## **Задание 1**

Скачайте и установите виртуальную машину Metasploitable: <https://sourceforge.net/projects/metasploitable/>.

Это типовая ОС для экспериментов в области информационной безопасности, с которой следует начать при анализе уязвимостей.

Просканируйте эту виртуальную машину, используя nmap.

Попробуйте найти уязвимости, которым подвержена эта виртуальная машина.

Сами уязвимости можно поискать на сайте <https://www.exploit-db.com/>.

Для этого нужно в поиске ввести название сетевой службы, обнаруженной на атакуемой машине, и выбрать подходящие по версии уязвимости.

Ответьте на следующие вопросы:

* Какие сетевые службы в ней разрешены?
* Какие уязвимости были вами обнаружены? (список со ссылками: достаточно трёх уязвимостей)

*Приведите ответ в свободной форме.*

## **Решение 1**

Все службы:

PS C:\Users\xussein> nmap 192.168.3.129

Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-17 16:49 Russia TZ 2 Standard Time

Nmap scan report for 192.168.3.129

Host is up (0.000077s latency).

Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

53/tcp open domain

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

2049/tcp open nfs

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: 00:0C:29:65:83:6E (VMware)

Обратить внимание можно например на такие службы:

Bind: 53/tcp open domain ISC BIND 9.4.2

<https://www.exploit-db.com/exploits/37721>

Samba: 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

<https://www.exploit-db.com/exploits/42060>

Tomcat: 8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

<https://www.exploit-db.com/exploits/29739>

## **Задание 2**

Проведите сканирование Metasploitable в режимах SYN, FIN, Xmas, UDP.

Запишите сеансы сканирования в Wireshark.

Ответьте на следующие вопросы:

* Чем отличаются эти режимы сканирования с точки зрения сетевого трафика?
* Как отвечает сервер?

*Приведите ответ в свободной форме.*

## **Решение 2**

SYN сканирование:

* В случае SYN сканирования сканер отправляет пакеты с установленным флагом SYN, который используется для начала установки TCP-соединения.
* Если порт открыт, сервер отвечает пакетом с флагами SYN/ACK (ответил на запрос на установку соединения). Если порт закрыт, сервер отправит пакет с флагом RST (сброс соединения).

FIN сканирование:

* В этом режиме сканер отправляет пакеты с установленным флагом FIN (закрытие соединения).
* Если порт закрыт, сервер может либо игнорировать такие пакеты, либо отправить пакет с флагом RST (сброс соединения). Если порт открыт, сервер должен игнорировать такие пакеты.

Xmas сканирование:

* В Xmas сканировании сканер отправляет пакеты с установленными флагами FIN, URG и PUSH.
* Поведение сервера по отношению к Xmas сканированию аналогично поведению при FIN сканировании. Если порт открыт, сервер может либо игнорировать такие пакеты, либо отправить пакет с флагом RST (сброс соединения).

UDP сканирование:

* В отличие от TCP, UDP сканирование не устанавливает соединение. Вместо этого, сканер отправляет UDP пакеты на целевой порт.
* Если порт открыт, сервер может ответить на запрос. Однако, если порт закрыт, сервер может отправить пакет с ICMP сообщением "Port Unreachable" (порт недоступен) или просто игнорировать пакет.