ОЦЕНКА ЗАЩИЩЕННОСТИ И ПРАКТИЧЕСКИЕ МЕТОДЫ ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ КОРПОРАТИВНЫХ МЕЖСЕТЕВЫХ ЭКРАНОВ НА ПРИМЕРЕ CHECK POINT T-110

Седляр А.С., Боздаг Бора, студенты гр.361402

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

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. В работе проведена комплексная оценка защищенности аппаратного межсетевого экрана корпоративного класса Check Point T-110. Описан процесс развертывания испытательного стенда и инициализации устройства в ОС Gaia. Проведен анализ устойчивости системы к ряду критических уязвимостей, включая CVE-2024-24919 и CVE-2024-6387. В ходе экспериментально-практического исследования выявлены условия реализации атаки типа IP-спуфинг при стандартных настройках политик безопасности. Предложены практические методы эксплуатации данной уязвимости и алгоритм ее нейтрализации с использованием встроенных механизмов Anti-Spoofing. Полученные результаты могут быть использованы при проектировании защищенных корпоративных сетей.

Ключевые слова. Информационная безопасность, межсетевой экран, Check Point T-110, ОС Gaia, оценка защищенности, уязвимость, CVE, сетевая атака, IP-спуфинг, эксплуатация уязвимостей, Anti-Spoofing, сетевой периметр, аудит безопасности.

Актуальность защиты периметра корпоративных сетей в современных условиях обусловлена постоянным усложнением киберугроз, что требует внедрения высоконадежных решений для обеспечения информационной безопасности. Одним из признанных лидеров на рынке средств сетевой защиты выступает оборудование компании Check Point Software Technologies, межсетевые экраны которой широко применяются для глубокой фильтрации трафика и предотвращения вторжений. Целью данной работы является проведение комплексного аудита безопасности аппаратного межсетевого экрана Check Point T-110 для оценки уровня его устойчивости к актуальным векторам атак.

В качестве объекта исследования рассматривается аппаратный межсетевой экран Check Point T-110, функционирующий под управлением специализированной операционной системы Gaia R80.40. Испытательный стенд был развернут путем аппаратного сброса устройства до заводских настроек и первоначальной инициализации через консоль FTW (First Time Wizard), при этом управление конфигурацией осуществлялось посредством клиентского программного обеспечения SmartConsole. С целью всестороннего аудита безопасности проведена проверка устойчивости объекта к актуальным угрозам путем выявления ряда критических уязвимостей, зафиксированных в базе CVE [1]. В ходе тестирования попытки эксплуатации CVE-2024-24919, связанной с произвольным чтением файлов (Path Traversal), а также CVE-2023-28130, допускающей внедрение команд через механизмы обработки DNS, не увенчались успехом. Отсутствие реализации данных векторов атак обусловлено спецификой конфигурации испытательного стенда, в частности, ограничением доступа к веб-интерфейсу управления, что минимизирует поверхность атаки. Аналогичные результаты были получены при анализе защищенности от уязвимости CVE-2024-6387 (regreSSHion). Исследование показало, что в операционной системе Gaia задействована версия OpenSSH 7.2p1, которая не входит в диапазон версий, подверженных данной бреши в защите, что свидетельствует об устойчивости системы к удаленной эксплуатации в процессе аутентификации. Дополнительно была проанализирована вероятность проведения атаки типа DLL Hijacking через клиентское приложение SmartConsole (CVE-2020-6024). Установлено, что используемая сборка программного обеспечения уже содержит необходимые исправления, блокирующие возможность подмены динамических библиотек. В итоге проведенная оценка подтвердила эффективность встроенных механизмов защиты и актуальность применяемых патчей безопасности для рассматриваемого оборудования.

Несмотря на устойчивость системы к известным программным уязвимостям, было выдвинуто предположение о возможности обхода защиты на сетевом уровне через IP-спуфинг. Теоретической основой реализации атаки данного типа является преднамеренная подмена адреса источника в IP-пакете с целью обхода политик контроля доступа или имитации трафика от доверенного узла сети [2]. Для практической проверки уязвимости использовалась сетевая утилита hping3 в ОС Kali Linux, предназначенная для генерации произвольных пакетов и анализа сетевых стеков. В ходе эксперимента с помощью hping3 был сформирован ICMP-пакет, в котором посредством параметра -a был указан IP-адрес, принадлежащий сегменту доверенной внутренней сети. При этом пакет физически отправлялся со стороны внешнего интерфейса межсетевого экрана. Тестирование показало, что при стандартной конфигурации политик безопасности устройство беспрепятственно пропускает поддельные пакеты, если они формально соответствуют разрешающим правилам фильтрации. Вследствие отсутствия автоматического сопоставления физического интерфейса получения пакета с его исходным адресом становится возможным проведение несанкционированного сканирования от имени легитимного хоста (рисунок 1).

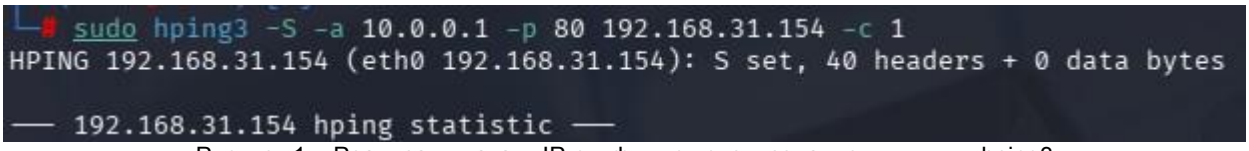

Рисунок 1 – Реализация атаки IP-спуфинг с использованием утилиты hping3

В отличие от угроз, связанных с программными ошибками в коде сервисов (CVE), нейтрализация выявленной проблемы требует не установки патчей, а корректной архитектурной настройки параметров безопасности. В среде SmartConsole для устранения данной уязвимости была задействована функция Anti-Spoofing [3]. Исправление конфигурации осуществлялось согласно следующему алгоритму: в свойствах конкретного сетевого интерфейса в разделе “Topology” активировался механизм “Perform Anti-Spoofing based on interface topology”, после чего указывалась конкретная сеть, закрепленная за данным интерфейсом (рисунок 2). Вследствие активации указанных настроек и последующей инсталляции политики межсетевой экран начал выполнять проверку соответствия входящего интерфейса и адреса источника пакета. Повторная попытка генерации трафика посредством hping3 привела к немедленной блокировке пакетов на уровне ядра ОС Gaia. Это позволяет обеспечить целостность сетевого периметра и исключить возможность эксплуатации доверительных отношений между узлами сети на основе IP-адресации [4].

Рисунок 2 – Активация функции Anti-Spoofing в среде SmartConsole

Проведенное исследование показало, что аппаратный межсетевой экран Check Point T-110 обладает высоким уровнем базовой защищенности на уровне ядра операционной системы и используемых версий программных компонентов, что подтверждается устойчивостью устройства к ряду актуальных критических уязвимостей (CVE). В то же время выявлено, что обеспечение безопасности от сетевых атак, связанных с подменой идентификационных данных (IP-спуфинг), требует обязательной экспертной настройки политик сетевой топологии и ручной активации механизмов Anti-Spoofing администратором. В итоге гарантированная защита корпоративного периметра достигается только при сочетании штатных обновлений безопасности и корректной конфигурации функций контроля трафика.

Список использованных источников:

1. CVE - CVE [Электронный ресурс] / CVE Program. – Режим доступа: https://www.cve.org/. – Дата доступа: 06.04.2026.

2. IP Spoofing: что это и как работает [Электронный ресурс] / АО «Лаборатория Касперского». – Режим доступа: https://www.kaspersky.ru/resource-center/threats/ip-spoofing. – Дата доступа: 07.04.2026.

3. Check Point Security Gateway Support for Anti-Spoofing [Electronic resource] / Check Point Support Center. – Mode of access: https://support.checkpoint.com/results/sk/sk180814. – Date of access: 07.04.2026.

4. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. пособие / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2020. – 992 с.