

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

# «МИРЭА – Российский технологический университет» РТУ МИРЭА РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

Кафедра КБ-2 «Прикладные информационные технологии»

Практическая работа № 4

по дисциплине «Безопасность Операционных систем»

«Основы Kali Linux»

|  |  |
| --- | --- |
|  | Выполнил:  Студент БББО-05-20  Кутьин З.С. |
|  | Проверил:  Абрамов Д.П. |

Москва 2022

# Цель работы

Установить Kali linux, metasploitable 2, настроить их взаимодействие.

Изучить инструменты Kali linux для сканирования сети. Утилита metasploit.

**Время выполнения работы:** 4 академических часа.

# Краткие теоретические сведения

Kali Linux был разработан фирмой Offensive Security, которая специализируется на безопасности. Он создан на основе Debian и содержит в себе наработки дистрибутива для цифровой криминалистики и тестирования безопасности BackTrack.

Первая версия BackTrack вышла в 2006 году, она объединила в себе несколько проектов, основным предназначением которых было тестирование на проникновение. Дистрибутив предназначался для использования в качестве LiveCD.

В 2012 году такой дистрибутив, как BackTrack прекратил существовать, а вместо него появился Kali Linux, который перенял все плюсы предыдущей версии и все программное обеспечение. Он был результатом слияния двух проектов: WHAX и Auditor Security Collection. Сейчас дистрибутив стабильно развивается и силы разработчиков направлены на исправление ошибок и расширение набора инструментов.

На официальном сайте есть такое описание дистрибутива: "Penetration Testing и Ethical Hacking Linux Distribution" или по-нашему дистрибутив для тестирования на проникновения и этичного хакинга. Проще говоря, этот дистрибутив содержит множество инструментов, связанных с безопасностью и сетями, которые ориентированы на экспертов в компьютерной безопасности.

Дистрибутив Linux - это не больше чем ядро и набор базовых утилит, приложений и настроек по умолчанию. Kali Linux не предоставляет ничего

уникального в этом плане. Большинство программ может быть просто установлено в любом другом дистрибутиве, или даже в Windows.

Отличие Kali Linux в том, что он наполнен такими инструментами и настройками, которые нужны для тестирования безопасности, а не для обеспечения нормальной работы обычного пользователя. Если вы хотите использовать Kali вместо основного дистрибутива - вы совершаете ошибку. Это специализированный дистрибутив для решения определенного круга задач, а это значит, что решение задач, для которых он не был предназначен будет более трудным, например, тот же поиск программ. Возможности Kali Linux сосредоточены на тестировании безопасности.

# Порядок выполнения работы

# Настраиваем цель

# Перечень известных систем виртуализации, их отличительные особенности:

# VMware. Гипервизор 1-го типа выполняется непосредственно на «голом железе». VMware Fault Tolerance — это технология VMware, разработанная для защиты критически важных виртуальных машин с реальной непрерывной доступностью. Distributed Resource Scheduler — это технология, позволяющая в автоматическом режиме балансировать нагрузку на ЦПУ и ОЗУ. Storage DRS (SDRS) выравнивает нагрузку на хранилища и позволяет обеспечить требуемый уровень заполненности хранилища (Utilized Space) и/или задержки ввода-вывода (I/O Latency).

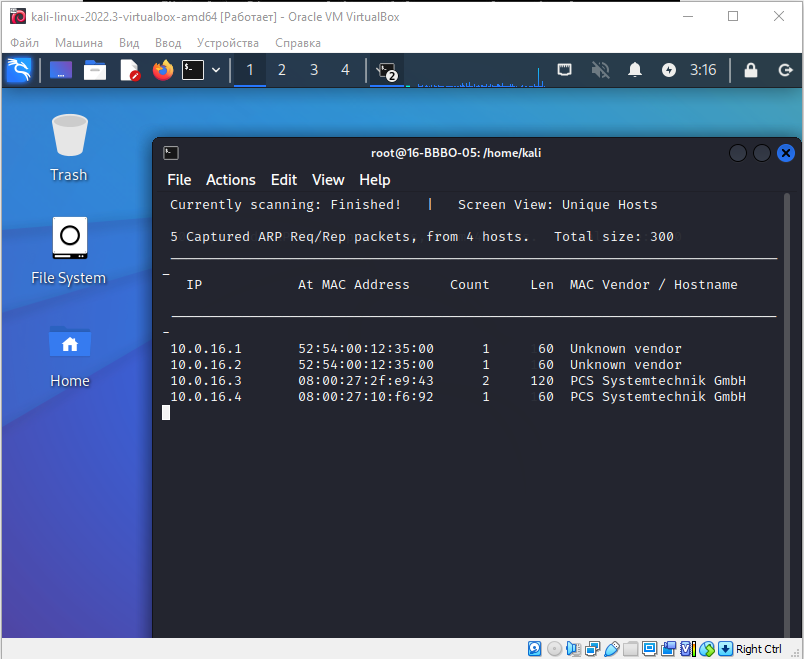
* Xen. Гипервизор работает на «голом железе», но для своей работы ему требуется управляющая операционная система в dom. Проброс GPU внутрь гостя GPU Pass-through (для конкретного виртуального гостя — конкретный GPU в физическом сервере). GPU Virtualization — возможность множеству виртуальных машин получить доступ к GPU хоста, что лучше, чем программная эмуляция. vGPU Live Migration — позволяет виртуальной машине перемещаться между хостами без потерь с доступом к GPU
* Hyper-V. Гибридный тип (Hybrid, Type-1+), где гипервизор контролирует процессор и память, а специальная служебная ОС даёт гостевым операционным системам доступ к физическому оборудованию. Hyper-V позволяет уменьшать размер диска.
* KVM. Гипервизор 2-го типа, входящий в состав операционной системы. Неприхотливость к аппаратной части сервера. Благодаря KVM можно получить недорогую виртуальную среду.

Краткое описание установленных ОС с описанием их назначения.

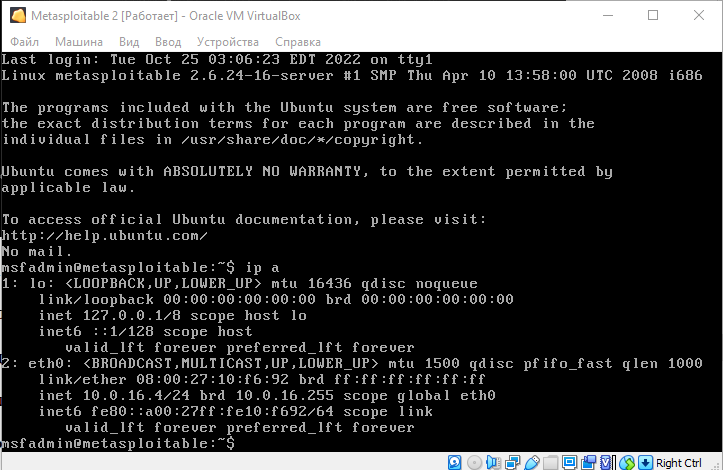
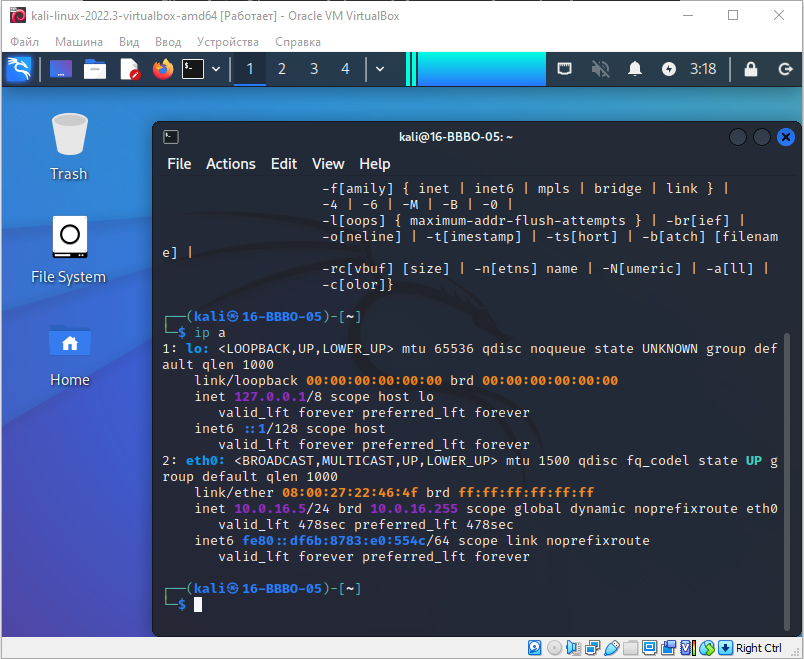
* Kali Linux — GNU/Linux-LiveCD, возникший как результат слияния WHAX и Auditor Security Collection. Предназначен прежде всего для проведения тестов на безопасность. Kali Linux включает инструменты безопасности, такие как:
  + Aircrack-ng
  + Burp suite
  + Cisco Global Exploiter
  + Ettercap
  + John the Ripper
  + Kismet
  + Maltego
  + Metasploit
  + nmap
  + ClamAV
  + rkhunter
  + chkrootkit
  + lynis auditing tool
  + Tiger security tool
  + havp
  + Инструменты социальной инженерии
  + Wireshark
  + jSQL Injection
  + Hydra
  + LKRG Linux Kernel Runtime Guard
  + out-of-tree
  + Инструменты обратной разработки
  + Инструменты судебной экспертизы, такие как Binwalk, Foremost, Volatility, и т. д.
* Metasploitable виртуальная машина, специально спроектированной на максимальную уязвимость для тренировки, тестов эксплойтов и обучения новичков. В отличие от других уязвимых виртуальных машин, Metasploitable фокусируется на уязвимостях в операционной системе Linux и сетевых сервисах, а не на отдельных приложениях. Metasploitable 2 — нечто вроде боксёрской груши для работы «пентестеров» и использования программ вроде Metasploit и Nmap. В ней открыты все порты и присутствуют все известные уязвимости, некоторые из которых вы можете встретить в реальной жизни на настоящих системах.

Примеры выполнения команд **netdiscover, ifconfig, ip**, которые были использованы в ходе работы с описанием их результатов.

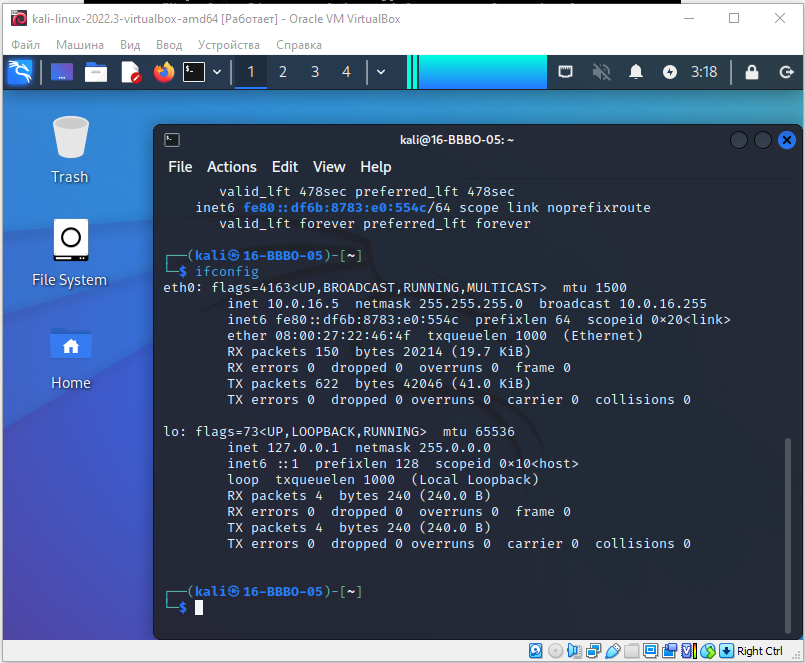
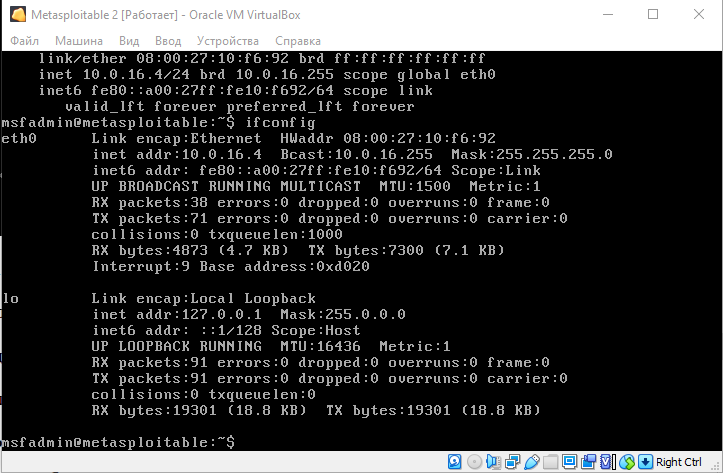
* **netdiscover –r 10.0.16.0/24 .** Вывела на экран ip и MAC адреса всех хостов, находящихся в той же сети, что и текущий.



* **ip a.** Вывела на экран информацию о портах и Ip-адресе.



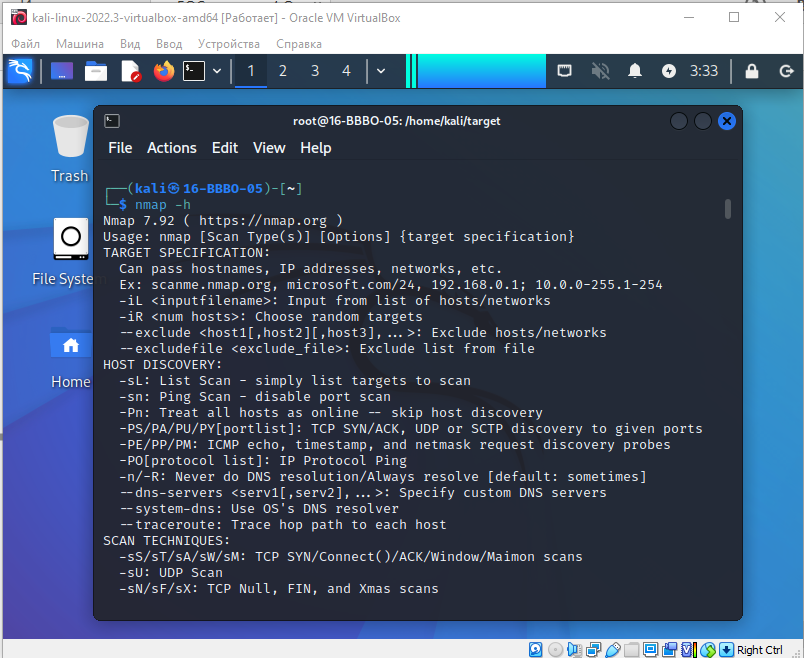
* **ifconfig.** Аналогична работе **ip a.**



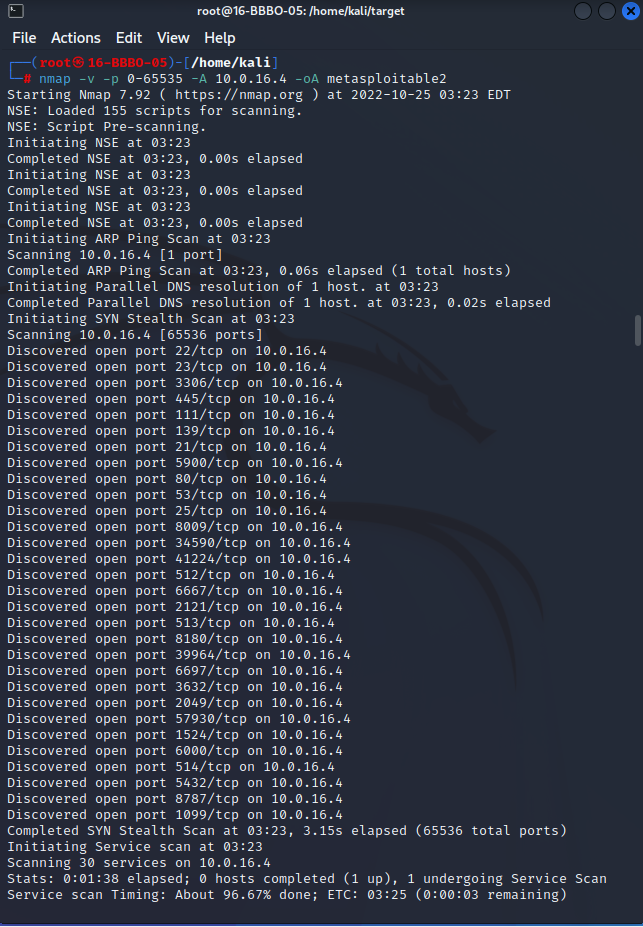
# Сканирование портов.

Примеры выполнения команды **nmap**, которые были использованы в ходе работы с описанием их результатов. Перечень основных ключей с их описанием.

* **nmap –h.** Вывела на экран все возможные опции с описанием их работы



* **nmap –v –p 0-65535 –A 10.0.16.4 –oA metasploitable2.** Вывела информацию о в подробном режиме работы сканирования всех tcp-портов с отображением версий ОС по ip: 10.0.16.4 с сохранением вывода данных в файлы в трех форматах: gnmap, nmap, xml с названиями «metasploitable2».



Перечень открытых портов, названия и версии сервисов, которые их используют.

* 22 – SSH (Secure SHell) — криптографический сетевой протокол для безопасной передачи данных
* 23 – Telnet — применяется для передачи текстовых сообщений в незашифрованном виде
* 3306 – Система управления базами данных MySQL
* 445 – MICROSOFT-DS — используется в Microsoft Windows 2000 и поздних версий для прямого TCP/IP-доступа без использования NetBIOS (например, в Active Directory)
* 111 – SUNRPC (Sun Remote Procedure Call)
* 139 – NETBIOS-SSN (NetBIOS Session Service)
* 21 – FTP — для передачи команд FTP
* 5900 – Virtual Network Computing (VNC) remote desktop protocol (used by Apple Remote Desktop and others)
* 80 – HTTP (HyperText Transfer Protocol); ранее — WWW
* 53 – DOMAIN (Domain Name System, DNS)
* 25 – SMTP (Simple Mail Transfer Protocol) — применяется для пересылки почтовых сообщений в виде незашифрованного текста
* 8009 – netware-rmgr, irdmi
* 34590 – Детали - Unassigned, Источник - LANA
* 41224 – Детали - Unassigned, Источник - LANA
* 512 – EXEC (Remote Process Execution)
* 6667 – Сервис – irc, Детали - Internet Relay Chat, Источник - SANS
* 2121 – Сервис – scientia-ssdb, Детали - SCIENTIA-SSDB, Источник - IANA
* 513 – LOGIN — удаленный вход наподобие Telnet; автоматическая проверка подлинности выполняется на основе номеров привилегированных портов и распределённых баз данных, которые идентифицируют «домены аутентификации»
* 8180 – Сервис – irdmi, Детали - Web service, iTunes Radio streams, Источник - Apple
* 39964 – Детали - Unassigned, Источник - LANA
* 6697 – IRC SSL (Secure Internet Relay Chat) — often used
* 3632 – distributed compiler
* 2049 – Network File System
* 57930 – Детали - Dynamic and/or Private Ports, Источник - LANA
* 1524 – ingreslock, ingres
* 6000 – X11—used between an X client and server over the network
* 514 – SHELL — для выполнения команд на удалённой системе; используется в аналогах командной строки с автоматической аутентификацией (например, rsh[en], rcp[en])
* 5432 – PostgreSQL Database
* 8787 – Сервис – irdmi, Детали - Web service, iTunes Radio streams, Источник – Apple; Сервис – msgsrvr, Детали - Message Server, Источник - IANA
* 1099 – rmiregistry (RMI Registry)

# Взлом FTP

Описание модулей **metasploit**.

Все модули делятся на несколько типов, в зависимости от предоставляемой функциональности:

* **Exploit** — код, эксплуатирующий определенную уязвимость на целевой системе (например, переполнение стека)
* **Payload** — код, который запускается на целевой системе после того, как отработал эксплойт (устанавливает соединение, выполняет шелл-скрипт и прочее)
* **Post** — код, который запускается на системе после успешного проникновения (например, собирает пароли, скачивает файлы)
* **Encoder** — инструменты для обфускации модулей с целью маскировки от антивирусов
* **NOP** — генераторы NOP’ов. Это ассемблерная инструкция, которая не производит никаких действий. Используется, чтобы заполнять пустоту в исполняемых файлах, для подгонки под необходимый размер
* **Auxiliary** — модули для сканирования сети, анализа трафика и так далее.

Опишите переменные в модуле **exploit/unix/ftp/vsftpd\_234\_backdoor**.

* Unix – платформа
* ftp – сервис ftp-сервер
* vsftpd\_234\_backdoor – уязвимость сервера ftp с версией vsftpd 2.3.4

Перечень и описание основных команд FTP (5 - 10 шт)

* ABOR — Прервать передачу файла.
* CDUP — Сменить каталог на вышестоящий.
* CWD — Сменить каталог.
* DELE — Удалить файл (DELE filename).
* EPSV — Войти в расширенный пассивный режим. ...
* HELP — Выводит список команд, принимаемых сервером.
* LIST — Возвращает список файлов каталога.

**Вывод:** Я изучил основы и функционал Kali Linux и metasploitable2. Применил несколько команд для проведения взлома и сканирования сетей. Изучил команду **nmap**  и утилиту metasploit.