

Мобильный офис глазами пентестера

Дмитрий Евтеев (Positive Technologies)



POSITIVE TECHNOLOGIES

Предисловие

- **Бизнес требует доступности всех ИТ-сервисов из любой точки земного шара и с любых мобильных устройств...**



- **Чем это может обернуться?**



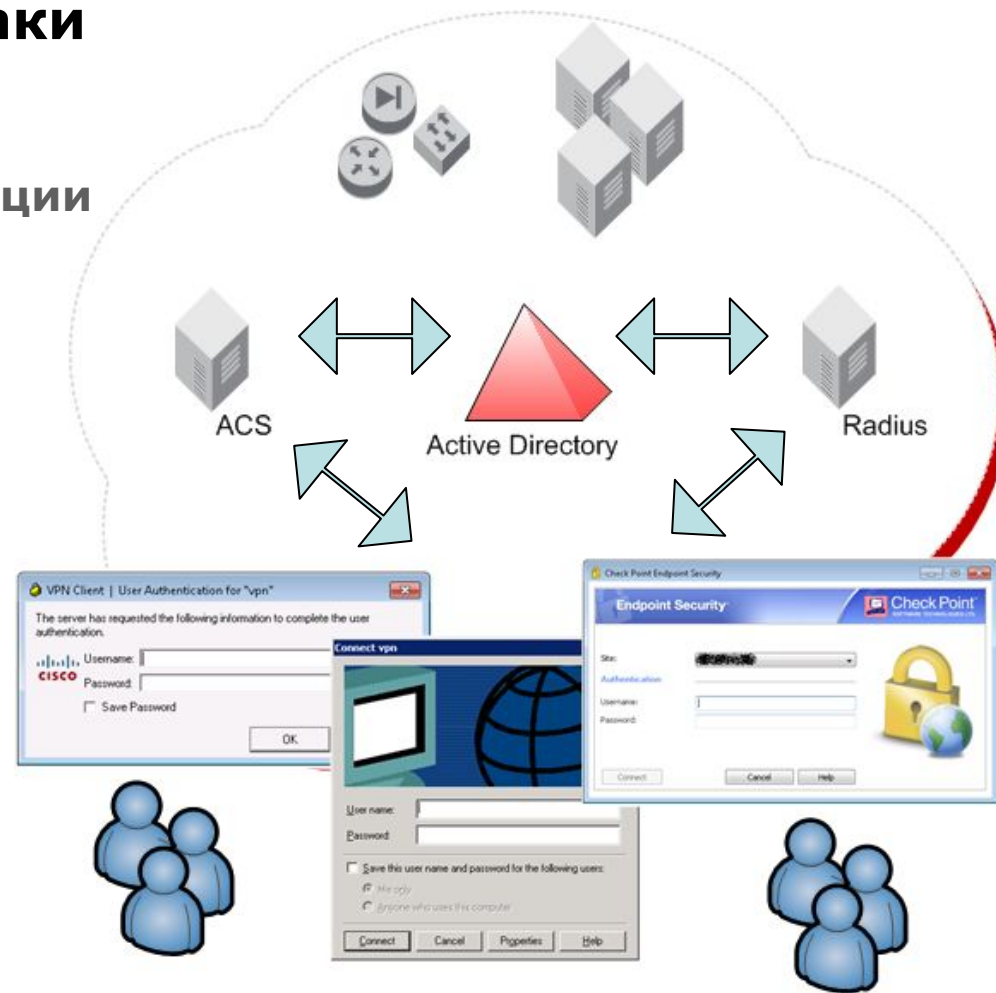
Основные точки входа в корпоративные сети

- **веб-приложения**
- **интерфейсы удаленного администрирования**
- **удаленный доступ к сети**
 - VPN-шлюзы
 - Доставка приложений через веб-сервисы
- **рабочие станции пользователей**
- **беспроводные сети**
- **сервисы инфраструктуры (базы данных, сторонние приложения и т.п.)**



Стандартная схема построения корпоративной ИС

- **Типовые сценарии атаки**
 - На Active Directory
 - На сервера аутентификации
 - На оборудование
 - На каналы связи
 - На VPN-шлюзы
 - На пользователя



Как действует атакующий

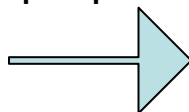
- **Атакующий идет по пути наименьшего сопротивления!**



1. Список идентификаторов



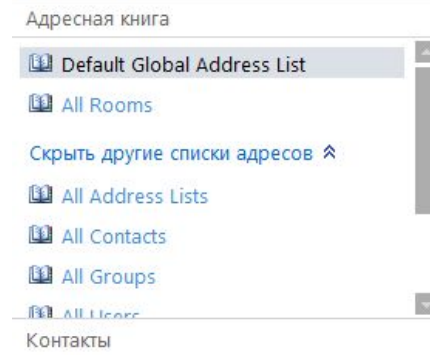
2. Перебор



3. Верификация доступа;
перебор действующих идентификаторов



3. Список действующих (!) идентификаторов



Проблема парольной защиты

- **Более половины пользователей в Российских компаниях используют цифровые пароли**
<http://www.ptsecurity.ru/download/PT-Metrics-Passwords-2009.pdf>
- **Политика сложности используемых паролей в сетях Microsoft имеет известные недостатки**
- **Чем больше сотрудников в компании, тем выше вероятность успешной атаки**
- **За последние три года (!) в ходе проведения тестирований на проникновение не было ни одного случая, когда не удавалось получить список всех идентификаторов Active Directory с использованием указанной атаки**



Агрессивный режим IPSEC

- Сортировка ▾ Узел ▾ Журнал
- 500 / udp - Internet Key Exchange
 - Подобран ключ защищенного режима
 - Доступен агрессивный режим**
 - Доступ к VPN
 - 4500 / udp - NAT-traversal
 - Подобран ключ защищенного режима
 - Доступен агрессивный режим
 - Доступ к VPN



Уязвимость

Доступен агрессивный режим

ID: 8139

Описание

Включена поддержка агрессивного режима с парольной защитой. Это

Responder KE :

054dd58b4a6b936722195415c115be49f820714a899c1b0d80dffcf917060;

Initiator KE :



Серьезная уязвимость

Подобран ключ защищенного режима

ID: 8145

Описание

Пароль : password123

CVSS

Базовая оценка: **9** (AV:N/AC:M/Au:N/C:C/I:C/A:P)

AV:N	данная уязвимость может эксплуатироваться удаленно
AC:M	для эксплуатации уязвимости нужна дополнительная информация или нестандартная конфигурация уязвимого ПО
Au:N	для эксплуатации уязвимости проходить аутентификацию не требуется
C:C	эксплуатация уязвимости влечет полное разглашение конфиденциальных данных
I:C	эксплуатация уязвимости влечет полное нарушение целостности системы
A:P	эксплуатация уязвимости ведет к сбоям в доступности системы или к уменьшению производительности



Основной режим IPSEC

- **Pre-shared key и GroupName могут быть восстановлены путем перебора**
- **Могут быть найдены в свободном корпоративном доступе**
 - Подробные инструкции по настройке
 - Сохраненные конфигурации
- **Могут быть получены с использованием других сценариев атак**



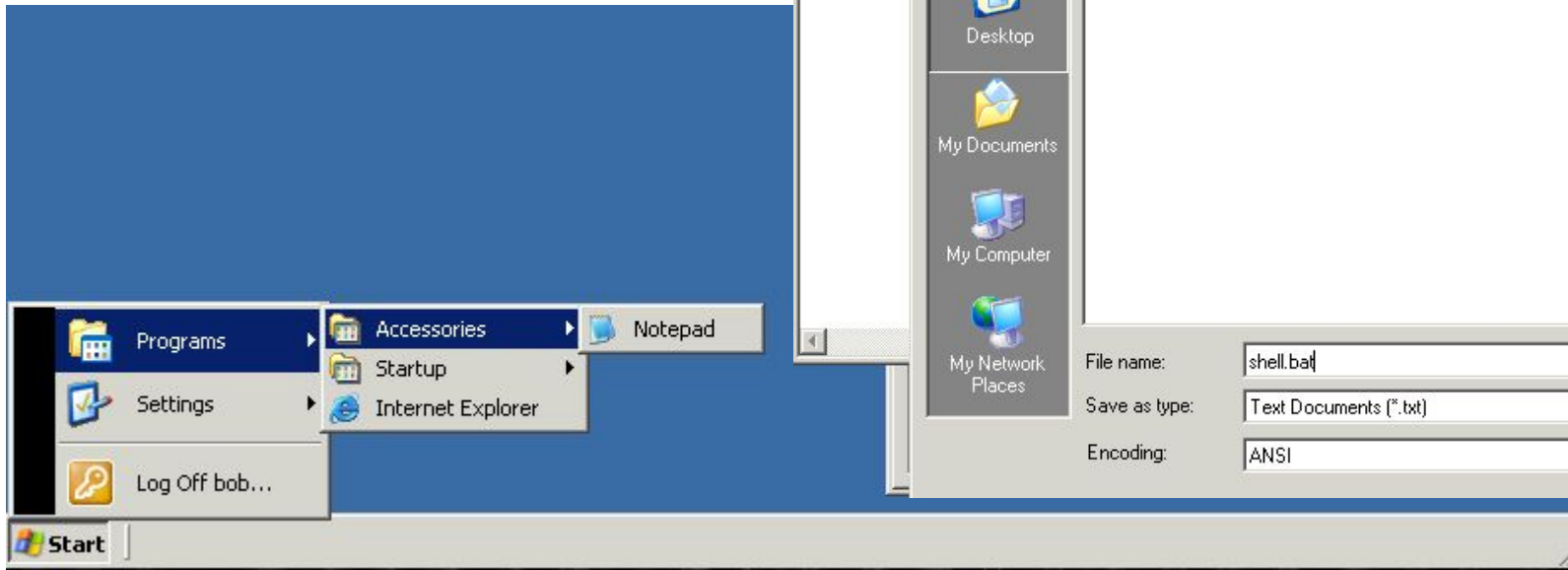
Чем опасен удаленный доступ к сети

- **Классический удаленный доступ к сети (IPSEC/PPTP)**
 - Пользователь обладает административными привилегиями в своей системе
- **Доставка приложений через веб-сервисы (eq Citrix)**
 - Пользователь обладает локальным доступом к ОС
 - Пользователь может расширить свои знания о существовании всех опубликованных приложениях
 - Пользователь из одной точки может получить сетевой доступ к любым опубликованным приложениям (в случае отсутствия правильной фильтрации)



Citrix Jailbreak (1/2)

- Существует 100 и 1 способ!



Citrix Jailbreak (2/2)

iKAT For Linux
iKAT Portable
iKAT PhotoKAT

Automatic Exploitation
1Click PWN

Reconnaissance

Installed Applications
Local Browser Variables
Remote Server Variables
Global Flash Settings
File Reflection
Local Browser Variables
Invoke Anti-Virus

FileSystem Links

FileSystem Links (HREF)
FileSystem Links (iFrames)
FileSystem Links (Manual Entry)

Common Dialogs

Common Dialogs
Flash Common Dialogs

Application Handlers

URI Handlers
Plugable Protocol Handlers
File Type Handlers

Browser Plugins

Java Applets
iKAT ActiveX
iKAT .NET Tools
iKAT SilverLight Tools
JavaScript Console
Media Players
PDF Reader

iKAT V - Vengeance Edition

Released at Defcon 19 - Las Vegas.
"Cry havoc and let loose the dogs of war."

iKAT was designed to aid security consultants with the task of auditing the security of internet Kiosk terminals.

iKAT is designed to provide access to the underlying operating system of a Kiosk terminal by invoking native OS functionality.

This tool should be (and is) used by Kiosk vendors/developers/suppliers to test the security of their own Kiosk products.

Donate to iKAT!

The iKAT project is 100% donate-ware, everything is donated, from the hosting to the trusted CA code signing certificate. We always need help in the form of extra donations to continue the project, so if iKAT helped you compromise a Kiosk, or you simply love the concept and want to donate, please do..

Donations can be made by clicking [HERE](#), or on the "Donate Now" link in the nav.. Help keep iKAT available, free and well stocked with 0day.

	A	B	C	D	E
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					

```
C:\Program Files\Microsoft Office\
C:\Documents and Settings\akado\adminad
C:\Documents and Settings\
Windows IP Configuration

Host Name . . . . .
Primary Dns Suffix . . . . .
Node Type . . . . .
IP Routing Enabled. . . . .
WINS Proxy Enabled. . . . .
DNS Suffix Search List. . . . .

Ethernet adapter Local Area

Connection-specific DNS
Description . . . . .
Physical Address. . . . .
DHCP Enabled. . . . .
IP Address. . . . .
Subnet Mask . . . . .
Default Gateway . . . . .
DNS Servers . . . . .

C:\Documents and Settings\
```

<http://ikata.cked.net/windows/>



- **Удаленный доступ к корпоративной сети через легитимный канал очень привлекателен с позиций атакующего**
- **Основные недостатки при организации удаленного доступа к корпоративной сети**
 - Использование паролей, вместо цифровых сертификатов
 - Повсеместное использование нестойких паролей (!)
 - Отсутствие безопасной сегментации сети
 - Недостаточное разграничение сетевого доступа
 - Отсутствие мониторинга аномалий и начала атаки



**Спасибо за внимание!
Вопросы?**

devteev@ptsecurity.ru

<http://devteev.blogspot.com/>

