УДК 004.77: 372.862

МОДЕЛИРОВАНИЕ АТАК НА КОМПОНЕНТЫ СЕТЕВОЙ ИНФРАСТРУКТУРЫ СРЕДСТВАМИ ГРАФИЧЕСКОГО СЕТЕВОГО ЭМУЛЯТОРА GNS3

А.М. Кадан[1], Н.В. Белоголовая[2]

[1]к.т.н., доцент, Гродненский государственный университет им. Янки Купалы, г.Гродно, Беларусь, kadan@mf.grsu.by
[2]студентка 4 курса, Гродненский государственный университет им. Янки Купалы, г.Гродно, Беларусь, belogolovay_nv_18@mf.grsu.by

При изучении методов и средств защиты компьютерных сетей существенные затруднения вызывает практическая часть исследования атак: построение топологии сети, настройка интерфейсов, взаимодействие сетевых протоколов, моделирование атак на сетевую инфраструктуру и организация противодействия им. Причины этому - высокая стоимость оборудования и сложность создания профильных учебных лабораторий. Используя эмуляторы компьютерных сетей, такие эксперименты можно проводить удобнее и экономичнее, чем на реальном оборудовании. В статье представлены примеры использования Графического Сетевого Эмулятора-3 (GNS-3) для создания специализированного контента в задачах моделирования трех типов сетевых атак. Разработанные модели могут быть использованы при подготовке специалистов по защите информации как в режиме очного так и дистанционного обучения.

Ключевые слова: виртуальная лабораторная среда; моделирование атак; GNS3; Graphical Network Simulator; Графический Сетевой Эмулятор; информационная безопасность; защита информации; дистанционное обучение.

SIMULATION OF ATTACKS ON NETWORK INFRASTRUCTURE COMPONENTS USING GNS3 GRAPHIC NETWORK EMULATOR GNS3

A.M. Kadan [a], N.V. Belogolovaya [b]

[a)]Candidate of technical sciences, assistant professor Yanka Kupala State University of Grodno, Belarus, kadan@mf.grsu.by
[b)]Student 4 courses of Yanka Kupala State University of Grodno, Belarus, belogolovay_nv_18@mf.grsu.by

When studying technologies and methods for protecting computer networks, the main difficulties are caused by the practical part of the study of attacks: building a network topology, configuring interfaces, interaction of network protocols, modeling attacks on network infrastructure and organizing counteraction to them. The reasons for this are the high cost of equipment and the complexity of creating specialized educational laboratories. Thanks to computer network emulators, such experiments can be carried out much more conveniently and economically than on real equipment. The article presents examples of

using the Graphical Network Emulator-3 (GNS-3) to create specialized content in the tasks of modeling three types of network attacks. The developed models can be used in the training of information security specialists both in full-time and distance learning.

Keywords: virtual laboratory environment; attack simulation; GNS3; Graphical Network Simulator; information security; information protection; distance learning.

Введение

При изучении технологий и методов защиты компьютерных сетей существенные затруднения вызывает практическая часть исследования атак на телекоммуникационные системы: построение топологии сети, настройка интерфейсов, взаимодействие сетевых протоколов, моделирование атак на сетевую инфраструктуру и организация противодействия им. Причинами этому являются высокая стоимость оборудования и сложность создания профильных учебных лабораторий. Для преодоления такого положения рядом исследователей предлагались проекты создания современных образовательных сред и специализированных лабораторий, ориентированных на формирование у специалистов по кибербезопасности и защите информации практических навыков тестирования на проникновение [1] и по поиску и устранению угроз в рамках аудита информационных систем [2, 3]. Создание подобных лабораторий в рамках облачного кластера на платформе OpenNebula изучались в работах [4, 5]. Развиваются проекты по тестированию на проникновение, представленные в работах [6, 7]. Интересен опыт работ по геймификации на платформе CTF учебного процесса в области компьютерной безопасности [8, 9].

Использование виртуальных лабораторий позволяет сформировать у студентов практические навыки использования методов тестирования на проникновение на примерах объектов различных уровней сложности, а также обеспечивает возможность быстрого изменения инфраструктуры и свойств тестируемых объектов.

1. Методология исследования

1.1. Особенности и возможности GNS-3

GNS3 - это графический эмулятор сети, который позволяет смоделировать виртуальную сеть из маршрутизаторов и виртуальных машин [9]. Работает практически на всех платформах. Эффективен при создании стендов на десктоп машинах. Представляет собой кроссплатформенную с открытым исходным кодом утилиту, которая основана на популярных продуктах - Dynamips (CISCO IOS эмулятор), Dynagen (текстовый интерфейс для вышеупомянутой Dynamips) и Pemu (Cisco PIX эмулятор). GNS3 предоставляет простой в использовании графический пользовательский

интерфейс, а также ряд других возможностей этих инструментов. В зависимости от аппаратной платформы, на которой будет использоваться GNS3, возможно построение комплексных проектов, состоящих из маршрутизаторов Cisco, Cisco ASA, Juniper, а также серверов под управлением сетевых операционных систем.

Эмулятор GNS3 достаточно требователен к ресурсам. Требования к ресурсам для ОС Windows при создании сложных сред с большим количеством устройств представлены в таблице1:

Таблица 1 – Требования к ресурсам для ОС Windows для работы GNS3

Элемент	**Требование**
Операционная система	Windows 7 (64 бит) или новее
Процессор	4 или более логических ядра - AMD-V / RVI Series или Intel VT-X / EPT
Виртуализация	Требуются расширения виртуализации. Возможно, вам потребуется включить это через BIOS вашего компьютера.
Объем памяти	16 ГБ RAM
Место хранения	Твердотельный накопитель (SDD) с 35 ГБ свободного места
Дополнительные замечания	Виртуализация устройств требует значительных ресурсов процессора и памяти. .

1.2. Проблемы использования GNS3

К общим достоинствам ‘эмулятора GNS3 относят [10]:

- Возможность создания сложных топологий сети высокого качества.
- Эмуляция многих Cisco IOS маршрутизаторов (IPS, PIX и ASA брандмауэры, JUNOS) и конечных устройств. Если вспомнить Cisco Packet Tracer, то там в качестве конечных устройств были доступны клиентские компьютеры или сервера с очень ограниченным функционалом. В GNS3 возможно добавление полноценного компьютера с Windows 7 или Ubuntu. Возможно использование в схеме Windows Server или RedHat, Linux-систем, а главное полных образов систем Cisco.
- Моделирование Ethernet, ATM и Frame Relay переключателей.
- Подключение моделируемой сети в реальную сеть. Таким образом возможно проверить в работе установку VPN клиента на рабочую станцию, аутентификацию пользователей через сервер AAA, использование настоящий браузер при подключении к Интернету.
- Захвата пакетов с помощью утилиты Wireshark

К недостаткам GNS3 относится следующее [10]:

- Сильная нагрузка на CPU компьютера (не более 10 маршрутизаторов на 1 ПК)
- Слабая работа на L2 уровне сети. Дело в том, что в реальных коммутаторах большое кол-во ASIC-микросхем, которые пока что невозможно эмулировать на обычном компьютере. Именно эти ASIC-микросхемы обеспечивают огромную скорость обработки пакетов. Маршрутизаторы же работают на основе процессора, который похож на процессор обычного компьютера, поэтому проблем с эмуляцией маршрутизаторов не возникает.

2. Результаты и их обсуждение

В ходе изучения возможностей симулятора GNS3 и различных сетевых протоколов были рассмотрены три модели (кейса) классических сетевых атак. Данные кейсы имеют как собственную академическую ценность, так и могут быть использованы в проведении соревнований в формате CTF, весьма популярных у специалистов по кибербезопасности и защите информации [8, 9]. К сожалению, в силу ограничений объема материала статьи, вынуждены ограничиться кратким описанием кейсов.

Учитываю значительную ресурсоемкость пакета GNS3, предложенные решения развернуты в облачном кластере Гродненского государственного университета им.Янки Купалы, что позволяет работать с ними вне зависимости от возможностей компьютерного оборудования студентов.

2.1. Кейс 1: Уязвимости SNMP и брутфорс паролей по SSH

В топологию кейса включены такие устройства как маршрутизатор R1, коммутатор Switch1 и атакующая машина злоумышленника с установленной на ней операционной системой KaliLinux (см. рис. 1).

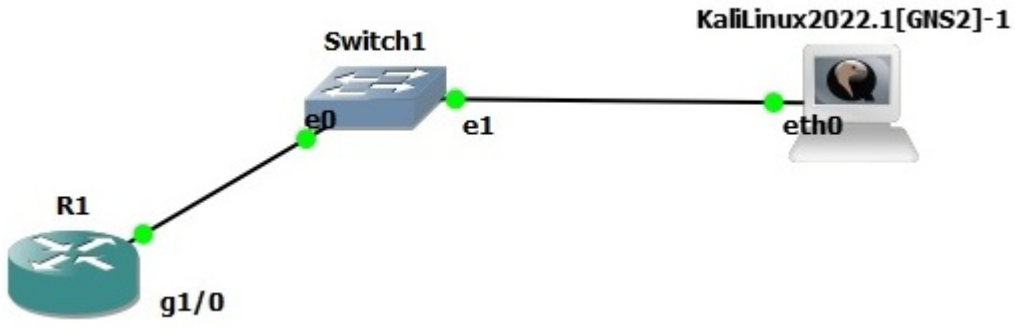

Рисунок 1 – Топология сети кейса «Уязвимости SNMP и брутфорс паролей по SSH»

С помощью уязвимости протокола SNMP возможно получение конфигурации операционной системы маршрутизатора, что позволит определить пользователей системы. Далее производим поведения брутфорс атаку по SSH с целью выяснения паролей пользователей. После проведения успешной атаки производиться настройка защиты от используемых уязвимостей.

2.2. Кейс 2: Моделирование ARP-спуфинга

Для моделирования ARP-спуфинга и защиты от него требуется смоделировать простейшую сеть (см. рис. 2). Сеть будет включать в себя маршрутизатор (в данном примере Cisco 7200 – R1), коммутатор ((Cisco Catalyst – SW1), два конечных устройства (laptop, KaliLinux).

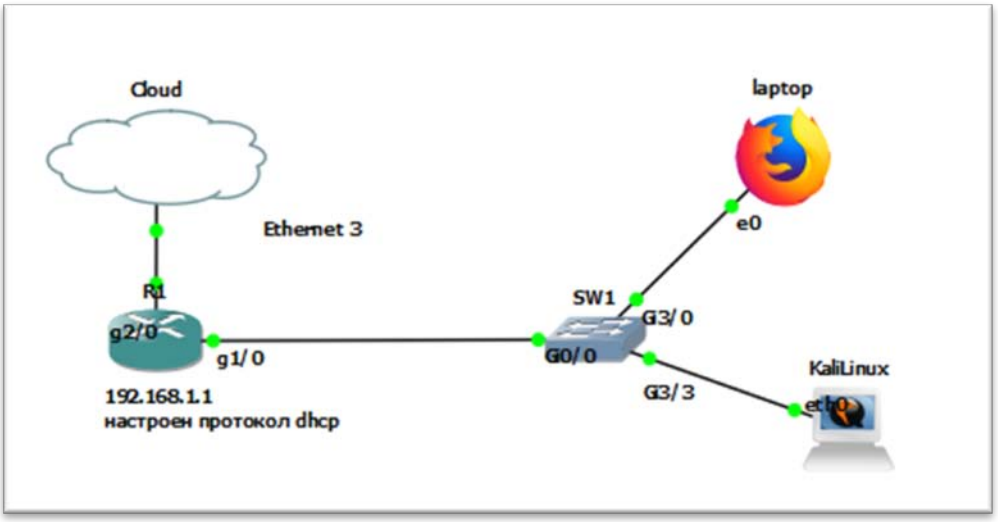

Рисунок 2 – Топология сети кейса «Моделирование ARP-спуфинга»

В данной модели требуется, используя недостатки протокола ARP, произвести перехват трафика, исходящего от laptop к маршрутизатору, используя утилиты, установленные в системе KaliLinux. Далее необходимо получить подтверждение перехвата трафика и настроить защиту от данной атаки.

2.3. Кейс 3: Базовые уязвимости серверов и коммутаторов

Для изучения базовых уязвимостей серверов и коммутаторов моделируется топология сети (см. рис. 3), включающая маршрутизатор R1, коммутатор CiscoIOSwl), три конечных устройства (Metasploitable, KaliLinux, Toolbox). На маршрутизаторе должен быть настроен DHCP с диапазоном адресов 192.168.1.2-192.168.1.253. На R1 так же настроен telnet, а на коммутаторе ssh.

Задача кейса разделяется на две отдельные задачи. Цель первой задачи состоит в том, чтобы, используя уязвимости, найденные на устройстве Metasploitable, получить root доступ к системам машины и найти флаг. Цель второй задачи в том, чтобы путем переполнения таблицы MAC-адресов коммутатора заставить его рассылать получаемые им пакеты широковещательно. В одном их таких пакетов скрыт флаг. Пакет с флагом отправляется через определенное время из машины Toolbox к маршрутизатору R1. Также возможно использование зеркалирования портов вместо переполнения таблицы MAC-адресов коммутатора.

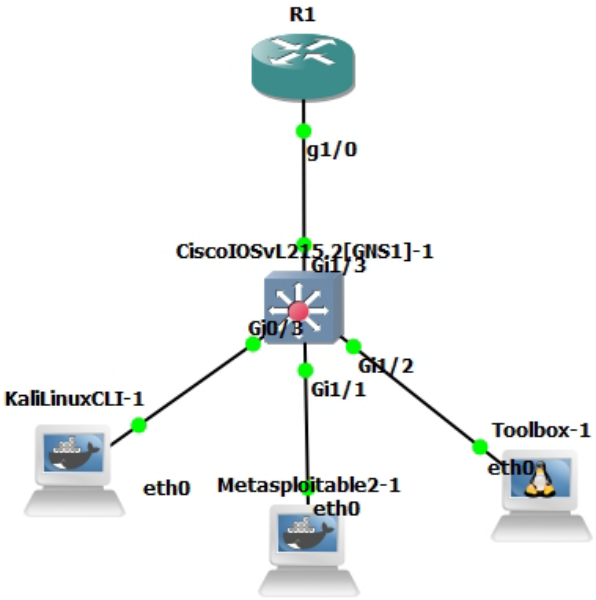

Рисунок 3 – Топология сети кейса «Базовые уязвимости серверов и коммутаторов»

Заключение

Существенным преимуществом GNS3 является возможность использования реального оборудования и операционных систем, инструментов KaliLinux, а также эмуляция сетевых устройств Cisco и возможность выхода в реальную сеть. Глобальным недостатком GNS3 является его большая ресурсоемкость, однако предложенное решение, использующее ресурсы облачного кластера университета, позволяет его минимизировать. Несомненно, применение GNS3-моделей в учебном процессе положительно скажется на обучении студентов, позволит повысить уровень их профессиональных компетенций в вопросах сетевых технологий и компьютерной безопасности. Также надо отметить, что использование GNS-моделей позволяет создать новый класс задач для использования в соревнованиях формата CTF, столь популярных среди специалистов по кибербезопаснсти.

Библиографические ссылки

1. Тестирование на проникновение / Портал по информационной безопасности. ООО «ПентестИТ», 2016. URL: https://www.pentestit.ru/audit/penetration-testing (дата обращения: 04.09.2022).
2. Макаренко С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. СПб.: Наукоемкие технологии, 2018. 122 с. URL: https://elibrary.ru/item.asp?id=36445362 (дата обращения: 04.09.2022).
3. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2018. – 272 с. ISBN 978-5-4461-0662-2.
4. Кадан, А.М., Доронин, А.К. Облачные лаборатории для задач тестирования на проникновение // Современные информационные технологии и ИТ-образование. 2016. №3-1. URL: https://cyberleninka.ru/article/n/oblachnye-laboratorii-dlya-zadach-testirovaniya-na-proniknovenie (дата обращения: 04.09.2022).
5. Кадан А.М. Изучение методов тестирования на проникновение в подготовке специалистов по защите информации / А.М. Кадан, А.К. Доронин // Информатизация образования. 2016. № 2. С. 3–11. URL: https://elibrary.ru/item.asp?id=32844238 (дата обращения: 10.10.2020).
6. Жданов Н.С., Матерухин А.В. Использование виртуальной лабораторной среды для обучения студентов навыкам тестирования на проникновение. Безопасность информационных технологий, [S.l.], v. 27, №. 4, p. 95–107, 2020.
7. Buchanan, William & Ramsay, Bruce & Macfarlane, Richard & Smales, Adrian & Russell, Gordon & (Jr, Bill. (2015). Teaching Penetration Testing and Malware Analysis within a Cloud-based Environment. URL: https://www.researchgate.net/publication/281030350_Teaching_Penetration_Testing_and_Malware_Analysis_within_a_Cloud-based_Environment (дата обращения: 04.09.2022).
8. Кобилев М.А. Опыт создания интерактивной образовательной платформы на основе инструментария соревнований CTF / М.А. Кобилев, Д.С. Зеленский, Е.С. Абрамов // Информационное противодействие угрозам терроризма. 2015. № 24. С. 321–328. URL: https://elibrary.ru/item.asp?id=23603864 (дата обращения: 04.09.2022).
9. Беззубик Г.А., Базыльчик А.П., Кадан А.М. Соревнования в формате CTF как элемент геймификации при подготовке специалистов по кибербезопасности / Технические средства защиты информации: тез. докл. XX Белорусско-российской науч.-техн. конф. (Республика Беларусь, Минск, 7 июня 2022 года) / редкол. : Т.В. Борботько [и др.]. Минск : БГУИР, 2022. С.20–21.
10. The software that empowers network professionals [Электронный ресурс] Сайт проекта GNS-3, 2022. URL: https://www.gns3.com (дата обращения: 04.09.2022).