

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 2

Тест начат	Суббота, 9 марта 2024, 10:32
Состояние	Завершены
Завершен	Суббота, 9 марта 2024, 17:00
Прошло времени	6 час. 28 мин.
Оценка	10,00 из 10,00 (100%)

Вопрос
Инфо
⚑ 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"

Вопрос 1
Выполнен
Не оценен
⚑ Отметить вопрос

вариант задания	время сбора, мин	протокол	количество пакетов
	3	udp	92
<p>Включить сбор данных на время, указанное в варианте, с автоматической остановкой сбора пакетов.</p> <p>Во время сбора данных выполнять действия с сетевым программным обеспечением:</p> <ul style="list-style-type: none">- загружать страницы веб-сайта в браузере (например, pnzgu.ru);- определить сетевой адрес веб-сайта (командой ping);- проверить доступность сетевого узла, на котором расположен веб-сайт (команда ping). <p>Перед выполнением задания рекомендуется очистить арг-кэш, набрать в адресной строке браузера адрес веб-сайта (но пока не переходить по адресу), в командной строке ввести команду (но не выполнять). После запуска сбора данных перейти по адресу в браузере и запустить команду. Дождаться автоматической остановки сбора пакетов.</p> <p>В ответе привести название веб-сайта, ip-адрес веб-сайта и выполненные действия.</p>			
веб-сайт	pnzgu.ru		
ip-адрес веб-сайта	82.179.91.20		
выполненные действия	1) Был очищен arp кеш: sudo ip neigh flush all		
	2) В адресной строке FireFox был набран сайт https://pnzgu.ru/		
	3) В первом окне терминала была введена команда: ping pnzgu.ru		
	4) Во втором окне терминала была введена команда: ping 82.179.91.20		
	5) На вкладке программы wireshark "Опции захвата" флаг "Автоматически останавливать захват после..." был установлен на 180 секунд		
	6) Был начат захват пакетов		
	7) Команды ping были запущены		
	8) Был осуществлен серфинг по сайту pnzgu.ru в течении 3-х минут		
Всего собранных пакетов: 63508			

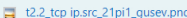
Вопрос 2
Выполнен
Баллов: 5,00 из 5,00
⚑ Отметить вопрос

1) Выполнить постфильтрацию собранного трафика по протоколу, указанному в варианте задания.
Определить количество выбранных пакетов.
Сохранить выбранные пакеты в файл (в файле должны быть **только пакеты протокола**, указанного в варианте).
В ответе привести параметры введенного фильтра, количество выбранных пакетов.

2) Очистить фильтр.
С использованием постфильтрации определить количество пакетов протокола TCP, полученных с веб-сервера, с которым устанавливалось соединение при выполнении п. 1).
Сохранить параметры созданного фильтра (дисплейный фильтр), **название фильтра должно включать фамилию и группу**.
В ответе привести параметры введенного фильтра, количество выбранных пакетов.
Результат добавления(сохранения) фильтра прикрепить скриншотом окна программы Wireshark (должен быть виден введенный фильтр, кнопка фильтра, результат фильтрации)

3) Очистить фильтр. Включить сбор данных с указанием автоматической остановки после сбора количества пакетов, указанного в варианте. Выполнять действия, указанные в п. 1).
После завершения сбора пакетов выбрать произвольный пакет. Скопировать содержимое фрейма в виде шестнадцатеричного потока.
Для скопированного пакета оформить формат кадра Ethernet (значения полей с указанием назначения полей).
Представить mac адреса отправителя и получателя в каноническом и бит-реверсивном форматах записи. Для бит-реверсивного формата указать значения полей адреса (с расшифровкой значения флагов).
Сохранить результаты сбора данных в файл.
Прикрепить файл в ответ.

введен фильтр:
udp
количество пакетов протокола после фильтрации:
2020

введен фильтр:
ip.src == pnzgu.ru and tcp
количество пакетов протокола после фильтрации:
17153


Формат кадра Ethernet


Поле	Pr	SFD	DA	SA	L/T	Data	CRC	EFD
Значение	---	---	00 50 56 e9 3e 3f	00 0c 29 63 8b 83	08 00	---	---	---
Расшифровка			Адрес назначения	Адрес источника	Длина/тип интерфейса			

MAC адрес отправителя
Канонический вид00:50:56:e9:3e:3f
Бит-реверсивный форматFC 7C 8B 6A 0A 00

Поля адресаI/GU/LOUIOUA
Значения полей00Значения полей00 50 56e9 3e 3f
Назначение полейиндивидуальныйуниверсально управляемыйID организацииID Устройства

MAC адрес получателя
Канонический вид00:0c:29:63:8b:83
Бит-реверсивный форматCA:D1:C6:94:30:00

Поля адресаI/GU/LOUIOUA
Значения полей00Значения полей00 0c 2963 8b 83
Назначение полейиндивидуальныйуниверсально управляемыйID организацииID Устройства



Навигация по тесту

Инф	1	2	3
		✓	✓

Закончить обзор

Вопрос 3

Выполнен

Баллов: 5,00 из 5,00

1" Отметить вопрос

Изучение протокола ARP

1) В терминале выведите содержимое arp таблицы узла. Укажите введенную команду и результат выполнения.

Очистите таблицу arp. Укажите введенную команду.

введена команда (вывод таблицы arp):

```
ip neigh
```

результат выполнения команды:

```
192.168.189.2 dev ens33 lladdr 00:50:56:e9:3e:3f STALE
192.168.189.254 dev ens33 lladdr 00:50:56:f8:03:b1 STALE
```

введена команда (очистка arp таблицы):


```
sudo ip neigh flush all
```

2) Установите в программе Wireshark фильтр, позволяющий перехватывать только пакеты arp. В отчет приведите снимок экрана окна "Опции Захвата" перед началом сканирования.

С использованием команды ip определите ip адрес своего компьютера и широковещательный адрес сети. Приведите их в отчете.

Введите команду для запуска ping-сканирования nmap. В отчет приведите введенную команду (команда, флаг сканирования, диапазон сканирования).

ip адрес компьютера:	192.168.189.129
широковещательный адрес сети (brd):	192.168.189.255
команда для запуска сканирования (nmap):	nmap -sn 192.168.189.0/24

 Снимок экрана 2024-03-09 143545.png

3) Запустите сбор трафика и сканирование сети.

После завершения сканирования остановите сбор трафика. В отчет приведите результат сканирования.

Выберите по результатам сканирования один узел.

Выведите таблицу arp. В результатах приведите запись в таблице arp для выбранного узла.

результат сканирования:

```
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-09 14:38 MSK
Nmap scan report for 192.168.189.1
Host is up (0.00022s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.189.2
Host is up (0.00015s latency).
MAC Address: 00:50:56:E9:3E:3F (VMware)
Nmap scan report for 192.168.189.254
Host is up (0.000078s latency).
MAC Address: 00:50:56:F8:03:B1 (VMware)
Nmap scan report for 192.168.189.129
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.94 seconds
```

выбран сетевой узел (запись из таблицы arp)

```
192.168.189.254 dev ens33 lladdr 00:50:56:f8:03:b1 STALE
```


4) С использованием постфильтрации выберите в трафике arp-запрос и arp-ответ, отправленный и полученный от выбранного сетевого узла. Сохраните результаты фильтрации в виде дампа (дамп должен содержать всего два arp пакета).

В ответе укажите введенный фильтр.

Прикрепите к ответу сохраненный дамп.

введен фильтр:

```
arp.dst.proto_ipv4 == 192.168.189.254 or eth.addr == 00:50:56:f8:03:b1
```

 t4.pcapng

5) Приведите значения полей arp-запроса (привести значения полей в 16м виде и расшифровку значений, например: Hardware type 0001 протокол канального уровня Ethernet)

поле	значение (hex)	расшифровка значения
Hardware type	00 01	Тип аппаратного уровня - Ethernet
Protocol type	08 00	Тип протокола - IPv4
Hardware size	06	Размер аппаратного адреса - 6 байт для MAC-адреса
Protocol size	04	Размер протокольного адреса - 4 байта для IPv4-адреса
Opcode	00 01	Код операции - запрос
Sender MAC address	00 0c 29 63 8b 83	MAC-адрес отправителя - 00:0c:29:63:8b:83
Sender IP address	c0 a8 bd 81	IP-адрес отправителя - 192.168.189.129
Target MAC address	00 00 00 00 00 00	MAC-адрес цели - 00:00:00:00:00:00
Target IP address	c0 a8 bd fe	IP-адрес цели - 192.168.189.254

Формат arp ответа

поле	значение (hex)	расшифровка значения
Hardware type	00 01	Тип аппаратного уровня - Ethernet
Protocol type	08 00	Тип протокола - IPv4
Hardware size	06	Размер аппаратного адреса - 6 байт для MAC-адреса
Protocol size	04	Размер протокольного адреса - 4 байта для IPv4-адреса
Opcode	00 02	Код операции - ответ
Sender MAC address	00 50 56 f8 03 b1	MAC-адрес отправителя - 00:50:56:f8:03:b1
Sender IP address	c0 a8 bd fe	P-адрес отправителя - 192.168.189.254
Target MAC address	00 0c 29 63 8b 83	MAC-адрес цели - 00:0c:29:63:8b:83
Target IP address	c0 a8 bd 81	IP-адрес цели - 192.168.189.129

Закончить обзор

← Отчет по лабораторной работе 1

Перейти на...

Отчет по лабораторной работе 3 ►

