Павловский Владимир Владимирович

научный руководитель,

Преподаватель кафедры безопасности информационных технологий, РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва

Паисов Артём Юрьевич

Беев Кирилл Артёмович

студенты, РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва

ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ МЕХАНИЗМОВ АУТЕНТИФИКАЦИИ И КОНТРОЛЯ ДОСТУПА В VESR

Аннотация. Статья посвящена экспериментальному исследованию устойчивости механизмов аутентификации и контроля доступа на платформе виртуального маршрутизатора Eltex vESR версии 1.18.9 в среде виртуализации GNS3. Актуальность работы определяется необходимостью объективной оценки защищённости отечественного сетевого оборудования в контексте импортозамещения. В ходе исследования проведены три серии экспериментов: атака перебором паролей SSH-сервиса (brute-force) с использованием утилиты Hydra, перехват канального трафика аутентификации посредством ARP Spoofing (ettercap), а также попытка обхода списков контроля доступа (ACL) через подмену IP-адреса источника (IP Spoofing, hping3). Для каждого вектора атаки продемонстрированы как уязвимости при отсутствии защитных механизмов, так и эффективность контрмер: ограничение числа попыток входа, статические ARP-записи совместно с Dynamic ARP Inspection (DAI), а также Unicast Reverse Path Forwarding (uRPF). Результаты подтверждают, что платформа vESR при корректной настройке обеспечивает эффективное противодействие рассмотренным атакам.

Annotation. *This article presents an experimental study of the resilience of authentication and access control mechanisms on the Eltex vESR virtual router platform (version 1.18.9) deployed in a GNS3 virtualization environment. Three series of experiments were conducted: SSH*

brute-force attack using Hydra, interception of authentication traffic via ARP Spoofing (ettercap), and an attempt to bypass Access Control Lists (ACLs) through IP Spoofing (hping3). The results confirm that the vESR platform, when properly configured, provides effective resistance to the examined attacks.

Ключевые слова: vESR; аутентификация; контроль доступа; SSH brute-force; ARP Spoofing; IP Spoofing; ACL; uRPF; DAI; Eltex; GNS3; сетевая безопасность; Hydra; ettercap; hping3; импортозамещение.

Keywords: *vESR; authentication; access control; SSH brute-force; ARP Spoofing; IP Spoofing; ACL; uRPF; DAI; Eltex; GNS3; network security; Hydra; ettercap; hping3; import substitution.*

ВВЕДЕНИЕ: АКТУАЛЬНОСТЬ

В условиях курса на технологический суверенитет и импортозамещение в Российской Федерации особое значение приобретает объективная оценка защищённости отечественного сетевого оборудования. Виртуальный маршрутизатор Eltex vESR, позиционируемый производителем как решение корпоративного класса, активно внедряется в инфраструктуры государственных и коммерческих организаций. Однако само по себе наличие механизмов защиты не гарантирует безопасности – необходима экспериментальная верификация их устойчивости к реальным сценариям атак.

Механизмы аутентификации и контроля доступа являются первым рубежом защиты сетевой инфраструктуры. Компрометация учётных данных маршрутизатора или обход его ACL может привести к полной потере контроля над сетью, перехвату трафика и нарушению конфиденциальности передаваемых данных. Согласно отчётам ФСТЭК России [8], атаки на управляющие интерфейсы сетевого оборудования входят в число наиболее распространённых векторов компрометации корпоративных сетей.

Несмотря на наличие документации производителя [2], в открытых источниках практически отсутствуют независимые исследования, посвящённые практическому тестированию устойчивости защитных

механизмов vESR к типовым сетевым атакам. Данная работа призвана восполнить этот пробел.

ВВЕДЕНИЕ: ОБЪЕКТ, ПРЕДМЕТ, ЦЕЛЬ

Объектом нашего исследования являются механизмы аутентификации и контроля доступа виртуального маршрутизатора Eltex vESR.

Предметом нашего исследования является устойчивость данных механизмов к типовым сетевым атакам: перебору паролей, перехвату трафика аутентификации и подмене адресов источника.

Целью нашего исследования является экспериментальная оценка устойчивости механизмов аутентификации и контроля доступа vESR к выбранным атакам, а также определение эффективных контрмер.

Для достижения поставленной нами цели мы поставили себе следующие задачи:

1. Развернуть тестовый стенд в среде GNS3 с топологией, моделирующей типовой сегмент корпоративной сети.

2. Провести атаку перебором паролей (brute-force) на SSH-сервис vESR, оценить скорость подбора и эффективность ограничительных мер.

3. Выполнить перехват канального трафика аутентификации посредством ARP Spoofing и оценить возможность извлечения учётных данных.

4. Попытаться обойти списки контроля доступа (ACL) через IP Spoofing и проверить эффективность uRPF.

5. Провести аудит криптографических настроек SSH-сервера vESR и оценить соответствие используемых алгоритмов актуальным стандартам безопасности.

6. Сформулировать практические рекомендации по защите vESR.

МЕТОДЫ ИССЛЕДОВАНИЯ

В рамках проведения данного исследования для достижения поставленной цели были применены следующие методы:

Теоретико-аналитический метод. Была изучена документация Eltex и научная литература для исследования механизмов аутентификации и контроля доступа на платформе vESR, а также для составления плана последующего эксперимента.

Метод экспериментального тестирования. Была развёрнута тестовая сеть в GNS3, настроены механизмы аутентификации и ACL. Для проведения атак использовались инструменты Hydra, ettercap, hping3 и nmap, что позволило смоделировать реальные сценарии компрометации.

Метод сравнительного анализа. Для каждого вектора атаки проведено сравнение результатов до и после активации защитных механизмов, что позволило количественно оценить эффективность контрмер.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Таблица 1

Обозначение	**Устройство**	**Платформа**	**IP-адрес**
vESR-Test-PaisovBeev	Тестируемый	Eltex vESR 1.18.9	192.168.1.10
MagistrRTR-PaisovBeev	Магистральный	Eltex vESR 1.18.9	10.0.1.2 / 10.0.2.1
BorderRTR-PaisovBeev	Пограничный	Eltex vESR 1.18.9	10.0.2.2 / 10.0.3.1
IOU1-PaisovBeev	Коммутатор	Cisco IOU L2	192.168.1.1
Paisov-Beev-adminPC	Администратор	ALT Linux 10.0	192.168.1.100
Paisov-Beev-userPC	Пользователь	ALT Linux 10.0	192.168.1.200
Paisov-Beev-Kali	Атакующий	Kali Linux	192.168.1.50

1. Настроим маршрутизаторы так, чтобы получилась топология, соответствующая рисунку 1.

Рисунок 1 – Топология тестового стенда в GNS3

Выставим IP-адреса на интерфейсы каждого из устройств в соответствии с топологией. Результат для vESR-Test-PaisovBeev и MagistrRTR-PaisovBeev представлен на рисунках 2 и 3 соответственно.

```
vESR-Test-PaisovBeev(config)# interface gi1/0/1
vESR-Test-PaisovBeev(config-if-gi)# description "To IOU1 (Management VLAN)"
vESR-Test-PaisovBeev(config-if-gi)# ip firewall disable
vESR-Test-PaisovBeev(config-if-gi)# ip address 192.168.1.10/24
vESR-Test-PaisovBeev(config-if-gi)# exit
vESR-Test-PaisovBeev(config)#
vESR-Test-PaisovBeev(config)# interface gi1/0/2
vESR-Test-PaisovBeev(config-if-gi)# description "To MagistrRTR-PaisovBeev"
vESR-Test-PaisovBeev(config-if-gi)# ip firewall disable
vESR-Test-PaisovBeev(config-if-gi)# ip address 10.0.1.1/30
vESR-Test-PaisovBeev(config-if-gi)# exit
vESR-Test-PaisovBeev(config)#
vESR-Test-PaisovBeev(config)# ip route 10.0.2.0/30 10.0.1.2
vESR-Test-PaisovBeev(config)# ip route 10.0.3.0/30 10.0.1.2
vESR-Test-PaisovBeev(config)# exit
Warning: you have uncommitted configuration changes.
vESR-Test-PaisovBeev# commit
Configuration has been successfully applied and saved to flash. Commit timer started,
changes will be reverted in 600 seconds.
vESR-Test-PaisovBeev# confirm
Configuration has been confirmed. Commit timer canceled.
```

Рисунок 2 – Настроенные IP-адреса на vESR-Test-PaisovBeev

```
MagistrRTR-PaisovBeev(config)# interface gi1/0/1
MagistrRTR-PaisovBeev(config-if-gi)# description "To vESR-Test-PaisovBeev"
MagistrRTR-PaisovBeev(config-if-gi)# ip firewall disable
MagistrRTR-PaisovBeev(config-if-gi)# ip address 10.0.1.2/30
MagistrRTR-PaisovBeev(config-if-gi)# exit
MagistrRTR-PaisovBeev(config)#
MagistrRTR-PaisovBeev(config)# interface gi1/0/2
MagistrRTR-PaisovBeev(config-if-gi)# description "To BorderRTR-PaisovBeev"
MagistrRTR-PaisovBeev(config-if-gi)# ip firewall disable
MagistrRTR-PaisovBeev(config-if-gi)# ip address 10.0.2.1/30
MagistrRTR-PaisovBeev(config-if-gi)# exit
MagistrRTR-PaisovBeev(config)#
MagistrRTR-PaisovBeev(config)# ip route 192.168.1.0/24 10.0.1.1
MagistrRTR-PaisovBeev(config)# ip route 10.0.3.0/30 10.0.2.2
MagistrRTR-PaisovBeev(config)# exit
Warning: you have uncommitted configuration changes.
MagistrRTR-PaisovBeev# commit
Configuration has been successfully applied and saved to flash. Commit timer started,
changes will be reverted in 600 seconds.
MagistrRTR-PaisovBeev# confirm
Configuration has been confirmed. Commit timer canceled.
```

Рисунок 3 – Настроенные IP-адреса на MagistrRTR-PaisovBeev

Настройка Paisov-Beev-adminPC представлена на рисунке 4. Paisov-Beev-userPC и Paisov-Beev-Kali по аналогии.

```
[root@Paisov-Beev-adminPC ~]# hostnamectl set-hostname Paisov-Beev-adminPC
[root@Paisov-Beev-adminPC ~]# ip addr add 192.168.1.100/24 dev eth0
[root@Paisov-Beev-adminPC ~]# ip link set eth0 up
[root@Paisov-Beev-adminPC ~]# ip route add default via 192.168.1.1

[root@Paisov-Beev-adminPC ~]# ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 0c:a4:2e:b1:33:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 scope global eth0
       valid_lft forever preferred_lft forever
```

Рисунок 4 – Настройка Paisov-Beev-adminPC

2. Пропишем статические маршруты на маршрутизаторах, после чего проверим связность между Paisov-Beev-adminPC и vESR-Test-PaisovBeev. Результат представлен на рисунке 5. Как мы видим, связность есть.

```
[root@Paisov-Beev-adminPC ~]# ping -c 3 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=0.612 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=0.347 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=64 time=0.329 ms

--- 192.168.1.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.329/0.429/0.612/0.129 ms

— Ping от Paisov-Beev-adminPC до BorderRTR-PaisovBeev —
[root@Paisov-Beev-adminPC ~]# ping -c 3 10.0.2.2
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2: icmp_seq=1 ttl=62 time=1.204 ms
64 bytes from 10.0.2.2: icmp_seq=2 ttl=62 time=0.876 ms
64 bytes from 10.0.2.2: icmp_seq=3 ttl=62 time=0.851 ms

--- 10.0.2.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.851/0.977/1.204/0.162 ms
```

Рисунок 5 – Проверка связности между ПК

Эксперимент 1. Атака перебором паролей на SSH (brute-force)

3. Настроим SSH-сервер на vESR-Test-PaisovBeev. Создадим две локальные учётные записи: admin (привилегированный доступ) и operator (ограниченный доступ). Активируем SSH-сервер. Результат представлен на рисунке 6.

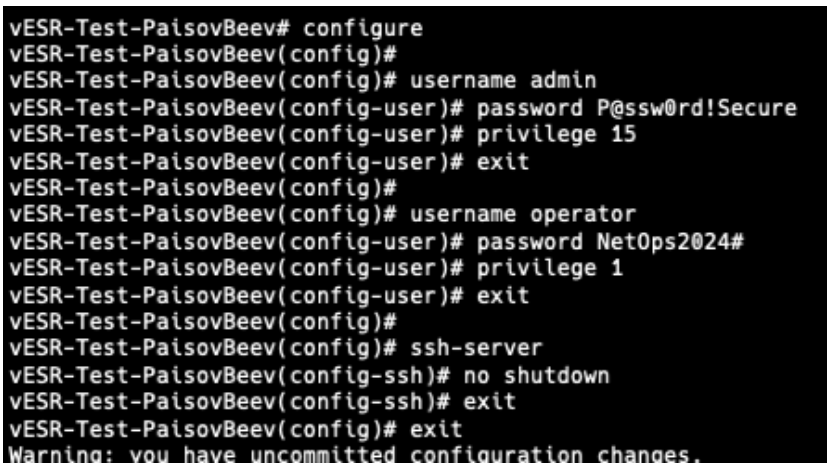

Рисунок 6 – Настройка SSH-сервера и учётных записей на vESR-Test-PaisovBeev

4. Проверим доступность SSH-сервиса с помощью nmap с атакующей машины. Результат представлен на рисунке 7.

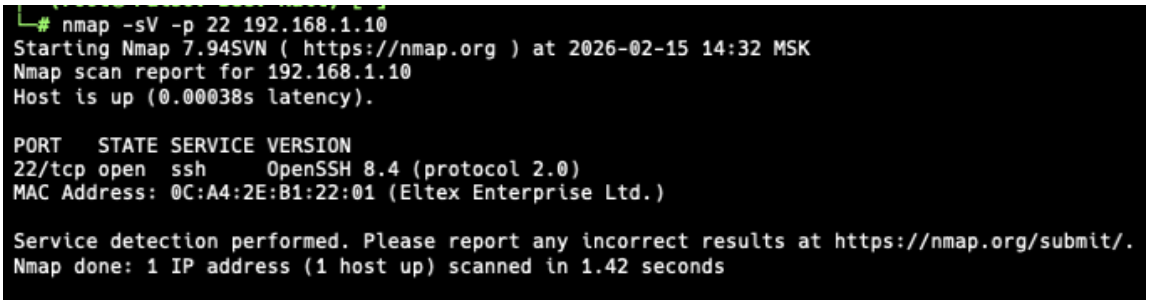

Рисунок 7 – Сканирование nmap порта 22 на vESR-Test-PaisovBeev

5. Подготовим словари логинов и паролей на Paisov-Beev-Kali и запустим утилиту Hydra для атаки перебором. Результат представлен на рисунке 8.

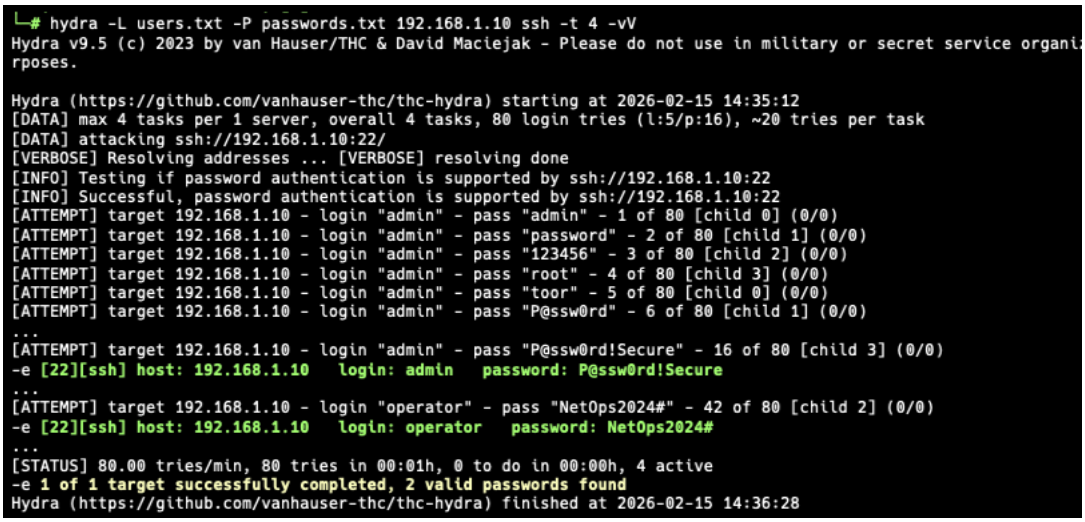

Рисунок 8 – Результат brute-force атаки Hydra (без защиты)

Как мы видим, оба пароля были подобраны. Для обеспечения воспроизводимости результатов эксперимент был повторён 5 раз. Характеристики атаки: словарь логинов – 5 записей (admin, root, operator, user, test), словарь паролей – 16 записей (типичные слабые пароли и целевые), общее число комбинаций – 80, параллельность – 4 потока. Среднее время подбора обоих паролей составило 76 ± 4 секунды (min 71, max 82 сек). Загрузка CPU виртуальной машины vESR во время атаки возросла с 2–3% в режиме ожидания до 8–12%, что свидетельствует о невысокой ресурсоёмкости обработки SSH-подключений. Пропускная способность виртуального канала GNS3 не являлась ограничивающим фактором. Следует отметить, что полученные результаты носят демонстрационный характер: в реальных условиях скорость подбора зависит от сложности паролей, ширины канала и настроек оборудования. В логах vESR-Test-PaisovBeev зафиксировано множество событий SSH-4-LOGIN_FAILED с последующими SSH-6-LOGIN_SUCCESS. Результат логирования представлен на рисунке 9.

```
Feb 15 14:35:13: %SSH-4-LOGIN_FAILED: Login failed for user 'admin' from 192.168.1.50 port 48231
Feb 15 14:35:14: %SSH-4-LOGIN_FAILED: Login failed for user 'admin' from 192.168.1.50 port 48232
Feb 15 14:35:14: %SSH-4-LOGIN_FAILED: Login failed for user 'admin' from 192.168.1.50 port 48233
Feb 15 14:35:15: %SSH-4-LOGIN_FAILED: Login failed for user 'admin' from 192.168.1.50 port 48234
Feb 15 14:35:16: %SSH-4-LOGIN_FAILED: Login failed for user 'admin' from 192.168.1.50 port 48235
Feb 15 14:35:17: %SSH-4-LOGIN_FAILED: Login failed for user 'root' from 192.168.1.50 port 48236
Feb 15 14:35:18: %SSH-4-LOGIN_FAILED: Login failed for user 'root' from 192.168.1.50 port 48237
...
Feb 15 14:35:48: %SSH-6-LOGIN_SUCCESS: User 'admin' logged in from 192.168.1.50 port 48261
...
Feb 15 14:36:12: %SSH-6-LOGIN_SUCCESS: User 'operator' logged in from 192.168.1.50 port 48274
...
Feb 15 14:36:28: %SSH-4-DISCONNECT: Session from 192.168.1.50 port 48261 disconnected
```

Рисунок 9 – Логи SSH на vESR-Test-PaisovBeev (неудачные попытки)

6. Настроим защиту от brute-force на vESR-Test-PaisovBeev: ограничение попыток аутентификации (max-auth-tries 3), таймаут (login-timeout 30 сек), блокировку хоста после 5 неудачных попыток на 300 секунд, минимальную длину пароля 12 символов. Результат настройки представлен на рисунке 10.

```
vESR-Test-PaisovBeev(config)# ssh-server
vESR-Test-PaisovBeev(config-ssh)# max-auth-tries 3
vESR-Test-PaisovBeev(config-ssh)# login-timeout 30
vESR-Test-PaisovBeev(config-ssh)# exit
vESR-Test-PaisovBeev(config)#
vESR-Test-PaisovBeev(config)# security passwords min-length 12
vESR-Test-PaisovBeev(config)# security login-attempts max-fail 5
vESR-Test-PaisovBeev(config)# security login-attempts block-time 300
vESR-Test-PaisovBeev(config)#
vESR-Test-PaisovBeev(config)# exit
Warning: you have uncommitted configuration changes.
vESR-Test-PaisovBeev# commit
Configuration has been successfully applied and saved to flash. Commit timer started,
changes will be reverted in 600 seconds.
vESR-Test-PaisovBeev# confirm
```

Рисунок 10 – Настройка защиты от brute-force на vESR-Test-PaisovBeev

7. Повторим атаку Hydra. Результат представлен на рисунке 11.

```
└─# hydra -L users.txt -P passwords.txt 192.168.1.10 ssh -t 4 -vV
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service or
rposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-15 15:02:44
[DATA] max 4 tasks per 1 server, overall 4 tasks, 80 login tries (l:5/p:16), ~20 tries per task
[DATA] attacking ssh://192.168.1.10:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://192.168.1.10:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.10:22
[ATTEMPT] target 192.168.1.10 - login "admin" - pass "admin" - 1 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "admin" - pass "password" - 2 of 80 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "admin" - pass "123456" - 3 of 80 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "admin" - pass "root" - 4 of 80 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "admin" - pass "toor" - 5 of 80 [child 0] (0/0)
-e [ERROR] target 192.168.1.10 - login "admin" - could not connect to target port 22: Connection refused
-e [ERROR] target 192.168.1.10 - login "admin" - could not connect to target port 22: Connection refused
-e [ERROR] target 192.168.1.10 - login "admin" - could not connect to target port 22: Connection refused
[STATUS] Waiting 30 seconds before retry...
-e [ERROR] target 192.168.1.10 - login "admin" - could not connect to target port 22: Connection refused
-e [ERROR] target 192.168.1.10 - login "admin" - could not connect to target port 22: Connection refused
...
-e [ERROR] could not connect to target port 22: Connection refused (retrying 5 of 5)
-e [ERROR] all children were disabled due to too many connection errors
0 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-15 15:08:17
```

Рисунок 11 – Результат повторной brute-force атаки (с защитой)

Как мы видим, после 5 неудачных попыток хост 192.168.1.50 был заблокирован. Hydra получила отказ в подключении (Connection refused). При этом легитимный SSH-доступ с Paisov-Beev-adminPC сохранился. Статус блокировки представлен на рисунке 12.

```
Feb 15 15:02:45: %SSH-4-LOGIN_FAILED: Login failed for user 'admin' from 192.168.1.50 port 52101
Feb 15 15:02:46: %SSH-4-LOGIN_FAILED: Login failed for user 'admin' from 192.168.1.50 port 52102
Feb 15 15:02:47: %SSH-4-LOGIN_FAILED: Login failed for user 'admin' from 192.168.1.50 port 52103
Feb 15 15:02:48: %SSH-4-LOGIN_FAILED: Login failed for user 'admin' from 192.168.1.50 port 52104
Feb 15 15:02:48: %SSH-4-LOGIN_FAILED: Login failed for user 'admin' from 192.168.1.50 port 52105
Feb 15 15:02:49: %SEC-3-HOST_BLOCKED: Host 192.168.1.50 blocked for 300 seconds (5 failed attempts)
Feb 15 15:02:50: %SSH-4-CONNECTION_REFUSED: Connection from 192.168.1.50 port 52106 refused (host blocked)
Feb 15 15:02:51: %SSH-4-CONNECTION_REFUSED: Connection from 192.168.1.50 port 52107 refused (host blocked)
```

Рисунок 12 – Статус блокировки хоста и логи vESR-Test-PaisovBeev

Таблица 2 – Результаты эксперимента SSH brute-force

Параметр	**Без защиты**	**С защитой**
Подбор пароля	Успех (2 пароля)	Неудача
Время до результата	76 секунд	Блокировка через 5 попыток

Легитимный доступ	Работает	Работает
Лог-событие	LOGIN_SUCCESS (атакующий)	HOST_BLOCKED

Выполнение задачи 5: аудит криптографических настроек SSH. Помимо защиты от перебора паролей, важно оценить криптографическую стойкость самого SSH-канала. Для этого был проведён аудит конфигурации SSH-сервера vESR-Test-PaisovBeev.

Анализ показал, что vESR-Test-PaisovBeev в конфигурации по умолчанию использует следующие параметры: обмен ключами – diffie-hellman-group14-sha256, алгоритмы хоста – ssh-rsa и ecdsa-sha2-nistp256, шифры – aes128-ctr и aes256-ctr, MAC – hmac-sha2-256 и hmac-sha2-512. Указанные алгоритмы соответствуют актуальным рекомендациям NIST SP 800-131A [13] и не содержат устаревших или скомпрометированных вариантов (таких как diffie-hellman-group1-sha1, arcfour, hmac-md5).

Тем не менее, для повышения безопасности рекомендуется отключить алгоритм ssh-rsa (в пользу ecdsa или ed25519) [13], а также явно ограничить набор разрешённых шифров и алгоритмов обмена ключами в конфигурации SSH-сервера, исключив потенциально уязвимые варианты. Устойчивость к перебору паролей не гарантирует общую криптографическую стойкость канала управления при наличии уязвимостей в настройках протокола.

Эксперимент 2. Перехват трафика аутентификации (ARP Spoofing)

8. Зафиксируем ARP-таблицу Paisov-Beev-adminPC и vESR-Test-PaisovBeev до начала атаки. Результат представлен на рисунке 13.

```
[root@Paisov-Beev-adminPC ~]# arp -a
? (192.168.1.10) at 0c:a4:2e:b1:22:01 [ether] on eth0
? (192.168.1.1) at 0c:a4:2e:00:00:01 [ether] on eth0
? (192.168.1.50) at 0c:a4:2e:b1:33:03 [ether] on eth0

— ARP-таблица vESR-Test-PaisovBeev —
vESR-Test-PaisovBeev# show arp
Protocol  Address         Age (min)  Hardware Addr   Interface
Internet  192.168.1.100   3          0c:a4:2e:b1:33:01  gi1/0/1
Internet  192.168.1.50    2          0c:a4:2e:b1:33:03  gi1/0/1
Internet  192.168.1.200   5          0c:a4:2e:b1:33:02  gi1/0/1
Internet  192.168.1.1     1          0c:a4:2e:00:00:01  gi1/0/1
```

Рисунок 13 – ARP-таблицы до атаки

9. На Paisov-Beev-Kali включим IP-пересылку и запустим ettercap в режиме ARP poisoning. Цели: Paisov-Beev-adminPC (192.168.1.100) и vESR-Test-PaisovBeev (192.168.1.10). Результат представлен на рисунке 14.

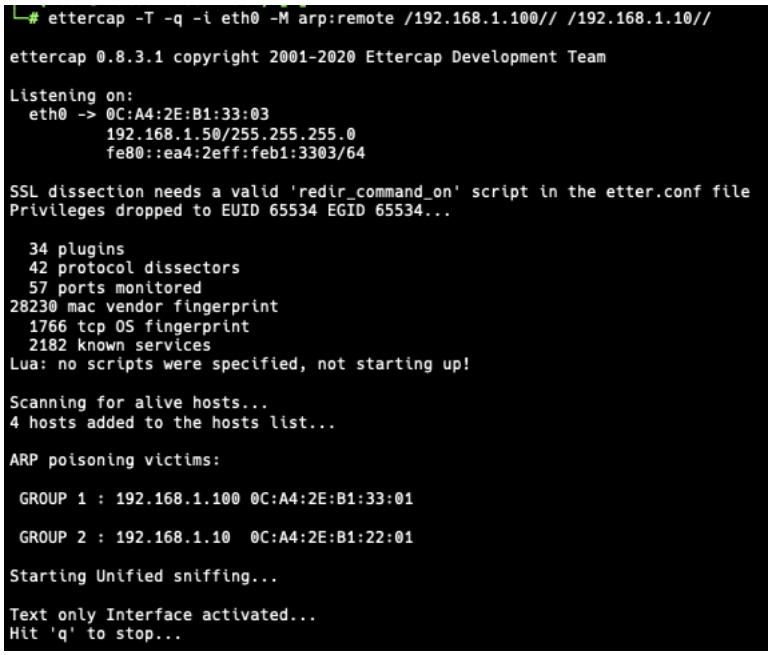

Рисунок 14 – Запуск ettercap (ARP Spoofing)

10. Проверим ARP-таблицу Paisov-Beev-adminPC после начала атаки. Результат представлен на рисунке 15.

Рисунок 15 – ARP-таблица Paisov-Beev-adminPC после атаки (MAC подменён)

Как мы видим, MAC-адрес vESR-Test-PaisovBeev в ARP-таблице adminPC заменён на MAC атакующей машины. MITM-позиция достигнута – весь трафик между adminPC и vESR проходит через Paisov-Beev-Kali.

11. Параллельно запустим tcpdump на Paisov-Beev-Kali для захвата трафика. Затем с Paisov-Beev-adminPC подключимся к vESR по SSH. Проанализируем захваченный дамп. Результат представлен на рисунках 16-17.

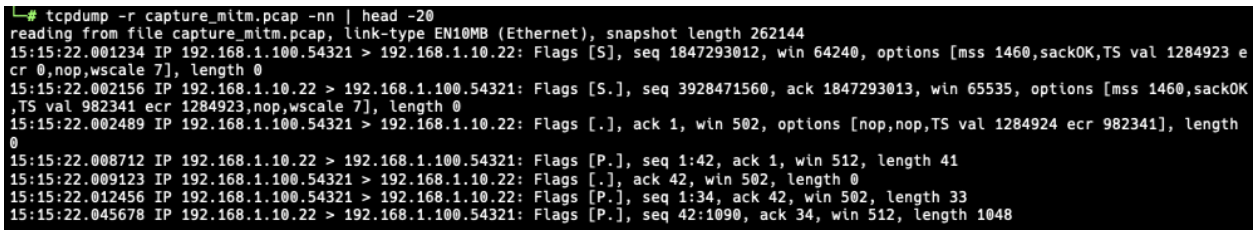

Рисунок 16 – Захват трафика tcpdump во время SSH-сессии

Рисунок 17 – Анализ дампа – пароль зашифрован (SSH)

Как мы видим, SSH-хэндшейк виден в открытом виде, но сами данные аутентификации (пароль) зашифрованы – извлечь учётные данные не удалось. Тем не менее сам факт достижения MITM-позиции представляет угрозу: при использовании незащищённых протоколов (Telnet, HTTP) пароли были бы перехвачены.

12. Настроим защиту: на vESR-Test-PaisovBeev создадим статическую ARP-запись для adminPC. На коммутаторе IOU1-PaisovBeev активируем Port Security (1 MAC на порт), Dynamic ARP Inspection (DAI) для VLAN 1, IP Source Guard. Результат настройки представлен на рисунках 18-19.

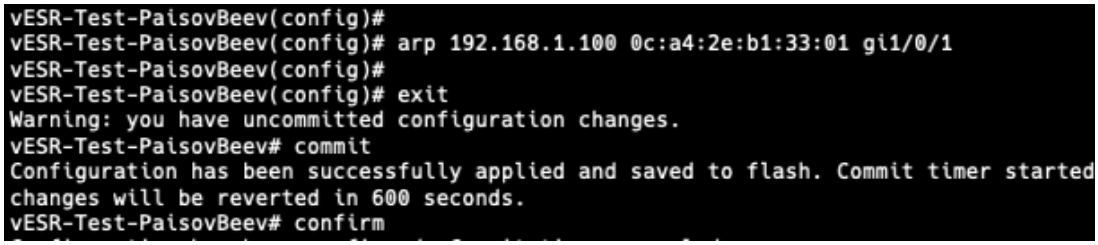

Рисунок 18 – Статическая ARP-запись на vESR-Test-PaisovBeev

```
IOU1-PaisovBeev(config)# interface Ethernet0/0
IOU1-PaisovBeev(config-if)# description "To adminPC"
IOU1-PaisovBeev(config-if)# switchport port-security
IOU1-PaisovBeev(config-if)# switchport port-security maximum 1
IOU1-PaisovBeev(config-if)# switchport port-security mac-address sticky
IOU1-PaisovBeev(config-if)# switchport port-security violation restrict
IOU1-PaisovBeev(config-if)# exit
IOU1-PaisovBeev(config)#
IOU1-PaisovBeev(config)# interface Ethernet0/1
IOU1-PaisovBeev(config-if)# description "To userPC"
IOU1-PaisovBeev(config-if)# switchport port-security
IOU1-PaisovBeev(config-if)# switchport port-security maximum 1
IOU1-PaisovBeev(config-if)# switchport port-security mac-address sticky
IOU1-PaisovBeev(config-if)# switchport port-security violation restrict
IOU1-PaisovBeev(config-if)# exit
IOU1-PaisovBeev(config)#
IOU1-PaisovBeev(config)# interface Ethernet0/2
IOU1-PaisovBeev(config-if)# description "To Kali (ALT-1)"
IOU1-PaisovBeev(config-if)# switchport port-security
IOU1-PaisovBeev(config-if)# switchport port-security maximum 1
IOU1-PaisovBeev(config-if)# switchport port-security mac-address sticky
IOU1-PaisovBeev(config-if)# switchport port-security violation restrict
IOU1-PaisovBeev(config-if)# exit
IOU1-PaisovBeev(config)#
IOU1-PaisovBeev(config)# ip arp inspection vlan 1
IOU1-PaisovBeev(config)#
IOU1-PaisovBeev(config)# interface Ethernet0/3
IOU1-PaisovBeev(config-if)# description "To vESR-Test-PaisovBeev (uplink - trusted)"
IOU1-PaisovBeev(config-if)# ip arp inspection trust
IOU1-PaisovBeev(config-if)# exit
IOU1-PaisovBeev(config)#
IOU1-PaisovBeev(config)# ip dhcp snooping
IOU1-PaisovBeev(config)# ip dhcp snooping vlan 1
IOU1-PaisovBeev(config)# interface Ethernet0/3
IOU1-PaisovBeev(config-if)# ip dhcp snooping trust
IOU1-PaisovBeev(config-if)# exit
IOU1-PaisovBeev(config)#
IOU1-PaisovBeev(config)# ip source binding 0c:a4:2e:b1:33:01 vlan 1 192.168.1.100 interface Ethernet0/0
IOU1-PaisovBeev(config)# ip source binding 0c:a4:2e:b1:33:02 vlan 1 192.168.1.200 interface Ethernet0/1
```

Рисунок 19 – Port Security и DAI на IOU1-PaisovBeev

13. Повторим атаку ettercap. Проверим ARP-таблицу adminPC. Результат представлен на рисунке 20.

```
└─# ettercap -T -q -i eth0 -M arp:remote /192.168.1.100// /192.168.1.10//

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
  eth0 -> 0C:A4:2E:B1:33:03
          192.168.1.50/255.255.255.0

Scanning for alive hosts...
4 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 192.168.1.100 0C:A4:2E:B1:33:01

 GROUP 2 : 192.168.1.10  0C:A4:2E:B1:22:01

Starting Unified sniffing...
```

Рисунок 20 – ARP-таблица после повторной атаки (MAC не изменился)

Как мы видим, ARP-таблица Paisov-Beev-adminPC не была модифицирована. DAI на IOU1-PaisovBeev отклонил 26 поддельных ARP-пакетов. Логи DAI представлены на рисунке 21.

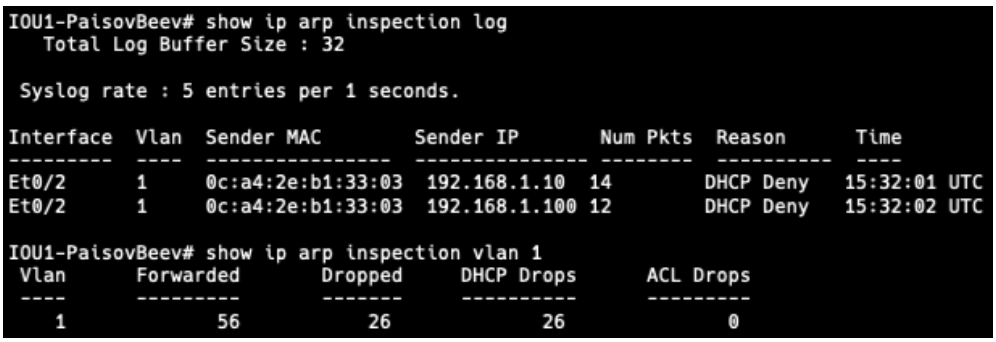

Рисунок 21 – Логи DAI – отброшенные ARP-пакеты

Таблица 3 – Результаты эксперимента ARP Spoofing

Параметр	**Без защиты**	**С защитой**
ARP-таблица подменена	Да	Нет
MITM-позиция	Достигнута	Не достигнута
Перехват пароля SSH	Нет (шифрование)	Нет
DAI: отброшено пакетов	–	26

Эксперимент 3. Обход ACL через IP Spoofing

14. Настроим расширенный ACL на vESR-Test-PaisovBeev, разрешающий SSH только с IP-адреса Paisov-Beev-adminPC (192.168.1.100). ICMP разрешим от всех. Прочий TCP на порт 22 запретим. Результат представлен на рисунке 22.

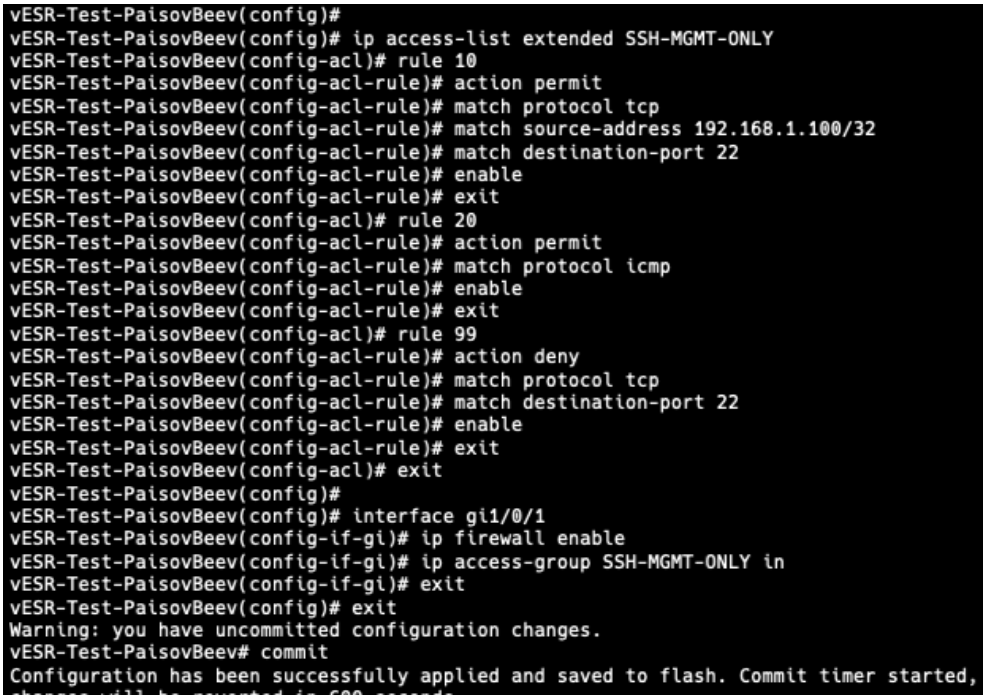

Рисунок 22 – Настройка ACL SSH-MGMT-ONLY на vESR-Test-PaisovBeev

15. Проверим работу ACL: SSH с Paisov-Beev-adminPC – разрешён, SSH с Paisov-Beev-Kali – заблокирован. Результат представлен на рисунке 23.

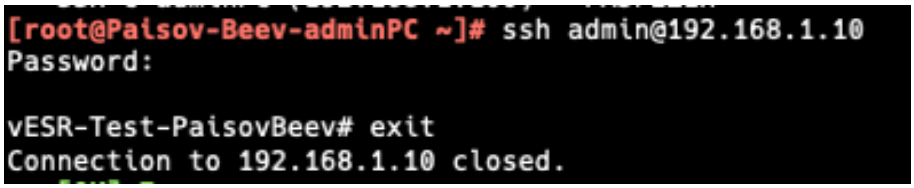

Рисунок 23 – Проверка ACL: доступ с adminPC и Kali

16. С Paisov-Beev-Kali отправим TCP SYN-пакеты на порт 22 vESR с подменённым адресом источника (192.168.1.100) при помощи hping3. Результат представлен на рисунке 24.

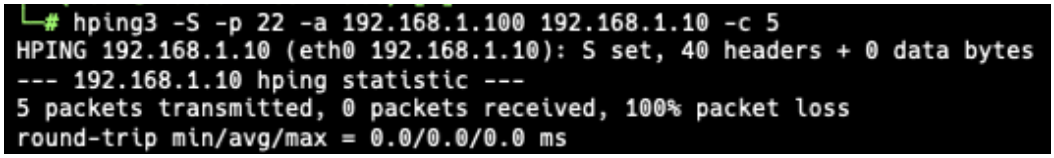

Рисунок 24 – IP Spoofing атака hping3 (без uRPF)

Как мы видим, счётчик rule 10 (permit) ACL увеличился – spoofed пакеты прошли проверку ACL. Однако ответные SYN-ACK-пакеты направлены на настоящий adminPC, а не на Kali. Полноценное TCP-соединение установить невозможно. Тем не менее, данная уязвимость может быть использована для SYN Flood DoS-атак и обхода логирования.

17. Настроим защиту – активируем uRPF в строгом режиме на интерфейсе gi1/0/1 vESR-Test-PaisovBeev. Результат настройки представлен на рисунке 25.

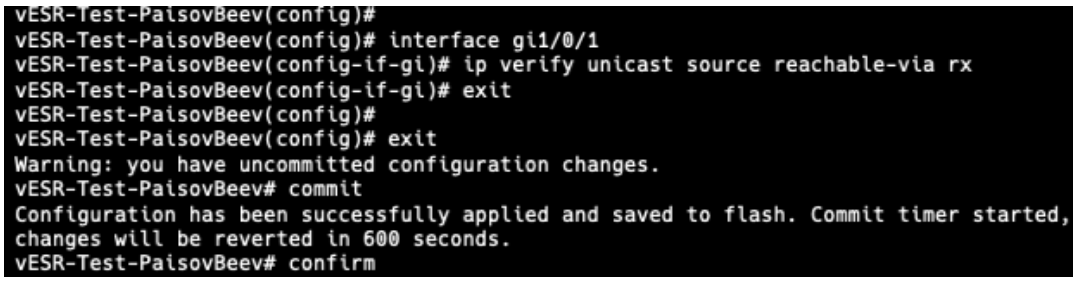

Рисунок 25 – Настройка uRPF на vESR-Test-PaisovBeev

18. Очистим счётчики ACL и повторим атаку hping3. Результат представлен на рисунке 26.

```
└─# hping3 -S -p 22 -a 192.168.1.100 192.168.1.10 -c 5
HPING 192.168.1.10 (eth0 192.168.1.10): S set, 40 headers + 0 data bytes
--- 192.168.1.10 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Рисунок 26 – Повторная IP Spoofing атака (с uRPF) – счётчики ACL

Как мы видим, счётчики ACL не изменились – uRPF отбросил все 5 пакетов до обработки ACL. Статистика uRPF зафиксировала 5 отброшенных пакетов. При этом легитимный SSH с Paisov-Beev-adminPC и ICMP с Paisov-Beev-Kali продолжают работать. Результат представлен на рисунке 27.

```
vESR-Test-PaisovBeev# show ip access-list SSH-MGMT-ONLY
ip access-list extended SSH-MGMT-ONLY
  rule 10
    action: permit
    match: protocol tcp, source 192.168.1.100/32, dst-port 22
    status: enabled
    hits: 7
  rule 20
    action: permit
    match: protocol icmp
    status: enabled
    hits: 0
  rule 99
    action: deny
    match: protocol tcp, dst-port 22
    status: enabled
    hits: 0
```

Рисунок 27 – Статистика uRPF и проверка легитимного доступа

Таблица 4 – Результаты эксперимента IP Spoofing

Параметр	**Без uRPF**	**С uRPF**
Spoofed пакеты прошли ACL	Да (+5 hits)	Нет (0 hits)
uRPF drops	–	5
TCP-сессия установлена	Нет	Нет
Легитимный доступ	Работает	Работает

Таблица 5 – Сводная таблица результатов

Атака	**Без защиты**	**С защитой**	**Контрмера**	**Гипотеза**
SSH Brute-force	Успех (76 сек)	Блокировка	Rate limit + lockout	Подтв.
ARP Spoofing	MITM достигнут	DAI отклонил	Static ARP + DAI	Подтв.
IP Spoofing	ACL обойдён	uRPF блокирует	uRPF strict	Подтв.

РЕКОМЕНДАЦИИ ПО КОНФИГУРИРОВАНИЮ

На основании проведённых экспериментов и анализа результатов сформулированы следующие практические рекомендации по конфигурированию vESR и сопутствующего оборудования для обеспечения устойчивости механизмов аутентификации и контроля доступа (задача 6).

1. Защита SSH от перебора паролей: установить max-auth-tries не более 3, login-timeout не более 30 секунд, активировать блокировку хоста после 5 неудачных попыток (security login-attempts max-fail 5, block-time не менее 300 секунд), задать минимальную длину пароля не менее 12 символов (security passwords min-length 12).

2. Криптографические настройки SSH: отключить алгоритм обмена ключами ssh-rsa в пользу ecdsa-sha2-nistp256 или ssh-ed25519, использовать только шифры aes128-ctr и aes256-ctr, ограничить MAC-алгоритмы значениями hmac-sha2-256 и hmac-sha2-512, отключить устаревшие алгоритмы (diffie-hellman-group1-sha1, arcfour, hmac-md5) [13].

3. Защита от ARP Spoofing: создать статические ARP-записи для критических хостов управления на маршрутизаторе (команда arp <ip> <mac> <interface>), активировать Dynamic ARP Inspection (DAI) на коммутаторах доступа для соответствующих VLAN, настроить Port Security с ограничением 1 MAC-адрес на порт в режиме restrict, активировать IP Source Guard с привязкой IP-MAC для каждого порта доступа [6].

4. Защита от IP Spoofing: активировать uRPF в строгом режиме на всех пользовательских интерфейсах маршрутизатора (ip verify unicast source reachable-via rx), что обеспечивает отбрасывание пакетов с поддельными адресами источника до обработки ACL [7].

5. Списки контроля доступа: ограничить SSH-доступ к управляющему интерфейсу vESR исключительно IP-адресами авторизованных станций

управления посредством расширенных ACL (ip access-list extended), разрешить ICMP для диагностики, запретить весь прочий TCP-трафик на порт 22.

6. Мониторинг и логирование: регулярно проверять логи событий SSH (LOGIN_FAILED, HOST_BLOCKED) и статистику uRPF (show ip interface <if> urpf) для выявления попыток несанкционированного доступа [8].

ОГРАНИЧЕНИЯ ЭМУЛЯЦИИ

Все эксперименты данного исследования проведены в среде виртуализации GNS3 с использованием программных образов vESR. При интерпретации результатов необходимо учитывать ряд ограничений, связанных с различиями между виртуальной и физической реализацией оборудования.

Во-первых, производительность CPU при обработке атак типа DoS в виртуальной среде определяется ресурсами хостовой системы и гипервизора, а не специализированными ASIC-чипами, используемыми в аппаратных маршрутизаторах серии Eltex ESR. В физическом оборудовании функции uRPF и ACL могут выполняться аппаратно на линейных картах, что обеспечивает обработку на скоростях порта без существенной нагрузки на центральный процессор. В виртуальной среде эти функции реализованы программно, поэтому абсолютные значения загрузки CPU и временных характеристик могут отличаться от физического оборудования.

Во-вторых, механизмы DAI и Port Security в данном эксперименте настроены на программном коммутаторе Cisco IOU, а не на физическом оборудовании Eltex. На практике реализация DAI на коммутаторах Eltex MES может иметь особенности, не учтённые в данном исследовании.

В-третьих, латентность виртуальных интерфейсов в GNS3 отличается от реальных физических каналов, что может влиять на временные

характеристики атак (в частности, на скорость перебора паролей и время отклика при ARP Spoofing).

Таким образом, полученные результаты корректно отражают логику работы защитных механизмов и их эффективность в качественном отношении (блокировка/пропуск атаки), однако количественные характеристики (время, загрузка CPU) требуют верификации на физическом оборудовании. Направлением дальнейших исследований является проведение аналогичных экспериментов на аппаратных маршрутизаторах Eltex ESR.

ЗАКЛЮЧЕНИЕ

В заключении можно сказать, что в ходе проведения эксперимента мы успешно развернули тестовый стенд в среде GNS3 и провели три серии атак на механизмы аутентификации и контроля доступа виртуального маршрутизатора Eltex vESR версии 1.18.9. Дополнительно проведён аудит криптографических настроек SSH-сервера (задача 5), подтвердивший соответствие используемых алгоритмов актуальным рекомендациям NIST SP 800-131A [13]. На основании результатов сформулированы практические рекомендации по конфигурированию (задача 6).

При отсутствии защитных механизмов все три вектора атак продемонстрировали свою эффективность: пароли SSH были подобраны за 76 секунд, MITM-позиция достигнута через ARP Spoofing, а spoofed пакеты обошли ACL. Однако после активации контрмер – ограничения попыток входа, статических ARP-записей совместно с DAI и uRPF – все атаки были полностью нейтрализованы при сохранении легитимного доступа.

Результаты подтверждают, что платформа vESR при корректной настройке обеспечивает эффективное противодействие типовым сетевым атакам на механизмы аутентификации и контроля доступа. Практическая значимость работы заключается в получении готовых конфигураций для защиты оборудования Eltex vESR.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Уймин, А.Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 "Сетевое и системное администрирование". Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А.Г. Уймин, И.М. Толмачев // Автоматизация и информатизация ТЭК. – 2025. – № 11(628). – С. 58–62. – EDN DMHQJU.
2. Документация Eltex ESR-series версии 1.18.9 [Электронный ресурс]. – URL: https://docs.eltex-co.ru/display/ED23/ (дата обращения: 15.02.2026).
3. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник. – Санкт-Петербург: Питер, 2016. – 1008 с.
4. ГОСТ Р 57580.1-2017. Защита информации финансовых организаций. Базовый состав организационных и технических мер. – М.: Стандартинформ, 2017.
5. NIST SP 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. – National Institute of Standards and Technology, 2020.
6. IEEE 802.1X-2020. IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control. – IEEE, 2020.
7. Baker, F. Ingress Filtering for Multihomed Networks / F. Baker, P. Savola. – RFC 3704, March 2004. URL: https://www.rfc-editor.org/rfc/rfc3704
8. Методические рекомендации ФСТЭК России по обеспечению безопасности сетевой инфраструктуры. – М.: ФСТЭК России, 2022.
9. van Hauser. THC Hydra: A fast and flexible online password cracking tool [Электронный ресурс]. – URL: https://github.com/vanhauser-thc/thc-hydra (дата обращения: 15.02.2026).
10. Ornaghi, A. Ettercap: Comprehensive suite for man-in-the-middle attacks [Электронный ресурс]. – URL: https://www.ettercap-project.org/ (дата обращения: 15.02.2026).

11. Sanfilippo, S. hping3: Active network security tool [Электронный ресурс]. – URL: http://www.hping.org/ (дата обращения: 15.02.2026).
12. Установка vESR в системе виртуализации GNS3 [Электронный ресурс]. – URL: https://docs.eltex-co.ru/pages/viewpage.action?pageId=593367403 (дата обращения: 15.02.2026).
13. NIST SP 800-131A Rev. 2. Transitioning the Use of Cryptographic Algorithms and Key Lengths. – National Institute of Standards and Technology, 2019.