForce.
19. Тестирование на проникновение с помощью Burp
20. SQL инъекции.
21. Cookie.
22. Union injection.
23. Интерфейс виртуальных туннелей IPsec.
24. Преимущества и недостатки NAT.
25. Варианты подключения к Интернет-провайдеру
26. Функция mysql(i)\_real\_escape\_string
27. Использование анализатора sqlmap.
28. Захват учетных записей
29. Атака протокола отладки Java Debug Wire Protocol
30. Веб-уязвимости
31. Социальная инженерия.
32. Методология тестирования на проникновение: Метод черного ящика (black box), Метод белого ящика (white box), Метод серого ящика (gray box)
33. Анализ защищённости веб-приложений путём внешних проверок (автоматизированных и ручных).
34. Разведка сайтов. Поиск каталогов и файлов. Dirb, Dirhunt, DirBuster.

35. dirsearch —инструмент командной строки, предназначенный для брут-форса (поиска путём полного перебора) директорий и файлов в веб-сайтах.
36. DVCS-Ripper
37. SQLmap
38. Автоматическое сканирование с помощью Striker.
39. Сокрытие с помощью Nipe.
40. Понимание сокетов и создание TCP-сервера
41. Создание TCP-клиента
42. Разработка сканера Nmap
43. WEP-атаки на конфиденциальность проводных сетей
44. Протоколы WPA и AES
45. Заблуждения о безопасности беспроводной сети
46. Беспроводные атаки и защита от них

## **7.2. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Программой дисциплины в целях проверки прочности усвоения материала предусматривается проведение различных форм контроля:

1. «Входной» контроль определяет степень сформированности знаний, умений и навыков обучающегося, необходимым для освоения дисциплины и приобретенным в результате освоения предшествующих дисциплин.
2. Тематический контроль определяет степень усвоения обучающимися каждого раздела (темы в целом), их способности связать учебный материал с уже усвоенными знаниями, проследить развитие, усложнение явлений, понятий, основных идей.
3. Межсессионная аттестация– рейтинговый контроль знаний студентов, проводимый в середине семестра.
4. Рубежной формой контроля является зачет. Изучение дисциплины завершается зачетом, проводимым в виде письменного опроса с учетом текущего рейтинга.

Общий результат выводится как интегральная оценка, складывающаяся из текущего контроля - 50% и промежуточного контроля - 50%.

Текущий контроль по дисциплине включает:

- посещение занятий – 5 баллов,
- участие на практических занятиях - 20 баллов,
- выполнение лабораторных заданий – 60 баллов,
- выполнение домашних (аудиторных) контрольных работ –15 баллов.

Промежуточный контроль по дисциплине включает:

- устный опрос - 30 баллов,
- письменная контрольная работа - 70 баллов.

Неявка студента на промежуточный контроль в установленный срок без уважительной причины оценивается нулевым баллом. Повторная сдача в течение семестра не разрешается.

Дополнительные дни отчетности для студентов, пропустивших контрольную работу по уважительной причине, подтвержденной документально, устанавливаются преподавателем дополнительно.

Итоговой формой контроля знаний, умений и навыков по дисциплине является зачет. Он проводится в форме устного опроса.

Критерии оценки зачета по 100-бальной системе:

- 100 баллов - дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, проявляющаяся в свободном ориентировании понятиями, умении выделять существенные и несущественные его признаки, причинно-следственные связи. Ответ формулируется в терминах науки, логичен, доказателен, демонстрирует авторскую позицию студента.

- 90 баллов - дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается чёткая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Ответ изложен литературным языком в терминах науки.

Могут быть допущены недочёты в определении понятий, исправленные студентом самостоятельно в процессе ответа.

- 80 баллов - дан полный, развёрнутый ответ на поставленный вопрос, доказательно раскрыты основные положения темы; в ответе прослеживается чёткая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Ответ изложен литературным языком в терминах науки. Могут быть допущены недочёты, исправленные студентом с помощью преподавателя.

- 70 баллов - дан полный, но недостаточно последовательный ответ на поставленный вопрос, но при этом показано умение выделить существенные и несущественные признаки и причинно-следственные связи. Ответ логичен и изложен в терминах науки. Могут быть допущены 1-2 ошибки в определении основных понятий, которые студент затрудняется исправить самостоятельно.

- 60 баллов - дан неполный ответ, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, теорий, явлений, вследствие непонимания студентом их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщённых знаний не показано. Речевое оформление требует поправок, коррекции.

- 50 баллов - дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствует фрагментарность, нелогичность изложения. Не понимает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы. Конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

- 40 баллов - ответ студента правилен лишь частично, при разъяснении материала допускаются серьезные ошибки.

- 20-30 баллов - студент имеет общее представление о теме, но не умеет логически обосновать свои мысли.

10 баллов - студент имеет лишь частичное представление о теме.

- 0 баллов – нет ответа.

## **8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.**

### **а) основная литература:**

1. Черняева С.Н. Имитационное Безопасность вычислительных сетей [Электронный ресурс]: учебное пособие/ Черняева С.Н., Денисенко В.В.— Электрон. текстовые данные.— Воронеж: Воронежский государственный университет инженерных технологий, 2016.— 96с.—Режим доступа: <http://www.iprbookshop.ru/50630.html>.— ЭБС «IPRbooks» [дата обращения 10.01.2022]
2. Афонин В.В. Безопасность вычислительных сетей [Электронный ресурс]/ Афонин В.В., Федосин С.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 269 с.— Режим доступа: <http://www.iprbookshop.ru/52179.html>.— ЭБС «IPRbooks» [дата обращения 10.10.2021]
3. Зариковская Н.В. Математическое Безопасность вычислительных сетей [Электронный ресурс]: учебное пособие/ Зариковская Н.В.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2014.— 168 с.—Режим доступа: <http://www.iprbookshop.ru/72124.html>.— ЭБС «IPRbooks» [дата обращения 10.10.2021]

### **б) дополнительная литература**

1. Кудряшов В.С. Безопасность вычислительных сетей [Электронный ресурс]: учебное пособие/ Кудряшов В.С., Алексеев М.В.— Электрон. текстовые данные.— Воронеж: Воронежский государственный университет инженерных технологий, 2012.— 208 с.— Режим доступа: <http://www.iprbookshop.ru/27320.html>.— ЭБС «IPRbooks» [дата обращения 30.08.2022]
2. Безопасность вычислительных сетей. Подходы и методы [Электронный ресурс]: учебное пособие/ В.Н. Волкова [и др.].— Электрон. текстовые данные.— СПб.: Санкт-Петербургский

политехнический университет Петра Великого, 2013.— 568 с.— Режим доступа: <http://www.iprbookshop.ru/43957.html>.— ЭБС «IPRbooks» [дата обращения 30.08.2022]

#### **9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.**

1. eLIBRARY.Ru [Электронный ресурс]: электронная библиотека / Науч. электр. б-ка.- МОСКВА.1999. – Режим доступа: <http://elibrary.ru> (дата обращения 15.04.2022). – Яз. рус., англ.
2. Moodle [Электронный ресурс]: система виртуального обучения: [база данных] / Даг.гос.универ. – Махачкала, - Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: <http://moodle.dgu.ru>. (дата обращения 22.05.22).
3. Электронный каталог НБ ДГУ Ru [Электронный ресурс]: база данных содержит сведения о всех видах лит., поступающих в фонд НБ ДГУ / Дагестанский гос.унив. – Махачкала. – 2010. – Режим доступа:<http://elib.dgu.ru>. свободный (дата обращения 11.03.2022)
4. Национальный Открытый Университете «ИНТУИТ» [Электронный ресурс]: - [www.intuit.ru](http://www.intuit.ru) (дата обращения 12.03.2022)

#### **10.Методические указания для обучающихся по освоению дисциплины.**

При освоении всех разделов дисциплины необходимо сочетание всех форм учебной деятельности: изучение лекционного материала, выполнение заданий на лабораторных работах, как с использованием компьютера, так и без него, самостоятельная работа с рекомендуемой литературой и использование методических указаний.

После каждого лекционного занятия студенты должны повторить материал лекции по конспектам, а перед каждым очередным занятием - освежить в памяти материал предыдущего.

Самостоятельная работа ориентирует студентов на углубленное изучение и осмысление тем учебного курса. При подготовке к лабораторной работе студент должен изучить рекомендуемые материалы. Если в задании на лабораторную работу есть непонятные неясные моменты, необходимо задать вопросы преподавателю. По каждой лабораторной работе необходимо подготовить отчет, в котором отразить все основные действия, выполняемые в процессе лабораторной работы, а также результаты, полученные при выполнении лабораторной работы.

#### **11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.**

1. Компьютерные классы с набором лицензионного базового программного обеспечения для проведения лабораторных занятий;
2. Лекционная мультимедийная аудитория для чтения лекций с использованием мультимедийных материалов.

#### **12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.**

При освоении дисциплины для выполнения лабораторных работ необходимы классы персональных компьютеров с ОС Kali Linux, Windows Server 2016. Для проведения лекционных занятий, необходима мультимедийная аудитория с набором лицензионного базового программного обеспечения.

#### **Лекционные занятия**

- Видеопроектор, ноутбук, презентатор
- Подключение к сети Интернет