государственное бюджетное профессиональное образовательное учреждение
«Пермский химико-технологический техникум»
(ГБПОУ «ПХТТ»)

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

для специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»
по МДК.02.01. Программные и программно-аппаратные средства защиты информации

2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 3
ПРАВИЛА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ 7
ОПИСАНИЕ РАБОЧЕГО МЕСТА ОБУЧАЮЩЕГОСЯ 8
ПРАКТИЧЕСКИЕ РАБОТЫ 9
Практическая работа № 1 9
Практическая работа № 2 13
Практическая работа № 3 16
Практическая работа № 4 19
Практическая работа № 5 20
Практическая работа № 6 24
Практическая работа № 7 28

ВВЕДЕНИЕ

Место дисциплины в ОПОП. МДК.02.01 «Программные и программно-аппаратные средства защиты информации» является обязательным разделом профессионального модуля ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами». В результате освоения ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» обучающийся должен:

уметь:

- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

знать:

- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
- методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

- типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
- особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;
- типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

Формируемые МДК.02.01 компетенции:

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

В результате освоения МДК.02.01 у обучающегося по базовой подготовке формируются общие компетенции (ОК):

ОК1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК3. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 9. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

Методические указания предназначены для проведения практических занятий по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Методические указания разработаны в соответствии с рабочей программой ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Содержание методических указаний по выполнению практических работ соответствует требованиям Федерального государственного стандарта среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Методические указания включают практические работы по темам:

- изучение сетевого взаимодействия между двумя оконечными оборудованиями. Сбор перехваченных данных;

- изучение процесса сканирования устройств. Анализ пакетов, используемые для проведения сканирования;
- защита каналов связи в информационных системах;
- защита субъектов сетевого доступа от сканирования;
- межсетевое экранирование. Системы обнаружения и предотвращения вторжений в информационных системах;
- сегментирование и изоляция вычислительных сетей.

Каждая практическая работа содержит сведения о теме, цели ее проведения и формируемых компетенциях, включает пояснение к работе, содержание отчета, контрольные задания или вопросы, список литературы.

К выполнению практических работ обучаемые приступают после подробного изучения соответствующего теоретического материала и прохождения инструктажа по технике безопасности.

Характер практических работ носит частично- репродуктивный.

ПРАВИЛА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

Практическое занятие по МДК.02.01 «Программные и программно-аппаратные средства защиты информации» проводиться в компьютерном классе. Необходимыми структурными элементами практического занятия являются инструктаж, проводимый преподавателем, а также организация обсуждения итогов выполнения практического задания. По окончании выполнения задания студент оформляет отчет.

Оценка за выполнение практических занятий выставляется по пятибалльной системе и учитывается как показатель текущей успеваемости студентов.

ОПИСАНИЕ РАБОЧЕГО МЕСТА ОБУЧАЮЩЕГОСЯ

1. Практические работы по МДК.02.01 «Программные и программно-аппаратные средства защиты информации» выполняются в компьютерном классе.

2. Для выполнения практических работ необходимы:

- персональный компьютер;
- операционная система Linux;
- приложения MS Office;
- WireShark;
- Zenmap;
- МЭ netfilter (iptables);
- FTP-server: VSFTPD;
- SSH-сервер: OpenSSH;
- Hydra;
- СОВ – Snort;
- СОВ – Surricata;
- методические указания.

ПРАКТИЧЕСКИЕ РАБОТЫ

Практическая работа №1

Изучение сетевого взаимодействия между двумя оконечными оборудованиями. Сбор перехваченных данных.

Цель работы:

Научиться настраивать сетевое взаимодействие устройств с ОС Linux, производить перехват трафика в Wireshark и осуществлять сбор статистики. **Формируемые компетенции:** ПК2.1, ПК2.2, ПК2.3, ПК2.4, ПК2.5, ПК2.6, ОК1-ОК10.

Оборудование:

персональный компьютер, операционная система Linux, приложения MS Office, Wireshark.

Пояснения к работе

Теоретический материал.

Для проверки ip адреса у машины необходимо использовать команду ifconfig. Проверьте, чтобы две машины находились в одной подсети, но имели разные ip адреса. Проверьте, что при команде ping пакеты передаются, как на рис. 1

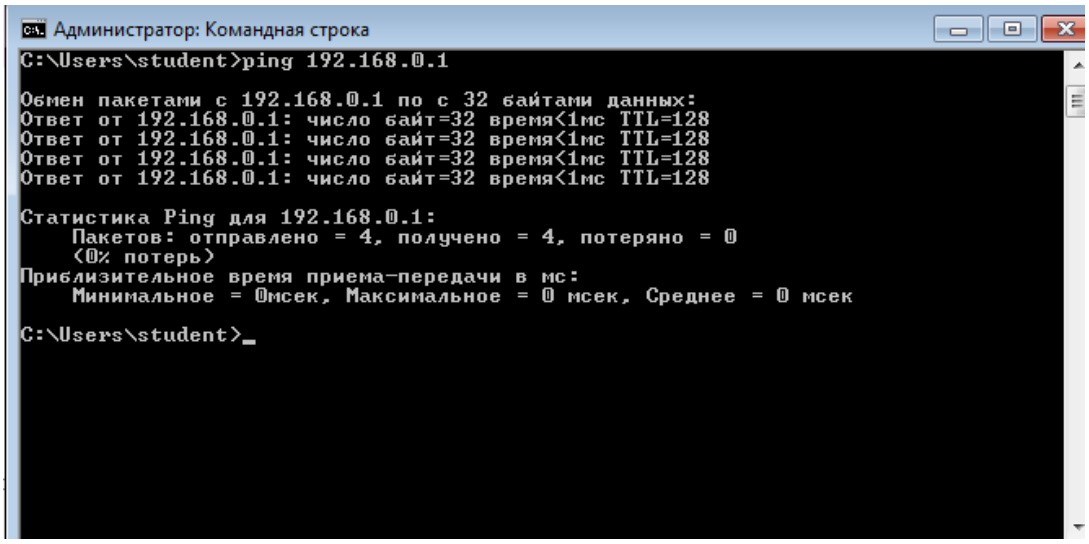

Рисунок 1 - Выполнение команды ping

Для открытия программы wireshark в командной строке напишите *wireshark* под суперпользователем. Одновременно передавайте пакеты одной

машины на другую и посмотрите какие пакеты передаются. Среди различных протоколов надо найти пакеты по протоколу tcp, icmp и тд.

Необходимо создать сетевую папку на машине и получить протокол SMB в wireshark. Провести сбор статистики для этого перейти на вкладку Статистика как на рис.2 .

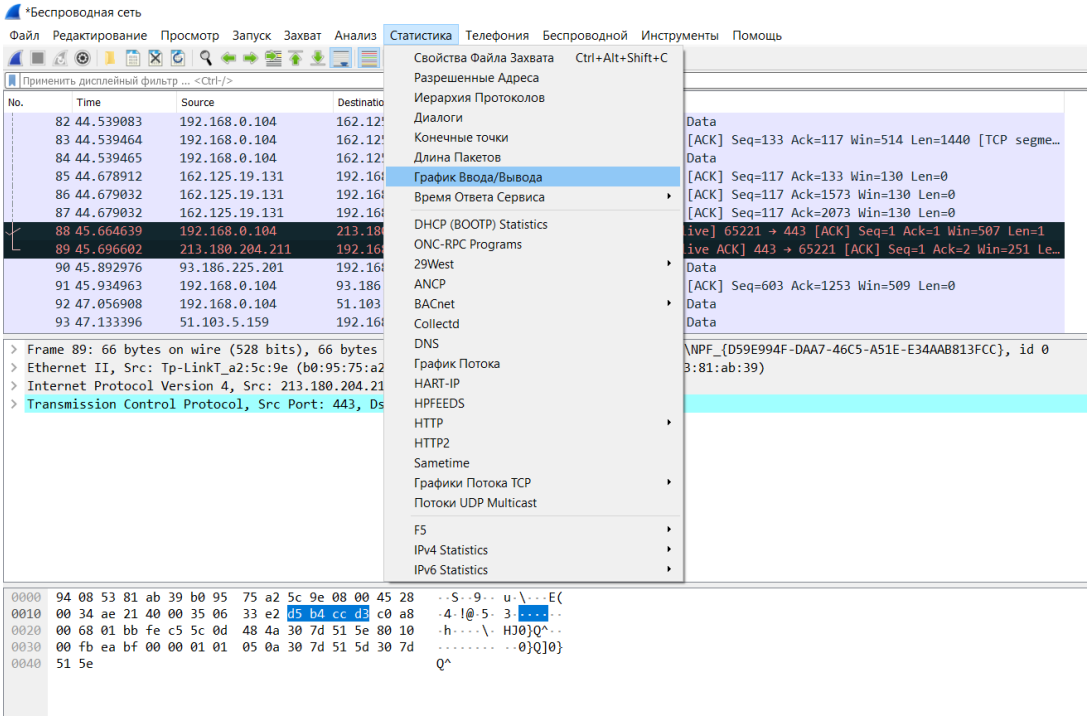

Рис.2 – Вкладка для сбора статистики

Далее получаем график (рис.3).

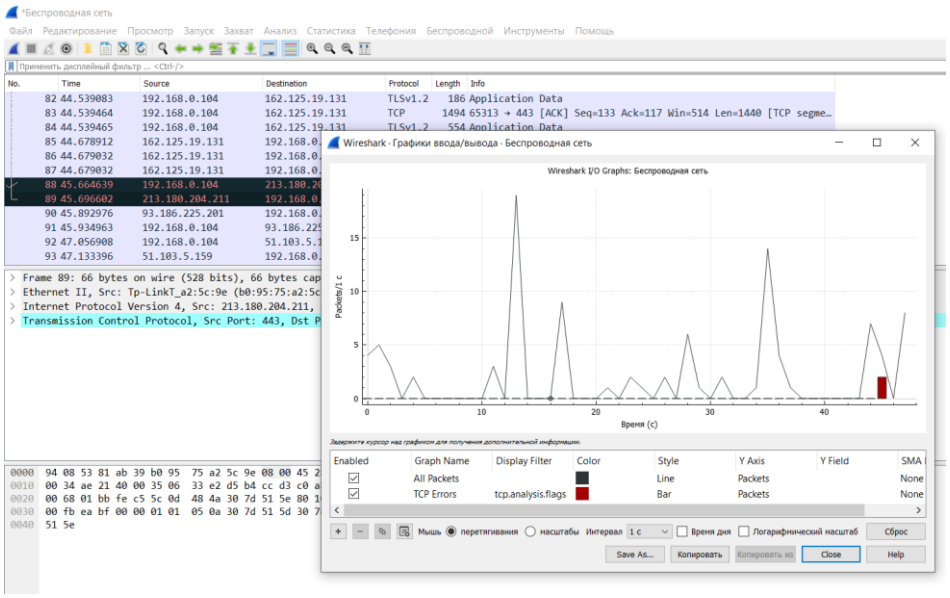

Рис.3 – График данных

Задание

Произвести перехват трафика в Wireshark и осуществить сбор статистики.

Содержание отчета:

- формулировка задачи;
- график результата перехвата трафика в Wireshark.

Указания к выполнению работы:

1. Изучить теоретический материал.

2. Настроить сетевое взаимодействие устройств для перехвата трафика данных.

Контрольные вопросы:

1. Для чего нужен Wireshark?

2. Какой командой проверить надежность сетевого взаимодействия устройств?

3. Какие сетевые протоколы существуют?

Литература

1. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.
2. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.
4. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф.

образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с.

5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012
6. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

Практическая работа №2

Изучение процесса сканирования устройств. Анализ пакетов, используемых для проведения сканирования.

Цель работы:

Провести сканирование заданного хоста. Определить ОС, открытые порты и сервисы. Проанализировать пакеты, используемые для проведения сканирования

Формируемые компетенции: ПК2.1, ПК2.2, ПК2.3, ПК2.4, ПК2.5, ПК2.6, ОК1-ОК10.

Оборудование:

персональный компьютер, операционная система Linux, приложения MS Office, Wireshark, nmap.

Пояснения к работе

Теоретический материал.

Для сканирования хоста используем следующий синтаксис: nmap host. Определяем сетевые интерфейсы пользуемся командой: ifconfig. В результате можно увидеть нужный ip адрес – пример: 192.168.1.1. Для смены ip адреса используйте синтаксис:

*[*Sudo ifconfig *интерфейс адрес* netmask *маска]*

Сканирование на виртуальной машине произвести с помощью утилиты nmap с помощью команды:

nmap 192.168.1.1– получаем порты, состояния, сервисы, mac адреса.

nmap –O 192.168.1.1 – получаем сканирование ОС.

Одновременно запускаем wireshark. Для вызова программы набираем: wireshark и в результате увидим передачу пакетов между двумя машинами по протоколу tcp. Если возникли проблемы с kali, он требует пароль root, а вы забыли. Тогда перезапускаем машину, в терминале водим команду: `passwd root`.

Задание

1. Провести сканирование заданного хоста. Определить ОС, открытые порты и сервисы.

2. Проанализировать пакеты, используемые для проведения сканирования и обычного соединения.

Содержание отчета:

- формулировка задачи;
- Результат сканирования хоста и анализ пакетов.

Указания к выполнению работы:

1. Изучить теоретический материал.

2. Провести сканирования с помощью утилиты nmap, проанализировать пакеты с помощью программы wireshark.

Контрольные вопросы:

1. Для чего нужен Wireshark?

2. Для чего нужен nmap?

3. Какие команды используются при сканировании хоста?

Литература

7. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.
8. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.
9. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.
10. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф.

образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с.

11. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012
12. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

Практическая работа №3

Защита каналов связи в информационных системах**.**

Цель работы:

Научиться защищать каналы связи в информационных системах.

Формируемые компетенции: ПК2.1, ПК2.2, ПК2.3, ПК2.4, ПК2.5, ПК2.6, ОК1-ОК10.

Оборудование:

персональный компьютер, операционная система Linux, приложения MS Office, Wireshark, Zenmap, FTP-server: VSFTPD, SSH-сервер: OpenSSH.

Пояснения к работе

Теоретический материал.

Сканирование на виртуальной машине необходимо произвести с помощью утилиты nmap с помощью команды:

nmap *адрес* – получаем порты, состояния, сервисы.

nmap – O *адрес* – получаем сканирование ОС.

Установить FTP-сервер с помощью команды *sudo apt install vsftpd и* SSH-сервер с помощью команды *sudo apt-get install openssh-server*. Если выдает ошибки необходимо воспользоваться командой *sudo apt-get update* для обновления.

Для проверки состояния ssh необходимо ввести команду *systemctl status ssh*. В результате состояние должно быть активным.

Для проверки работы ftp вводим команду *ftp адрес*. Для работы с ftp воспользуйтесь сведениями:

$ ftp опции *адрес сервера*

Опции:

1) **-A** - использовать активный режим во время передачи файлов;
2) **-p** - использовать пассивный режим, используется по умолчанию;
3) **-i** - отключать интерактивный режим во время передачи файлов;
4) **-n** - попытаться использовать автоматический вход;
5) **-e** - отключить историю команд;
6) **-v** - максимально подробный вывод;

7) **-d** - включить режим отладки.

Команды, которые необходимо использовать для подключения к серверу и управления файлами:

- **account** - отправить серверу свой пароль для авторизации;
- **append** - добавить локальный файл в конец удаленного файла на сервере;
- **ascii** - передавать файлы в кодировке ASCII;
- **binary** - передавать файлы в бинарном формате;
- **bye** - завершить сессию;
- **cd** - перейти в папку;
- **cdup** - перейти в папку уровнем выше;
- **chmod** - изменить права на файл;
- **delete** - удалить файл с сервера;
- **dir** - посмотреть список файлов в папке;
- **get** - скачать файл из сервера на локальную машину;
- **hash** - отображать статус передачи файла;
- **lcd** - сменить рабочую директорию на локальной машине;
- **ls** - список файлов в папке;
- **mdelete** - удалить несколько файлов;
- **mget** - скачать несколько файлов;
- **mkdir** - создать папку;
- **mput** - передать несколько файлов на сервер;
- **open** - подключится к удаленному FTP серверу;
- **put** - передать файл на сервер;
- **pwd** - вывести текущую папку;
- **rename** - переименовать файл на сервере;
- **rmdir** - удалить папку;
- **size** - узнать размер файла;
- **user** - авторизоваться на сервере.

Задание

1. Провести сканирование заданного хоста. Определить ОС, открытые порты и сервисы;
2. Проанализировать пакеты, используемые для проведения сканирования и обычного соединения;
3. Установить FTP-сервер и осуществить передачу любого файла с FTPсервера на клиентское устройство;
4. Проанализировать угрозы для ИС с FTP-сервером;
5. Реализовать угрозу перехвата сетевого трафика;
6. Установить защищенное соединение с помощью протокола SSH;
7. Повторить пункт 5;
8. Проанализировать угрозы для ИС с SSH-сервером;

Содержание отчета:

- формулировка задачи;
- результат сканирования хоста и анализ пакетов;
- результат передачи файлов по протоколам: FTP, SSH;
- результат реализации угрозы перехвата трафика.

Указания к выполнению работы:

1. Изучить теоретический материал.

2. Провести сканирование с помощью утилиты nmap, проанализировать пакеты с помощью программы wireshark.

3. /etc/ssh/sshd_config \\ конфигурационный файл OpenSSH-сервера.

Контрольные вопросы:

1) Для чего нужен nmap?
2) Какие команды используются при сканировании хоста?
3) Каким угрозам подвержены протоколы ARP, IP, TCP, FTP?
4) На каких уровнях модели OSI могут быть реализованы угрозы?

Литература

1. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной

безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.

2. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.
4. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с.
5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012
6. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

Практическая работа № 4

Защита субъектов сетевого доступа от сканирования**.**

Цель работы:

Научиться защищать субъекты сетевого доступа от сканирования в информационных системах.

Формируемые компетенции: ПК2.1, ПК2.2, ПК2.3, ПК2.4, ПК2.5, ПК2.6, ОК1-ОК10.

Оборудование:

- персональный компьютер, операционная система Linux;
- приложения MS Office;
- Wireshark;
- Zenmap;
- SSH-сервер:OpenSSH;
- МЭ netfilter (iptables).

Пояснения к работе

Теоретический материал.

Для проведения сканирования на виртуальной машине (рис.1) необходимо воспользоваться утилитой nmap с помощью команды:

nmap *адрес* – получаем порты, состояния, сервисы, mac адреса.

nmap – *адрес* – получаем сканирование ОС.

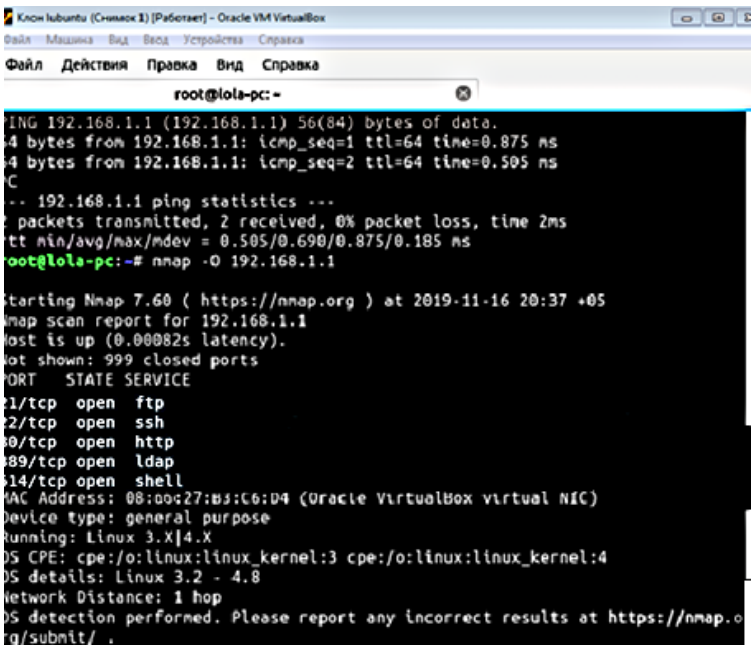

Рис.1 Сканирование lubuntu

Проанализировать пакеты, используемые для проведения сканирования и обычного соединения с помощью программы: wireshark (рис.2).

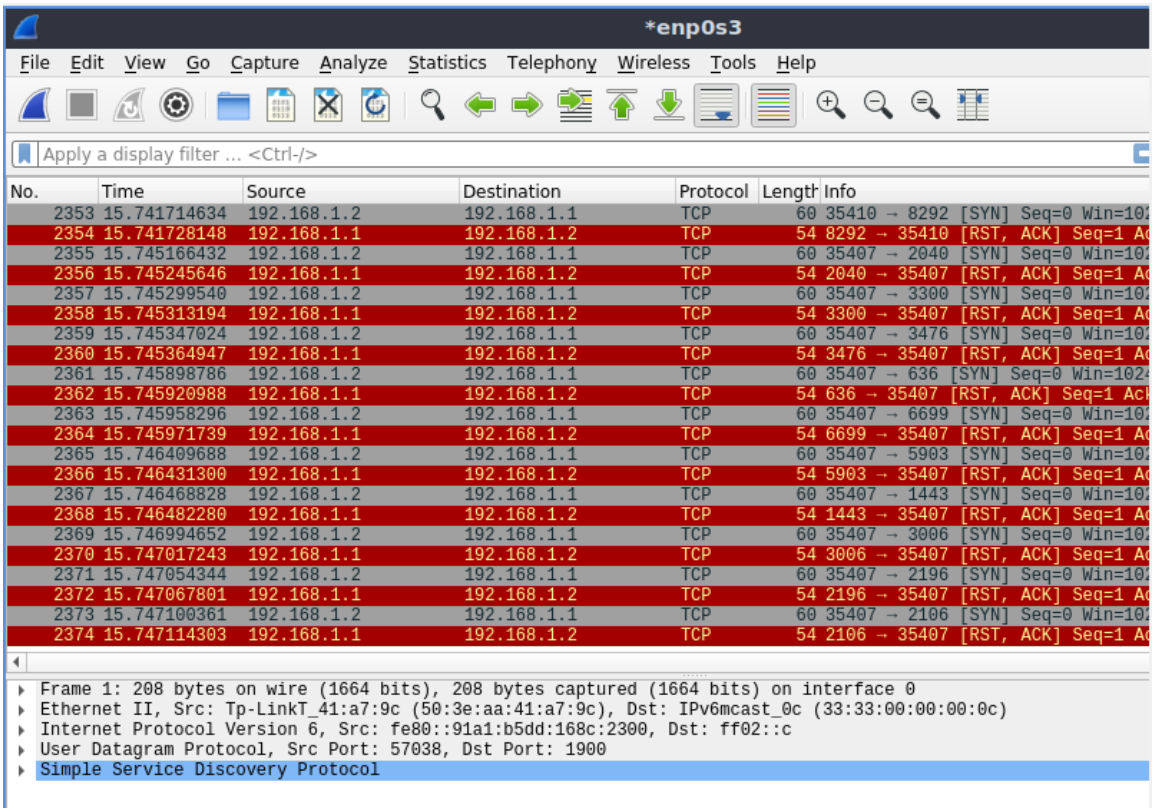

Рис.2 Результаты анализа пакетов

После анализа необходимо выделить те признаки, по которым можно создать правило для защиты от сканирования: по флагам пакета; по размеру пакета; по времени жизни пакета.

Для написания правила МЭ для блокировки сканирования необходимо воспользоваться правилом (рис.3): sudo iptables –A OUTPUT –p tcp –m length –length 1:60 –j DROP.

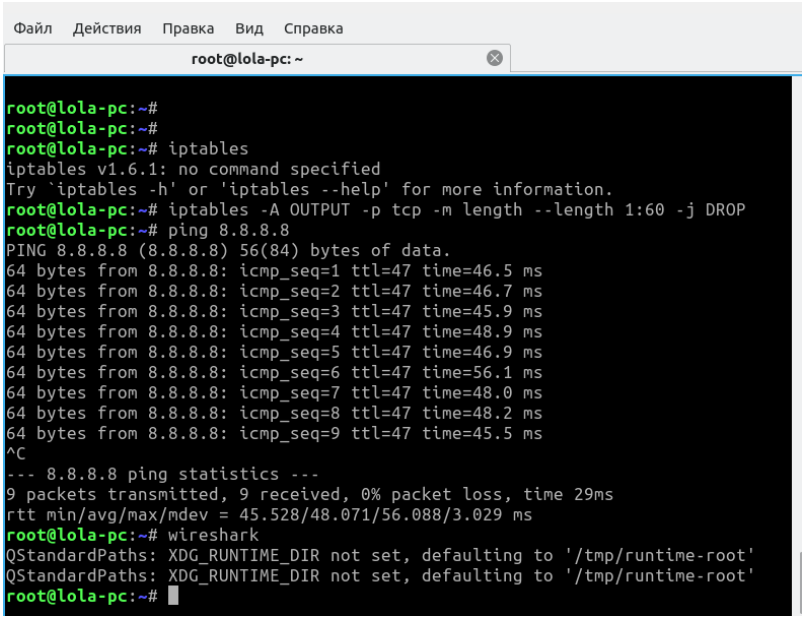

Рис.3 Применение правила

В результате повторного сканирования виртуальной машины не должно получиться узнать о открытых портах или ОС хоста.

Задание

1. Провести сканирование заданного хоста. Определить ОС, открытые порты и сервисы.
2. Проанализировать пакеты, используемые для проведения сканирования и обычного соединения.
3. Написать правила МЭ для блокировки сканирования.

Содержание отчета:

- формулировка задачи;
- результат сканирования хоста и анализ пакетов;
- результат написания правила МЭ для блокировки сканирования.

Указания к выполнению работы:

1. Изучить теоретический материал.
2. Провести сканирование с помощью утилиты nmap, проанализировать пакеты с помощью программы wireshark.
3. nmap host \\сканирование хоста.
4. ssh user@host \\создание сессии по протоколу ssh с host от имени user.
5. sudo iptables -A INPUT -p tcp -s host -j DROP \\добавление правила в

таблицу filter цепочку INPUT правила для протокола tcp блокировать источник host.

Контрольные вопросы:

1. Какие задачи выполняет протокол ICMP?
2. Как сканирование может быть использовано злоумышленником?
3. Как определяется открытый порт на хосте?
4. Какие данные позволяют предположить проведение атаки?

Литература

1. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.
2. Руководство по Wireshark: https://www.wireshark.org/docs/
3. Полная информация по настройке МЭ netfilter и iptables: https://www.netfilter.org/documentation/
4. Руководство по использованию nmap: https://nmap.org/man/ru/
5. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.
6. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с.
7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012
8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

Практическая работа № 5

Межсетевое экранирование. Системы обнаружения и предотвращения вторжений в информационных системах**.**

Цель работы:

Научиться настраивать netfilter (iptables) и систему обнаружения и предотвращения вторжений в информационных системах (СОВ).

Формируемые компетенции: ПК2.1, ПК2.2, ПК2.3, ПК2.4, ПК2.5, ПК2.6, ОК1-ОК10.

Оборудование:

- персональный компьютер, операционная система Linux;
- приложения MS Office;
- Wireshark;
- Hydra;
- СОВ – Snort;
- СОВ – Surricata;
- МЭ netfilter (iptables).

Пояснения к работе

Теоретический материал.

Для настройки iptables для блокировки атаки «Brute force»:

1) recent - это специальный критерий, позволяющий запоминать проходящие через него пакеты, а затем использовать полученную информацию для принятия решений.
2) Ctstate – для получения информации о признаке состояния соединения, что позволяет судить о состоянии соединения.
3) --update: опция будет проверять наличие адреса отправителя пакета в списке.
4) --hitcount hits: счетчик, возвращает true при наличии адреса в списке, когда число принятых пакетов с адреса больше или равно заданного значения.
5) --set: служит для добавления адреса отправителя пакета в список.

МЭ позволяет ограничить количество попыток установки соединения в определённый период. Например, пользователь раз в 15 минут может установить соединение с сервером на SSH порт. Только по истечении этого времени он может это сделать ещё раз. То есть даже особо не важно, правильный или нет был указан пароль. Система помечает его пакеты для себя. И если попытка повторяется — ему будет отказано. Поэтому сама атака будет замедляться.

Пример написания правила для оповещения. СОВ - Suricata. Правило: alert tcp any any → any any (msg:“BRUTE“; sid:1000001; rev:1; flow:to_server; flag:S; detection_filter:track by_src, count 5, seconds 120.

1) Ключевое слово sid дает каждой подписи свой собственный идентификатор. Ключевое слово sid почти всегда сопровождается оборотом. Rev представляет версию подписи. Если подпись изменена, число оборотов будет увеличиваться авторами подписи.
2) flow - цель этого правила - проверить совпадение в userlogin и отметить его в потоке.
3) to_server - совпадение пакетов от клиента к серверу.
4) Detection_filter может использоваться для оповещения о каждом совпадении после достижения порогового значения.
5) track by_src - отслеживание совпадения правил. При использовании by_src / by_dst отслеживание осуществляется по IP-адресу.

Задание

1. Произвести настройку netfilter (iptables) для блокирования «Brute force» атаки.
2. Проанализировать влияние МЭ на угрозу подбора пароля.
3. Произвести успешную атаку подбора пароля.
4. Установить и настроить СОВ для мониторинга попыток подбора пароля.

Содержание отчета:

- формулировка задачи;
- результат настройки netfilter (iptables);

- результат атаки подбора пароля;
- результат настройки СОВ для мониторинга попыток подбора пароля.

Указания к выполнению работы:

1. Изучить теоретический материал.
2. Snort –A console –c /etc/snort/snort.conf \\ Запуск snort с конфигурацией препроцессоров и правил snort.conf и выводом логов в консоли.
3. alert icmp any any -> any any (msg: "WTF"; sid: 10000002;) \\ Пример правила для выдачи предупреждения при обнаружении icmp-трафика Source (any,any) Destination (any,any) вывести сообщение «W», уникальный идентификатор правила - 10000002.

Контрольные вопросы:

1. Какую информацию и на каких уровнях анализирует МЭ?
2. Какие функции выполняет модуль state?
3. Какие функции выполняет модуль recent?
4. Какие функции выполняет модуль connlimit?
5. Какие функции выполняет модуль hashlimit?
6. В чем разница между МЭ и СОВ?
7. Какие схемы интеграции МЭ и СОВ существуют? В чем их преимущества и недостатки?

Литература

1. Полная информация по настройке МЭ netfilter и iptables: https://www.netfilter.org/documentation/
2. Полная информация по настройке СОВ: https://www.snort.org/#documents https://suricata-ids.org/docs/
3. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.
4. Руководство по Wireshark: https://www.wireshark.org/docs/

5. Полная информация по настройке МЭ netfilter и iptables: https://www.netfilter.org/documentation/
6. Руководство по использованию nmap: https://nmap.org/man/ru/
7. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.
8. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с.
9. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012.

Практическая работа №7

Сегментирование и изоляция вычислительных сетей.

Цель работы:

Провести аудит доступности серверов за МЭ и сформировать предложения по усилению защиты внутренних серверов.

Формируемые компетенции: ПК2.1, ПК2.2, ПК2.3, ПК2.4, ПК2.5, ПК2.6, ОК1-ОК10.

Оборудование:

- персональный компьютер, операционная система Linux;
- приложения MS Office;
- Wireshark;
- Zenmap;
- МЭ netfilter (iptables).

Пояснения к работе

Теоретический материал.

Аудит – это процесс проверки работы предприятия. Главная цель аудита информационной безопасности – это дать максимально точную оценку защищенности. Однако в основном под аудитом понимают проверку соответствия системы защиты требованиям стандартов, что входит в цели аудита, но не является единственной целью.

Межсетевые экраны (МЭ) – это класс устройств, осуществляющих физическое и логическое разделение сетей. Для этого в межсетевом экране реализованы функции мониторинга и контроля проходящего трафика. В зависимости от того, на ка□ком уровне модели OSI осуществляется мониторинг и контроль трафика межсетевые экраны разделяются на три класса:

1. Пакетные фильтры, осуществляющие контроль на уровне сетевых и транспортных протоколов.

2. Межсетевые экраны с контролем состояния, осуществляющие контроль на сеансовом уровне.

3. Межсетевые экраны уровня приложения, осуществляющие контроль на прикладном уровне модели OSI.

Задание

1. Провести аудит доступности серверов за МЭ.
2. Реализовать парольную атаку на сервер за МЭ.
3. Сформировать предложения по усилению защиты внутренних серверов.

Содержание отчета:

- формулировка задачи;
- результат настройки МЭ netfilter (iptables);
- результат атаки подбора пароля;

Указания к выполнению работы:

1. Изучить теоретический материал.
2. ssh user@host \\создание сессии по протоколу.
3. sudo iptables -A INPUT -p tcp -s host -j DROP \\добавление правила в таблицу filter цепочку INPUT правила для протокола tcp блокировать источник host.

Контрольные вопросы:

1. Какую информацию и на каких уровнях анализирует МЭ?
2. Отличительные характеристики МЭ.
3. Какие схемы интеграции МЭ существуют? В чем преимущества и недостатки?

Литература

1. Полная информация по настройке МЭ netfilter и iptables: https://www.netfilter.org/documentation/
2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.
3. Руководство по Wireshark: https://www.wireshark.org/docs/

4. Полная информация по настройке МЭ netfilter и iptables: https://www.netfilter.org/documentation/
5. Руководство по использованию nmap: https://nmap.org/man/ru/
6. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.
7. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с.
8. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012.