УДК 004

Нарминов Д.Х.
студент 4 курса, факультет «Комплексной безопасности ТЭК»
РГУНГ (НИУ) имени И. М. Губкина
Россия, г. Москва

ОБНАРУЖЕНИЕ RECONNAISSANCE-АКТИВНОСТИ С ПОМОЩЬЮ ПРАВИЛ SURICATA.

ВВЕДЕНИЕ

Данный материал поможет читателям как углубить знания в области защиты систем от reconnaissance-активности на отечественной операционной системе Альт Рабочая станция 11, так и с нуля изучить данную область, поскольку в нем содержатся фундаментальные понятия и принципы, необходимые для понимания работы IDS систем, подобных Suricata. Данная тема актуальна – при обучении специалиста по обеспечению компьютерной безопасности важно понимать фундаментальные вещи, в том числе принципы работы различного ПО, используемого в сфере информационной безопасности.

Объект исследования: Процесс мониторинга сетевой активности и выявления этапов компьютерной разведки с использованием IDS Suricata.

Предмет исследования: Механизмы настройки правил системы обнаружения вторжений Suricata для выявления reconnaissance-активности в среде операционной системы «Альт Рабочая станция 11» и оценка их эффективности.

Цель исследования: на примере ОС Альт изучить методы сигнатурного и поведенческого анализа Suricata для реализации защиты от этапов компьютерной разведки.

Ключевые слова: IDS, Suricata, Reconnaissance-активность, nmap, nikto, dirb, сетевое сканирование, конфигурационный файл, правила выявления, вредоносный трафик, алерт, brute-force, информационная безопасность, программное обеспечение.

Система обнаружения вторжений (IDS) — это тип программного обеспечения безопасности, предназначенного для автоматического оповещения администраторов о попытке компрометации IT-системы. [6, 9]

Suricata — высокопроизводительный движок сетевой безопасности, объединяющий функции IDS, IPS и мониторинга сети. Проект распространяется с открытым исходным кодом и развивается некоммерческим фондом OISF при поддержке сообщества. [7]

Reconnaissance-активность — это начальный этап кибератаки, представляющий собой комплекс мероприятий по сбору информации о целевой информационной системе – топология сети, открытые порты, версии программного обеспечения, наличие средств защиты – с целью выявления уязвимостей для последующей эксплуатации. [8]

Тип исследования: Аналитическое и практическое с элементами сравнительного анализа – изучение методов сканирования и способов их выявления.

Характеристика выборки: Выборка ограничивается искусственно созданным сетевым трафиком, сгенерированным в ходе эмуляции атак в изолированной виртуальной среде между узлом атаки и узлом защиты с целью его дальнейшей детекции системой Suricata.

Методы сбора данных: изучение документации, лабораторных работ, поиск в сети «Интернет».

Описание процедуры проведения исследования:

1. Установка ОС Альт Рабочая станция 11 на виртуальную машину.
2. Сбор данных из указанных источников.
3. Практический этап.
4. Систематизация результатов, полученных на всех этапах работы.

Методы обработки данных: Создание таблиц с описанием в рамках определенной области, создание сравнительных сводных таблиц, визуальное представление наиболее важных этапов, а также, создание дополнительного текстового описания полученной информации.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Архитектура Suricata, основные протоколы и стандарты

Особенностью архитектуры, отличающей Suricata от предшественников, таких как Snort, является поддержка многопоточности. При помощи этого система распараллеливает обработку трафика на все ядра процессора – это спасает от потери пакетов на высоких скоростях передачи данных. [7]

Таблица 1. Компоненты архитектуры Suricata и используемые технологии

Компонент	Стандарты и механизмы	Описание функционала
Packet Acquisition	Протоколы: AF_PACKET, NFQUEUE Механизм: Zero-copy (AF_PACKET V3)	Получение трафика с сетевого интерфейса.
Decoder & Stream Engine	Стандарты: TCP/IP, UDP, VLAN	Декодер преобразует битовый поток в структурированные данные.
Detection Engine	Механизмы: Hyperscan, PCRE	Компонент, выполняющий сопоставление нормализованных данных с базой сигнатур.
Output	Формат: EVE JSON	Интерфейс регистрации событий.

Применяется конвейерный принцип обработки трафика – все пакеты последовательно проходят через модули анализа. Одновременно несколько пакетов могут обрабатываться в разных потоках.

Таблица 2. Обработка трафика в архитектуре Suricata

Название этапа	Компоненты, Протокол / Механизм	Описание процесса
1. Прием трафика (Физический уровень)	NIC (Сетевая карта) Драйвер сетевого интерфейса	Сетевая карта получает электрические/оптические сигналы, преобразует их в биты и инициирует прерывание для передачи данных ядру ОС.
2. Захват пакетов (Packet Acquisition)	Packet Acquisition Module AF_PACKET V3 (Linux) / Zero-copy	Модуль захвата копирует «сырые» пакеты из кольцевого буфера ядра в пространство пользователя Suricata, используя механизм mmap для минимизации задержек.
3. Первичное декодирование (Decoding)	Decoder Ethernet, IPv4/IPv6, TCP/UDP/ICMP	Разбор заголовков канального, сетевого и транспортного уровней. Проверка на корректность (контрольная сумма), отбрасывание битых пакетов, извлечение IP-адресов и портов.
4. Отслеживание потоков (Flow Tracking)	Flow Engine Hash-table, 5-tuple	Пакет привязывается к конкретной сессии (потоку) на основе 5 признаков (IP отправителя/получателя, порты, протокол). Создается или обновляется контекст потока в памяти.
5. Сборка TCP-потоков (Stream Reassembly)	Stream Engine TCP State Machine	Восстановление порядка следования сегментов tcp, устранение дублей и склейка фрагментированных данных в единый поток для анализа полезной нагрузки.
6. Определение протокола (Protocol Detection)	Probing Parser Сигнатуры протоколов / Port-independent	Анализ начала полезной нагрузки (payload) для идентификации протокола прикладного уровня (например, обнаружение HTTP на нестандартном порту 8080).
7. Парсинг прикладного уровня (App Parsing)	AppLayer Parsers (Rust) HTTP, DNS, TLS, SMB, FTP	Глубокий разбор структуры протокола. Извлечение метаданных (URI, User-Agent, SNI, DNS Query) и помещение их в специальные буферы для проверки.
8. Сигнатурный анализ (Detection)	Detection Engine MPM (AC/Hyperscan), PCRE, Rule API	Сопоставление нормализованных данных (заголовков, собранного потока и метаданных приложений) с базой правил. Поиск совпадений с сигнатурами атак.
9. Регистрация событий (Output)	Output Module EVE JSON, Fast Log, Syslog	В случае срабатывания правила формируется объект события (Alert) с полной информацией о пакете и потоке. Данные сериализуются в JSON и записываются на диск.

Методика реализации системы защиты на базе ОС Альт

Была спроектирована топология, состоящая из двух ВМ – первая с установленной suricata, вторая используется для проведения сканирования. [1]

Таблица 3. Параметры узлов лабораторного стенда

Роль узла	Имя хоста	Службы и ПО	IP-адрес (Сеть)
Сервер защиты	suricata	Suricata 8.0, Apache 2.4	192.168.10.10/24
Атакующий	scanner	Nmap, Nikto, Dirb	192.168.10.11/24

Схема взаимодействия:

— scanner генерирует вредоносный трафик, направленный на 192.168.10.10.

— Узел suricata принимает трафик на интерфейсе enp0s8. Копия трафика передается движку IDS через механизм AF_PACKET.

— Веб-сервер Apache отвечает на запросы, генерируя коды ответов (200, 404), которые также анализируются IDS (в ответе сервера).

Для эмуляции кибератак был развернут узел scanner. В качестве ОС использована ОС Альт, на которую был установлен набор необходимых утилит.

Таблица 4. Инструментарий атакующего узла

Инструмент	Версия	Назначение в эксперименте	Угроза
Nmap	7.94	Сетевой сканер. Используется для отправки ICMP-запросов, SYN-сканирования портов и определения версий сервисов.	Сетевая разведка, OS Fingerprinting.
Nikto	2.1.6	Сканер веб-уязвимостей. Генерирует типовые HTTP-запросы для поиска устаревших скриптов и ошибок конфигурации.	Автоматизированный поиск уязвимостей (Vulnerability Scan).
Dirb	2.22	Утилита перебора директорий. Осуществляет поиск скрытого контента методом «грубой силы» (fuzzing) по словарю.	Перебор ресурсов (Directory Brute-force).
Curl	8.x	Консольный HTTP-клиент. Используется для точечной отправки запросов с поддельными заголовками User-Agent.	Проверка сигнатурных правил и обхода защиты.

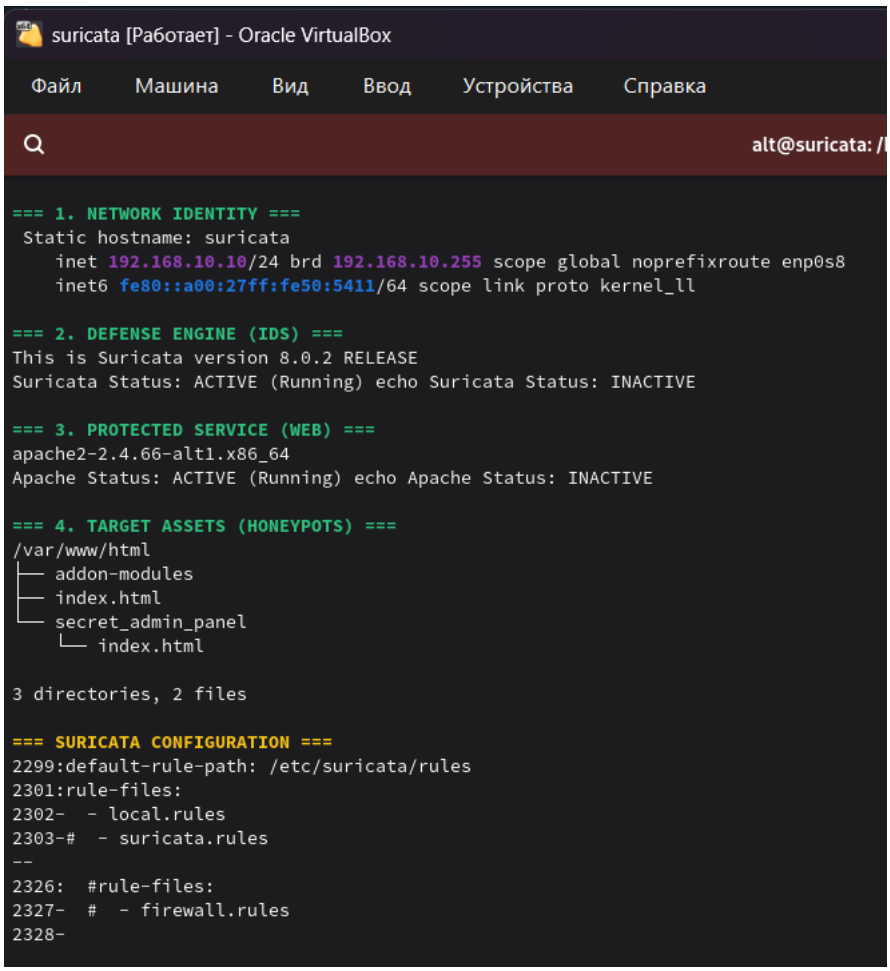

Рисунок 1 - Инфраструктура Защитника

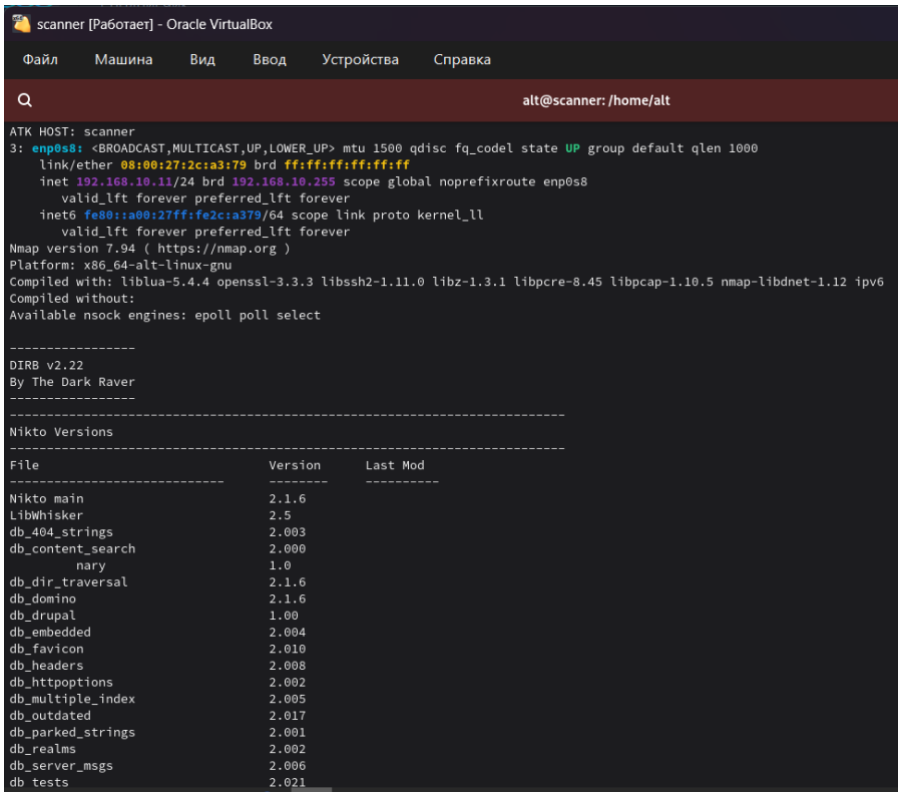

Рисунок 2 - Инфраструктура Атакующего

Разработка политики обнаружения и сигнатурных правил

В рамках исследования была разработана политика безопасности, основанная на комбинации сигнатурного и поведенческого анализа. Для каждого класса угроз, выявленного на этапе анализа предметной области, было создано и внедрено соответствующее правило детектирования. [3, 8]

Информация о реализованных мерах защиты приведена в таблице 5. [5]

Таблица 5. Реализованные меры противодействия угрозам

Угроза (Вектор атаки)	Метод обнаружения	Реализация в работе (local.rules)
1. Обнаружение активных хостов (Ping Sweep) Первичная разведка сети с использованием ICMP-запросов (Nmap -sn).	Анализ заголовков протокола ICMP - Отслеживание пакетов типа Echo Request, направленных во внутреннюю сеть.	Правило sid:1000001 – Фиксация любых попыток сканирования доступности узла по протоколу ICMP (itype:8).
2. Агрессивное сканирование портов Попытка быстрого определения открытых сервисов (Nmap -A / Fast Scan).	Частотный анализ (Rate Limiting) - Выявление аномально высокой скорости установки соединений с одного источника.	Правило sid:1000002 - Использован пороговый фильтр: генерация тревоги, если источник отправляет более 20 SYN-пакетов в секунду. Блокирует «шумные» сканеры.
3. Скрытое «медленное» сканирование Растянутая во времени атака для обхода стандартных IDS (Low-and-Slow).	Временна́я корреляция событий - Накопление статистики по источнику на длительном временном интервале.	Правило sid:1000003 - Специальный сценарий для выявления скрытых угроз: правило срабатывает при накоплении 5 событий за 600 с, что позволяет обнаружить даже осторожного злоумышленника.
4. Использование хакерского ПО (Сканеры Nikto, Dirb, Nmap NSE).	Сигнатурный анализ заголовков (DPI) - Глубокая инспекция HTTP-трафика на предмет наличия известных цифровых отпечатков.	Правила sid:1000004-1000006 - Проверка поля User-Agent в HTTP-запросах. Настроено детектирование строк: "Nikto", "Nmap Scripting Engine", "DIRB".

Угроза (Вектор атаки)	Метод обнаружения	Реализация в работе (local.rules)
5. Перебор директорий (Brute-force) Поиск скрытых ресурсов методом перебора по словарю.	Анализ ответов сервера (Response Tracking) - Отслеживание аномального количества ошибок, возвращаемых веб-сервером одному клиенту.	Правило sid:1000007 - Анализ трафика *от сервера к клиенту*. Если зафиксировано более 20 ответов «404 Not Found» за 10 секунд, событие классифицируется как перебор (Directory Brute-force).

Экспериментальная оценка эффективности системы

Мы успешно подготовили оба хоста для эксперимента:

Узел защиты:

— На машине suricata развернули веб-сервер, который будет выступать целью атаки, и саму систему обнаружения вторжений.

— Сначала выполняется обновление пакетов и установка необходимых служб – suricata и веб-сервера Apache. [2]

— Далее запускаем веб-сервер, добавляем в автозагрузку и создали структуру директорий для имитации админ-панели.

— Необходимо сделать так, чтобы трафик перехватывался – для этого определим интерфейс enp0s8 как прослушиваемый и укажем это в файле конфигурации /etc/sysconfig/suricata. Строка OPTIONS приводится к следующему виду: # OPTIONS="-i enp0s8". Далее добавим в автозагрузку службу suricata. [4]

Узел атаки:

— Были установлены утилиты для сетевой разведки, веб-сканирования и перебора директорий из официального репозитория ОС Альт [10, 11, 12].

 # apt-get install nmap nikto dirb curl

Переходим к тестированию созданных нами правил обнаружения атак класса разведки – на узле защиты проводим онлайн мониторинг при помощи чтения файла логов. Данная команда будет держать файл открытым и выводить алерты по мере их появления. [6]

 # tail -f /var/log/suricata/fast.log

Таблица 6. Описание эксперимента

Тип атаки	Команда запуска	Описание сценария тестирования	Результат обнаружения и анализ
Базовая сетевая разведка (ICMP)	nmap -sn --send-ip 192.168.10.10	Выполняется Ping Sweep для определения активных хостов. Флаг --send-ip используется для принудительной отправки пакетов на IP-уровне, исключая ARP-запросы внутри локальной сети, что позволяет проверить реакцию IDS на входящий ICMP-трафик.	Сработало: Правило sid:1000001. Анализ: Система корректно классифицировала пакеты типа Echo Request (itype:8) как Generic ICMP event. Без флага --send-ip атака не детектировалась бы на уровне NIDS в одном сегменте сети.
Агр-ое скан-ие (SYN-Flood)	nmap -A -T4 192.168.10.10	Комплексное сканирование с определением версий ОС (-A) и агрессивным временным шаблоном (-T4). Генерируется плотный поток SYN-пакетов для быстрого перебора портов, создающий высокую нагрузку на сеть.	Сработало: Правило sid:1000002. Анализ: Активирован механизм частотного анализа (thresholding). Зафиксировано превышение лимита соединений: более 20 SYN-пакетов за 1 секунду с одного IP-адреса источника.
Скрытое сканирование (Low-and-Slow)	nmap -sS -T2 --scan-delay 1s -p 21...443 192.168.10.10	Попытка обхода защиты методом «медленного» сканирования. Используется SYN-режим (-sS) с задержкой между пакетами в 1 секунду (--scan-delay) и медленным шаблоном (-T2), чтобы трафик сливался с легитимным шумом.	Сработало: Правило sid:1000003. Анализ: Сработала временная корреляция событий. Правило накопило статистику по источнику (5 попыток соединения на разные порты) в течение широкого временного окна (600 секунд), что позволило выявить растянутую во времени атаку.
Скрипты скан-ия (Nmap NSE)	curl -A "Mozilla/5.0 ... Nmap Scripting Engine)" http://192.168.10.10	Эмуляция HTTP-запроса от скриптового движка Nmap. Тестируется способность DPI (Deep Packet Inspection) анализировать заголовки прикладного уровня, которые Nmap отправляет при запуске скриптов вроде http-enum.	Сработало: Правило sid:1000004. Анализ: Успешный сигнатурный анализ поля User-Agent. IDS извлекла строку "Nmap Scripting Engine" из HTTP-заголовка. Событие классифицировано в логе как WEB-RECON.
Скан-ие веб-уязвимостей (Nikto)	nikto -h http://192.168.10.10	Запуск специализированного сканера Nikto, генерирующего тысячи типовых запросов для поиска устаревших скриптов и ошибок конфигурации сервера. Инструмент работает «шумно», не скрывая свой User-Agent.	Сработало: Правило sid:1000005. Анализ: Множественные срабатывания сигнатурного правила с приоритетом 1 (High). Детектирование выполнено по наличию подстроки "Nikto" в заголовках пакетов. Подтверждена защита от автоматизированных сканеров.
Перебор дир-ий (Dirb)	curl -A "DIRB/2.22 (Linux; Client)" http://192.168.10.10	Эмуляция работы утилиты Dirb, используемой для поиска скрытых ресурсов методом перебора (Brute-force) по словарю. Проверяется реакция на специфический цифровой отпечаток инструмента.	Сработало: Правило sid:1000006. Анализ: Правило идентифицировало вредоносный User-Agent "DIRB". В журнале создана запись WEB-RECON: DIRB Scan detected, подтверждающая возможность атрибуции инструмента атаки.

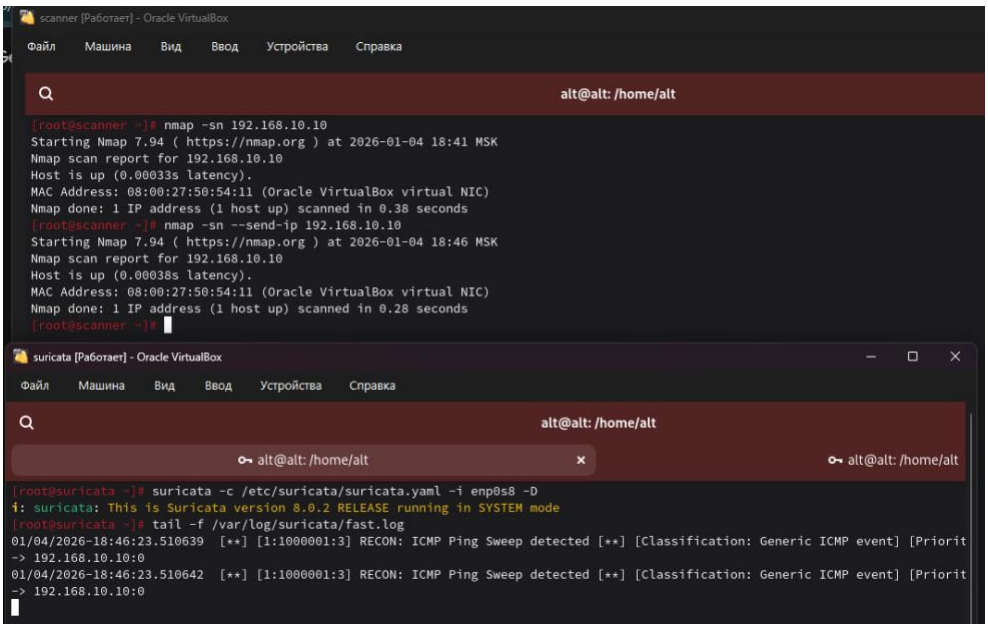

Рисунок 3 — Результаты обнаружения ICMP-сканирования – тест 1

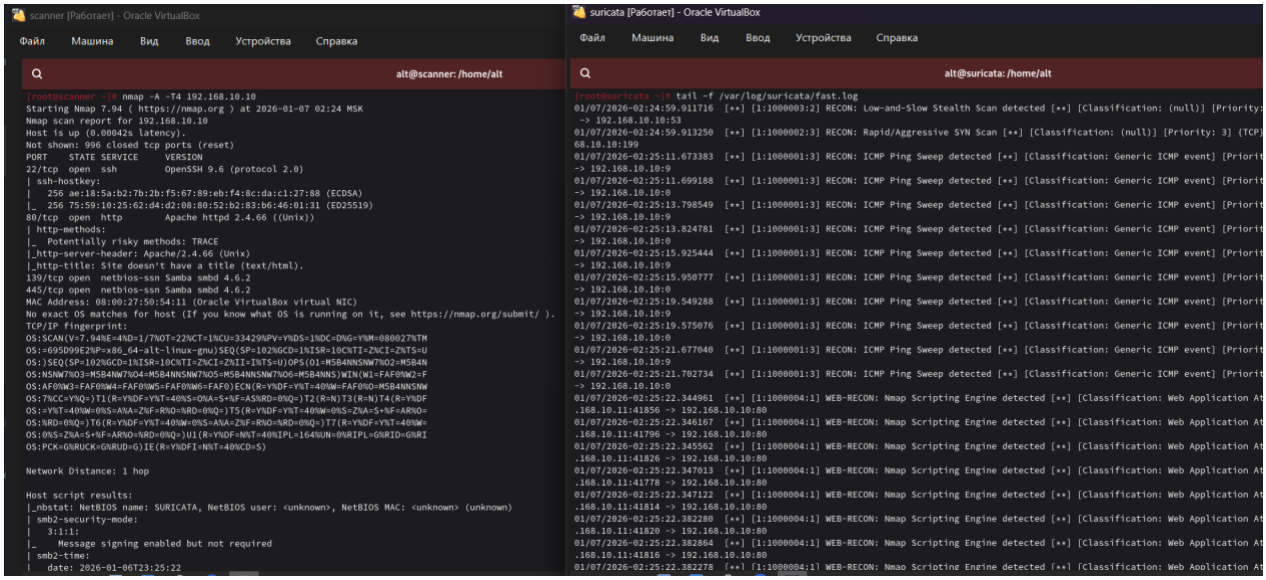

Рисунок 4 — Детектирование агрессивного сканирования – тест 2

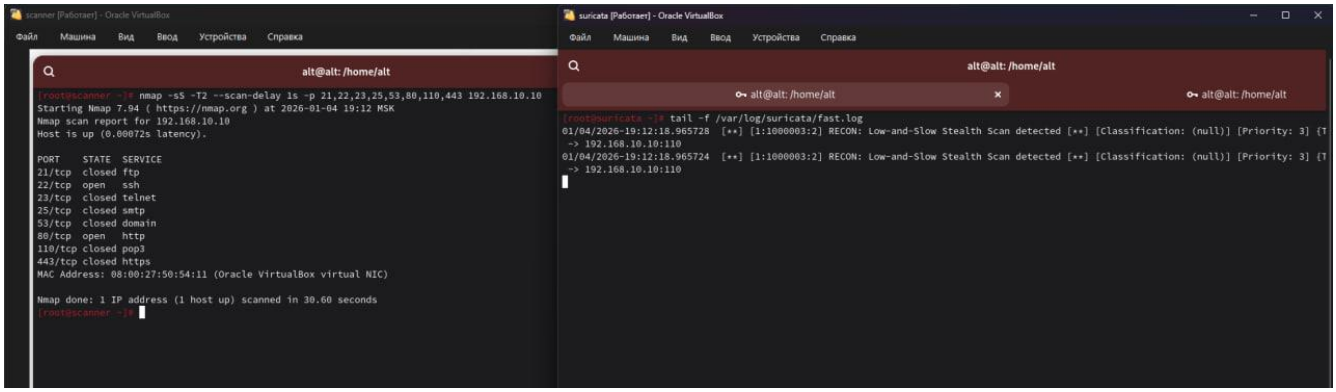

Рисунок 5 — Обнаружение скрытного сканирования – тест 3

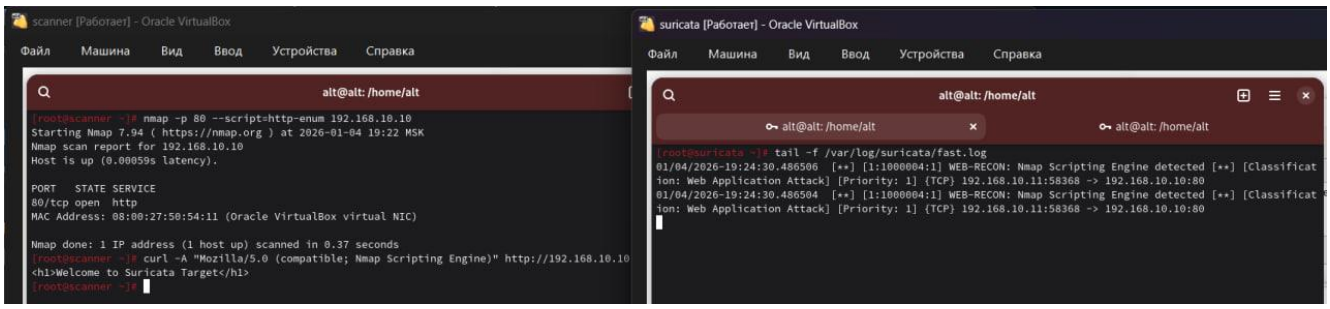

Рисунок 6 — Сигнатурное обнаружение скриптов Nmap – тест 4

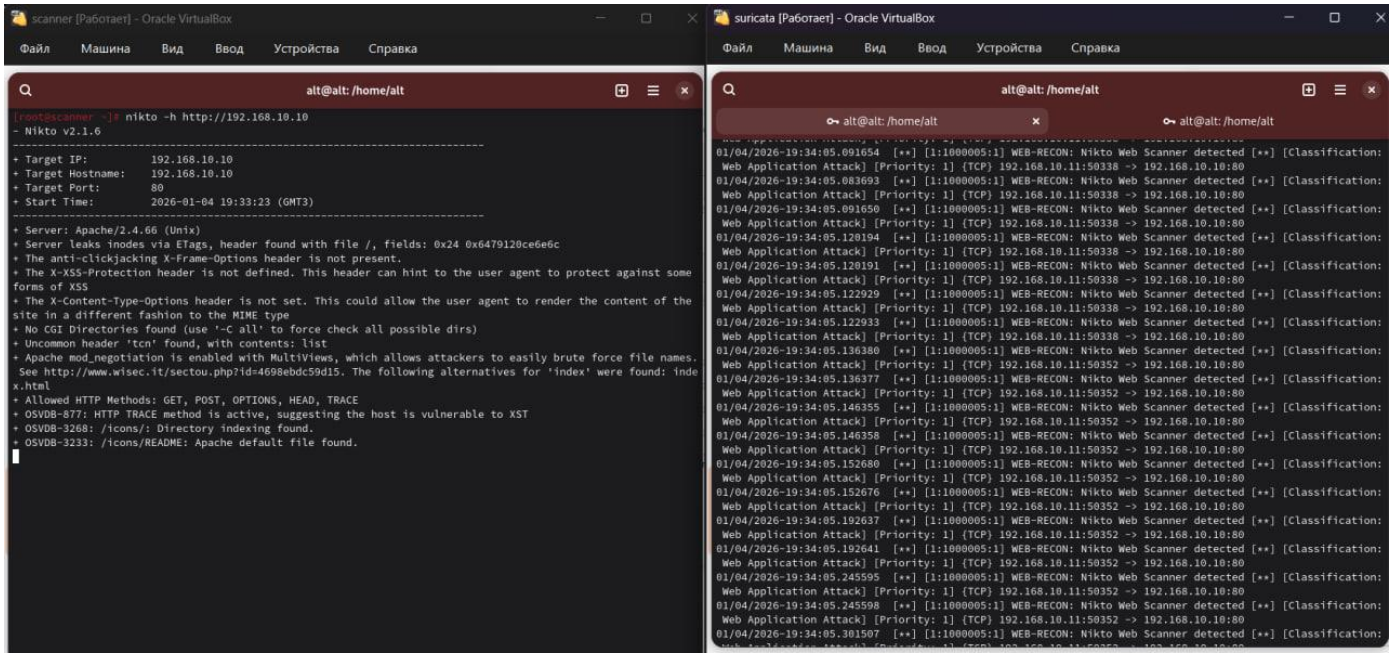

Рисунок 7 — Обнаружение сканера Nikto – тест 5

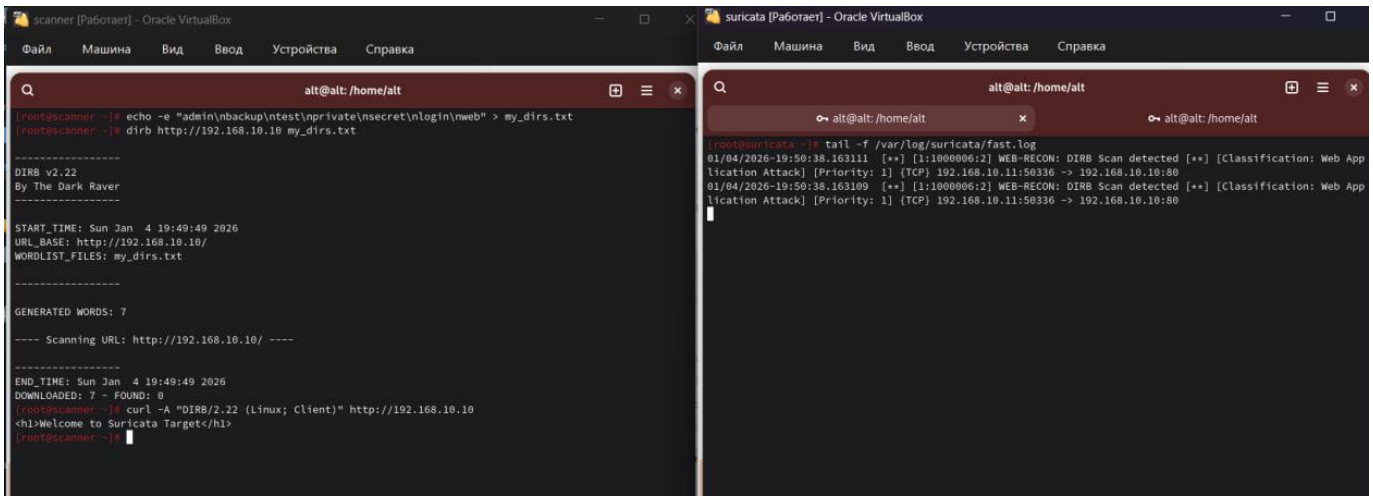

Рисунок 8 — Обнаружение инструмента перебора Dirb – тест 6

ЗАКЛЮЧЕНИЕ

В результате исследования были достигнуты цели: мы успешно развернули IDS Suricata и реализовали эксперимент с эмуляцией различных видов компьютерной разведки.

Результаты эксперимента подтвердили эффективность разработанных нами политик безопасности, сочетающей сигнатурный и поведенческий методы анализа. В частности:

1. Механизмы порогового анализа (Thresholding) позволили успешно блокировать агрессивное сканирование портов и ICMP-флуд, отсекая «шумную» активность на сетевом уровне.
2. Временная корреляция событий доказала свою эффективность против скрытых атак класса «Low-and-Slow», которые традиционно пропускаются стандартными межсетевыми экранами.
3. Технология глубокой инспекции пакетов (DPI) обеспечила точную идентификацию специализированного программного обеспечения (Nikto, Dirb, Nmap NSE) по их цифровым отпечаткам в заголовках прикладного уровня.

Также, было доказано, что Suricata отлично адаптирована к ОС Альт и стабильно функционирует в данной среде. Кроме того, на основании наших политик было определено, что данный вид IDS обладает достаточным набором функций и инструментов для выявления инцидентов reconnaissance-активности.

Разработанный нами набор политик потенциально может быть использован для защиты реальной инфраструктуры, но, вероятно, будет требовать индивидуальных доработок.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Education applications/Suricata — ALT Linux Wiki [Электронный ресурс]. URL: https://www.altlinux.org/Education_applications/Suricata (дата обращения: 04.01.2026).
2. Quickstart guide — Suricata 8.0.2 documentation [Электронный ресурс]. URL: https://docs.suricata.io/en/suricata-8.0.2/quickstart.html#installation (дата обращения: 04.01.2026).
3. Rules Format — Suricata 8.0.2 documentation [Электронный ресурс]. URL: https://docs.suricata.io/en/suricata-8.0.2/rules/intro.html (дата обращения: 04.01.2026).
4. Suricata.yaml — Suricata 8.0.2 documentation [Электронный ресурс]. URL: https://docs.suricata.io/en/suricata-8.0.2/configuration/suricata-yaml.html (дата обращения: 04.01.2026).
5. Rule Management with Suricata-Update — Suricata 8.0.2 documentation [Электронный ресурс]. URL: https://docs.suricata.io/en/suricata-8.0.2/rule-management/suricata-update.html (дата обращения: 04.01.2026).
6. Система обнаружений вторжений (IDS): что нужно знать, чтобы защитить корпоративную сеть [Электронный ресурс]. URL: https://www.securitylab.ru/analytics/536551.php. (дата обращения: 04.01.2026).
7. What is Suricata — Suricata 8.0.2 documentation [Электронный ресурс]. URL: https://docs.suricata.io/en/suricata-8.0.2/what-is-suricata.html (дата обращения: 04.01.2026).
8. Reconnaissance, Tactic TA0043 - Enterprise | MITRE ATT&CK® [Электронный ресурс]. URL: https://attack.mitre.org/tactics/TA0043/ (дата обращения: 04.01.2026).
9. Методический документ ФСТЭК РФ. профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ — Редакция от 03.02.2012 — Контур.Норматив [Электронный ресурс]. URL:

https://normativ.kontur.ru/document?moduleId=1&documentId=225741 (дата обращения: 04.01.2026).

10. ALT Linux - sisyphus - nmap-7.94-alt4 - Network exploration tool and security scanner [Электронный ресурс]. URL: https://packages.altlinux.org/en/sisyphus/srpms/nmap/ (дата обращения: 04.01.2026).
11. ALT Linux - sisyphus - nikto-2.1.6-alt1.git6f8c472 - web server vulnerability scaner [Электронный ресурс]. URL: https://packages.altlinux.org/en/sisyphus/srpms/nikto/ (дата обращения: 04.01.2026).
12. ALT Linux - p11 - dirb-2.22-alt3 - Web Content Scanner. [Электронный ресурс]. URL: https://packages.altlinux.org/en/p11/srpms/dirb/ (дата обращения: 04.01.2026).