МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НОВОСИБИРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра компьютерных систем

Направление подготовки 09.03.01 Информатика и вычислительная техника

Направленность (профиль) Программная инженерия и компьютерные науки

ОТЧЕТ

о прохождении учебной практики, научно-исследовательской работы (получение первичных навыков научно-исследовательской работы)
(указывается наименование практики)

Обучающегося Кондренко Кирилла Павловича **группы №** 21203 **курса** 3
(Ф.И.О. полностью)

Тема задания: изучение межсетевых экранов следующего поколения «UserGate» в условиях реальной эксплуатации

Место прохождения практики: ООО «Юзергейт», 630090, г. Новосибирск, ул. Николева, 11
(полное наименование организации и структурного подразделения, индекс, адрес)

Сроки прохождения практики: с 02.10.2023 г. по 22.12.2023 г.

Руководитель практики от профильной организации _____ _____
(Ф.И.О. полностью, должность) (подпись)

Руководитель практики от НГУ Пестунова Тамара Михайловна, доцент _____
(Ф.И.О. полностью, должность) (подпись)

Руководитель ВКР _____ _____
(Ф.И.О. полностью) (должность)

Оценка по итогам защиты отчета: _____
(неудовлетворительно, удовлетворительно, хорошо, отлично)

Отчет заслушан на заседании кафедры компьютерных систем
(наименование кафедры)

протокол _____ **от «**_____**»** _____ 20_____г.

Новосибирск 2023

Содержание

1 Введение

Цель прохождения практики состояла в изучение межсетевых экранов следующего поколения «UserGate» в условиях реальной эксплуатации. Для достижения этой цели нужно было решить следующие задачи:

- Изучить основы информационной безопасности, компьютерных сетей и основных интернет-протоколов;
- Изучить принципы работы межсетевого экрана нового поколения «Usergate»;
- Научиться создавать «стенды» в гипервизоре Oracle VM VirtualBox для эмуляции работы межсетевого экрана;
- Научиться использовать «стенды» для решения проблем, возникших у клиентов, использующих «Usergate».

Актуальность темы межсетевых экранов следующего поколения существенна в современном мире технологий, так как постоянно открываются новые способы осуществления атак на компьютерные сети, в то время как межсетевые экраны позволяют защищаться от них. Межсетевые экраны следующего поколения же являются их «продолжением» и поэтому позволяют гораздо более эффективно защищаться от различных атак. Также помимо этого они позволяют настраивать инфраструктуру и топологию компьютерной сети, производить мониторинг и диагностику, что делает их инструментом не только для предотвращения атак, но и для администрирования компьютерных сетей.

Организация, Usergate, в которой проходила практика, является российским разработчиком программного обеспечения и микроэлектроники и обеспечивает своими решениями информационную безопасность корпоративных сетей самого разного размера от малого и среднего бизнеса до крупных корпораций с распределенной инфраструктурой. В группу компаний UserGate входят ООО «Юзергейт» (разработка программного обеспечения) и ООО «Катунь Электроника» (разработка в области микроэлектроники) [1].

Практика проходила в подразделении под названием «Tech support», которое занимается решением проблем, возникших у клиентов Usergate, посредством создания «стендов» и эмуляции возникших сбоев и ошибок.

Предполагаемые результатами прохождения данной практики описывает следующий список:

- Понимание основ информационной безопасности, компьютерных сетей и основных интернет-протоколов;
- Умение пользоваться современными гипервизорами (в том числе Oracle VM VirtualBox);
- Умение администрировать межсетевые экраны следующего поколения «Usergate»
- Умение эмулировать ошибки и сбои в компьютерных сетях посредством использование «стендов».

2 Введение в предметную область

Межсетевой экран — это это программный или программно-аппаратный комплекс, предназначенный для контроля и фильтрации проходящего через него сетевого трафика в соответствии с заданными правилами. Например, «брандмауер» в семействе операционных систем Windows можно считать межсетевым экраном. В общем случае межсетевые экраны позволяют лишь осуществлять контроль и фильтрацию трафика для защиты от различных атак (Например, IP-spoofing, SYN-flood).

В то время как **Межсетевой экран нового поколения** (**NGFW** — **N**ext **G**eneration **F**ire**w**all) — это комплексный инструмент, предназначенный для контроля трафика, управления доступом пользователей и приложений, предотвращения атак. Межсетевой экран следующего поколения объединяет в себе функционал антивирусов, брандмауэров и других приложений безопасности. То есть межсетевой экран нового поколения совмещает в себе все возможности межсетевого экрана, но к этому ещё добавляет новый функционал. Также негласным правилом является то что межсетевой экран нового поколения анализирует трафик на всех уровнях модели OSI, в то время как обычный межсетевой экран — только до четвёртого уровня включительно.

3 Принципы работы «Usergate»

«Usergate» является межсетевым экраном [1] со следующими возможностями [2]:

- Системы обнаружения вторжений (IDS/IPS);
- Advanced Threat Protection [2] (Опция);
- Доступ к внутренним ресурсам через SSL VPN Portal;
- Анализ и выгрузка информации об инцидентах безопасности (SIEM);
- Обратный прокси (Reverse proxy);
- Автоматизация реакции на угрозы безопасности информации (SOAR);
- Контроль Приложений L7;

[1] Компания Usergate предоставляет как аппаратные, так и программные решения, однако в рамках практики работа происходила лишь с программным решением — виртуальным межсетевым экраном нового поколения.

[2] Advanced Threat Protection включает в себя фильтрацию по категориям URL Filtering 3.0, морфологический анализ контента, облачный антивирус, поддержку списков Роскомнадзора, модуль блокировки рекламы ADblock.

- Защита почты (Mail Security) [3] (Опция);
- Контроль доступа в интернет;
- Дешифрование SSL;
- Гостевой портал;
- Идентификация пользователей;
- Виртуальная частная сеть (VPN);
- Поддержка АСУ ТП (SCADA);
- Удаленное администрирование;
- Безопасная публикация внутренних ресурсов и сервисов;
- Поддержка концепции BYOD (Bring Your Own Device);
- Поддержка высокой отказоустойчивости и кластеризации.

То есть «Usergate» не только производит анализ и фильтрацию сетевого трафика, но ещё и позволяет организовывать инфраструктуру сети (позволяет настройки правил NAT, выступать в качестве DHCP-сервера и т.д.), производить удалённое администрирование, мониторинг и диагностику трафика, управлять авторизацией пользователей, их правами и ролями и т.д.

4 Создание и использование «стендов»

«Usergate» как виртуальный межсетевой экран нового поколения представлен фактически операционной системой, которая может установлена из ISO-образа. ISO-образ можно импортировать в любом современном гипервизоре (например, OracleVM VirtualBox или VMware Workstation). В рамках практики использовался гипервизор OracleVM VirtualBox.

Для эмуляции работы компьютерной сети необходимо эмулировать всех хостов в сети. В рамках обучения стенд состоял из шести виртуальных машин:

- Виртуальная машина с «Usergate» (**UTM** — **U**nifi**e**d **T**hreat **M**anagement);
- Виртуальная машина на операционной системе Debian 12.4.0, эмулирующая интернет-провайдера (**ISP** — **I**nternet **S**ervice **P**rovider);
- Виртуальная машина на операционной системе Windows Server 2012, эмулирующая сервер некоторой компании, находящийся в локальной сети компании (**DC** — **D**ata **C**enter).

[3] Mail Security включает в себя антиспам, антивирусную проверку почты, поддержку методов фильтрации нежелательной почты.

- Три виртуальные машины на операционной системе Windows-10, две из которых эмулируют клиентов, находящихся в локальной сети некоторой компании (**CLI-A** и **CLI-B**, **CLI** — **Cli**ent), а третий — клиента вне локальной сети компании, но имеющего доступ к локальной сети с помощью Remote Access VPN (**CLI-EXT** — **Cli**ent **Ext**ernal).

Стоит отметить, что конфигурация «стенда» заключается не только в поиске и импорте в гипервизор нужных ISO-образов операционных систем. Для полноценной работы стенда необходимо: осуществить настройку сетевой топологии в самом гипервизоре (указать сколько каждая виртуальная машины будет иметь виртуальных сетевых интерфейсов и какого они будут типа), осуществить настройку каждой виртуальной машины по-отдельности.

CLI-A, **CLI-B** и **DC** имели лишь один виртуальный сетевой интерфейс каждая, при этом интерфейсы этих виртуальных машин находились в одной локальной сети (*LOCAL-NETWORK*) [4]. **UTM** же имела 2 виртуальных интерфейса: один — в виртуальной локальной сети *LOCAL-NETWORK*, а второй — в виртуальной локальной сети *ISP-NETWORK*. **ISP** имела 2 виртуальных интерфейса: один в виртуальной локальной сети *ISP-NETWORK*, а второй виртуальный интерфейс имел тип «bridge», что означает, что он имеет доступ к сетевому пространству «хостовой» операционной системы. **CLI-EXT** имела лишь один интерфейс, у которого был тип «bridge».

На **CLI-A** и **CLI-B** не было никаких настроек поскольку все нужны IP-адреса и доступ к интернету они получали от **UTM**. На **DC** нужно было установить и настроить необходимые сервисы (такие как «Active Directory», «DNS-Manager», центр управления сертификатами и т.д.), а все нужные IP-адреса и доступ в интернет виртуальная машина опять-таки получала от **UTM**. На **ISP** были настроены правила NAT и статические маршруты для доступа в интернет. На **CLI-EXT** был настроен доступ к **UTM** с помощью VPN (указан IP-адрес нужного интерфейса **UTM** и тип подключения). На **UTM** были произведены самые различные настройки:

- Настроена фильтрация контента по протоколам, URL, IP-адресам клиентов;
- Настроены captive-портал и способы авторизации (через captive-портал, «прозрачная» авторизация по протоколу Kerberos);
- Настроен сбор диагностических данных;
- Настроены сценарии при атаках;
- Настроена проверка на писем электронной почты на наличие «вирусов» с помощью протокола ICAP.

[4] Они находились в виртуальной локальной сети гипервизора, но тем не менее они не имели прямого доступа к сетевому пространству операционной системы, на которой был запущен гипервизор.

Данный «стенд» использовался в рамках обучения. После обучения создавались различные «стенды» для решения проблем, возникших у пользователей продуктов Usergate.

5 Заключение

В результате прохождения практики были изучены принципы работы межсетевого экрана следующего поколения «Usergate» и способы его администрирования. Также были получены навыки в создании «стендов» в гипервизоре OracleVM VirtualBox для эмуляции работы компьютерных сетей и межсетевых экранов.

Также был получен опыт работы с литературными источниками и выделения необходимой и полезной информации, а также опыт работы в крупной российской компании наряду с её штатными сотрудниками.

В течение прохождения практики пришлось столкнуться с двумя трудностями: трудность в работе с гипервизором OracleVM VirtualBox (а именно, настройке сетевой топологии); трудность в понимании принципов работы «Usergate» ввиду многоплановости и сложности данного продукта.

Список литературы

[1] *О компании UserGate*. URL: https://www.usergate.com/ru/company/about-us.

[2] *Возможности виртуального межсетевого экрана «Usergate»*. URL: https://www.usergate.com/ru/products/usergate-vm.