

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

Швалов Даниил Андреевич

Проверил:

преподаватель практики, КТН

Назаров Михаил Сергеевич

Санкт-Петербург

2024

Оглавление

Введение.....	3
Содержание отчета.....	4
1. Работа в лаборатории для тестирования и поиска уязвимостей.....	4
2. Работа с инструментом NMAP.....	8
3. Установка и работа с metasploit.....	14
Вывод по работе.....	18

Введение

Цель работы. Изучить типовой алгоритм работы с нарушителя информационных систем. Приобрести практические навыки по использованию инструментов сканирования ИС. Научиться идентифицировать узлы в информационной системы.

Содержание отчета

1. Работа в лаборатории для тестирования и поиска уязвимостей

Для настройки лаборатории для тестирования и поиска уязвимостей были запущены контейнеры «metasploitable1» и «metasploitable2» на основе образа «tleemcjr/metasploitable2». Также был запущен контейнер «kalibox» на основе образа «kalilinux/kali-rolling». Этот процесс показан на рисунках 1-3.

```
~ > docker run --network=pentest -h victim -it --rm --name metasploitable1 tleemcjr/metasploitable2
WARNING: The requested image's platform (linux/amd64) does not match the detected host platform (linux/arm64/v8) and no specific platform was requested
* Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 172.18.0.2 for ServerName

* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
Starting distccd [ OK ]
* 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.
snmpd[1896]: error finding row index in _ifXTable_container_row_restore

* Starting OpenBSD Secure Shell server sshd [ OK ]
* Starting system log daemon... [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting internet superserver xinetd [ OK ]
* Doing Wacom setup...
cat: */id: No such file or directory [ OK ]

* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

root@victim:/#
```

Рисунок 1 — Запуск контейнера «metasploitable1»

```
~ > docker run --network=pentest -h victim2 -it --rm --name metasploitable2 tleemcjr/metasploitable2
WARNING: The requested image's platform (linux/amd64) does not match the detected host platform (linux/arm64/v8) and no specific platform was requested
* Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 172.18.0.3 for ServerName

* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
Starting distccd [ OK ]
* 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.
snmpd[1896]: error finding row index in _ifXTable_container_row_restore

* Starting OpenBSD Secure Shell server sshd [ OK ]
* Starting system log daemon... [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting internet superserver xinetd [ OK ]
* Doing Wacom setup...
cat: */id: No such file or directory [ OK ]

* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

root@victim2:/#
```

Рисунок 2 — Запуск контейнера «metasploitable2»

```
~ > docker run --network=pentest -h attacker -it --rm --name kalibox kalilinux/kali-rolling
(root@attacker)-[/]
#
```

Рисунок 3 — Запуск контейнера «kalibox»

После этого в контейнер «kalibox» была установлена утилита «ping». С ее помощью была проверена сетевая доступность контейнеров «metasploitable1» и «metasploitable2», имеющих адреса 172.18.0.2 и 172.18.0.3 соответственно. После отправки ICMP-запросов были получены ICMP-ответы. Таким образом, было установлено, что контейнер «kalibox» может взаимодействовать с контейнерами «metasploitable1» и «metasploitable2» по сети. Это видно на рисунке 4.

```
(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=0.429 ms
64 bytes from 172.18.0.2: icmp_seq=2 ttl=64 time=0.127 ms
64 bytes from 172.18.0.2: icmp_seq=3 ttl=64 time=0.250 ms
^C
--- 172.18.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2038ms
rtt min/avg/max/mdev = 0.127/0.268/0.429/0.123 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=0.512 ms
64 bytes from 172.18.0.3: icmp_seq=2 ttl=64 time=0.254 ms
64 bytes from 172.18.0.3: icmp_seq=3 ttl=64 time=0.096 ms
^C
--- 172.18.0.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2069ms
rtt min/avg/max/mdev = 0.096/0.287/0.512/0.171 ms
```

Рисунок 4 — Проверка доступности контейнеров «metasploitable1» и «metasploitable2» из контейнера «kalibox» с помощью утилиты «ping»

Затем была установлена утилита «fping», которая позволяет отправлять ICMP-запросы сразу по нескольким адресам. С ее помощью была повторно проверена доступность адресов 172.18.0.2 и 172.18.0.3. В

добавок к этому, был указан IP-адрес, не принадлежащий ни к одному из узлов. После запуска утилиты «fping» было выведено сообщение, что адреса 172.18.0.2 и 172.18.0.3 доступны, а адрес 172.18.0.5 — нет. Этот процесс показан на рисунках 5-6.

```
(root@attacker)-[/]
# apt install fping
Installing:
  fping

Installing dependencies:
  netbase

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 12
  Download size: 52.5 kB
  Space needed: 127 kB / 44.3 GB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main arm64 netbase all 6.4 [12.8 kB]
Get:2 http://mirror.cspacehostings.com/kali kali-rolling/main arm64 fping arm64 5.1-1 [39.7 kB]
Fetched 52.5 kB in 1s (98.5 kB/s)
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd/Dialog.pm line 79, <STDIN> line 2.)
debconf: falling back to frontend: Readline
debconf: unable to initialize frontend: Readline
debconf: (Can't locate Term/ReadLine.pm in @INC (you may need to install the Term::ReadLine module) (@INC entries checked: /etc/perl /usr/local/lib/aarch64-linux-gnu/perl/5.38.2 /usr/local/share/perl/5.38.2 /usr/lib/aarch64-linux-gnu/perl5/5.38 /usr/share/perl5 /usr/lib/aarch64-linux-gnu/perl-base /usr/lib/aarch64-linux-gnu/perl/5.38 /usr/share/perl/5.38 /usr/local/lib/site_perl) at /usr/share/perl5/Debconf/FrontEnd/Readline.pm line 8, <STDIN> line 2.)
debconf: falling back to frontend: Teletype
Selecting previously unselected package netbase.
(Reading database ... 5400 files and directories currently installed.)
Preparing to unpack .../archives/netbase_6.4_all.deb ...
Unpacking netbase (6.4) ...
Selecting previously unselected package fping.
Preparing to unpack .../archives/fping_5.1-1_arm64.deb ...
Unpacking fping (5.1-1) ...
Setting up netbase (6.4) ...
Setting up fping (5.1-1) ...
```

Рисунок 5 — Установка утилиты «fping»

```
(root@attacker)-[/]
# fping 172.18.0.2 172.18.0.3 172.18.0.6
172.18.0.2 is alive
172.18.0.3 is alive
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.6
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.6
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.6
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.6
172.18.0.6 is unreachable
```

Рисунок 6 — Проверка доступности узлов с помощью утилиты «fping»

После этого была протестирована работы утилиты «fping» с опцией «-g», которая позволяет протестировать доступность списка адресов заданной подсети. В данном случае была указана подсеть 172.18.0.0/16.

После запуска утилиты «fping» началась проверка доступности всех хостов из данной подсети. Через некоторое время утилита «fping» вывела информацию о недоступных узлах. Это показано на рисунках 7-8.

```
(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
172.18.0.5 is alive
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.10
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.10
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.10
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.10
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.9
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.9
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.9
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.9
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.8
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.8
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.8
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.0.8
```

Рисунок 7 — Проверка доступности всех узлов в подсети 172.18.0.0/16 с помощью утилиты «fping»

```
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.255.254
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.255.254
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.255.254
ICMP Host Unreachable from 172.18.0.5 for ICMP Echo sent to 172.18.255.254
172.18.0.6 is unreachable
172.18.0.7 is unreachable
172.18.0.8 is unreachable
172.18.0.9 is unreachable
172.18.0.10 is unreachable
172.18.0.11 is unreachable
172.18.0.12 is unreachable
172.18.0.13 is unreachable
172.18.0.14 is unreachable
172.18.0.15 is unreachable
172.18.0.16 is unreachable
172.18.0.17 is unreachable
```

Рисунок 8 — Информация о недоступных узлах

2. Работа с инструментом NMAP

При работе с утилитой «nmap» были изучены и протестированы различные опции. Первой из них была опция «-A», которая позволяет просканировать операционную систему, ее версию, наличие различных скриптов, а также определить маршрут так, как это делает утилита «traceroute». Результат запуска утилиты показан на рисунке 9.

```
(root@attacker)-[/]
# nmap -A 172.18.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 18:34 UTC
Nmap scan report for metasploitable1.pentest (172.18.0.2)
Host is up (0.00028s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 172.18.0.5
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ssl-date: 2024-10-19T18:38:14+00:00; 0s from scanner time.
```

Рисунок 9 — Запуск утилиты «nmap» с опцией «-A»

После этого утилита «nmap» была запущена с опцией «-sT», которая

позволяет провести TCP-сканирование подключения с помощью трехстороннего рукопожатия. После запуска сканирования на экран были выведены все открытые TCP-порты. Результат запуска утилиты показан на рисунке 10.

```
(root@attacker)-[/]
# nmap -sT 172.18.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 18:39 UTC
Nmap scan report for metasploitable1.pentest (172.18.0.2)
Host is up (0.00016s latency).
Not shown: 980 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
8180/tcp  filtered  unknown
MAC Address: 02:42:AC:12:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
```

Рисунок 10 — Запуск утилиты «nmap» с опцией «-sT»

Затем утилита «nmap» была запущена с опцией «-sS», которая позволяет провести SYN-сканирование. После запуска сканирования на экран были выведены все открытые TCP-порты. Результат запуска утилиты показан на рисунке 11.

```
(root@attacker)-[/]
# nmap -sS 172.18.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 18:40 UTC
Nmap scan report for metasploitable1.pentest (172.18.0.2)
Host is up (0.0000080s latency).
Not shown: 980 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
8180/tcp  filtered  unknown
MAC Address: 02:42:AC:12:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
```

Рисунок 11 — Запуск утилиты «nmap» с опцией «-sS»

После этого утилита «nmap» была запущена с опцией «-sN», которая позволяет провести TCP NULL-сканирование. После запуска сканирования на экран были выведены все открытые и фильтруемые TCP-порты. Результат запуска утилиты показан на рисунке 12.

```

(root@attacker)-[/]
# nmap -sN 172.18.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 18:41 UTC
Nmap scan report for metasploitable1.pentest (172.18.0.2)
Host is up (0.0000070s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell
1099/tcp  open|filtered rmiregistry
1524/tcp  open|filtered ingreslock
2121/tcp  open|filtered ccproxy-ftp
3306/tcp  open|filtered mysql
5432/tcp  open|filtered postgresql
5900/tcp  open|filtered vnc
6000/tcp  open|filtered X11
6667/tcp  open|filtered irc
8180/tcp  open|filtered unknown
MAC Address: 02:42:AC:12:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds

```

Рисунок 12 — Запуск утилиты «nmap» с опцией «-sN»

Затем утилита «nmap» была запущена с опцией «-sM», которая позволяет провести ТСР-сканирование Маймона. После запуска сканирования на экран было выведено сообщение, что все сканируемые порты находятся в состоянии игнорирования. Результат запуска утилиты показан на рисунке 13.

```

(root@attacker)-[/]
# nmap -sM 172.18.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 18:42 UTC
Nmap scan report for metasploitable1.pentest (172.18.0.2)
Host is up (0.0000050s latency).
All 1000 scanned ports on metasploitable1.pentest (172.18.0.2) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 02:42:AC:12:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

```

Рисунок 13 — Запуск утилиты «nmap» с опцией «-sM»

После этого утилита «nmap» была запущена с опцией «-sA», которая позволяет провести TCP ACK-сканирование. После запуска сканирования на экран было выведено сообщение, что все сканируемые порты находятся в состоянии игнорирования. Результат запуска утилиты показан на рисунке 14.

```
(root@attacker)-[/]
# nmap -sA 172.18.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 18:42 UTC
Nmap scan report for metasploitable1.pentest (172.18.0.2)
Host is up (0.0000080s latency).
All 1000 scanned ports on metasploitable1.pentest (172.18.0.2) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 02:42:AC:12:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Рисунок 14 — Запуск утилиты «nmap» с опцией «-sA»

Затем утилита «nmap» была запущена с опцией «-sW», которая позволяет провести TCP Window-сканирование. После запуска сканирования на экран было выведено сообщение, что все сканируемые порты находятся в состоянии игнорирования. Результат запуска утилиты показан на рисунке 15.

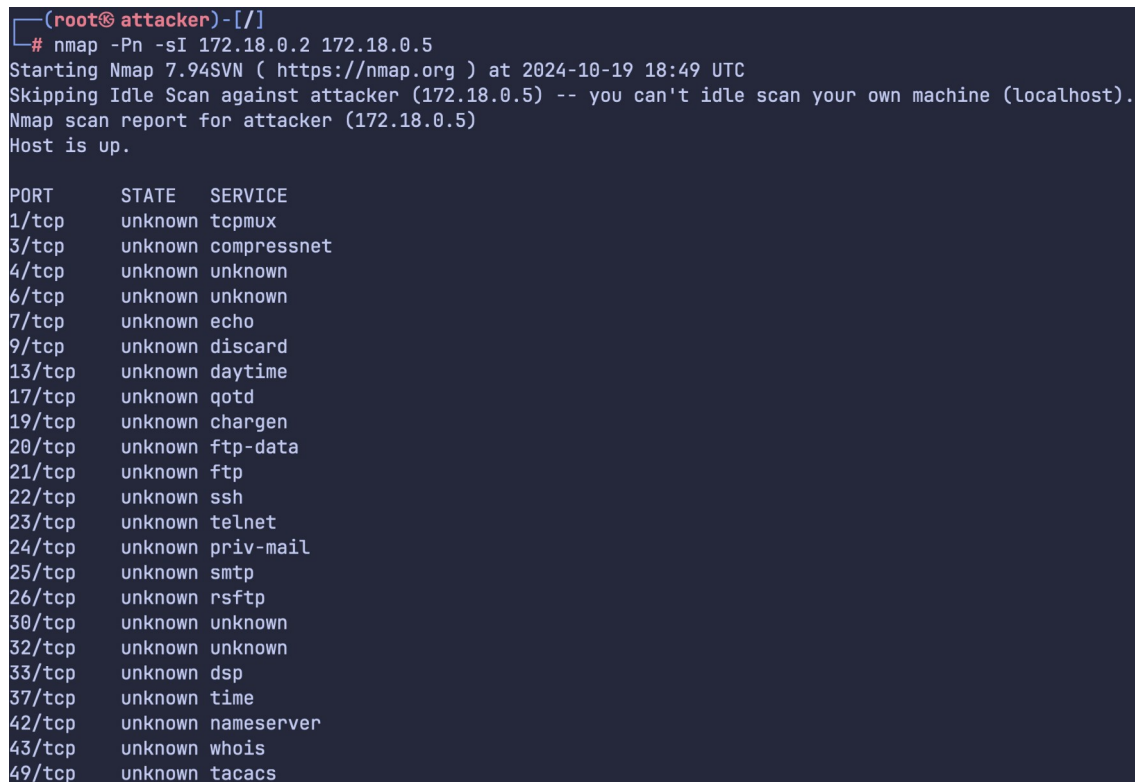
```
(root@attacker)-[/]
# nmap -sW 172.18.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 18:42 UTC
Nmap scan report for metasploitable1.pentest (172.18.0.2)
Host is up (0.0000070s latency).
All 1000 scanned ports on metasploitable1.pentest (172.18.0.2) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 02:42:AC:12:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Рисунок 15 — Запуск утилиты «nmap» с опцией «-sW»

После этого утилита «nmap» была запущена с опцией «-sI», которая позволяет провести TCP Idle-сканирование. В качестве зомби-хоста был

выбран IP-адрес атакующего. После запуска сканирования на экран было выведено сообщение, что сканируемые порты находятся в состоянии «unknown». Результат запуска утилиты показан на рисунке 16.



```
(root@attacker)-[/]
# nmap -Pn -sI 172.18.0.2 172.18.0.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 18:49 UTC
Skipping Idle Scan against attacker (172.18.0.5) -- you can't idle scan your own machine (localhost).
Nmap scan report for attacker (172.18.0.5)
Host is up.

PORT      STATE SERVICE
1/tcp     unknown tcpmux
3/tcp     unknown compressnet
4/tcp     unknown unknown
6/tcp     unknown unknown
7/tcp     unknown echo
9/tcp     unknown discard
13/tcp    unknown daytime
17/tcp    unknown qotd
19/tcp    unknown chargen
20/tcp    unknown ftp-data
21/tcp    unknown ftp
22/tcp    unknown ssh
23/tcp    unknown telnet
24/tcp    unknown priv-mail
25/tcp    unknown smtp
26/tcp    unknown rsftp
30/tcp    unknown unknown
32/tcp    unknown unknown
33/tcp    unknown dsp
37/tcp    unknown time
42/tcp    unknown nameserver
43/tcp    unknown whois
49/tcp    unknown tacacs
```

Рисунок 16 — Запуск утилиты «nmap» с опцией «-sI»

Затем утилита «nmap» была запущена с опцией «-O», которая позволяет просканировать операционную систему. После запуска сканирования на экран была выведена информация о стандартных портах, а также об операционной системе. Результат запуска утилиты показан на рисунке 17.

```

(root@attacker)-[/]
# nmap -O 172.18.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 18:55 UTC
Nmap scan report for metasploitable1.pentest (172.18.0.2)
Host is up (0.00025s latency).
Not shown: 980 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
8180/tcp  filtered unknown
MAC Address: 02:42:AC:12:00:02 (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 2.69 seconds

```

Рисунок 17 — Запуск утилиты «nmap» с опцией «-O»

3. Установка и работа с metasploit

Для дополнительного сканирования уязвимостей была установлена утилита «metasploit» с помощью Docker. Эта утилита предоставляет возможности для создания и отладки эксплойтов.

После загрузки образа «strm/metasploit» и запуска контейнера «metasploit» на его основе на экран было выведено приветственное сообщение. Данное сообщение показано на рисунке 18.

```
      .:ok000kdc'          'cdk000ko:.
      .x0000000000000c      c000000000000x.
      :00000000000000k,      ,k00000000000000:
      '000000000k00000: :000000000000000000'
      o00000000.MMMM.o0000o0000L.MMMM,00000000o
      d00000000.MMMMMM.c00000c.MMMMMM,00000000x
      L00000000.MMMMMMMMM;d;MMMMMMMMM,00000000L
      .00000000.MMM.;MMMMMMMMMMMM;MMM,00000000.
      c0000000.MMM.OOc.MMMMM'o00.MMM,0000000c
      o000000.MMM.0000.MMM:0000.MMM,000000o
      L00000.MMM.0000.MMM:0000.MMM,00000L
      ;0000'MMM.0000.MMM:0000.MMM;0000;
      .d00o'WM.0000occcx0000.MX'x00d.
      ,k0L'M.0000000000000.M'd0k,
      :kk;.0000000000000.;0k:
      ;k000000000000000k:
      ,x000000000000x,
      .L00000000L.
      ,d0d,
      .

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

Metasploit tip: View all productivity tips with the
tips command

msf6 > 
```

Рисунок 18 — Приветственное сообщение при запуске контейнера «metasploit»

После этого была запущена утилита «db_nmap», позволяющая просканировать TCP-порты так, как это делает утилита «nmap». В качестве сканируемого адреса был указан адрес контейнера «metasploitable1», т. е. адрес 172.18.0.2. Результат запуска утилиты «db_nmap» показан на рисунке 19.

```

msf6 > db_nmap 172.18.0.2
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-19 19:37 UTC
[*] Nmap: Nmap scan report for metasploitable1.pentest (172.18.0.2)
[*] Nmap: Host is up (0.00024s latency).
[*] Nmap: Not shown: 980 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: 8180/tcp  filtered unknown
[*] Nmap: MAC Address: 02:42:AC:12:00:02 (Unknown)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 2.93 seconds

```

Рисунок 19 — Запуск утилиты «db_nmap» в контейнере «metasploit»

Затем была протестирована утилита «exploit/unix/http/xdebug_unauth_exec». С помощью команды «options» были выведены все доступные опции утилиты. С помощью команды «set RHOST» был изменен хост цели. После изменения хоста цели в выводе «options» в поле «RHOST» начал отображаться ранее установленный хост. Это видно на рисунках 20-21.


```
msf6 > use exploit/unix/http/xdebug_unauth_exec
[*] Using configured payload php/meterpreter/reverse_tcp
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              no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes             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              no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

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

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

Рисунок 20 — Опции утилиты «exploit/unix/http/xdebug_unauth_exec»

```
msf6 exploit(unix/http/xdebug_unauth_exec) > set RHOSTS 172.18.0.2
RHOSTS => 172.18.0.2
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              no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     172.18.0.2      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              no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

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

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

Рисунок 21 — Опции утилиты «exploit/unix/http/xdebug_unauth_exec»
после настройки RHOST

Вывод по работе

В результате выполнения данной практической работы был изучен типовой алгоритм работы с нарушителями информационных систем, приобретены практические навыки по использованию инструментов сканирования ИС, получены навыки идентификации узлов в информационной системе.