Разработка и внедрение системы мониторинга сетевой активности с использованием встроенных средств безопасности операционной системы Альт

Введение

В современных условиях цифровой трансформации организаций обеспечение сетевой безопасности становится одной из приоритетных задач. С развитием технологий, увеличением объемов передаваемой информации и распространением удаленного доступа возрастает угроза несанкционированного доступа, утечек данных и кибератак. В этих условиях необходимость создания систем мониторинга сетевой активности, способных эффективно предотвращать инциденты безопасности, становится крайне актуальной.

Операционная система Альт, разработанная на базе отечественных технологий, активно используется в корпоративной среде благодаря своей надежности, адаптируемости и соответствию требованиям информационной безопасности. Одной из ключевых особенностей ОС Альт является наличие встроенных инструментов, которые позволяют обеспечивать высокий уровень защиты данных без необходимости использования стороннего ПО. Основное назначение системы – создание безопасной и стабильной среды для обработки данных в корпоративных и государственных структурах.

Для обеспечения безопасности в ОС Альт используются различные инструменты.

Например, для управления правилами фильтрации сетевого трафика на уровне ядра, применяется утилита iptables. Она тесно интегрирована с компонентом Netfilter, который предоставляет механизмы контроля и обработки пакетов на уровне сетевого стека. Основные функции iptables включают:

1. Создание правил для фильтрации входящего, исходящего и транзитного трафика.
2. Настройку маршрутизации пакетов и их перенаправления.

3. Логирование сетевых событий для последующего анализа.

Использование iptables и Netfilter позволяет настроить индивидуальные политики безопасности для каждой подсети и обеспечить детализированный контроль над сетевым трафиком.

Также применяется инструмент защиты от атак, направленных на взлом сервисов путем подбора паролей (брутфорс-атаки), называемый Fail2Ban. Он анализирует системные журналы на предмет подозрительной активности и автоматически блокирует IP-адреса, с которых осуществляются атаки. Основные возможности Fail2Ban:

1. Настройка фильтров для анализа журналов различных сервисов (например, SSH, Apache, Nginx).
2. Автоматическая блокировка злоумышленников на основе заданных правил.
3. Гибкая настройка временных рамок и условий блокировки.

Fail2Ban позволяет эффективно противодействовать атакам на основные сетевые сервисы, минимизируя нагрузку на администратора.

Средства безопасности ОС Альт обладают рядом преимуществ, которые делают их привлекательными для использования в корпоративной среде.

1. Все инструменты являются частью ОС Альт и не требуют дополнительных затрат на приобретение или настройку.
2. Используемые технологии позволяют адаптировать настройки безопасности под конкретные требования компании.
3. Инструменты, такие как iptables и Fail2Ban, поддерживают российские криптографические стандарты и отвечают требованиям законодательства.
4. Встроенные средства демонстрируют высокую производительность и низкую нагрузку на ресурсы системы.

Предметом статьи является система мониторинга сетевой активности, использующая встроенные средства безопасности ОС Альт, такие как

iptables, Netfilter и Fail2Ban. Объектом статьи является сетевая безопасность и защита информации на платформе ОС Альт, а также методы и инструменты мониторинга сетевой активности в рамках данной системы.

Целью данной работы является разработка и внедрение системы мониторинга сетевой активности с использованием встроенных средств безопасности ОС Альт. Основное внимание уделяется настройке правил фильтрации сетевого трафика, организации логирования и предотвращению атак. Задачи работы включают анализ функциональных возможностей инструментов, их интеграцию в единую систему, а также тестирование эффективности системы в условиях симуляции угроз.

В рамках эксперимента моделируются три сценария сетевых атак:

1. Брутфорс-атака SSH: проверяется способность Fail2Ban блокировать IP-адрес злоумышленника после нескольких неудачных попыток входа.
2. Сканирование портов: оценивается реакция системы на сканирование открытых портов и её способность ограничить доступ к нежелательным сервисам.
3. DoS-атака: исследуется нагрузка на сеть и эффективность iptables в блокировке трафика, направленного на перегрузку сервера.

Методы:

1. Сценарии атак запускаются с машины Kali Linux.
2. Машина на ОС Alt выступает в роли защищаемого сервера.
3. Используются инструменты для анализа (vnstat, htop), чтобы замерить сетевую нагрузку до и после активации защитных мер.

Результаты исследования направлены на создание практического решения, которое может быть рекомендовано для использования в корпоративной среде, где важна надежная защита данных и соответствие требованиям информационной безопасности.

Исследований, связанных со встроенными средствами безопасности на дистрибутивах Линукса, существует достаточно много [1,2]. При этом также есть официальная документация [3] и изучение уже существующих

систем мониторинга сетевой активности [4,5]. Но исследований, связанных с разработкой новых систем и тестирование их в среде ОС Альт найдено не было.

Для достижения цели был проведен анализ системной документации и были проведены тестовые запуски системы в условиях симуляции угроз. Для этого на компьютере с процессором 13th Gen Intel Core i9-13980HX 2.20 GHz и оперативной памятью 16,0, доступно которой 15,6 ГБ, была установлена среда VirtualBox. Внутри нее была установлена и запущена виртуальная машина с дистрибутивом Linux ОС АЛЬТ и Kali Linux.

В рамках эксперимента машине было выданы следующие параметры: оперативная память 2048 Мб, 2 процессора, порядок загрузки: гибкий диск, оптический диск, жесткий диск, ускорение: Nested Paging, Паравитуализация KVM, видеопамять 16 Мб, а также в качестве носителя обычный vdi размером 60,00 Гб.

Результаты исследования

Будем проверять нашу систему брутфорсом ssh. Для этого предварительно создадим текстовый файл с самыми популярными паролями password.txt.

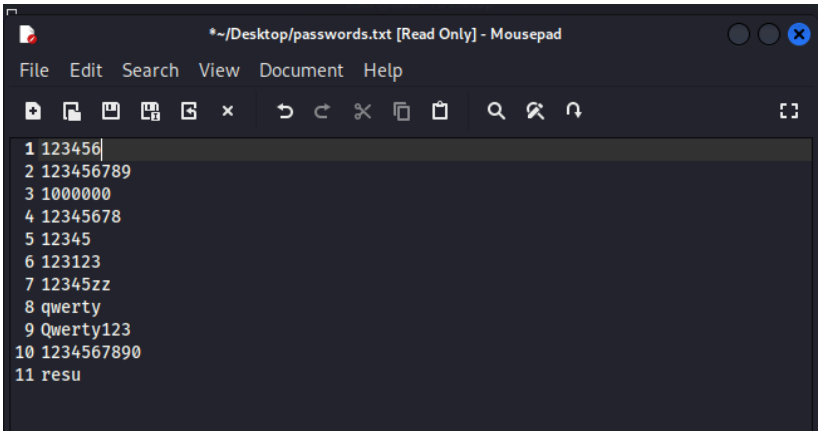

Рис.1. Создание текстового файла с популярными паролями.

Проведем атаку утилитой hydra на Kali Linux

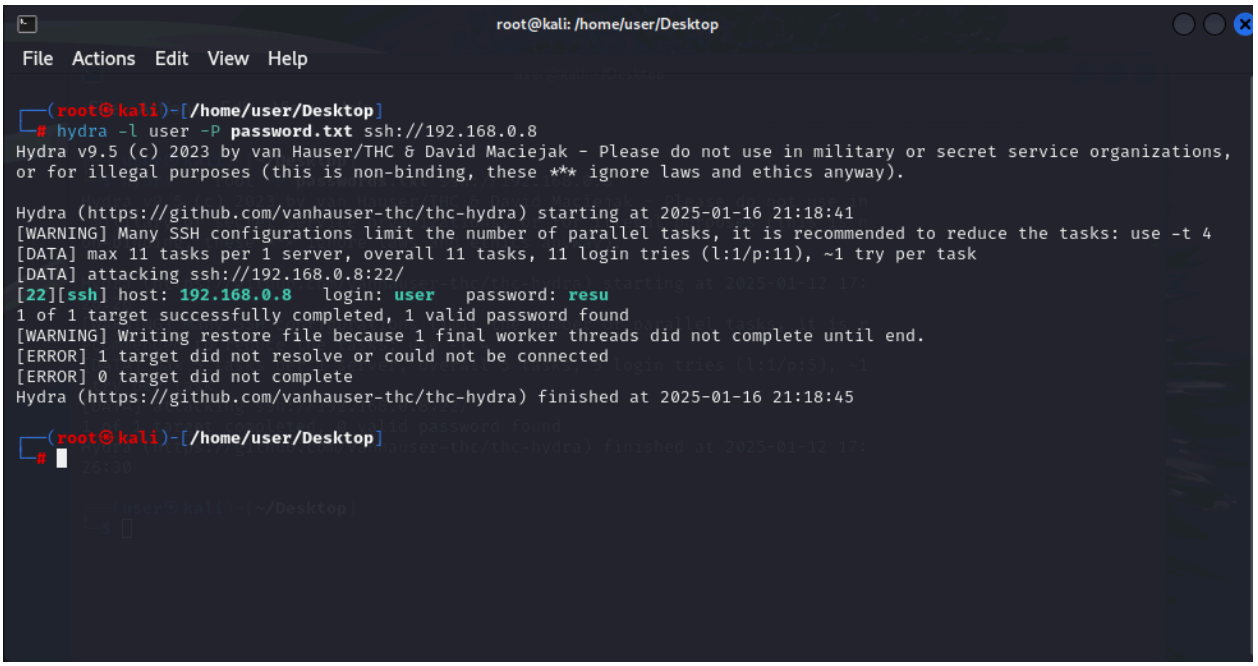

Рисунок 2.Успешная атака методом брутфорс ssh.

Настроим Fail2Ban для защиты от атак. Скопируем конфигурацию.

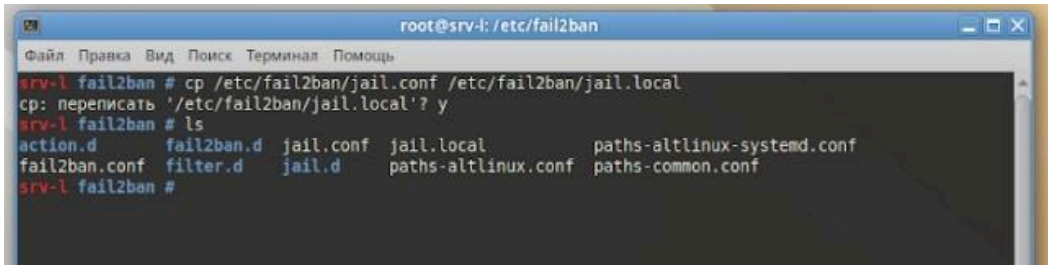

Рисунок 3. Выполнение команды sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

Настроем Fail2Ban для SSH в файле /etc/fail2ban/jail.local. В данном файле найдём секцию [sshd] и включим её. Настройки файла указывают на то, что Fail2Ban будет применяться к сервису SSH (Secure Shell) (секция [sshd]). Опция enabled установлена в значение true, что значит, что данное правило активно. Порт, на котором работает SSH, указан как 22. Лог-файл для отслеживания неудачных попыток входа установлен как /var/log/auth.log. После трех неудачных попыток входа подряд пользователь будет заблокирован на 1 час (3600 секунд).

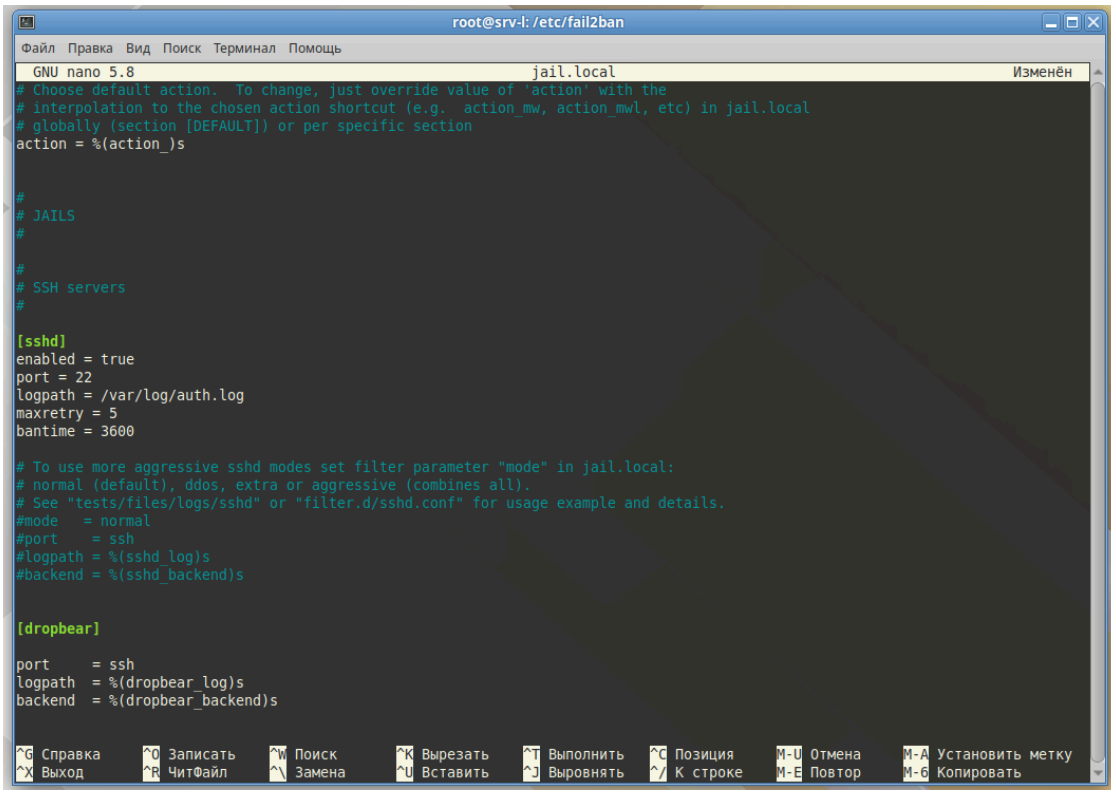

Рисунок 4. - включим sshd

Перезапустим Fail2Ban с помощью команды sudo systemctl restart fail2ban, а после проверим статус утилит, чтобы убедиться, что они корректно запущены и отрабатывают.

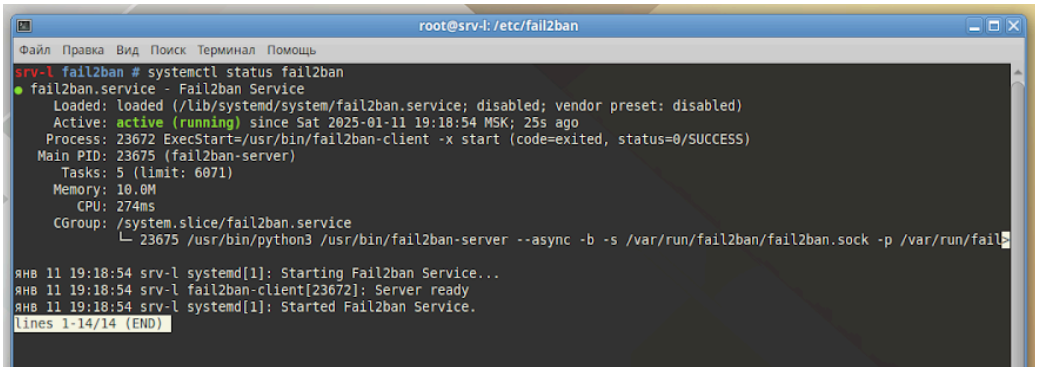

Рисунок 5. - проверка статуса Fail2Ban

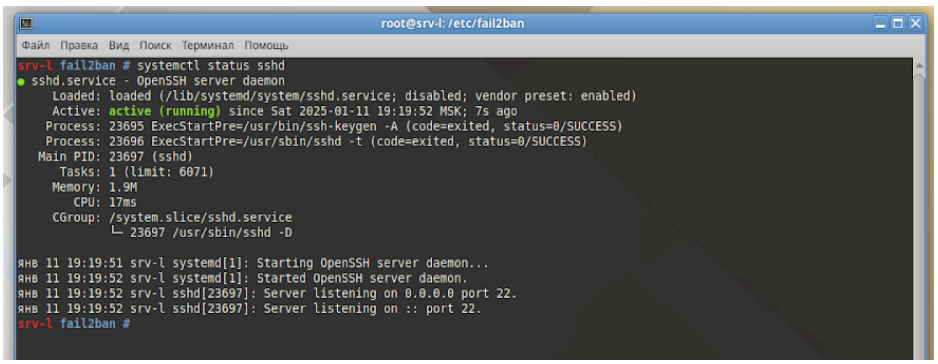

Рисунок 6. - проверка статуса sshd

Далее перейдем к тестированию системы. Проверим блокировку через Fail2Ban. Попробуем несколько раз ввести неправильный пароль через SSH. Убедимся, что IP-адрес заблокирован.

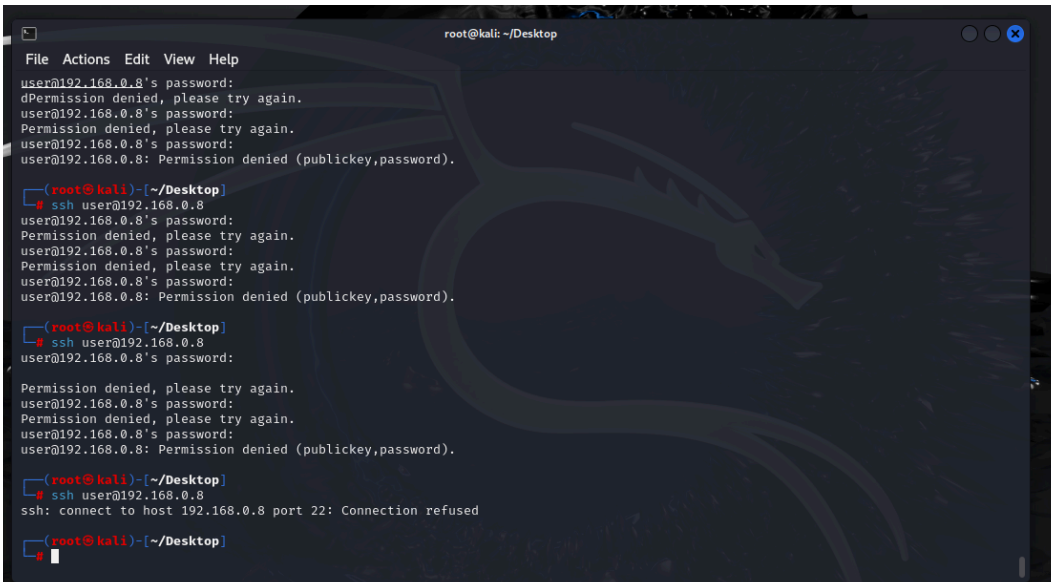

Рисунок 7. - проверка блокировки через Fail2Ban

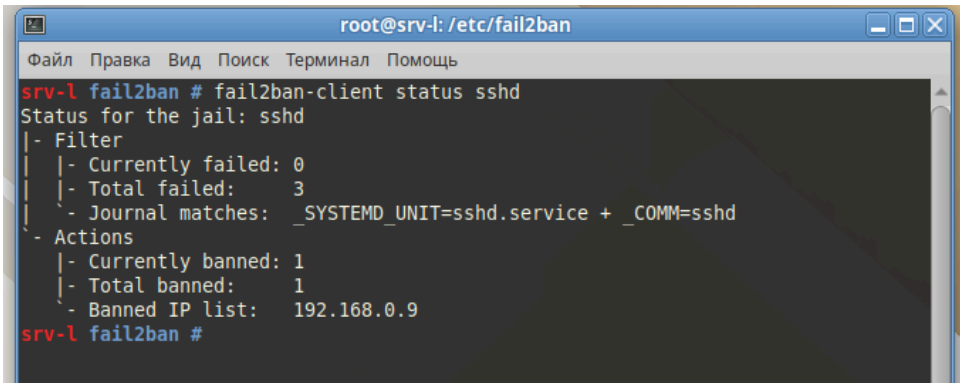

Рисунок 8. - проверка статуса sshd Fail2Ban-client

Произведем проверку брутфорсом ssh с помощью утилиты hydra.

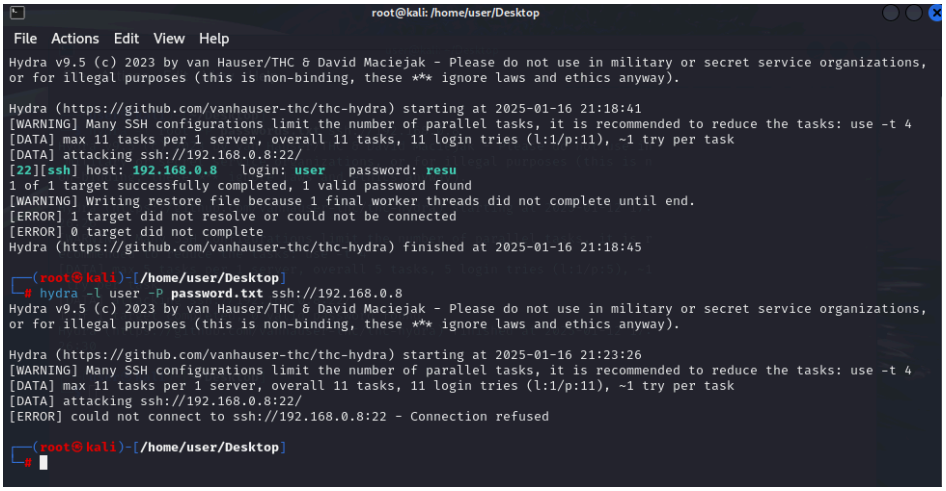

Рисунок 9. - проверка брутфорсом ssh

Настройка iptables

Создадим и применим правила iptables.

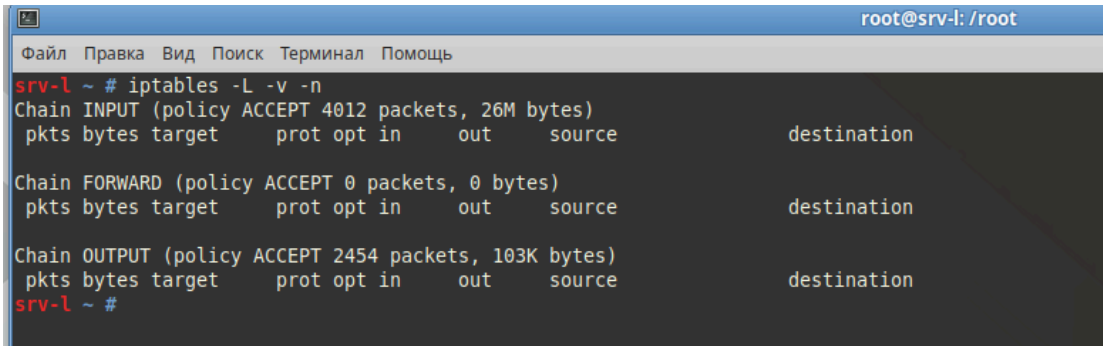

Рисунок 10. - iptables -L -v -n

Проведём настройку правил, для разрешения только входящих SSH (порт 22) и блокировки всего остального:

1. sudo iptables -F # Очистить текущие правила
2. sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT # Разрешить SSH
3. sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT # Разрешить HTTP
4. sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT # Разрешить HTTPS
5. sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT # Разрешить активные соединения
6. sudo iptables -P INPUT DROP # Блокировать всё остальное
7. sudo iptables -P FORWARD DROP
8. sudo iptables -P OUTPUT ACCEPT

Этот скрипт iptables настраивает правила файрволла для разрешения входящих подключений к SSH (порт 22), HTTP (порт 80) и HTTPS (порт 443), а также разрешает активные соединения. Все остальные входящие соединения будут блокированы. Правила FORWARD и OUTPUT установлены на DROP и ACCEPT соответственно. В итоге, только указанные типы трафика будут разрешены, а все остальные будут заблокированы.

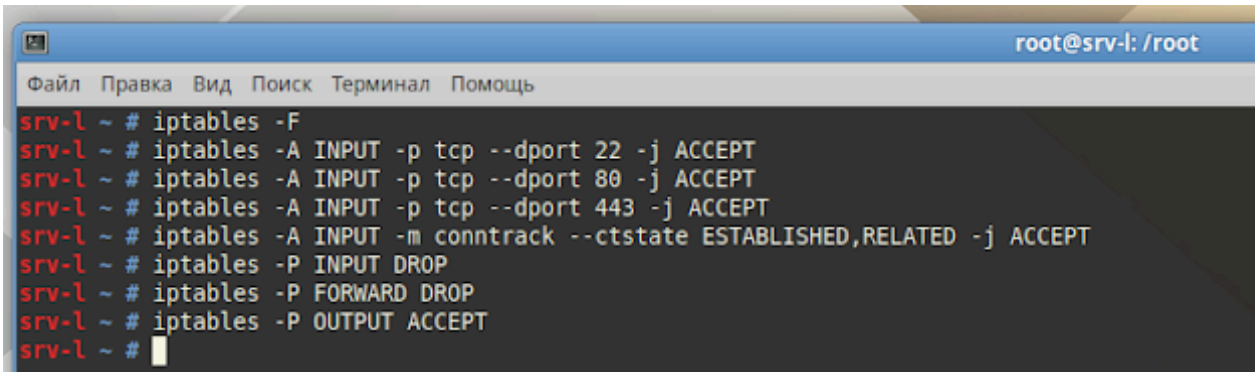

Рисунок 11. - настройка правил

Дале сохраним правила в папку /etc/sysconfig/iptables и проверим их.

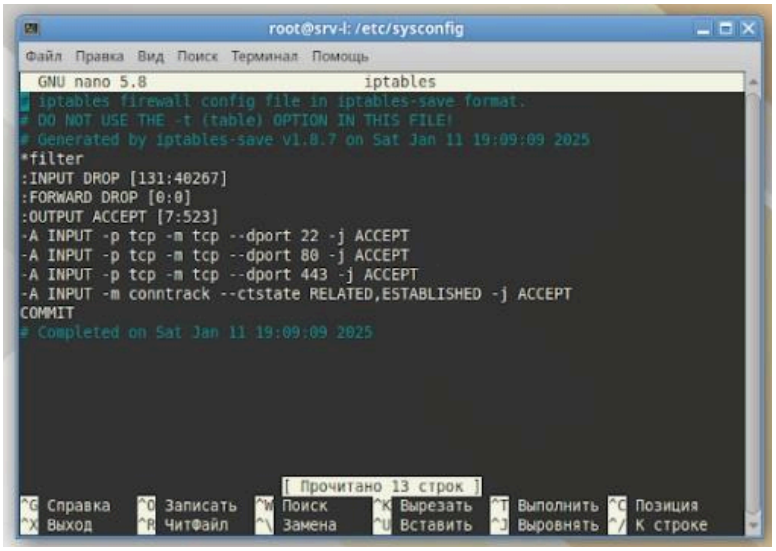

Рисунок 12. -проверка сохранения правил

Произведем логирование подозрительного трафика с помощью Netfilter. Добавим правило для логирования подозрительного трафика.

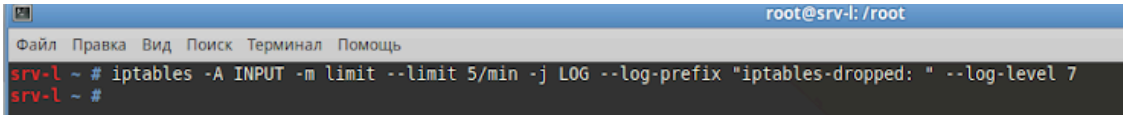

Рисунок 13. - sudo iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables-test: " --log-level 7

Просмотрим логи через journalctl.

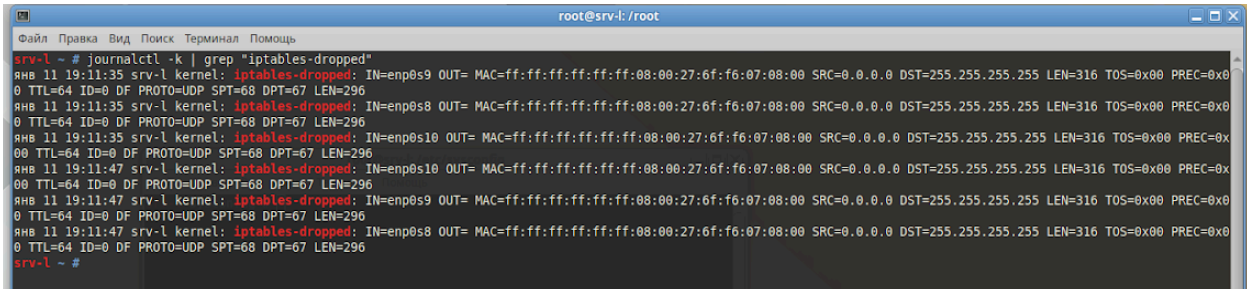

Рисунок 14. - journalctl -k | grep "iptables-dropped"

Произведем симуляцию сетевых атак. Для тестирования правил iptables используем nmap и hping3. Для сканирования портов будем использовать команду nmap -p 1-1000 с указанием IP-адреса.

Рисунок 15. - nmap -p 1-1000 <IP-адрес> до применения правил

Рисунок 16. - nmap -p 1-1000 <IP-адрес> после применения правил

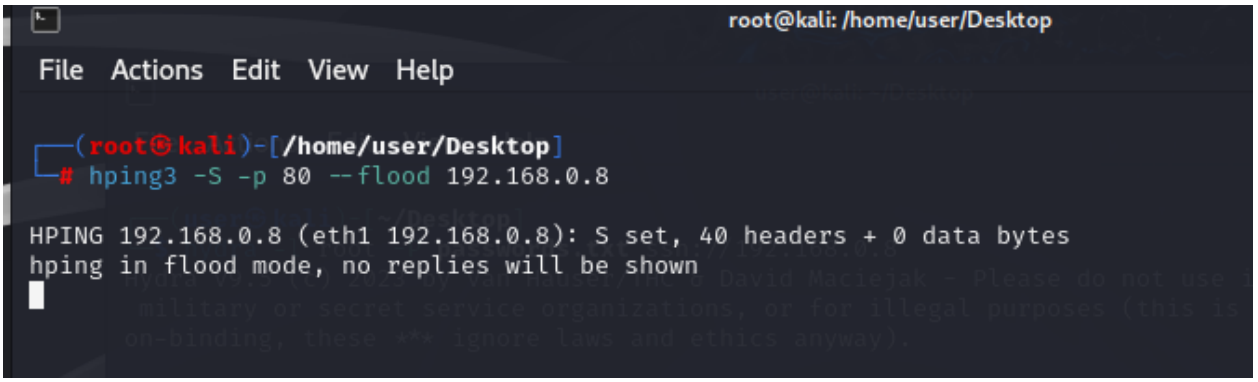

Рисунок 17. - hping3 -S -p 80 --flood 192.168.0.8

Анализ результатов

htop – компьютерная программа, предназначенная для вывода на терминал списка запущенных процессов и информации о них (монитор процессов). С ее помощью отследим нагрузку на систему запущенных до этого утилит.

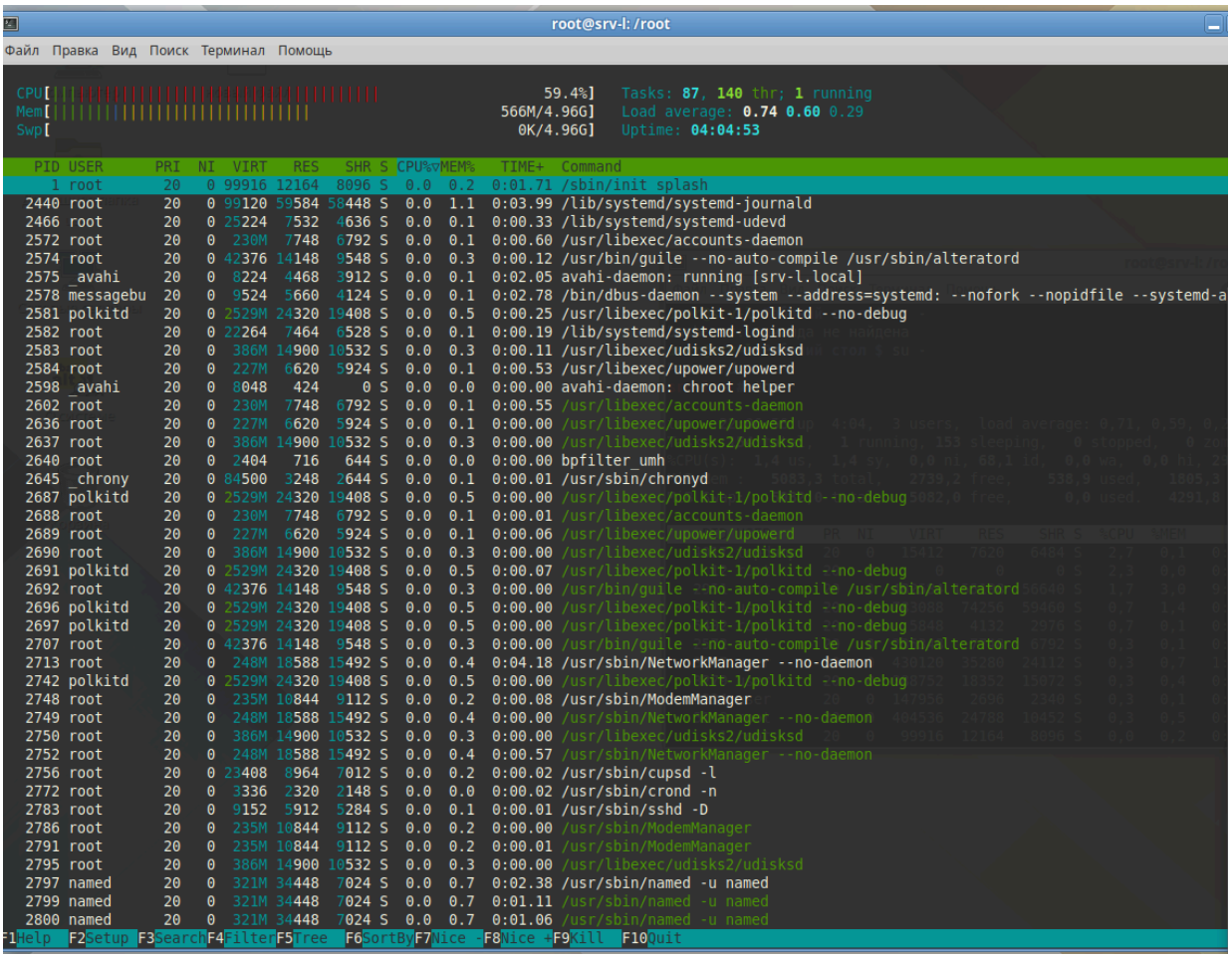

Рисунок 18. – нагрузка на систему «до»

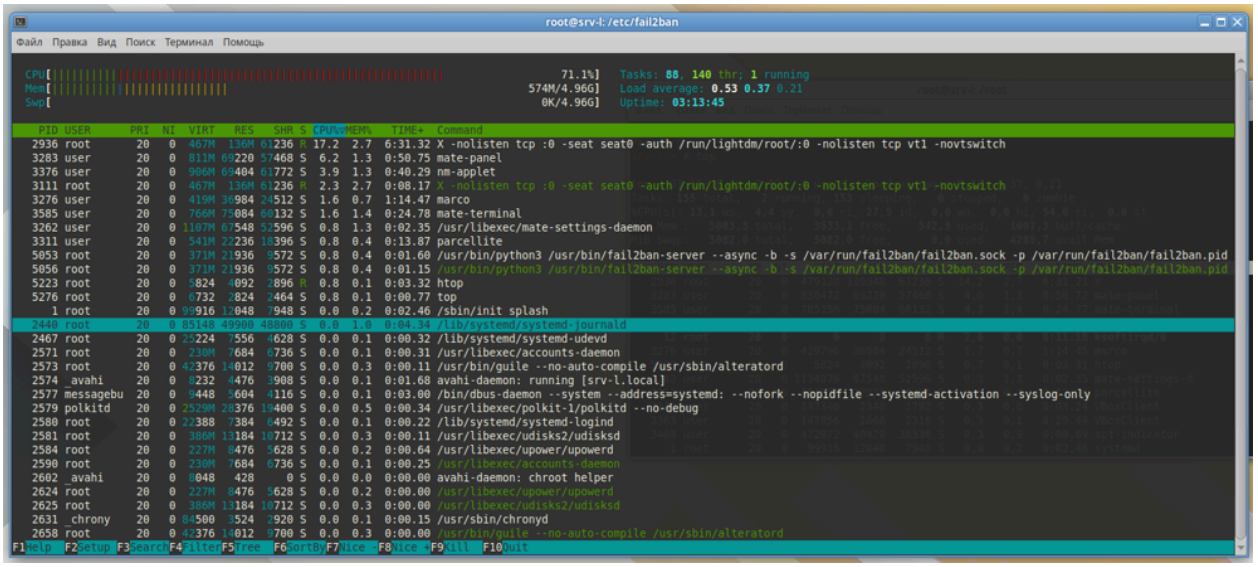

Рисунок 19. - нагрузка на систему «после»

Рисунок 17 - нагрузка на систему с помощью утилиты top

Проверим нагруженность сети с помощью утилиты vnstat.

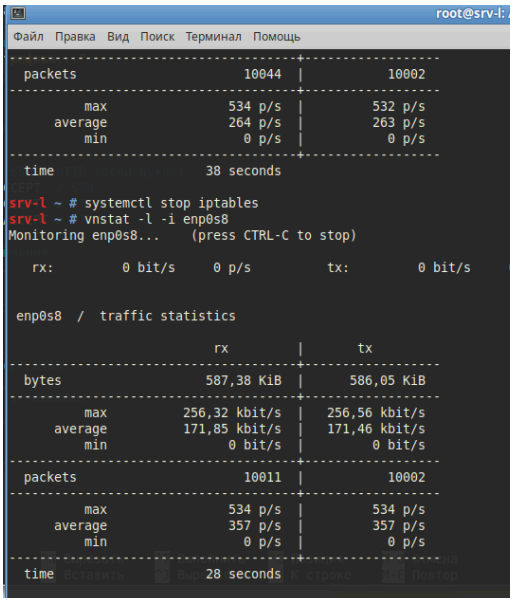

Рисунок 20. – нагруженность сети с выключенным iptables

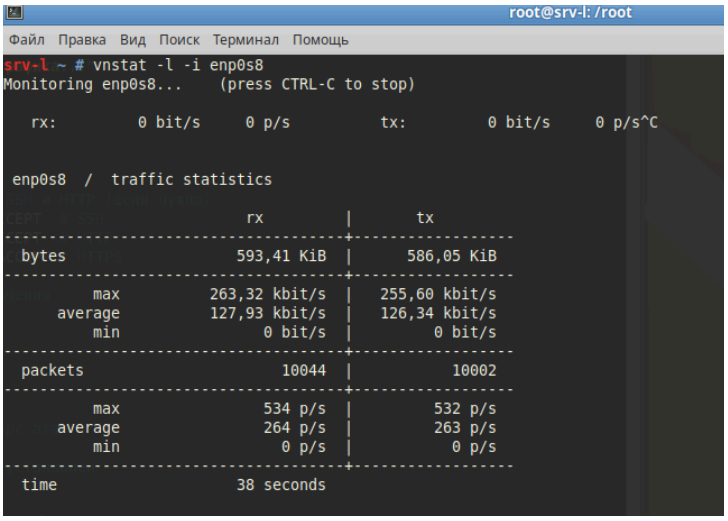

Рисунок 21 – нагруженность сети с включенным iptables

Объединим полученные в результаты в единую таблицу и сравним результаты «до» и «после».

Таблица 1. Результаты проведенных тестов «до»

Тип теста	**Результат**	**Время реакции**	**Примечания**
Брутфорс-атака SSH	Пароль подобран	10 секунд	Не было никакой защиты
Сканирование портов	Порты 22, 445, 631, 139 открыты	Мгновенно	Остальные не открыты
DoS-атака	Трафик пропускается	Мгновенно	Нагрузка в пике в htop 59,4%, в vnstat средняя скорость отправленных

			и полученных данных составляет 171 КБ/сек

Таблица 2. Результаты проведенных тестов «после»

Тип теста	**Результат**	**Время реакции**	**Примечания**
Брутфорс-атака SSH	IP заблокирован	10 секунд	Fail2Ban сработал
Сканирование портов	Порты 22, 80, 443 открыты	Мгновенно	Остальные заблокированы
DoS-атака	Трафик заблокирован	Мгновенно	Нагрузка в пике в htop 71,1%, в vnstat средняя скорость отправленных и полученных данных составляет 127 КБ/сек

На основе двух таблиц можно сделать выводы что по результатам тестирования системы мониторинга следует следующее:

1. Брутфорс-атака SSH:

1. Таблица 1 (до настройки Fail2Ban):
   Результат: Пароль был подобран за 10 секунд, что свидетельствует о том что отсутствует защита от брутфорс-атак.
2. Таблица 2 (с настройкой Fail2Ban):
   Результат: IP-адрес атакующей машины был заблокирован через 10 секунд, в результате работы Fail2Ban.

После настройки Fail2Ban система осуществляет блокировку IP-адресов, которые совершают многократные попытки входа.

2. Сканирование портов:

1. Таблица 1 (до настройки Fail2Ban):
   Результат: Порты 22, 445, 631 и 139 стали открыты, остальные порты заблокированы.

2. Таблица 2 (с настройкой Fail2Ban):

   Результат: После настройки Fail2Ban порты 22, 80 и 443 были открыты, остальные порты стали заблокированы.

После настройки Fail2Ban порты 80 (HTTP) и 443 (HTTPS) стали открыты что позволило сервису работать в исправном состоянии. Также, количество открытых портов уменьшилось, а порты которые не используются системой, были заблокированы.

3. DoS-атака:

1. Таблица 1 (до настройки Fail2Ban):

   Результат: Трафик проходит без блокировки, нагрузка в htop достигала значения в 59,4%, средняя скорость передачи данных через vnstat составила 171 КБ/сек.

2. Таблица 2 (с настройкой Fail2Ban):

   Результат: Трафик был заблокирован, нагрузка в htop - 71,1%, средняя скорость передачи данных через vnstat снизилась до 127 КБ/сек.

После настройки весь трафик был заблокирован, что способствовало снижению нагрузки на систему и уменьшению скорости передачи данных. Однако нагрузка в пике была равна = 71,1%, после изучения причины высокой нагрузки, было выявлено что существуют дополнительные факторы, влияющие на производительность.

Вывод:

Внедрение Fail2Ban привело к:

1. Работе защиты от брутфорс-атак, IP-адреса блокируются после нескольких неудачных попыток.
2. После настройки системы порты стали корректно фильтроваться, что повышает безопасность.
3. DoS-атаки стали блокироваться, что способствовало снижению нагрузки на систему.

Заключение

Таким образом, ОС Альт предоставляет мощный набор встроенных средств для обеспечения сетевой безопасности. Комбинированное использование iptables, Netfilter и Fail2Ban позволяет эффективно фильтровать трафик, предотвращать атаки и логировать подозрительную активность. Эти инструменты являются основой для построения надежной системы мониторинга сетевой активности, что делает ОС Альт оптимальным выбором для организаций, стремящихся к повышению уровня защиты своих данных.

Литература

1. Бархатов Александр Обзор и практическое использование Iptables / Александр Бархатов. — Текст : электронный // timeweb.cloud : [сайт]. — URL: https://timeweb.cloud/tutorials/network-security/obzor-i-prakticheskoe-ispolzovanie-iptables (дата обращения: 14.01.2025).

2. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование : Практикум. Учебное пособие для вузов / А. Г. Уймин. – Санкт-Петербург : Издательство "Лань", 2024. – 116 с. – (Высшее образование). – ISBN 978-5-507-48647-2. – EDN BZJRIQ (дата обращения: 14.01.2025).

3. Настройка и использование Fail2ban на Linux. — Текст : электронный // dmosk : [сайт]. — URL: https://www.dmosk.ru/instruktions.php?object=fail2ban (дата обращения: 14.01.2025).

4. Пакет vnstat: Информация. — Текст : электронный // alt linux team : [сайт]. — URL: https://packages.altlinux.org/ru/sisyphus/srpms/vnstat/ (дата обращения: 14.01.2025).

5. Установка vnStat для мониторинга сети в Unix/Linux. — Текст : электронный // linux-notes : [сайт]. — URL: https://linux-notes.org/ustanovka-vnstat-dlya-monitoringa-seti-v-unix-linux/ (дата обращения: 14.01.2025).

6. Система централизованного и распределенного мониторинга удаленных сетей, сетевого оборудования, офисов и организаций - 10-Страйк Мониторинг Сети Pro. — Текст : электронный // 10-strike sotware : [сайт]. — URL: https://www.10-strike.ru/network-monitor/pro/?ysclid=m5wrwt2j8g253083612 (дата обращения: 14.01.2025).