**Министерство образования и науки Кыргызской республики**

**Кыргызский Государственный Технический**

**Университет**

**им.И.Раззакова**

**Институт информационных технологий**

**Кафедра информатики и вычислительной техники**

**ОТЧЕТ**

**На тему: Лабораторная работа №2**

**Выполнил(а):Асенов И.**

**Группа: ИБ (инж)-1-21**

**Проверил(а): Куручбеков Б.З.**

**Бишкек 2024**

Linux предлагает гораздо более высокий уровень контроля над операционной системой, не говоря уже о том, что она имеет открытый исходный код. Это также делает Linux прозрачным и более . Прежде чем пытаться что-то "взломать", необходимо знать, как это работает, поэтому прозрачность в Linux - это огромный плюс.

Поскольку Linux очень популярен среди сообщества пен-тестеров, большинство используемых

Инструменты и фреймворки для тестирования на проникновение также создаются для Linux.

Обслуживание также сравнительно простое, поскольку программное обеспечение можно легко установить из репозитория. Кроме того, она очень стабильна по сравнению с традиционными операционными системами, такими как Windows.

Основные команды Linux

Подобно тому, как мы ежедневно используем Windows, создавая папки, перемещая файлы, копируя их, мы научимся этим повседневным операциям и в Linux.

Большую часть времени мы будем проводить в терминале, который является интерфейсом командной строки нашей операционной системы. Именно здесь мы вводим команды для выполнения нужных нам операций.

Команда "pwd"

Прежде чем приступить к работе, необходимо узнать, в какой директории мы работаем и где будут созданные нами файлы. Команда pwd - один из способов определить каталог, в котором мы находимся.

Итак, в нашем случае мы обнаружили, что находимся в каталоге /root.

Команда "whoami"

Используя команду whoami, мы видим, каким пользователем мы вошли в систему. Здесь мы вошли в систему под именем

root (что в терминах windows означает администратор)

Cd: Изменение каталогов

Для смены каталогов через терминал используется команда cd. Давайте изменим наш текущий каталог на Desktop.

Ls: Перечисление содержимого

Чтобы просмотреть содержимое каталога, мы используем команду "ls" (очень похожую на команду dir в

windows).

Команда "Помощь"

Почти каждая команда, приложение или утилита в Linux имеет специальный файл справки, в котором описано их использование. Если вы хотите узнать больше о конкретной команде или застряли, справка (- h, -help) станет вашим лучшим другом.

Давайте узнаем больше о фреймворке волатильности.

Человек: Руководство Страницы

Помимо файла справки, большинство команд и приложений имеют страницу руководства, доступ к которой можно получить, набрав man перед командой.

Как показано ниже, он содержит описание и все теги, которые можно использовать с командой ls.

Найти: Поиск по ключевым словам

При поиске определенного ключевого слова одним из самых простых способов является использование функции locate. Введите locate, а затем ключевое слово на терминале, и он выполнит поиск по всей файловой системе в поисках этого слова.

Правда, есть несколько недостатков использования locate: он предоставляет слишком много информации, а база данных, которую он использует, обновляется раз в день, поэтому вы не сможете найти файлы, созданные несколько минут или часов назад.

Давайте выполним поиск по ключевому слову: CTF с

Whereis: Поиск двоичных файлов

Начнем этот раздел с того, что такое двоичные файлы?

Файлы, которые могут быть выполнены, подобно .exe в Windows, называются двоичными файлами. Эти файлы обычно находятся в каталогах /usr/bin или /user/sbin.

Такие утилиты, как ls, cd, cat, ps (о некоторых из них мы расскажем позже), тоже хранятся в этих каталогах.

Для поиска двоичного файла можно использовать команду whereis. Она возвращает путь к двоичному файлу, а также его man-страницу. Находим двоичный файл: git.

Что: Поиск двоичных файлов

Команда which является более конкретной и возвращает только расположение двоичного файла в переменной PATH в Linux. Поиск двоичного файла: git.

Фильтрация с помощью grep

Очень часто при работе с командной строкой требуется выполнить поиск по определенному ключевому слову, и здесь на помощь приходит grep.

Давайте поищем слово: echo в файле simple\_bash.sh, набрав

Думается, наиболее распространенный вариант использования grep - это передача в него вывода с ключевыми словами для фильтрации вывода.

Здесь мы используем grep только для того, чтобы получить IP-адрес нашей машины, а не всю остальную информацию, которая появляется при выполнении команды ifconfig. (Мы еще коснемся обычной команды ifconfig в следующем разделе)

Поиск с помощью команды "find"

Команда find - самая мощная и гибкая из поисковых утилит. Она может задавать различные параметры, включая имя файла (очевидно), дату создания и модификации, владельца, группу, разрешение и размер.

Здесь мы используем теги -type и -name, которые указывают тип искомого файла, а его имя. Обратная косая черта (/) указывает на корневой каталог, в котором мы хотим искать файл.

Если ваш результат выглядит следующим образом:

Это происходит потому, что команда find также ищет в каталогах, к которым у вашей учетной записи нет прав доступа. Поэтому для получения более чистого результата мы используем 2>&1, который отправляет все ошибки с отказом в разрешении в /dev/null (в ничто), а затем с помощью grep отфильтровывает их из вывода)

Команда "cat"

С помощью команды cat мы выводим содержимое файла на терминал. Давайте воспользуемся командой

cat для файла "hacking-articles.txt".

Создание файлов с помощью "touch"

Команда touch позволяет создать новый файл. Простое указание имени файла после команды touch

приведет к созданию этого файла.

Давайте создадим текстовый файл и назовем его "hacking-articles-2.txt".

Mkdir: Создание каталога

Чтобы создать каталог, или сокращенно mkdir, нам нужно просто указать имя каталога после команды

mkdir.

Давайте создадим каталог: ignite

Cp: Копирование файлов

Для копирования файлов мы используем команду cp, которая создает дубликат файла в указанном месте. Давайте скопируем созданный нами ранее текстовый файл в каталог, который мы только что создали выше. Затем мы просмотрим содержимое каталога, чтобы убедиться, что файл был скопирован.

Чтобы скопировать файл, введите cp <файл, который мы хотим скопировать> <место назначения "скопированного" файла>.

Mv: Перемещение/переименование файлов

Мы можем использовать команду перемещения: mv не только для перемещения файлов в указанное место, но и для их переименования. Теперь попробуем переместить файл, который мы скопировали в папку ignite, за ее пределы.

Rm: Удаление файлов

Чтобы удалить файл, достаточно воспользоваться командой rm. Давайте удалим файл "hacking-articles- 2.txt".

Как видно из ls, файл больше не существует.

Rmdir: Удаление каталога

Чтобы удалить каталог, мы используем команду rmdir, которая расшифровывается как "удалить каталог". Давайте удалим каталог "ignite\_screenshots".

(Используйте rm -r для каталогов с содержимым внутри, r означает рекурсивный)

Работа с текстом

В Linux почти все, с чем вам приходится иметь дело, представляет собой файл, чаще всего текстовый; например, файлы конфигурации. Поэтому умение работать с текстом приобретает решающее значение при управлении Linux и его приложениями.

Захват головки файла

При работе с большими файлами мы можем использовать команду head, которая по умолчанию отображает первые 10 строк файла. Давайте посмотрим первые 10 строк файла etter.dns.

(etter.dns - это файл конфигурации инструмента под названием Ettercap, который используется для DNS-спуфинга и ARP-атак)

Захват хвоста файла

Как и команда head, команда tail используется для просмотра последних строк файла. Давайте посмотрим нижние строки файла etter.dns.

Nl: Нумерация строк

Мы можем использовать команду nl для нумерации строк, пока она выводит их в окно терминала. Снова используя команду etter.dns, пронумеруем все строки.

Сед: Найти и заменить текст

Команда sed позволяет искать вхождение слова или текстового шаблона, а затем выполнять с ним определенные действия. Здесь мы будем использовать тег /s для поиска вхождения WWW и /g для глобальной замены на www.

Подробнее: Управление отображением файла

Команда more отображает одну страницу файла за раз и позволяет прокручивать ее вниз с помощью клавиши ENTER. Открытие файла etter.dns с помощью команды more.

Меньше: Отображение и фильтрация файла

Команда less очень похожа на more, но обладает дополнительной функциональностью - возможностью фильтрации ключевых слов. Давайте откроем файл etter.dns с помощью less. Далее мы можем нажать на клавиатуре обратную косую черту (/), а затем ввести ключевое слово, которое мы найти, здесь я искал свой собственный IP-адрес.

Установка и удаление программного обеспечения

Нам часто приходится устанавливать программы, не входящие в дистрибутив Linux, а и вовсе удалять ненужные программы.

В дистрибутивах Linux на базе Debian, таких как Kali Linux (тот, который я использую), менеджером ПО по умолчанию является Advance Packaging Tool или сокращённо apt. Так же, как мы заходим в Appstore, чтобы скачать приложение, в Linux есть репозитории. Мы узнаем, как получить доступ к репозиторию, найти в нем нужный файл и скачать его.

Поиск пакета для установки

Прежде чем загружать какой-либо программный пакет, давайте проверим, доступен ли он в репозитории, где хранится информация о нашей операционной системе Linux. Мы будем использовать инструмент apt.

Введите apt-cache search и затем пакет, который вы хотите , давайте искать Hydra, который является инструментом для взлома логинов. Выделена утилита, о которой мы говорим.

Установка пакетов

Теперь давайте установим нужные нам пакеты. На этот раз мы используем команду apt-get, после которой следует install и название пакета.

Давайте установим git, который в дальнейшем позволит нам извлекать репозитории из Github для установки дополнительных инструментов.

Удаление пакетов

Чтобы удалить любой пакет с машины, просто введите remove после apt-get с именем пакета. Давайте удалим пакет git. (Я рекомендую нажать n, чтобы прервать этот шаг)

Очистка пакетов

Иногда пакет, который мы только что удалили, оставляет после себя остаточные файлы (например, файлы конфигурации). Чтобы полностью все, мы используем опцию purge в apt-get.

Давайте попробуем очистить git (снова можно нажать n, чтобы прервать процесс).

Обновление репозитория

Обновление репозитория является хорошей практикой, поскольку они обычно обновляются новыми программами или новыми версиями существующих программ. Эти обновления необходимо запрашивать, что можно сделать, набрав update после apt-get.

Давайте обновим наш репозиторий. (Примечание: обновление не применяет эти изменения, а только загружает их)

Обновление репозитория

Чтобы применить изменения из команды, которую мы выполнили выше: update, нужно запустить команду apt- get с тегом upgrade. Это позволит установить или, скорее, обновить все новые обновления, которые были загружены в систему.

(Примечание: Обновление может занять много времени, поэтому вы можете некоторое время не использовать свою систему)

Добавление репозиториев в файл sources.list

Серверы, на которых хранится информация о программном обеспечении для конкретных дистрибутивов Linux, называются репозиториями. Мы можем зайти nano в файл /etc/apt/sources.list и добавить сюда репозитории.

(Я не рекомендую добавлять экспериментальные репозитории в список sources.list, потому что они могут загружать проблемное программное обеспечение и приводить к поломкам. )

Выделен репозиторий, который использует мой Kali Linux.

Игра с разрешениями

Прежде чем мы начнем изучать команды Linux для работы с разрешениями, давайте сначала узнаем, что такое разрешение файла/директории в Linux.

Как вы уже знаете, в Linux корневой пользователь является всемогущим, он может делать в системе все, что угодно. Остальные пользователи имеют ограниченные возможности и обычно объединены в группывыполняющие схожие функции.

Например, разные группы для команды разработчиков, команды развертывания и администраторов, чтобы инициировать разные уровни доступа и разрешения.

Все файлы и каталоги в Linux имеют три уровня прав доступа:

r разрешение: Позволяет пользователю открывать и просматривать файл

w разрешение: Это позволяет пользователю просматривать и редактировать файл

x разрешение: Это позволяет пользователю выполнять файл (но не обязательно просматривать или редактировать его).

Предоставление права собственности отдельному пользователю

Мы меняем владельца файла, чтобы новый пользователь мог управлять его разрешениями. Для смены владельца мы используем команду chown.

Давайте изменим владельца файла hacking-artciles.txt с root на Raj

Предоставление права собственности группе

Чтобы передать право собственности на файл группе, мы используем команду chgrp. Чтобы право собственности было только у члена команды ignite, давайте изменим группу на ignite.

Проверка права собственности

Как вы можете видеть на скриншотах выше, мы используем команду ls с тегом l для просмотра разрешений, предоставленных файлам и каталогам.

Представляем,

Тип файла (- обозначает файл, а d - каталог)

Разрешения на доступ к файлу для владельца, группы и пользователей соответственно

Количество ссылок

Владелец файла, пользователь, а затем группа

Размер файла в байтах

Когда файл был создан или изменен в последний раз

Имя файла

Выделены разделы файла, посвященные собственности.

Изменение разрешений

Чтобы изменить права доступа к файлу, мы используем команду chmod. Эта таблица поможет вам решить, какие права вы хотите дать файлу:

0

-

1

-x

2

-w-

3

-wx

4

r-

5

r-x

6

rw-

7

rwx

Мы можем выполнить команду chmod 777 $filename, чтобы дать файлу ВСЕ разрешения, или просто chmod 111 $filename, чтобы дать ему разрешение на выполнение.