Teach Me Skills

Kali-linux

Или история, о том чем я «ломал» пентагон)

Teach
Me
Skills

Собираемся и отмечаемся

Mini-quize по прошлой теме:

1. **В чем отличие между бэкапом и снапшотом?**
2. **Какой тип адаптера пробросит ВМ напрямую в сеть?**
3. **Где сейчас активно применяется виртуализация?**
4. **Основные отличия bare-metal от hosted гипервизоров?**
5. **В чем основное отличие между аппаратной и программной реализацией?**

Mini-quize по текущей теме:

1. **Что такое дистрибутив?**
2. **Какие существуют редакторы в консоли?**
3. **Что такое LiveUSB?**
4. **Для чего применяется nmap?**
5. **За что отвечают команды rm, touch, sudo, ping, lsblk, pwd, zip.**
6. **Что такое права доступа?**

Teach Me Skills

План занятия

1. Рассмотрим ОС.
2. Изучим некоторый функционал ОС.
3. Рассмотрим какие есть инструменты.
4. Попрактикуемся в командах и донастроим нашу ОС.

Знакомство с ОС

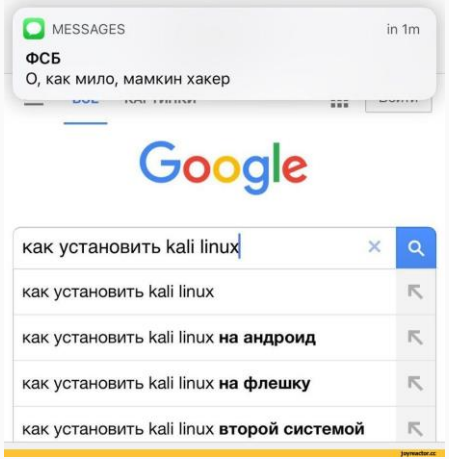
Kali Linux — это специализированный дистрибутив Linux, предназначенный для пентеста с упором на сети. Он включает в себя множество предустановленных инструментов для оценки безопасности компьютерных систем. Разработан и поддерживается компанией Offensive Security.

Основные инструменты:

- Nmap: Сканер сетей и портов.
- Wireshark: Анализатор сетевых пакетов.
- Metasploit Framework: Платформа для разработки и выполнения эксплойтов.
- Aircrack-ng: Набор инструментов для аудита безопасности Wi-Fi.
- John the Ripper: Утилита для взлома паролей.
- Burp Suite: Средство для тестирования безопасности веб-приложений.

Kali доступен в различных версиях: для x86, x64 архитектур, а также для ARM-устройств, таких как Raspberry Pi.

Компания Offensive Security предоставляет обширные учебные материалы, включая курсы и сертификационные программы, такие как **OSCP** (Offensive Security Certified Professional).



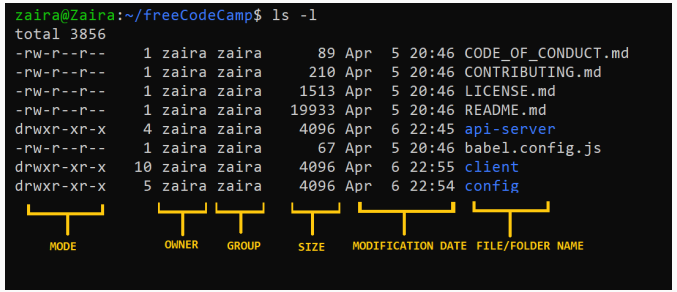
Особенности:
Основан на Debian
Поддерживает LiveCD/USB
Пакетный менеджер dpkg
Системные требования:
1+ GB **RAM**
20+ GB **ROM**

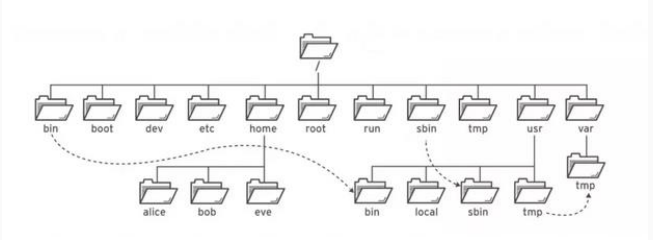
https://www.kali.org

Расположение компонентов

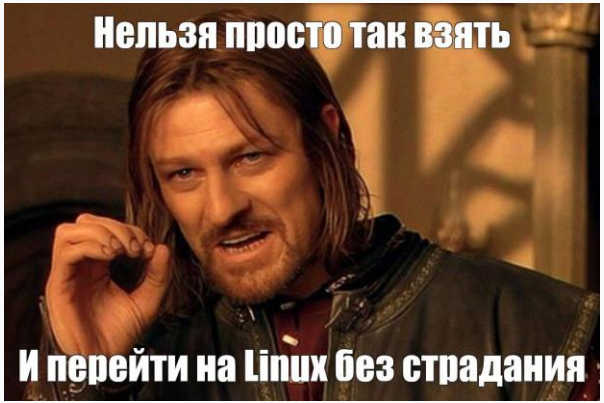
Основные директории:

1. **/** (корнень) - Главная директория файловой системы. Все остальные директории расположены под корнем.
2. **/bin** - Содержит важные системные бинарные файлы (исполняемые программы), которые необходимы для работы системы, например, **ls**, **cp**, **mv**.
3. **/sbin** - Содержит системные бинарные файлы, например, **ifconfig**, **reboot**.
4. **/usr** - Содержит пользовательские программы и утилиты.
   - **/usr/bin** — Бинарные файлы программ.
   - **/usr/sbin** — Системные утилиты для администрирования.
   - **/usr/lib** — Библиотеки программ.
5. **/etc** - Содержит конфигурационные файлы системы и программ.
   - **/etc/fstab** — Таблица монтирования файловых систем.
   - **/etc/passwd** — Информация о пользователях.
   - **/etc/hosts** — Локальная таблица сопоставлений имен и IP-адресов.
6. **/var** - Хранит изменяющиеся данные, такие как журналы и временные файлы.
   - **/var/log** — Лог-файлы системы и приложений.
   - **/var/tmp** — Временные файлы, которые сохраняются между перезагрузками.
7. **/home** - Содержит домашние каталоги пользователей.
   - **/home/username** — домашний каталог пользователя username.
8. **/root** - Домашний каталог пользователя **root** (суперпользователя).





Важные компоненты ОС #2



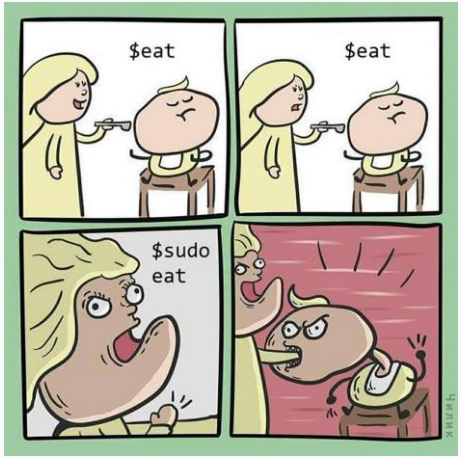
Важные конфигурационные файлы:

1. **/etc/hostname**
   - Содержит имя хоста системы.
2. **/etc/hosts**
   - Локальная таблица сопоставлений IP-адресов и имен хостов.
3. **/etc/resolv.conf**
   - Настройки DNS-серверов.

4. **/etc/network/interfaces** (или /etc/netplan/*.yaml) - Настройки сетевых интерфейсов.
5. **/etc/fstab** - Конфигурация для автоматического монтирования файловых систем.
6. **/etc/passwd** - Информация о пользователях системы.
7. **/etc/shadow** - Хеши паролей пользователей.
8. **/etc/sudoers** - Настройки для утилиты sudo.
9. **/etc/systemd/system** - Пользовательские файлы для управления службами и настройками systemd.
10. **/etc/apt** - Конфигурация и источники для управления пакетами через apt.

Устройство команд

КОМАНДА ОПЦИИ АРГУМЕНТЫ ПОТОК ФАЙЛ_ПОТОКА
cat –b data.txt
echo test message > data.txt



Ввод и вывод распределяется между тремя стандартными потоками:
0 - stdin — стандартный ввод (клавиатура),
1 - stdout — стандартный вывод (экран),
2 - stderr — стандартная ошибка (вывод ошибок на экран).

cmd < file — использовать файл как источник данных для стандартного потока ввода.
cmd > file — направить стандартный поток вывода в файл. Если файл нет, будет создан, иначе — перезаписан.
cmd 2> file — направить стандартный поток ошибок в файл. Если файл нет, будет создан, иначе — перезаписан.
cmd >> file — направить стандартный поток вывода в файл. Если файл нет, будет создан, иначе — данные будут дописаны к нему в конец.
cmd 2>> file — направить стандартный поток ошибок в файл. Если файл нет, будет создан, иначе — данные будут дописаны к нему в конец.

Команды Unix

Команды для работы с файловой системой ОС:

1) ls – просмотр файлов (ll, -la)
2) cd – перемещение по каталогам (.. , ../../ , /bob/data/video/)
3) mkdir – создание директории/пути (bob , bob/data/video)
4) rm – удаление файла/диреткории (-r /dir, filename.txt)
5) mv – перемещение файла/каталога (source destination,
6) cp – копирование (по аналогии с mv)
7) lsblk – информация о устройствах хранения(-f)
8) df – информация о файловых системах (-h)
9) pwd – информация о текущем каталоге
10) which – информация о расположении команды или сценария

Команды для работы с файлами в ОС:

1) cat – вывод для чтения ***cat file.txt***
2) nano – редактирование файла ***nano file.txt***
3) vim - редактирование файла ***vim/vi file.txt***
4) touch – создание файла ***touch file.tx***
5) tail – вывод последних строк ***tail –n 20 –f file.txt***
6) head – вывод первых строк ***head –n 20 –f file.txt***

Команды для управления состоянием ОС:

1) reboot – перезапуск ***reboot***
2) shutdown – выключение ***shutdown now***

Системные компоненты [CRON]

Службы, демоны и планировщик:

1) **crontab**(демон) **-** используется для периодического выполнения заданий в определённое время
2) **Systemctl –** управление запущенными службами (демонами)
3) **Service –** управление запущенными сервисами

Systemctl:

```
systemctl status ssh.service
systemctl start ssh.service
systemctl stop ssh.service
systemctl restart ssh.service
systemctl enable ssh.service
systemctl disable ssh.service
```

Пример:

каждый день в 2:30 AM:

30 2 * * *

каждую пятницу в 3:00 PM:

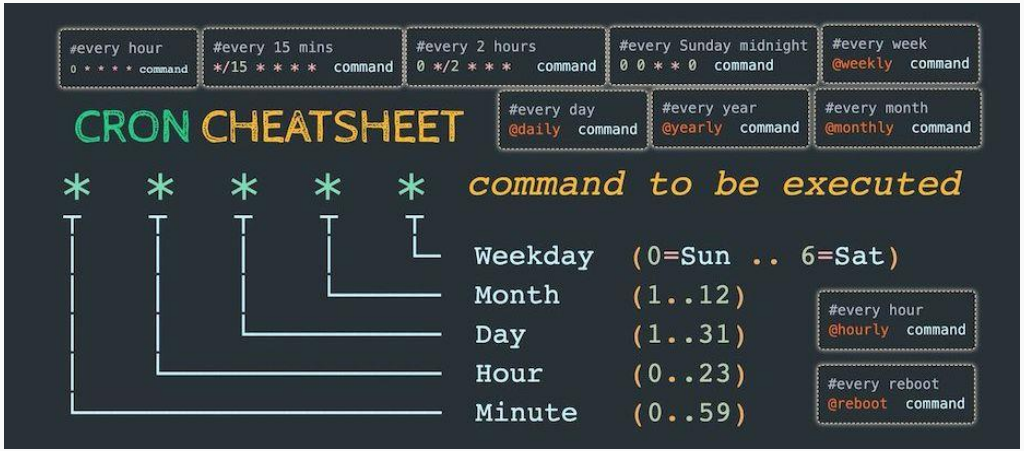
0 15 * * 5

1-го числа каждого месяца в полночь:

0 0 1 * *

Cron:

crontab –e (edit) –l (show) –r(remove) filepath(start)



Системные компоненты [Доступ+Пользователи]

Команды для работы с правами в ОС:

1) Chmod – изменение прав доступа
2) Chown - изменение владельца и/или группы для указанных файлов
3) Groupadd – создание группы пользователей
4) Usermod – управление пользователями в контексте групп

groupadd опции имя_группы
groupadd group1
usermod -a -G group1 user

chown пользователь опции /путь/к/файлу
chown root ./books
chown root:root ./books
chown root:root –R ./books

useradd -d home-dir name
userdel name

Chmod **777 (u, g, o)**

u - владелец файла **g** - группа файла **o** - все остальные пользователи

Модификаторы доступа

двоичная	символьная	права на файл	права на каталог
000	---	нет	нет
001	--x	выполнение	чтение свойств файлов
010	-w-	запись	нет
011	-wx	запись и выполнение	всё, кроме получения имени файлов
100	r--	чтение	чтение имён файлов
101	r-x	чтение и выполнение	доступ на чтение файлов/их свойств
110	rw-	чтение и запись	чтение имён файлов
111	rwx	все права	все права

Настройка ОС

Обновление и доустановка пакетов:

```
sudo apt update -y
sudo apt upgrade -y
```

Доустановка SSH сервера:

```
sudo apt install openssh-server
sudo systemctl enable --now ssh
```

Установка пароля рута:

```
sudo su
passwd
```

Настройка ssh:

```
ssh-keygen -t rsa
cat key.pub >> .ssh/authorized_keys (приватный ключ копируем себе на ПК)
```

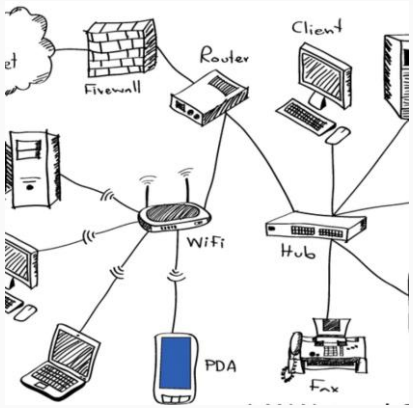
Отключение доступа по паролю:

```
sudo nano /etc/ssh/sshd_config
PasswordAuthentication no
```

Системные компоненты [Сети]

Сети и фаерволы:

1) Ip – утилита настройки сетей
2) Route – команда настройки сетевых маршрутов
3) Ufw – утилита для управления файерволлом netfilter
4) Iptables - утилита для управления файерволлом netfilter
5) Netplan – утилита настройки сети



В Linux основные компоненты IP включают:

1. **iproute2** (`ip`): Это утилита командной строки, предназначенная для управления сетевыми интерфейсами, маршрутизацией, политиками трафика, адресацией и другими аспектами IP-сетей.
2. Управление сетевыми интерфейсами: **ip link** set /show/
3. Позволяет просматривать, добавлять, изменять и удалять IP-адреса на интерфейсах **ip addr** show/add.
4. Настройка маршрутов **ip route**
5. iptables: Межсетевой экран (firewall) в Linux, для фильтрации и манипулирования сетевым трафиком на уровне IP и выше (например, TCP/UDP).

Практика работы с Linux

Основные инструменты Kali

sqlmap
Инструмент для **выявления** и **эксплуатации SQL-инъекций**.
- Команда: sqlmap -u "http://example.com/vuln.php?id=1" --dbs.

Hydra
Инструмент для перебора паролей.
- Команда: hydra -l user -P password_list.txt ftp://192.168.1.100 (перебор паролей для FTP).

John the Ripper
Утилита для взлома паролей.
- Команда: john --wordlist=wordlist.txt hashfile.txt (использование словаря для атаки на хеши паролей).

Metasploit Framework
Платформа для **разработки** и **выполнения эксплойтов**.
- Команда: msfconsole (запуск интерфейса командной строки Metasploit).

Burp Suite
Платформа для тестирования безопасности **веб-приложений**.
- Команда: burpsuite (запуск графического интерфейса Burp Suite).

Aircrack-ng
Набор инструментов для работы с **беспроводными сетями**. Поддерживает взлом WEP и WPA/WPA2.
- Команда: aircrack-ng -w wordlist.txt -b 00:11:22:33:44:55 capture.cap (взлом WPA/WPA2).

Nmap
Сканер сети для обнаружения хостов и сервисов.
- Команда: nmap -sP 192.168.1.0/24 (сканирование сети для обнаружения активных хостов).

Hashcat
Инструмент для перебора паролей.
- Команда: hashcat -m 0 -a 0 hashfile.txt wordlist.txt (взлом хешей с помощью словаря).

nmap

Nmap — opensource инструмент для сканирования и аудита безопасности сетей. Он используется для обнаружения активных хостов, открытых портов, служб, а также для выявления уязвимостей и информации о сети.

Основные возможности Nmap

1. Сканирование портов: Определение открытых портов на хостах.
2. Определение служб: Определение служб и версий, работающих на открытых портах.
3. Определение операционных систем: Определение операционных систем и версий.
4. Скриптовое сканирование: Использование скриптов для обнаружения уязвимостей и получения дополнительной информации.
5. Создание сетевых карт: Создание топологии сети.
6. Обнаружение брандмауэров и IDS: Обход и анализ сетевых фильтров и систем обнаружения вторжений.

Crunch

Crunch — инструмент для генерации словарей паролей, также позволяет создавать кастомные словари с различными параметрами, такими как длина пароля, используемые символы, шаблоны и многое другое.

Базовый синтаксис:

```
crunch <min> <max> [<charset>] [-o <output_file>]
```

- <min>: Минимальная длина пароля.
- <max>: Максимальная длина пароля.
- <charset>: Набор символов (необязательно).
- -o <output_file>: Файл для сохранения словаря.

1. Генерация словарей с заданной длиной паролей: Установка минимальной и максимальной длины паролей.
2. Настройка используемых символов: Определение набора символов для генерации паролей.
3. Поддержка шаблонов: Создание словарей на основе шаблонов, включающих фиксированные части и переменные символы.
4. Вывод в файл или стандартный вывод: Возможность сохранения словарей в файл или вывода непосредственно на экран.

hydra

Hydra — инструмент для проведения брутфорс-атак на различные протоколы. Поддерживает FTP, SSH, HTTP(S), SMB, RDP и другие.

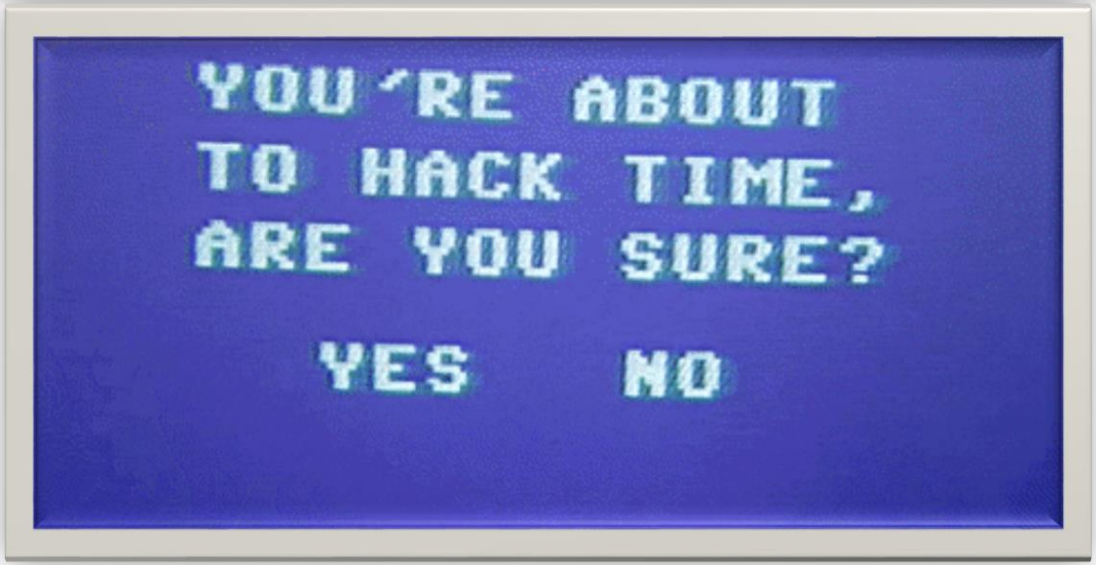
Устанавливается при помощи:
```
sudo apt-get install hydra
```

- Запуск атаки на SSH:
```
hydra -l <username> -P <password_list> ssh://<target_ip>
hydra -l root -P /path/to/passwords.txt ssh://192.168.1.100
```

- Запуск атаки на FTP:
```
hydra -l <username> -P <password_list> ftp://<target_ip>
hydra -l admin -P /path/to/passwords.txt ftp://192.168.1.100
```

-L: Использовать файл со списком логинов.
```
hydra -L /path/to/usernames.txt -P /path/to/passwords.txt ssh://192.168.1.100
```

Практика Kali



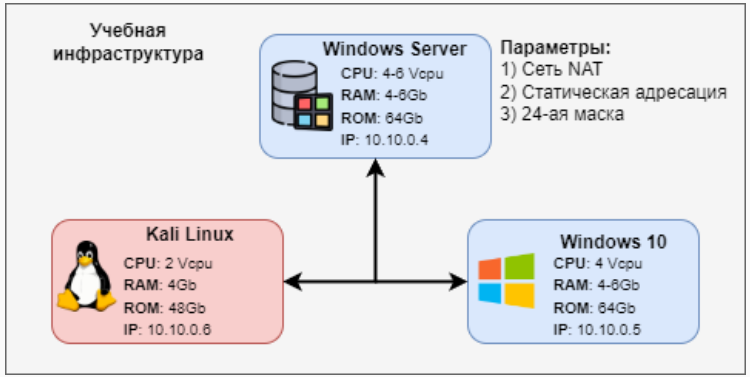
1) Сканируем сеть
2) Пробуем генерацию словариков по нашему шаблону
3) Прослушиваем трафик
4) Пробуем брутфорс по словарику

ДЗ

1) На VM Win10/WinServer установить SSH Server и запустить его.
2) Разрешить подключение по RDP.
3) Провести сканирование подсети с ВМ Kali
4) Провести BruteForce (ssh) пароля от ВМ Win10

*

1) **На FireWall Win10 разрешить подключение по SSH только с VM WinServer.**
2) **Настроить в политиках блокировки УЗ блокировку на 5 мин после 7 не удачных попыток.**



Teach
Me
Skills

Спасибо за внимание!