Домашнее задание к занятию

"Уязвимости и атаки на информационные системы"

Акимов Александр

Инструкция по выполнению домашнего задания

1. Сделайте `fork` данного репозитория к себе в Github и переименуйте его по названию или номеру занятия, например, https://github.com/имя-вашего-репозитория/git-hw или https://github.com/имя-вашего-репозитория/7-1-ansible-hw).
2. Выполните клонирование данного репозитория к себе на ПК с помощью команды `git clone`.
3. Выполните домашнее задание и заполните у себя локально этот файл README.md:
    - впишите вверху название занятия и вашу фамилию и имя
    - в каждом задании добавьте решение в требуемом виде (текст/код/скриншоты/ссылка)
    - для корректного добавления скриншотов воспользуйтесь инструкцией "Как вставить скриншот в шаблон с решением
    - при оформлении используйте возможности языка разметки md (коротко об этом можно посмотреть в инструкции по MarkDown)
4. После завершения работы над домашним заданием сделайте коммит (`git commit -m "comment"`) и отправьте его на Github (`git push origin`);
5. Для проверки домашнего задания преподавателем в личном кабинете прикрепите и отправьте ссылку на решение в виде md-файла в вашем Github.
6. Любые вопросы по выполнению заданий спрашивайте в чате учебной группы и/или в разделе “Вопросы по заданию” в личном кабинете.

Желаем успехов в выполнении домашнего задания!

Дополнительные материалы, которые могут быть полезны для выполнения задания

1. Руководство по оформлению Markdown файлов

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.

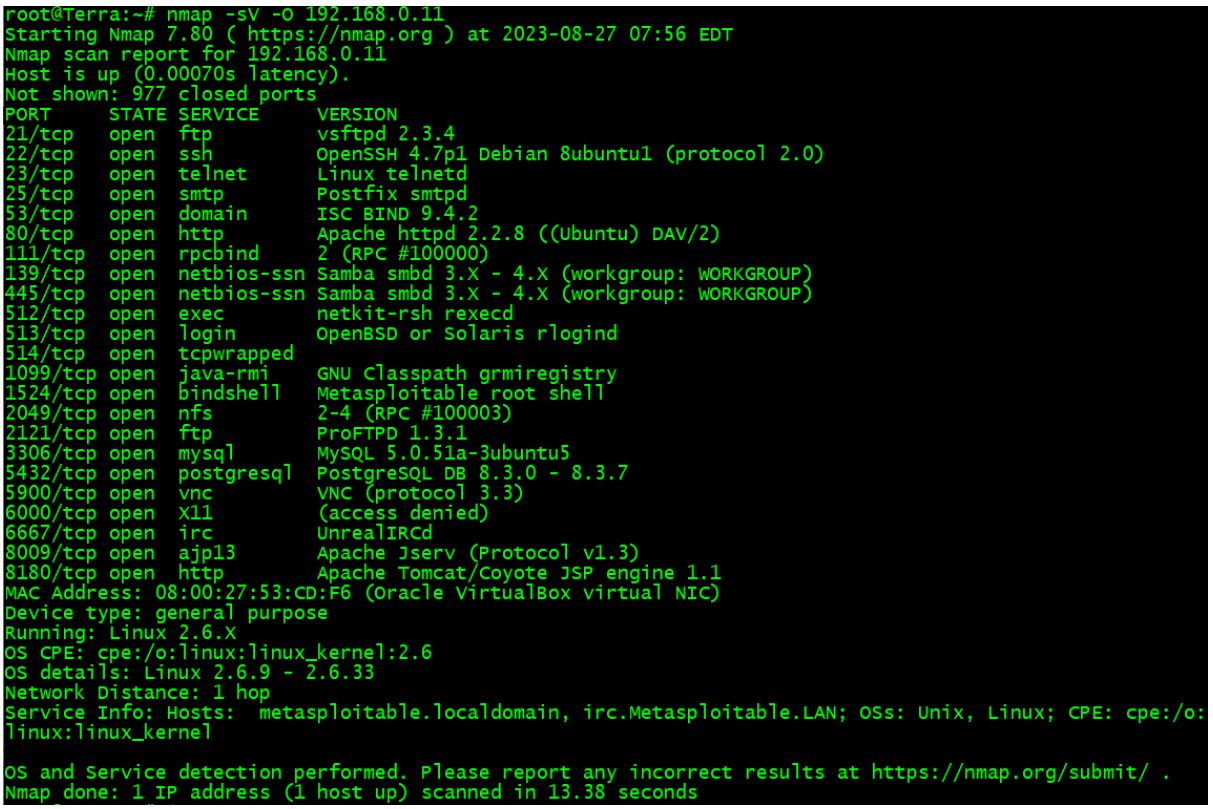
Ответьте на следующие вопросы:

- Какие сетевые службы в ней разрешены?

```
nmap -sv -O 192.168.0.11
```

977 портов закрыты - 23 открыты

Службы - ftp, ssh, telnet, smtp, domain, http, rpcbind, netbios-ssn, exec, login, tcpwrapped, java-rmi, bindshell, nfs, ftp, mysql, postgresql, vnc, X11, irc, ajp13, http



- Какие уязвимости были вами обнаружены? (список со ссылками: достаточно трёх уязвимостей)

```
https://www.exploit-db.com/exploits/17491
https://www.exploit-db.com/exploits/6122
https://www.exploit-db.com/exploits/30020
https://www.exploit-db.com/exploits/27407
https://www.exploit-db.com/exploits/31965
```

Задание 2

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

Запишите сеансы сканирования в Wireshark.

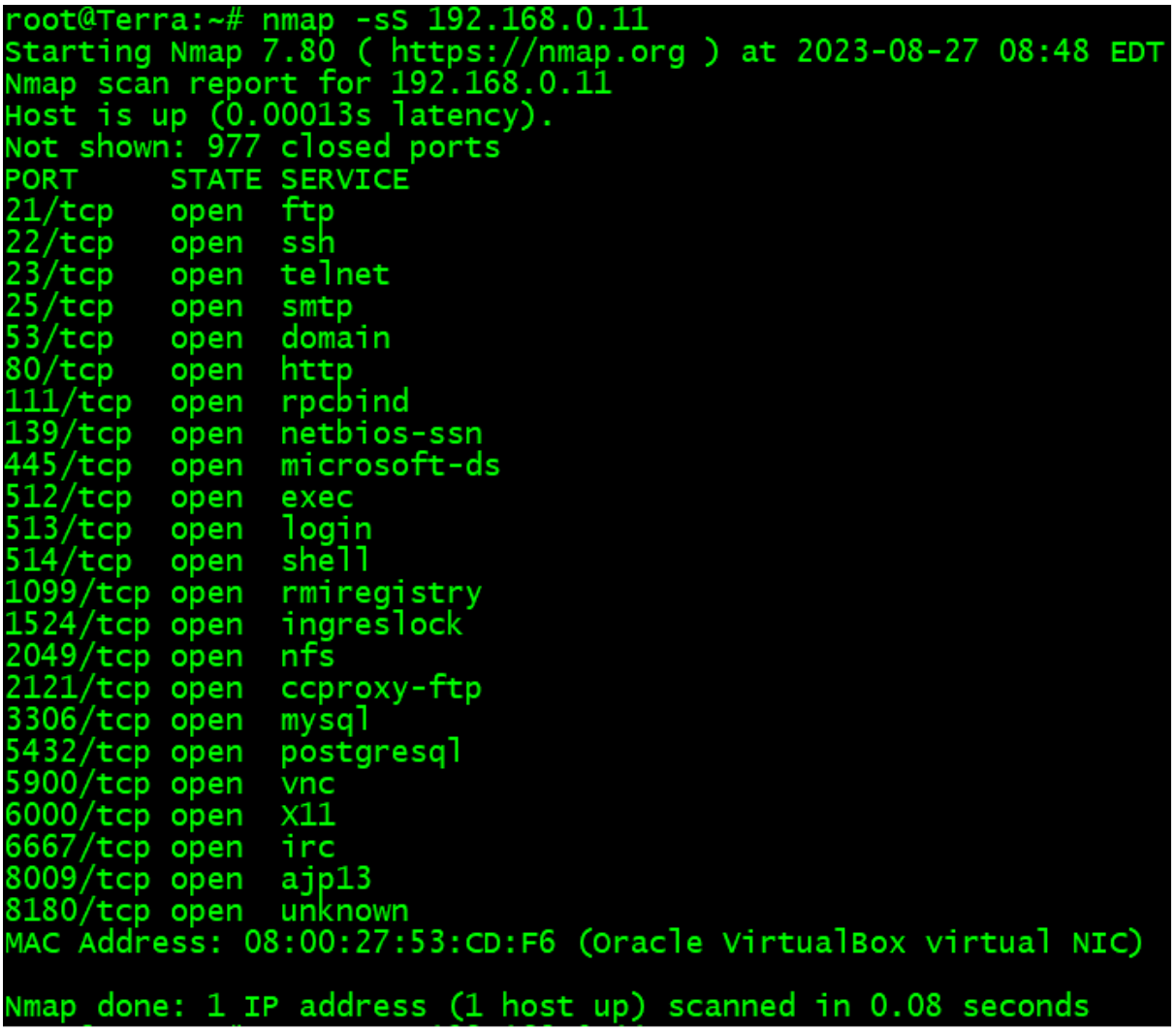
Ответьте на следующие вопросы:

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

SYN - Nmap посылает SYN-пакет, как бы намереваясь открыть настоящее соединение, и ожидает ответ. Наличие флагов SYN|ACK в ответе указывает на то, что порт удаленной машины открыт и прослушивается. Флаг RST в ответе

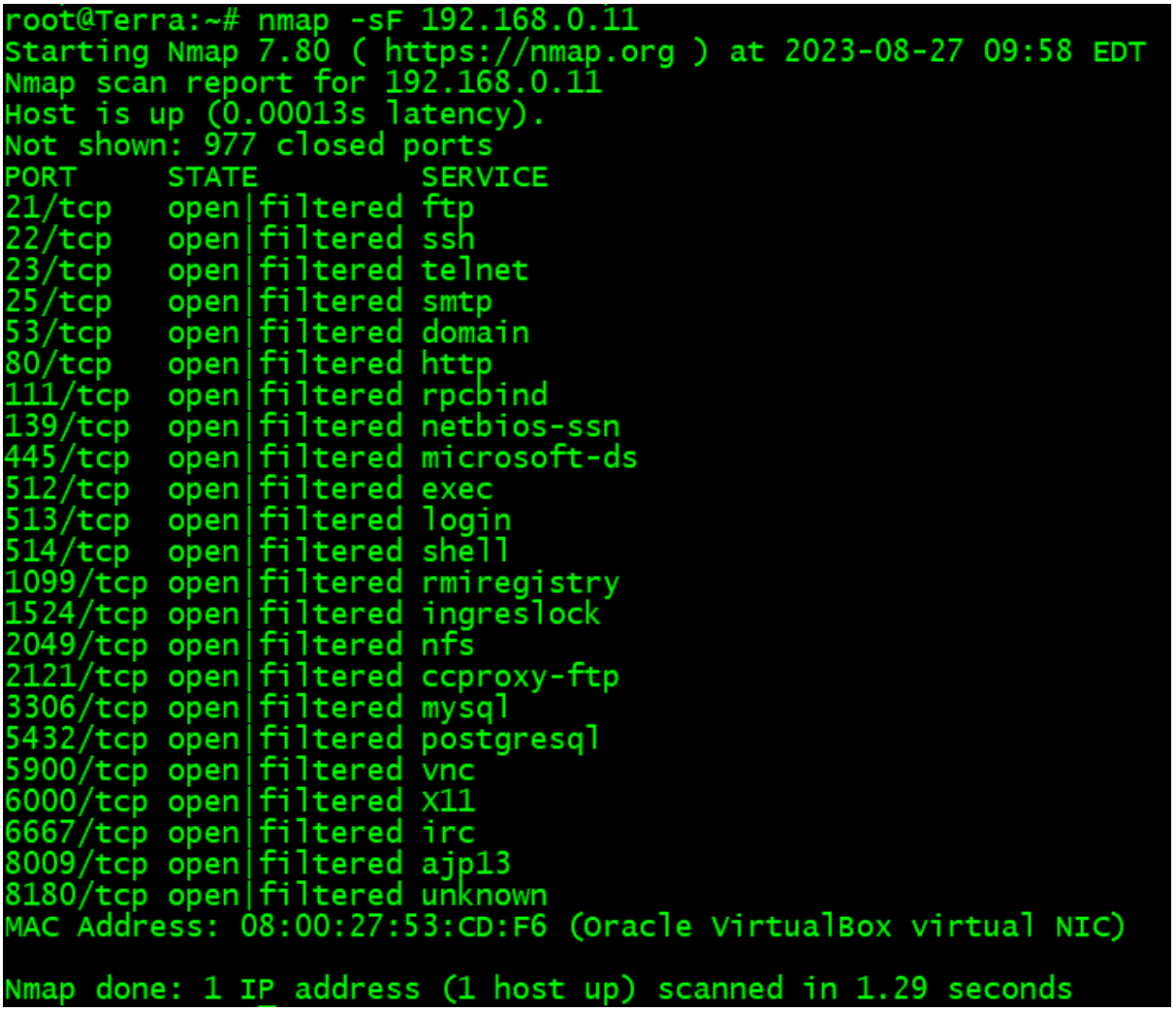
означает обратное. Если Nmap принял пакет SYN|ACK, то в ответ немедленно отправляет RST-пакет для сброса еще не установленного соединения

`nmap -sS <ip> - TCP SYN сканирование. SYN это используемый по умолчанию и наиболее популярный тип сканирования.`



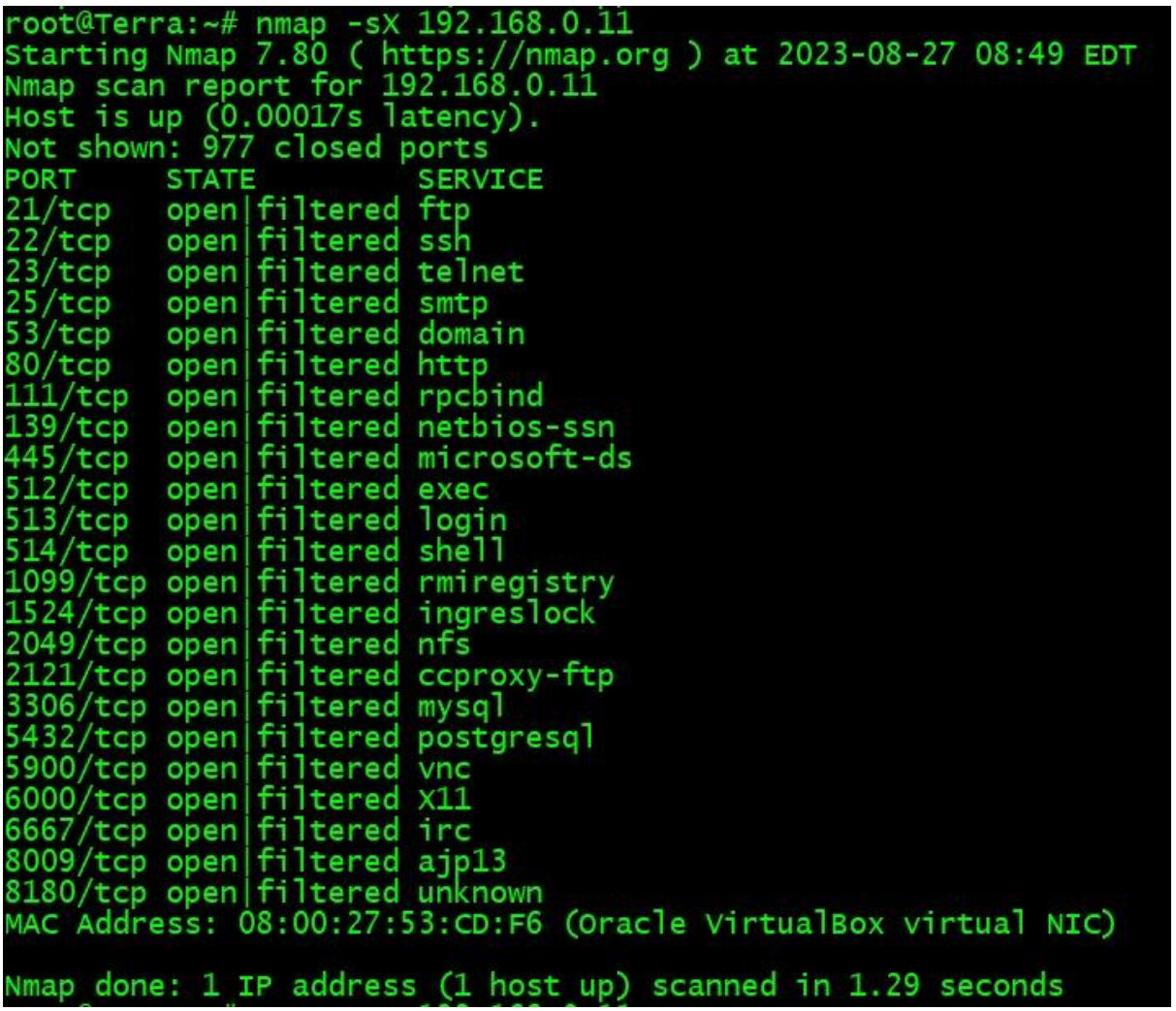
FIN - Nmap посылает FIN-пакет, в TCP заголовок ставится флаг FIN. Согласно RFC 793, на прибывший FIN-пакет на закрытый порт сервер должен ответить пакетом RST. FIN-пакеты на открытые порты должны игнорироваться сервером. По этому различию становится возможным отличить закрытый порт от открытого.

`nmap -sF <ip> - FIN сканирование. Устанавливается только TCP FIN бит.`



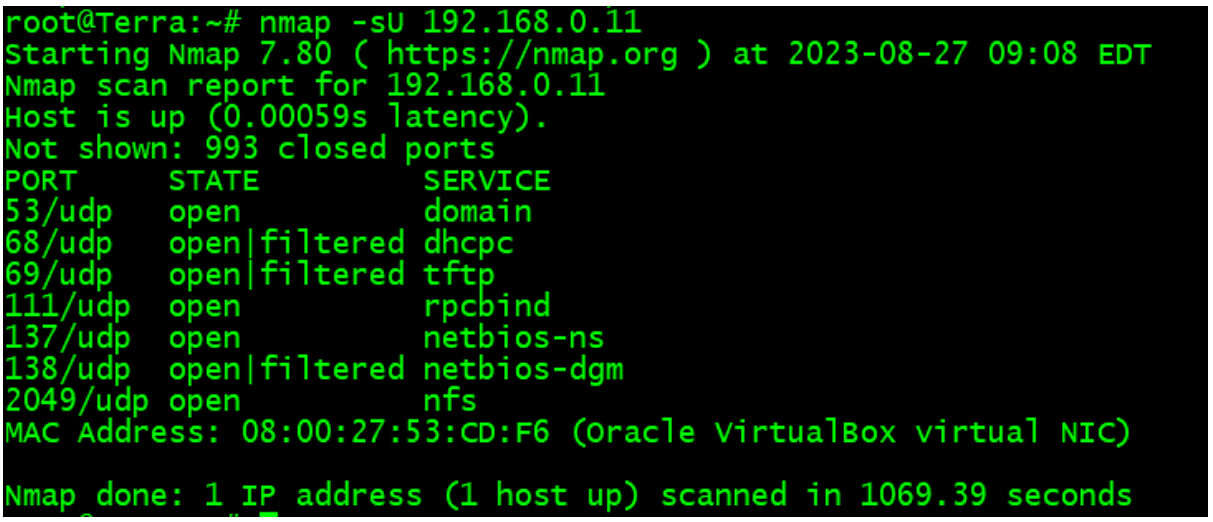
Xmas - Устанавливаются FIN, PSH и URG флаги. Если в результате FIN-сканирования мы получили список открытых портов, то это не Windows. Если же все эти методы выдали результат, что все порты закрыты, а SYN-сканирование обнаружило открытые порты, то мы скорей всего имеете дело с ОС Windows, Cisco, BSDI, IRIX, HP/UX и MVS. Все эти ОС не отправляют RST-пакеты.

`nmap -sX <ip> - Xmas сканирование. Устанавливаются FIN, PSH и URG флаги.`



UDP - На каждый порт сканируемой машины отправляется UDP-пакет без данных. Этот метод используется для определения, какие UDP-порты на сканируемом хосте являются открытыми.Если в ответ было получено ICMP-сообщение "порт недоступен", это означает, что порт закрыт. В противном случае предполагается, что сканируемый порт открыт.

`nmap -sU <ip> - Различные типы UDP сканирования. Большой проблемой при UDP сканировании является его медленная скорость работы.`


root@Terra:~# nmap -sU 192.168.0.11
Starting Nmap 7.80 (https://nmap.org) at 2023-08-27 09:08 EDT
Nmap scan report for 192.168.0.11
Host is up (0.00059s latency).
Not shown: 993 closed ports
PORT STATE SERVICE
53/udp open domain
68/udp open|filtered dhcpc
69/udp open|filtered tftp
111/udp open rpcbind
137/udp open netbios-ns
138/udp open|filtered netbios-dgm
2049/udp open nfs
MAC Address: 08:00:27:53:CD:F6 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1069.39 seconds