ПРОФЕССИОНАЛИТЕТ, 2025, № 4 (008)

УДК *004.7:004.056*

И.К. Селиванов [1], Д.А. Леденёв [1]

[1]*ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация*

ТЕСТИРОВАНИЕ ШТАТНОЙ ЗАЩИТЫ СЕТЕВЫХ УСТРОЙСТВ L2+ СРЕДСТВАМИ NMAP ПРИ АКТИВНОМ КОНСОЛЬНОМ ДОСТУПЕ

Аннотация. В статье рассматривается вопрос оценки эффективности штатных механизмов защиты сетевых устройств уровня L2+ при проведении сетевого сканирования средствами утилиты nmap. Актуальность работы обусловлена широким использованием управляемых сетевых устройств в корпоративных и учебных сетях, а также необходимостью минимизации поверхности атаки на уровне интерфейсов управления без применения специализированных средств защиты. Особое внимание уделяется анализу management-плоскости устройств в условиях активного консольного доступа администратора.

Целью исследования является практическая оценка сетевой доступности сервисов управления и состояния сетевых портов в начальной конфигурации сетевых устройств различных производителей. В качестве объектов исследования использовались управляемый коммутатор MikroTik CRS326-24G-2S+ и маршрутизаторы Cisco серий 1900 и 800. Экспериментальная методика основана на применении активных методов сетевой разведки с использованием TCP SYN-сканирования, а также сопоставлении результатов сетевого сканирования с фактической конфигурацией устройств, полученной через консольный доступ.

В ходе исследования установлено, что в штатной конфигурации исследуемые сетевые устройства остаются обнаруживаемыми на уровне IP, однако не предоставляют открытых сервисов удалённого управления. Управляющие порты находятся в состояниях filtered или closed, что свидетельствует о функционировании встроенных механизмов фильтрации и ограничения доступа. Показано, что наличие активного консольного доступа не оказывает прямого влияния на результаты сетевого сканирования.

Полученные результаты подтверждают эффективность базовой конфигурации сетевых устройств с точки зрения снижения сетевой поверхности атаки и могут быть использованы при анализе защищённости сетевой инфраструктуры, а также в учебной практике.

Ключевые слова: сетевые устройства L2+, информационная безопасность, management-плоскость, сетевое сканирование, nmap, консольный доступ.

Введение

В современных корпоративных и учебных сетях управляемые сетевые устройства уровня L2+ играют ключевую роль в обеспечении связности, отказоустойчивости и безопасности информационной инфраструктуры. Коммутаторы и маршрутизаторы данного класса обладают развитой системой управления, включающей как консольные, так и сетевые интерфейсы администрирования, что делает их потенциальной целью для атак на уровне management-плоскости. В условиях роста числа инцидентов, связанных с компрометацией сетевого оборудования, вопросы оценки защищённости таких устройств приобретают особую значимость [1, 2].

Практика эксплуатации сетевой инфраструктуры показывает, что уязвимости сетевых устройств зачастую обусловлены не ошибками реализации протоколов, а особенностями конфигурации сервисов управления и механизмов фильтрации доступа. Даже при отсутствии явных уязвимостей некорректные или избыточные настройки могут приводить к расширению сетевой поверхности атаки. В этой связи актуальной задачей является анализ поведения сетевых устройств в их исходной, штатной конфигурации, без применения дополнительных средств защиты и специализированных систем мониторинга.

Одним из наиболее распространённых инструментов первичной сетевой разведки является утилита nmap, широко используемая как в практическом аудите безопасности, так и в учебных лабораторных работах [3, 4]. Результаты сетевого сканирования позволяют выявлять доступные сетевые сервисы, определять состояние портов и косвенно оценивать эффективность встроенных механизмов фильтрации трафика. При этом корректная интерпретация результатов сканирования требует учёта архитектурных особенностей сетевых устройств и способов их администрирования.

Отдельного внимания заслуживает вопрос влияния консольного доступа администратора на результаты сетевого сканирования. Консольное подключение традиционно рассматривается

как изолированный и наиболее защищённый канал управления, однако на практике его наличие нередко вызывает вопросы о возможной взаимосвязи с сетевой доступностью сервисов управления. Анализ данного аспекта позволяет уточнить границы применимости результатов сетевой разведки и избежать ошибочных выводов при оценке защищённости сетевых устройств [5].

Таким образом, рассмотрение штатных механизмов защиты сетевых устройств уровня L2+ в контексте сетевого сканирования и консольного администрирования представляет практический и методический интерес и способствует формированию более корректного подхода к анализу безопасности сетевой инфраструктуры.

Материалы и методы

Настоящее исследование носит прикладной экспериментальный характер и направлено на оценку эффективности штатных механизмов защиты сетевых устройств уровня L2+ в условиях сетевого сканирования. Методологической основой работы является анализ management-плоскости сетевых устройств с использованием активных методов сетевой разведки и последующего сопоставления результатов сканирования с фактической конфигурацией оборудования.

В качестве объектов исследования использовались управляемый коммутатор MikroTik CRS326-24G-2S+ и маршрутизаторы Cisco серий 1900 и 800, относящиеся к классу сетевых устройств уровня L2+ и широко применяемые в корпоративных и учебных сетях. Выбор оборудования обусловлен его типичностью, наличием встроенных механизмов управления и фильтрации доступа, а также возможностью администрирования как через консольный, так и через сетевые интерфейсы.

Для проведения эксперимента применялась утилита nmap, которая является одним из наиболее распространённых инструментов первичной сетевой разведки и используется для выявления доступных сетевых сервисов, определения состояния TCP-портов и анализа особенностей фильтрации сетевого трафика. В рамках работы использовалось TCP SYN-сканирование, позволяющее определить состояния портов open, closed и filtered на основе реакции узла на инициирование соединения. Состояние open интерпретируется как наличие активного сетевого сервиса, closed — как явный отказ в установлении соединения, filtered — как признак функционирования механизмов фильтрации или ограничения доступа [6].

Администрирование исследуемых устройств осуществлялось исключительно через консольный доступ, который не использует сетевой стек TCP/IP и не формирует дополнительных сетевых сервисов. Для обеспечения возможности проведения сетевого сканирования на всех устройствах применялась минимальная начальная сетевая конфигурация: на интерфейсы управления вручную назначались IP-адреса, необходимые для сетевой доступности оборудования. Указанные действия носили исключительно технический характер и не сопровождались включением сервисов удалённого управления, изменением политик фильтрации или настройкой списков контроля доступа. Таким образом, условия эксперимента соответствовали штатной конфигурации устройств за исключением минимально необходимой IP-адресации.

Сетевое сканирование выполнялось с тестовой станции под управлением операционной системы Windows. При проведении эксперимента использовались режимы сканирования, не требующие предварительного ICMP-обнаружения узла, что позволило учитывать возможную фильтрацию эхо-запросов. Полученные результаты фиксировались и сопоставлялись с данными о состоянии интерфейсов и конфигурации устройств, полученными через консольный доступ с использованием стандартных команд операционных систем сетевого оборудования.

Обработка и интерпретация результатов осуществлялись методом качественного анализа. Основное внимание уделялось сопоставлению состояний сетевых портов, выявленных средствами nmap, с фактическим состоянием сервисов управления и механизмов фильтрации доступа. Статистические методы обработки данных в рамках исследования не применялись, поскольку целью работы являлась оценка защитных свойств конкретных конфигураций сетевых устройств, а не получение обобщённых количественных характеристик.

Результаты исследования

Устройство 1. MikroTik CRS326-24G-2S+

На первом этапе эксперимента в качестве исследуемого сетевого устройства использовался управляемый коммутатор MikroTik CRS326-24G-2S+. Перед началом тестирования устройство было сброшено к заводским настройкам, что позволило анализировать его начальную, штатную конфигурацию без дополнительных изменений со стороны администратора.

Подключение к устройству осуществлялось через консольный доступ с использованием клиента PuTTY. Полученная информация о системе свидетельствует, что коммутатор функционирует под управлением операционной системы RouterOS версии 6.48.4 (stable), установленной производителем. Аппаратная платформа основана на архитектуре ARMv7 с одноядерным процессором с тактовой частотой 800 МГц и объёмом оперативной памяти 512 МБ, что соответствует типовым характеристикам устройств данного класса (см. Рисунок 1).

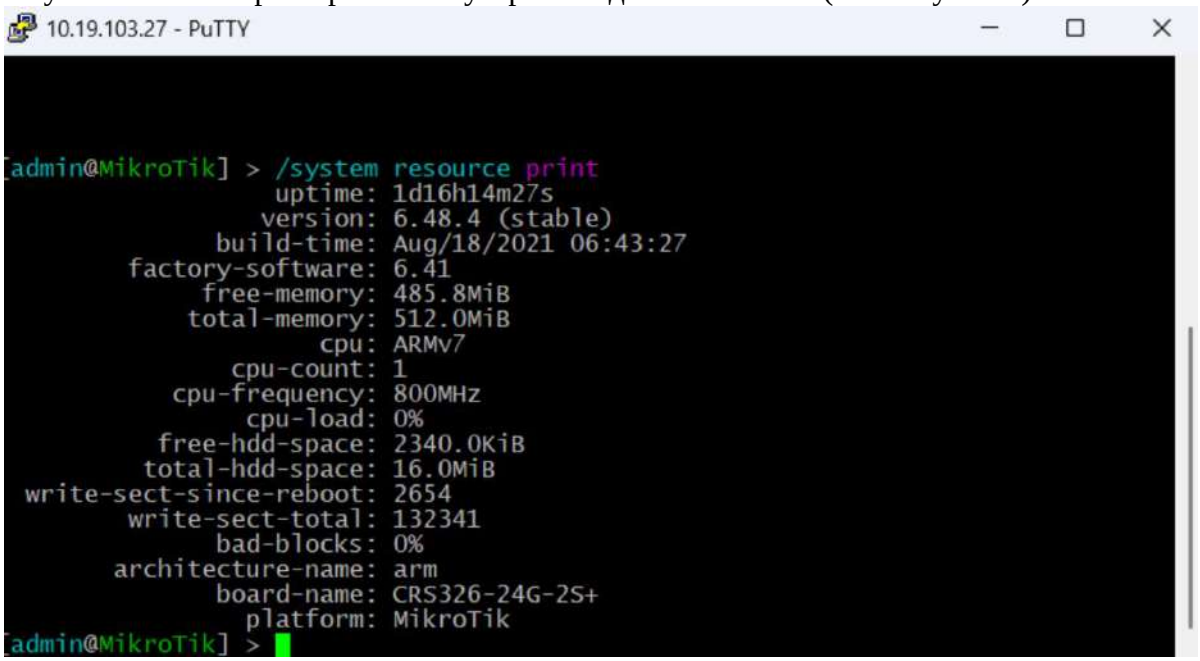

Рис. 1. Коммутатор MikroTik

На втором этапе эксперимента была зафиксирована начальная сетевая конфигурация коммутатора MikroTik после сброса к заводским настройкам и выполнено внешнее сетевое сканирование с использованием утилиты nmap.

С консольной стороны устройства показан вывод команды /interface print, из которого следует, что все физические интерфейсы Ethernet (ether1–ether24), а также два SFP+-интерфейса находятся в отключённом состоянии и объединены в логический bridge с конфигурацией по умолчанию (defconf). Это подтверждает отсутствие пользовательской настройки портов и использование стандартной схемы коммутации.

Вывод команды /ip address print демонстрирует, что на устройстве присутствует IP-адрес 192.168.88.1/24, назначенный интерфейсу bridge в рамках заводской конфигурации RouterOS. Дополнительно отображаются адреса, привязанные к отдельным интерфейсам, что указывает на ранее существовавшие подключения, однако ключевым для эксперимента является именно адрес управления по умолчанию.

С внешней стороны, со стороны тестовой станции под управлением Windows, выполнено сетевое сканирование устройства с помощью nmap. Результаты ping-сканирования подтверждают доступность узла по IP-адресу 192.168.88.1. При выполнении TCP SYN-сканирования (-sS -Pn) было выявлено, что большинство TCP-портов находятся в состоянии фильтрации или закрыты, а стандартные сервисы, такие как SMTP, DNS, MSRPC и Microsoft-DS, не принимают входящие соединения (см. Рисунок 2).

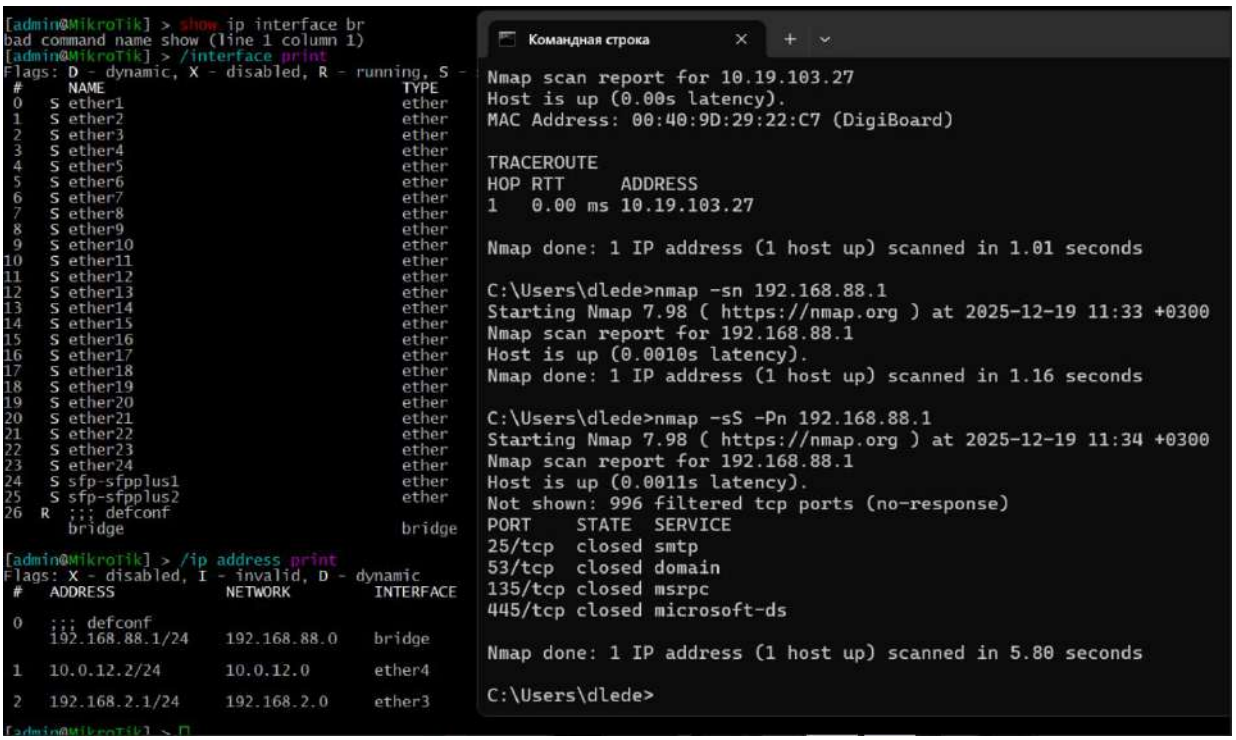

Рис. 2. Сканирование TCP портов

При выборочном сканировании портов управления и прикладных сервисов (22/SSH, 23/Telnet, 80/HTTP, 443/HTTPS, 8291/Winbox) все они определяются как filtered, то есть пакеты блокируются и не получают ответа (см. Рисунок 3).

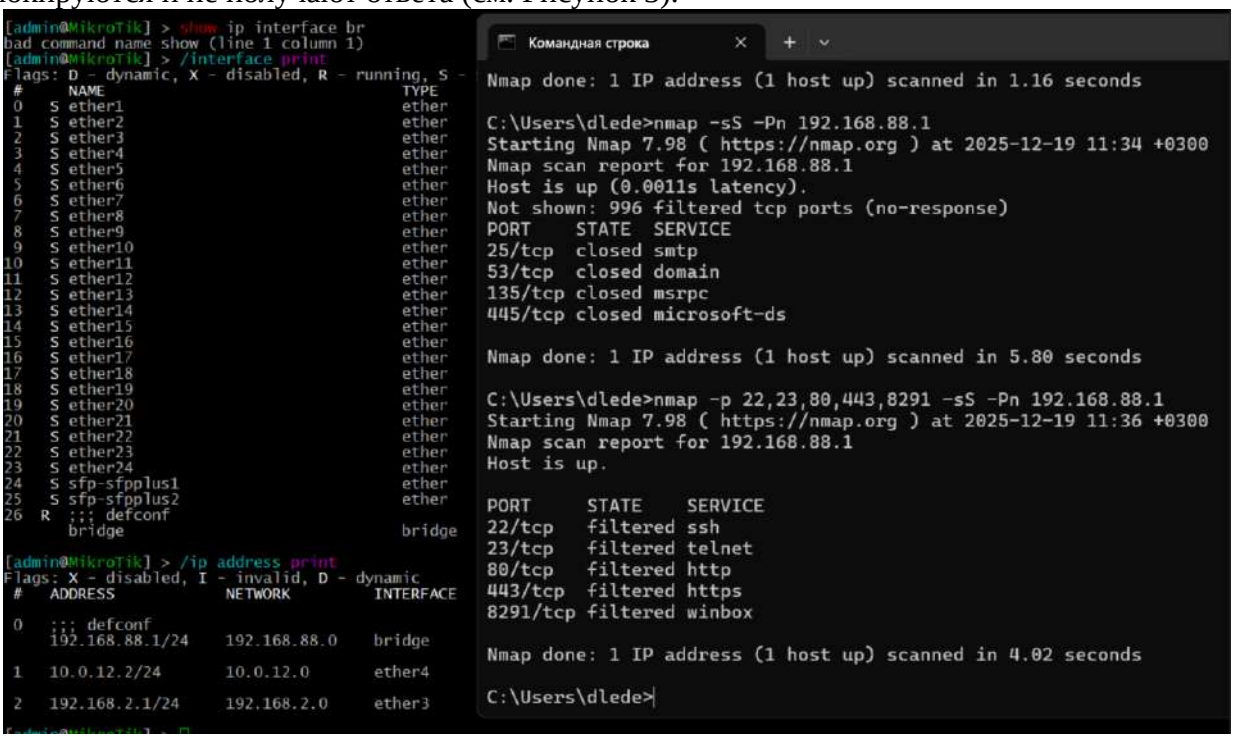

Рис 3. Выборочное сканирование TCP портов

Полученные результаты свидетельствуют о том, что даже при активном сетевом присутствии и назначенном IP-адресе управления MikroTik в начальной конфигурации применяет штатные механизмы фильтрации трафика. Это ограничивает доступ к консольным и веб-сервисам с неавторизованных узлов и существенно снижает поверхность атаки на уровне транспортных протоколов [6].

Устройство 2. Cisco 1941

Устройство функционирует под управлением Cisco IOS Software линейки C1900 (образ C1900-UNIVERSALK9-M), версия операционной системы — 15.7(3)M6, что указывает на

использование универсального образа с поддержкой механизмов маршрутизации и встроенных криптографических функций. Согласно выводу команды show version, маршрутизатор был загружен штатным образом из flash-памяти, без аварийных перезапусков.

Также отображается информация о версии загрузчика (ROM Bootstrap), дате компиляции прошивки и причине последней перезагрузки, которая была выполнена вручную командой перезапуска. Это косвенно подтверждает, что перед началом исследования устройство находилось в контролируемом состоянии и не испытывало сбоев. Наличие стандартного консольного приглашения Router> и переход в привилегированный режим (enable) указывает на активный консольный доступ, используемый для администрирования и мониторинга параметров устройства в рамках эксперимента (см. Рисунок 4).

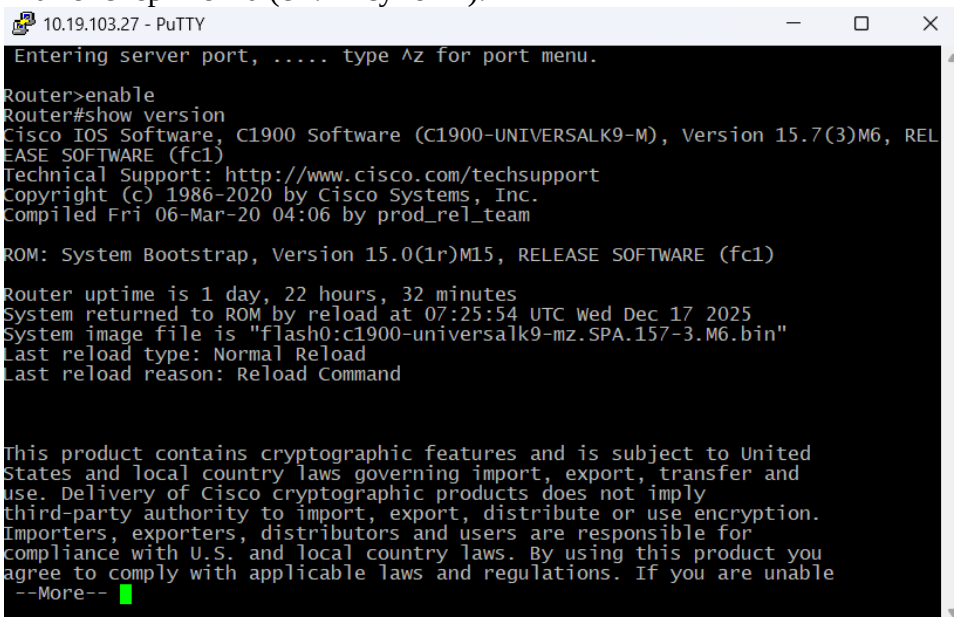

Рис. 4. Маршрутизатор Cisco 1941

Первоначально была выполнена проверка доступности узла (nmap -sn), подтвердившая, что хост находится в сети и отвечает на запросы. Далее осуществлён TCP SYN-скан (nmap -sS -Pn), в ходе которого выявлено, что большинство портов маршрутизатора находятся в состоянии filtered или closed, а ответы от сервисов отсутствуют (см. Рисунок 5). Это свидетельствует о работе встроенных механизмов фильтрации и ограничений доступа, реализованных в штатной конфигурации устройства.

Следует отметить, что результаты сетевого сканирования и вывод команды show ip interface brief, представленные на рисунке 5, были получены в разные моменты времени. Во время проведения сетевого сканирования интерфейс GigabitEthernet0/1 находился во включённом состоянии, что обеспечивало сетевую доступность узла 192.168.1.1. Впоследствии интерфейс был переведён в состояние administratively down, что зафиксировано на приведённом скриншоте. Данное обстоятельство не влияет на интерпретацию результатов эксперимента, однако уточняется для устранения логического противоречия.

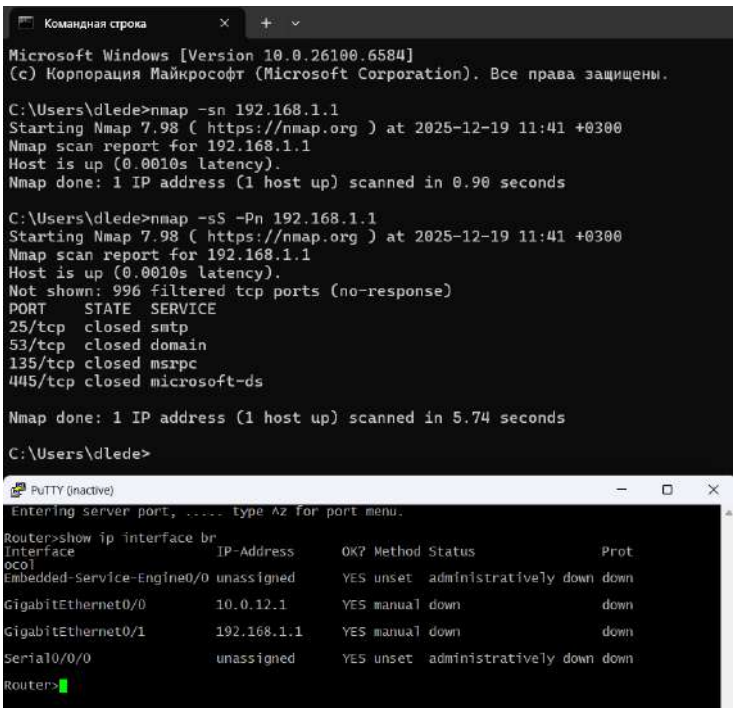

Рис. 5. Сканирование TCP портов Cisco 1941

На следующем этапе эксперимента зафиксирован результат целенаправленного сканирования управляющих портов маршрутизатора Cisco средствами nmap после сброса конфигурации и при наличии только консольного доступа. Сканирование выполнялось по наиболее распространённым портам удалённого управления и администрирования: SSH (22), Telnet (23), HTTP (80), HTTPS (443), а также Winbox (8291). Результаты сканирования показывают, что узел 192.168.1.1 доступен на сетевом уровне (Host is up), однако все проверяемые порты находятся в состоянии filtered (см. Рисунок 6). Это означает, что маршрутизатор не отвечает на SYN-запросы, направленные на данные порты, и не возвращает явных сообщений о закрытии соединения (RST). Такое поведение характерно для работы встроенных механизмов фильтрации трафика, в том числе ACL и базовых политик безопасности Cisco IOS.

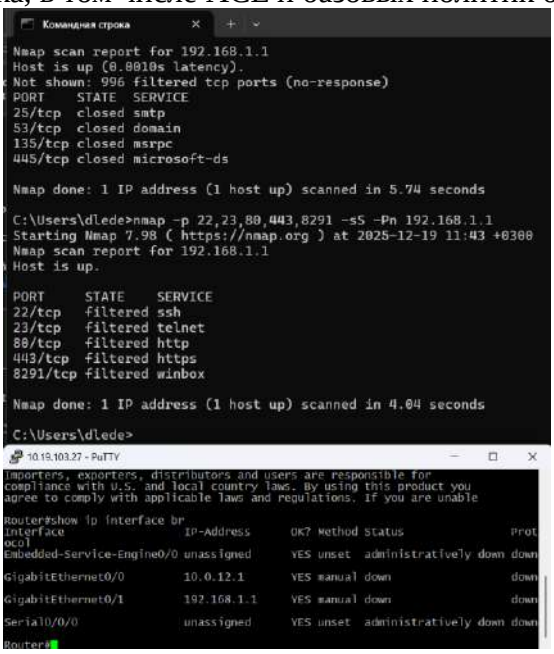

Рис. 6. Выборочное сканирование TCP портов Cisco 1941

Полученные результаты подтверждают, что в начальной (базовой) конфигурации после сброса настроек маршрутизатор Cisco реализует консервативную модель безопасности: сетевое устройство обнаруживается в сети, но все потенциально опасные сервисы управления скрыты или отфильтрованы. Это существенно снижает поверхность атаки и демонстрирует

эффективность штатных средств защиты при отсутствии явного включения веб- и сетевого управления [6].

Устройство 3. Cisco 881

На данном этапе эксперимента представлен вывод информации о втором исследуемом сетевом устройстве — маршрутизаторе Cisco серии 800, полученный по консольному доступу после сброса конфигурации к исходному состоянию. На рисунке 7 представлены сведения о программно-аппаратной платформе устройства. Установлена операционная система Cisco IOS версии 15.8(3)M2, устройство относится к линейке Cisco C800, время непрерывной работы составляет около 15 часов, а последняя перезагрузка была выполнена при включении питания. Тип загрузки указан как штатный (Normal Reload), что также подтверждает отсутствие аварийных состояний (см. Рисунок 7).

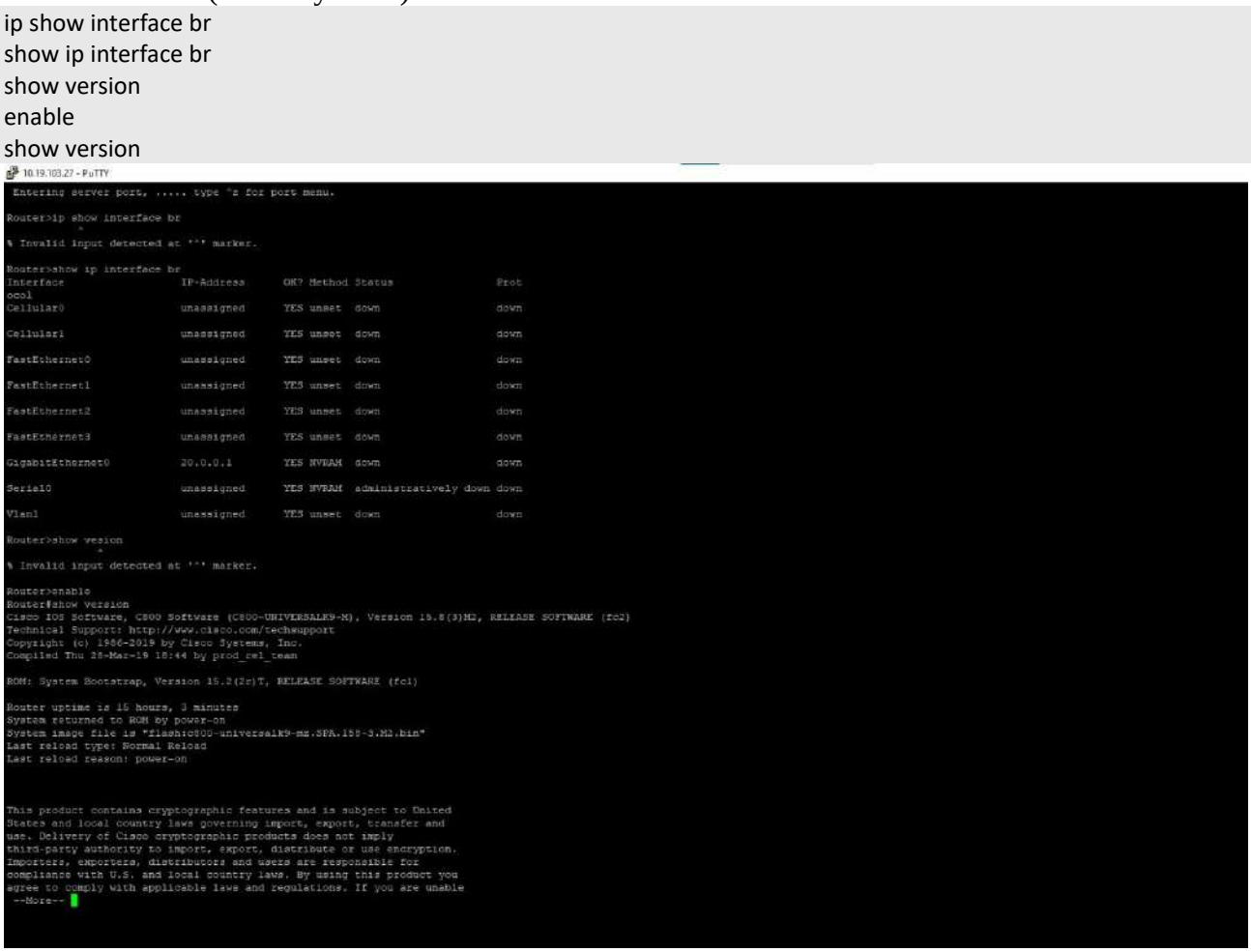

Рис.7. Маршрутизатор Cisco 881

На следующем этапе эксперимента зафиксирован результат сканирования второго исследуемого устройства — маршрутизатора Cisco C800 — с использованием графического интерфейса Zenmap (GUI-оболочка nmap). Сканирование выполнялось по IP-адресу 20.0.0.1, который ранее был назначен интерфейсу GigabitEthernet0 маршрутизатора.

Данный режим предполагает выполнение TCP SYN-сканирования без предварительной проверки доступности хоста ICMP-запросами, что позволяет оценить реакцию устройства на сетевые попытки установления соединений. Результаты сканирования подтверждают, что хост доступен на сетевом уровне (Host is up), при этом задержка отклика минимальна, что указывает на прямую сетевую связность без промежуточных маршрутизаторов [6].

В выводе сканирования указано, что подавляющее большинство TCP-портов (996 из 1000) находятся в состоянии filtered и не возвращают ответа на запросы. Среди отображённых портов зафиксированы порты 25 (SMTP), 53 (DNS), 135 (MSRPC) и 445 (Microsoft-DS), все они находятся в состоянии closed, то есть маршрутизатор явно отклоняет попытки соединения [6,

7]. Открытых портов и активных сетевых сервисов в результате сканирования не выявлено (см. Рисунок 8 и Рисунок 9).

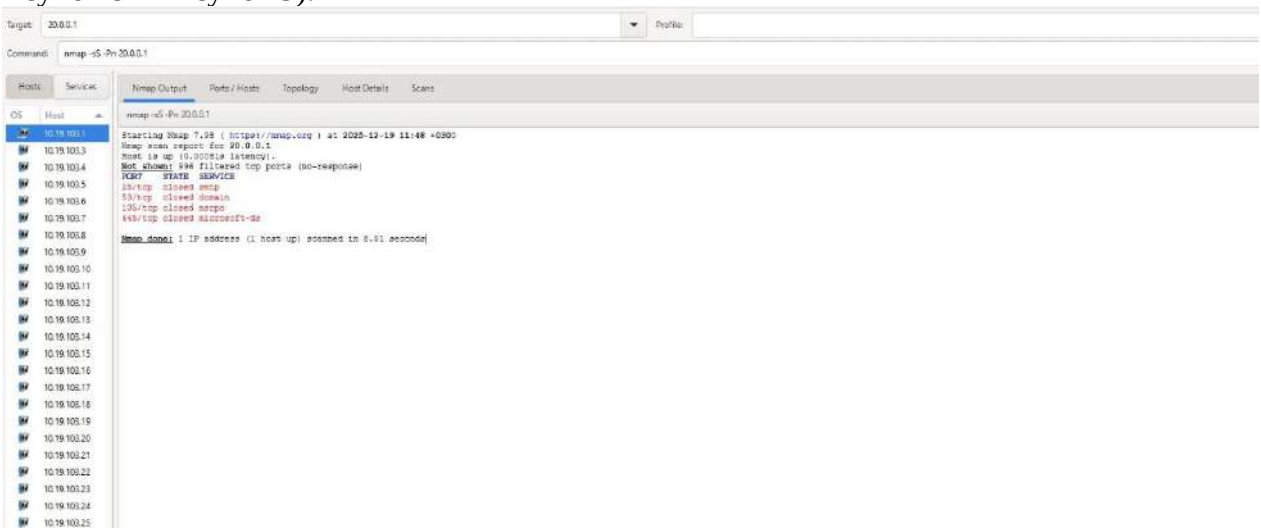

Рис. 8. Сканирование TCP портов Cisco 881

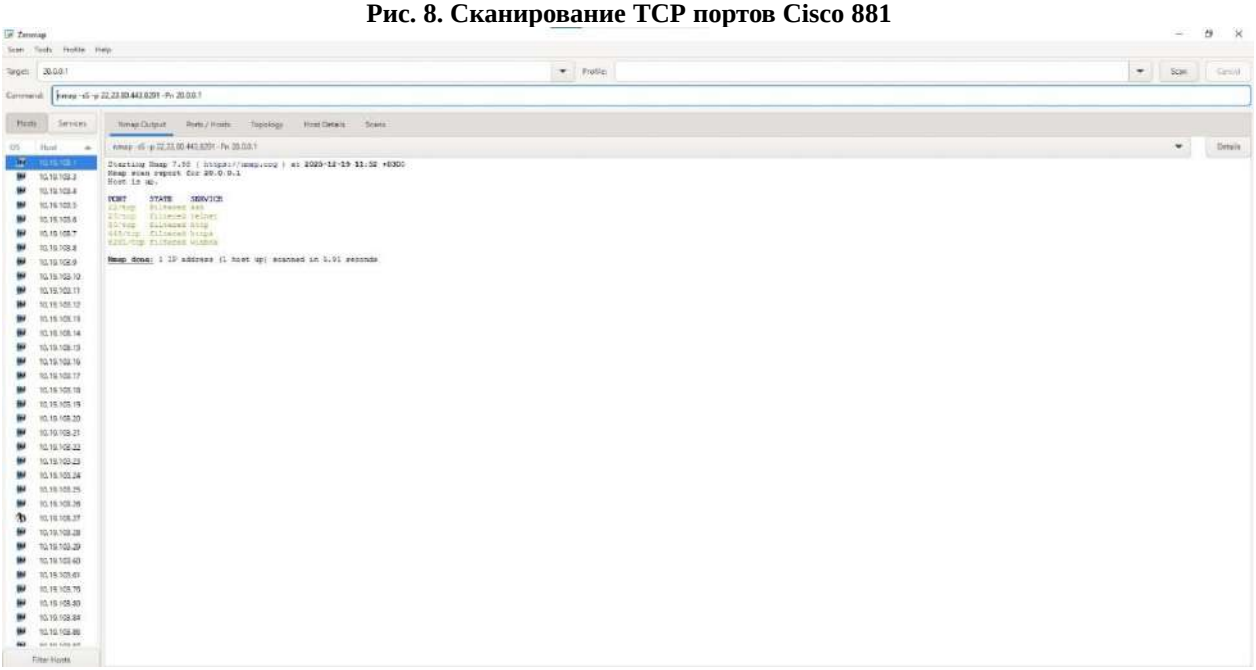

Рис. 9. Выборочное сканирование TCP портов Cisco 881

Аналитический сценарий изменения поверхности атаки при включении сервисов управления

В рамках настоящего исследования экспериментальная часть была ограничена анализом штатной конфигурации сетевых устройств без явного включения сервисов удалённого управления. Вместе с тем, для повышения интерпретационной ценности полученных результатов целесообразно рассмотреть аналитический сценарий изменения поверхности атаки при активации сервисов управления.

При включении на сетевом устройстве сервиса удалённого администрирования, такого как SSH или Web-интерфейс (HTTP/HTTPS), соответствующие TCP-порты переходят из состояния filtered или closed в состояние open, что фиксируется средствами сетевого сканирования nmap. В этом случае утилита nmap получает явный ответ на SYN-запросы, что указывает на наличие активного сервиса и формирует дополнительную поверхность атаки [6].

Данный эффект подробно описан в документации nmap и в работах, посвящённых анализу сетевой безопасности, где подчёркивается, что состояние open является индикатором доступного сетевого сервиса, потенциально подверженного атаке при наличии уязвимостей или слабой аутентификации. Таким образом, включение сервисов управления принципиально изменяет результаты сетевого сканирования и требует применения дополнительных мер защиты,

таких как списки контроля доступа, ограничение источников подключения и использование защищённых протоколов [6, 7].

Рассмотренный аналитический сценарий позволяет наглядно интерпретировать результаты, полученные в рамках эксперимента, и подчёркивает, что эффективность штатной защиты в конфигурации по умолчанию обусловлена именно отсутствием активных сервисов управления, а не влиянием консольного доступа администратора.

Обсуждение

Полученные в ходе исследования результаты подтверждают, что штатная конфигурация сетевых устройств уровня L2+ ориентирована на минимизацию сетевой поверхности атаки за счёт отсутствия активных сервисов удалённого управления. Обнаружение устройств на уровне IP при одновременном отсутствии открытых управляющих портов соответствует консервативной модели безопасности, реализуемой производителями сетевого оборудования.

Важно отметить, что результаты сетевого сканирования, полученные средствами nmap, требуют корректной интерпретации с учётом архитектурных особенностей сетевых устройств и способов их администрирования. В частности, наличие активного консольного доступа не коррелирует с сетевой доступностью сервисов управления и не влияет на состояние TCP-портов, выявляемых в процессе сканирования. Это подчёркивает необходимость сопоставления данных сетевой разведки с фактической конфигурацией устройств, полученной через консольный доступ.

Ограничением проведённого исследования является отсутствие экспериментальной проверки сценариев с включением сервисов удалённого управления. Вместе с тем, аналитический анализ показывает, что активация таких сервисов приводит к принципиальному изменению результатов сетевого сканирования и требует применения дополнительных мер защиты. Указанные сценарии представляют практический интерес и могут быть реализованы в рамках дальнейших исследований.

Заключение

В рамках данной работы проведено экспериментальное исследование штатных механизмов защиты сетевых устройств уровня L2+ с использованием утилиты nmap. Анализ выполнялся на реальном сетевом оборудовании различных производителей при активном консольном доступе и минимальной начальной конфигурации, необходимой для обеспечения сетевой доступности устройств.

В ходе исследования установлено, что в штатной конфигурации сетевые устройства обнаруживаются на уровне IP, однако не предоставляют открытых сервисов удалённого управления. Управляющие порты находятся в состояниях filtered или closed, что свидетельствует о функционировании встроенных механизмов фильтрации и ограничения доступа. Показано, что наличие активного консольного доступа не оказывает прямого влияния на результаты сетевого сканирования.

Полученные результаты подтверждают эффективность базовой конфигурации сетевых устройств с точки зрения снижения сетевой поверхности атаки и подчёркивают значимость корректной интерпретации данных сетевой разведки. Материалы работы могут быть использованы при анализе защищённости сетевой инфраструктуры, а также в образовательной практике при изучении вопросов сетевой безопасности и администрирования.

Библиографический список

1. Компьютерные сети. Принципы, технологии, протоколы : юбилейное издание, доп. и испр. — Санкт-Петербург : Питер, 2024. — 1008 с.
2. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. — 3rd ed. — Indianapolis : Wiley, 2020. — 1182 p.
3. Использование Nmap для обнаружения сетевых служб и идентификации сервисов [Электронный ресурс]. — URL: https://labex.io/ru/tutorials/nmap-how-to-use-nmap-for-network-discovery-and-service-identification-in-cybersecurity-415099 (дата обращения: 19.11.2025).

4. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебно-методическое пособие для СПО / А. Г. Уймин. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 480 с. — ISBN 978-5-8114-9255-8.
5. Denzler, P. An iterative and toolchain-based approach to automate scanning and mapping computer networks / P. Denzler, R. Teixeira // arXiv.org. — 2017. — URL: https://arxiv.org/abs/1710.01026 (дата обращения: 06.12.2025).
6. Lyon, G. F. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning / G. F. Lyon. — Sunnyvale : Insecure.Com LLC, 2009. — 468 p.
7. Полное руководство по сетевому сканированию с использованием Nmap [Электронный ресурс]. — URL: https://codeby.net/threads/kniga-po-nmap-na-russkom-polnoye-rukovodstvo-po-setevomu-skanirovaniyu.67190/ (дата обращения: 21.11.2025).

References

1. Computer networks. Principles, technologies, protocols (2024). Anniversary edition, revised and expanded. Saint Petersburg: Piter.
2. Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). Indianapolis, IN: Wiley.
3. LabEx. (2025). How to use Nmap for network discovery and service identification in cybersecurity. Retrieved November 19, 2025, from https://labex.io/ru/tutorials/nmap-how-to-use-nmap-for-network-discovery-and-service-identification-in-cybersecurity-415099
4. Uymin, A. G. (2022). Network and system administration. Demonstration exam CODE 1.1: Study guide for secondary vocational education (3rd ed.). Saint Petersburg: Lan Publishing House.
5. Denzler, P., & Teixeira, R. (2017). An iterative and toolchain-based approach to automate scanning and mapping computer networks. arXiv. Retrieved December 6, 2025, from https://arxiv.org/abs/1710.01026
6. Lyon, G. F. (2009). Nmap network scanning: The official Nmap project guide to network discovery and security scanning. Sunnyvale, CA: Insecure.Com LLC.
7. Codeby.net. (2025). Complete guide to network scanning using Nmap. Retrieved November 21, 2025, from https://codeby.net/threads/kniga-po-nmap-na-russkom-polnoye-rukovodstvo-po-setevomu-skanirovaniyu.67190/

Информация об авторах

Селиванов Иван Константинович — студент, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация, e-mail: gt0305@mail.ru

Леденёв Дмитрий Алексеевич — студент, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация, e-mail: dledenev@list.ru

TESTING BUILT-IN SECURITY MECHANISMS OF L2+ NETWORK DEVICES USING NMAP UNDER ACTIVE CONSOLE ACCESS

Selivanov I.K. [1]***, Ledenev D.A.*** [1]

[1]*National University of Oil and Gas «Gubkin University», Moscow, Russian Federation*

Abstract. The article examines the effectiveness of built-in security mechanisms of L2+ network devices under network scanning performed using the nmap utility. The relevance of the study is determined by the widespread use of managed network devices in corporate and educational networks, as well as by the need to minimize the attack surface of management interfaces without deploying additional security tools. Special attention is paid to the analysis of the management plane in the presence of active console access.

The purpose of the study is to assess the network accessibility of management services and the state of network ports in the default configuration of network devices from different vendors. The research objects include a MikroTik CRS326-24G-2S+ managed switch and Cisco routers of the 1900 and 800 series. The experimental methodology is based on active network reconnaissance techniques using TCP SYN scanning and on correlating scanning results with actual device configurations obtained via console access.

The study shows that in the default configuration the examined devices remain detectable at the IP level but do not expose open remote management services. Management ports are identified as filtered or closed, indicating the operation

of built-in traffic filtering and access restriction mechanisms. It is demonstrated that the presence of active console access does not directly affect the results of network scanning.

The obtained results confirm the effectiveness of default security configurations in reducing the network attack surface and may be applied in network security assessments as well as in educational and training environments.

Keywords: L2+ network devices, information security, management plane, network scanning, nmap, console access.

Information about the authors

Selivanov Ivan Konstantinovich — student, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russian Federation, e-mail: gt0305@mail.ru

Ledenev Dmitriy Alekseevich — student, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russian Federation, e-mail: dledenev@list.ru