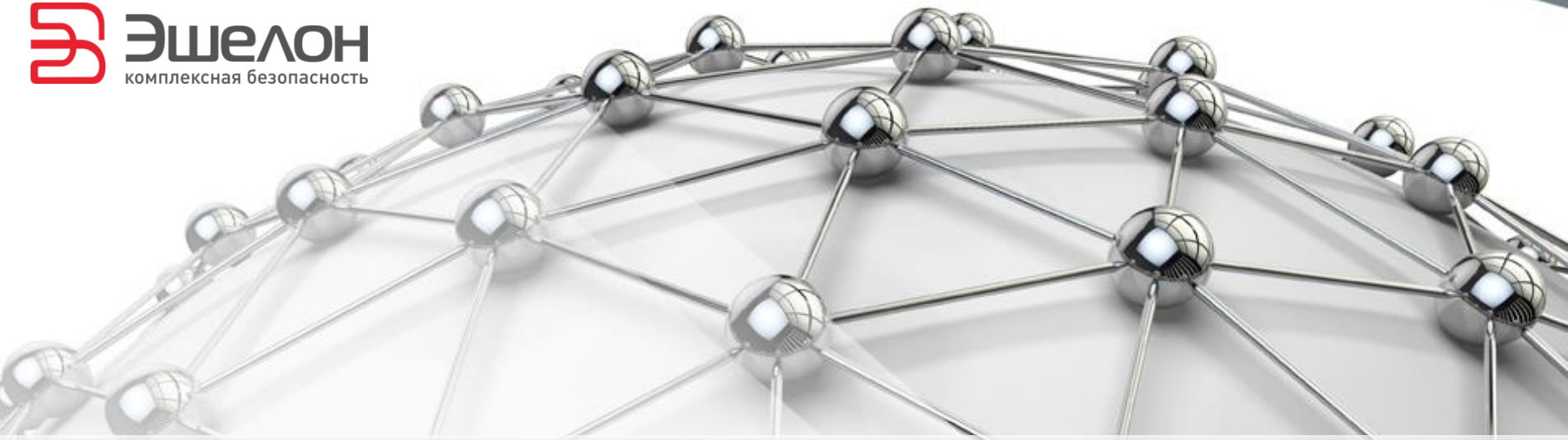
Эшелон
комплексная безопасность



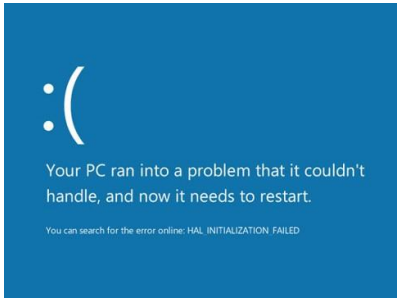
SIEM-система как основа для выявления компьютерных атак несигнатурными методами

Дорофеев А.В.
CISA, CISSP, CISM

План

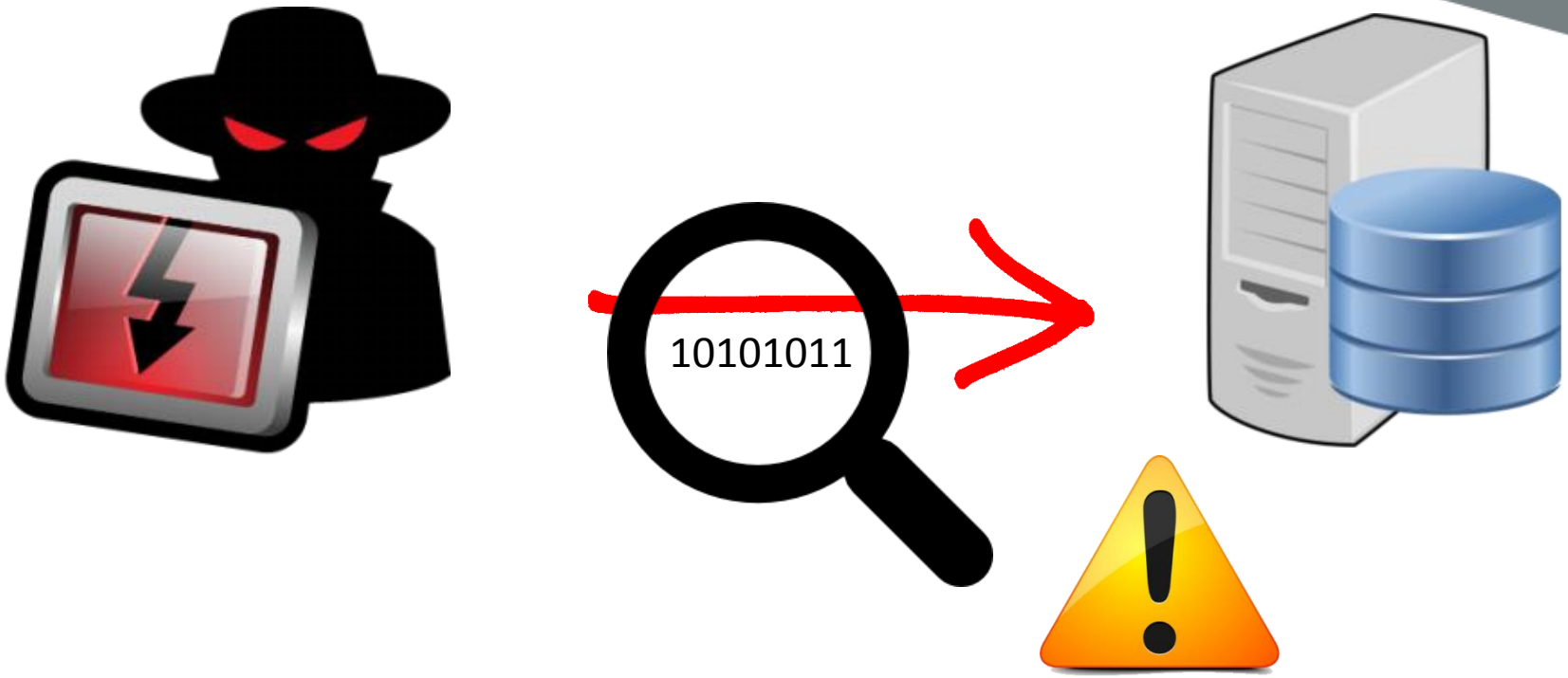
1) Традиционные атаки и сигнатурные методы их обнаружения
2) Современные таргетированные атаки
3) SIEM-система: основные принципы работы
4) Выявление таргетированной атаки с помощью SIEM

Традиционный взгляд на атаку



Эшелон
комплексная безопасность

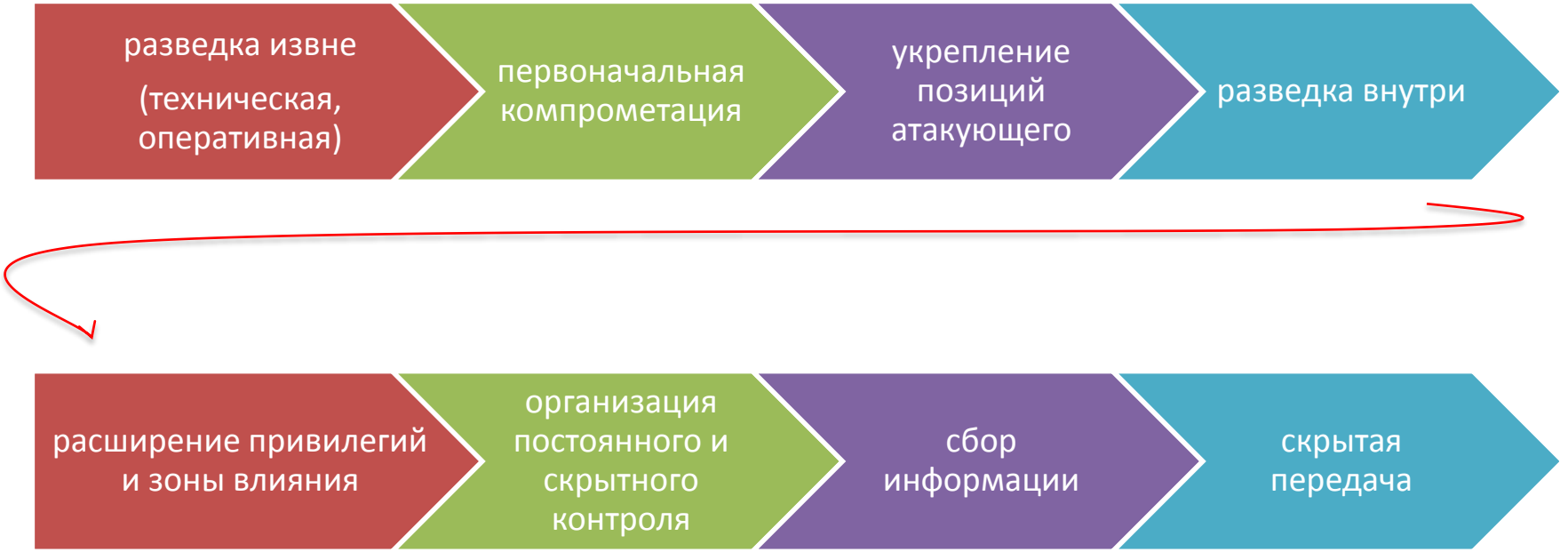
Сигнатурный метод выявления вторжений



Срабатывание антивируса, СОВ

Эшелон
комплексная безопасность

Современные сетевые атаки



Эшелон
комплексная безопасность

Фазы современной атаки (1)

Можно выделить несколько фаз атаки, необязательно идущих последовательно:

- ✓ **Разведка.** Сбор информации о целях для осуществления атаки.
- ✓ **Первоначальная компрометация**. Например, взлом нескольких рабочих станций организации с помощью вирусов, социальной инженерии и т.п.
- ✓ **Укрепление позиции.** Например, установка скрытых средств администрирования на первоначально взломанные системы для комфортного доступа в сеть извне.

Фазы современной атаки (2)

- **Внутренняя разведка**. Например, сбор подробной информации об информационных потоках организации, используемых ИТ-решениях.
- **Расширение привилегий.** Например, взлом критичных серверов организации и элементов сетевой инфраструктуры.
- **Организация постоянного и скрытого контроля.** Например, использование скомпрометированных учетных записей администраторов.
- **Сбор и передача вовне интересующей информации.**

Технологический уровень современных атак

Традиционная атака

Современная таргетированная атака

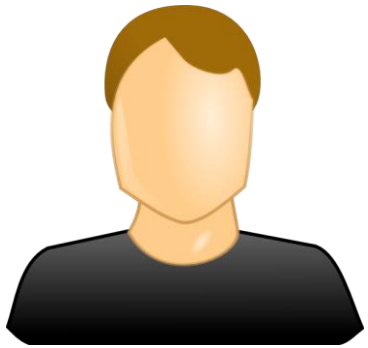
Эшелон
комплексная безопасность

Как обнаруживать современные сетевые атаки?

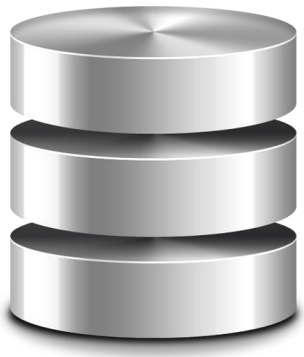
Признаки атак

Аутентификация: как успешная, так и неуспешная

Срабатывания антивирусного ПО



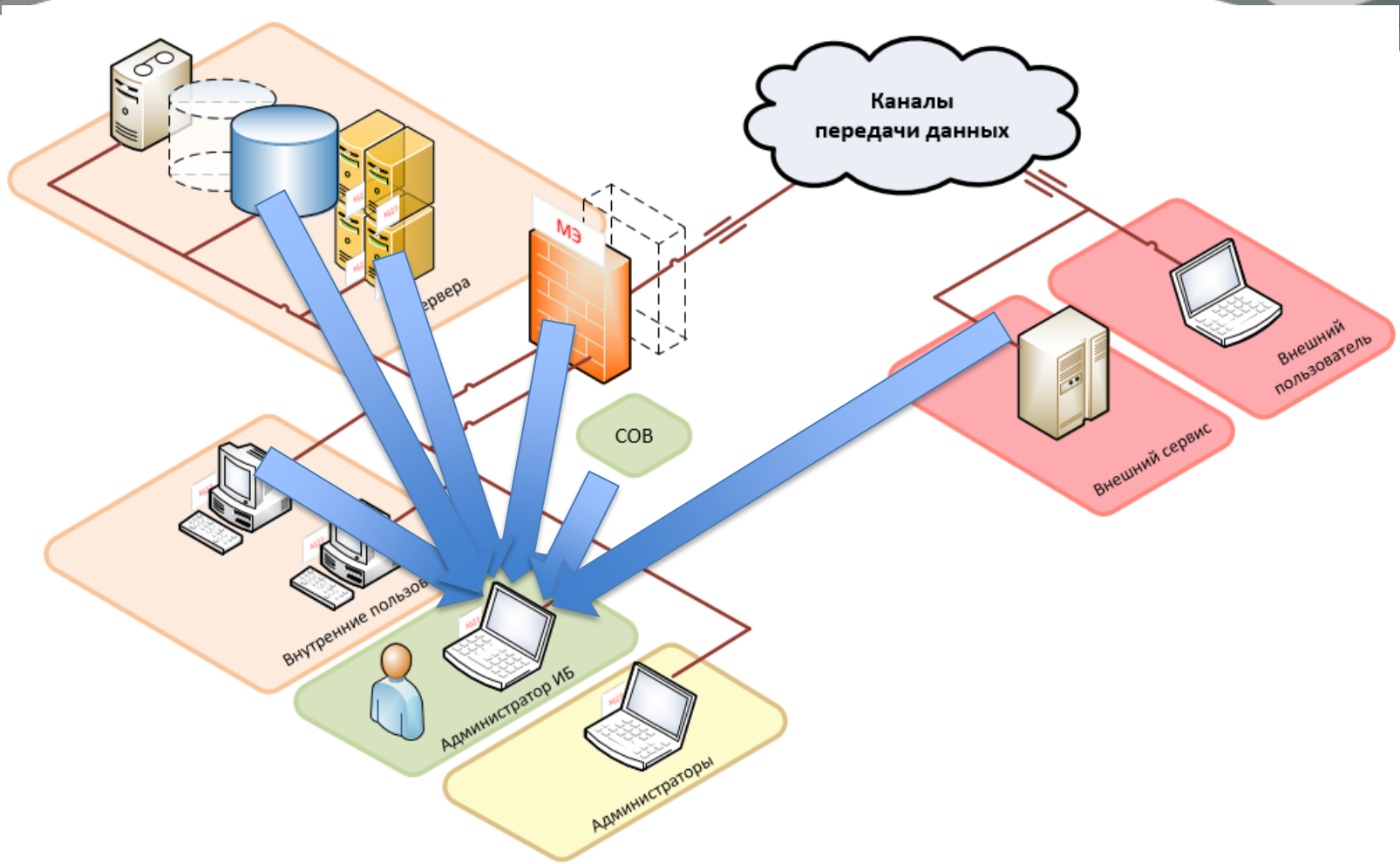
Нетипичное поведение пользователя в ОС



Подозрительные запросы к СУБД

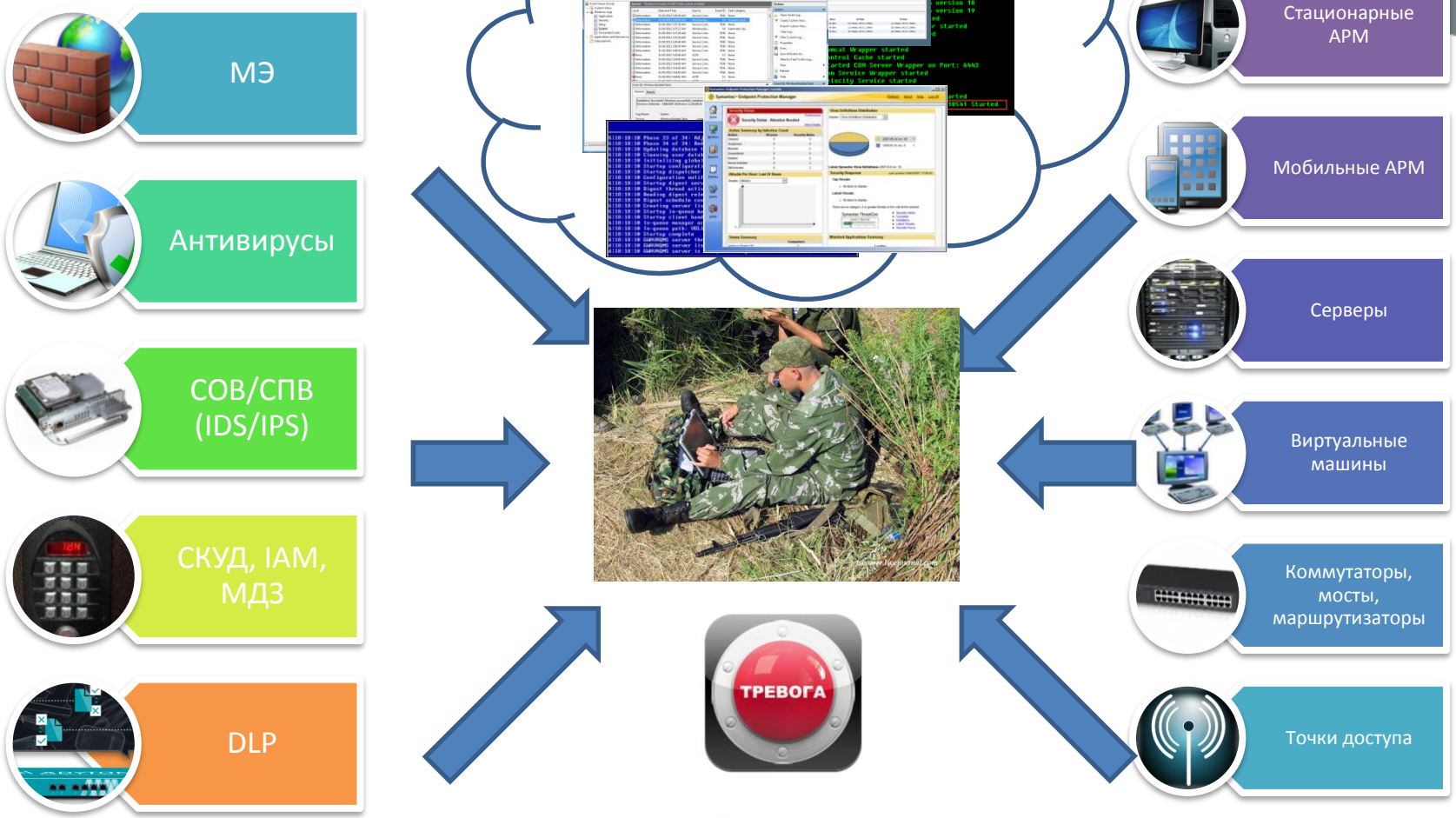
и т.д. и т.п.

Необходимо осуществлять мониторинг всей инфраструктуры



Эшелон
комплексная безопасность

Ручной сбор может быть проблематичным



Эшелон
комплексная безопасность

Принцип работы SIEM-системы

Источники событий

Фильтрация

Нормализация

Агрегирование

Корреляция

Приоритезация

Оповещение
и учёт инцидентов

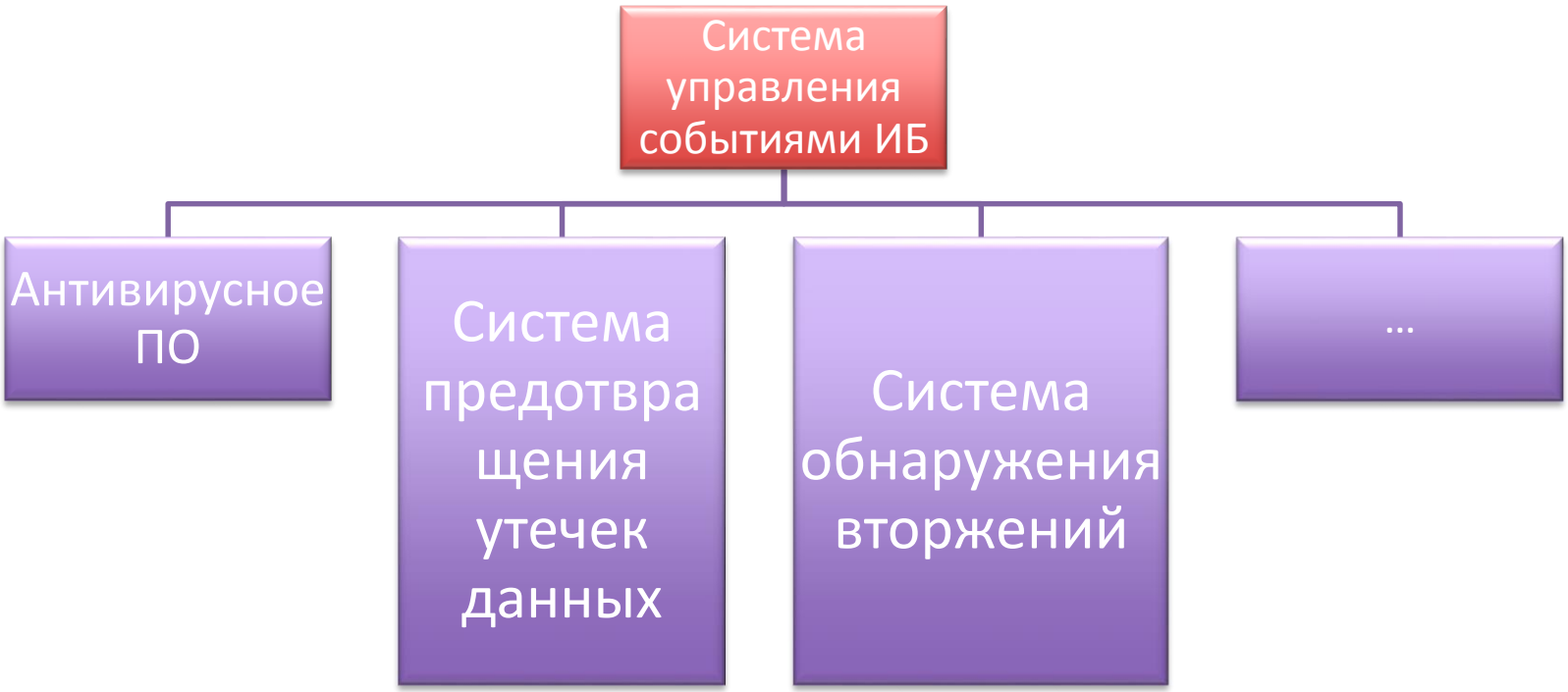
Аналитика

Эшелон
комплексная безопасность

Основные задачи, решаемые SIEM-системой

- ✓ Мониторинг событий информационной безопасности
- ✓ Анализ событий
- ✓ Консолидация и хранение журналов событий от разнообразных источников
- ✓ Управление инцидентами
- ✓ Выявление угроз

Связь с другими классами систем защиты



Эшелон
комплексная безопасность

Источники событий

Сетевое оборудование

Операционные системы

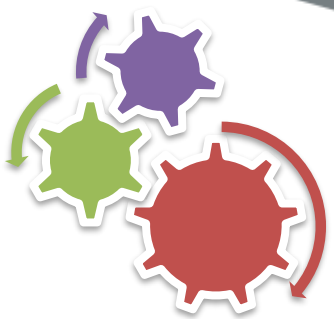
СУБД

Средства Защиты Информации

Системы Управления Контролем Доступа

и многое другое…

Полноценное внедрение SIEM-системы



Обследо-вание

Дизайн процессов управления инцидентами

Проектиро-вание системы

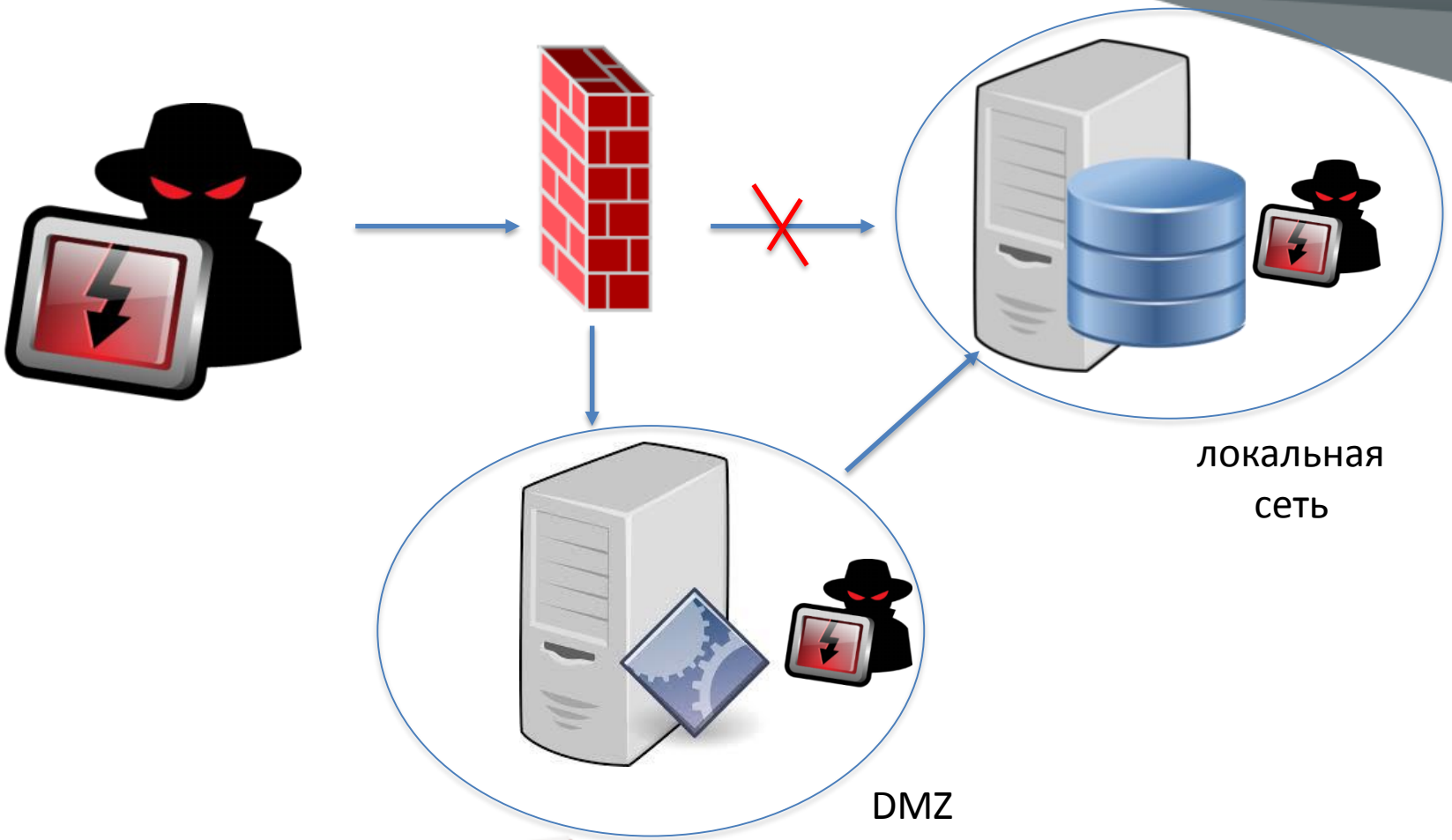
Поставка

Инсталляция, настройка и обучение

Опытная эксплуатация и внедрение процессов

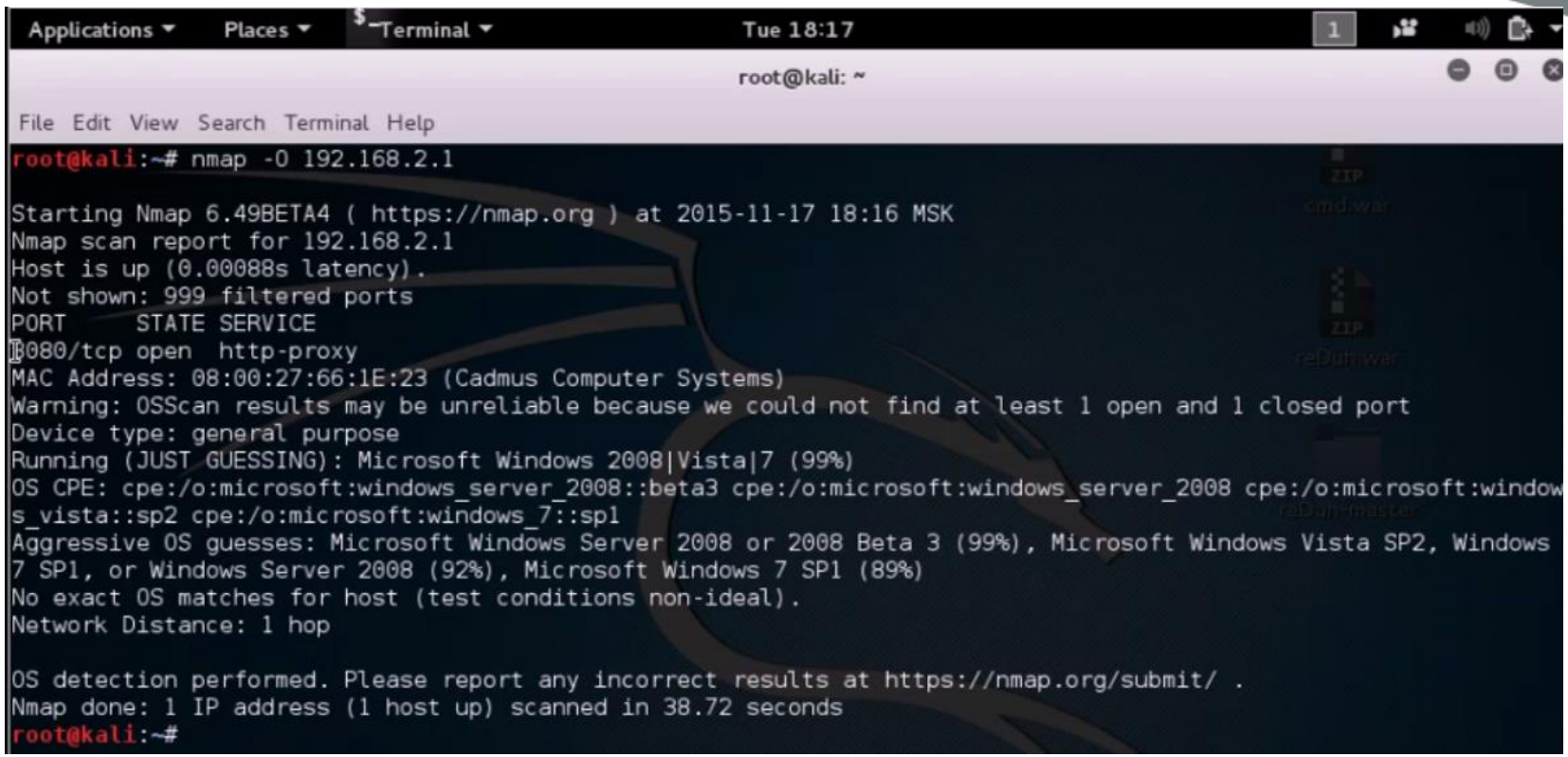
Эшелон
комплексная безопасность

Демонстрация

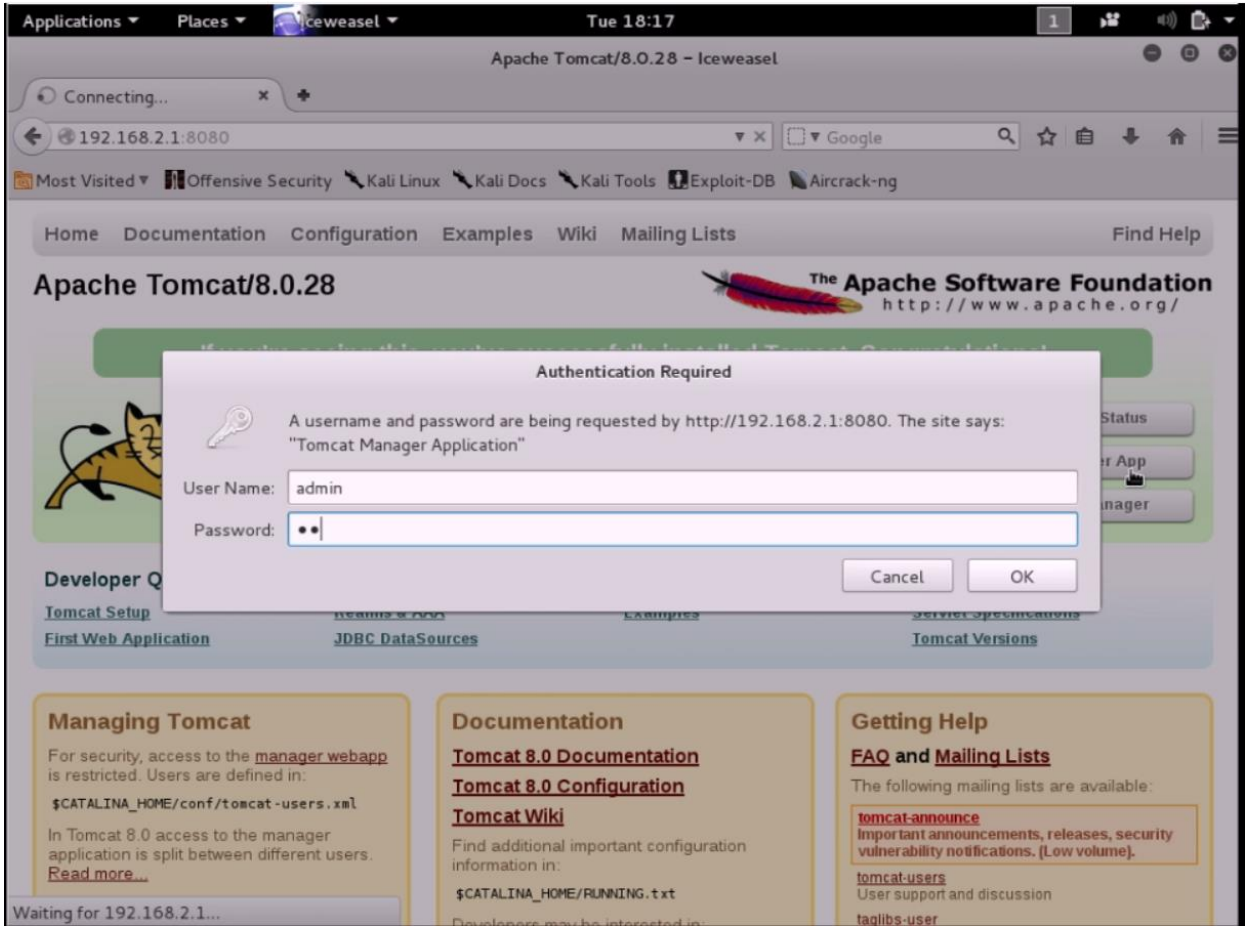


Эшелон
комплексная безопасность

1. Злоумышленник сканирует порты

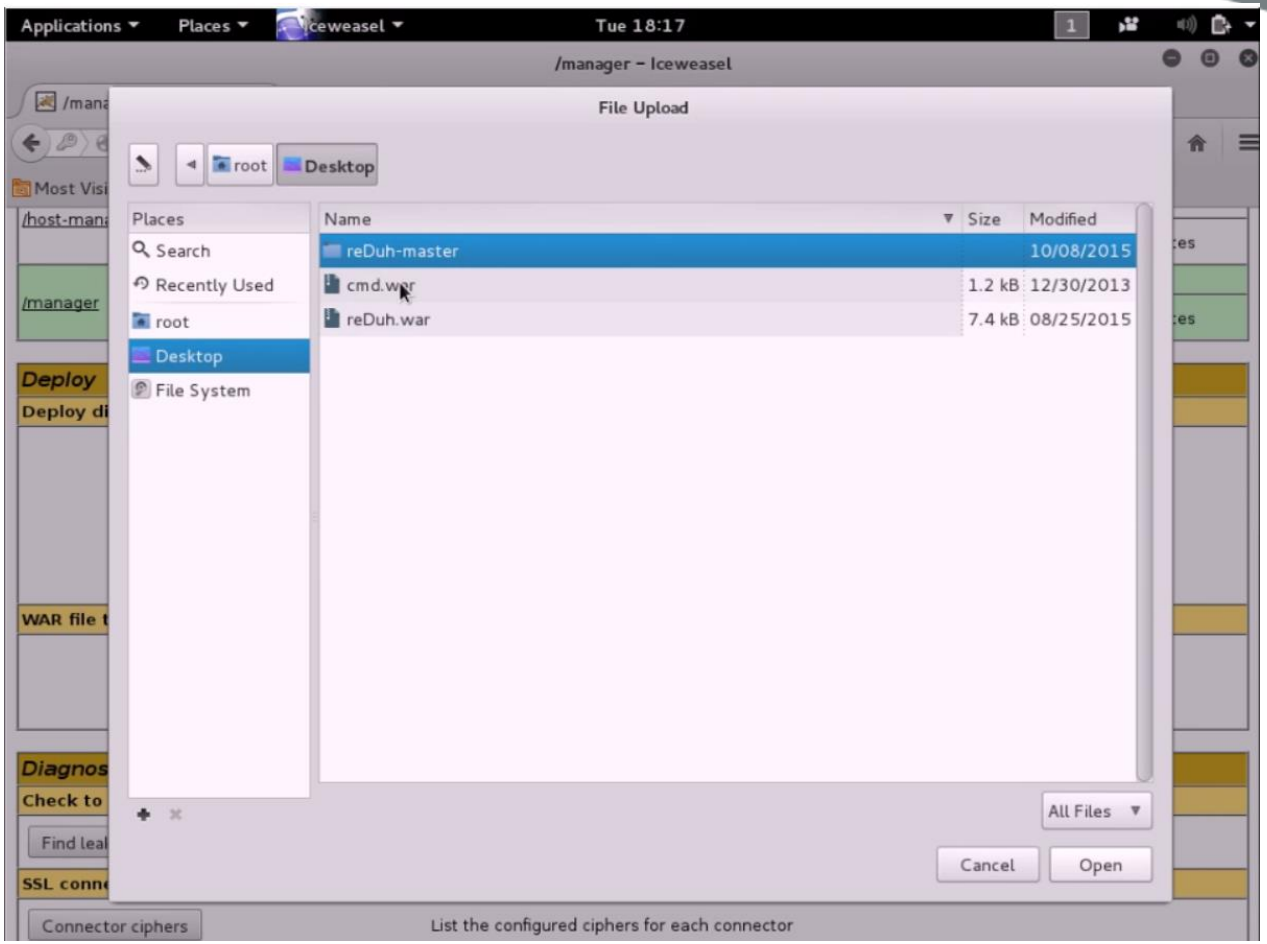


2. Злоумышленник подбирает пароль



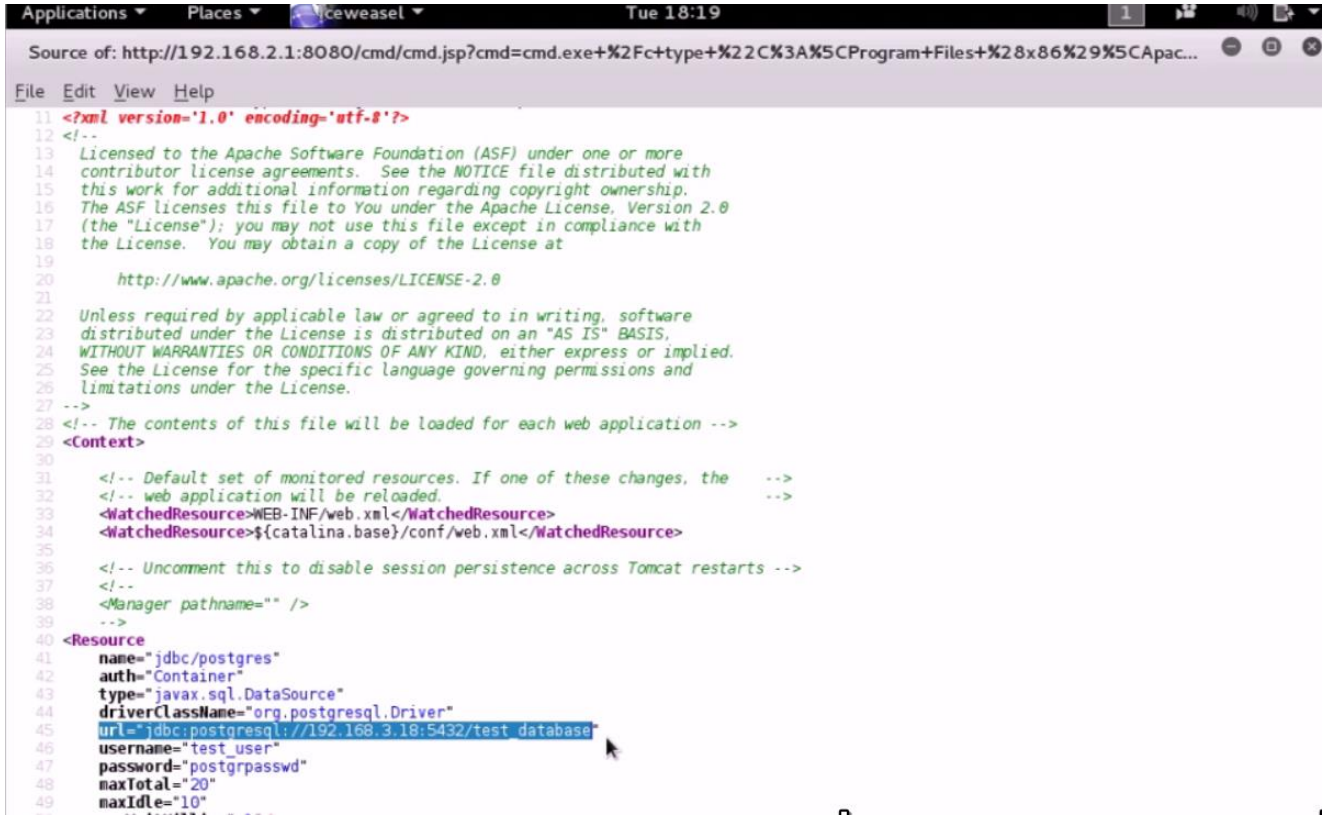
Эшелон
комплексная безопасность

3. Злоумышленник загружает вредоносные веб-приложения



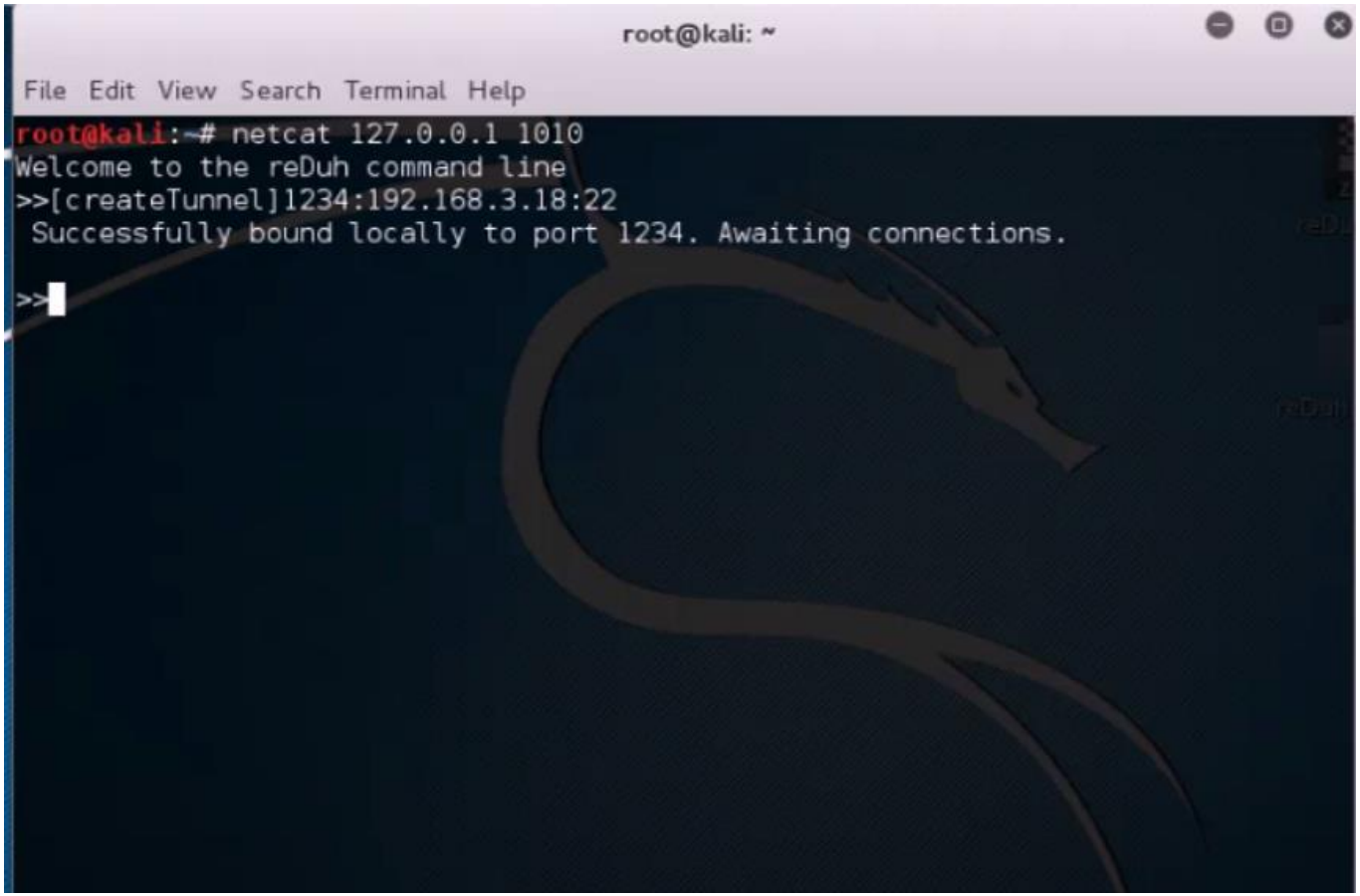
Эшелон
комплексная безопасность

4. Злоумышленник узнает пароль для доступа к БД



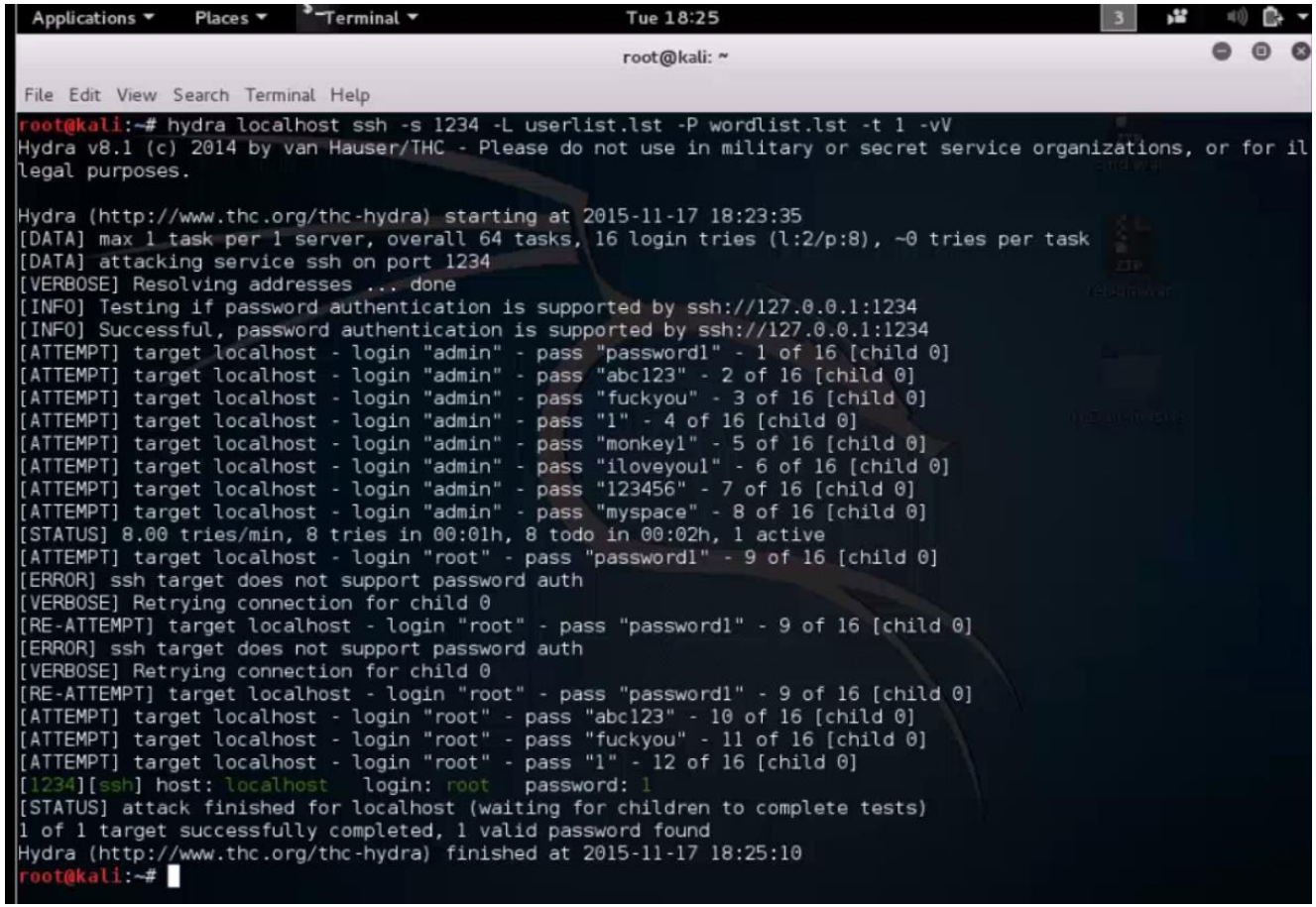
Эшелон
комплексная безопасность

5. Злоумышленник создает туннель для доступа к БД

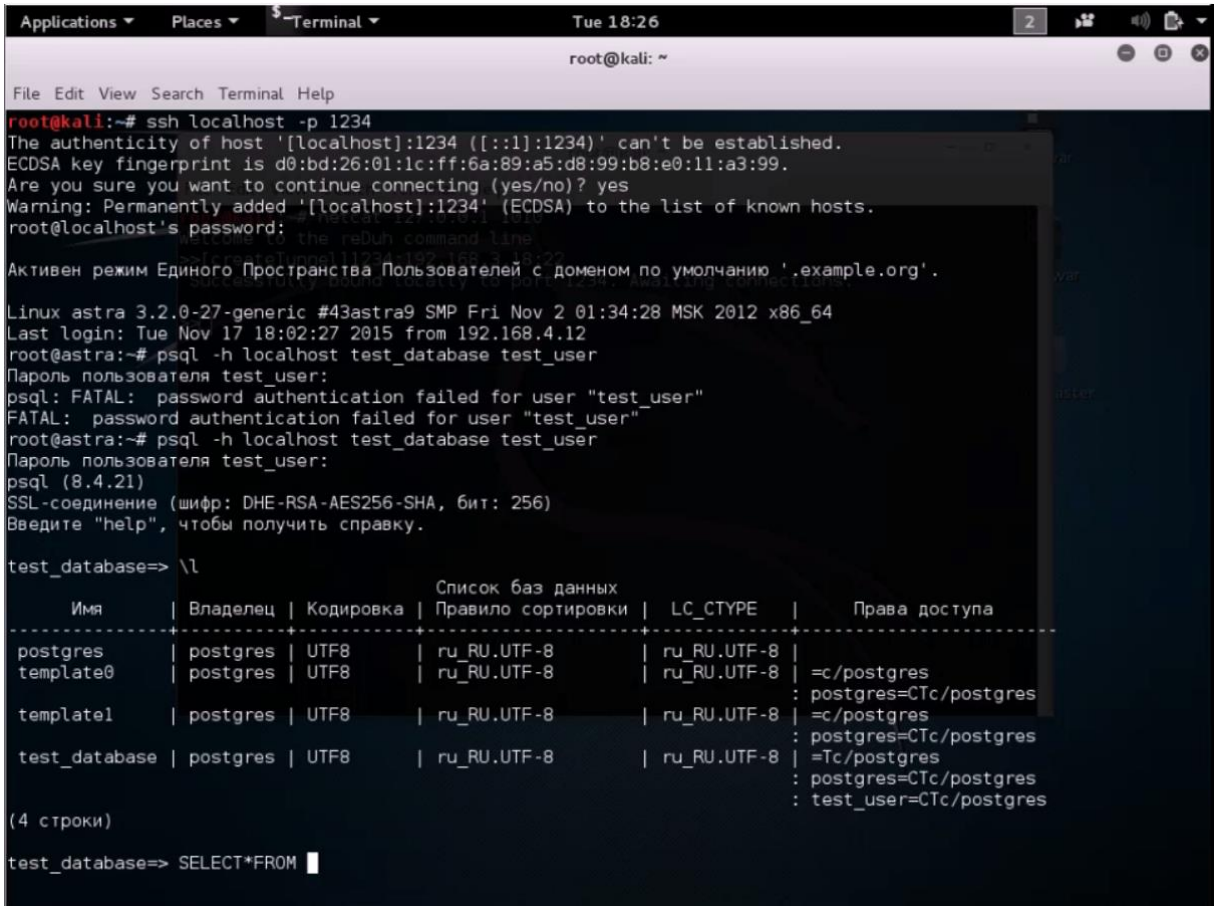


Эшелон
комплексная безопасность

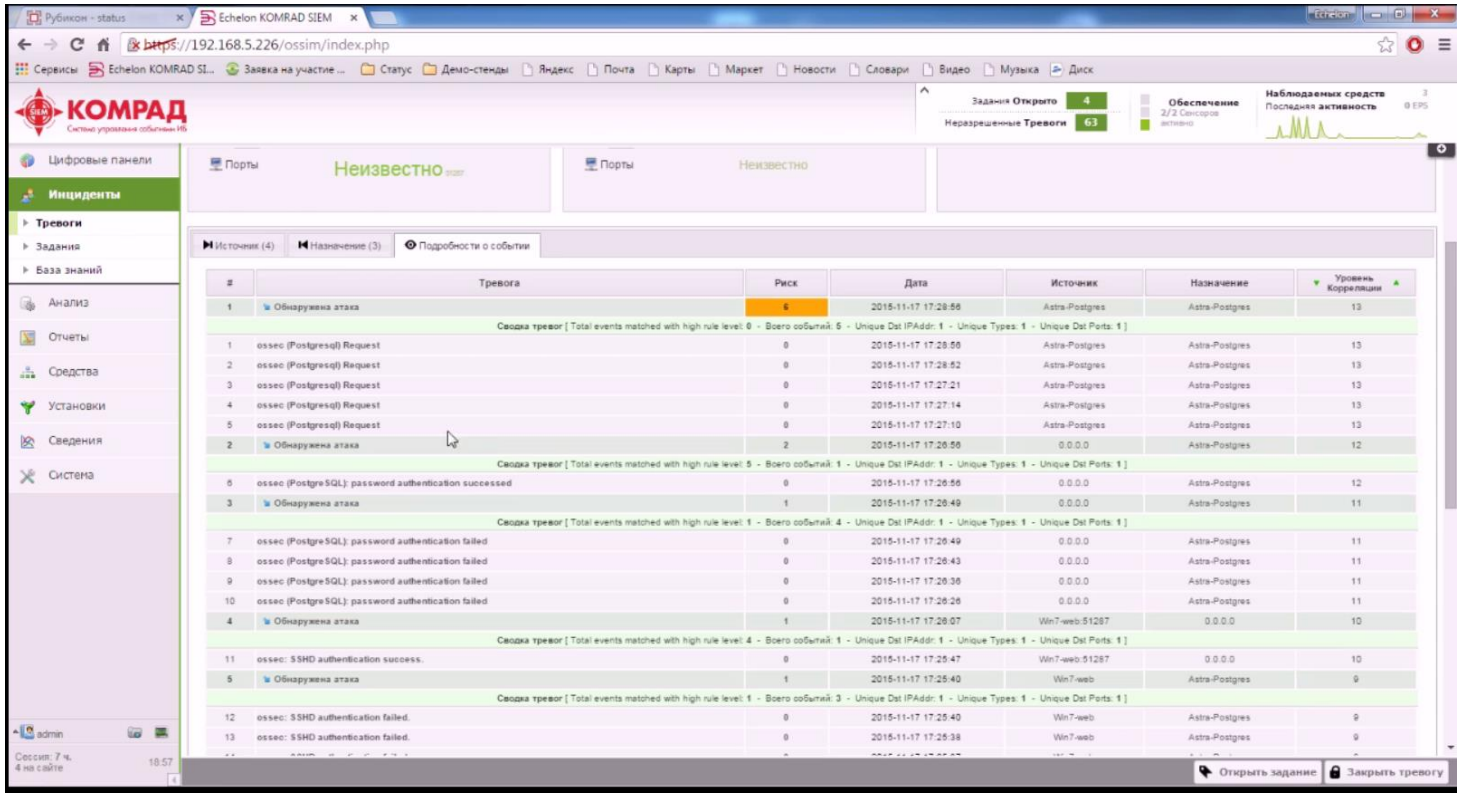
6. Подбор пароля к серверу БД



7. SQL-запросы к серверу БД



8. Все события зарегистрированы SIEM-системе



Эшелон
комплексная безопасность

SIEM - единая точка контроля состояния ИБ

Эшелон
комплексная безопасность

НАУЧНЫЙ, ПРАКТИЧЕСКИЙ, ПЕРИОДИЧЕСКИЙ, РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ
ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

Контактная информация

107023, ул. Электрозаводская, д. 24

+7(495) 223-23-92
+7(495) 645-38-11

http://www.npo-echelon.ru

mail@npo-echelon.ru