26 - 28 NOVEMBER 2024
RIYADH, SAUDI ARABIA

How an attacker can hack any Organization through their misconfigured Active Directory (AD)

ORGANISED BY: Ahmed Hassan

Ahmed Hassan

Cyber Security Consultant & Penetration Tester @ Condignum, AUSTRIA (Vienna)

Title: How an attacker can hack any Organization through their misconfigured Active Directory (AD)

talking @ BlackHat Saudi Arabia 2024

Agenda

1. Self-Introduction
2. What is an Active Directory (AD) ?
3. Different Vulnerabilities & Misconfigurations in Active Directory (AD)
4. DCSnyc attack Live Demo – how we can extract all the users Hashes
5. Questions from the audience & further Explanations (Q&A)?

Self-Introduction

Working since almost 6 years as a Cyber Security Engineer & Penetration Tester @ Condignum, AUSTRIA

Speaker at various international security conferences & Universities (USA-United States of America), Egypt, UAE, Saudi Arabia, Austria etc.)

Securing the Clients environment (Web, API, Active Directory, Mobile, internal & external Infrastructure etc.)

Where am I from ?

Qualifications & professional Certifications

studied and working in Austria in the Cyber Security Field as **Cyber Security Engineer, Penetration Tester and Bug Bounty Hunter**

Certifications for advanced IT professionals

Certified EC-council Instructor

Certified Ethical Hacker

Offensive Security Certified Professional

Offensive Security Web Assessor

Importance of Cyber Security in Active Directory

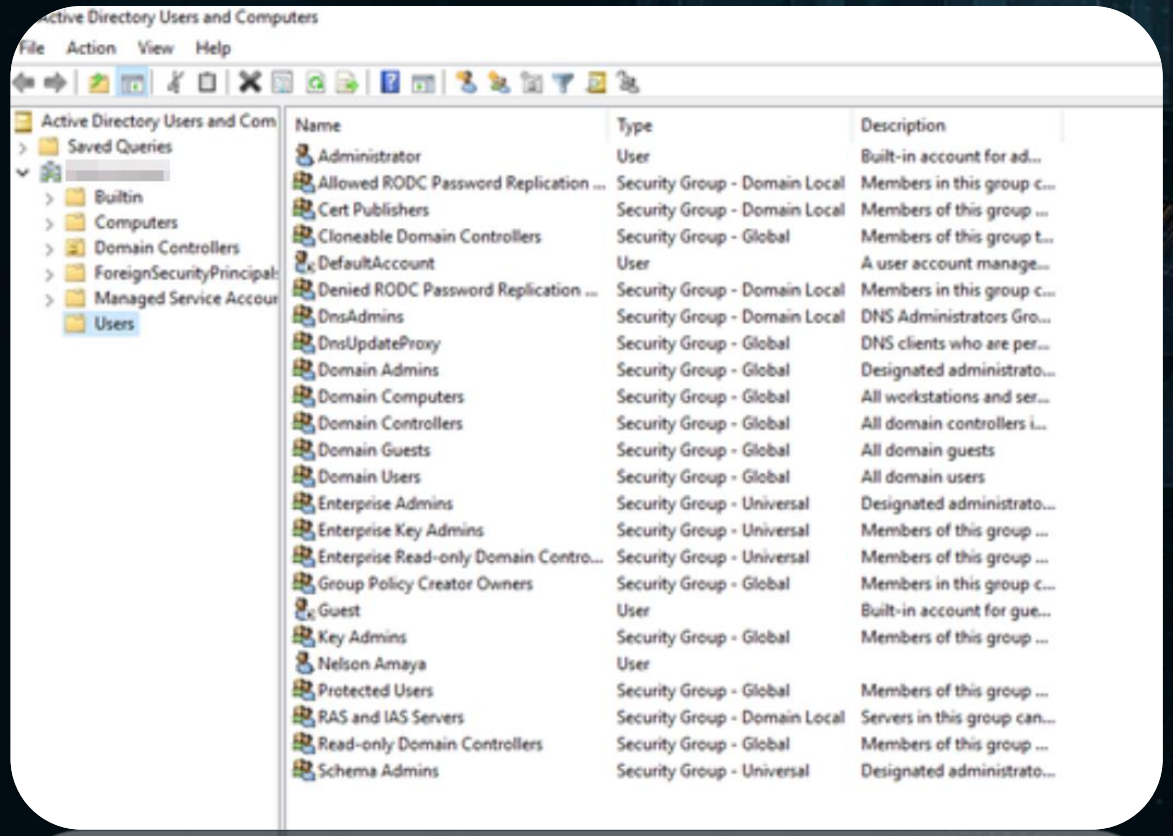
Active Directory penetration testing is crucial as it helps identify and mitigate potential weaknesses before they can be exploited by malicious actors. By simulating attacks, penetration testing assesses the resilience of Active Directory defenses against unauthorized access, privilege escalation, and lateral movement across the network.

What is an Active Directory ?

Active Directory Explanation

The database (or directory) contains critical information about your environment, including what users and computers there are and who's allowed to do what. For example, the database might list 100 user accounts with details like each person's job title, phone number and password. It will also record their permissions.
The services control much of the activity that goes on in your IT environment. They make sure each person is who they claim to be (authentication), usually by checking the user ID and password they enter and allow them to access only the data they're allowed to use (authorization).

Active Directory simplifies life for administrators and end users while enhancing security for organizations. Administrators enjoy centralized user and rights management, as well as centralized control over computer and user configurations through the AD Group Policy feature.



Lack of unique Passwords & Password re-use

In many organizations, domain-joined users (users authenticated through the network's domain) share similar or identical passwords across multiple accounts. While convenient for users, this practice introduces significant security vulnerabilities.

When users share the same password across different accounts or systems, the risk of unauthorized access increases dramatically. If one account's password is compromised, attackers can exploit that password across the network. This threat can escalate quickly in environments where password reuse is common among domain-joined accounts.

Mitigation: Using unique passwords for domain-joined accounts is critical in protecting an organization from breaches and unauthorized access. By enforcing unique, strong passwords, the organization can significantly reduce the risk of attacks, safeguard sensitive data, and maintain compliance with security standards.

```
┌──(ahmed㉿LAPTOP-PJ1Q80N7)-[~/Downloads]
└─$ crackmapexec smb 192.168[redacted] -u '[redacted]' -p 'Ap[redacted]
SMB         192.168.1.132   445                [*] Windows 10.0 Build 20348 x64 [redacted] (signing:True) (SMBv1:False)
SMB         192.168.1.132   445                [+] [redacted]

┌──(ahmed㉿LAPTOP-PJ1Q80N7)-[~/Downloads]
└─$ crackmapexec smb 192.168.[redacted] -u '[redacted]' -p 'Ap[redacted]
SMB         192.168.1.132   445                [*] Windows 10.0 Build 20348 x64 [redacted] (signing:True) (SMBv1:False)
SMB         192.168.1.132   445                [+] [redacted]

┌──(ahmed㉿LAPTOP-PJ1Q80N7)-[~/Downloads]
└─$ crackmapexec smb 192.168.[redacted] -u '[redacted]' -p 'Ap[redacted]
SMB         192.168.1.132   445                [*] Windows 10.0 Build 20348 x64 [redacted] (signing:True) (SMBv1:False)
SMB         192.168.1.132   445                [redacted]

┌──(ahmed㉿LAPTOP-PJ1Q80N7)-[~/Downloads]
└─$ crackmapexec smb 192.168[redacted] -u '[redacted]' -p 'Ap[redacted]
SMB         192.168.1.132   445                [*] Windows 10.0 Build 20348 x64 [redacted] (signing:True) (SMBv1:False)
SMB         192.168.1.132   445                [+] [redacted]
```

The same password has been assigned to multiple users. + the used Password is very weak

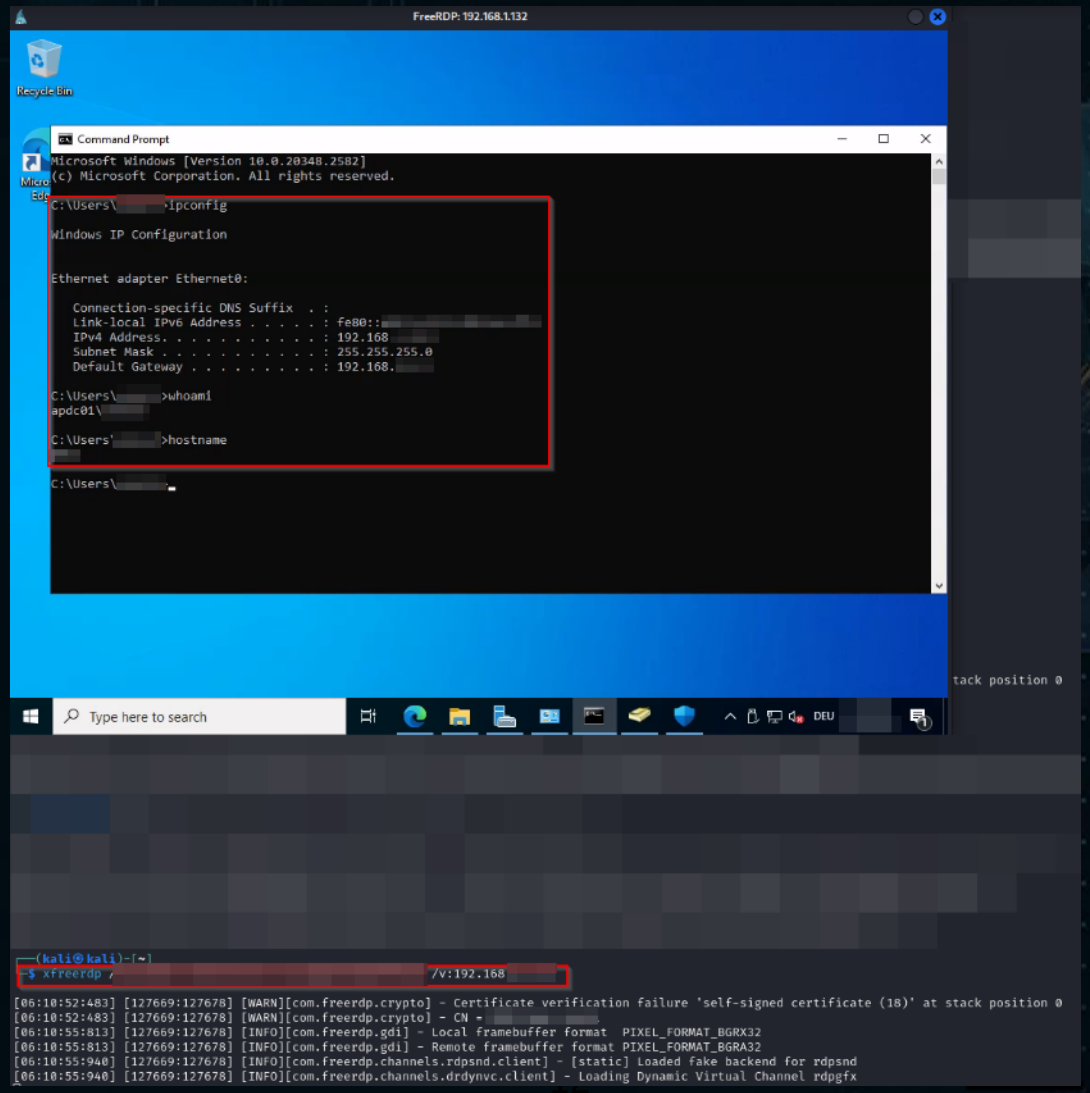
weak and no strong Password Policy at all

The absence of a robust password policy, or the presence of a weak one, within Active Directory (AD) poses a significant security vulnerability. Without stringent password requirements—such as minimum length, complexity, expiration intervals, and history enforcement—users may set easily guessable or reused passwords. This increases the risk of unauthorized access, particularly through brute-force or credential-stuffing attacks. The configured password policy requires a minimum length of 7 characters, as evidenced by the screenshot provided.

```
crackmapexec smb 192.168      -u      ' -p '                ' --pass-pol
SMB         192.168      445                [*] Windows 10.0 Build 20348 x64                    (signing:True) (SMBv1:False)
SMB         192.168      445                [+]
SMB         192.168      445                [+] Dumping password info for domain:
SMB         192.168      445                Minimum password length: 7
SMB         192.168      445                Password history length: 24
SMB         192.168      445                Maximum password age: 41 days 23 hours 53 minutes
SMB         192.168      445
SMB         192.168      445                Password Complexity Flags: 000001
SMB         192.168      445                    Domain Refuse Password Change: 0
SMB         192.168      445                    Domain Password Store Cleartext: 0
SMB         192.168      445                    Domain Password Lockout Admins: 0
SMB         192.168      445                    Domain Password No Clear Change: 0
SMB         192.168      445                    Domain Password No Anon Change: 0
SMB         192.168      445                    Domain Password Complex: 1
SMB         192.168      445
SMB         192.168      445                Minimum password age: 1 day 4 minutes
SMB         192.168      445                Reset Account Lockout Counter: 30 minutes
SMB         192.168      445                Locked Account Duration: 30 minutes
SMB         192.168      445                Account Lockout Threshold: None
SMB         192.168      445                Forced Log off Time: Not Set
```

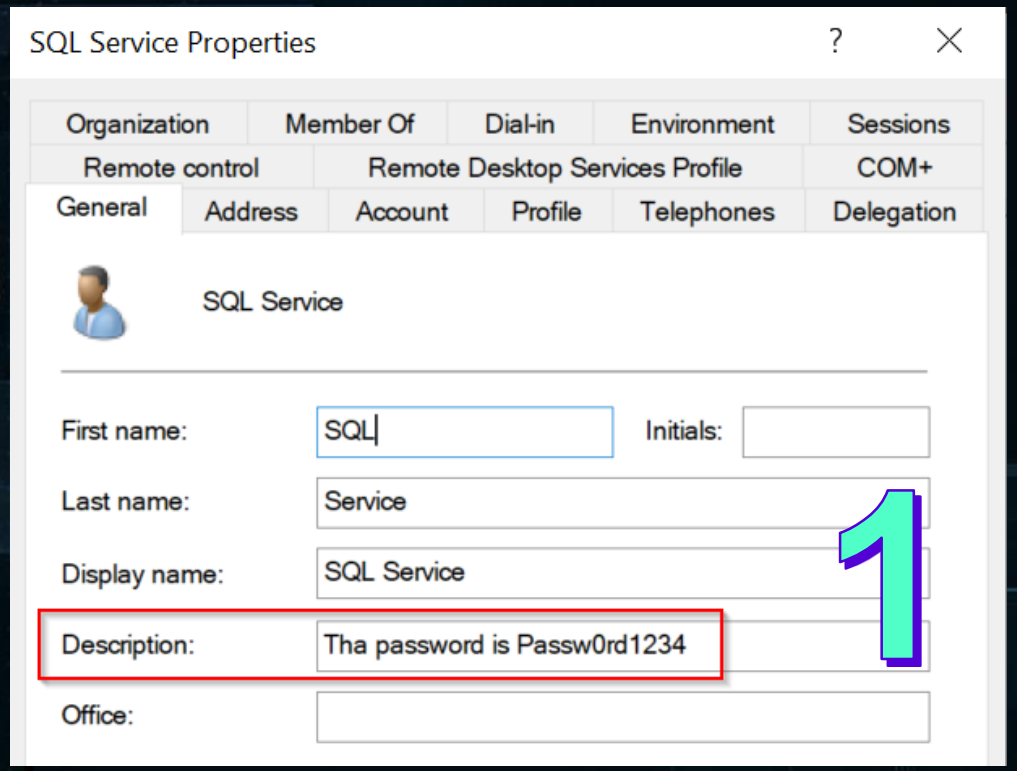
Non-administrative Domain Users and low-Privileged Users have RDP Access to the Domain Controller

Non-administrative domain users and other low-privileged users are granted Remote Desktop Protocol (RDP) access to the Domain Controller (DC). Domain Controllers are highly sensitive systems, as they store and manage credentials, security policies, and authentication for the entire network. Allowing users with minimal privileges to connect to the Domain Controller poses a serious security risk, as it increases the potential for malicious activities, accidental misconfigurations, and exposure to malware.



Cleartext Passwords in the Description Field written by the System Administrator

In this scenario, passwords are being stored in plain-text within the description fields of Active Directory (AD) objects, typically user accounts, by a system administrator. The description field is intended for brief, non-sensitive notes, not for storing credentials or other confidential information. Since these fields can be easily viewed by users with basic permissions or accessed through scripts and AD queries, storing passwords here poses a significant security risk.



2

Leading to

Hacking the SQL-Service with the visible Password

Excessive Unnecessary Domain Administrator Accounts

In this vulnerability, an excessive number of user accounts have been assigned Domain Administrator privileges within Active Directory (AD). Domain Administrator accounts hold elevated privileges, granting full control over all AD objects, policies, and settings within the domain. When too many users have Domain Administrator privileges—especially if the accounts are unnecessary or belong to users who do not require such access—this increases the attack surface and the risk of privilege abuse, misconfigurations, and security breaches.

Domain Admins

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID
			07/17/23 05:41:21	08/26/24 10:39:46	09/04/24 09:56:59	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/17/23 05:53:50	
			04/20/21 18:48:26	09/08/24 06:15:30	09/09/24 04:34:11	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/22/24 12:55:25	
			09/04/17 17:08:33	02/20/24 14:48:09	02/20/24 14:48:09	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/04/17 17:08:33	
			09/04/17 08:08:42	08/10/24 20:20:41	06/01/20 06:08:29	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/04/17 08:08:42	
			08/23/17 09:47:20	09/07/24 17:22:18	09/08/24 19:49:54	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	08/23/17 09:47:20	
			04/13/08 06:47:44	07/14/24 07:15:29		NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	04/13/08 06:47:44	
			05/13/08 09:01:02	04/17/23 08:45:44	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/23/17 05:46:52	
			07/10/17 12:11:34	08/07/24 13:52:08	05/24/23 07:38:14	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	03/10/21 07:56:19	
			01/28/10 11:51:15	09/07/24 09:05:02	09/09/24 04:44:52	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	03/01/21 10:04:21	
			01/10/10 12:24:00	09/01/24 00:40:57	09/09/24 04:40:57	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	03/04/21 12:15:09	
			06/15/08 05:29:25	04/17/23 08:45:44		NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/08 05:29:25	
Administrator	Administrator		10/03/02 07:28:18	09/06/24 12:15:05	06/24/24 05:18:52	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD, TRUSTED_FOR_DELEGATION	06/24/24 05:16:18	500

Domain Administrator Group Analysis

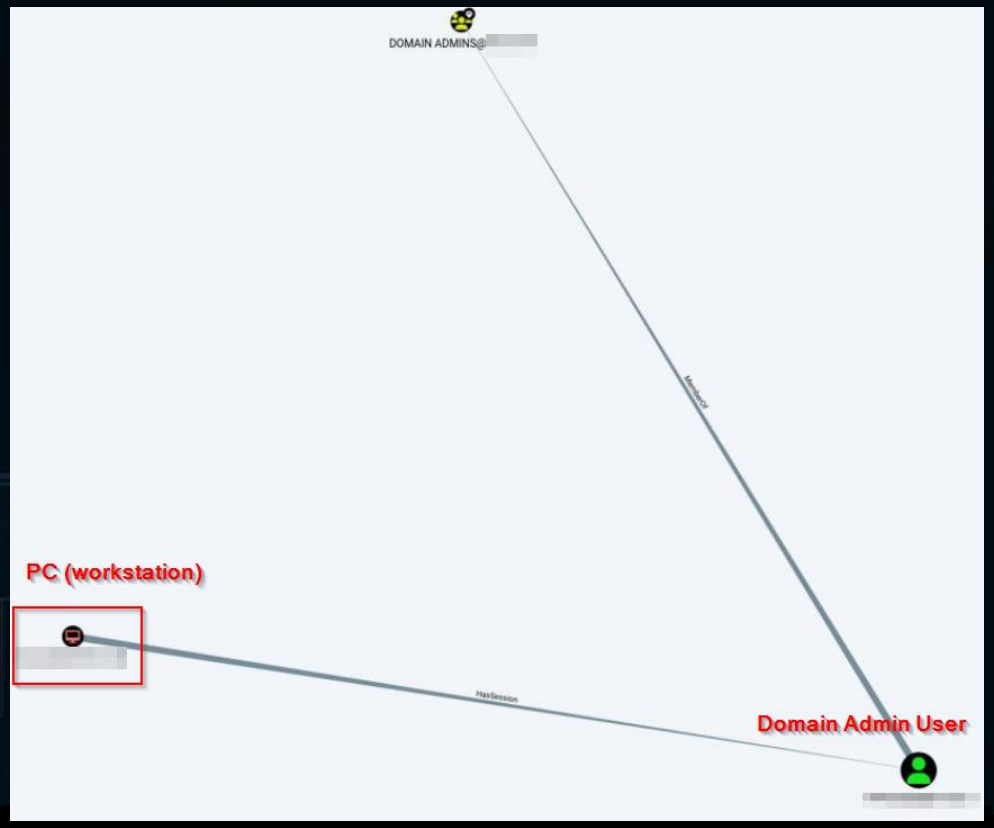
Several Domain Administrator accounts exhibit signs of poor password hygiene and inactivity, including:
<u>Inactive Domain Administrator Accounts:</u> Accounts that are no longer in active use but still retain elevated privileges.
<u>Stale Passwords:</u> Domain Administrator accounts with passwords that haven't been updated since 2008 or older.
<u>"Password Never Expires" Attribute</u>: Some Domain Administrator accounts are set with the "Password Never Expires" flag, preventing routine password changes.

Domain Admins

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
			07/17/23 05:41:21	08/26/24 10:39:46	09/04/24 09:56:59	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/17/23 05:53:50		
			04/20/21 18:48:26	09/08/24 06:15:30	09/09/24 04:34:11	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/22/24 12:55:25		
			09/04/17 17:08:33	02/20/24 14:48:09	02/20/24 14:48:09	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/04/17 17:08:33		
			09/04/17 08:08:42	08/10/24 20:20:41	06/01/20 06:08:29	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/04/17 08:08:42		
			08/23/17 09:47:20	09/07/24 17:22:18	09/08/24 19:49:54	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	08/23/17 09:47:20		
			04/13/08 06:47:44	07/14/24 07:15:29		NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	04/13/08 06:47:44		
			05/13/08 09:01:02	04/17/23 08:45:44	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/23/17 05:46:52		
			07/10/17 12:11:34	08/07/24 13:52:08	05/24/23 07:38:14	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	03/10/21 07:56:19		
			01/28/10 11:51:15	09/07/24 09:05:02	09/09/24 04:44:52	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	03/01/21 10:04:21		
			01/10/10 12:24:00	09/01/24 00:40:57	09/09/24 04:40:57	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	03/04/21 12:15:09		
			06/15/08 05:29:25	04/17/23 08:45:44		NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/15/08 05:29:25		
	1. Password never expires 2. Password changed last time changed in the year 2017 3. Inactive Domain Admins like "SCCMAdmin"		10/03/02 07:28:18	09/06/24 12:15:05	06/24/24 05:18:52	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD, TRUSTED_FOR_DELEGATION	06/24/24 05:16:18		

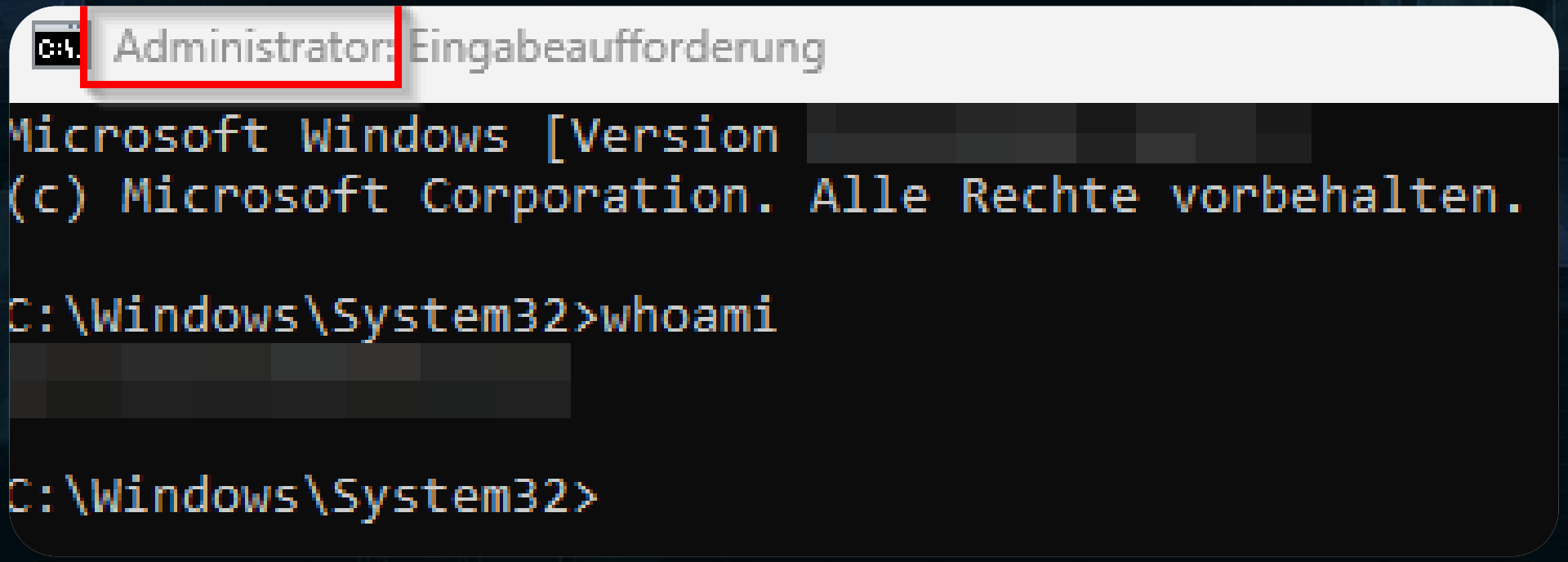
Domain Administrator Sessions on non-Domain Controller meaning normal workstations

Domain Administrator accounts are used to log in on standard workstations rather than exclusively on Domain Controllers or secure administrative systems. Domain Administrator accounts hold elevated privileges that allow full control over the Active Directory (AD) environment. When these high-privilege accounts are used on regular workstations, they are exposed to a higher risk of compromise from malware, phishing attacks, or unauthorized access on less secure machines like Hash dumping etc.



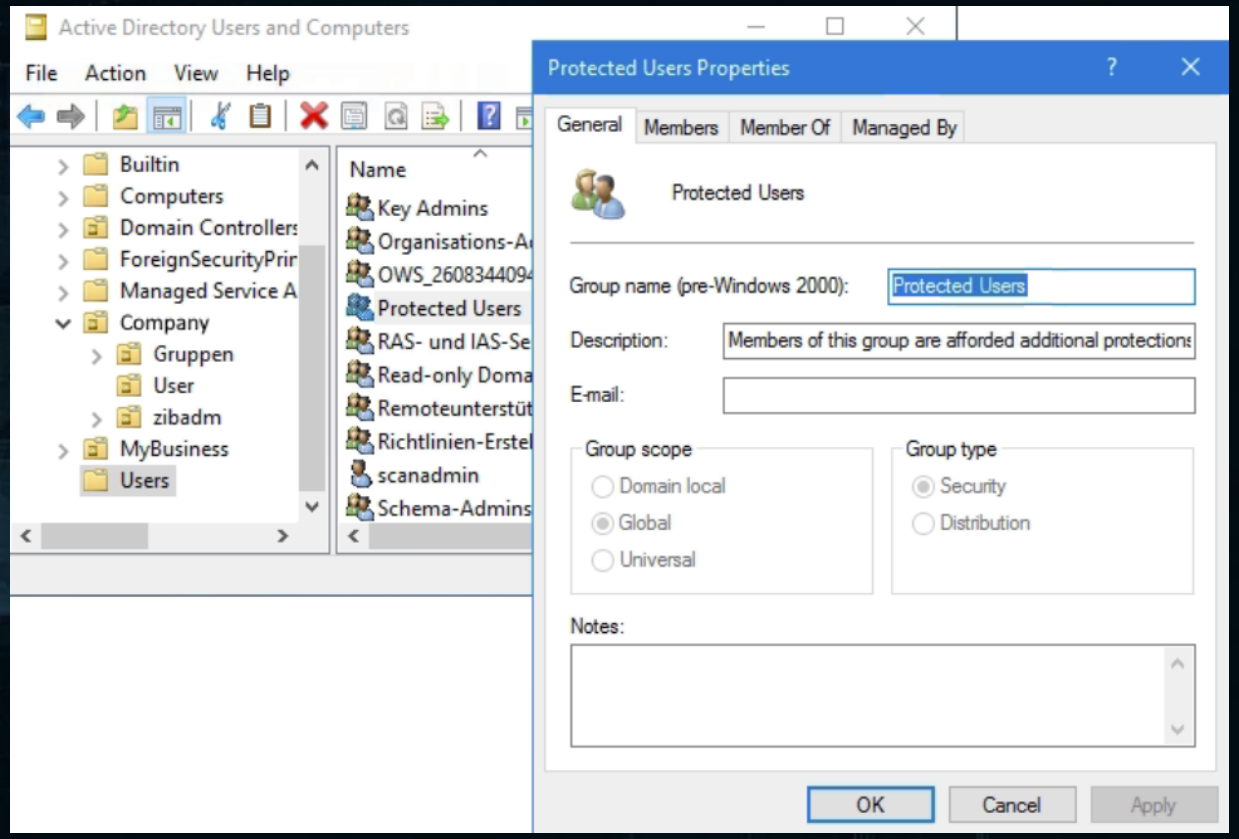
Absence of Least Privilege: All Users granted Full local Administrator Permissions

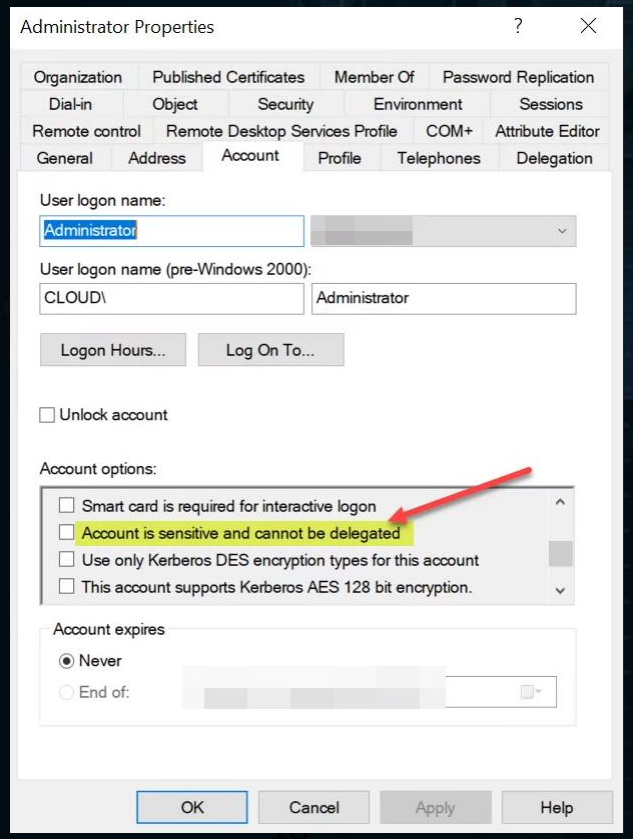
Here in this vulnerability, all users within the organization are granted full local Administrator permissions on their workstations or devices, bypassing the principle of least privilege. Local Administrator access allows users to install software, alter system settings, and manage other user accounts on the device. This broad level of access can result in users unintentionally misconfiguring systems, installing unauthorized software, or exposing the system to malware and security threats.



All Domain Admin Users not included in the Protected Group + Presence of administrative Accounts lacking the "This account is sensitive and can not be delegated" Flag

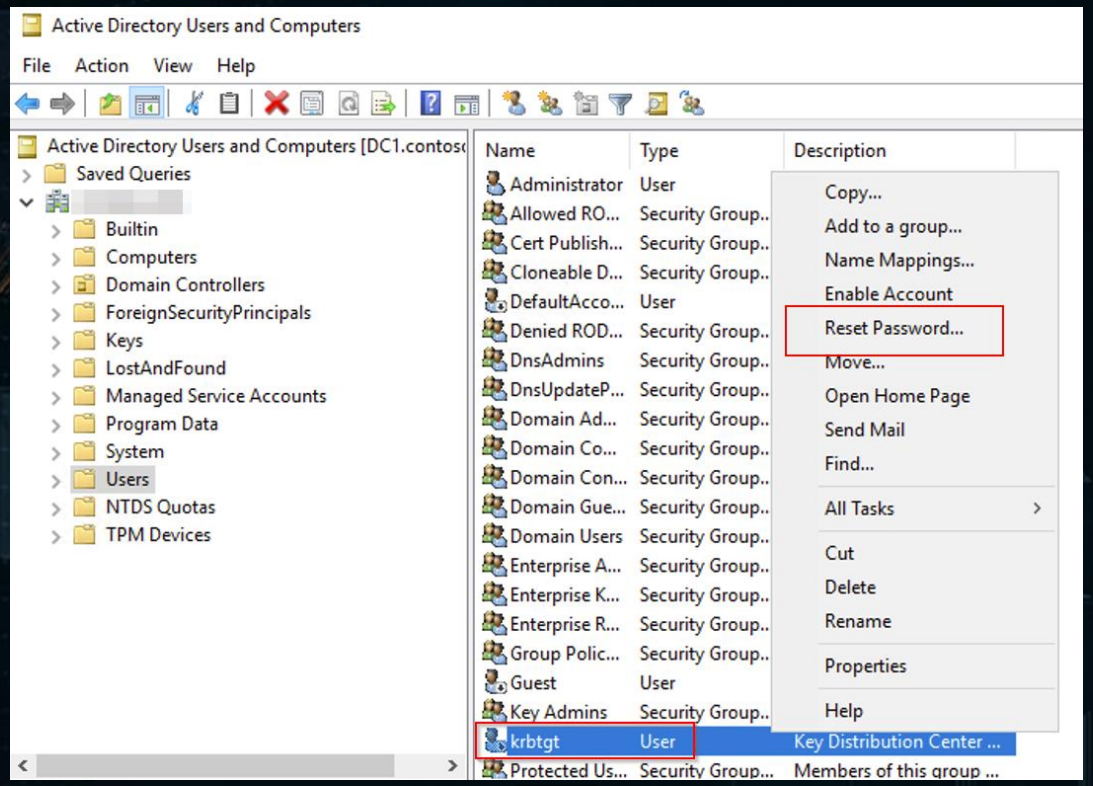
In Active Directory, certain accounts, such as Domain Admins or highly privileged service accounts, should be protected from unauthorized delegation or access. The "Protected Group" setting and the "This Account is sensitive and can not be delegated" flag help secure these accounts by preventing them from being delegated to other users or services, which could lead to privilege escalation or unauthorized access.





Last Change of Kerberos (KRBTGT) Password

The Kerberos service account, known as KRBTGT, is a critical component in the Kerberos authentication protocol used by Active Directory. This account is responsible for issuing Ticket Granting Tickets (TGTs), which are used by users and services to authenticate and gain access to network resources. If an attacker compromises the KRBTGT account or its password, they can forge Golden Tickets—special Kerberos tickets that grant unauthorized access to any service in the domain, including Domain Controllers. This attack can lead to complete domain compromise.



Mitigate golden ticket attack via a regular change of the krbtgt password

Rule ID:
A-Krbtgt

Description:
The purpose is to alert when the password for the krbtgt account can be used to compromise the whole domain. This password can be used to sign every Kerberos ticket. Monitoring it closely often mitigates the risk of golden ticket attacks greatly.

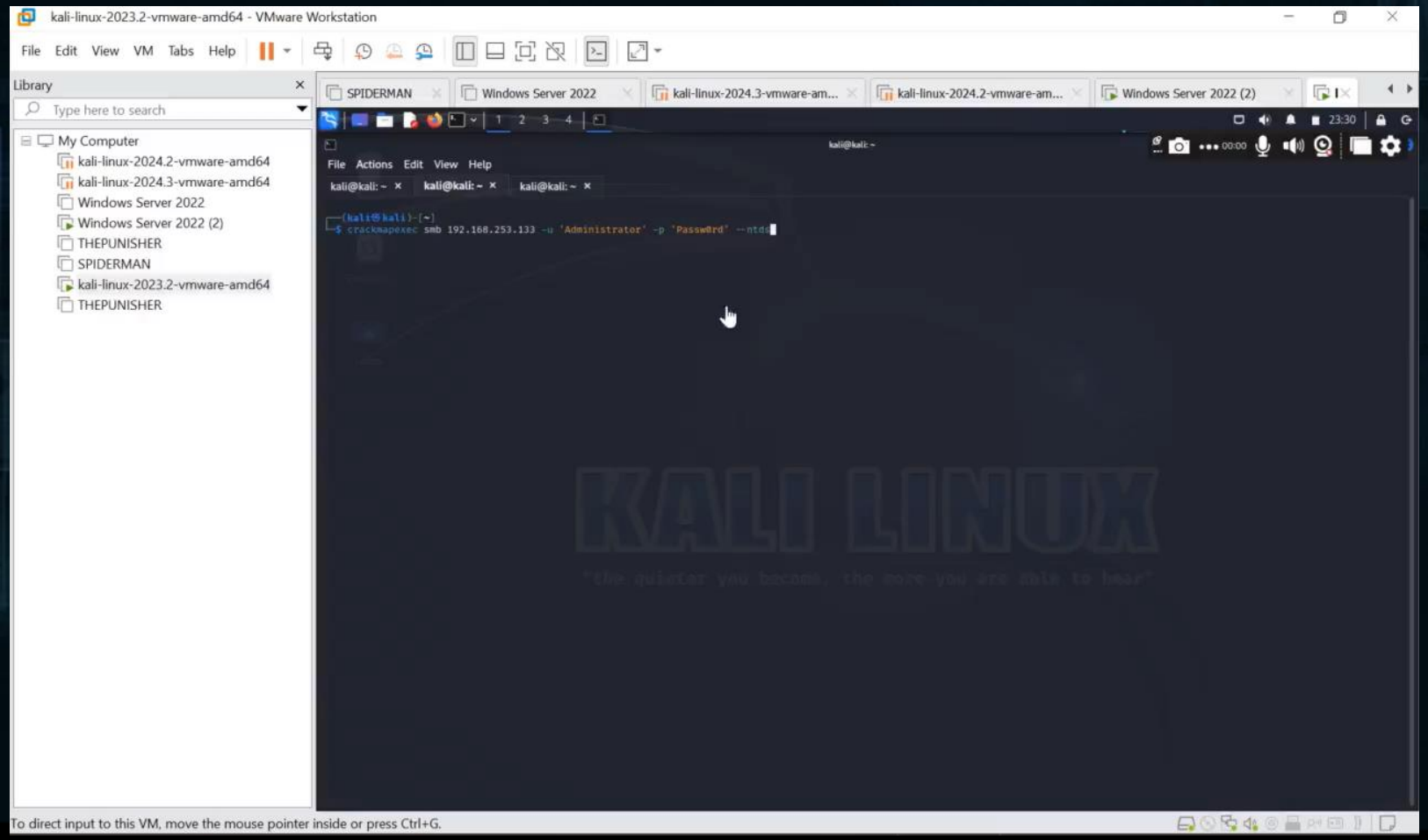
Technical explanation:
Kerberos is an authentication protocol. It is using a secret, stored as the password of the krbtgt account, to sign its tickets. If the hash of the password of the krbtgt account is retrieved, it can be used to generate authentication tickets at will.
To mitigate this attack, it is recommended to change the krbtgt password between 40 days and 6 months. If this is not the case, every backup done until the last password change of the krbtgt account can be used to emit Golden tickets, compromising the entire domain.
Retrieval of this secret is one of the highest priority in an attack, as this password is rarely changed and offer a long term backdoor.
Also this attack can be performed using the former password of the krbtgt account. That's why the krbtgt password should be changed twice to invalidate its leak.

Advised solution:
The password of the krbtgt account should be changed twice to invalidate the golden ticket attack.
Beware: two changes of the krbtgt password not replicated to domain controllers can break these domain controllers You should wait at least 10 hours between each krbtgt password change (this is the duration of a ticket life).

There are several possibilities to change the krbtgt password.
First, a Microsoft script can be run in order to guarantee the correct replication of these secrets.
Second, a more manual way is to essentially reset the password manually once, then to wait 3 days (this is a replication safety delay), then to reset it again. This is the safest way as it ensures the password is no longer usable by the Golden ticket attack.

We got Domain Administrator access -> What now ? -> DCSync Attack Lab and Walkthrough

DCSync attack Explanation: DCSync is an attack that allows an adversary to simulate the behavior of a domain controller (DC) and retrieve password data via domain replication. The classic use for DCSync is as a precursor to a Golden Ticket attack, as it can be used to retrieve the KRBTGT hash and all the other user hashes.



vulnerable Active Directory Setup

A vulnerable Active Directory local setup created by me.

GitHub Link: https://github.com/ahmedvienna/Active-Directory

ahmedvienna / Active-Directory Public

Notifications | Fork 0 | Star 2

Code | Issues | Pull requests | Actions | Projects | Security | Insights

main | 1 Branch | 0 Tags | Go to file | Code

ahmedvienna Add files via upload 53fffd1 · 2 weeks ago 9 Commits

README.md	Update README.md	2 weeks ago
Vulnerable Active Directory in VMWAR...	Add files via upload	2 weeks ago

README

Easy vulnerable Active-Directory environment Setup in Vmware

Are you looking to set up a local Active Directory environment with all virtual machines pre-configured?

About

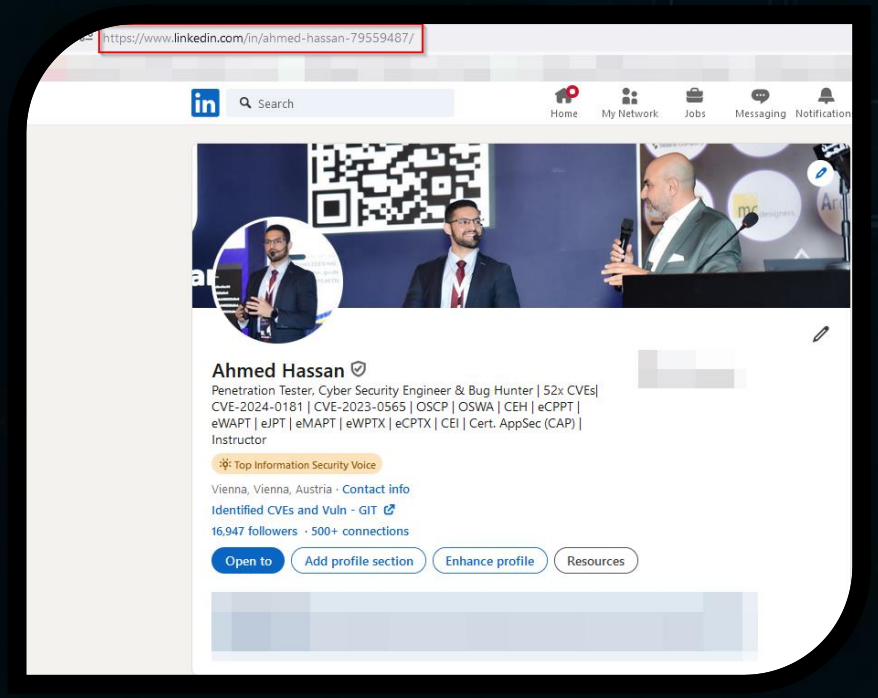
Vulnerable Active Directory easy local setup

Readme
Activity
2 stars
1 watching
0 forks
Report repository

Releases

No releases published

Packages



THANK YOU very much ☺

My LinkedIn: https://www.linkedin.com/in/ahmed-hassan-79559487/

Contact -> LinkedIn QR-Code