Визуализация сетевых атак в задачах подготовки кадров в сфере кибербезопасности

Романова З. А., магистр института кибербезопасности и защиты информации СПбПУ, zinaida.romanova@lanit-tercom.com

Аннотация

В докладе приводится исследование нового подхода для обучения кибербезопасности на основе веб-симулятора компьютерной сети.

Введение

Для проектирования, настройки и тестирования сетей необязательно иметь огромное количество оборудования. Для этих целей существуют различные программные обеспечения, называемые эмуляторами или симуляторами сетей.

Симуляторы, представляют собой программное обеспечение, которое имитирует топологию сети, состоящей из одного или нескольких сетевых устройств.

Эмулятор – это часть программного обеспечения, которая запускает и подключает виртуальные сетевые устройства. Эмуляторы виртуализируют реальные сетевые устройства, которые имеют более "продвинутые" функции, чем устройства, отображаемые симулятором. Поведение виртуального сетевого оборудования в большей степени отражает поведение физического оборудования в реальном мире [1].

Помимо основной функции: построение и тестирование сетей, симуляторы и эмуляторы могут выступать как платформа для обучения сетевым атакам. На данный момент существуют для таких целей киберполигоны, но они рассчитаны на продвинутый уровень знаний и не годятся для изучения базовых вещей в области кибербезопасности. Поэтому было разработано новое решение.

Сетевые симуляторы и эмуляторы

Для того, чтобы визуализировать сетевые атаки нужно было выбрать платформу, которая отвечает ряду критериев:

1. Открытый исходный код;
2. Веб-версия;

3. Расширенный набор возможностей (например, можно вручную задавать MAC-адрес);
4. Доступен для использования.

Проанализировав известные симуляторы и эмуляторы на соответствующие критерии была составлена Таблица 1.

Симулятор/эмулятор	1	2	3	4
Cisco Packet Tracer	-	-	+	-
NS3	+	-	-	+
EVE-NG	-	+	+	-
Mininet	+	-	+	+

Таблица 1: Критерии симуляторов/эмуляторов

Таким образом, Mininet подошел по ряду критериев и был взят за основу нового симулятора.

Miminet

Miminet – отечественный веб-симулятор компьютерной сети для образовательных целей, который реализован на базе эмулятора mininet. Проект находится в процессе разработки с открытыми исходными кодами на кафедре Системного программирования в Санкт-Петербургском государственном университете при поддержке компании Yadro. Отличительными особенностями симулятора являются:

- не нужно устанавливать ПО, работа ведется в веб-приложении;
- использует пакетный режим;
- нет привязки к конкретным моделям устройств;
- Backend mininet позволяет добавлять различные возможности для симулятора, например, ручная настройка MAC-адресов;
- подходит для демонстрации «поломанных» сетей, например, добавление двух устройств в одной подсети с одинаковыми IP-адресами;
- гибкий программный код, который позволяет расширять возможности симулятора.

Благодаря расширенному набору возможностей этого симулятора появилась возможность визуализировать сетевые атаки, для этого был отобран перечень тех, которые наиболее известны.

Сетевые атаки

ARP spoofing – разновидность сетевой атаки типа MITM (англ. Man in the middle), применяемая в сетях с использованием протокола ARP. Атака

основана на недостатках протокола ARP. При использовании в распределённой вычислительной сети алгоритмов удалённого поиска существует возможность осуществления в такой сети типовой удалённой атаки «ложный объект распределённой вычислительной системы». Анализ безопасности протокола ARP показывает, что, перехватив на атакующем узле внутри данного сегмента сети широковещательный ARP-запрос, можно послать ложный ARP-ответ, в котором объявить себя искомым узлом (например, маршрутизатором), и в дальнейшем активно контролировать сетевой трафик дезинформированного узла, воздействуя на него по схеме «ложный объект РВС» [2].

Dos – «отказ в обслуживании». Это атака со стороны одиночного IP-адреса, связанная с отправкой нелегитимного трафика и приводящая к неработоспособности системы, что, в свою очередь, приводит к простою площадки или сервиса и потере финансовой составляющей.

DDos – «распределенный отказ в обслуживании». Отличие данной атаки от описанной выше в том, что отправка трафика в данном случае будет идти с различных IP-адресов. Этот аспект приводит к сложности защиты сервисов [3].

Визуализация сетевых атак

Все три сценария были реализованы в веб-приложении Miminet, пример DoS-атаки (см. Рис. 1):

1. Хост1 злоумышленник;
2. Хост2 сервер с данными;
3. Хост3 пользователь.

- хост1 посылает подряд 10 пакетов (каких-то запросов) на свитч, со свитча 10 пакетов идут на хост2 (время обработки 1 пакета 1 с);
- хост3 отправляет 1 пакет (настоящий запрос) на свитч, со свитча 1 пакет идет на хост2, хост2 не отвечает, тк занят обработкой запросов от хоста1 (атакующего).

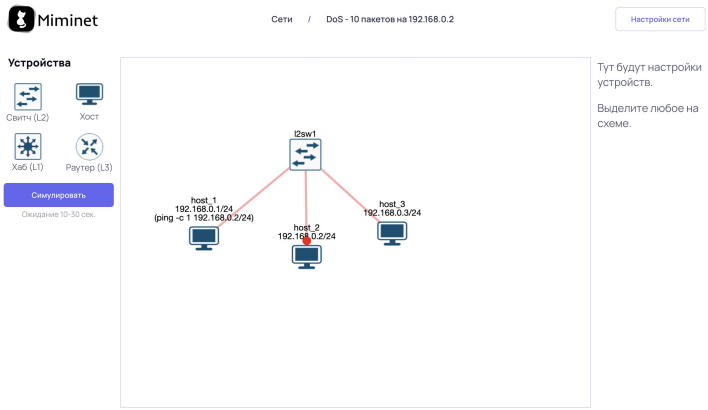

Рисунок 1: Реализация DoS-атаки

Чтобы проанализировать насколько новый подход, основанный на визуализации сетевых атак на базе веб-приложения Miminet эффективен, было принято решение провести два эксперимента: провести лекцию в старом формате с устными объяснениями материала по сетевым атакам с последующим тестированием остаточных знаний, во втором случае уже с применением визуализированных сценариев атак и также с последующим тестированием.

Были получено, что средняя оценка за тестирование в первом случае равно 3.8 по 5-ти бальной шкале, а во втором случае средний показатель равен 4.2. Помимо этого была получена обратная связь от студентов, в которой было отмечено, что визуальный вариант сетевых атак намного проще воспринимается.

Заключение

В докладе представлен новый подход, который поможет более продуктивно подготавливать кадры в области кибербезопасности. В дальнейшем планируется активно развивать возможности и инструменты веб-приложения Miminet, чтобы можно было охватить намного больше теоретического материала, который можно визуализировать.

Литература

1. СЕТЕВЫЕ СИМУЛЯТОРЫ И ЭМУЛЯТОРЫ // Современные наукоемкие технологии URL: https://top-technologies.ru/ru/article/view?id=38134 (дата обращения: 10.03.2023).

2. ARP спуфинг // Securitylab.ru by Positive Technologies URL: https://www.securitylab.ru/glossary/arp_spoofing_arp_poisoning/ (дата обращения: 15.03.2023).
3. DOS и DDoS-атаки: понятие, разновидности, методы выявления и защиты // Compconfig.ru URL: https://compconfig.ru/net/dos-i-ddos-ataki.html (дата обращения: 15.03.2023).