Predict | Protect | Prevent

ARCON|PAM

ARCON|CLI Proxy

arcon

Table of Contents

1 Overview 4
1.1 Accessing the SSH Services 4

Disclaimer

The handbook of ARCON PAM solution is being published to guide stakeholders and users. If any of the statements in this document are at variance or inconsistent it shall be brought to the notice of ARCON through the support team. Wherever appropriate, references have been made to facilitate a better understanding of the PAM solution. ARCON team has made every effort to ensure that the information contained in it was correct at the time of publishing.

Nothing in this document constitutes a guarantee, warranty, or license, expressed or implied. ARCON disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non-infringement of intellectual property or other rights of any third party or of ARCON; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of ARCON.

Copyright Notice

ARCON retains the right to make changes to this document at any time without notice. ARCON makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Trademarks

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

Sales Contact

You can directly contact us with sales-related topics at the email address <sales@arconnet.com>, or leave us your contact information and we will call you back.

1 Overview

The ARCON|CLIProxy module improves the efficiency and ease to taking connections to *nix systems a 100 fold. This module allows an end user/ bot etc use the command line/ tools like MobaXterm, SecureCRT to not only authenticate a user in PAM but also establish a connection to any *nix target device. Since this does not require a login to the Web console of ARCON | PAM, it is being welcomed by a lot of our clients since it is easing their automation projects(all organizations seem to be running them lately) tremendously. The ARCON | CLI is also very powerful because previously if we were able to apply restriction policies only on sessions executed through the ARCON putty, we are now able to not only monitor but also control all sessions taken from any source. This allows administrators to connect to the target device - as they would do so without the pam, hence acceptance of PAM solutions also becomes easier.

⚠ Currently, either SMS or Email OTP can be configured (A Single Dual-Factor Authentication) at a given instance.

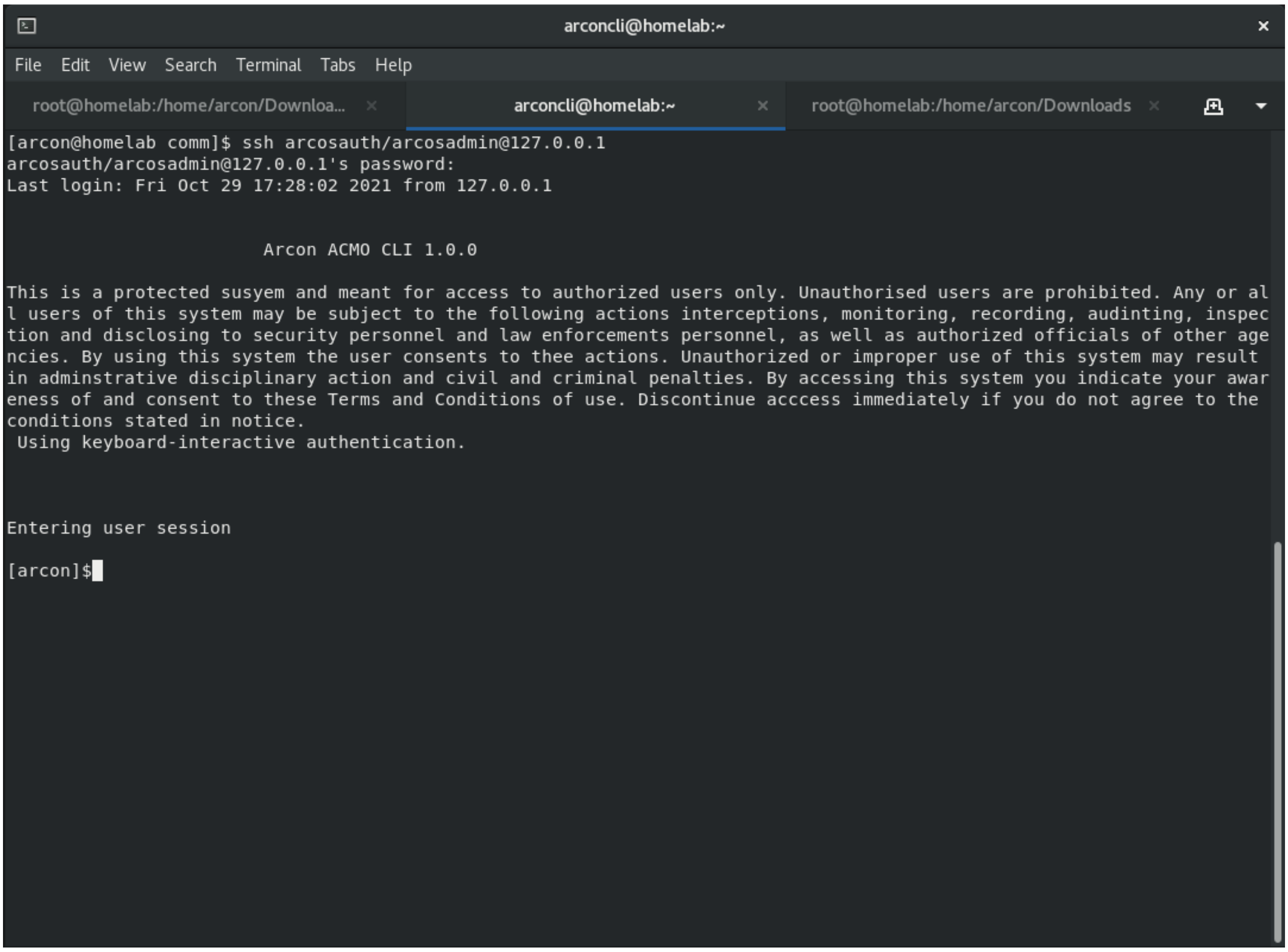
ACMO CLI helps us to audit services accessed and log commands that were triggered by the end-user in the ACMO Reports or Server Manager.

1.1 Accessing the SSH Services

To access the SSH nodes, follow the below steps:

1. Open any SSH-supported software, for example, Putty/WinFIOL/Mobaexterm/SecureCRT to login to the ARCON PAM Console and then, type the gateway LB IP.

ⓘ Login through the SSH Console for SSH nodes with AD/ARCOSAUTH credentials as shown in the image below.

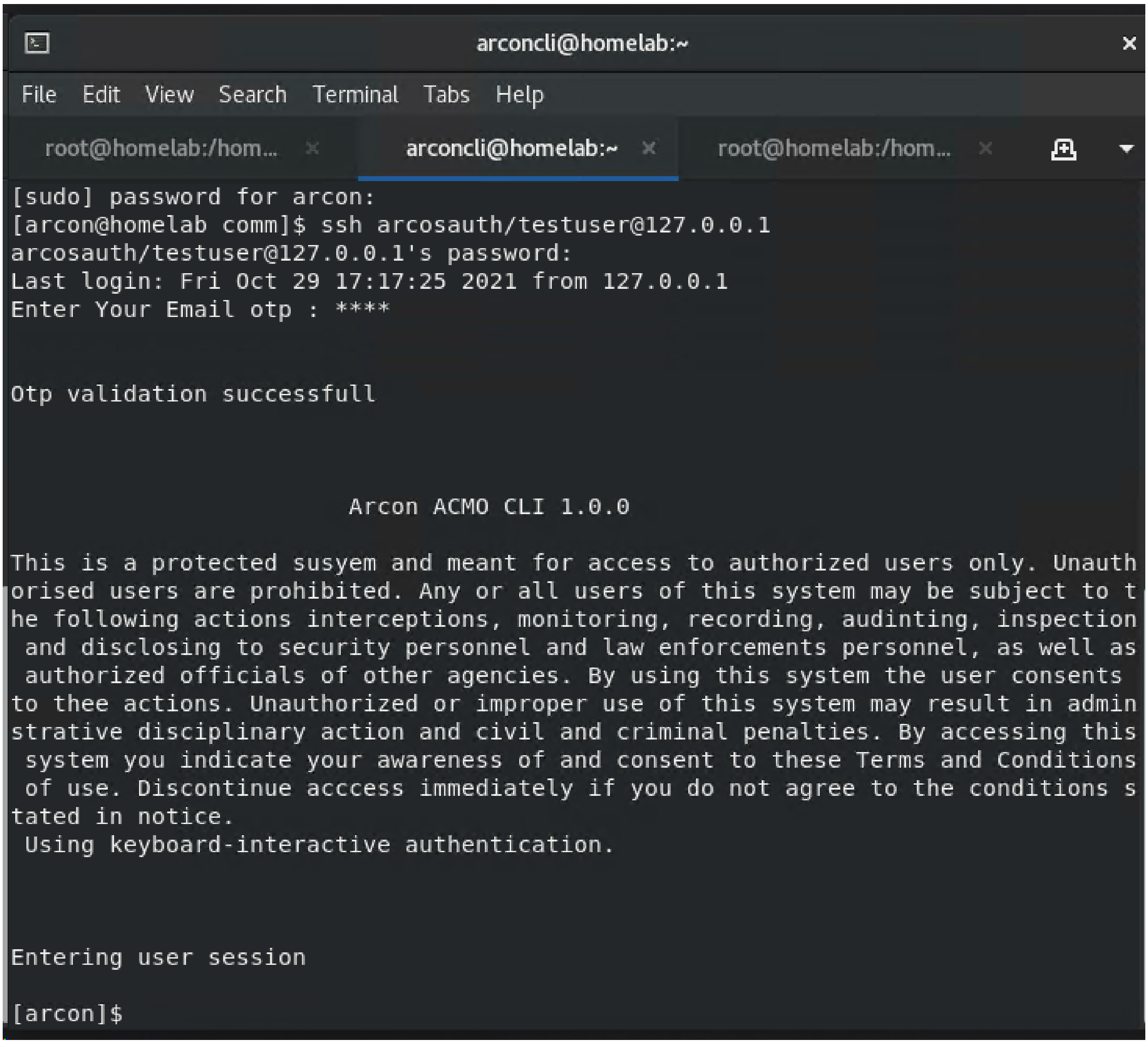


arconcli@homelab:~
File Edit View Search Terminal Tabs Help
root@homelab:/home/arcon/Downloa...
arconcli@homelab:~
root@homelab:/home/arcon/Downloads

```
[arcon@homelab comm]$ ssh arcosauth/arcosadmin@127.0.0.1
arcosauth/arcosadmin@127.0.0.1's password:
Last login: Fri Oct 29 17:28:02 2021 from 127.0.0.1


                        Arcon ACMO CLI 1.0.0

This is a protected susyem and meant for access to authorized users only. Unauthorised users are prohibited. Any or al
l users of this system may be subject to the following actions interceptions, monitoring, recording, audinting, inspec
tion and disclosing to security personnel and law enforcements personnel, as well as authorized officials of other age
ncies. By using this system the user consents to thee actions. Unauthorized or improper use of this system may result
in adminstrative disciplinary action and civil and criminal penalties. By accessing this system you indicate your awar
eness of and consent to these Terms and Conditions of use. Discontinue acccess immediately if you do not agree to the
conditions stated in notice.
 Using keyboard-interactive authentication.



Entering user session

[arcon]$
```

2. Enter the SMS or Email OTP. The authentication is processed the same as ACMO.

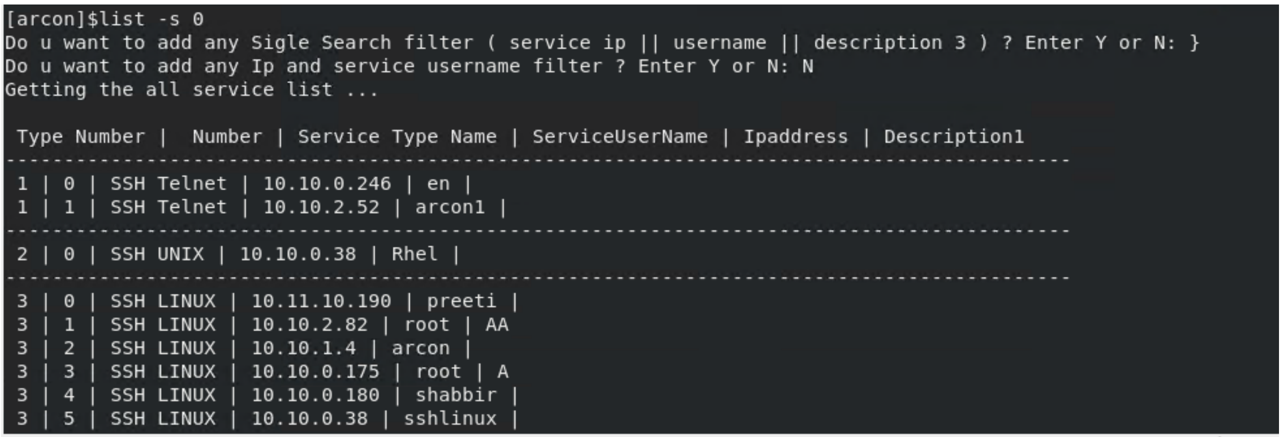
⚠ If Two-Factor Authentication is configured, then the same needs to be entered in the CLI window for successful authentication.



```
[sudo] password for arcon:
[arcon@homelab comm]$ ssh arcosauth/testuser@127.0.0.1
arcosauth/testuser@127.0.0.1's password:
Last login: Fri Oct 29 17:17:25 2021 from 127.0.0.1
Enter Your Email otp : ****


Otp validation successfull



                        Arcon ACMO CLI 1.0.0

This is a protected susyem and meant for access to authorized users only. Unauth
orised users are prohibited. Any or all users of this system may be subject to t
he following actions interceptions, monitoring, recording, audinting, inspection
 and disclosing to security personnel and law enforcements personnel, as well as
 authorized officials of other agencies. By using this system the user consents
to thee actions. Unauthorized or improper use of this system may result in admin
strative disciplinary action and civil and criminal penalties. By accessing this
 system you indicate your awareness of and consent to these Terms and Conditions
 of use. Discontinue acccess immediately if you do not agree to the conditions s
tated in notice.
 Using keyboard-interactive authentication.



Entering user session

[arcon]$
```

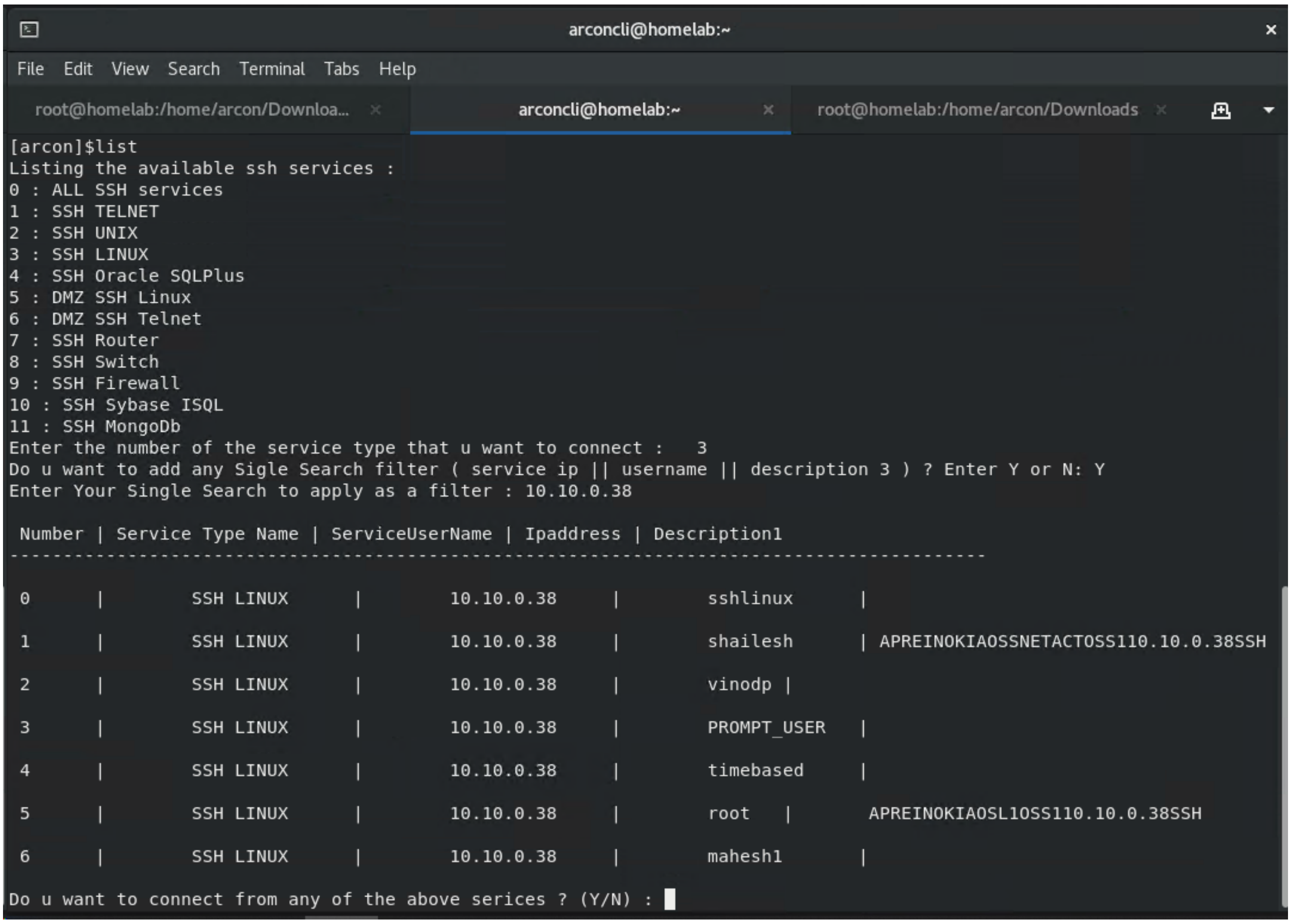
3. Type the **list -s 0** command. A list of all assigned SSH services across LOB appears on the screen.

> Or you can filter the node by typing the command **list** <required node> (via Ip or Description1).
>
> Post login, there will be a wildcard-based node listing. The information on the CLI screen is displayed as shown below:
>
> **Type Number | Number | Service Type Name | ServicerUserName | Ipaddress | Description1**

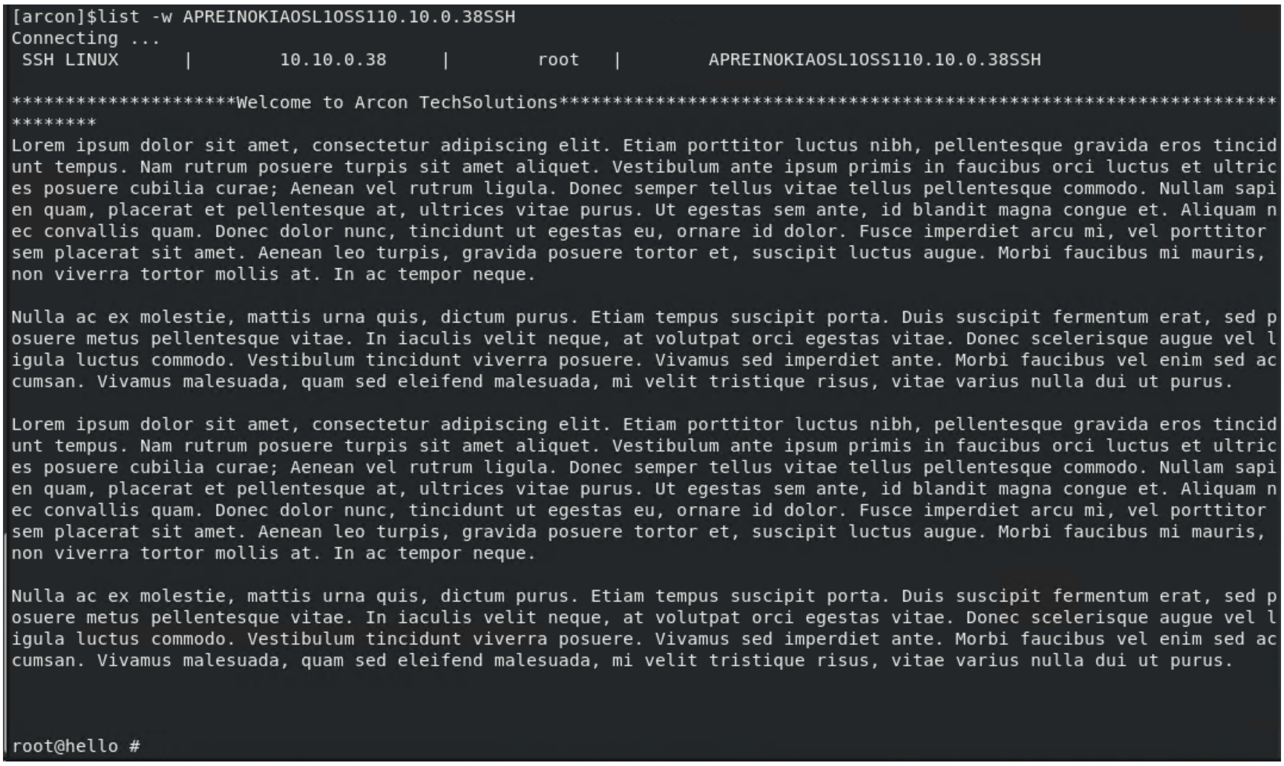


```
[arcon]$list -s 0
Do u want to add any Sigle Search filter ( service ip || username || description 3 ) ? Enter Y or N: }
Do u want to add any Ip and service username filter ? Enter Y or N: N
Getting the all service list ...

 Type Number |  Number | Service Type Name | ServiceUserName | Ipaddress | Description1
-------------------------------------------------------------------------------------------
 1 | 0 | SSH Telnet | 10.10.0.246 | en |
 1 | 1 | SSH Telnet | 10.10.2.52 | arcon1 |
-------------------------------------------------------------------------------------------
 2 | 0 | SSH UNIX | 10.10.0.38 | Rhel |
-------------------------------------------------------------------------------------------
 3 | 0 | SSH LINUX | 10.11.10.190 | preeti |
 3 | 1 | SSH LINUX | 10.10.2.82 | root | AA
 3 | 2 | SSH LINUX | 10.10.1.4 | arcon |
 3 | 3 | SSH LINUX | 10.10.0.175 | root | A
 3 | 4 | SSH LINUX | 10.10.0.180 | shabbir |
 3 | 5 | SSH LINUX | 10.10.0.38 | sshlinux |
```

Without displaying the list, you can also search for a specific IP from CLI by typing **list x.x.x.x** or **list hostname** or whatever value from the information displayed above.


arconcli@homelab:~
File Edit View Search Terminal Tabs Help
root@homelab:/home/arcon/Downloa...
arconcli@homelab:~
root@homelab:/home/arcon/Downloads

```
[arcon]$list
Listing the available ssh services :
0 : ALL SSH services
1 : SSH TELNET
2 : SSH UNIX
3 : SSH LINUX
4 : SSH Oracle SQLPlus
5 : DMZ SSH Linux
6 : DMZ SSH Telnet
7 : SSH Router
8 : SSH Switch
9 : SSH Firewall
10 : SSH Sybase ISQL
11 : SSH MongoDb
Enter the number of the service type that u want to connect :   3
Do u want to add any Sigle Search filter ( service ip || username || description 3 ) ? Enter Y or N: Y
Enter Your Single Search to apply as a filter : 10.10.0.38

 Number | Service Type Name | ServiceUserName | Ipaddress | Description1
-------------------------------------------------------------------------------------------

 0      |        SSH LINUX      |        10.10.0.38     |        sshlinux      |

 1      |        SSH LINUX      |        10.10.0.38     |        shailesh      | APREINOKIAOSSNETACTOSS110.10.0.38SSH

 2      |        SSH LINUX      |        10.10.0.38     |        vinodp |

 3      |        SSH LINUX      |        10.10.0.38     |        PROMPT_USER   |

 4      |        SSH LINUX      |        10.10.0.38     |        timebased     |

 5      |        SSH LINUX      |        10.10.0.38     |        root   |       APREINOKIAOSL1OSS110.10.0.38SSH

 6      |        SSH LINUX      |        10.10.0.38     |        mahesh1       |

Do u want to connect from any of the above serices ? (Y/N) :
```



```
[arcon]$list -w APREINOKIAOSL1OSS110.10.0.38SSH
Connecting ...
 SSH LINUX      |        10.10.0.38     |        root   |        APREINOKIAOSL1OSS110.10.0.38SSH

*********************Welcome to Arcon TechSolutions*******************************************************************
********
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam porttitor luctus nibh, pellentesque gravida eros tincid
unt tempus. Nam rutrum posuere turpis sit amet aliquet. Vestibulum ante ipsum primis in faucibus orci luctus et ultric
es posuere cubilia curae; Aenean vel rutrum ligula. Donec semper tellus vitae tellus pellentesque commodo. Nullam sapi
en quam, placerat et pellentesque at, ultrices vitae purus. Ut egestas sem ante, id blandit magna congue et. Aliquam n
ec convallis quam. Donec dolor nunc, tincidunt ut egestas eu, ornare id dolor. Fusce imperdiet arcu mi, vel porttitor
sem placerat sit amet. Aenean leo turpis, gravida posuere tortor et, suscipit luctus augue. Morbi faucibus mi mauris,
non viverra tortor mollis at. In ac tempor neque.

Nulla ac ex molestie, mattis urna quis, dictum purus. Etiam tempus suscipit porta. Duis suscipit fermentum erat, sed p
osuere metus pellentesque vitae. In iaculis velit neque, at volutpat orci egestas vitae. Donec scelerisque augue vel l
igula luctus commodo. Vestibulum tincidunt viverra posuere. Vivamus sed imperdiet ante. Morbi faucibus vel enim sed ac
cumsan. Vivamus malesuada, quam sed eleifend malesuada, mi velit tristique risus, vitae varius nulla dui ut purus.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam porttitor luctus nibh, pellentesque gravida eros tincid
unt tempus. Nam rutrum posuere turpis sit amet aliquet. Vestibulum ante ipsum primis in faucibus orci luctus et ultric
es posuere cubilia curae; Aenean vel rutrum ligula. Donec semper tellus vitae tellus pellentesque commodo. Nullam sapi
en quam, placerat et pellentesque at, ultrices vitae purus. Ut egestas sem ante, id blandit magna congue et. Aliquam n
ec convallis quam. Donec dolor nunc, tincidunt ut egestas eu, ornare id dolor. Fusce imperdiet arcu mi, vel porttitor
sem placerat sit amet. Aenean leo turpis, gravida posuere tortor et, suscipit luctus augue. Morbi faucibus mi mauris,
non viverra tortor mollis at. In ac tempor neque.

Nulla ac ex molestie, mattis urna quis, dictum purus. Etiam tempus suscipit porta. Duis suscipit fermentum erat, sed p
osuere metus pellentesque vitae. In iaculis velit neque, at volutpat orci egestas vitae. Donec scelerisque augue vel l
igula luctus commodo. Vestibulum tincidunt viverra posuere. Vivamus sed imperdiet ante. Morbi faucibus vel enim sed ac
cumsan. Vivamus malesuada, quam sed eleifend malesuada, mi velit tristique risus, vitae varius nulla dui ut purus.



root@hello #
```

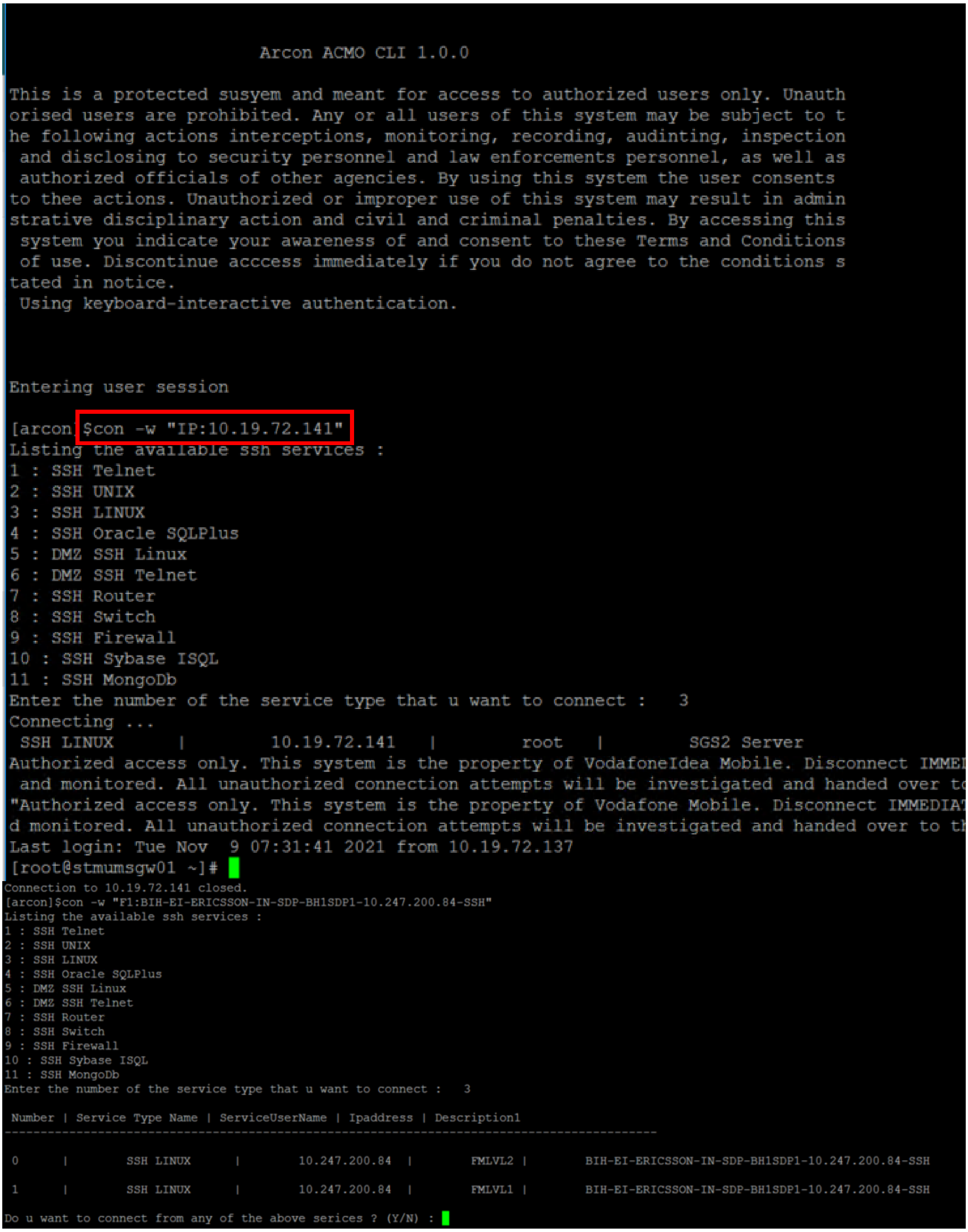
4. From the list of servers that are displayed, select the server by typing the commands shown below:

con -w "<parameter 1>:<paramter 2"
list -w "<parameter 1>:<paramter 2".

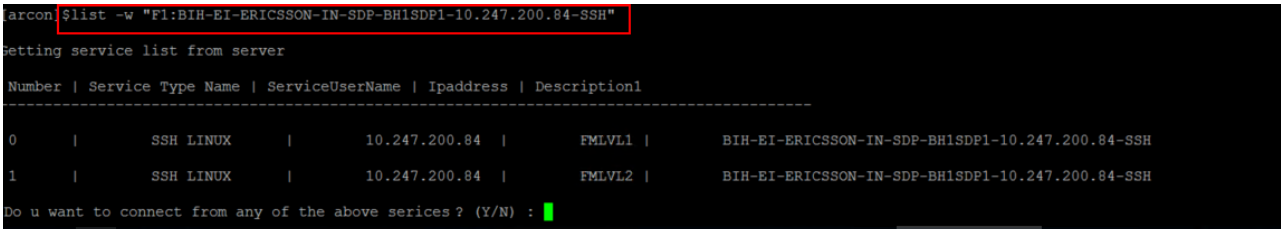
ⓘ Here, Parameter 1 is the wildcard value from which you want to filter out the service. Following are the 5 values supported:

- IP: Stands for IP
- UN: Stands for target server username
- F1: Description 1 of the service
- F2: Description 2 of the service
- F3: Description 3 of the service

Parameter 2 is the actual value you would enter, which needs to be filtered out.
For example:
con -w "IP:1.1.1.1"
list -w "UN:root"



```
                        Arcon ACMO CLI 1.0.0

This is a protected susyem and meant for access to authorized users only. Unauth
orised users are prohibited. Any or all users of this system may be subject to t
he following actions interceptions, monitoring, recording, audinting, inspection
 and disclosing to security personnel and law enforcements personnel, as well as
 authorized officials of other agencies. By using this system the user consents
to thee actions. Unauthorized or improper use of this system may result in admin
strative disciplinary action and civil and criminal penalties. By accessing this
 system you indicate your awareness of and consent to these Terms and Conditions
 of use. Discontinue acccess immediately if you do not agree to the conditions s
tated in notice.
 Using keyboard-interactive authentication.



Entering user session

[arcon]$con -w "IP:10.19.72.141"
Listing the available ssh services :
1 : SSH Telnet
2 : SSH UNIX
3 : SSH LINUX
4 : SSH Oracle SQLPlus
5 : DMZ SSH Linux
6 : DMZ SSH Telnet
7 : SSH Router
8 : SSH Switch
9 : SSH Firewall
10 : SSH Sybase ISQL
11 : SSH MongoDb
Enter the number of the service type that u want to connect :   3
Connecting ...
 SSH LINUX     |         10.19.72.141    |         root    |         SGS2 Server
Authorized access only. This system is the property of VodafoneIdea Mobile. Disconnect IMMEI
 and monitored. All unauthorized connection attempts will be investigated and handed over to
"Authorized access only. This system is the property of Vodafone Mobile. Disconnect IMMEDIAT
d monitored. All unauthorized connection attempts will be investigated and handed over to th
Last login: Tue Nov  9 07:31:41 2021 from 10.19.72.137
[root@stmumsgw01 ~]# 
Connection to 10.19.72.141 closed.
[arcon]$con -w "F1:BIH-EI-ERICSSON-IN-SDP-BH1SDP1-10.247.200.84-SSH"
Listing the available ssh services :
1 : SSH Telnet
2 : SSH UNIX
3 : SSH LINUX
4 : SSH Oracle SQLPlus
5 : DMZ SSH Linux
6 : DMZ SSH Telnet
7 : SSH Router
8 : SSH Switch
9 : SSH Firewall
10 : SSH Sybase ISQL
11 : SSH MongoDb
Enter the number of the service type that u want to connect :   3

 Number | Service Type Name | ServiceUserName | Ipaddress | Description1
---------------------------------------------------------------------------------------------

 0      |         SSH LINUX      |         10.247.200.84  |         FMLVL2 |        BIH-EI-ERICSSON-IN-SDP-BH1SDP1-10.247.200.84-SSH

 1      |         SSH LINUX      |         10.247.200.84  |         FMLVL1 |        BIH-EI-ERICSSON-IN-SDP-BH1SDP1-10.247.200.84-SSH

Do u want to connect from any of the above serices ? (Y/N) : 
```

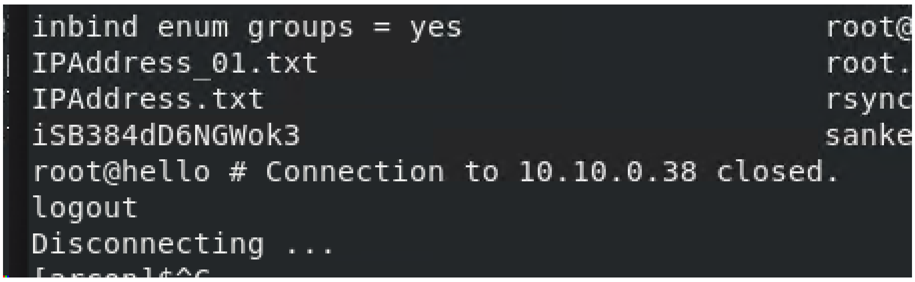


```
[arcon]$list -w "F1:BIH-EI-ERICSSON-IN-SDP-BH1SDP1-10.247.200.84-SSH"

Getting service list from server

 Number | Service Type Name | ServiceUserName | Ipaddress | Description1
------------------------------------------------------------------------------------------

 0      |       SSH LINUX     |        10.247.200.84  |        FMLVL1 |       BIH-EI-ERICSSON-IN-SDP-BH1SDP1-10.247.200.84-SSH

 1      |       SSH LINUX     |        10.247.200.84  |        FMLVL2 |       BIH-EI-ERICSSON-IN-SDP-BH1SDP1-10.247.200.84-SSH

Do u want to connect from any of the above serices ? (Y/N) :
```

ⓘ Once written, the CLI PAM will select that service and route the connections via the same putty to the target server via the PAM gateway.

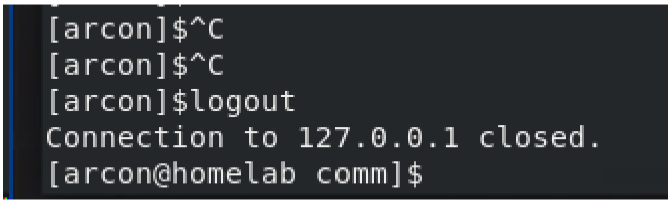
5. Press **Ctrl+D** to end or exit the session from the current server and return to the PAM CLI landing page. Here, you can select some other server from Point B.

ⓘ Disconnect from the gateway by typing the CTRL+D / exit command.



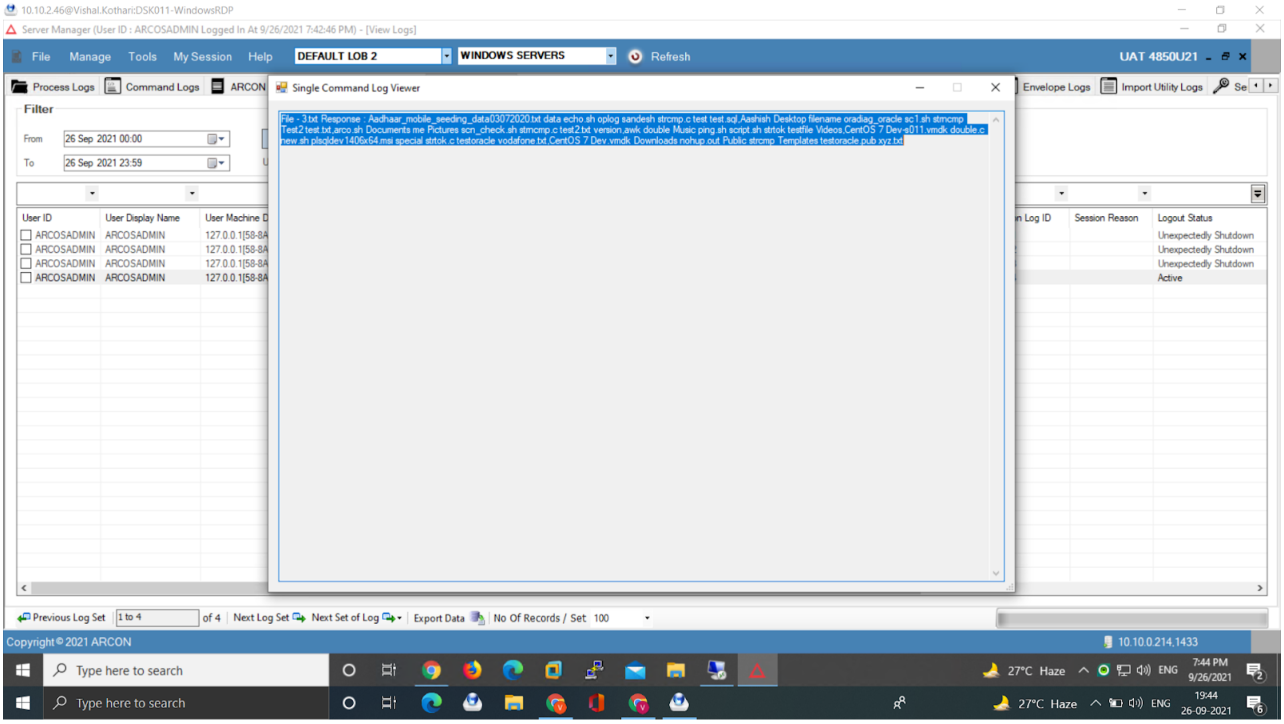
```
inbind enum groups = yes                       root@
IPAddress_01.txt                               root.
IPAddress.txt                                  rsync
iSB384dD6NGWok3                                sanke
root@hello # Connection to 10.10.0.38 closed.
logout
Disconnecting ...
```

ⓘ Disconnect from the target by typing CTRL+D /exit command. The CLI gets closed by killing the target server connection.



```
[arcon]$^C
[arcon]$^C
[arcon]$logout
Connection to 127.0.0.1 closed.
[arcon@homelab comm]$
```

ⓘ The entire session of input and output commands is recorded in PAM similar to the current functionality in ACMO or Server Manager.



From: 26 Sep 2021 00:00

To: 26 Sep 2021 23:59

User ID	User Display Name	User Machine D	n Log ID	Session Reason	Logout Status
□ ARCOSADMIN	ARCOSADMIN	127.0.0.1[58-8A			Unexpectedly Shutdown
□ ARCOSADMIN	ARCOSADMIN	127.0.0.1[58-8A			Unexpectedly Shutdown
□ ARCOSADMIN	ARCOSADMIN	127.0.0.1[58-8A			Unexpectedly Shutdown
□ ARCOSADMIN	ARCOSADMIN	127.0.0.1[58-8A			Active

```
File - 3.txt Response : Aadhaar_mobile_seeding_data03072020.txt data echo.sh oplog sandesh strcmp.c test test.sql,Aashish Desktop filename oradiag_oracle sc1.sh stmcmp
Test2 test.txt,arco.sh Documents me Pictures scn_check.sh stmcmp.c test2.txt version,awk double Music ping.sh script.sh strtok testfile Videos,CentOS 7 Dev-s011.vmdk double.c
new.sh plsqldev1406x64.msi special strtok.c testoracle vodafone.txt,CentOS 7 Dev.vmdk Downloads nohup.out Public strcmp Templates testoracle.pub xyz.txt
```

Privileged Access Management Suite

arcon

Predict | Protect | Prevent