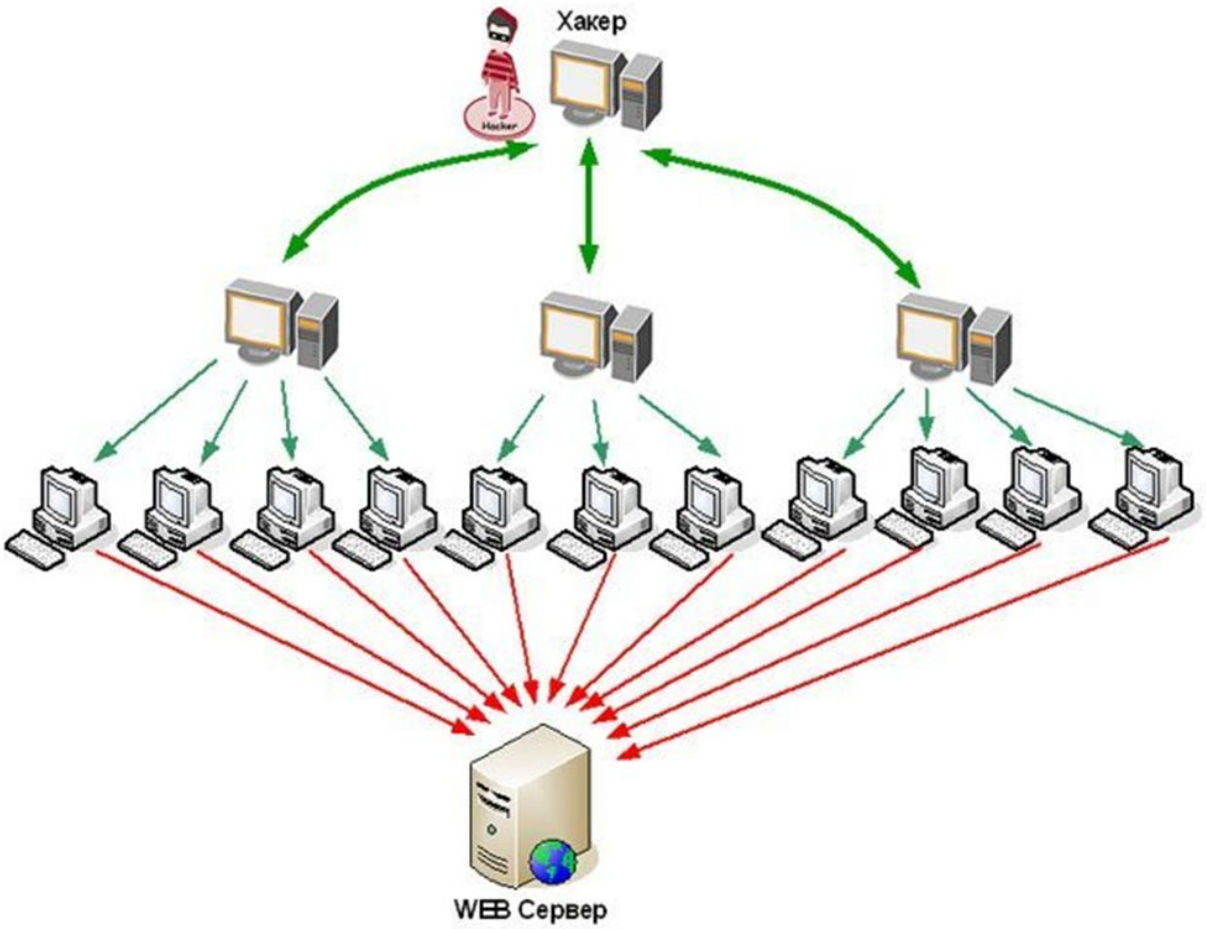
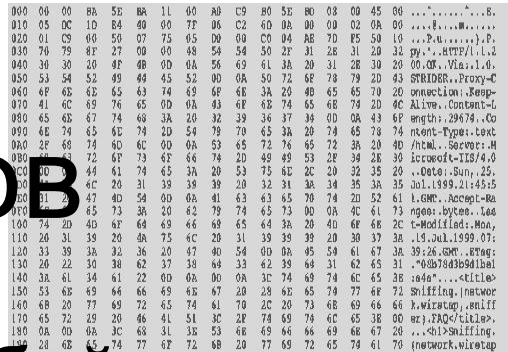
Распространенные атаки на персональный компьютер

Защита информационных ресурсов компьютерных систем и сетей

Классификация сетевых атак



Снифферы пакетов



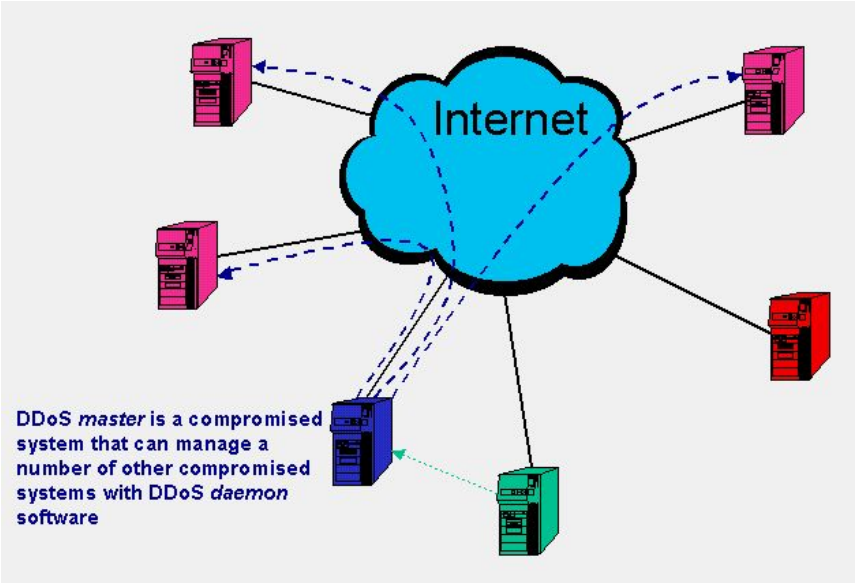
Сниффер пакетов представляет собой прикладную программу, которая использует сетевую карту, работающую в режиме promiscuous mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки). При этом сниффер перехватывает все сетевые пакеты, которые передаются через определенный домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика.

IP-спуфинг

IP-спуфинг происходит, когда хакер, находящийся внутри корпорации или вне ее выдает себя за санкционированного пользователя. Это можно сделать двумя способами. Во-первых, хакер может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример - атака DoS, которая начинается с чужого адреса, скрывающего истинную личность хакера.

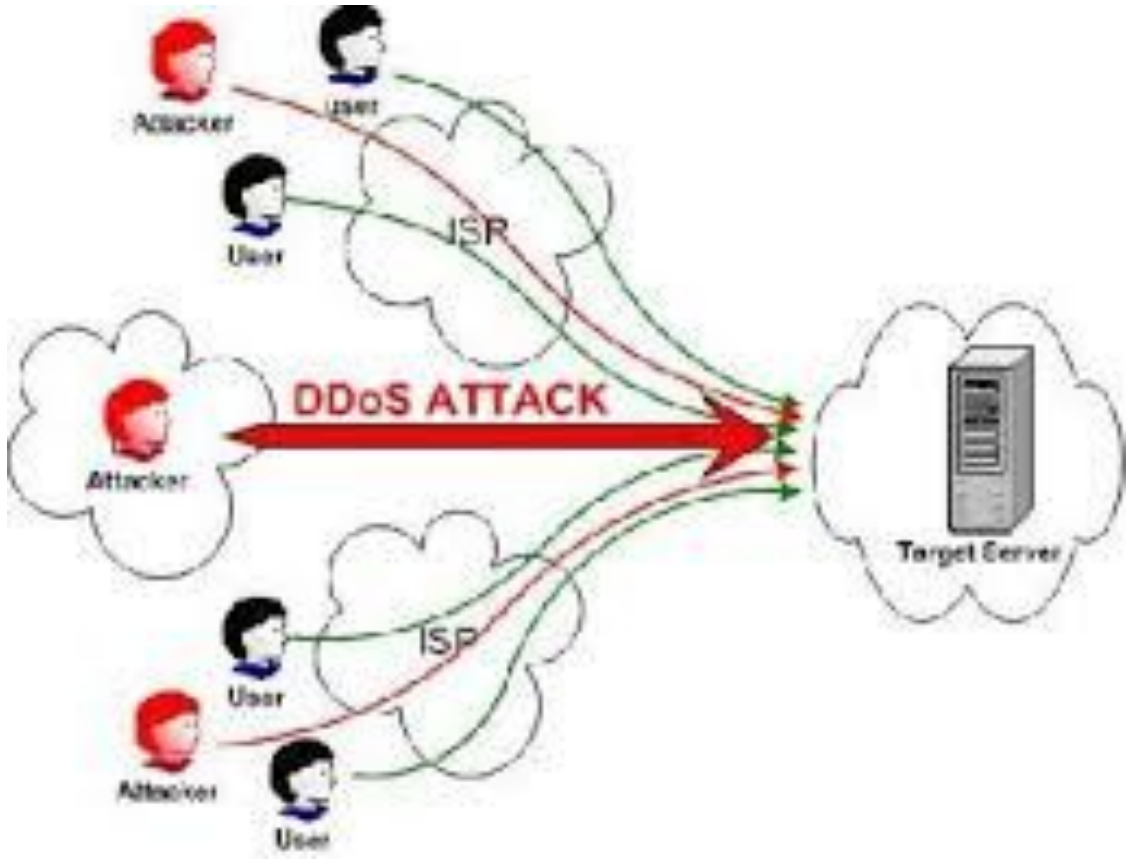
Отказ в обслуживании (Denial of Service - DoS)

DoS, без всякого сомнения, является наиболее известной формой хакерских атак. Кроме того, против атак такого типа труднее всего создать стопроцентную защиту



Краткий обзор известных атак на втором уровне OSI

- jam distribution
- marker slowing
- arp poisoning
- overflow (flood)



jam distribution

DoS атака в CSMA/CD сети (например ethernet). В случае, если сеть не имеет коммутаторов, результатом является выход из строя на время атаки всей сети, если же есть коммутаторы - отказ работы одного сегмента сети, в котором стоит атакующая станция (в пределах коллизионного домена). Кстати, важно понимать, что несмотря на то, что VLAN'ы призваны разделять броадкастные и коллизионные домены, к MAC-based VLAN'ам это не относится, поскольку они организуются поверх имеющихся коллизионных доменов.

marker slowing

DoS атака на сети, построенные на принципах логического кольца с передачей маркера. Результатом является, как минимум, снижение пропускной способности сети, за счет задержек передачи маркера в рамках определенных стандартами таймаутов. Возможно есть шанс добиться DoS.

arp poisoning

изменение таблицы соответствия MAC и IP-адресов на удаленном хосте путем посылки ему пакетов arp-reply с ложными данными о MAC-адресе, соответствующем интересующему IP-адресу. Эта атака очень близка к 2-му уровню OSI, однако ее скорее стоит позиционировать как находящуюся на стыке между 2-м и 3-м уровнями OSI.

overflow (flood)

использование потока блоков данных административно-информативных протоколов на максимально допускаемых носителем скоростях. К таким атакам относится в том числе cdp-flooding. Практическое обнаружение подобных атак затруднено необходимостью проводить массу тестирований на работу оборудования при нарушении спецификации, заданной стандартом. Например, как поведет себя коммутатор, если будет получать TCN/C-BPDU в количестве во много раз превышающем предусмотренную стандартом нагрузку?

Наиболее известные разновидности

- TCP SYN Flood
- Ping of Death
- Tribe Flood Network (TFN) и Tribe Flood Network 2000 (TFN2K)
- Trinco
- Stacheldracht
- Trinity

TCP SYN Flood

Заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в достаточно короткий срок.

Согласно процессу «трёхкратного рукопожатия» TCP, клиент посылает пакет с установленным флагом SYN (synchronize). В ответ на него сервер должен ответить комбинацией флагов SYN+ACK (acknowledges). После этого клиент должен ответить пакетом с флагом ACK, после чего соединение считается установленным.

Принцип атаки заключается в том, что злоумышленник, посылая SYN-запросы, переполняет на сервере (цели атаки) очередь на подключения. При этом он игнорирует SYN+ACK пакеты цели, не высылая ответные пакеты, либо подделывает заголовок пакета таким образом, что ответный SYN+ACK отправляется на несуществующий адрес. В очереди подключений появляются так называемые полуоткрытые соединения (англ. half-open connection), ожидающие подтверждения от клиента. По истечении определенного тайм-аута эти подключения отбрасываются. Задача злоумышленника заключается в том, чтобы поддерживать очередь заполненной таким образом, чтобы не допустить новых подключений. Из-за этого легитимные клиенты не могут установить связь, либо устанавливают её с существенными задержками.

Ping of Death

Компьютер-жертва получает особым образом подделанный эхо-запрос (ping), после которого он перестает отвечать на запросы вообще (DoS).

Обычный эхо-запрос имеет длину 64 байта (плюс 20 байт IP-заголовка). По стандарту RFC 791 IPv4 суммарный объем пакета не может превышать 65 535 байт (). Отправка же ICMP-пакета такого или большего размера может привести к переполнению сетевого стека компьютера и вызвать отказ от обслуживания. Такой пакет не может быть передан по сети целиком, однако для передачи его можно фрагментировать на несколько частей, число которых зависит от MTU физического канала.

При фрагментации каждая часть получает смещение фрагментации, которое представляет собой положение начала содержимого части относительно исходного пакета и занимает в заголовке IP-пакета 13 бит. Это позволяет получить максимальное смещение, равное 65 528 байт (), что означает, что фрагмент с максимальным смещением не должен превышать 7 бит (), иначе он превысит разрешённый размер IP-пакета, что может вызвать переполнение буфера жертвы, размер которого рассчитан на стандартный пакет, и аварийную остановку компьютера.

Данная уязвимость применима к любому транспортному протоколу, который поддерживает фрагментацию (TCP, UDP, IGMP, ICMP и др.).

Tribe Flood Network (TFN) и Tribe Flood

Является еще одной атакой отказа в обслуживании, в которой используются ICMP-сообщения, использует несколько компьютеров.

Локальные атаки

Обход пароля!

Восстановление пароля root (RHEL)

1. При загрузке нажать пробел, потом «E».
2. Выделить строчку kernel и, снова нажав «E», добавить в конец строки слово single.
3. Загрузиться и сменить пароль.

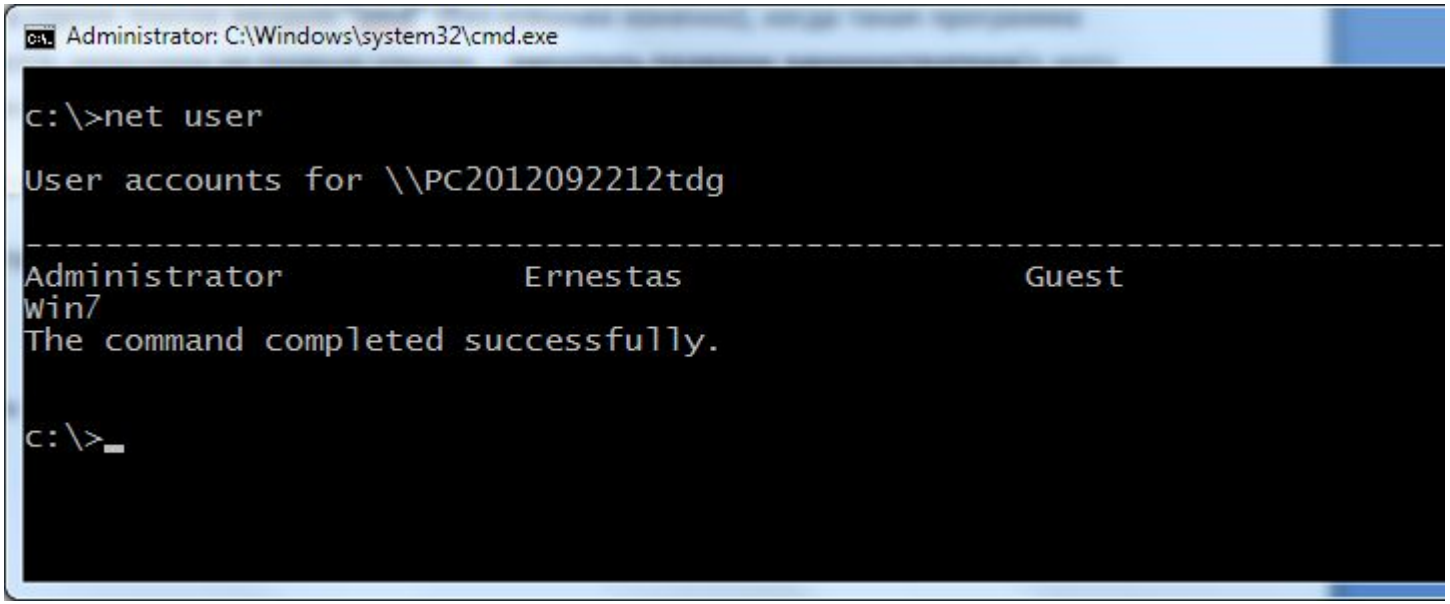
Восстановление пароля root (RHEL)

1. Предыдущие пункты 1 и 2 выполняем без изменений, но вместо single пишем init=/bin/bash, так указываем ядру, что вместо /sbin/init первой программой пользовательского режима будет оболочка.
2. Перемонтируем корневую ФС в режим rw:
3. # /sbin/mount -o remount,rw /
4. Задаем пароль командой /bin/passwd.
5. Жмем следующие комбинации клавиш: <Alt + SysRq + s>, <Alt + SysRq + u>, <Alt + SysRq + b> — аварийная синхронизация буферов ФС, перемонтирование ФС в режим ro и перезагрузка. Пароль изменен.

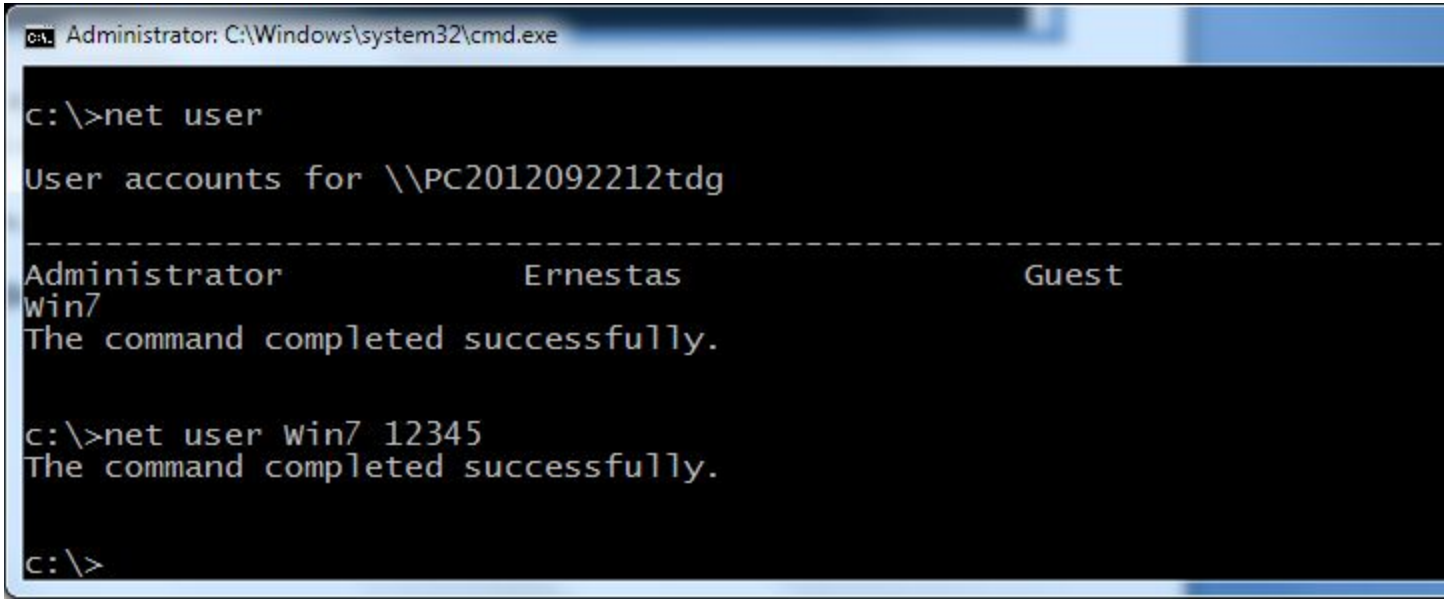
Изменения пароля в Windows

- Без специальных иснтрументов!

Часть1

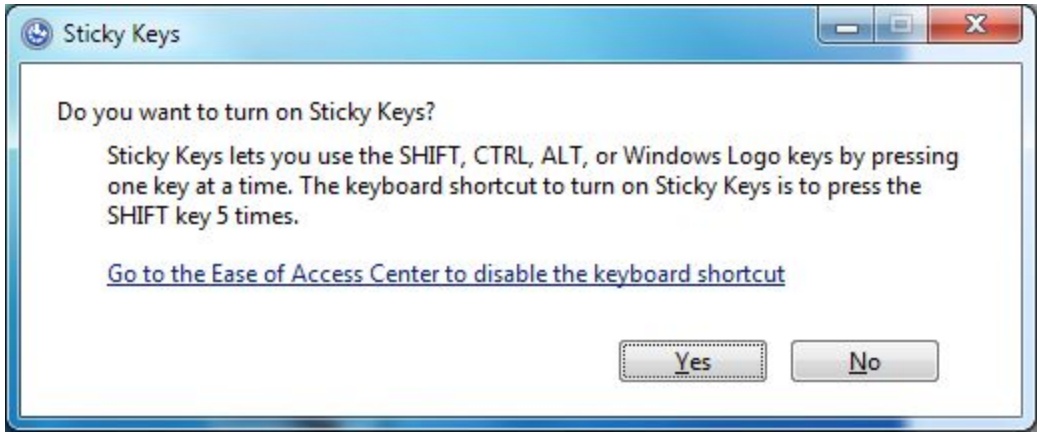

Administrator: C:\Windows\system32\cmd.exe
c:\>net user
User accounts for \\PC2012092212tdg
Administrator Ernestas Guest
Win7
The command completed successfully.
c:\>

Часть 1


Administrator: C:\Windows\system32\cmd.exe
c:\>net user
User accounts for \\PC2012092212tdg
Administrator Ernestas Guest
Win7
The command completed successfully.
c:\>net user Win7 12345
The command completed successfully.
c:\>

Часть 2

Часть 2


Sticky Keys
Do you want to turn on Sticky Keys?
Sticky Keys lets you use the SHIFT, CTRL, ALT, or Windows Logo keys by pressing one key at a time. The keyboard shortcut to turn on Sticky Keys is to press the SHIFT key 5 times.
Go to the Ease of Access Center to disable the keyboard shortcut
Yes
No

Часть 2

При пятикратном нажатии клавиши ”Shift” запускается файл ”sethc.exe” который находится в папке Windows\System32. Там же кстати находится и файл ”cmd.exe” – наша желанная коммандная срока.

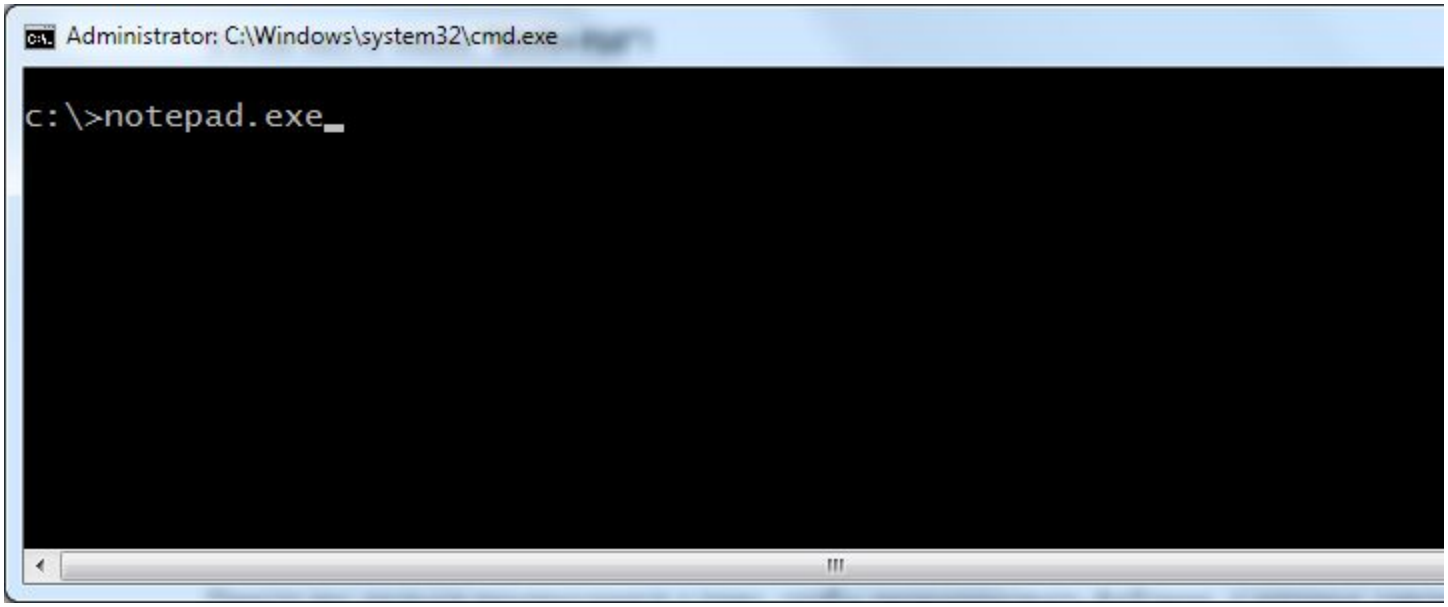
Часть 3


Install Windows
Windows 7
Language to install: English
Time and currency format: English (United States)
Keyboard or input method: US
Enter your language and other preferences and click "Next" to continue.
Copyright © 2009 Microsoft Corporation. All rights reserved.
Next

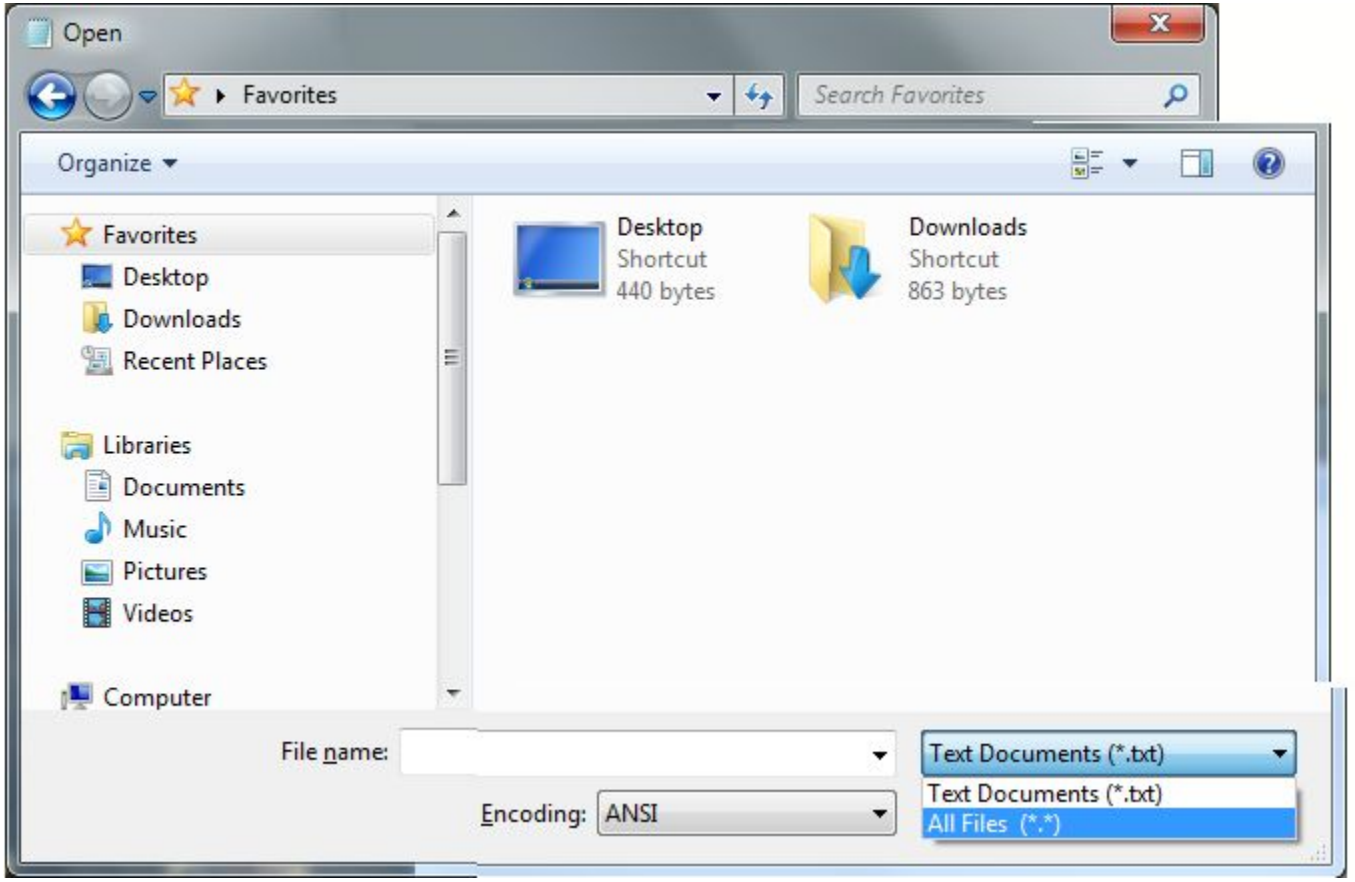
Часть 3

- В этом месте жмем “Shift+ F10”!

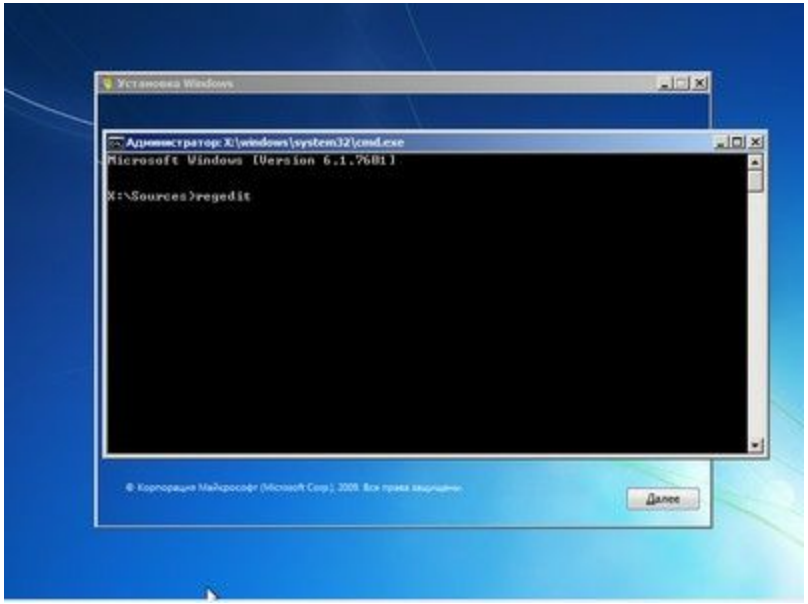
Часть 3



Часть 3

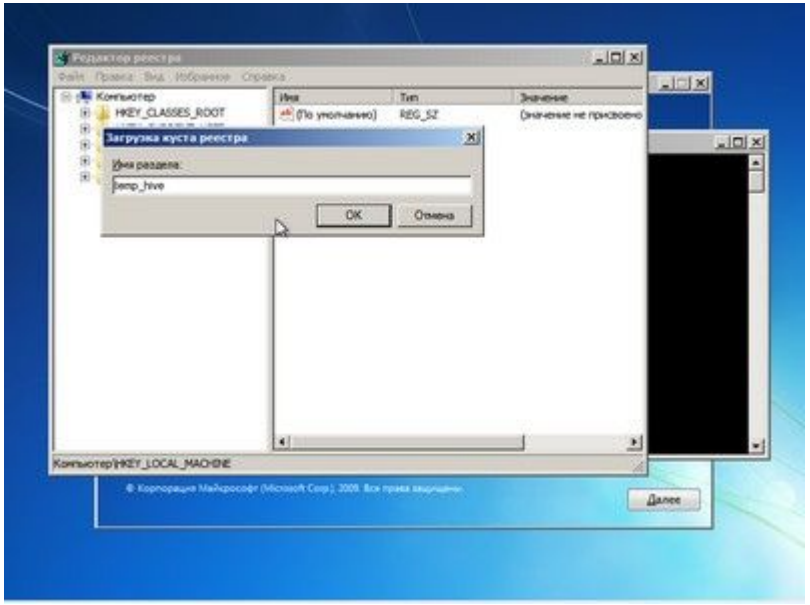

Open
Favorites
Search Favorites
Organize
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Desktop
Shortcut
440 bytes
Downloads
Shortcut
863 bytes
File name:
Text Documents (*.txt)
Encoding:
ANSI
Text Documents (*.txt)
All Files (*.*)

Часть 4

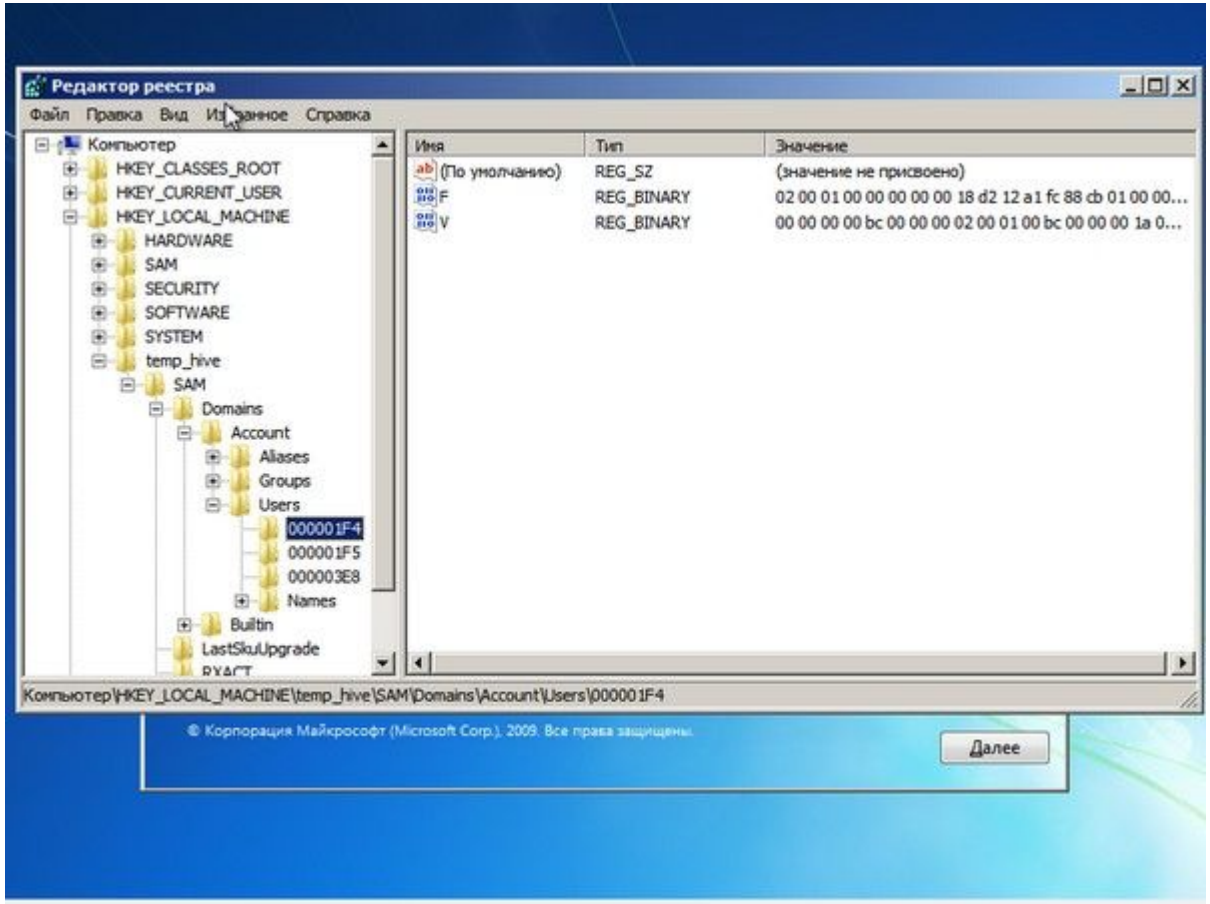

Установка Windows
Администратор: X:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
X:\Sources>regedit
Далее

Часть 4

Выделяем раздел HKEY_LOCAL_MACHINE, а в меню выбираем «Файл» → «Загрузить куст…» (File → Load hive…). Нам надо открыть файл SAM, который находится в папке \Windows\System32\config на том разделе, где установлена Windows 7. При открытии будет предложено ввести имя загружаемого куста — вбивайте любое.



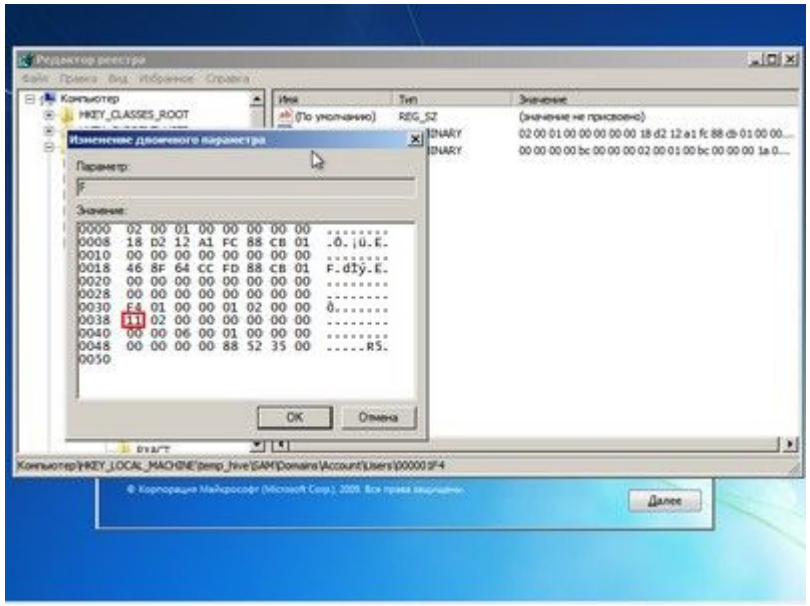
Часть 4

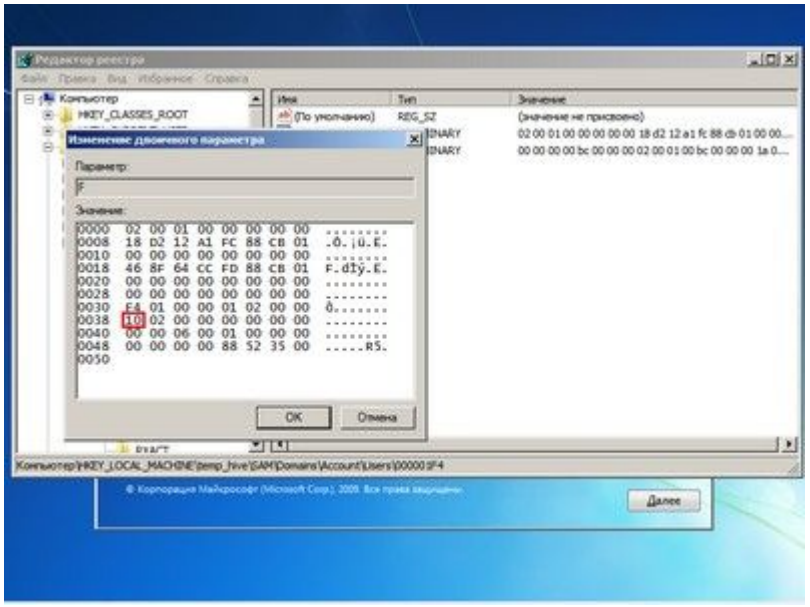

Редактор реестра
Файл Правка Вид Избранное Справка
Компьютер
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
temp_hive
SAM
Domains
Account
Aliases
Groups
Users
000001F4
000001F5
000003E8
Names
Builtin
LastSkuUpgrade
Имя
Тип
Значение
(По умолчанию)
REG_SZ
(значение не присвоено)
F
REG_BINARY
02 00 01 00 00 00 00 00 18 d2 12 a1 fc 88 cb 01 00 00...
V
REG_BINARY
00 00 00 00 bc 00 00 00 02 00 01 00 bc 00 00 00 1a 0...
Компьютер\HKEY_LOCAL_MACHINE\temp_hive\SAM\Domains\Account\Users\000001F4
© Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
Далее

Часть 4

- Теперь надо выбрать раздел HKEY_LOCAL_MACHINE\имя_куста\SAM\Domains\Account\Users\000001F4 и дважды кликнуть по ключу F. Откроется редактор, в котором надо перейти к первому числу в строке 038 — это 11. Его надо изменить на 10. Будьте аккуратны и не ошибитесь — поменять надо только его, не добавляя и не удаляя другие числа!

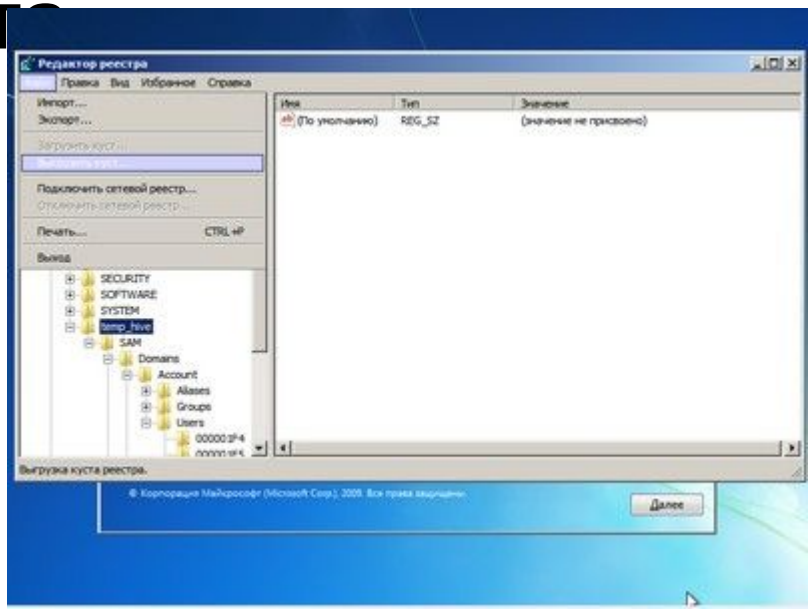
Часть 4


Редактор реестра
Изменение двоичного параметра
Параметр:
F
Значение:
0000 02 00 01 00 00 00 00 00
0008 18 D2 12 A1 FC 88 CB 01
0010 00 00 00 00 00 00 00 00
0018 46 8F 64 CC FD 88 CB 01
0020 00 00 00 00 00 00 00 00
0028 00 00 00 00 00 00 00 00
0030 F4 01 00 00 01 02 00 00
0038 11 02 00 00 00 00 00 00
0040 00 00 06 00 01 00 00 00
0048 00 00 00 00 88 52 35 00
0050
OK
Отмена
Далее


Редактор реестра
Изменение двоичного параметра
Параметр:
F
Значение:
0000 02 00 01 00 00 00 00 00
0008 18 D2 12 A1 FC 88 CB 01
0010 00 00 00 00 00 00 00 00
0018 46 8F 64 CC FD 88 CB 01
0020 00 00 00 00 00 00 00 00
0028 00 00 00 00 00 00 00 00
0030 F4 01 00 00 01 02 00 00
0038 10 02 00 00 00 00 00 00
0040 00 00 06 00 01 00 00 00
0048 00 00 00 00 88 52 35 00
0050
OK
Отмена
Далее

Часть 4

Теперь надо выделить наш куст HKEY_LOCAL_MACHINE\имя_куста\ и в меню выбрать «Файл» → «Выгрузить куст…» (File → Unload hive…), а затем подтвердить выгрузку куста.



Часть 4

Источники

- http://bugtraq.ru/library/books/stp/chapter11/
- http://lagman-join.narod.ru/spy/CNEWS/cisco_attacks.html
- http://ru.wikipedia.org/wiki/SYN-флуд
- http://ru.wikipedia.org/wiki/Ping_of_death
- http://bezopasnieseti.ru/protokol-icmp/ataka-tribe-flood-network.html
- http://www.xakep.ru/post/61403/
- http://kpnemo.ws/appz/2013/04/19/ruchnoy-vzlom-parolya-windows-7/
- http://www.3dnews.ru/623507