МОДЕЛЬ НАРУШИТЕЛЯ: КВАЛИФИЦИРОВАННЫЙ МОТИВИРОВАННЫЙ ВЗЛОМЩИК

Соколов Андрей
консультант
ЗАО «ДиалогНаука»
25 сентября 2013

ДиалогНаука

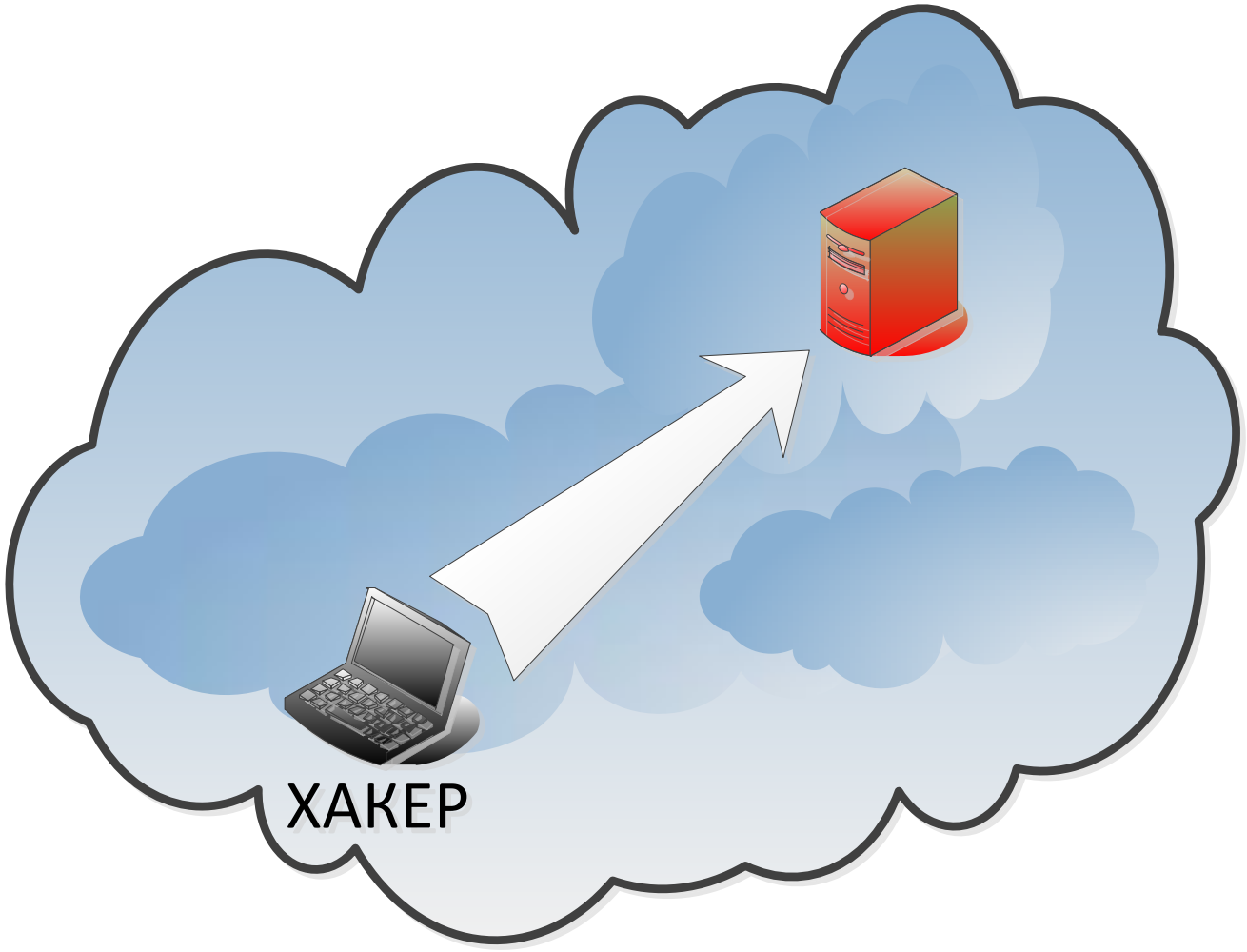
Тестирование на проникновение

(WikiPedia) Тестирование на проникновение – метод оценки безопасности компьютерных систем и сетей посредством моделирования атак потенциальных злоумышленников

(ДиалогНаука) Тестирование на проникновение – имитация действий реального злоумышленника по осуществлению целенаправленного проникновения к наиболее ценным информационным активам компании-Заказчика

Внешний нарушитель

Внутренний нарушитель



Внутренняя корпоративная сеть

Квалифицированный мотивированный взломщик

ЦЕННЫЕ ИНФОРМАЦИОННЫЕ АКТИВЫ

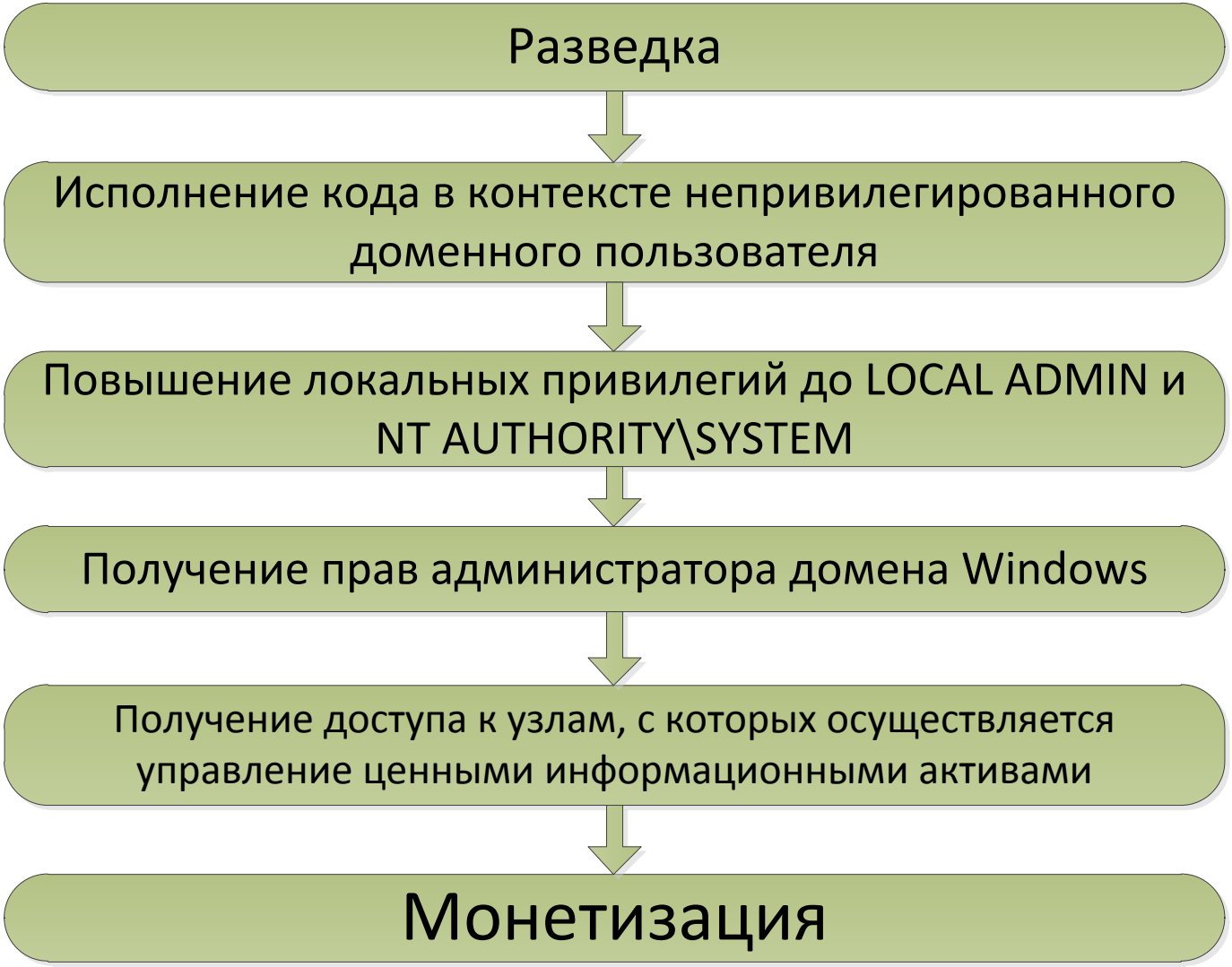
1. ЦЕЛЬ:

- **Причинение ущерба**: например, извлечение информации, за сохранность конфиденциальности которой компания несет существенную юридическую ответственность;
- **Извлечение прибыли**: например, получение несанкционированного доступа к какой-либо системе, участвующей в движении денежной массы.

2. СКРЫТНОСТЬ:

Хакер не может позволить себе быть обнаруженным

Путь хакера


Разведка
Исполнение кода в контексте непривилегированного доменного пользователя
Повышение локальных привилегий до LOCAL ADMIN и NT AUTHORITY\SYSTEM
Получение прав администратора домена Windows
Получение доступа к узлам, с которых осуществляется управление ценными информационными активами
Монетизация

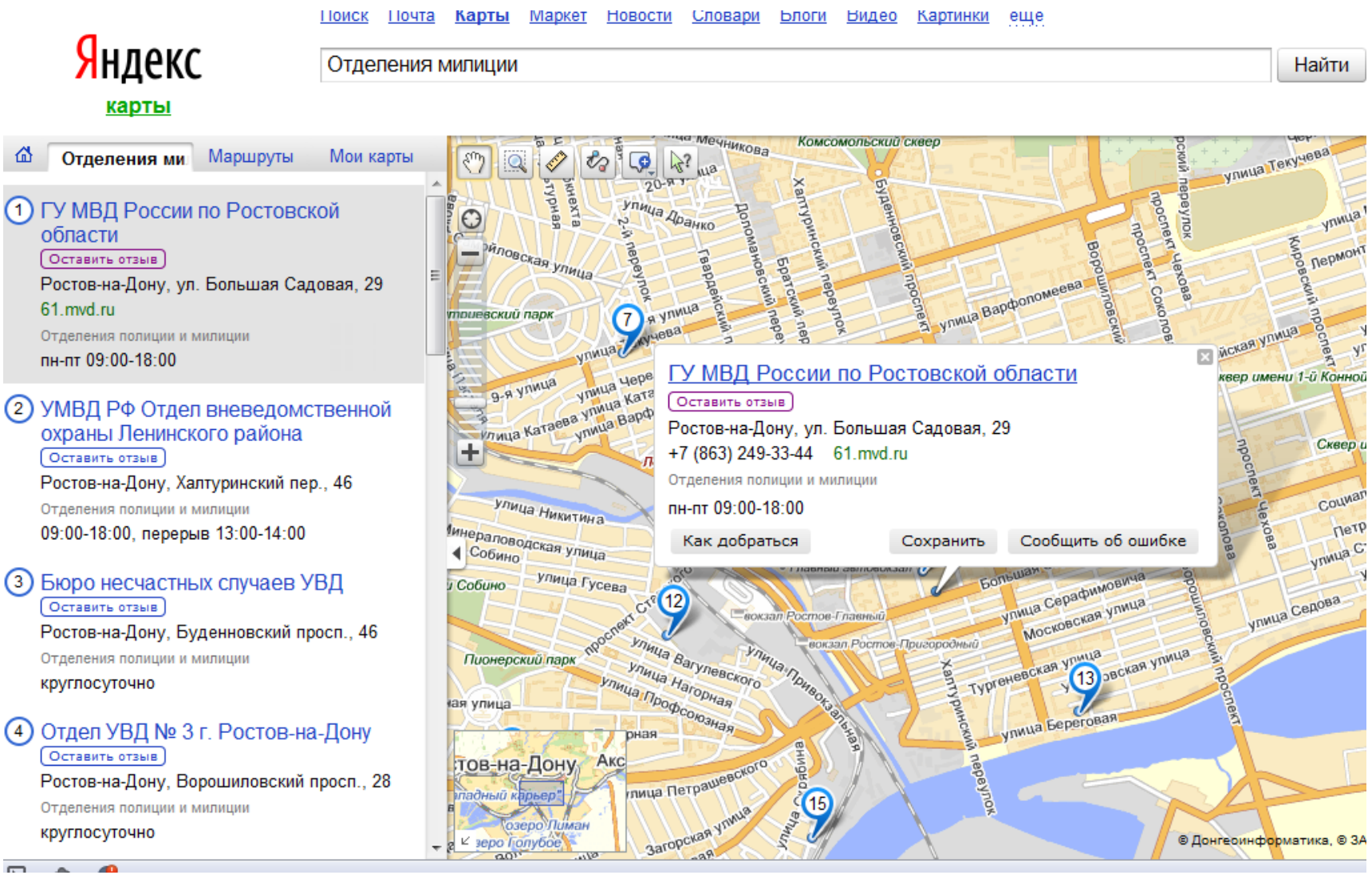
Система скрытого удаленного управления

DNS covert channel

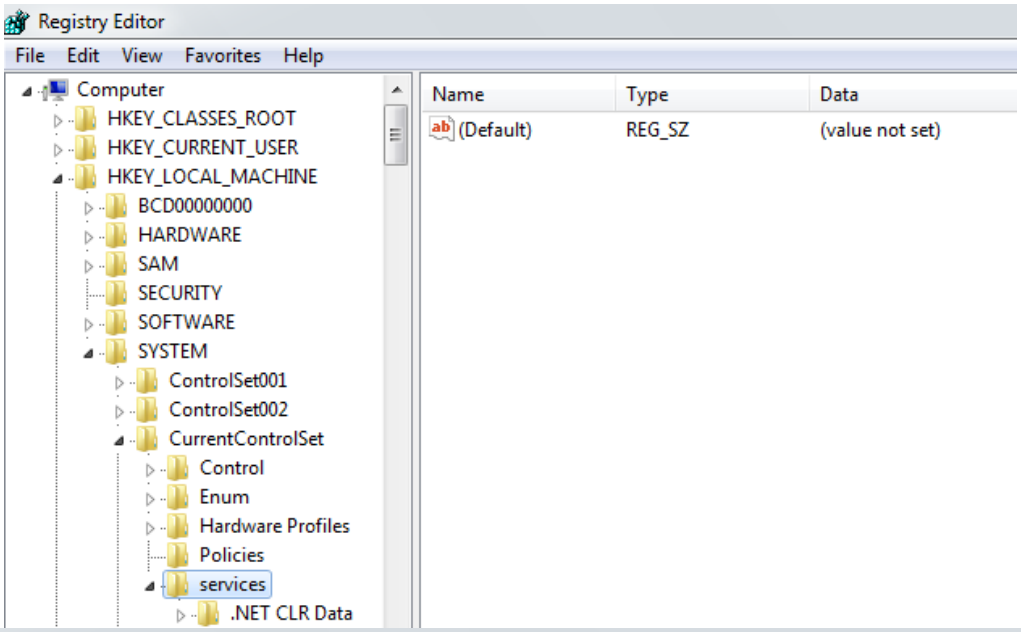
- A-запрос:
- aOp1sMQauNDFasdkn982sda.s91asAY81M5Qse31.asN6D943J2105F32OwWawe.z1a82sSdDDd19a7123.H196FHcd8iIlO9a.zone.com
- A-ответ:
- 142.32.211.57

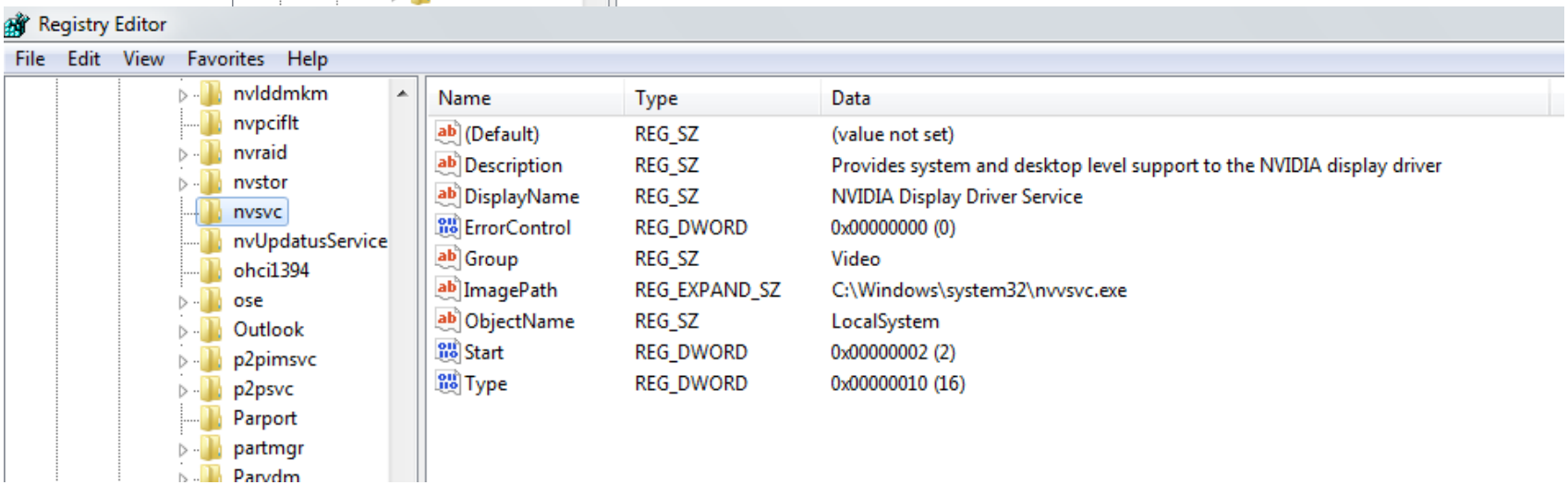
- TXT-запрос:
- aisodjiqowqd.zone.com
- TXT-ответ:
- *^% A*SDHHFkjhga791b2eda&*ASkjga73ujhB^2598NJKSDn09asd-109&#*(!@(*HAjgAOI38g6%1f9wrgge5t12edasd126SDOin3#221

Творческий подход



Эскалация локальных привилегий

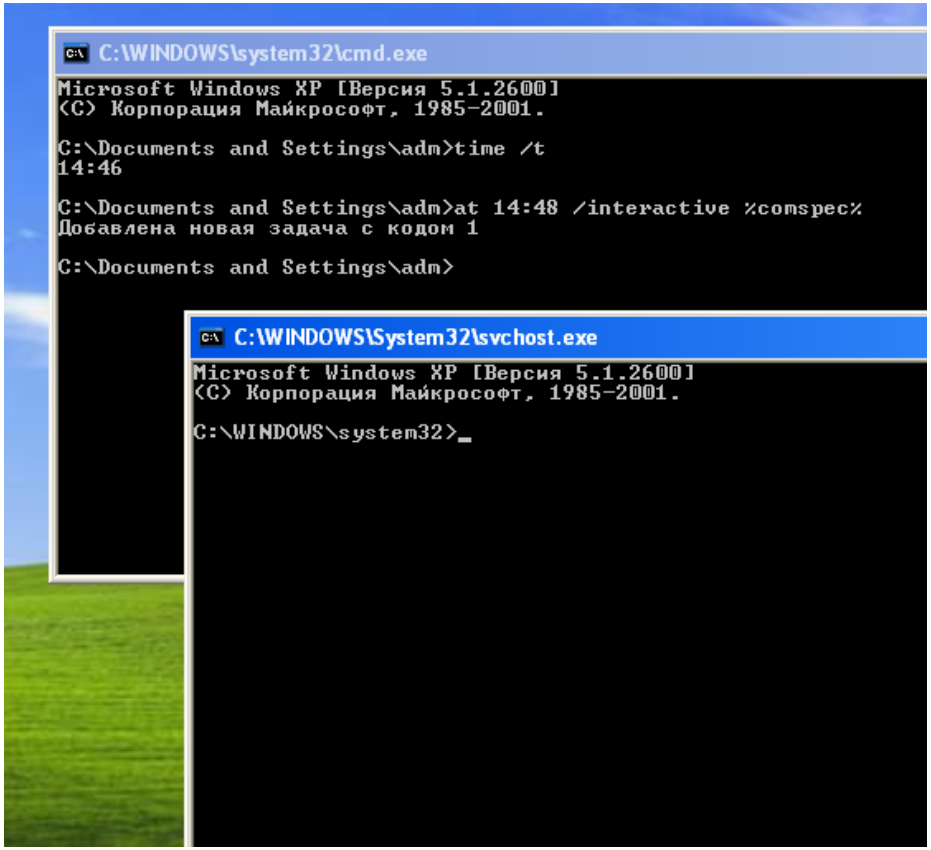




Эскалация локальных привилегий

```
cmd - Far 2.0.1807 x86
hese Windows services are started:

  Adobe Acrobat Update Service
  Application Information
  Base Filtering Engine
  Bluetooth Support Service
  CNG Key Isolation
  COM+ Event System
  Cryptographic Services
  DCOM Server Process Launcher
  Desktop Window Manager Session Manager
  DHCP Client
  Diagnostic Policy Service
  Diagnostic Service Host
  Distributed Link Tracking Client
  DNS Client
  Encrypting File System (EFS)
  Extensible Authentication Protocol
  Group Policy Client
  IKE and AuthIP IPsec Keying Modules
  IP Helper
  Multimedia Class Scheduler
  Network Connections
  Network List Service
  Network Location Awareness
  Network Store Interface Service
  NVIDIA Display Driver Service
  NVIDIA Stereoscopic 3D Driver Service
  NVIDIA Update Service Daemon
  Offline Files
  Plug and Play
  Power
  Print Spooler
  Program Compatibility Assistant Service
- More  -- _
```



Распределение локальных администраторов

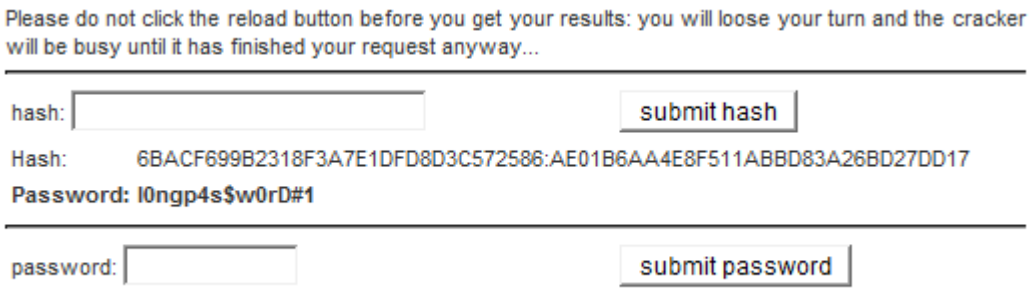
- VIP-пользователи, top-менеджмент: те, кто принимают законы, обычно не выполняют их сами;
- Системные администраторы, сотрудники IT-отделов: те, кто охраняют законы, обычно не подчиняются им;

- Разработчики ПО: подобного рода деятельность невозможна без прав локального администратора;
- Пользователи программного обеспечения, которое нуждается в правах локального администратора – особый бухгалтерский или банковский софт;
- Харизматические пользователи, получающие права локального администратора путём социального воздействия на группу системных администраторов.

Повышение привилегий в домене Windows

Administrator:500:74EDBB740DB08CA6D563857102316682:691FA30C46D1658E18DDC55FF8E5AE80:::

Пароль меньше 16 символов, расшифровываем за 400 миллисекунд на http://www.objectif-securite.ch/en/products.php



Administrator:500:aad3b435b51404eeaad3b435b51404ee:134b33244029b2ccfee08bb726111afe:::

Пароль более 16 символов или Windows 7. Варианты: john the ripper или Pass the Hash

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Пустой хэш, пользователь отключен

Социальная инженерия: сисадмины

Социальная инженерия: менеджеры

Вы ещё не знаете Паниковского!
Паниковский всех вас продаст,
купит, и снова продаст, но уже
дороже!

Социальная инженерия: боссы

Социальная инженерия: группа

```
c:\>telnet mx.domain.com 25

220 mx.domain.com for some domain.com
HELO arbitrary.hostname
250 mx.domain.com says HELO
MAIL FROM: <admin@domain.com>
250 MAIL FROM accepted
RCPT TO: <arbitrary.recipient@domain.com>
250 RCPT TO accepted
DATA
354 continue
Subject: some subject
<CR/LF>
.
<CR/LF>
250 message queued
221 mx.domain.com closing connection
```

Физический вектор проникновения

Физический вектор проникновения

Физический вектор проникновения

Наши контакты

117105, г. Москва, ул. Нагатинская, д. 1, стр.1

Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: sav@DialogNauka.ru