АНДРЕЙ «SKVZ» КОМАРОВ
/ KOMAROV@ITDEFENCE.RU /

АНОНИМНЫЙ ШТУРМ WINDOWS

ХИТРЫЕ ПРИЕМЫ БЫВАЛОГО ХАКЕРА

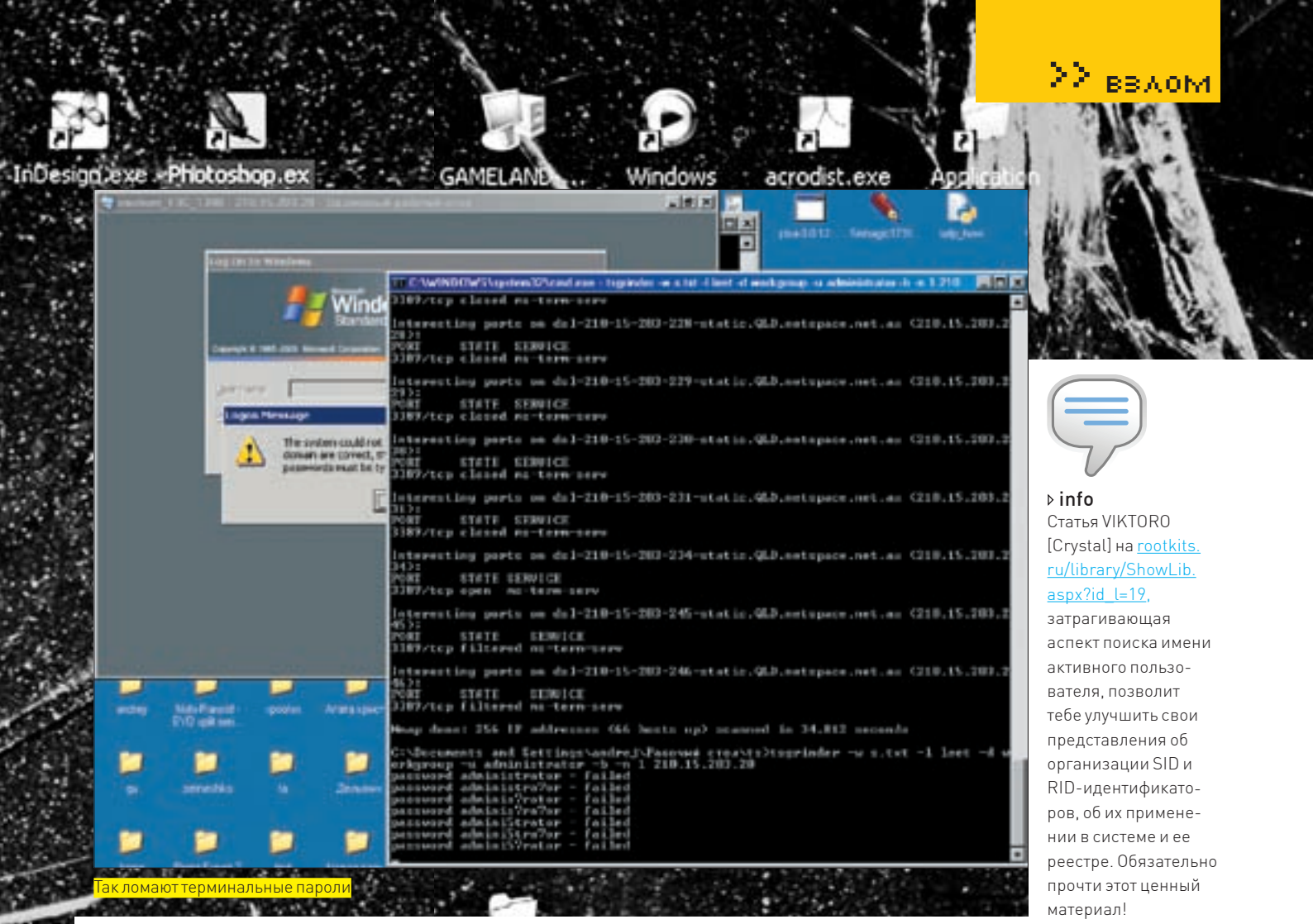
В сетевой атаке используется немыслимое число хакерских инструментов. В андеграунде даже говорят, что от количества утилит зависит профессионализм взломщика. Но самые интересные взломы происходят внезапно — на улице с полуразряженным ноутбуком, в универе на большой перемене — в общем, там, где возможности слить определенный софт просто нет. Приходится проявить максимум смекалки и либо пользоваться тем, что предоставляет твоя собственная ОС, либо иметь боевой комплект на все случаи жизни. Об этом минимальном комплекте я сейчас расскажу.

Несмотря на пафосные крики на форумах о том, что «Винда — сакс, два клика — пароль в руках», в ряде случаев завершить (а иногда, даже и инициировать) взлом не получается. В этой статье тебя ожидает подборка уловок, которые позволят чувствовать себя увереннее при штурме Windows. Итак, поехали!

НУЛЕВАЯ СЕССИЯ ИЛИ ПОЛУЧЕНИЕ СПИСКА ПОЛЬЗОВАТЕЛЕЙ

Нулевая сессия — лучшая лазейка для удаленного сбора информации с виндовой машины через NetBIOS. Но даже зная это, нередко возникает вопрос, как правильно использовать нулевую сессию. Лучшей, на мой взгляд, программой для эксплуатации нулевых сессий является **Winfo** (ntsecurity.nu/toolbox/winfo). Убедительная просьба не путать софтину с другими winfo (для сбора информации с локальной машины: хэндл окна, положение мыши и т.п).

Синтаксис команды предельно прост: `winfo.exe IP-адрес -n -v`. Замечу, что существует ряд ограничений, не позволяющих забрать с удаленной машины необходимые данные о пользователях. Например, применение параметра «`RestrictAnonymous=`» со значениями 1 и 2. **Ключи реестра**: `HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=1` (запрет показа шар; при этом анонимно авторизированные пользователи будут их видеть — значение 2 наотрез отсекает и то, и другое). Более того, анонимные подключения используются различными служебными программами (такими, как проводник Microsoft Windows, редактор таблиц доступа и диспетчер пользователей) для администрирования нескольких доменов Windows. За примером далеко ходить не надо: при уста-



Так ломают терминальные пароли

новке служб IIS создаются два объекта пользователей: `IUSR_«имя машины»` (служит для анонимного доступа к серверу) и `IWAM_«имя машины»` (для запуска внепроцессных приложений). Поэтому, если ты сразу же ринулся применять значение «2» в вышеуказанном ключе реестра, хорошенько подумай — не помешает ли опция работе легитимных пользователей. Симптомом значения «2» будет ошибка: «**Unable to browse the selected domain because the following error occurred:**».

Переходим к следующему ключу реестра: `HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=1` (запрет показа пользовательских аккаунтов).

И, наконец, `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver` (установить значение параметра `RestrictNullSessionAccess = 1`). Более подробно о значении ключей можно прочитать здесь — support.microsoft.com/default.aspx?scid=KB;en-us;143474.

Применение всех трех ключей осложнит задачу хакера, но не сделает ее невыполнимой. Мало кто знает, что у Windows есть «встроенные» (built-in) юзеры. Называются они для разных региональных версий по-разному, но везде обозначают администратора и гостя. Эти учетные записи имеют фиксированные относительные идентификаторы Relative Identifier (RID). У администратора — 500, у гостя — 501. Нумерация новых аккаунтов начинается с 1000. Суть задумки — узнать уникальный SID группы или домена по существующим встроенным RID, используя анонимное подключение. Узнав SID, мы легко можем вернуть соответствующие данные (`LookupAccountName`, `LookupSidName`). Этим занимаются следующие программы, которые обязательно нужно скачать и изучить:

- **GetAcct** (securityfriday.com/tools/getacct_sla.html). Все, что требуется для определения SID — указать IP или NETBIOS-имя машины. Вторым параметром — диапазон RID. Дело в том, что RID — это последняя часть SID (добавочная). Соответственно, указав определенный интервал, мы ограничиваем пределы перебора для поиска SID.
- **Dumpusers** (www.ntsecurity.nu/toolbox/dumpusers/). Консольная аналогия вышеназванной программы. Обе проги ты найдешь на нашем диске.

Отмечу, что основополагающими в работе софта являются алгоритмы, написанные нашими соотечественниками (evgenii.rudnyi.ru/soft/sid/) в проектах user2sid и sid2user. Не обойди стороной эту страницу, авторы прилагают исходный код!

ЗАХВАТ ТЕРМИНАЛА

Иногда знание учетных записей пользователей позволяет успешно захватить терминал. Впрочем, надо понимать, что не всем пользователям разрешено быть в группе Remote Desktop users, тем более, когда цель атаки — контроллер домена. В таком случае, подключаться по умолчанию к удаленной системе с использованием RDP разрешено только администратору. Между прочим, на днях обновилась самая лучшая утилита для взлома терминальных серверов — TSGRINDER (release 2). В новой версии автором улучшены способы перебора пароля. Синтаксис запуска прост, как два рубля:

```
tsgrinder – w paroli.txt – l leet – d workgroup
– u administrator – b –n 1 210.15.203.20,
```

— где leet это файл для преобразования пароля в хакерско-читабельный (h3k3rz) вид; — d — указание на домен или рабочую группу.

info

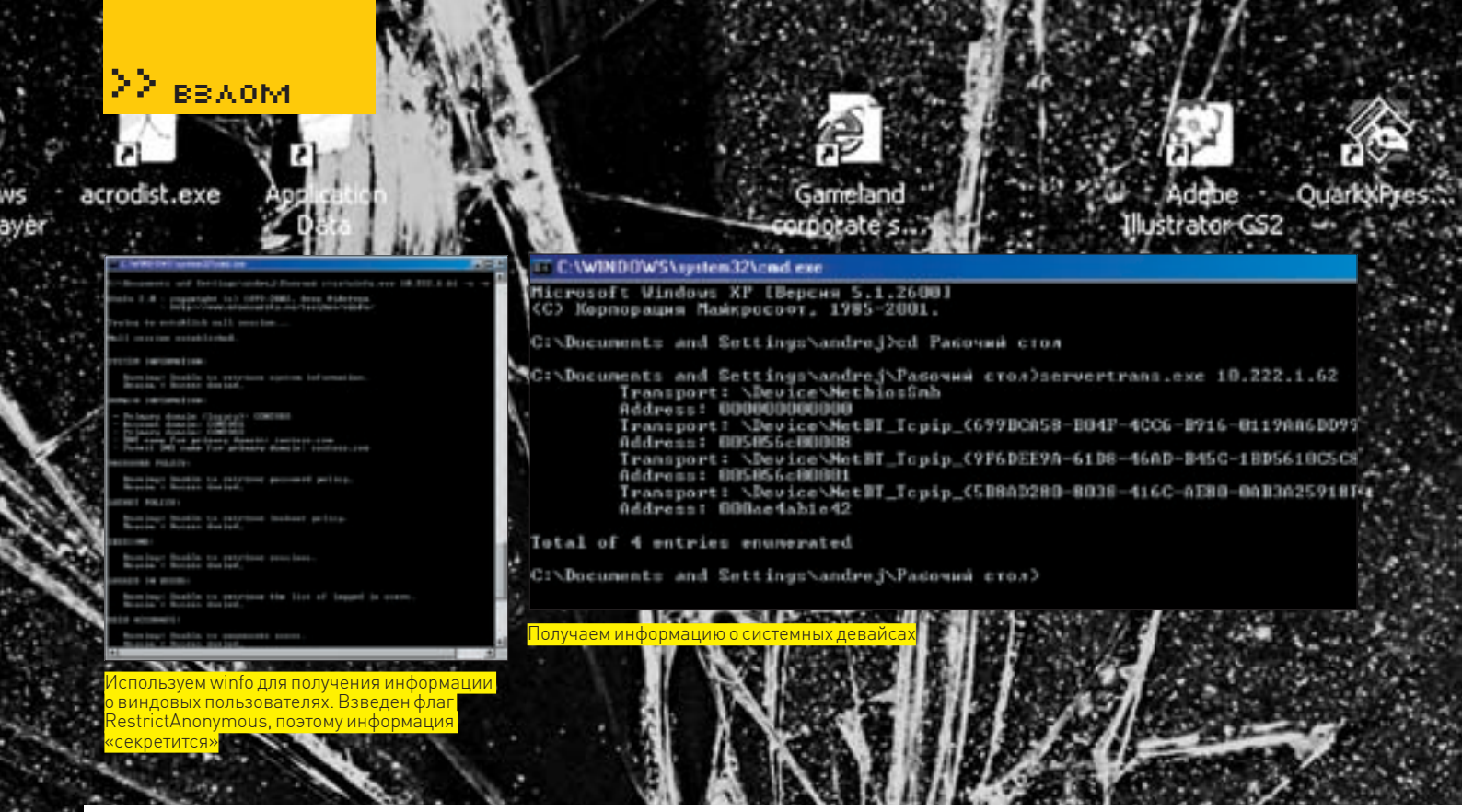
Статья VIKTORO [Crystal] на rootkits.ru/library/ShowLib.aspx?id_l=19, затрагивающая аспект поиска имени активного пользователя, позволит тебе улучшить свои представления об организации SID и RID-идентификаторов, об их применении в системе и ее реестре. Обязательно прочти этот ценный материал!

links

Более подробно о встроенных аккаунтах и дефолтных SID ты можешь узнать на support.microsoft.com/default.aspx?scid=KB;en-us;163846.

warning

Вся информация приведена исключительно в ознакомительных целях. Ответственность за ее применение несешь только ты. Помни об этом!



Получаем информацию о системных девайсах

Используем winfo для получения информации о виндовых пользователях. Взведен флаг RestrictAnonymous, поэтому информация «секретится»

Определить — терминал перед тобой или нет, довольно сложно. Дело в том, что стандартный порт для подключения (3389 tcp/rdp) может быть изменен админом на нестандартный путем редактирования ключа: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp\PortNumber`. Делается это так — в меню «Правка» выбирается команда «Изменить» и устанавливается система исчисления «Десятичная», а затем редактируется само поле. Поэтому хакеру требуется применять техники, отличные от простого поиска (как например, «`nmap 10.222.1.0/24 -p 3389`»). Одной из них можно считать приведенный в моей статье «Терминальная эпопея» метод поиска через компонент tsweb по Google (перерывай в поиске подшивку][за 2006 год). Можно пойти и другим путем, юзая программы `ProbeTS` и `TSEnum`.

Probets использует RPC-вызовы для установления подлинности терминала, тем самым сканируя подсеть с целью поиска терминальных серверов. Синтаксис: `Probets.exe 10.222.1.1 1 200` (последний параметр — конечный IP-адрес из сканируемого диапазона).

А вот в TSEnum применяется иной механизм детектирования. Когда рабочая станция или сервер присоединяются к домену, они регистрируют себя с помощью опции «master browser». Регистрация включает в себя указание типа сервера (терминал, файловый и т.п.). Эту информацию можно удаленно выудить с помощью функции `NetServerEnum()` — что и проделывает `TSENum`.

Слово о browstat

В стандартном виндовом арсенале есть популярная и дельная команда — net view. Она позволяет просматривать сетевое окружение в консольном режиме. Порой можно столкнуться с проблемой успешного ее выполнения. Это связано с тем, что на домене отключена опция «browsing». Проверить, так это или нет, можно с помощью утилиты, часто используемой виндовыми системными администраторами — browstat.exe (ты найдешь ее на нашем диске). Синтаксис запуска: browstat.exe status. Подробнее об устранении ошибок, связанных с обозревателем окружения (8021, 8032), можно прочесть здесь: support.microsoft.com/kb/135404/ru.

ЗНАЙ ВРАГА В ЛИЦО

Представь себе, что с использованием анонимного подключения реально перечислить все сетевые карты и их интерфейсы на удаленной машине. Выполнить это можно с помощью функции `NetServerTransportEnum`, даже если `RestrictAnonymous` имеет значение 1. Для подобной цели создана утилита `TransportEnum`, которая возвращает данные о структуре `SERVER_TRANSPORT_INFO_0` (msdn.microsoft.com/en-us/library/aa370949(VS.85).aspx). Между прочим, структура содержит информацию о количестве подключенных клиентов, названии сетевого интерфейса и адресации на нем. Программа пишет нам CSID устройства:

```
Transport: \Device\NetBT_Tcpip_{CE081110-126E-4BD1-88B0-2FF8C1D83D10}
Address: 00c0f06cdf7a
```

— то есть, данные от обычной сетевой карты и интерфейса TCP/IP. Так, кстати, получится узнать, поддерживает ли удаленная машина Wi-Fi или какие-то экзотические вещи. Короче, дерзай, и удача тебе улыбнется!

Тоже winfo. Без дополнительных настроек — имена как на ладони