

Сетевые технологии

Кабинет moodle / Мои курсы / Специалитет / 10.05.03 Информационная безопасность автоматизированных систем / Разработка автоматизированных систем в защищенном исполнении (5 лет 6 месяцев-очная форма-ФГОС 3+) / 3 курс / Сетевые технологии / Отчеты по лабораторным работам / Отчет по лабораторной работе 4

Тест начат	Суббота, 30 марта 2024, 10:15
Состояние	Завершены
Завершен	Среда, 24 апреля 2024, 18:01
Прошло времени	25 дн. 7 час.
Оценка	Еще не оценено

Вопрос
Инфо
1 Отметить вопрос

Время выполнения теста не ограничено (4 недели до автоматического завершения попыток). После полного выполнения задания можно завершить попытку - отчет отправится на проверку. Если заполнена только часть вопросов и есть необходимость продолжить выполнение позднее, то нажмите **ОДИН РАЗ** кнопку "Закончить попытку", затем закройте вкладку с тестом или перейдите на другую страницу. Для продолжения выполнения нажмите кнопку "Продолжить последний просмотр"

Навигация по тесту



Закончить обзор

Вопрос 1
Выполнен
Балл: 10.00
1 Отметить вопрос

Изучение протоколов udp и tcp

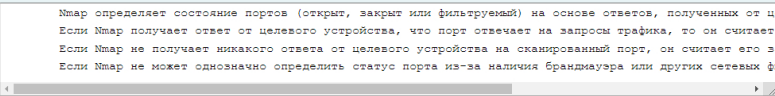
1) Определите ip адрес своего сетевого узла. В отчете приведите введенную команду и ip адрес. С использованием программы nmap в режиме простого сканирования (пинг-сканирование, без сканирования портов) в локальной сети определите работающие сетевые узлы.в результатах сканирования выберите один работающий сетевой узел для последующего сканирования. В отчете приведите введенную команду, результаты сканирования, ip адрес выбранного для сканирования сетевого узла.

192.168.1.165	
Введена команда (определение адреса)	ping a
ip адрес собственного узла	192.168.1.154/24
Введена команда (сканирование)	nmap -sn 192.168.1.154
	Starting Nmap 7.93 (https://nmap.org) at 2024-04-24 17:00 MSK
	Nmap scan report for Netis-N6.lan (192.168.1.1)
	Host is up (1.1s latency).
	MAC Address: BC:E0:01:98:8A:76 (Shenzhen Netis Technology)
	Nmap scan report for GOOSE-SERVER.lan (192.168.1.133)
	Host is up (0.00043s latency).
	MAC Address: 00:E0:4F:24:67:68 (Cisco Systems)
	Nmap scan report for VM-GOOSE-DEBIAN.lan (192.168.1.143)
	Host is up (0.00011s latency).
	MAC Address: 00:0C:29:90:44:17 (VMware)
	Nmap scan report for GOOSE-PC.lan (192.168.1.165)
	Host is up (0.000080s latency).
	MAC Address: B4:2E:99:A8:1E:72 (Giga-byte Technology)
	Nmap scan report for Redmi-Note-11S.lan (192.168.1.166)
	Host is up (0.048s latency).
	MAC Address: 66:9C:7C:7E:09:83 (Unknown)
	Nmap scan report for 192.168.1.154
	Host is up.
	Nmap done: 256 IP addresses (6 hosts up) scanned in 27.04 seconds
Результаты сканирования	
ip адрес выбранного узла	192.168.1.1

2) Запустите программу Wireshark, установите префильтрацию для сбора трафика по протоколам udp и icmp и ip адресу сканируемого узла. В отчете приведите **строку фильтра**. В программе nmap выполните udp сканирование портов от 1 до 100 на выбранном сетевом узле с одновременным сбором трафика в Wireshark. В отчете приведите **формат команды**. После завершения сканирования остановите сбор трафика. В отчете приведите результаты сканирования. По результатам сканирования определите **открытые порты** на сканируемом сетевом узле и **названия сетевых служб**, которые им соответствуют. Сохраните собранный трафик в файл, прикрепите дамп к отчету.

Строка фильтра (Wireshark)	(udp or icmp) and (host 192.168.1.1)
Команда для udp сканирования диапазона портов выбранного узла (nmap)	sudo nmap -sU 192.168.1.1 -p 1-100
Результаты сканирования (nmap)	Host is up (0.0010s latency).Not shown: 98 closed udp ports (port-unreach)PORT STATE SERVICES/udp open domain67/udp open dhcpsMAC Address: BC:E0:01:98:8A:76 (Shenzhen Netis Technology)
Открытые порты (номер, сервис)	53 - domain67 - dhcps

3) Отсортируйте собранный трафик по номеру порта получателя по возрастанию (при необходимости добавьте столбцы в верхнем окне программы). Анализируя отправляемые запросы и полученные ответы, опишите алгоритм определения открытых и закрытых портов сетевым сканером.



4) С использованием постфильтрации выделите в трафике пакеты протокола udp, отправленные на открытый порт сканируемого сетевого узла. Приведите в отчете строку фильтра и количество пакетов, отображенное по результатам фильтрации. Сохраните результаты фильтрации в файл (в дампе должны быть **только udp пакеты, отправленные на открытый порт**). Прикрепите дамп к отчету. Сбросьте фильтр. Установите фильтр, позволяющий выделить из трафика udp запросы, отправленные при сканировании на порт 53. Выберите один пакет udp, отправленный на порт 53 и оформите заголовок (конкретные значения полей и расшифровка значений).

введена строка фильтра	(udp.dstport == 67)
количество отображенных пакетов	1
Выбор udp пакета, отправленного на порт 53	
введена строка фильтра	(udp.dstport == 53)
Формат udp пакета	
Source Port	Destination Port
Source Port: 47132	Destination Port: 53
Порт отправителя	Порт назначения
Length	Checksum
Length: 20	Checksum: 0xb388 [unverified]
Длина	Контрольная сумма
	Data
10000000000000000000	
Полезная нагрузка	
(udp.dstport == 53) or (udp.dstport == 67).pcapng	

5) Определите IP-адрес веб-сайта **ibst.pnzgu.ru**. В отчете приведите команду и IP-адрес.

2) Наберите в адресной строке браузера **ibst.pnzgu.ru**, но не переходите на сайт. В программе Wireshark установите предфильтрацию для перехвата пакетов только с IP-адреса веб-сайта **ibst.pnzgu.ru**. Запустите сбор трафика, переключитесь к браузеру и загрузите веб-сайт. После окончания загрузки страницы закройте вкладку в браузере (или сам браузер) и остановите сбор трафика в программе Wireshark. В отчете приведите строку фильтра. Сохраните собранный трафик в файле, прикрепите дампы к отчету. В перехваченном трафике выполните постфильтрацию для выделения TCP-пакетов, отправленных и/или полученных с порта 80. В отчете приведите строку фильтра.

7) В результатах фильтрации определите количество TCP-потоков. Выберите поток, в котором есть пакеты протокола TCP, относящиеся к установлению и завершению соединения. В отчете укажите строку фильтра для выделения этого потока из дампа. Приведите в отчете изменения значений порядковых номеров (SN и AN в формате raw) и изменение состояния флагов сегментов (значение поля в 16м формате и названия установленных флагов), соответствующих установлению соединения.

4) Выделите пакеты, относящиеся к закрытию соединения. В отчете приведите изменения порядковых номеров и изменение флагов сегментов, соответствующих закрытию соединения. Постройте диаграмму выбранного TCP-потока с использованием Wireshark. **Прикрепите** к отчету снимок окна диаграммы потока.

введена команда


ping -c 1 netis.cc

IP-адрес сайта

192.168.1.1

строка фильтра (предфильтрация)

строка фильтра (постфильтрация)

 tcp.port == 80,pcapng

строка фильтра (для выделения потока)


tcp.port == 80 and tcp.stream eq 0

Установление соединения

№	Адрес:порт отправителя	Адрес:порт получателя	Sequence Number (raw)	Acknowledgment number (raw)	Flags
1	Source Port: 56734	Destination Port: 80	Sequence Number (raw): 4227583000	Acknowledgment number (raw): 0	Flags: 0x002 (SYN); 0xA002
2	Source Port: 80	Destination Port: 56734	Sequence Number (raw): 3787250353	Acknowledgment number (raw): 4227583001	Flags: 0x012 (SYN, ACK); 0xA012
3					

Завершение соединения

№	Адрес:порт отправителя	Адрес:порт получателя	Sequence Number (raw)	Acknowledgment number (raw)	Flags
1	Source Port: 80	Destination Port: 56734	Sequence Number (raw): 3787488384	Acknowledgment number (raw): 4227584370	Flags: 0x010 (ACK); 0x8010
2	Source Port: 56734	Destination Port: 80	Sequence Number (raw): 4227584370	Acknowledgment number (raw): 3787488385	Flags: 0x010 (ACK); 0x8010
3					
4					

 Снимок экрана 2024-04-24 175741.png

[Закончить обзор](#)

[← Отчет по лабораторной работе 3](#)

Перейти на...

[Защита отчета по лабораторной работе 5 ➔](#)

