УДК 004.056.53

АНАЛИЗ И ЗАЩИТА ОТ DDOS-АТАК В СЕТЯХ НА БАЗЕ GNS3

Самаке Б.А.

гр.267241

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Научный руководитель: Белоусова Е.А. – кандидат технических наук

Аннотация. В данной статье рассматривается один из наиболее распространенных типов атак, который является DDoS-атак, которая направлена на перегрузку серверов и сетей большим объемом сетевого трафика. В данной статье будет проведен анализ DDoS-атак и рассмотрены способы их защиты в сетях, построенных на базе симулятора сетей GNS3.

Ключевые слова: DDoS-атак, Hping3, wireshark, IP-адрес, локальная сеть.

Введение. С динамическим развитием технологий информационной безопасности, компьютерные атаки становятся все более сложными и разрушительными. Одним из наиболее распространенных типов атак является DDoS-атаки, которые направлены на нарушение нормального трафика сервера. Они направлены на то, чтобы перегрузить устройства, службы или сеть предполагаемой цели фальшивым интернет-трафиком, сделав их недоступными для пользователей [1]. В данной статье будет проведен анализ DDoS-атак построенных на базе симулятора сетей GNS3.

Рассмотрим сценарий атаки, для выполнения DDos-атак, воспользуемся сетевым инструментом Hping3, который является утилитом командной строки для создания и отправки пользовательских пакетов TCP/IP. Это универсальный инструмент, позволяющий выполнять различные задачи. А в качестве анализатора трафика для анализа DDos-атаки воспользуемся инструментом wireshark.

Для проверки DDoS-атак необходимо было смоделировать локальную сеть. Для этого был мы воспользовались программой GNS3. Он основан на Qemu и Dynamips и является графическим интерфейсом для создания локальных сетей с использованием Qemu. В GNS3 устройства разных производителей можно добавлять самостоятельно. Также GNS3 предоставляет более точную представление в настройки оборудований [2].

На рисунке 1 представлена модель локальной сети в программном эмуляторе сети GNS3. В смоделированной сети выделено четыре виртуальные сети (VLAN),один веб сервер на котором будет произведена атака, а также оборудование который будет проводить DDos-атаку с помощью Hping3.

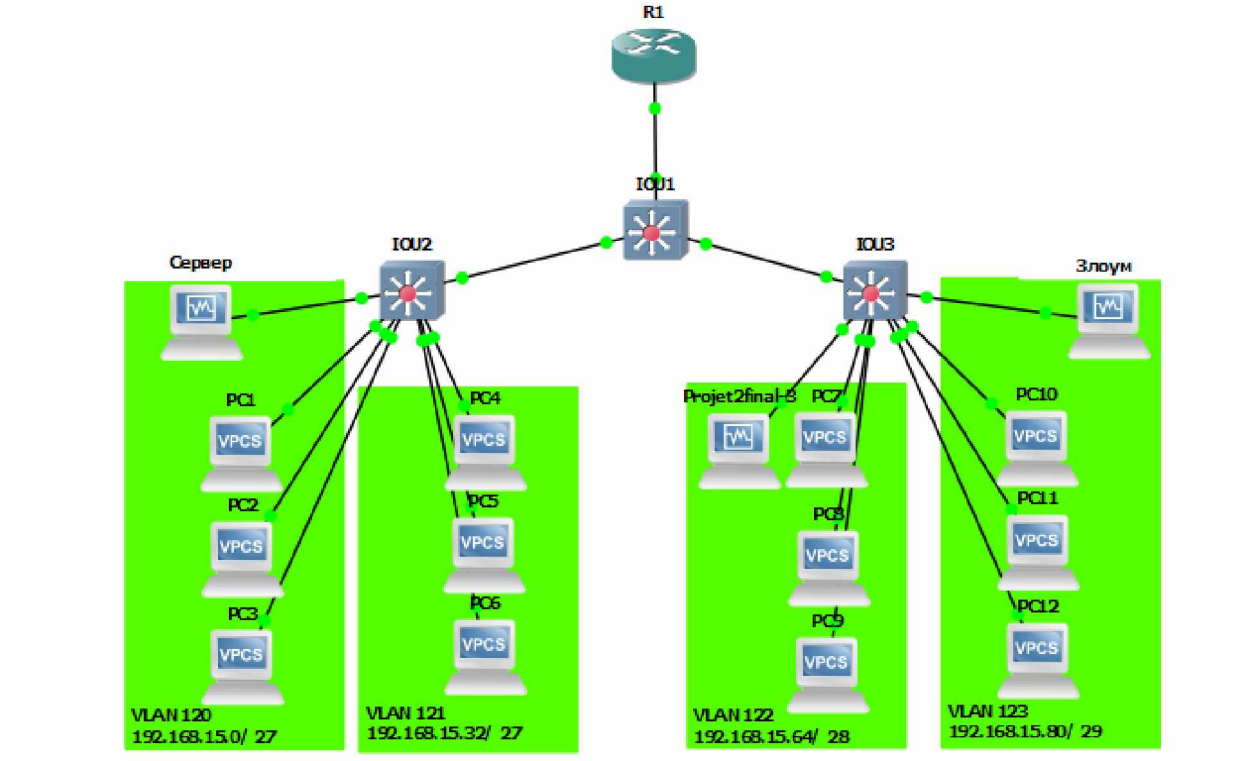

Рисунок 1 – Модель локальной сети для моделирования атаки

После построение модели, на рисунке 2 представлена команда с помощью, которого будет сгенерировано большое количество пакетов ICMP на указанный IP адрес.

```
glpi@Glpi:~$ sudo hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood 192.168.15.2
[sudo] Mot de passe de glpi :
HPING 192.168.15.2 (enp0s8 192.168.15.2): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Рисунок 2 – команда для генерирование большого количества пакетов ICMP

После генерирование такого большого количество пакетов, сервер будет перегрузон этими пакетами и выйдет из строя, что приведет к невозможности другим пользователям получать доступ к серверу. Рисунок 3 покаживает аномальный трафик, который может является признаком DDoS-атаки.

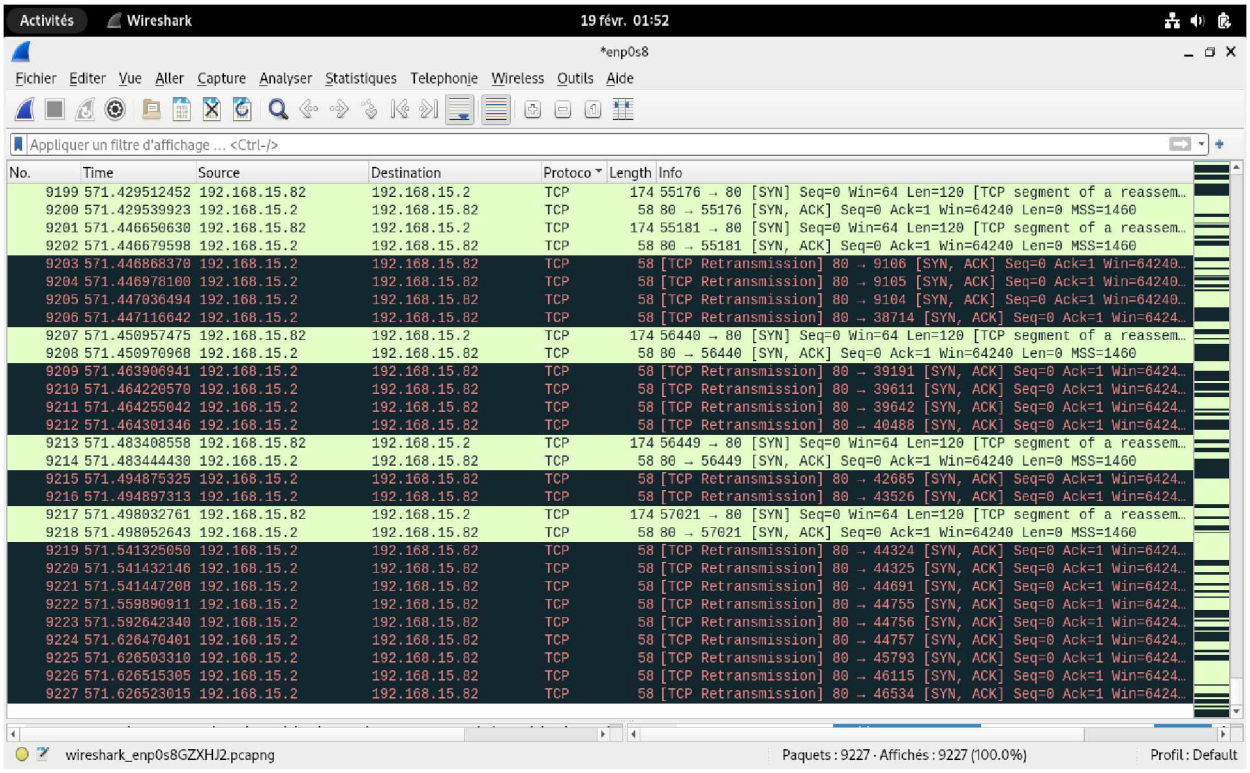

Рисунок 3 – Признак DDoS-атаки

На рисунке ниже представлен результат успешной DDoS-атаки, после которого нет доступа к серверу.

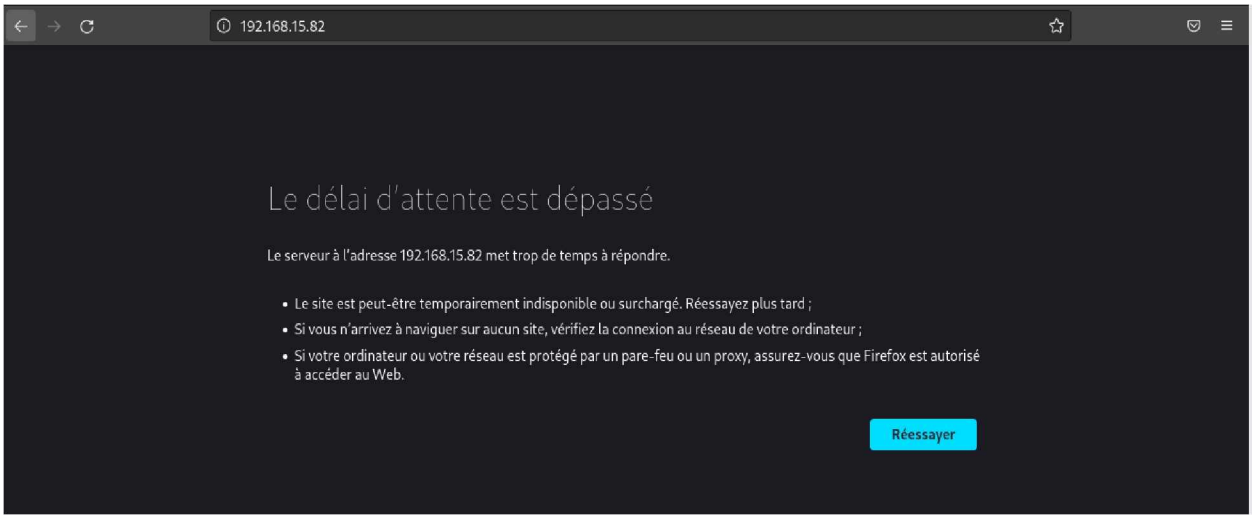

Рисунок 4 – Результат выполнение DDoS-атак

Существует несколько методов защиты от DDoS-атак, один из способов защиты - это использование механизмов обнаружения и фильтрации DDoS-трафика на уровне сети. Для этого можно использовать специализированные устройства, такие как фаерволы и IPS/IDS, которые могут распознавать и блокировать подозрительный трафик.

Другим методом защиты от DDoS-атак является распределение нагрузки на несколько серверов или узлов сети. Это позволяет снизить вероятность отказа в обслуживании в случае DDoS-атаки путем равномерного распределения нагрузки между несколькими узлами сети.

Заключение. DDoS-атаки представляют серьезную угрозу для сетей и серверов, поэтому необходимы соответствующие меры защиты. На базе симулятора сетей GNS3 можно провести анализ и защиту от DDoS-атак, используя различные методы, такие как обнаружение и фильтрация трафика, распределение нагрузки и алгоритмы маршрутизации. Эти методы помогут снизить вероятность успешной DDoS-атаки и обеспечить стабильную работу сети.

Список использованных источников:

1. Богомолова Л.В. КЛАССИФИКАЦИЯ DDOS-АТАК И ИХ РЕАЛИЗАЦИЯ. – Режим доступа : КЛАССИФИКАЦИЯ DDOS-АТАК И ИХ РЕАЛИЗАЦИЯ (cyberleninka.ru) . – Дата доступа : 19.02.2024.

2. Кулябов Д. С. Средства моделирования сетей для целей обучения– режим доступа: Средства моделирования сетей для целей обучения | Д. С. Кулябов (yamadharma.github.io). – Дата доступа: 25.03.2025.

UDC 004.056.53

ANALYSIS AND PROTECTION AGAINST DDOS ATTACKS IN GNS3-BASED NETWORKS

Samake B.A.

gr.267241

Belarusian State University of Informatics and Radioelectronics. Minsk. Republic of Belarus

Belousova E.S. – PhD (Tech.), associate professor at the information security department

Annotation This article considers one of the most common types of attacks. which is DDoS attacks. which are aimed at overloading servers and networks with a large volume of network traffic. This article will analyze DDoS attacks and consider ways of their protection in networks built on the basis of the GNS3 network simulator.

Keywords: DDoS attack. Hping3. wireshark, IP address, local area network

Annotation. The materials of the report discuss the development of a system for protecting a dedicated (protected) room from leakage of speech information via a vibroacoustic channel. The development of this system includes an integrated approach to ensuring the protection of speech information and is associated with the use of modern technologies and methods, which will help increase the level of security of secret negotiations.

Keywords: protected room, speech information, active protection, vibroacoustic channel.