SAFEINSPECT

Ключи от королевства под контролем!

Зачем нужен SAFEINSPECT? Он необходим, если Вы хотите:

- Иметь неопровержимые доказательства факта компрометации целевого сервера
- Наиболее быстро реагировать на инциденты
- Анализировать поведение злоумышленника
- Выявить нанесение умышленного или неумышленного вреда ресурсам компании системными администраторами
- Контролировать подрядчиков, которые обслуживают конечное оборудование

Архитектура:

- Законченное решение, поставляется в виде .iso или .ovf (виртуальный appliance)
- Основа – FreeBSD
- Одна машина может иметь две роли – Менеджер либо Коллектор
- Менеджер – хранилище и единая консоль для администрирования, управления политиками, просмотра подключений
- Коллектор – инспектирует и аудирует подключения администраторов к конечным серверам
- Три режима работы коллектора:
    1. Маршрутизатор (L3)
    2. Сетевой мост/бридж (L2/поддерживает VLAN)
    3. Бастион (user@host)
- Не требует установки агентов
- Не требует специальных клиентов – используется стандартное ПО для подключений

Основные возможности:

Запись и воспроизведение сессий:

- SSH (*nix)
- RDP (Windows)
- HTTP(s)
- Telnet,TN3270 и т.д.

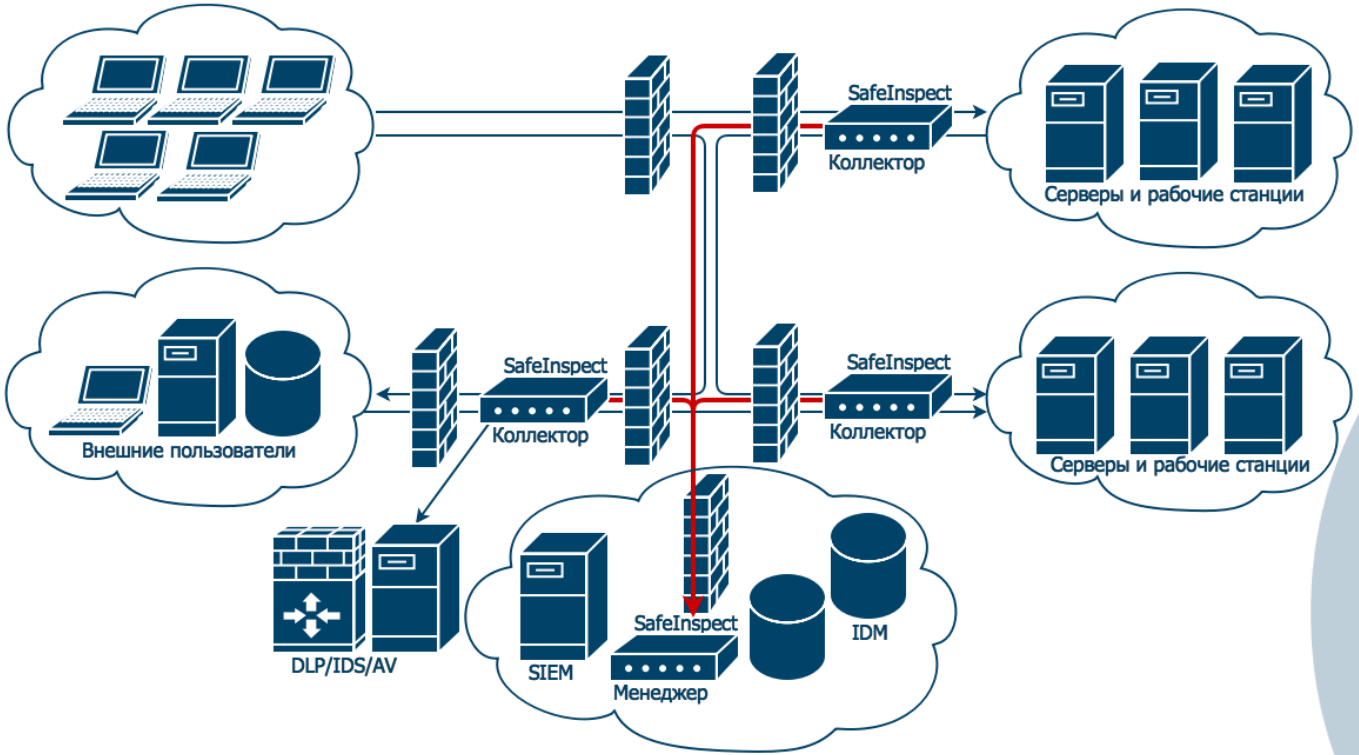
Определение и аудит подканалов:

- SCP,SFTP, X11 и др. (SSH)
- Буфер обмена, подключаемые устройства (RDP)

Индексация содержимого, поиск по ключевым словам

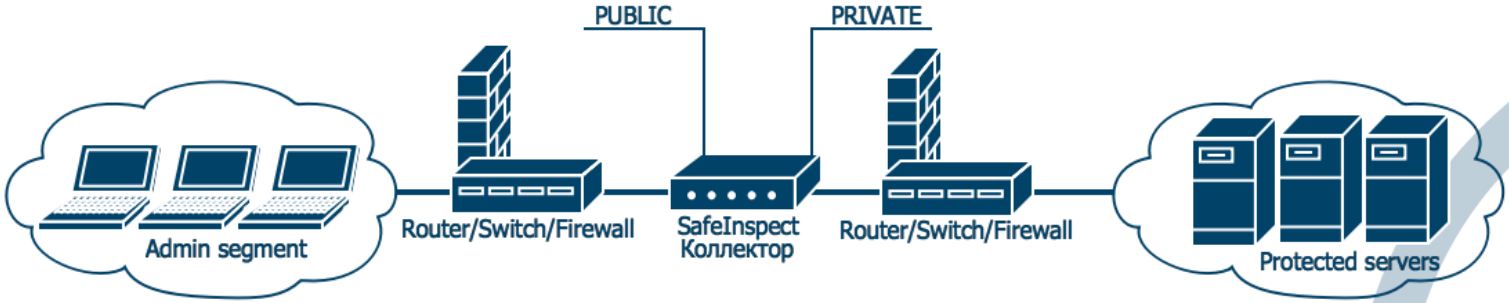
Оптическое распознавание символов в RDP (OCR)

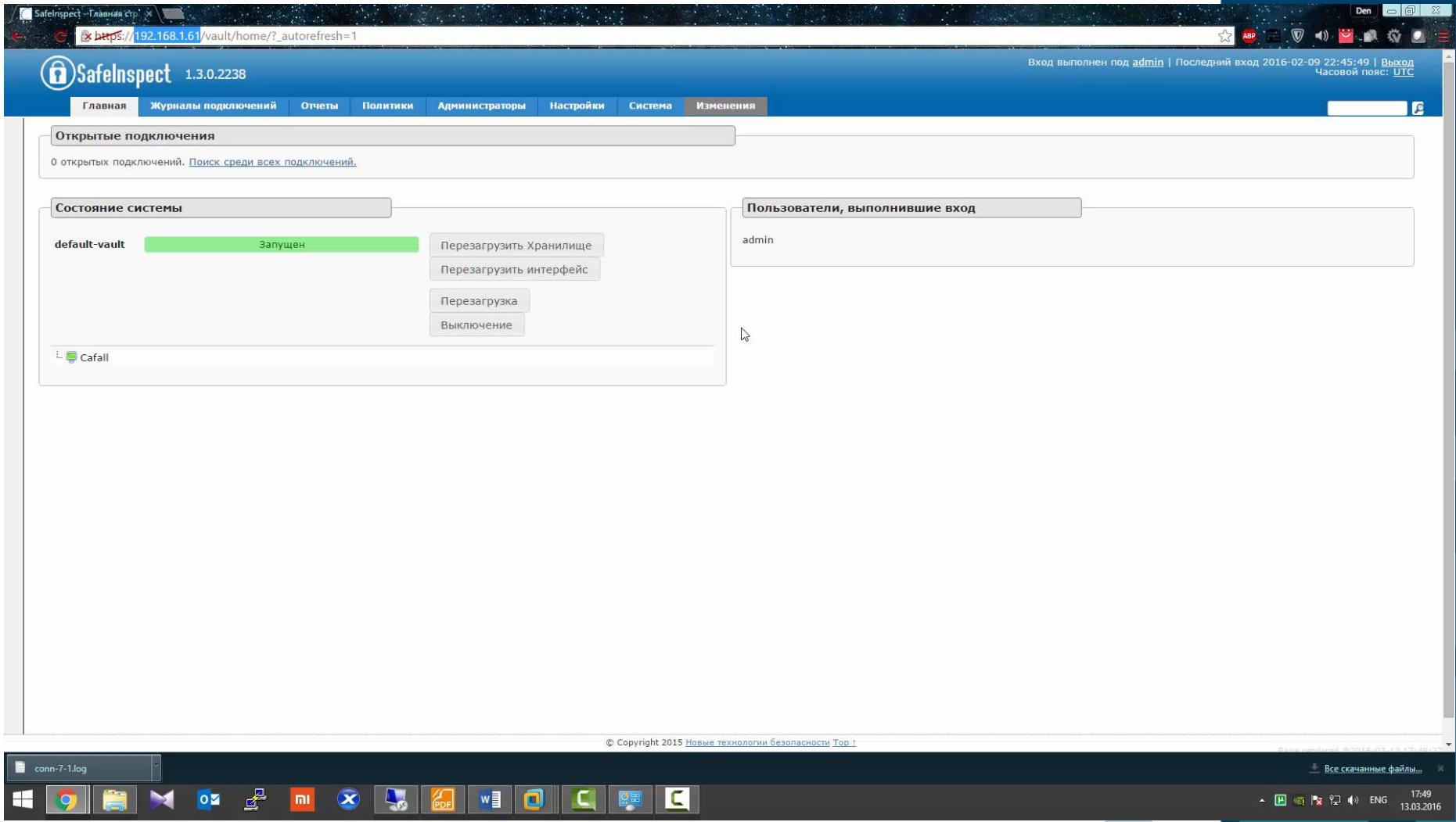
Общая схема:


SafeInspect
Коллектор
Серверы и рабочие станции
Внешние пользователи
SafeInspect
Коллектор
SafeInspect
Коллектор
Серверы и рабочие станции
DLP/IDS/AV
SIEM
SafeInspect
Менеджер
IDM

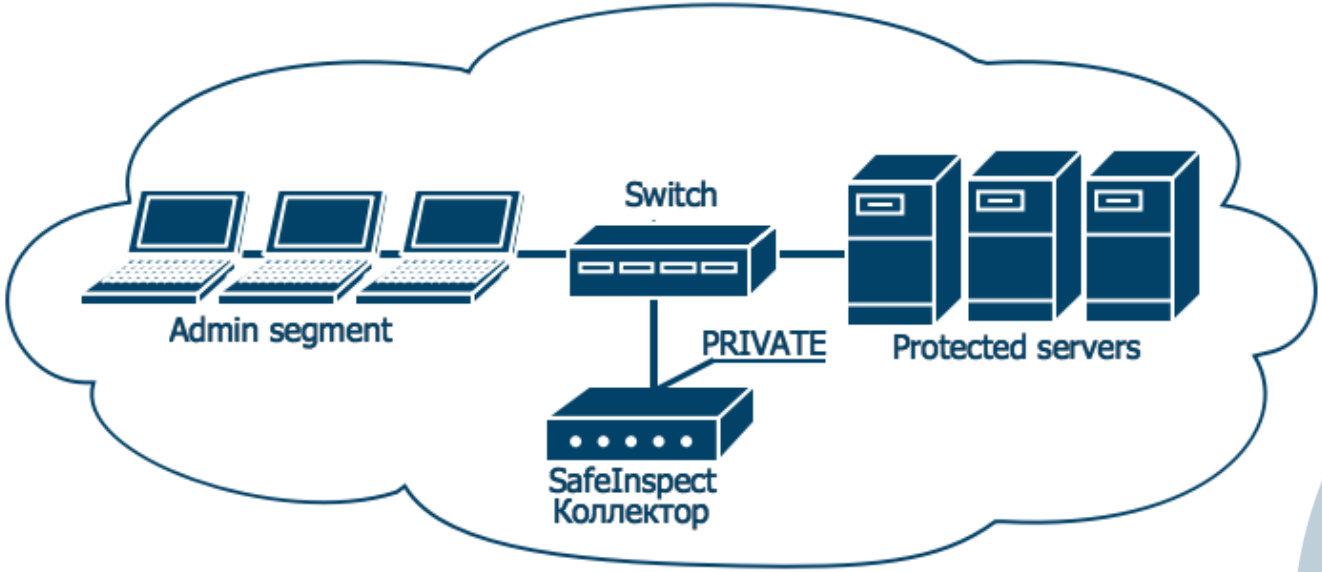
Режим L-2 мост:

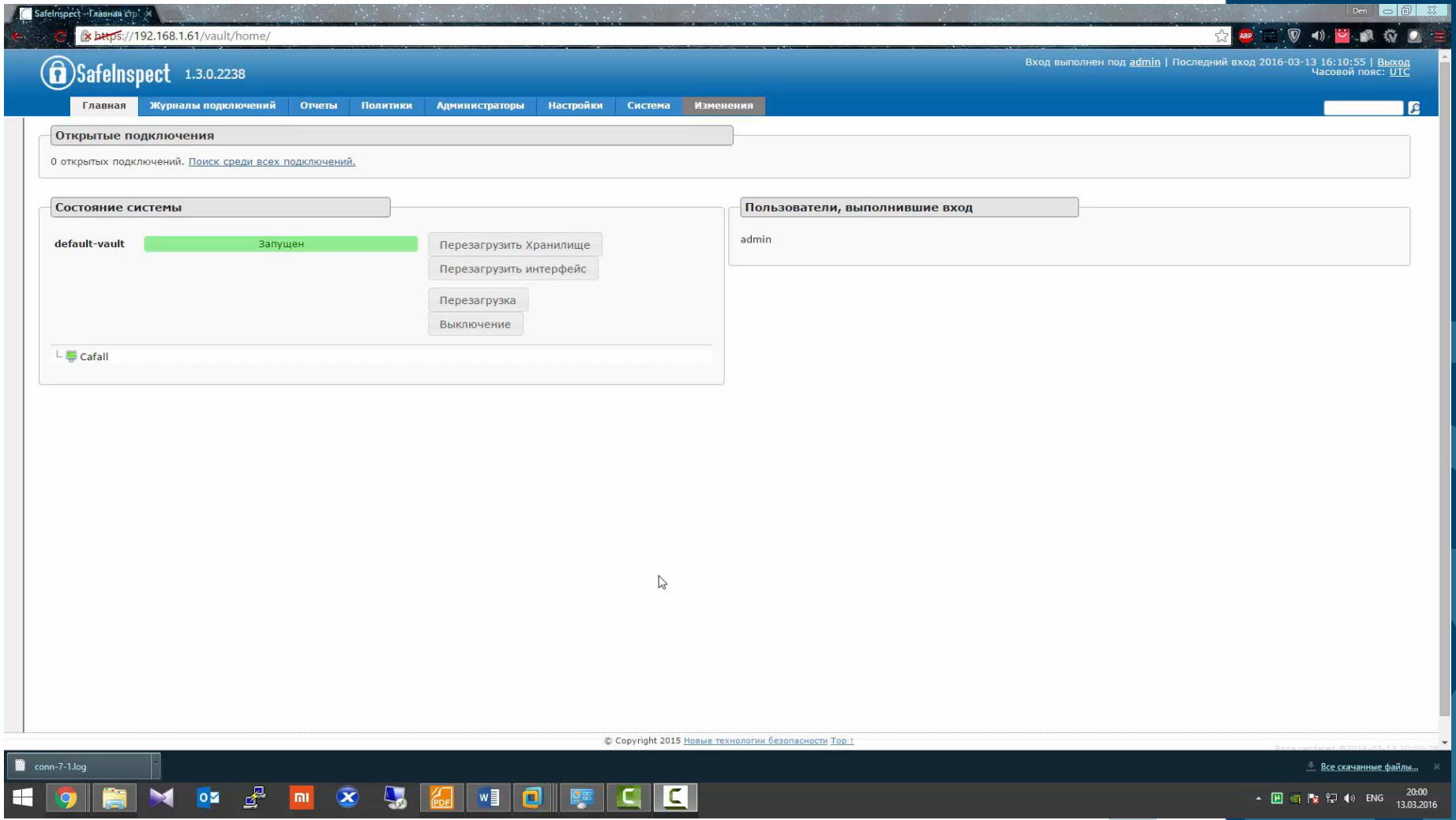
Режим L-3 маршрутизатор:




SafeInspect --Главная стр
https://192.168.1.61/vault/home/?_autorefresh=1
Den
SafeInspect 1.3.0.2238
Вход выполнен под admin | Последний вход 2016-02-09 22:45:49 | Выход
Часовой пояс: UTC
Главная
Журналы подключений
Отчеты
Политики
Администраторы
Настройки
Система
Изменения
Открытые подключения
0 открытых подключений. Поиск среди всех подключений.
Состояние системы
default-vault
Запущен
Перезагрузить Хранилище
Перезагрузить интерфейс
Перезагрузка
Выключение
Cafall
Пользователи, выполнившие вход
admin
© Copyright 2015 Новые технологии безопасности Top ↑
conn-7-1.log
Все скачанные файлы...
ENG
17:49
13.03.2016

РЕЖИМ БАСТИОН




SafeInspect - Главная стр
https://192.168.1.61/vault/home/
SafeInspect 1.3.0.2238
Вход выполнен под admin | Последний вход 2016-03-13 16:10:55 | Выход
Часовой пояс: UTC
Главная
Журналы подключений
Отчеты
Политики
Администраторы
Настройки
Система
Изменения
Открытые подключения
0 открытых подключений. Поиск среди всех подключений.
Состояние системы
default-vault
Запущен
Перезагрузить Хранилище
Перезагрузить интерфейс
Перезагрузка
Выключение
Cafall
Пользователи, выполнившие вход
admin
© Copyright 2015 Новые технологии безопасности Top ↑
conn-7-1.log
Все скачанные файлы...
ENG
20:00
13.03.2016

Дополнительные возможности:

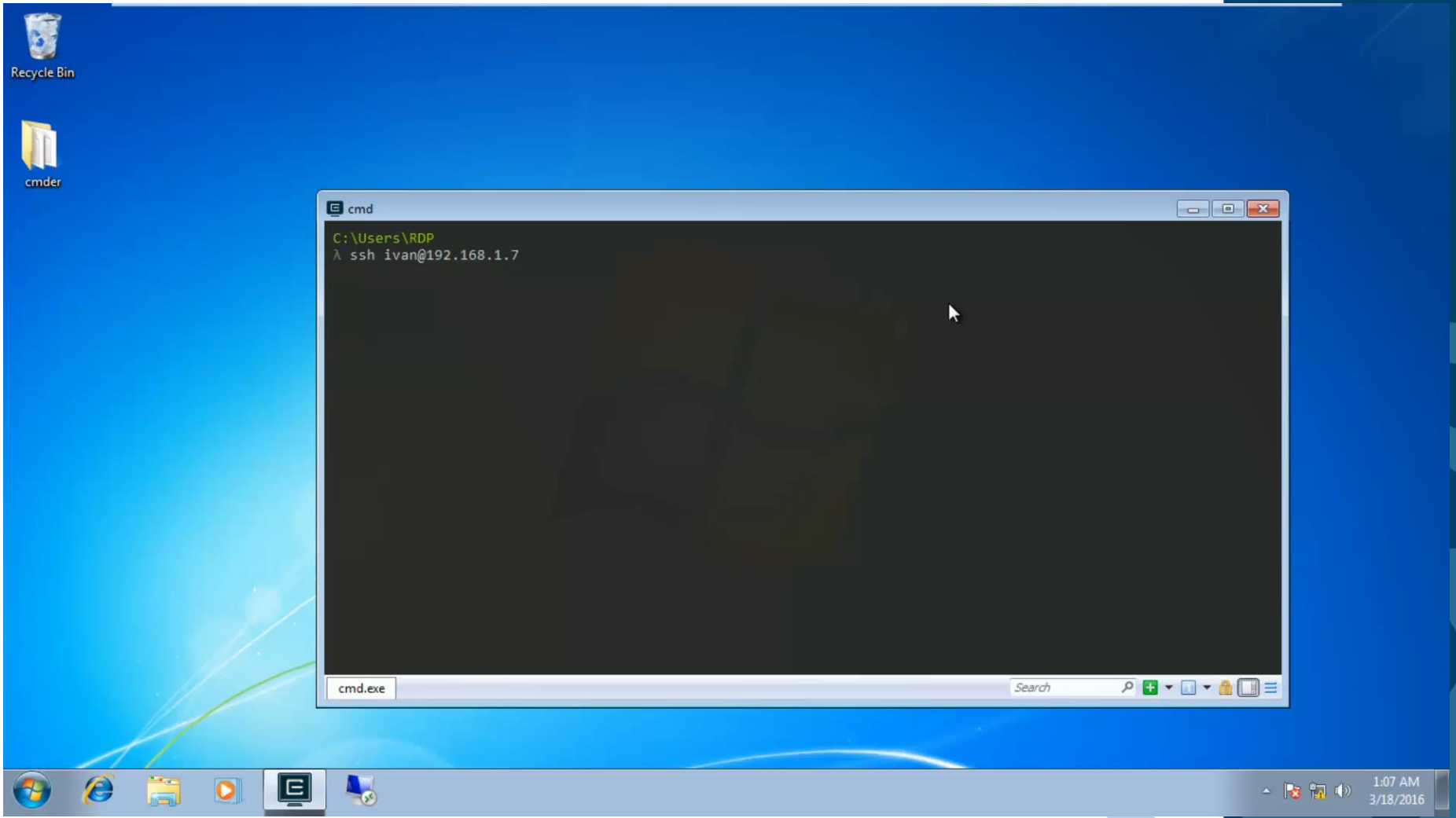
User-maping (для SSH и RDP)

- Возможность скрытия учетных данных конечного администратора
- Работает с паролями и приватными ключами

Дополнительная авторизация

- Отправка уведомления вышестоящему руководителю или офицеру безопасности с возможностью принять/отклонить подключение

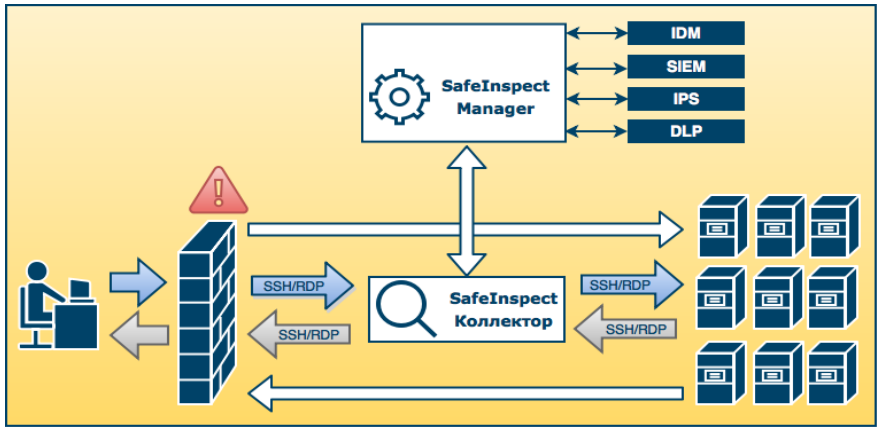
- Ролевая модель администрирования
- Дополнительная защита - разделение на «зоны аудита»
- Каждой «зоне» назначается свой пароль, без которого невозможно просмотреть данные подключений
- Записанные данные подключений шифруются в центральном хранилище (AES-128)
- Коммуникации между Коллектором и Менеджером защищены, используется TLS-соединение


Recycle Bin
cmder
cmd
C:\Users\RDP
λ ssh ivan@192.168.1.7
cmd.exe
Search
1:07 AM
3/18/2016

Обеспечение комплексной защиты и контроля

Интегрируется со следующей инфраструктурой и процессами:

- Identity management (AD, RADIUS, RSA SecurID)
- SIEM – Syslog/LEEF/CEF (IBM QRadar, RSA key, Splunk и т.д.)
- IDS/IPS
- DLP (RSA DLP, McAfee, ICAP-сервера и т.д.)



Технические требования

Размер сохраняемых подключений:

SSH:

- 1 Мб/ч (без индекса),
  3 Мб/ч (с индексом)

RDP *(для разрешения 1024x768):*

- Типичное административное использование: 30 Мб/ч
- С интенсивным использованием графики: 300 Мб/ч

Требования для Менеджера:

- 8 Гб ОЗУ
- 500 Гб диск

Требования для Коллектора:

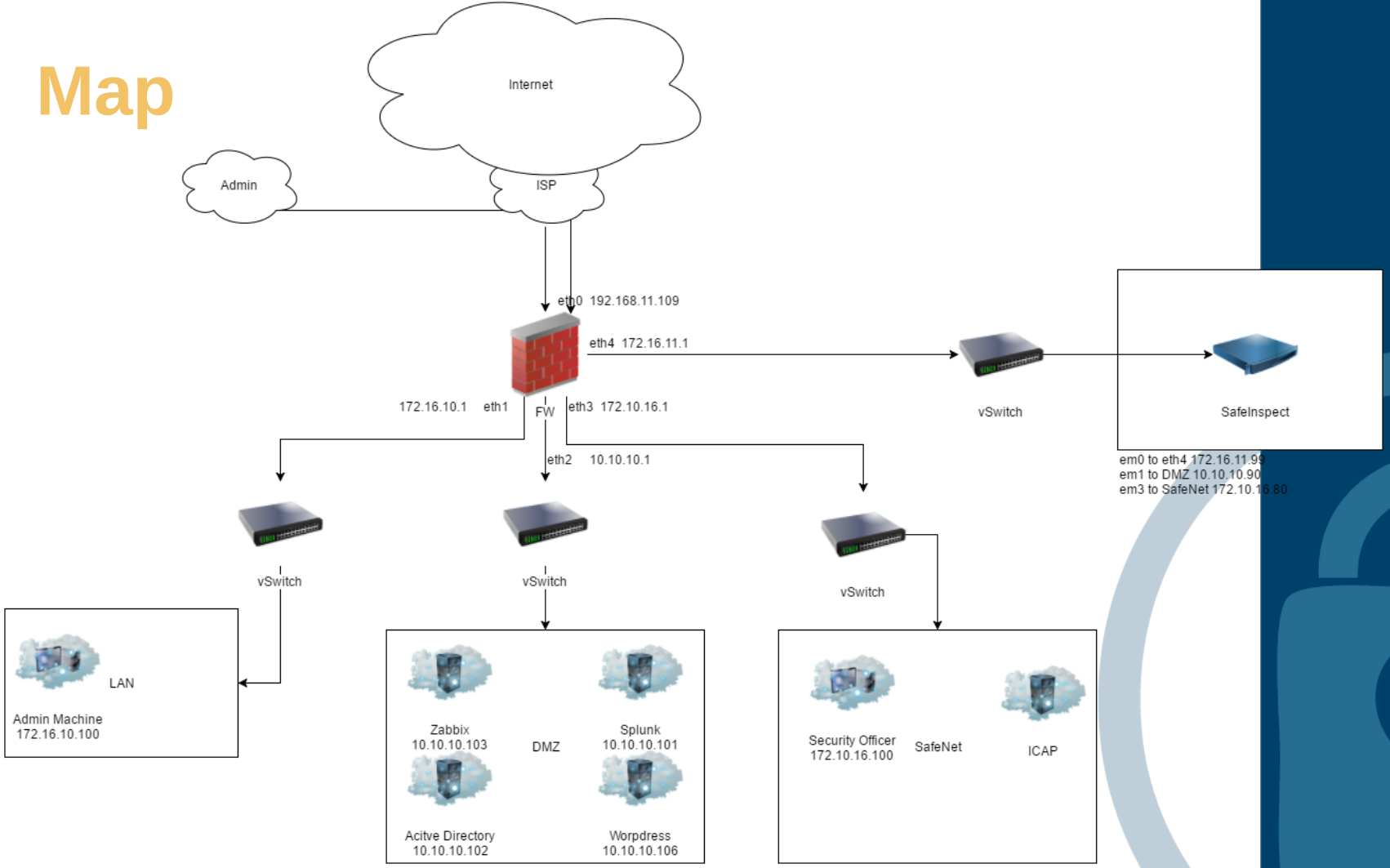
- 4 Гб ОЗУ
- 50 Гб диск

Производительность Коллектора:

- 6000 SSH подключений
- 600 RDP

(1 Менеджер ~ 12 Коллекторов)

Map


Internet
Admin
ISP
eth0 192.168.11.109
eth4 172.16.11.1
172.16.10.1 eth1
FW
eth3 172.16.16.1
eth2 10.10.10.1
vSwitch
vSwitch
SafeInspect
em0 to eth4 172.16.11.99
em1 to DMZ 10.10.10.90
em3 to SafeNet 172.10.16.80
vSwitch
vSwitch
vSwitch
LAN
Admin Machine
172.16.10.100
Zabbix
10.10.10.103
DMZ
Splunk
10.10.10.101
Acitve Directory
10.10.10.102
Worpdress
10.10.10.106
Security Officer
172.16.16.100
SafeNet
ICAP

Cases

- Brute Force Attack
- Time Bomb
- Shell Upload

Brute Force Attack Demo

Video in

Не бывает слабых паролей?

3.1.3. Default SSH password: root password "root" (ssh-default-account-root-password-root)

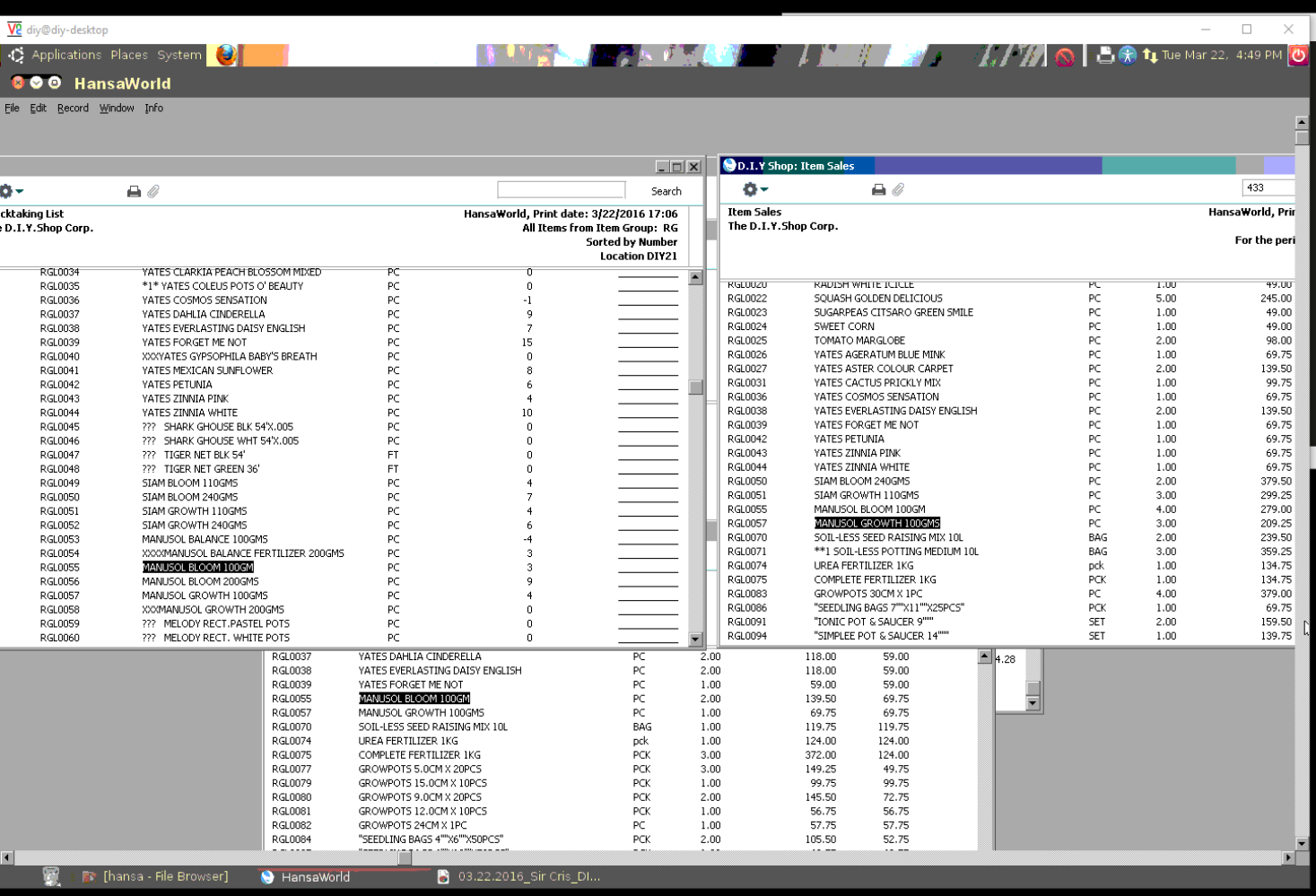
Description:

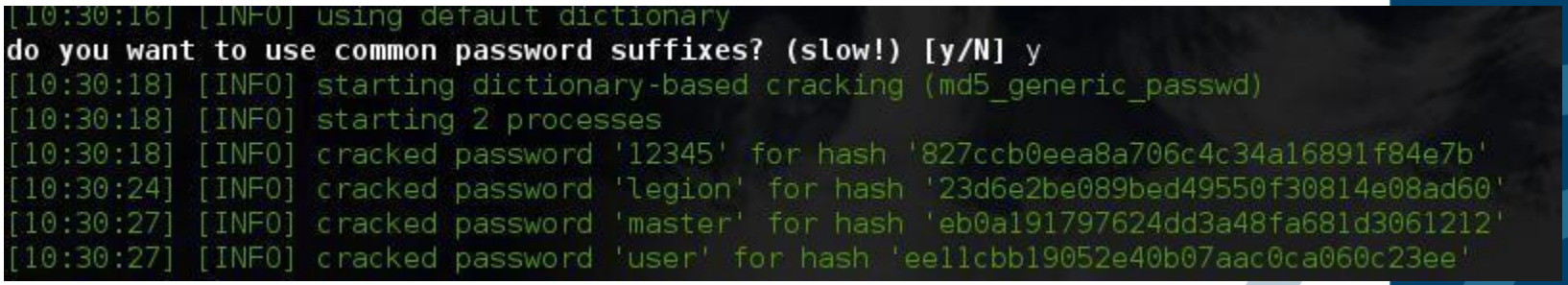
The root account uses a password of "root". This would allow anyone to log into the machine via SSH and take complete control.

Affected Nodes:

Affected Nodes:	Additional Information:
[redacted]:22	Running SSH serviceSuccessfully authenticated to the SSH service with credentials: uid[root] pw[root] realm[]

Affected Nodes:	Additional Information:
[redacted]:22	Running SSH serviceSuccessfully authenticated to the SSH service with credentials: uid[root] pw[root] realm[]
[redacted]:22	Running SSH serviceSuccessfully authenticated to the SSH service with credentials: uid[root] pw[root] realm[]
[redacted]:22	Running SSH serviceSuccessfully authenticated to the SSH service with credentials: uid[root] pw[root] realm[]
[redacted]:22	Running SSH serviceSuccessfully authenticated to the SSH service with credentials: uid[root] pw[root] realm[]


diy@diy-desktop
Applications Places System
Tue Mar 22, 4:49 PM
HansaWorld
File Edit Record Window Info
Search
cktaking List
e D.I.Y.Shop Corp.
HansaWorld, Print date: 3/22/2016 17:06
All Items from Item Group: RG
Sorted by Number
Location DIY21
RGL0034 YATES CLARKIA PEACH BLOSSOM MIXED PC 0
RGL0035 *1* YATES COLEUS POTS O' BEAUTY PC 0
RGL0036 YATES COSMOS SENSATION PC -1
RGL0037 YATES DAHLIA CINDERELLA PC 9
RGL0038 YATES EVERLASTING DAISY ENGLISH PC 7
RGL0039 YATES FORGET ME NOT PC 15
RGL0040 XXXYATES GYPSOPHILA BABY'S BREATH PC 0
RGL0041 YATES MEXICAN SUNFLOWER PC 8
RGL0042 YATES PETUNIA PC 6
RGL0043 YATES ZINNIA PINK PC 4
RGL0044 YATES ZINNIA WHITE PC 10
RGL0045 ??? SHARK GHOUSE BLK 54'X.005 PC 0
RGL0046 ??? SHARK GHOUSE WHT 54'X.005 PC 0
RGL0047 ??? TIGER NET BLK 54' FT 0
RGL0048 ??? TIGER NET GREEN 36' FT 0
RGL0049 SIAM BLOOM 110GMS PC 4
RGL0050 SIAM BLOOM 240GMS PC 7
RGL0051 SIAM GROWTH 110GMS PC 4
RGL0052 SIAM GROWTH 240GMS PC 6
RGL0053 MANUSOL BALANCE 100GMS PC -4
RGL0054 XXXXMANUSOL BALANCE FERTILIZER 200GMS PC 3
RGL0055 MANUSOL BLOOM 100GM PC 3
RGL0056 MANUSOL BLOOM 200GMS PC 9
RGL0057 MANUSOL GROWTH 100GMS PC 4
RGL0058 XXXMANUSOL GROWTH 200GMS PC 0
RGL0059 ??? MELODY RECT.PASTEL POTS PC 0
RGL0060 ??? MELODY RECT. WHITE POTS PC 0
D.I.Y Shop: Item Sales
433
Item Sales
The D.I.Y.Shop Corp.
HansaWorld, Pri
For the peri
RGL0020 RADISH WHITE ICICLE PC 1.00 49.00
RGL0022 SQUASH GOLDEN DELICIOUS PC 5.00 245.00
RGL0023 SUGARPEAS CITSARO GREEN SMILE PC 1.00 49.00
RGL0024 SWEET CORN PC 1.00 49.00
RGL0025 TOMATO MARGLOBE PC 2.00 98.00
RGL0026 YATES AGERATUM BLUE MINK PC 1.00 69.75
RGL0027 YATES ASTER COLOUR CARPET PC 2.00 139.50
RGL0031 YATES CACTUS PRICKLY MIX PC 1.00 99.75
RGL0036 YATES COSMOS SENSATION PC 1.00 69.75
RGL0038 YATES EVERLASTING DAISY ENGLISH PC 2.00 139.50
RGL0039 YATES FORGET ME NOT PC 1.00 69.75
RGL0042 YATES PETUNIA PC 1.00 69.75
RGL0043 YATES ZINNIA PINK PC 1.00 69.75
RGL0044 YATES ZINNIA WHITE PC 1.00 69.75
RGL0050 SIAM BLOOM 240GMS PC 2.00 379.50
RGL0051 SIAM GROWTH 110GMS PC 3.00 299.25
RGL0055 MANUSOL BLOOM 100GM PC 4.00 279.00
RGL0057 MANUSOL GROWTH 100GMS PC 3.00 209.25
RGL0070 SOIL-LESS SEED RAISING MIX 10L BAG 2.00 239.50
RGL0071 **1 SOIL-LESS POTTING MEDIUM 10L BAG 3.00 359.25
RGL0074 UREA FERTILIZER 1KG pck 1.00 134.75
RGL0075 COMPLETE FERTILIZER 1KG PCK 1.00 134.75
RGL0083 GROWPOTS 30CM X 1PC PC 4.00 379.00
RGL0086 "SEEDLING BAGS 7""X11""X25PCS" PCK 1.00 69.75
RGL0091 "IONIC POT & SAUCER 9""" SET 2.00 159.50
RGL0094 "SIMPLEE POT & SAUCER 14""" SET 1.00 139.75
RGL0037 YATES DAHLIA CINDERELLA PC 2.00 118.00 59.00
RGL0038 YATES EVERLASTING DAISY ENGLISH PC 2.00 118.00 59.00
RGL0039 YATES FORGET ME NOT PC 1.00 59.00 59.00
RGL0055 MANUSOL BLOOM 100GM PC 2.00 139.50 69.75
RGL0057 MANUSOL GROWTH 100GMS PC 1.00 69.75 69.75
RGL0070 SOIL-LESS SEED RAISING MIX 10L BAG 1.00 119.75 119.75
RGL0074 UREA FERTILIZER 1KG pck 1.00 124.00 124.00
RGL0075 COMPLETE FERTILIZER 1KG PCK 3.00 372.00 124.00
RGL0077 GROWPOTS 5.0CM X 20PCS PCK 3.00 149.25 49.75
RGL0079 GROWPOTS 15.0CM X 10PCS PCK 1.00 99.75 99.75
RGL0080 GROWPOTS 9.0CM X 20PCS PCK 2.00 145.50 72.75
RGL0081 GROWPOTS 12.0CM X 10PCS PCK 1.00 56.75 56.75
RGL0082 GROWPOTS 24CM X 1PC PC 1.00 57.75 57.75
RGL0084 "SEEDLING BAGS 4""X6""X50PCS" PCK 2.00 105.50 52.75
4.28
[hansa - File Browser]
HansaWorld
03.22.2016_Sir Cris_DI...
Search


[10:30:16] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[10:30:18] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[10:30:18] [INFO] starting 2 processes
[10:30:18] [INFO] cracked password '12345' for hash '827ccb0eea8a706c4c34a16891f84e7b'
[10:30:24] [INFO] cracked password 'legion' for hash '23d6e2be089bed49550f30814e08ad60'
[10:30:27] [INFO] cracked password 'master' for hash 'eb0a191797624dd3a48fa681d3061212'
[10:30:27] [INFO] cracked password 'user' for hash 'ee11cbb19052e40b07aac0ca060c23ee'

Database: [redacted]
Table: adm_admin
[6 entries]

a_id	a_name	a_pass	a_mail	a_skin	a_lang	a_group	a_login	a_status
7	[redacted]	cb2aa430617f812bce817f5f6504b324	[redacted]	classic	ru_RU	0	[redacted]	1
12	[redacted]	17657e1686c178352283dc3b8139d2aa	[redacted]	classic	ru_RU	0	[redacted]	1
21	[redacted]	7ea426d1b1e5fc00cfbd47be224ea371	[redacted]	classic	en_EN	0	[redacted]	1
20	[redacted]	1a83510dcaa69d880c7925f47a07c625	[redacted]	classic	ru_RU	0	[redacted]	1
22	[redacted]	ef2b92f9275664ccfe26ee0e232e5a4c	[redacted]	classic	ru_RU	0	[redacted]	1
23	[redacted]	81bad0b55c951d99ad627b62a9225e65	[redacted]	classic	ru_RU	0	[redacted]	1

super#
nbveh!

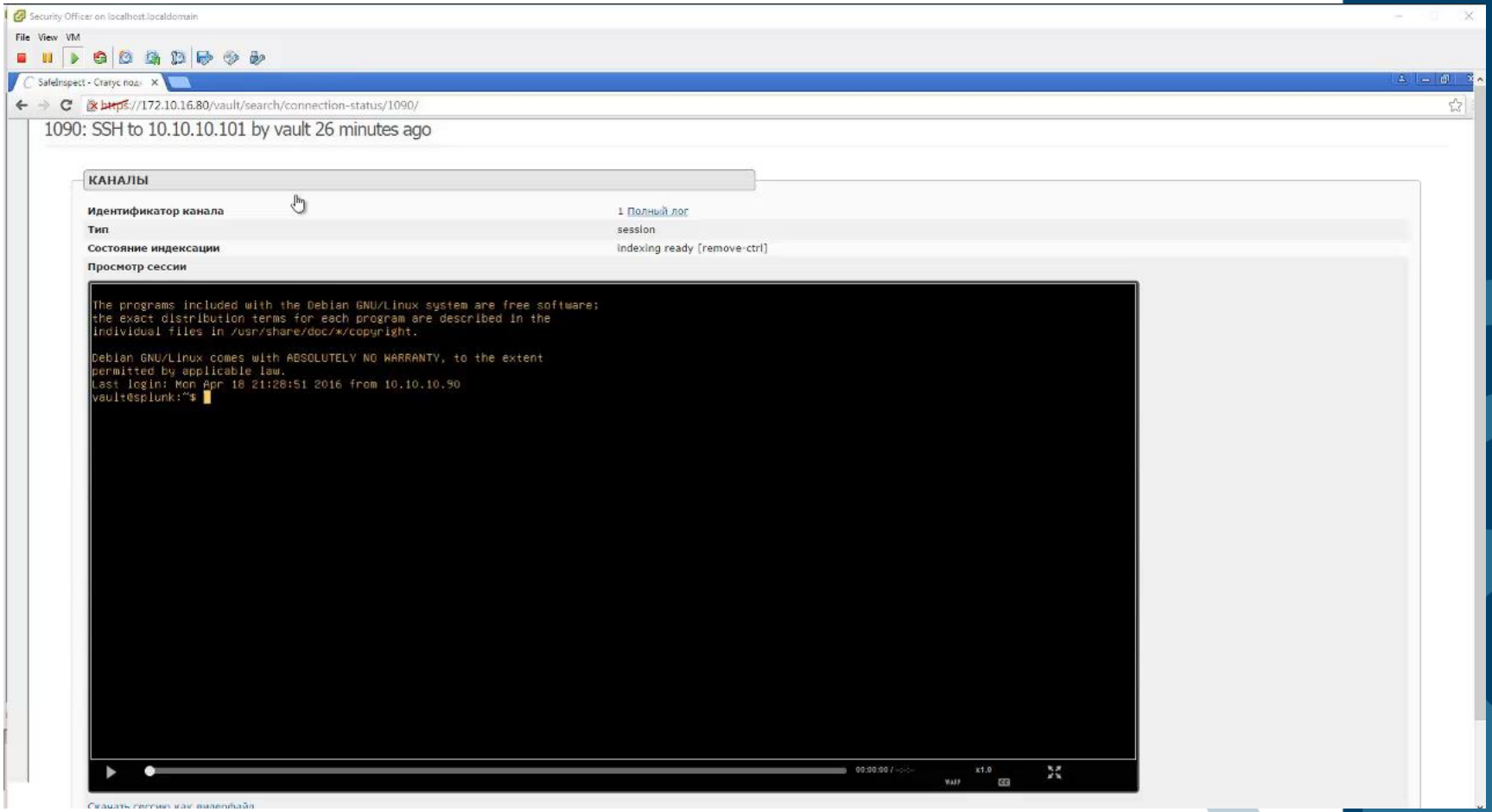
Database:
Table: adm_admin
[9 entries]

a_pass
122b054f79a722020e2b0a13a4782858 (2222222223)
23d6e2be089bed49550f30814e08ad60 (legion)
827ccb0eea8a706c4c34a16891f84e7b (12345)
827ccb0eea8a706c4c34a16891f84e7b (12345)
827ccb0eea8a706c4c34a16891f84e7b (12345)
891db9dd21362300aa56c99e199f8bb3
eb0a191797624dd3a48fa681d3061212 (master)
ee11cbb19052e40b07aac0ca060c23ee (user)
f746d505abada608d5981a80747c3d07

Time Bomb Attack Demo

Screencast_04-18-2016_09_35_15 PM.webm.webm

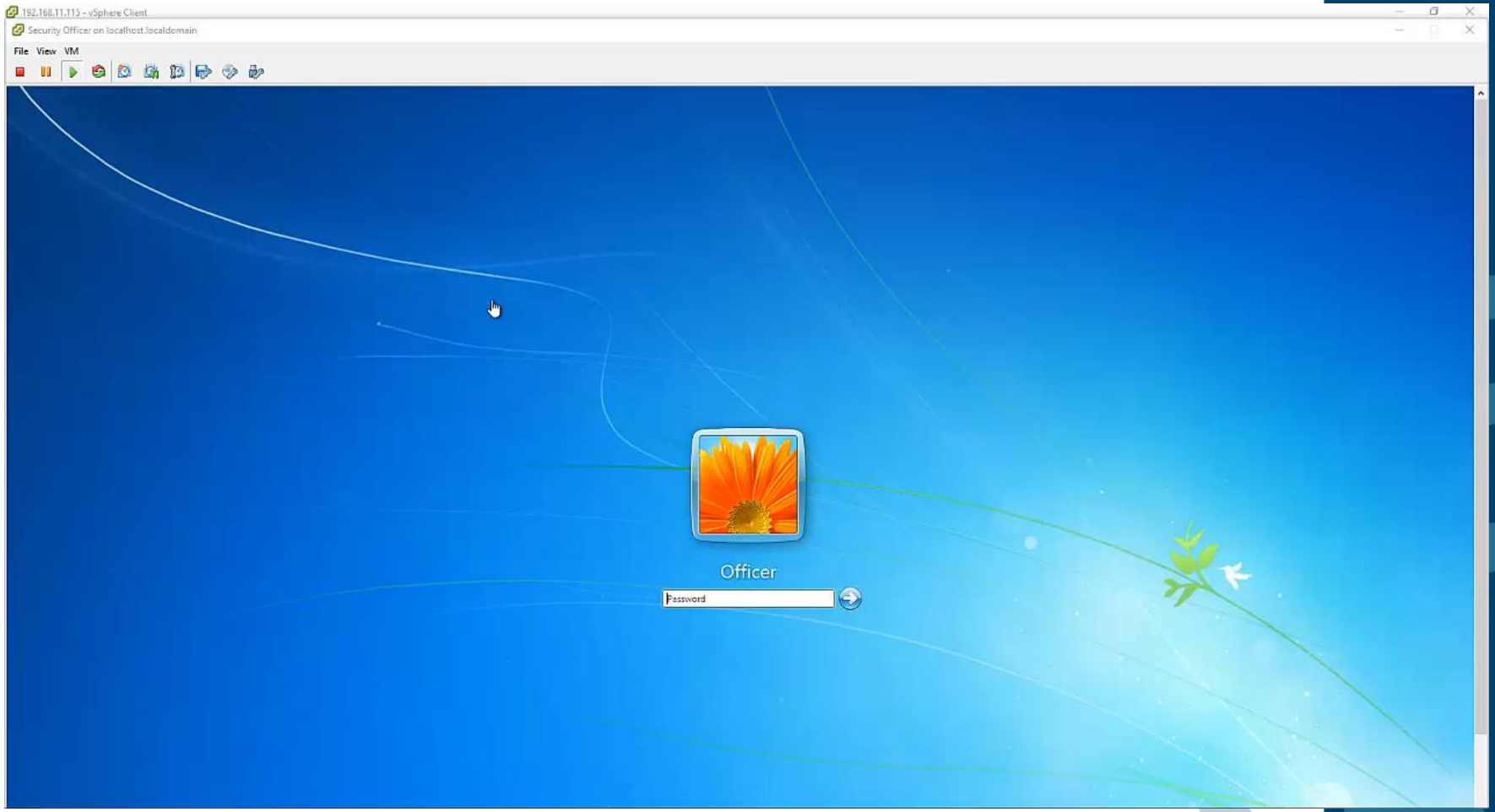
Time Bomb Attack



Shell Upload

Screencast_04-18-2016_09_35_15 PM.webm.webm

Shell Upload



Время для Ваших вопросов ☺

Спасибо за внимание!

Контакты:
ООО «Новые технологии безопасности»
Москва, ул. Трубная, 12
Телефон/Факс: +7 (495) 787 99 36
www.newinfosec.ru