



Автоматизация ключевых задач пентестов.
Система AlphaSense от Alpha Systems

Кто типовой заказчик AlphaSense?

/1

Компании и организации, не имеющие выделенного штата на содержание отделов анализа угроз (с функциями pentest_ов).

/2

Компании с задачей выделения сегментов по оценке защищенности (подход экономии ресурсов).

/3

Компании с актуальной задачей автоматизации отчетности по защите от уязвимостей (задачи внешние и/или внутренние).

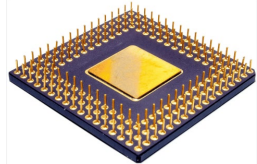
/4

Требуется универсальный, компактный инструмент для тестов как изнутри сети, так и снаружи.



Требования к вычислительным ресурсам решения AlphaSense

- **Минимальные (пилот):** 4 CPU, 8 GB RAM, 50 GB SSD. До 8 одновременных задач сканирования (~ до 1000 хостов);
- **Рекомендуемые:** 8 CPU, 16 GB RAM, 100 GB SSD. До 14 одновременных задач сканирования (до ~ 2000 хостов);
- **Для больших установок:** 24 CPU, 48 GB RAM, 400 GB SSD. До 40 одновременных задач сканирования (до ~ 6000).
- **Дистрибутив:** OVA или OVF, все компоненты (СУБД, Web-сервер, «движки», сценарии и т.п.) на борту;
- **Большинство современных систем виртуализации** (VMWare ESXi (6.7 и >), Oracle VirtualBox, Hyper-V, KVM).



Ключевые задачи создания AlphaSense

- Встроить наиболее эффективные инструменты для теста ОС/ПО, Web-оценки, подбора паролей;
- Добавить механизмы оценки по CVE, CPE, CWE, CAPECs (Mitre.org), CIPHER_SUITES и FSTEK DB;
- Разработать движки «моделей сопоставления» (ИИ-модели) и «эмуляции атаки» (EXPLOIT-DBs);
- Доработать механизмы и создать эффективный модуль «эмуляции обхода WAF» (ИИ-модели);
- Выполнить управляющий интерфейс в виде легкого и доступного для понимания Web-интерфейса;
- Упростить настройку аналитических задач и аккуратно автоматизировать эмуляцию эксплуатации.



Пример: интерфейс сканирования и обнаружения целей AlphaSense

Параметры обнаружения хостов

Общие настройки

- Использовать быстрый поиск хостов**
Если хост не отвечает на простые проверки, AlphaSense выполняет дополнительные тесты, чтобы убедиться, что хост действительно доступен. Быстрый поиск хостов пропускает эти дополнительные тесты. Если вы установили пользовательские диапазоны портов, эта опция будет отключена.
- Использовать широковещательный поиск**
Этот параметр используется для более точного поиска хостов и сервисов через широковещательные запросы в локальной сети. Будьте осторожны, это может привести к увеличению использования лицензий на хосты.

Методы пинга

- ARP
- SYN
- ACK
- UDP
- Расширенные методы**
Используются следующие методы: ICMP-эхо, отметка времени, определение маски сети, SCTP, TCP Connect и IPProto.

Диапазон портов для пинга:

Влияет только на методы пинга: SYN, ACK, TCP Connect и SCTP. По умолчанию используется пятьдесят общих сервисных портов.

Поиск сервисов SSL/TLS/DTLS

Поиск сервиса SSL/TLS:

Поиск сервиса DTLS:

- Найти сертификаты, истекающие через (дни)**
- Перечислить все SSL/TLS шифры**
При выборе этой опции AlphaSense игнорирует список шифров, рекламируемых сервисами SSL/TLS, и перечисляет их, пытаясь установить соединение с использованием всех возможных шифров.

Сканирование портов

Методы сканирования

Тип:

- UDP
- SCTP INIT и COOKIE-ECHO

Параметры портов

- Использовать последовательное сканирование портов**
- Использовать быстрое сканирование портов**
Быстрое сканирование использует только top100 известных портов. Если вы установили пользовательские диапазоны портов, эта опция будет отключена.

Диапазон TCP-сканирования:

Диапазон UDP-сканирования:

Вы также можете ввести порты в формате 1,2,3,4 или в диапазоне 80-90, а также использовать предустановленные значения, такие как top10, top50, top100, top1000 и т.д. Это поле влияет на все типы сканирования. Включение UDP-сканирования может значительно увеличить время сканирования.

Обнаружение сервисов и ОС

- Использовать расширенное обнаружение ОС**
По умолчанию AlphaSense использует быструю проверку и пытается определить ОС только для хостов с хотя бы одним открытым и закрытым портом. Эта опция повысит точность и выполнит определение ОС для всех доступных хостов.
- Использовать расширенное обнаружение сервисов**
Эта опция используется для более точного обнаружения сервисов и версий через расширенные скрипты и запросы. Увеличение количества запросов может повысить точность, но замедлит процесс сканирования. Однако будьте осторожны: эта опция может вызвать нежелательные эффекты, например, принтеры могут выводить ненужные данные, HTTP-запросы GET или попытки SSL-сессий на некоторых портах, например TCP 9100.

Параметры времени

Некоторые преимущества управления и конфигурации AlphaSense

- Достаточно начального понимания работы базовых протоколов для организации соединений;
- Опции конфигурирования и тонкой настройки инструментов сведены к выпадающим спискам и типовым значениям;
- Для большинства расширенных опций дано смысловое пояснение на русском языке;
- Весомое количество продвинутых функций:
 1. Функционал обхода межсетевых экранов (поиск уязвимостей для динамического открытия портов);
 2. Фрагментация IP-пакетов и сокрытие сканирования, расширенное обнаружение параметров ОС;
 3. Эмуляция подменных заголовков HTTP (WAF) и обработка токенов Anti-CSRF (Web);
 4. Указание обработки Web-перенаправлений, подстановка суффиксов и шаблонов URL;
 5. Повторное сканирование в режиме атаки и другое.

Лицензирование AlphaSense и действующие заказчики



ГИДРОМАШ



BAON

ТРИНФИКО

BIDZAAR

ЕАПТЕКА



АКТИВ
БИЗНЕС
КОНСАЛТ



росинтер
ресторантс

Лицензирование
по числу IP-адресов

Модель подписок:
1, 2, 3 года

Постоянные лицензии:
индивидуально под проект,
по запросу



NETWELL

Контакты

📍 Москва
115114, 1-й Дербеневский пер., 5 БЦ «Дербеневская Плаза»

📍 Санкт-Петербург
190000, Английская набережная, 70

📍 Казань
190000, Карла Маркса 7

+7 (495) 662 39 66

info@netwell.ru

netwell.ru

