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

Key Active Directory Vulnerabilities

valeraleontev · 25.08.2021 · active directory red team translated

Go to new Trace

valeraleontev
RAID User

25.08.2021 New #1

Active Directory 1 Major Vulnerabilities Part 1

Most organizations and enterprises around the world today use Active Directory in their infrastructure as a solution for centralized management of their resources. But like any other similar technology, Active Directory is very complex, and its protection requires considerable effort and many years of experience.
This list consists of 16 issues that are most often detected during internal infrastructure penetration tests and vulnerability assessments. There's nothing special or new about it, it's just a list of typical problems.
The list is randomly organized - so it looks more like a checklist than

an ordered ranking list: 1. Users who have the right to add computers to domain
2. The AdminCount attribute is set for standard users.
3. A large number of users in privileged groups.
4. Service accounts that are members of domain administrators.
5. Excessive privileges
6. Service accounts that are vulnerable to Kerberoasting.
7. Users with passwords that do not expire.
8. Users without password.

9. Storing passwords using reversible encryption..
10. Storing passwords using LM hashes.
11. Accounts vulnerable to AS-REP Roasting'y.
12.Weak domain
password policy 13. Inactive Domain
14 accounts. Privileged users with expired passwords.
15. Users with a
weak password 16. Credentials in SYSVOL and Group Policy Settings

(GPP) Let's get started.

1. Users who have the right to add computers to the domain.

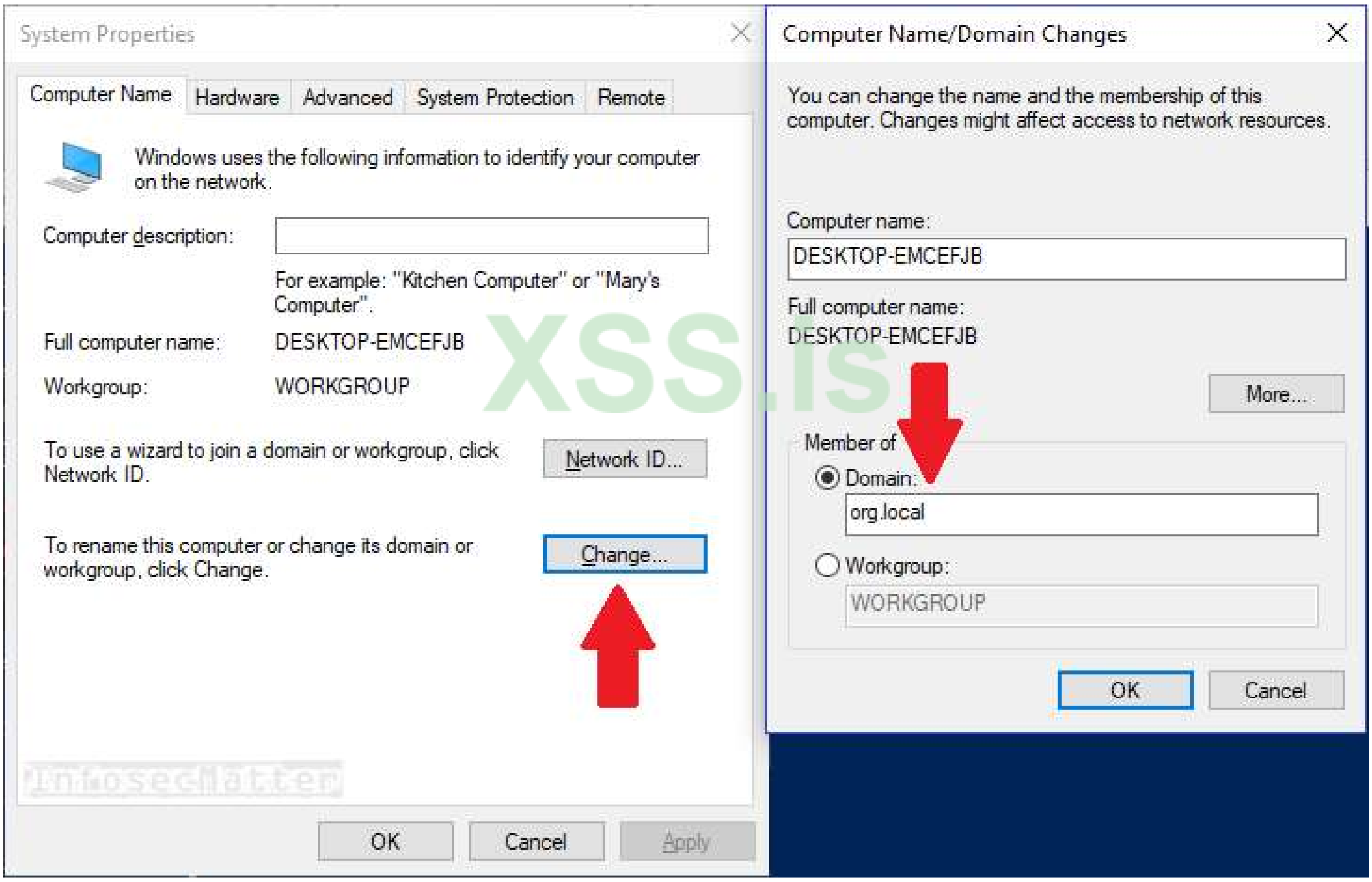
When you install Active Directory by default, any domain user can add workstations to the domain. This is determined by the ms-DS-MachineAccountQuota attribute, which is set to 10 by default.
This means that any user in a low-privileged domain can join up to 10 computers to the domain. Not really, well, probably, but what's the big deal?
The problem is that these settings allow any user to join their own unmanaged computer to access the corporate domain with the following benefits:

- Antivirus software or EDR solutions will not be downloaded to their machine.
- No settings or GPO policies will apply to their system.
- Allows them to have administrator privileges on their system

In enterprise environments, users should never have local administrator privileges on their machines. This is one of the fundamental security measures that should be applied everywhere.
If users have administrative privileges on their machines, they can perform privileged operations on the network, such as creating raw network packets, performing network scans, running exploits from their machine to attack other systems on the network, and more.
Therefore, users should never be allowed to join computers to the domain.

How to check

The easiest way to test this is to connect the Windows test machine (physical or virtual) to the target corporate network so that it can connect to domain controllers.
1) Run sysdm.cpl to open "System Properties" -> click "Edit" and specify the name of the target domain:



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: DESKTOP-EMCEFJB

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: DESKTOP-EMCEFJB

Full computer name: DESKTOP-EMCEFJB

Member of

● Domain: org.local

○ Workgroup: WORKGROUP

Click OK.
2) We will now be prompted to enter our credentials.
Provide any credentials for a low-privileged domain user.
If successful, we should see the message "Welcome to the domain org.local!" message, and our test machine should be added to AD in the container CN =
Computers.
Alternatively, we can also attach our test machine to AD using the following PowerShell command:

Code: Copy to clipboard

```
add-computer -domainname <FQDN-DOMAIN> -Credential <DOMAIN>\<USER> -restart -force

# Пример
add-computer -domainname org.local -Credential ORG\john -restart -force
```

After restarting our test machine, the machine must be fully joined to the domain.
3) Now we should be able to check whether our computer has actually been added to the domain by listing the domain

computers.
Note that if we had access to domain controllers, here's how we could list all the computers that were added by non-administrators:

Code: Copy to clipboard

```
Import-Module ActiveDirectory
Get-ADComputer -LDAPFilter "(ms-DS-CreatorSID=*)" -Properties ms-DS-CreatorSID
```

2. The AdminCount attribute is set for standard users.

The AdminCount attribute in Active Directory is used to protect administrative users and members of a privileged group, for example:

- Domain Admins
- Enterprise Admins
- Schema Admins
- Backup Operators
- Server Operators
- Replicator
- and the like

The problem is that the AdminCount attribute is automatically set to 1 when a user is assigned to a privileged group, but it is never reset automatically when a user is removed from those groups.

How to check

To find users with an AdminCount attribute of 1, we can use the LDAPDomainDump tool. This tool collects important information about all users, groups, and computers in the domain. 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) First collect information from the domain
controller:

Python: Copy to clipboard

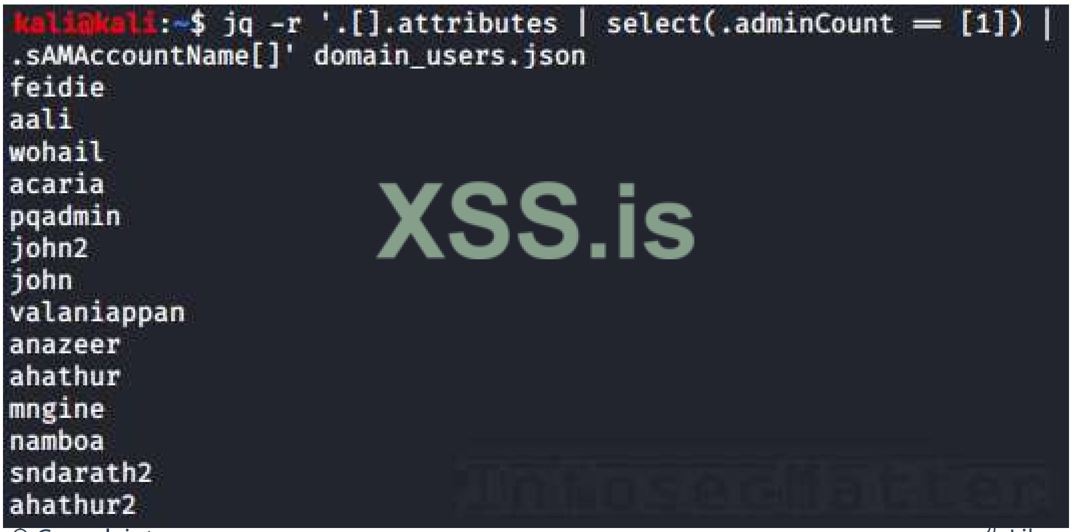
```
python ldapdomaindump.py -u <DOMAIN>\\<USER> -p <PASS> -d <DELIMITER> <DC-IP>

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

(we could easily pass the password hash)
2) After the collection is complete, we can get a list of users with the AdminCount attribute equal to 1 by analyzing the domain_users.json
file:

Code: Copy to clipboard

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



```
kali@kali:~$ jq -r '.[].attributes | select(.adminCount == [1]) |
.sAMAccountName[]' domain_users.json
feidie
aali
wohail
acaria
pqadmin
john2
john
valaniappan
anazeer
ahathur
mngine
namboa
sndarath2
ahathur2
```

Complaint Like + Quotation Answer

Alternatively, if we have access to a domain controller, we can get a list of these users as follows:

Artem N, SEAdm1n, morsmros and 12 more

Code: Copy to clipboard

Dilock

RAID User

25.08.2021 New #2

On this the first part is over, so far only to put a fishing rod, I want to hear feedback and recommendations. If it comes in, I'll continue without a problem!)

Very useful. Handsome TS

Last edited: 8/25/2021

Complaint Like + Quotation Answer

valeraleontev

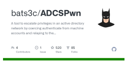
pqk veawo

CD User

25.08.2021 New #3

Do you think reprinting a well-known book is a good idea?) Add the kind of fordiion of different types such

Hidden content for registered users.



GitHub - bats3c/ADCSPwn: A tool to escalate privileges in an active directory net...

A tool to escalate privileges in an active directory network by coercing authenticate from machine accounts and relaying to the certificate service. - GitHub - bats3c/ADCSPwn: A tool to escalate pr...

github.com

Complaint Like + Quotation Answer

> valeraleontev

valeraleontev

RAID User

25.08.2021 New #4

> pqk veawo said:
>
> Do you think reprinting a well-known book is a good idea?) Add a blassy of different types such Hidden Content

Interesting, but there is an interesting thing. You can easily grab the hash of the admin with the responder, initiating a request for an antivirus scan to any file. I don't know how it is now, I've retired, but it has to work. If it takes and there is time, I can throw an article on the promotion of privileges

Complaint Like + Quotation Answer

valeraleontev

RAID User

25.08.2021 New #5

> Dilock said:
>
> Very useful. Handsome TS

Thanks) Tomorrow I will try to post the second part here

Complaint Like + Quotation Answer

pqk veawo

CD User

25.08.2021 New #6

> valeraleontev said: ⊕
>
> Interesting, but there is an interesting thing. You can easily grab the hash of the admin with the responder, initiating a request for an antivirus scan to any file. I don't know how it is now, I've retired, but it has to work. If it takes and there is time, I can throw an article on the promotion of privileges

Yeah, interesting. Its use fits well into the context. I suggest you take the video below as the basis for your next opus) success.

> Hidden content for users: valeraleontev.

Complaint Like + Quotation Answer

> fordf2544

valeraleontev

RAID User

25.08.2021 New #7

> pqk veawo said: ⊕
>
> Yeah, interesting. Its use fits well into the context. I suggest you take the video below as the basis for your next opus) success.Hidden content

Accepted, friend

> Hidden content for users: pqk veawo.

Complaint Like + Quotation Answer

valeraleontev

RAID User

25.08.2021 New #8

Posted the second part - https://xss.is/threads/55849/

🔔 Complaint 👍 Like + Quotation ↩ Answer

Scully

Premium Premium

26.08.2021 New #9

> valeraleontev said:
>
> Interesting, but there is an interesting thing. You can easily grab the hash of the admin with the responder, initiating a request for an antivirus scan to any file. I don't know how it is now, I've retired, but it has to work. If it takes and there is time, I can throw an article on the promotion of privileges

Let's talk about raising privileges, thank you for wasting your time on this. It will be very useful for beginners and not only.

🔔 Complaint 👍 Like + Quotation ↩ Answer

valeraleontev

RAID User

26.08.2021 New #10

> Scully said:
>
> Let's talk about raising privileges, thank you for wasting your time on this. It will be very useful for beginners and not only.

Okay, no problem. I'll also try to link privileges to hell, I'll throw a draft closer to the weekend and post next week.

🔔 Complaint 👍 Like + Quotation ↩ Answer

valeraleontev

RAID User

26.08.2021 New #11

third part, friends! https://xss.is/threads/55891/

Complaint

Like + Quotation Answer

Write an answer...

Attach files

Answer

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