DOI 10.36622/1682-7813.2025.28.2.006
УДК 004.056

УЯЗВИМОСТЬ ПЕРЕЧИСЛЕНИЯ УЧЕТНЫХ ЗАПИСЕЙ В КОРПОРАТИВНЫХ WI-FI СЕТЯХ НА БАЗЕ MICROSOFT NPS

В.П. Лось, А.Г. Иванов, Р.Е. Просветов

С развитием мобильных компьютеров и умных устройств все больше организаций внедряют корпоративные беспроводные сети, ориентированные на современные стандарты безопасности. Одним из ключевых элементов таких сетей является использование Enterprise-аутентификации на основе Radius-сервера, среди которых широко распространен Microsoft Network Policy Server (NPS). Этот сервер привлекает внимание благодаря простоте развертывания и удобной интеграции с существующей доменной инфраструктурой Active Directory, что делает его востребованным решением для централизованной аутентификации пользователей. В ходе проведенного исследования был выявлен недостаток Microsoft NPS, позволяющий неавторизованным пользователям перечислять учетные записи корпоративного домена. В настоящей работе подробно рассматривается данный недостаток, выполняется анализ механизмов и способов его эксплуатации, а также предлагается метод автоматизированной реализации атаки. В завершении приводятся рекомендации по устранению обнаруженного недостатка.

Ключевые слова: беспроводные сети, перечисление пользователей, Enterprise-сеть, уязвимость, недостаток, эксплуатация, эксплойт.

Введение

После завершения пандемии COVID-19 в Российской Федерации многие организации начали возвращать сотрудников в офисы, что сделало актуальной задачу создания комфортных условий работы [1]. Современные информационные технологии предлагают широкий спектр решений для повышения удобства в офисных пространствах и эффективности работы с корпоративными ресурсами. В условиях растущей цифровизации рабочей среды компании все активнее внедряют интеллектуальные системы управления, направленные на оптимизацию бизнес-процессов и повышение гибкости инфраструктуры. Это включает в себя автоматизацию рабочих пространств, применение облачных сервисов для удаленного доступа и более активное использование мобильных устройств в повседневной деятельности сотрудников.

На фоне этих изменений многие компании переходят к концепции открытых офисных пространств (open space), где сотрудники не имеют закрепленных рабочих мест. Такая модель повышает мобильность персонала, но требует гибкой и надежной сетевой инфраструктуры [2]. Для обеспечения мобильности сотрудников и организации гибкого рабочего пространства компании используют беспроводные сети, обеспечивающие удобный и масштабируемый доступ к корпоративным ресурсам.

Существует несколько способов организации беспроводных корпоративных сетей, включая открытые сети, сети с общим ключом (Pre-Shared-Key, PSK) и сети стандарта Enterprise. Последний вариант считается наиболее безопасным, поскольку использует централизованную аутентификацию пользователей через учетные данные или сертификаты [3].

Несмотря на активное внедрение политики импортозамещения, программные продукты Microsoft по-прежнему широко используются в российских организациях, а значительная часть корпоративных устройств продолжает функционировать под управлением ОС семейства Windows [4]. Внедрение беспроводных сетей стандарта Enterprise на базе Microsoft Network Policy Server (NPS) позволяет компаниям централизованно управлять доступом к сети и применять различные методы аутентификации по протоколу Extensible Authentication Protocol (EAP), включая

безопасные на момент написания статьи EAP-TLS и PEAP-MS-CHAPv2 [3].

Однако исследование процесса аутентификации беспроводных Enterprise-сетей, функционирующих с использованием Microsoft NPS, выявило уязвимость, позволяющую злоумышленникам определять наличие учетных записей в корпоративном домене. Данная особенность может быть использована для формирования списка пользователей и дальнейшего развития атак на их учетные записи.

1 Теоретическое обоснование существующего недостатка

1.1 Процесс подключения к беспроводным Enterprise-сетям

Для построения защищенной беспроводной инфраструктуры корпоративного уровня компании используют сети стандарта Enterprise. В отличие от PSK-сетей, такой подход базируется на централизованной системе аутентификации, что повышает уровень безопасности и управляемости. В среде Microsoft реализация этого механизма осуществляется через Network Policy Server, который является компонентом Windows Server и взаимодействует с Active Directory.

Использование Microsoft NPS в роли RADIUS-сервера позволяет администраторам централизованно управлять политиками доступа и контролировать процесс подключения клиентов к сети. Он включает несколько этапов: обнаружение доступных сетей, инициализацию аутентификации, передачу учетных данных на сервер NPS, их проверку и установление защищенного соединения [5]. Данный процесс может быть представлен в виде схемы, отраженной на рис. 1.

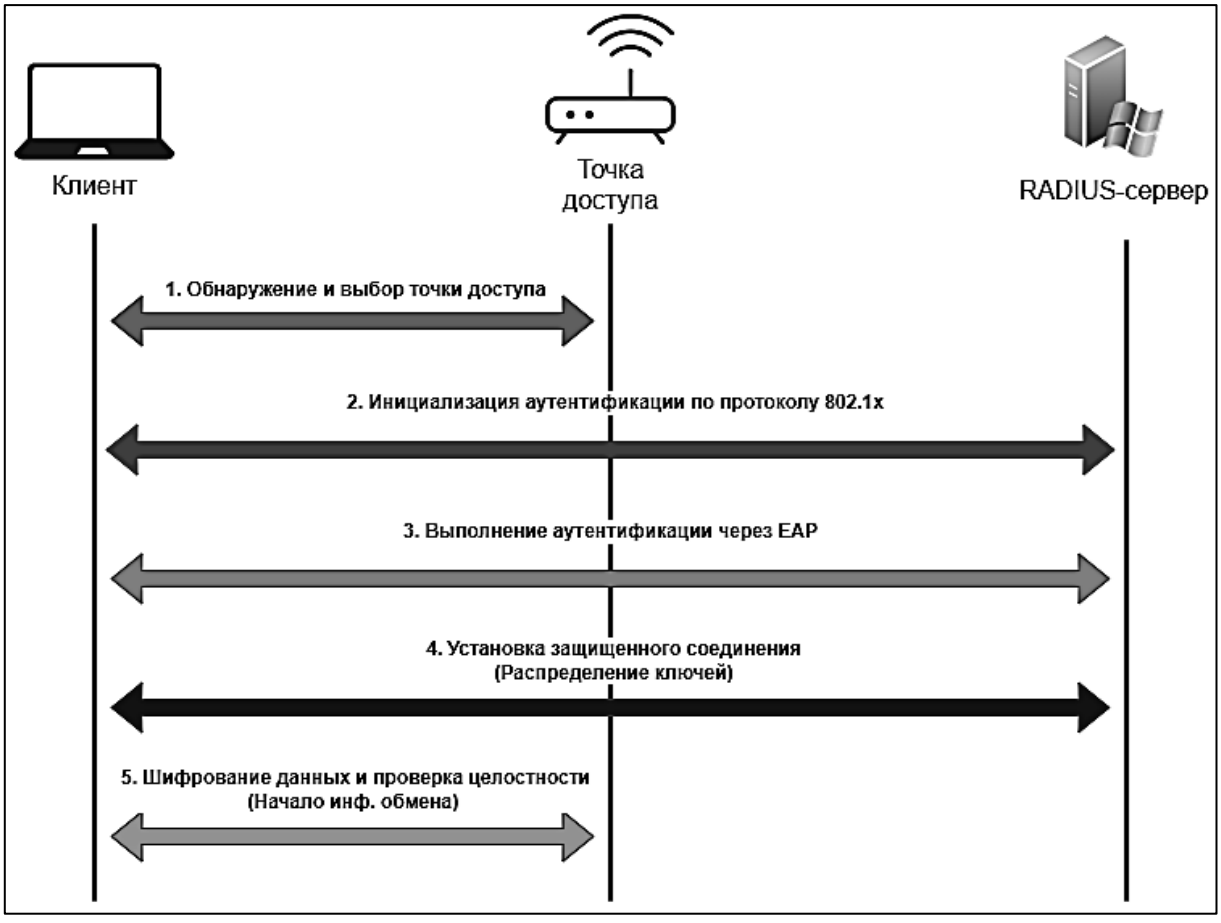

Рис. 1. Схема подключения клиента к беспроводной Enterprise-сети

1.1.1 Обнаружение и выбор точки доступа

Клиентское устройство осуществляет сканирование доступных беспроводных сетей, используя активные или пассивные методы. В процессе этого анализа исследуются кадры Beacon и Probe Response, которые передаются точками доступа и содержат информацию о поддерживаемых механизмах безопасности, таких как WPA-Enterprise или WPA2-Enterprise. Если точка доступа поддерживает Enterprise-аутентификацию, в её параметрах (IE, Information Elements) указывается наличие RSN (Robust Security Network) с механизмами 802.1X и EAP.

1.1.2 Инициализация аутентификации по протоколу 802.1X

На этом этапе точка доступа выполняет функцию авторизатора (Authenticator), а клиентское устройство действует в роли супликанта (Supplicant). Аутентификация осуществляется посредством протокола EAP, обеспечивающего передачу учетных данных между клиентом и сервером NPS (RADIUS) через точку доступа.

Процесс инициализируется с отправки точкой доступа EAP-запроса (EAP-Request/Identity), на который клиент отвечает идентификатором (EAP-Response/Identity). Далее этот идентификатор передается на сервер NPS, который в ходе взаимодействия с Active Directory, определяет, какой метод EAP будет использоваться для дальнейшей аутентификации.

1.1.3 Выполнение аутентификации через EAP

В результате анализа поступившего идентификатора клиента (EAP-Response/Identity), NPS-сервер выбирает поддерживаемый и разрешенный в данной сети метод аутентификации. В зависимости от конфигурации корпоративной сети возможны различные варианты, включая EAP-TLS, PEAP-MS-CHAPv2, EAP-TTLS, EAP-FAST и другие методы, ориентированные на конкретные особенности инфраструктуры и подключаемого клиента.

В инфраструктуре Microsoft наиболее широко применяются методы аутентификации EAP-TLS и PEAP-MS-CHAPv2. Их популярность обусловлена высокой степенью безопасности, достигаемой за счёт использования учетных записей Active Directory и цифровых сертификатов. EAP-TLS предоставляет аутентификацию на основе клиентских и серверных сертификатов, исключая необходимость передачи паролей, что значительно снижает вероятность их компрометации. В свою очередь, PEAP-MS-CHAPv2 реализует двухэтапный процесс, сначала устанавливая защищённый туннель на основе TLS, а затем передавая учетные данные в зашифрованном виде.

1.1.4 Установление защищенного соединения

После успешного прохождения аутентификации точка доступа и клиентское устройство осуществляют обмен криптографическими ключами для защиты передаваемых данных. Этот процесс включает генерацию Pairwise Master Key (PMK) на основе аутентификационных данных EAP и его передачу точке доступа в рамках Access-Accept от сервера NPS. Далее выполняется четырёхэтапный процесс установки ключей (4-way handshake), в ходе которого подтверждается владение ключами и устанавливаются окончательные параметры шифрования, включая Pairwise Transient Key (PTK) и Group Temporal Key (GTK).

1.1.5 Подтверждение установки ключей и начало защищенного обмена данными.

После завершения процесса обмена ключами клиентское устройство получает полный доступ к сети. Передача данных при этом осуществляется в зашифрованном виде, что обеспечивает конфиденциальность передаваемой информации.

1.2 Особенность EAP-аутентификации в Microsoft NPS

Для анализа функционирования процесса установки соединения с беспроводной Enterprise сетью, реализованной с использованием Microsoft NPS в качестве Radius-сервера, был подготовлен стенд, имеющий представленную на рис. 2 сетевую структуру.

В локальной сети, по адресу 192.168.1.203, развернут Microsoft Windows Server 2022, выступающий в роли

контроллера домена «study.local». На данном узле также развернуты центр сертификации (Active Directory Center Services), для подключения к беспроводной сети с использованием сертификатов, и сам сервер аутентификации (NPS). Сетевая точка доступа, представляющая собой коммутатор модели «Cisco WAP 4410N», доступен по адресу 192.168.1.106. Роль сетевого шлюза и DHCP-сервера выполняет маршрутизатор «Xiaomi Redmi Router AC2100». В качестве клиентского устройства использовался ноутбук, функционирующий на базе ОС «Kali Linux 6.8.11». С данного устройства выполнялись основные проверки, а также демонстрировалась атака, представленная в разделе 2 настоящей работы.

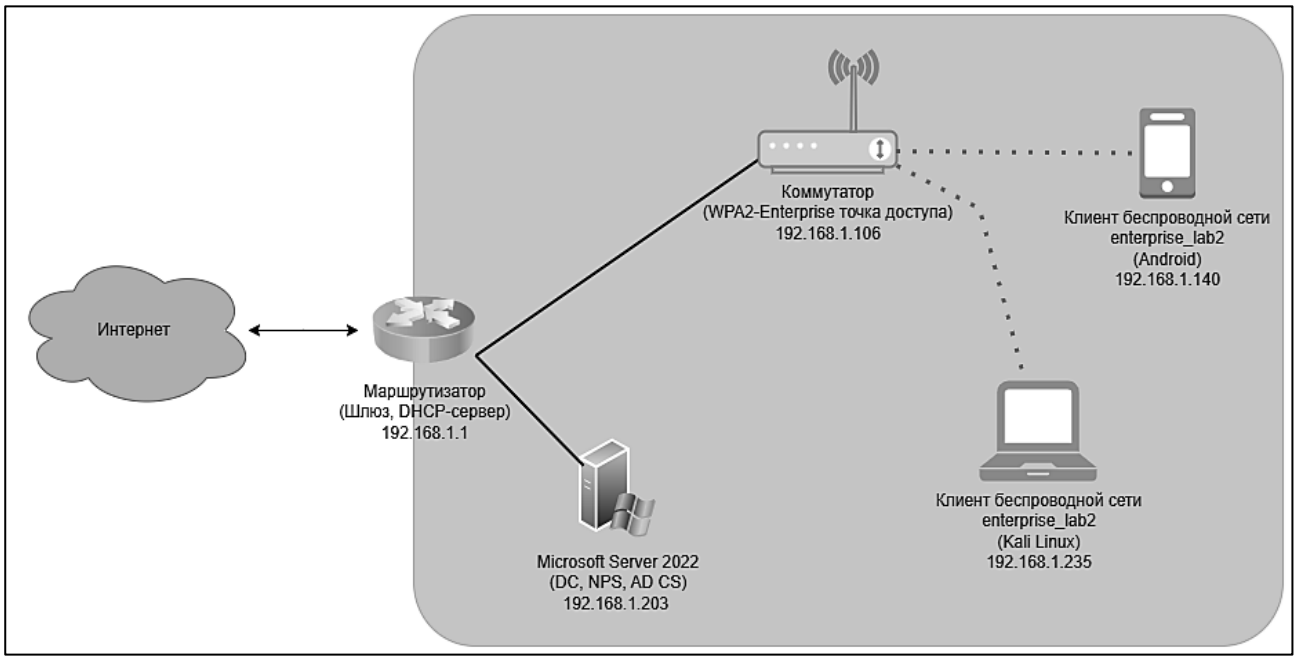

Рис. 2. Схема сети демонстрационного стенда

В подготовленном домене «study.local» имеется несколько предварительно созданных пользователей – «ivan», «petr», «georgiy» и «maria». Первые два пользователя обладают привилегиями на подключения к беспроводной сети с использованием доменных учетных данных (механизм PEAP-MS-CHAPv2), тогда как последние два – только с использованием сертификатов (механизм EAP-TLS).

Используя стандартную утилиту для подключения к беспроводным сетям в ОС Kali Linux (NetworkManager), было выполнено успешное подключение к предварительно настроенной беспроводной сети «enterprise_lab2», функционирующей по стандарту WPA2-Enterprise. Процесс подключения, запущенный с использованием внешней сетевой карты «ALFA AWUS036ACH», был захвачен инструментом для анализа сетевого трафика Wireshark (рис. 3).

Рассматривая содержимое пакетов аутентификации по 802.1x, отправленных и полученных устройством, можно увидеть, что процесс подключения к беспроводной сети начался с Request/Response запросов Identity. После этого был выполнен процесс согласования протокола для подключения (в нашем случае, EAP-PEAP), а также последующее прохождение аутентификации по данному протоколу. После успешного получения пакета об успешной аутентификации (EAP-пакет «Success»), было осуществлено стандартное 4-х этапное рукопожатие, в результате которого были получены ключи и установлено успешное подключение к сети.

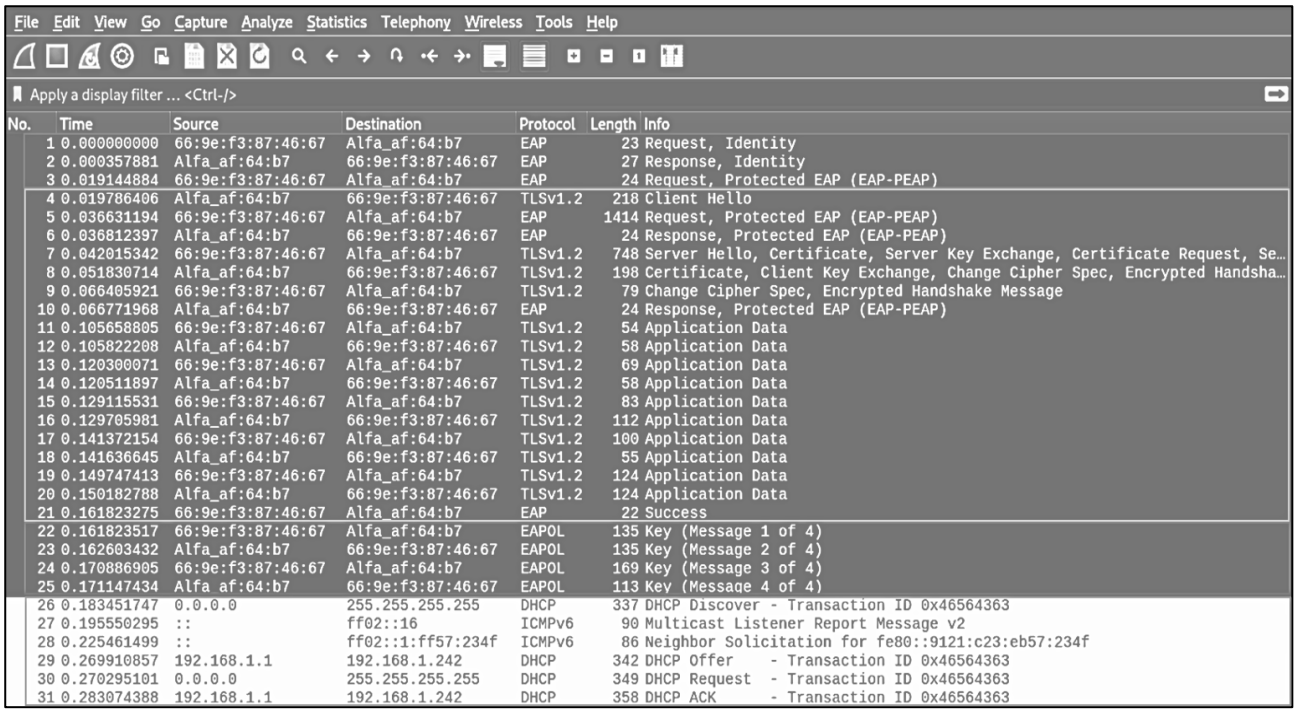

Рис. 3. Успешное подключение к беспроводной Enterprise-сети

Описанный процесс подключения к беспроводной точке доступа выполнялся с использованием действительных учетных данных пользователя «ivan» (доменный логин и пароль). При попытке подключения с недействительным паролем пользователя «ivan», процесс подключения останавливался перед ожидаемым этапом получения EAP-пакета, сообщающим об успешной аутентификации у RADIUS-сервера (рис. 4).

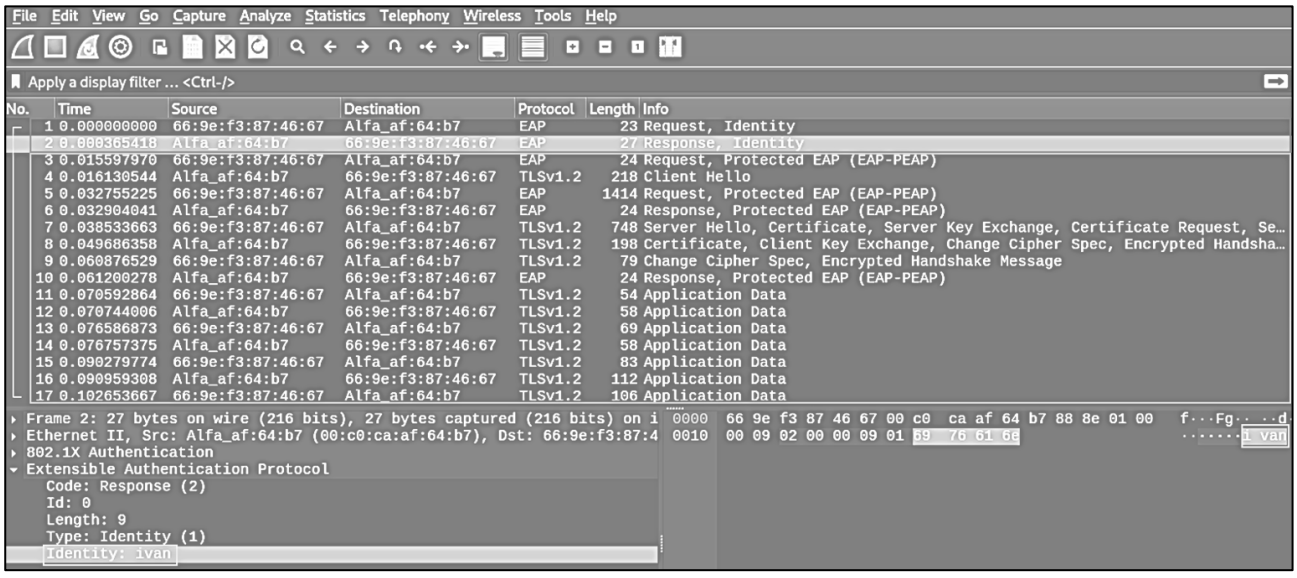

Рис. 4. Попытка подключения к Enterprise-сети с недействительным паролем существующего пользователя

Представленные ранее попытки подключения от имени существующего в домене пользователя «ivan» являются ожидаемыми и не противоречат рассмотренной методологии подключения к беспроводной Enterprise-сети. Однако отличия начинают происходить при инициализации подключения от имени

пользователя, не существующего в домене (к примеру, пользователя «semen»), что можно увидеть на рис. 5.

Подключение к беспроводной сети вновь начинается с Request и Response запросов Identity. Однако, сразу после них, от точки доступа поступает EAP-пакет, сообщающий об ошибке («Failure»). Такое поведение объясняется тем, что представленный в EAP Response пользователь «semen» отсутствует в базе данных пользователей домена «study.local». По этой причине, осуществлять согласование протокола подключения, с последующим прохождением аутентификации не имеет смысла – она будет заведомо неуспешной.

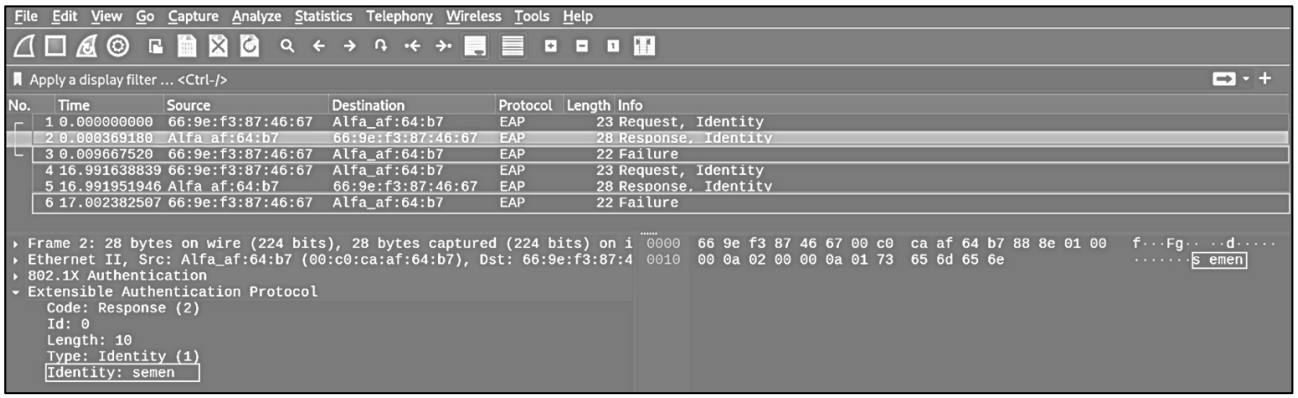

Рис. 5. Попытка подключения к Enterprise-сети от имени несуществующего пользователя

Детально рассмотрев выполненные попытки установки соединения с беспроводной точкой доступа, можно проследить особенность функционирования NPS-сервера Microsoft, выступающего в роли RADIUS-сервера. Если имя пользователя, осуществляющего подключение к беспроводной точке доступа, отсутствует в базе данных пользователей корпоративного домена, то такое подключение сразу считается неуспешным. В случае, если пользователь существует, то инициируется процесс подключения к беспроводной сети, оканчивающийся, в случае корректно переданных данных, успешной установкой соединения, либо, в случае некорректной переданных данных, ошибкой.

Дополнительно было осуществлена попытка подключения к беспроводной сети от имени пользователя, имеющего возможность проходить аутентификацию только по сертификату (протокол EAP-TLS). Аналогично случаю аутентификации по EAP-PEAP, в случае существования пользователя, инициируется процесс согласования метода аутентификации, а если же такого пользователя нет – появляется ошибка. На рис. 6 представлены две попытки подключения с использованием случайного сертификата – первая выполняется от имени несуществующего пользователя «alex», вторая – от имени существующего пользователя «georgiy».

Необходимо также отметить, что при попытке выполнить подключение от имени пользователя «georgiy» с использованием учетных данных (EAP-PEAP), RADIUS-сервер сообщит о намерении сменить метод аутентификации на EAP-TLS, по сертификату (рис. 7). Данное поведение может также рассматриваться, как констатация факта наличия представленного пользователя в корпоративном домене. На практике полученное заключение позволяет установить, что для эксплуатации недостатка не важен используемый механизм аутентификации в беспроводной Enterprise-сети – с использованием учетных данных или по сертификату.

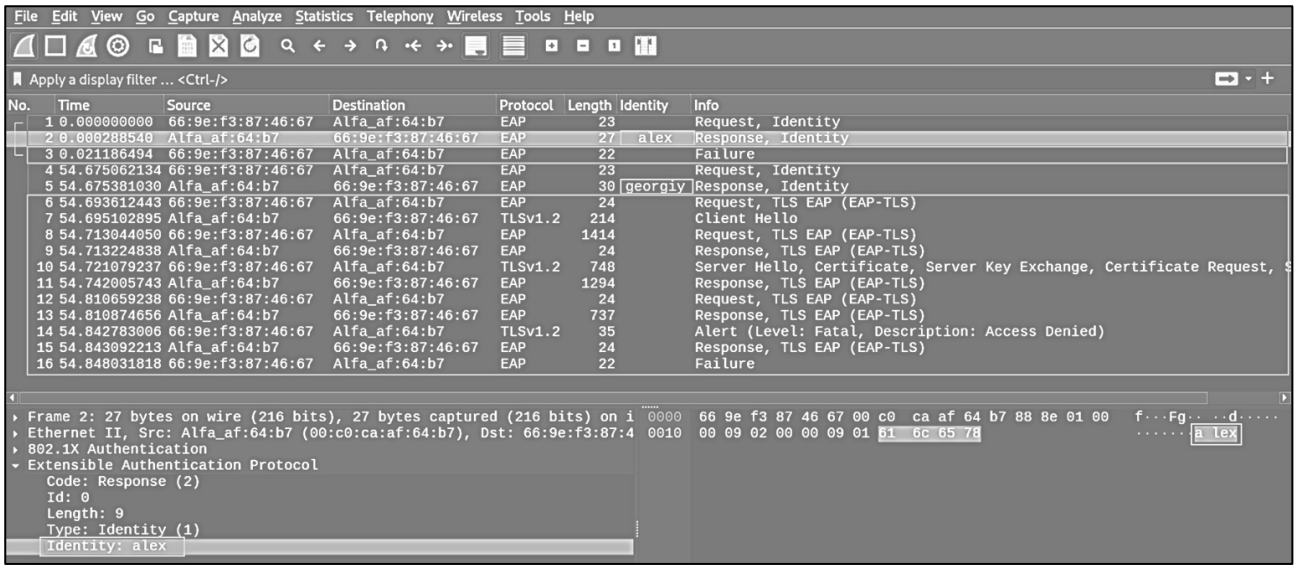

Рис. 6. Проверка наличия недостатка при аутентификации по протоколу EAP-TLS

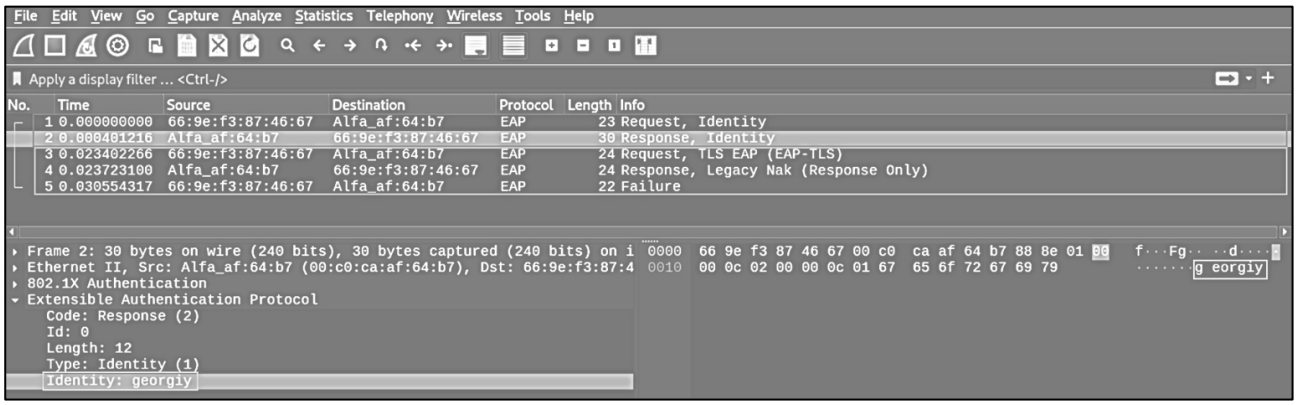

Рис. 7. Попытка принудительного подключения по протоколу EAP-PEAP

2 Практическая демонстрация возможности реализации атаки перечисления пользователей

Анализ функционирования сервера Microsoft NPS, развернутого на платформе Windows Server 2022, выявил возможность определения существования учетных записей пользователей в домене Microsoft Active Directory. Данный механизм фактически демонстрирует наличие уязвимости, связанной с возможностью перечисления пользователей (User Enumeration), что может быть использовано неавторизованным злоумышленником, обладающим физическим доступом к зоне действия беспроводной сети, для выявления перечня учетных записей, зарегистрированных в корпоративном домене Active Directory [6]. В дальнейшем полученный список может быть задействован злоумышленником для развития ряда атак, включая атаку распыления паролей (как на беспроводную сеть, так и на другие корпоративные сервисы, интегрированные в инфраструктуру организации), а также проведение атак, основанных на методах социальной инженерии (например, фишинговые атаки при наличии корпоративной почтовой инфраструктуры).

Процесс атаки на перечисление пользователей может быть полностью автоматизирован. В качестве подтверждения данной возможности был разработан демонстрационный программный инструмент с использованием языка программирования Python и его стандартных библиотек subprocess, time, os и argparse.

Разработанный инструмент осуществляет автоматизированный процесс аутентификации пользователей в

беспроводных сетях стандарта WPA2-Enterprise с использованием механизма EAP-PEAP и протокола MSCHAPv2. На первом этапе функционирования выполняется обработка входных параметров, передаваемых через аргументы командной строки, включая идентификатор беспроводного интерфейса, SSID сети и путь к файлу, содержащему предварительно составленный перечень имен пользователей. Затем осуществляется последовательное считывание списка пользователей, после чего для каждого из них инициируется процедура установления соединения.

Перед каждой попыткой аутентификации, с использованием инструмента tshark активируется пассивный сбор сетевого трафика, содержащего пакеты протокола EAP/EAPOL. Далее создается новое подключение к сети с заданными параметрами, включающими SSID и алгоритмы аутентификации, после чего инициируется процесс передачи учетных данных. По завершении попытки соединения выполняется анализ захваченного трафика с целью определения ответа сервера аутентификации и установления статуса пользователя («учетная запись существует», «успешная аутентификация» или «пользователь не зарегистрирован в системе»). Завершающий этап работы включает очистку временных данных, удаление PCAP-файла и переход к следующему идентификатору из списка.

Процесс функционирования разработанного инструмента и результаты его работы представлены на рис. 8.

```
└─$ sudo python3 user_enumeration_enterprise.py --iface wlan1 --ssid "enterprise_lab2" --names_file names.txt
🔗 Пробуем подключиться как 'john'...
✓ john: Пользователь не существует
🔗 Пробуем подключиться как 'petr'...
✓ petr: Пользователь существует
🔗 Пробуем подключиться как 'ivan'...
✓ ivan: Успешная авторизация
🔗 Пробуем подключиться как 'alex'...
✓ alex: Пользователь не существует
🔗 Пробуем подключиться как 'georgiy'...
✓ georgiy: Пользователь существует
🔗 Пробуем подключиться как 'semen'...
✓ semen: Пользователь не существует
🔗 Пробуем подключиться как 'maria'...
✓ maria: Пользователь существует
```

Рис. 8. Автоматизированный процесс перечисления пользователей с использованием Enterprise-сети

3 Применение атаки перечисления пользователей и способы её противодействия

Разработанный демонстрационный инструмент, хотя и позволяет осуществлять атаку на перечисление пользователей, обладает ограниченной практической значимостью. Это обусловлено простотой применяемых компонентов и высоким уровнем абстракции, необходимым для обеспечения универсальности работы инструмента в отношении беспроводных точек доступа различных производителей.

Так, для корректного функционирования утилиты требуется операционная система семейства Linux с установленными инструментами nmcli и tshark, а также наличие административных привилегий, необходимых для выполнения сетевых операций и мониторинга трафика. Беспроводной интерфейс должен работать в управляемом режиме (managed mode) и поддерживать аутентификацию по стандарту WPA2-Enterprise.

Ключевым недостатком используемого в инструменте подхода является невысокая скорость работы. Атака на перечисление пользователей реализуется посредством полной инициализации подключения к беспроводной сети. В среднем одной сетевой карте требуется около 15 секунд (в зависимости от характеристик точки доступа) для проверки существования одного пользователя.

В случае, если в организации применяется формат именования учетных записей вида «имя_фамилия» (например, «aleksandr_ivanov»), потенциальный

злоумышленник, используя 1000 наиболее распространенных фамилий и 100 наиболее популярных имен, будет вынужден проверить 100.000 возможных учетных записей. При текущей скорости работы утилиты этот процесс займет порядка 17 дней непрерывной работы, что может сильно замедлить процесс атаки и привести к обнаружению атакующего средствами защиты или сотрудникам отделов мониторинга.

Для ускорения атаки возможно использование нескольких сетевых интерфейсов, что позволит проводить параллельное перечисление пользователей. Однако существенное повышение производительности может быть достигнуто при применении низкоуровневых методов инициализации подключения к беспроводной сети, например, с использованием библиотеки Scapy для языка программирования Python [7]. Однако данный подход сопряжен с техническими сложностями, связанными с различиями в функционировании беспроводных сетевых адаптеров, что затрудняет разработку универсального инструмента. Тем не менее, реализация специализированного инструмента, генерирующего индивидуально составленные пакеты для конкретной беспроводной сети, представляется возможной. Внедрение подобного механизма существенно повысит скорость работы утилиты, что сделает данный метод атаки практически значимым.

При рассмотрении возможных способов защиты от данной атаки следует учитывать, что одним из наиболее эффективных решений является использование систем предотвращения вторжений, анализирующих обращения к контроллеру домена. В процессе атаки на перечисление пользователей совершается значительное количество неудачных попыток аутентификации, что может быть выявлено современными системами мониторинга, способными зафиксировать аномальную активность и сформировать инцидент о возможной атаке.

Еще одним важным аспектом защиты является реализация принципа минимально необходимых привилегий. В данном контексте это можно рассматривать, как предоставление прав на подключение к беспроводной Enterprise-сети исключительно тем сотрудникам, которым это необходимо для выполнения служебных обязанностей. Такой подход ограничивает возможность злоумышленника получить полный перечень учетных записей корпоративного домена.

Дополнительно следует учитывать и физические меры защиты. Реализация атаки возможна только при наличии у злоумышленника доступа к беспроводному сигналу. Таким образом, усиление физической охраны объекта, а также контроль мощности сигнала точки доступа, исключающий его распространение за пределы контролируемой зоны, значительно снижают возможности успешного осуществления атаки.

Кроме того, одним из наиболее очевидных способов защиты является полный отказ от использования Enterprise-сетей в пользу сетей, работающих по механизму PSK. Однако такой подход несет в себе дополнительные риски, включая возможность атак на PMKID, эксплуатацию уязвимости Evil Twin, а также перехват четырехэтапного рукопожатия (4-way handshake) [8]. Помимо этого, важно учитывать, что Enterprise-сети, за счёт применения стороннего Radius-сервера, обладают рядом преимуществ, таких как гибкость настройки и индивидуальная аутентификация, что отсутствует в сетях с единым предустановленным ключом.

Наиболее благоприятным решением данной проблемы может стать выпуск официального исправления от Microsoft, устраняющего выявленную уязвимость. Ошибка, возникающая после получения клиентского запроса Response Identity и указывающая на отсутствие пользователя в домене, предположительно является рудиментарным механизмом оптимизации сетевой нагрузки. Технология Microsoft NPS активно развивается с момента выхода Windows 2003, то есть более 20 лет на момент написания данной работы [9]. В момент его разработки вычислительные мощности сетевых устройств были значительно ниже современных, и раннее завершение аутентификации, при отсутствии пользователя в домене, могло быть

реализовано с целью экономии вычислительных ресурсов. В пользу этого предположения свидетельствуют множественные механизмы оптимизации сетевой нагрузки (например, при репликации контроллеров домена) разработанные в рамках Active Directory и частично сохранившиеся до настоящего времени [10]. Однако в современных условиях экономия ресурсов, создающая угрозу раскрытия информации о пользователях домена, может оказаться неоправданной, учитывая возросшую вычислительную мощность оборудования.

Интересно отметить, что в другой общедоступной реализации Radius-сервера, публичному ПО FreeRADIUS, данная уязвимость отсутствует (рис. 9) [3]. Отсутствие уязвимости и корректное поведение сервера в случае запроса к несуществующему пользователю подтверждают возможность внедрения исправления для Microsoft NPS. На рис. 10 приведен пример неуспешной работы разработанной утилиты в отношении беспроводной Enterprise-сети, использующей FreeRADIUS, что демонстрирует наличие существующего решения для устранения данной проблемы.

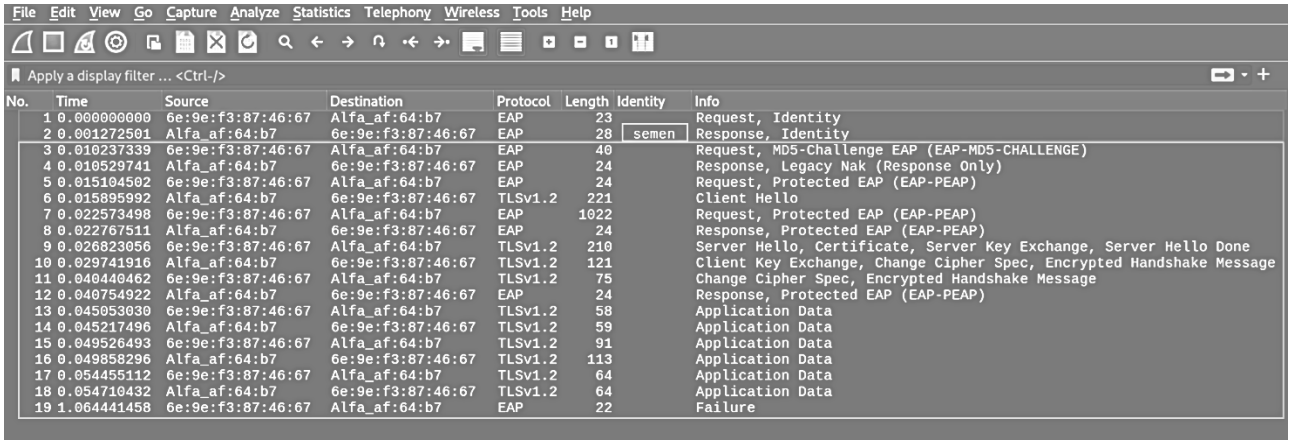

Рис. 9. Демонстрация отсутствие уязвимости при подключении к Enterprise-сети, использующей FreeRadius

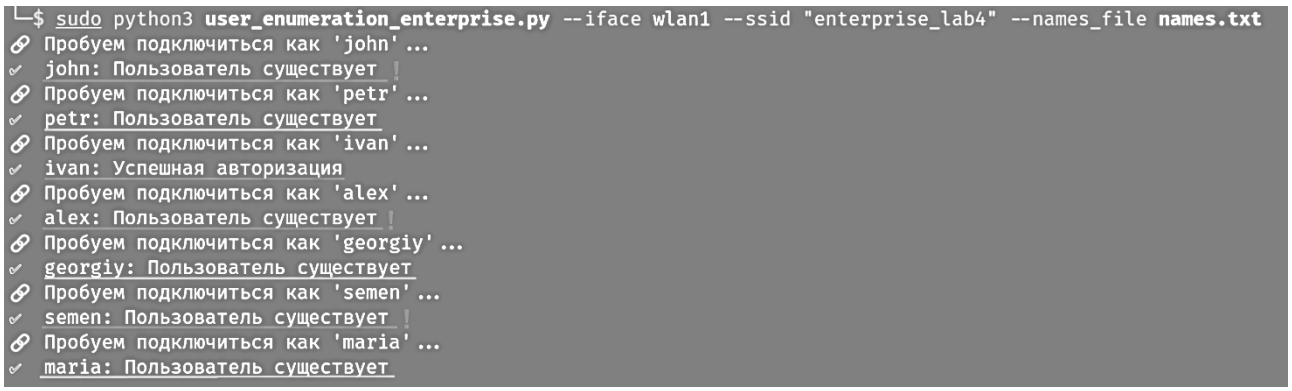

Рис. 10. Демонстрация неуспешной работы утилиты в отношении Enterprise-сети, использующей FreeRadius

Заключение

В ходе проведенного исследования было установлено, что решения, соответствующие современным лучшим практикам и использующие один из наиболее популярных RADIUS-серверов, могут содержать уязвимости, потенциально представляющие угрозу безопасности.

Обнаруженный недостаток, связанный с возможностью перечисления пользователей, а также реализация инструмента, позволяющего эксплуатировать данную уязвимость, подчеркивают вероятность создания более универсальных и высокоскоростных решений, значительно упрощающих процесс сбора информации о сотрудниках организации – учетных записях

домена. Это, в свою очередь, может повысить эффективность разведывательных атак, создавая предпосылки для дальнейших действий, направленных на получение несанкционированного доступа к корпоративной сети.

Разработка и применение официального исправления может способствовать исключению возможности эксплуатации уязвимости. Его реализация на уровне Microsoft NPS представляется технически осуществимой, что подтверждается примером корректной обработки аналогичных запросов к беспроводной сети, использующей FreeRADIUS. Вместе с тем существует вероятность, что Microsoft не расценит выявленную особенность работы RADIUS-сервера как уязвимость. Аналогичный прецедент уже имел место с рядом продуктов Microsoft, включая Outlook Web Access (OWA) и Active Directory Federation Services (AD FS), где анализ времени отклика сервера позволял определить наличие учетной записи в Active Directory. Несмотря на популярность данного метода атаки, сотрудники Microsoft не признали уязвимый механизм угрозой безопасности [11].

В случае отсутствия официального исправления со стороны Microsoft организациям рекомендуется применять методы защиты, представленные в данной работе. Ограничение числа сотрудников, имеющих доступ к беспроводной Enterprise-сети, а также внедрение систем мониторинга, способных в реальном времени выявлять и реагировать на аномальные попытки аутентификации, могут существенно снизить вероятность успешного проведения атаки.

Таким образом, несмотря на потенциально возможные ограничения в вопросе устранении данной уязвимости на уровне Microsoft, грамотная организация защиты корпоративных сетей позволяет минимизировать риски её эксплуатации.

Список литературы

1. Когда и как работодатели возвращают сотрудников с удалёнки. URL: https://hh.ru/article/26942 (дата обращения: 30.04.2025).

2. В России снова растет число опенспейсов. Чем это грозит. URL: https://www.ridus.ru/v-rossii-snova-rastet-chislo-openspejsov-chem-eto-grozit-401404.html (дата обращения: 30.04.2025).

3. WPA2-Enterprise Secure your Organization Wi-Fi Network. URL: https://sysopstechnix.com/wpa2-enterprise-secure-your-organization-wi-fi-network/ (дата обращения 30.04.2025).

4. Цифра дня: сколько российских компаний используют Windows и Office под санкциями. URL: https://www.ferra.ru/news/v-rossii/cifra-dnya-skolko-rossiiskikh-kompanii-ispolzuyut-windows-i-office-pod-sankciyami-25-04-2024.htm (дата обращения: 30.04.2025).

5. RFC5247. Extensible Authentication Protocol (EAP) Key Management Framework. URL: https://datatracker.ietf.org/doc/html/rfc5247 (дата обращения 30.04.2025).

6. What Is User Enumeration? URL: https://www.rapid7.com/blog/post/2017/06/15/about-user-enumeration (дата обращения: 30.04.2025).

7. Scapy Tutorial: WiFi Security. URL: http://www.cs.toronto.edu/~arnold/427/18s/427_18S/indepth/scapy_wifi/scapy_tut.html (дата обращения 30.04.2025).

8. Vink M. A Comprehensive Taxonomy of Wi-Fi Attacks / M. Vink. – Nijmegen: Master Thesis Cyber Security, 2020. 78 с.

9. Сервер политики сети (NPS) | Microsoft Learn. URL: https://learn.microsoft.com/ru-ru/windows-server/networking/technologies/nps/nps-top (дата обращения 30.04.2025).

10. Desmond B. Active Directory: Designing, Deploying, and Running Active Directory / B. Desmond, J, Richards, R. Allen, A.G. Lowe-Norris. – Sebastopol: O'Reilly, 2008. 866 с.

11. User Enumeration in Microsoft Products: An Incident Waiting to Happen? URL: https://www.intruder.io/blog/user-enumeration-in-microsoft-products-an-incident-waiting-to-happen (дата обращения: 30.04.2025).

РГГУ – Российский государственный гуманитарный университет
RSUH – Russian State University for the Humanities

Поступила в редакцию 3.05.25

Информация об авторах

Лось Владимир Павлович – д-р воен. наук, профессор, Российский государственный гуманитарный университет, e-mail: los-vladimir@yandex.ru

Иванов Александр Григорьевич – аспирант, Российский государственный гуманитарный университет, e-mail: alexandr.link.ivanov@gmail.com

Просветов Роман Евгеньевич – независимый исследователь, сотрудник ООО «АТ Груп» («Angara Security»), e-mail: r.prosvetov@angarasecurity.ru

USER ENUMERATION VULNERABILITY IN ENTERPRISE MICROSOFT NPS-BASED WI-FI NETWORKS

V.P. Los, A. G. Ivanov, R. E. Prosvetov

With the evolution of mobile computers and smart devices, more and more organizations are implementing enterprise wireless networks focused on modern security standards. One of the key elements of such networks is the use of Enterprise-authentication based on Radius server, among which Microsoft Network Policy Server (NPS) is widely used. This server attracts attention due to its easy deployment and convenient integration with the existing Active Directory domain infrastructure, which makes it a popular solution for centralized user authentication. In the current research, a weakness of Microsoft NPS was identified which allows unauthorized users to enumerate corporate domain accounts. This paper discusses this flaw in detail, analyzes the mechanisms and methods for exploiting it, and proposes a method for automated implementation of the attack. In conclusion, recommendations are provided for correcting the detected flaw.

Keywords: wireless networks, user enumeration, Enterprise-network, vulnerability, weakness, exploitation, exploit.

Submitted 3.05.25

Information about the authors

Vladimir P. Los – Dr. Sc. (Military), RSUH – Russian State University for the Humanities, e-mail: los-vladimir@yandex.ru

Alexander G. Ivanov – postgraduate student, RSUH – Russian State University for the Humanities, e-mail: alexandr.link.ivanov@gmail.com

Roman E. Prosvetov – independent researcher, employee of LLC «АТ Груп» («Angara Security»), e-mail: r.prosvetov@angarasecurity.ru