

Министерство науки и высшего образования Российской Федерации  
федеральное государственное автономное образовательное учреждение  
высшего образования «Национальный исследовательский университет  
ИТМО»

Факультет инфокоммуникационных технологий

**Основы кибербезопасности**

Практическая работа №4

**Выполнил:**

студент группы К34211

Фисенко Максим Вячеславович

**Проверил:**

преподаватель практики, КТН

Назаров Михаил Сергеевич

Санкт-Петербург

2024

## Оглавление

<b>Введение .....</b>	<b>3</b>
<b>Содержание отчета.....</b>	<b>4</b>
Задание 1. Работа в лаборатории для тестирования и поиска уязвимостей ..	4
Задание 2. Работа с инструментом <i>Nmap</i> .....	6
Опция -A.....	7
Опция -sT .....	7
Опция -sS.....	8
Опция -sN.....	8
Опции -sM, -sA, -sW .....	8
Опция -sO.....	9
Задание 3. Установка Metasploit.....	10
<b>Вывод по работе.....</b>	<b>12</b>

## **Введение**

В данной практической работе было необходимо изучить типовой алгоритм работы с нарушителями информационных систем. В ходе практической работы необходимо было приобрести практические навыки по использованию инструментов сканирования информационных систем, а также научиться идентифицировать узлы в информационной системе.

Для выполнения данной практической работы использовался персональный компьютер на операционной системе *Windows* с подключенной через *WSL* дистрибутивом *Linux Ubuntu*.

## Содержание отчета

### Задание 1. Работа в лаборатории для тестирования и поиска уязвимостей

Первым делом для выполнения данной практической работы необходимо было создать и запустить все необходимые *Docker*-контейнеры, а также проверить их связность. Работа велась в сети *pentest*, созданной в ходе выполнения предыдущей практической работы. В первую очередь был создан контейнер *metasploitable1* (рисунок 1). Аналогичным способом был создан контейнер *metasploitable2*.

```
maksim@pc:~$ sudo docker run --network=pentest -h victim -it --rm --name metasploitable1 tleemcjr/metasploitable2
[sudo] password for maksim:
* Starting web server apache2
ly qualified domain name, using 172.18.0.2 for ServerName
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
Starting distccd
* Starting MySQL database server mysqld [ OK ]
* Checking for corrupt, not cleanly closed and upgrade needing tables.
* Configuring network interfaces... [ OK ]
* Starting portmap daemon... [ OK ]
* Starting Postfix Mail Transport Agent postfix [ OK ]
* Starting PostgreSQL 8.3 database server [ OK ]
* Starting ftp server proftpd [ OK ]
Starting Samba daemons: nmbd smbd.
Starting network management services: snmpd.
* Starting OpenBSD Secure Shell server sshd [ OK ]
snmpd[687]: error finding row index in _ifxTable_container_row_restore
* Starting system log daemon... [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting internet superserver xinetd [ OK ]
* Doing Wacom setup... [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
root@victim:/#
```

Рисунок 1 – Запуска контейнера *metasploitable1*

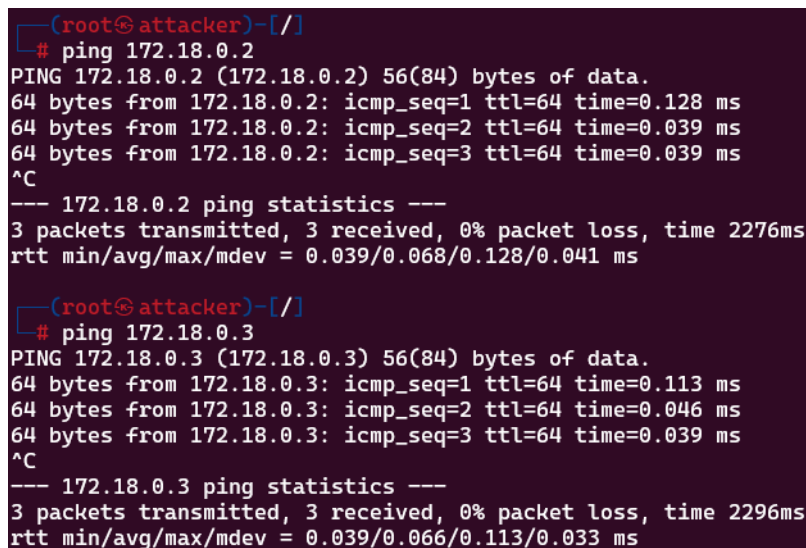
Затем было необходимо создать контейнер, имитирующий нарушителя информационной системы, на образе *kalilinux/kali-rolling*. В этот контейнер была установлена утилита *ping*, необходимая для работы с сетью.

Далее было необходимо узнать *ip*-адреса всех созданных контейнеров, что и было сделано с помощью утилиты *ifconfig*. Так, на рисунке 2 видно, что *ip*-адрес контейнера *metasploitable1* – 172.18.0.2. Адреса контейнеров *metasploitable2* и *kalibox* – 172.18.0.3 и 172.18.0.4 соответственно.

```
root@victim:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:ac:12:00:02
          inet addr:172.18.0.2  Bcast:172.18.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8705 (8.5 KB)  TX bytes:4388 (4.2 KB)
```

Рисунок 2 – *Ip*-адрес контейнера *metasploitable1*

После нахождения *ip*-адресов контейнеров с помощью утилиты *ping* была проверена их связность. Как видно на рисунке 3, контейнер *kalibox* видит оба контейнера, а значит, на данном этапе всё сделано правильно.



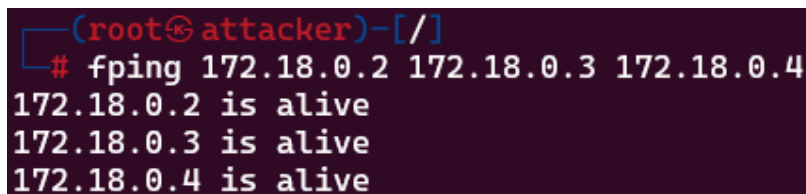
```
(root@attacker)-[/]
# ping 172.18.0.2
PING 172.18.0.2 (172.18.0.2) 56(84) bytes of data.
64 bytes from 172.18.0.2: icmp_seq=1 ttl=64 time=0.128 ms
64 bytes from 172.18.0.2: icmp_seq=2 ttl=64 time=0.039 ms
64 bytes from 172.18.0.2: icmp_seq=3 ttl=64 time=0.039 ms
^C
--- 172.18.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2276ms
rtt min/avg/max/mdev = 0.039/0.068/0.128/0.041 ms

(root@attacker)-[/]
# ping 172.18.0.3
PING 172.18.0.3 (172.18.0.3) 56(84) bytes of data.
64 bytes from 172.18.0.3: icmp_seq=1 ttl=64 time=0.113 ms
64 bytes from 172.18.0.3: icmp_seq=2 ttl=64 time=0.046 ms
64 bytes from 172.18.0.3: icmp_seq=3 ttl=64 time=0.039 ms
^C
--- 172.18.0.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2296ms
rtt min/avg/max/mdev = 0.039/0.066/0.113/0.033 ms
```

Рисунок 3 – Проверка связности контейнеров

Затем в контейнер *kalibox* была установлена утилита *fping*. Данная утилита делает то же самое, что и утилита *ping*, однако отличается от нее тем, что в одной строке можно сразу указать несколько *ip*-адресов, что более удобно при работе с несколькими контейнерами.

Первым делом данной утилиты были просканированы все 3 контейнера и, как и ожидалось, был получен ответ, говорящий о том, что все 3 узла доступны (рисунок 4).



```
(root@attacker)-[/]
# fping 172.18.0.2 172.18.0.3 172.18.0.4
172.18.0.2 is alive
172.18.0.3 is alive
172.18.0.4 is alive
```

Рисунок 4 – Доступность трех узлов

Затем в качестве аргументы утилите была передана целая сеть – 172.18.0.0/16, и данная утилита начала сканировать всю сеть, обращаясь к каждому узлу.

Первые 4 узла, как и ожидалось, были доступны (рисунок 5). Узлы 172.18.0.2–172.18.0.4 – это *ip*-адреса запущенных контейнеров, доступность которых уже была проверена на предыдущем шаге, а *ip*-адрес 172.18.0.1

использует *Docker* для выхода из сети в *pentest* во внешнюю сеть, поэтому он тоже оказался доступным.

```
(root@attacker)-[/]
# fping -g 172.18.0.0/16
172.18.0.1 is alive
172.18.0.2 is alive
172.18.0.3 is alive
172.18.0.4 is alive
```

Рисунок 5 – Доступные узлы в сети

Все же остальные *ip*-адреса в подсети оказались недоступны, ведь кроме трех контейнеров больше в данной сети запущено ничего не было (рисунок 6). Как и ожидалось, утилита не могла получить от них ответ. Так как узлов в сети было достаточно много, в какой-то момент работу утилиты пришлось прервать.

```
ICMP Host Unreachable from 172.18.0.4 for ICMP Echo sent to 172.18.6.85
ICMP Host Unreachable from 172.18.0.4 for ICMP Echo sent to 172.18.6.85
ICMP Host Unreachable from 172.18.0.4 for ICMP Echo sent to 172.18.6.85
ICMP Host Unreachable from 172.18.0.4 for ICMP Echo sent to 172.18.6.85
ICMP Host Unreachable from 172.18.0.4 for ICMP Echo sent to 172.18.6.93
ICMP Host Unreachable from 172.18.0.4 for ICMP Echo sent to 172.18.6.93
ICMP Host Unreachable from 172.18.0.4 for ICMP Echo sent to 172.18.6.93
ICMP Host Unreachable from 172.18.0.4 for ICMP Echo sent to 172.18.6.93
ICMP Host Unreachable from 172.18.0.4 for ICMP Echo sent to 172.18.6.92
ICMP Host Unreachable from 172.18.0.4 for ICMP Echo sent to 172.18.6.92
ICMP Host Unreachable from 172.18.0.4 for ICMP Echo sent to 172.18.6.92
```

Рисунок 6 – Недоступность остальных узлов

## Задание 2. Работа с инструментом *Nmap*

Для выполнения данного задания первым делом в контейнер *kalibox* была установлена утилита *Nmap*. *Nmap* – это инструмент, предназначенный для сканирования сетей. После установки утилиты необходимо было, воспользовавшись ей, просканировать узел информационной сети. В качестве узла был взят *metasploitable2* с *ip*-адресом 172.18.0.3. Данная утилита обладает следующим синтаксисом: *nmap* <опция сканирования> <цель сканирования>. Ниже приведены результаты сканирования узла 172.18.0.3 с различными опциями.

## Опция -A

Данная опция включает полное сканирование. Утилита выводит в консоль всю полученную информацию об узле, включая операционную систему и детальную информацию о сервисах, работающих на портах (рисунок 7).

```
2121/tcp open  ftp          ProFTPD 1.3.1
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: SupportsTransactions, Speaks41ProtocolNew, SupportsCompression, SwitchToSSLAfterHandshake
| Status: Autocommit
|_ Salt: }(Ht2:k.@711B:9MZ]E#
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-12-09T15:23:31+00:00; 0s from scanner time.
5900/tcp open  vnc          VNC (protocol 3.3)
vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
```

Рисунок 7 – Работа утилиты *nmap* с опцией -A

## Опция -sT

Работая с данной опцией, утилита проверяет порты узла, устанавливая *TCP*-соединение и используя трехстороннее рукопожатие. В консоль выводится список открытых, закрытых и фильтрованных портов, а также идентифицируются все службы, работающие на этих портах (рисунок 8).

```
(root@attacker)~[/]
# nmap -sT 172.18.0.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 15:26 UTC
Nmap scan report for metasploitable2.pentest (172.18.0.3)
Host is up (0.000057s latency).
Not shown: 979 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 02:42:AC:12:00:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Рисунок 8 – Работа утилиты *nmap* с опцией -sT

## Опция -sS

При данной опции выполняется *SYN*-сканирование, которое отличается от *TCP*-сканирования тем, что оно не использует трехстороннее рукопожатие, вследствие чего оно работает быстрее и является менее заметным. Как видно на рисунке 9, вывод совпадает с тем, что было при опции -sT.

```
(root@attacker)-[/]
# nmap -sS 172.18.0.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 15:27 UTC
Nmap scan report for metasploitable2.pentest (172.18.0.3)
Host is up (0.0000030s latency).
Not shown: 979 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 02:42:AC:12:00:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

Рисунок 9 – Работа утилиты *nmap* с опцией -sS

## Опция -sN

При данной опции выполняется *TCP NULL*-сканирование, которое отличается от простого *TCP*-сканирования тем, что у отправленных *TCP*-пакетов нет установочных флагов. Результат такого сканирования был аналогичен результатам сканирований с опциями -sT и -sS, представленных выше.

## Опции -sM, -sA, -sW

Используя данные опции, утилита принимает *TCP*-сканирование Маймона, *TCP ACK*-сканирование и *TCP Window*-сканирование соответственно. Однако при использовании данных опции в лабораторной работе был получен одинаковый результат: в консоль выводилось сообщение о том, что ни один порт просканировать не получилось (рисунок 10).



Вероятнее всего, это связано с тем, что фаерволл *kalibox* блокирует такие типы подключений.

```
(root@attacker)~[/]
# nmap -sM 172.18.0.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 15:29 UTC
Nmap scan report for metasploitable2.pentest (172.18.0.3)
Host is up (0.0000020s latency).
All 1000 scanned ports on metasploitable2.pentest (172.18.0.3) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 02:42:AC:12:00:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds

(root@attacker)~[/]
# nmap -sA 172.18.0.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 15:29 UTC
Nmap scan report for metasploitable2.pentest (172.18.0.3)
Host is up (0.0000030s latency).
All 1000 scanned ports on metasploitable2.pentest (172.18.0.3) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 02:42:AC:12:00:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

(root@attacker)~[/]
# nmap -sW 172.18.0.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 15:30 UTC
Nmap scan report for metasploitable2.pentest (172.18.0.3)
Host is up (0.0000030s latency).
All 1000 scanned ports on metasploitable2.pentest (172.18.0.3) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 02:42:AC:12:00:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Рисунок 10 – Работа утилиты *nmap* с опциями *-sM*, *-sA*, *-sW*

## Опция *-sO*

Данная опция позволяет узнать характеристики операционной системы, установленной на устройстве (рисунок 11).

```
(root@attacker)~[/]
# nmap -O 172.18.0.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 15:33 UTC
Nmap scan report for metasploitable2.pentest (172.18.0.3)
Host is up (0.000032s latency).
Not shown: 979 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 02:42:AC:12:00:03 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds
```

Рисунок 11 – Работа утилиты *nmap* с опцией *-sO*

### Задание 3. Установка Metasploit

Для выполнения данного задания первым делом с помощью команды из инструкции к лабораторной работе был установлен и запущен контейнер на основе образа *Metasploit* (рисунок 12).

```
..\\.../

/ it looks like you're trying to run a \
\ module /

\

[

@ @

| |

| |

| |

| |

]

+ -- ==[ metasploit v6.1.41-dev-9737d030a7 ]
+ -- ==[ 2216 exploits - 1171 auxiliary - 397 post ]
+ -- ==[ 616 payloads - 45 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: Use the resource command to run
commands from a file

msf6 >
```

Рисунок 12 – Установленный *Metasploit*

Далее в этом контейнере была запущена утилита *db\_nmap*. Можно сказать, что данная утилита является той же утилитой *nmap*, которая была использована в предыдущем задании. В данном случае утилита была запущена без явного указания на тип сканирования, в результате чего был получен вывод в консоль, аналогичный выводу в предыдущем задании (рисунок 13).

```
msf6 > db_nmap 172.18.0.3
* Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2024-12-09 15:41 UTC
* Nmap: Nmap scan report for metasploitable2.pentest (172.18.0.3)
* Nmap: Host is up (0.0000050s latency).
* Nmap: Not shown: 979 closed ports
* Nmap: PORT      STATE SERVICE
* Nmap: 21/tcp    open  ftp
* Nmap: 22/tcp    open  ssh
* Nmap: 23/tcp    open  telnet
* Nmap: 25/tcp    open  smtp
* Nmap: 80/tcp    open  http
* Nmap: 111/tcp   open  rpcbind
* Nmap: 139/tcp   open  netbios-ssn
* Nmap: 445/tcp   open  microsoft-ds
* Nmap: 512/tcp   open  exec
* Nmap: 513/tcp   open  login
* Nmap: 514/tcp   open  shell
* Nmap: 1099/tcp  open  rmiregistry
* Nmap: 1524/tcp  open  ingreslock
* Nmap: 2121/tcp  open  ccproxy-ftp
* Nmap: 3306/tcp  open  mysql
* Nmap: 5432/tcp  open  postgresql
* Nmap: 5900/tcp  open  vnc
* Nmap: 6000/tcp  open  X11
* Nmap: 6667/tcp  open  irc
* Nmap: 8009/tcp  open  ajp13
* Nmap: 8180/tcp  open  unknown
* Nmap: MAC address: 02:42:AC:12:00:03 (Unknown)
* Nmap: Nmap done: 1 IP address (1 host up) scanned in 1.77 seconds
```

Рисунок 13 – Работы утилиты *db\_nmap*

Затем с помощью команды `search http`, которая используется для поиска модулей, связанных с `http` и, таким образом, позволяет найти эксплойты, связанные с `http` (рисунок 14).

2762	auxiliary/dos/http/marked_redos		normal	No	marked npm module "heading" ReDoS
2763	exploit/unix/webapp/mybb_backdoor	2011-10-06	excellent	Yes	myBB 1.6.4 Backdoor Arbitrary Command Execution
2764	exploit/linux/http/op5_config_exec	2016-04-08	excellent	Yes	op5 v7.1.9 Configuration Command Execution
2765	exploit/unix/webapp/opensis_chain_exec	2020-06-30	excellent	Yes	openSIS Unauthenticated PHP Code Execution
2766	exploit/multi/http/oscommerce_installer_unauth_code_exec	2018-04-30	excellent	Yes	osCommerce Installer Unauthenticated Code Execution
2767	exploit/unix/http/pfsense_diag_routes_webshell	2022-02-23	excellent	Yes	pfSense Diag Routes Web Shell Upload
2768	exploit/unix/http/pfsense_graph_injection_exec	2016-04-18	excellent	No	pfSense authenticated graph status RCE
2769	exploit/unix/http/pfsense_group_member_exec	2017-11-06	excellent	Yes	pfSense authenticated group member RCE
2770	exploit/linux/http/php_imap_open_rce	2018-11-01	good	Yes	php imap_open Remote Code Execution
2771	exploit/unix/webapp/phpcollab_upload_exec	2017-09-29	excellent	Yes	phpCollab 2.5.1 Unauthenticated File Upload
2772	exploit/multi/http/phpfilemanager_rce	2015-08-28	excellent	Yes	phpFileManager 0.9.8 Remote Code Execution
2773	exploit/multi/http/phpldapadmin_query_engine	2011-10-24	excellent	Yes	phpLDAPadmin query_engine Remote PHP Code Execution
2774	exploit/multi/http/phpmyadmin_3522_backdoor	2012-09-25	normal	No	phpMyAdmin 3.5.2.2 server_sync.php Backdoor
2775	exploit/multi/http/phpmyadmin_lfi_rce	2018-06-19	good	Yes	phpMyAdmin Authenticated Remote Code Execution
2776	exploit/multi/http/phpmyadmin_null_termination_exec	2016-06-23	excellent	Yes	phpMyAdmin Authenticated Remote Code Execution
2777	exploit/multi/http/phpmyadmin_preg_replace	2013-04-25	excellent	Yes	phpMyAdmin Authenticated Remote Code Execution
2778	exploit/multi/http/phpscheduleit_start_date	2008-10-01	excellent	Yes	phpScheduleIt PHP reserve.php start_date Remote Code Execution
2779	exploit/linux/local/ptrace_sudo_token_priv_esc	2019-03-24	excellent	Yes	ptrace Sudo Token Privilege Escalation
2780	exploit/multi/http/qdpm_upload_exec	2012-06-14	excellent	Yes	qdPM v7 Arbitrary PHP File Upload Vulnerability
2781	exploit/linux/http/rconfig_vendors_auth_file_upload_rce	2021-03-17	excellent	Yes	rConfig Vendors Auth File Upload RCE
2782	exploit/unix/webapp/rconfig_install_cmd_exec	2019-10-28	excellent	Yes	rConfig install Command Execution
2783	auxiliary/dos/syslog/rsyslog_long_tag	2011-09-01	normal	No	rsyslog Long Tag Off-By-Two DoS
2784	exploit/unix/http/tftp_savefile	2014-10-28	excellent	No	tftp "savefile" Arbitrary Command Execution
2785	auxiliary/dos/http/ua_parser_js_redos		normal	No	ua-parser-js npm module ReDoS
2786	exploit/multi/http/v0pcr3w_exec	2013-03-23	great	Yes	v0pcr3w Web Shell Remote Code Execution

Рисунок 14 – Поиск эксплойтов с `http`

После этого один из таких эксплойтов был выбран с помощью команды `use`. Затем для данного типа атаки был с помощью `set RHOSTS` был указан `ip-адрес` контейнера, атаку на который планировалось провести (рисунок 15).

```
msf6 > use exploit/unix/http/xdebug_unauth_exec
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/http/xdebug_unauth_exec) > set RHOSTS 172.18.0.3
RHOSTS => 172.18.0.3
msf6 exploit(unix/http/xdebug_unauth_exec) > show options

Module options (exploit/unix/http/xdebug_unauth_exec):



| Name    | Current Setting | Required | Description                                                                                  |
|---------|-----------------|----------|----------------------------------------------------------------------------------------------|
| PATH    | /index.php      | yes      | Path to target webapp                                                                        |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                 |
| RHOSTS  | 172.18.0.3      | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT   | 80              | yes      | The target port (TCP)                                                                        |
| SRVHOST | 0.0.0.0         | yes      | Callback host for accepting connections                                                      |
| SRVPORT | 9000            | yes      | Port to listen for the debugger                                                              |
| SSL     | false           | no       | Negotiate SSL/TLS for outgoing connections                                                   |
| VHOST   |                 | no       | HTTP server virtual host                                                                     |



Payload options (php/meterpreter/reverse_tcp):



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



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

Рисунок 15 – Настройка атаки

Наконец, была введена команда `run`, которая запускает атаку на выбранный хост, однако сама атака выполнена не было, так как не удалось подтвердить параметр `LHOST` выбранной атаки (рисунок 16), в результате чего эксплойт использован не был.

```
msf6 exploit(unix/http/xdebug_unauth_exec) > run

[-] 172.18.0.3:80 - Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
```

Рисунок 16 – Попытка запуска атаки

### **Вывод по работе**

В результате выполнения данной практической работы был изучен типовой алгоритм работы с нарушителями информационных систем, а также были приобретены практические навыки по использованию инструментов сканирования информационных систем. В ходе выполнения практической работы была проведена работа в лаборатории для поиска уязвимостей, затем была проведена работа с утилитой *Nmap* и, наконец, была произведена установка *Metasploit*.