

Karthick VM

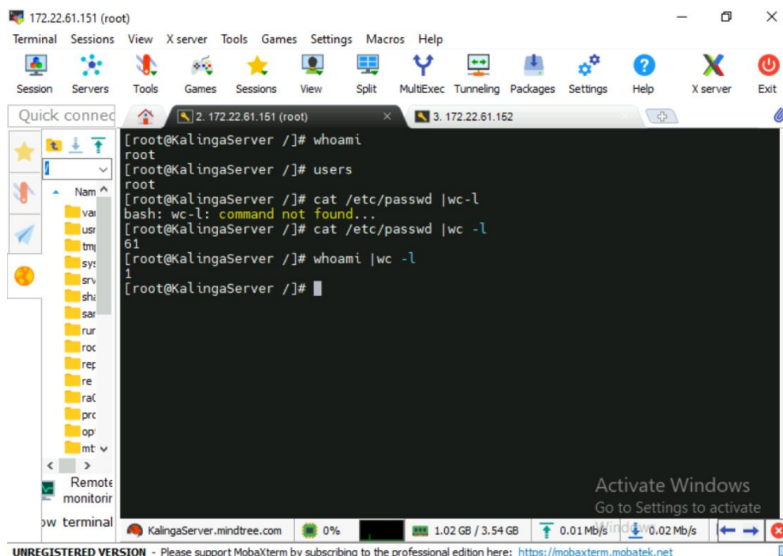
Batch – CIS -1.3

Mock Assessment -2 – Linux

Execute the following tasks

a. Display how many users logged in your machine

- #whoami – display current logged-in user – here:1
- At file : /etc/passwd we have the whole list of users in server – here:61

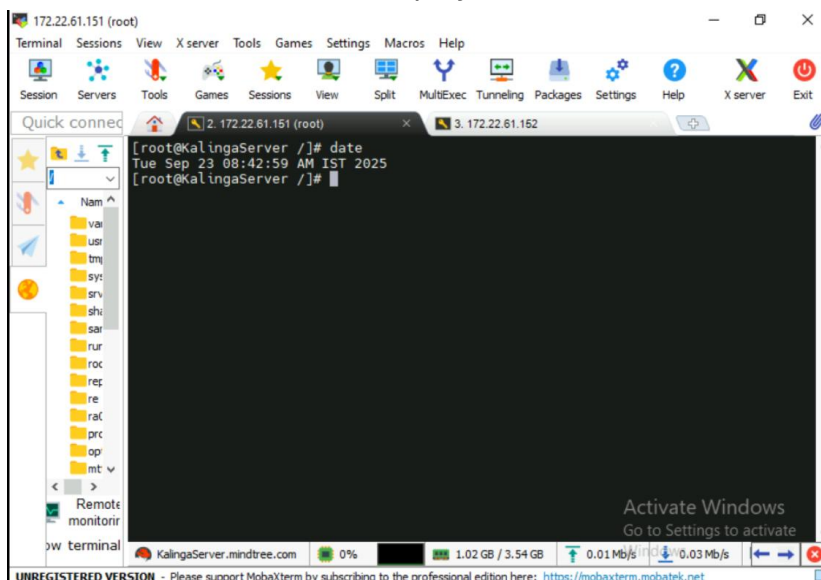


The screenshot shows a MobaXterm terminal window with the following commands and output:

```
[root@KalingaServer /]# whoami
root
[root@KalingaServer /]# users
root
[root@KalingaServer /]# cat /etc/passwd |wc -l
bash: wc -l: command not found...
[root@KalingaServer /]# cat /etc/passwd |wc -l
61
[root@KalingaServer /]# whoami |wc -l
1
[root@KalingaServer /]#
```

b. Display the Date and Time of Server Machine

- Command: #date – displays the date,time and timestamp

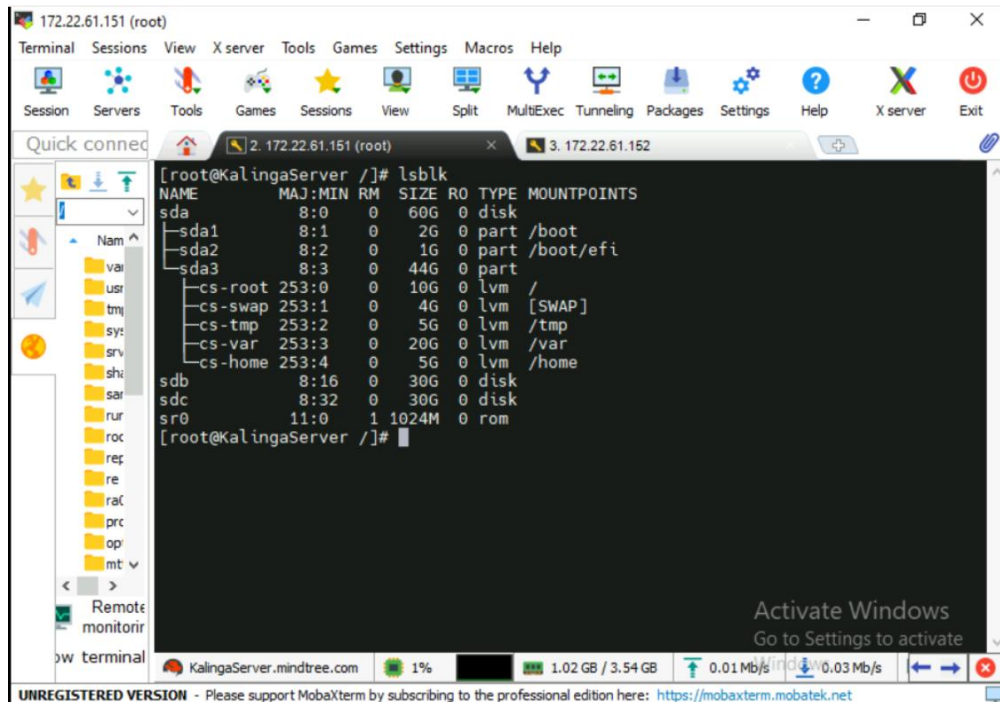


The screenshot shows a MobaXterm terminal window with the following command and output:

```
[root@KalingaServer /]# date
Tue Sep 23 08:42:59 AM IST 2025
[root@KalingaServer /]#
```

c. What is the command to check mounted partitions

- #lsblk – Displays the details of size of disk and details of partitioned disk with details of mount points.

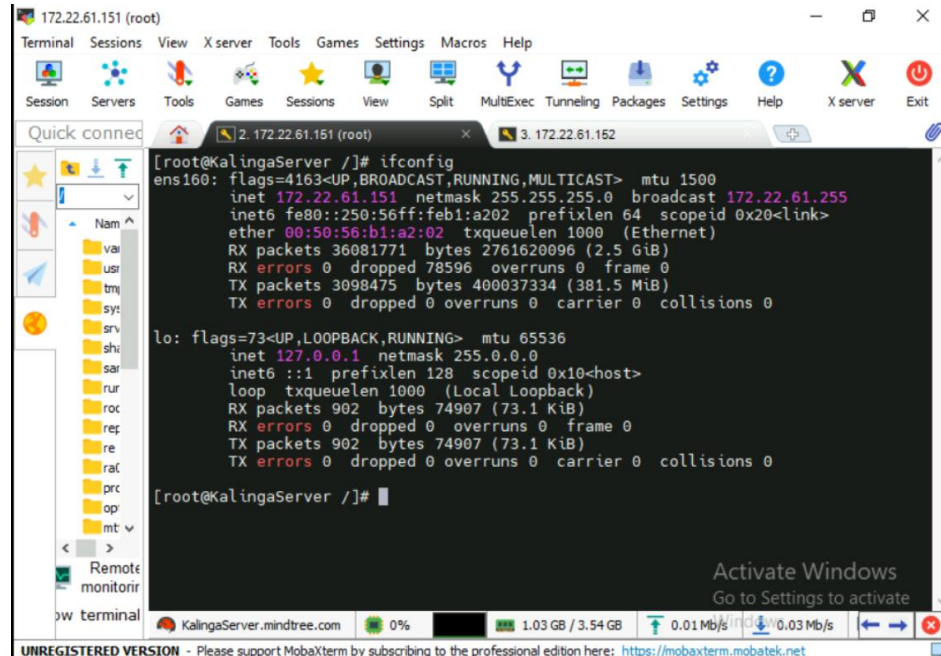


The screenshot shows a MobaXterm window with a terminal session on a Kali Linux server. The terminal displays the output of the `lsblk` command, which lists the details of the disk and its partitions, including their names, sizes, and mount points.

```
[root@KalingaServer ~]# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
sda          8:0    0   60G  0 disk
├─sda1       8:1    0    2G  0 part  /boot
├─sda2       8:2    0    1G  0 part  /boot/efi
└─sda3       8:3    0   44G  0 part
   ├─cs-root 253:0    0   10G  0 lvm    /
   ├─cs-swap 253:1    0    4G  0 lvm    [SWAP]
   ├─cs-tmp   253:2    0    5G  0 lvm    /tmp
   ├─cs-var   253:3    0   20G  0 lvm    /var
   └─cs-home  253:4    0    5G  0 lvm    /home
sdb          8:16   0   30G  0 disk
sdc          8:32   0   30G  0 disk
sr0         11:0    1 1024M  0 rom
```

d. Display the Ip configuration of both client and server

- Server – Command : #ipconfig



The screenshot shows a MobaXterm window with a terminal session on a Kali Linux server. The terminal displays the output of the `ifconfig` command, which shows the IP configuration for the `ens160` and `lo` interfaces.

```
[root@KalingaServer ~]# ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.22.61.151 netmask 255.255.255.0 broadcast 172.22.61.255
    inet6 fe80::250:56ff:feb1:a202 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:b1:a2:02 txqueuelen 1000 (Ethernet)
    RX packets 36081771 bytes 2761620096 (2.5 GiB)
    RX errors 0 dropped 78596 overruns 0 frame 0
    TX packets 3098475 bytes 400037334 (381.5 MiB)
    TX errors 0 dropped 0 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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 902 bytes 74907 (73.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 902 bytes 74907 (73.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@KalingaServer ~]#
```

- Client

The screenshot shows a MobaXterm terminal window with two sessions. The active session is '2. 172.22.61.151 (root)'. The terminal output shows the result of the 'ifconfig' command, displaying details for the 'ens160' and 'lo' network interfaces.

```
[root@KalingaClient ~]# ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.22.61.152 netmask 255.255.255.0 broadcast 172.22.61.255
    inet6 fe80::250:56ff:feb1:d85a prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:b1:d8:5a txqueuelen 1000 (Ethernet)
    RX packets 54207798 bytes 4113870093 (3.8 GiB)
    RX errors 0 dropped 119709 overruns 0 frame 0
    TX packets 1199913 bytes 138540389 (132.1 MiB)
    TX errors 0 dropped 0 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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 5208 bytes 411541 (401.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5208 bytes 411541 (401.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@KalingaClient ~]#
```

e. Display the content of /proc directory

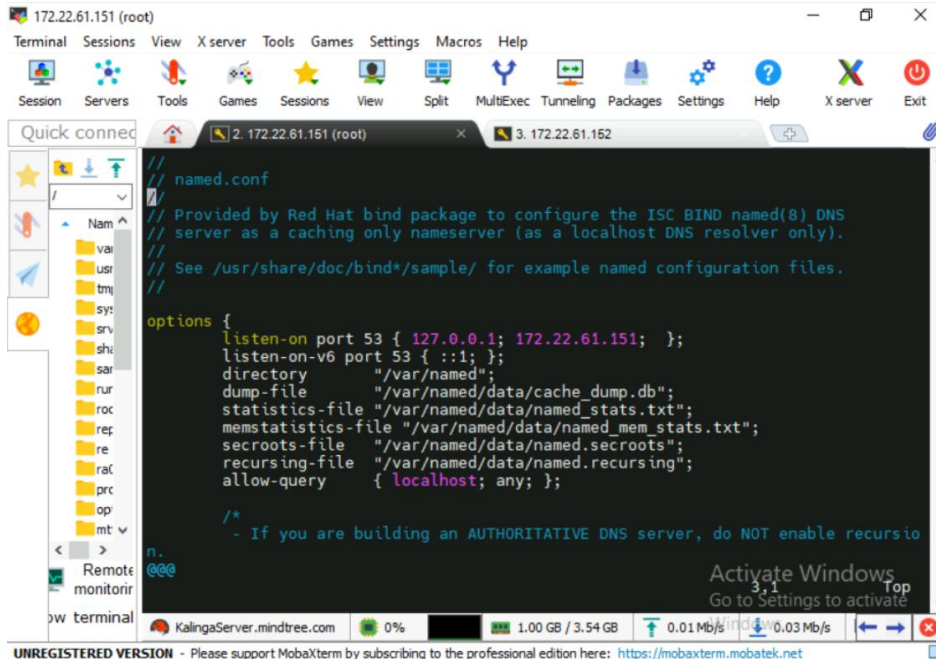
- #ls – This Command displays the contents present in the directory.

The screenshot shows a MobaXterm terminal window with two sessions. The active session is '2. 172.22.61.151 (root)'. The terminal output shows the result of the 'ls /proc' command, displaying a list of files and directories in the /proc directory.

```
[root@KalingaServer /]# ls /proc
1 16 1944441 2119 458 69 809 894 kallsyms
1064658 17 1944442 2128 459 7 81 896542 kcore
1064955 1790960 1944443 2140 46 70 810 9 keys
1073 1790961 1944444 23 461 71 811 90 key-users
1074 1790962 1944445 24 462 72 812 909 kmsg
108 1790963 1944446 25 47 73 813 91 kpagegroup
1082260 1794 1944447 26 49 733 814 92 kpagecount
1082262 18 1945704 27 5 734 815 93 kpageflags
1083 1804 1945795 29 50 735 816 94 loadavg
1086431 1811 1945797 3 51 74 817 940745 locks
1088 1812 1945867 34 52 745 818 940747 mdstat
1089 1815 1945872 35 53 746 819 940748 meminfo
1091 1841 1945873 36 533 747 82 95 misc
1093504 1872 1945874 37 54 75 820 951992 modules
1093505 1873 1945876 388493 540 76 821 96 mounts
1093506 1874 1945891 388494 55 77 83 97 mpt
1093507 1876 1945892 39 558 774 835 acpi
1093670 1883 1945928 394963 559 78 837 asound
11 1885 1945929 394971 56 787 84 bootconfig
1111 1888 1997 394972 560 788 85 buddyinfo
1126 1891 2 394973 561 789 86 bus
1128 1892 20 394974 562 79 863 cgroups
115 1894 2005135 394975 563 791 864 cmdline
116 1895 2017400 394976 564 793 865 consoles
```



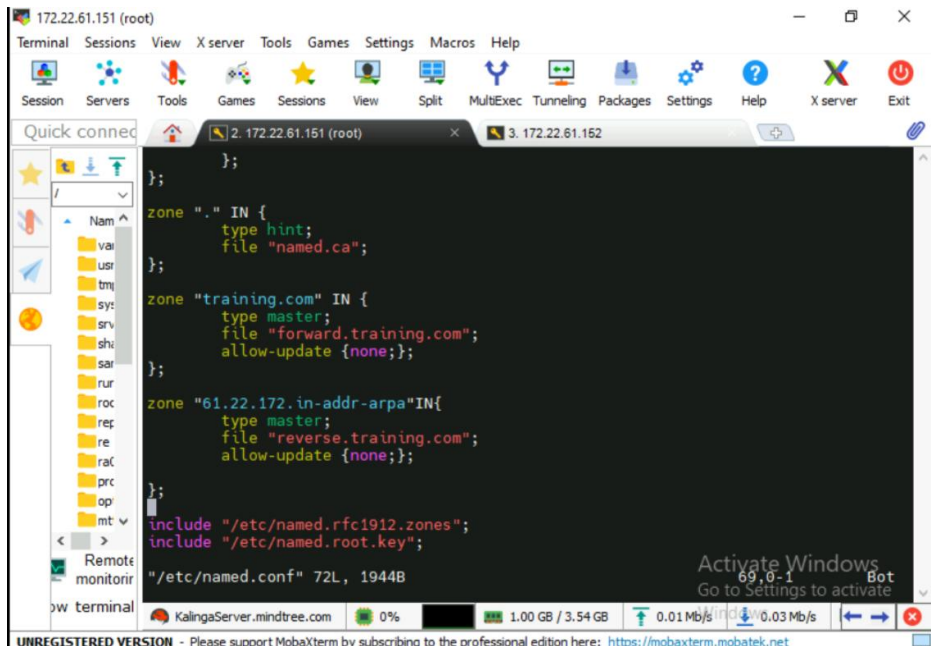
1. Install and configure DNS server and do the name resolution of both Server and client Machines.
  - Configure file -- /etc/named.conf
    - Add your ip in port 53 then add 'any;' in allow-query



The screenshot shows the MobaXterm interface with a terminal window displaying the contents of the `/etc/named.conf` file. The file is a configuration for the ISC BIND named(8) DNS server. It includes comments about its purpose and a reference to sample files. The `options` block is configured with `listen-on port 53` for `127.0.0.1` and `172.22.61.151`, and `listen-on-v6 port 53` for `::1`. It also sets various data files like `directory`, `dump-file`, `statistics-file`, `memstatistics-file`, `secroots-file`, and `recursing-file`. The `allow-query` is set to `{ localhost; any; }`. A comment at the bottom states: `/* - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion */`. The interface includes a sidebar with a file explorer, a top menu bar, and a status bar at the bottom.

```
// named.conf
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
options {
    listen-on port 53 { 127.0.0.1; 172.22.61.151; };
    listen-on-v6 port 53 { ::1; };
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    secroots-file "/var/named/data/named.secroots";
    recursing-file "/var/named/data/named.recursing";
    allow-query { localhost; any; };

    /*
     * - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion
     */
};
```



The screenshot shows the MobaXterm interface with a terminal window displaying the contents of the `/etc/named.conf` file. The file is a configuration for the ISC BIND named(8) DNS server. It includes comments about its purpose and a reference to sample files. The `options` block is configured with `listen-on port 53` for `127.0.0.1` and `172.22.61.151`, and `listen-on-v6 port 53` for `::1`. It also sets various data files like `directory`, `dump-file`, `statistics-file`, `memstatistics-file`, `secroots-file`, and `recursing-file`. The `allow-query` is set to `{ localhost; any; }`. A comment at the bottom states: `/* - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion */`. The interface includes a sidebar with a file explorer, a top menu bar, and a status bar at the bottom.

```
};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "training.com" IN {
    type master;
    file "forward.training.com";
    allow-update {none;};
};

zone "61.22.172.in-addr-arpa" IN {
    type master;
    file "reverse.training.com";
    allow-update {none;};
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

"/etc/named.conf" 72L, 1944B
```

- Configure file -- /var/named/forward.training.com and /var/named/reverse.training.com

The screenshot shows a MobaXterm window with a terminal session on a server at 172.22.61.151 (root). The terminal displays the configuration for the 'forward.training.com' zone in a BIND zone file. The configuration includes a \$TTL of 1D, an IN SOA record for 'server.training.com.', and several resource records: NS for 'server.training.com.', A records for 'server' and 'client' pointing to 172.22.61.151, and PTR records for '151' and '152' pointing to 'server.training.com.' and 'client.training.com.' respectively. The file size is 11L, 232B.

```

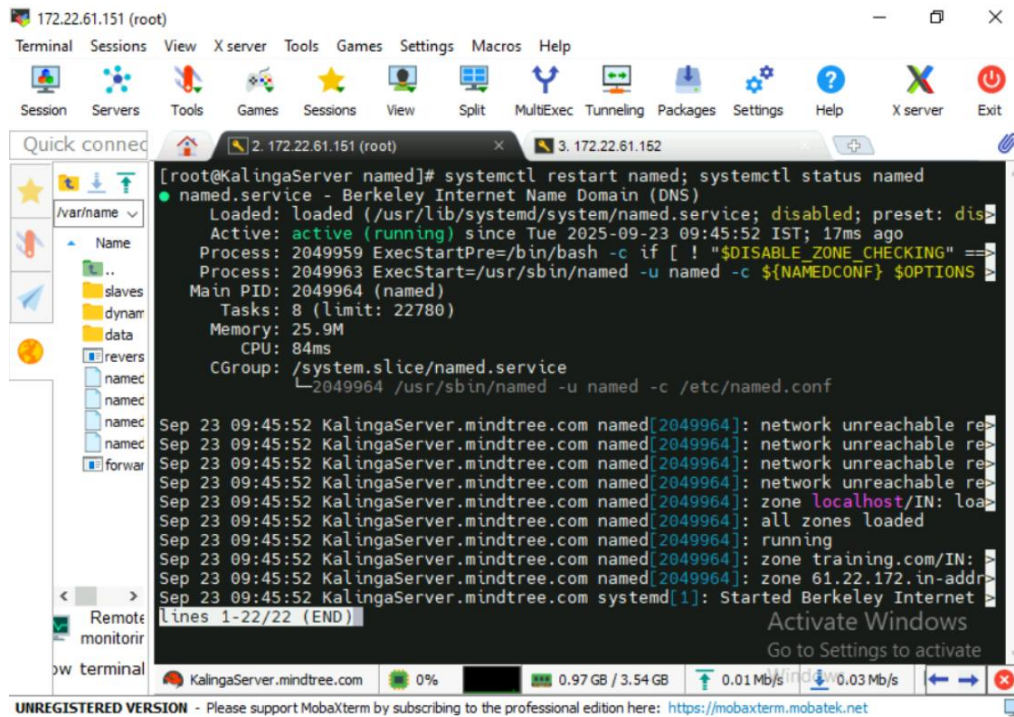
$TTL 1D
@ IN SOA server.training.com. (
    0      ; serial
    1D     ; refresh
    1H     ; retry
    1W     ; expire
    3H     ; minimum
)
@ IN NS   server.training.com.
@ IN A    172.22.61.151
server IN A 172.22.61.151
client IN A 172.22.61.152
"forward.training.com" 11L, 232B
  
```

The screenshot shows a MobaXterm window with a terminal session on a server at 172.22.61.151 (root). The terminal displays the configuration for the 'reverse.training.com' zone in a BIND zone file. The configuration includes a \$TTL of 1D, an IN SOA record for 'server.training.com.', and several resource records: NS for 'server.training.com.', PTR records for '151' and '152' pointing to 'server.training.com.' and 'client.training.com.' respectively, and A records for 'server' and 'client' pointing to 172.22.61.151. The file size is 14L, 319B.

```

$TTL 1D
@ IN SOA server.training.com. (
    0      ; serial
    1D     ; refresh
    1H     ; retry
    1W     ; expire
    3H     ; minimum
)
@ IN NS   server.training.com.
@ IN PTR  training.com.
@ IN A    172.22.61.151
server IN A 172.22.61.151
client IN A 172.22.61.152
151 IN PTR server.training.com.
152 IN PTR client.training.com.
"reverse.training.com" 14L, 319B
  
```

- Restart and check status of named using “systemctl”



The screenshot shows a MobaXterm window with a terminal session on a Kali Linux server (172.22.61.151). The user has executed the following commands:

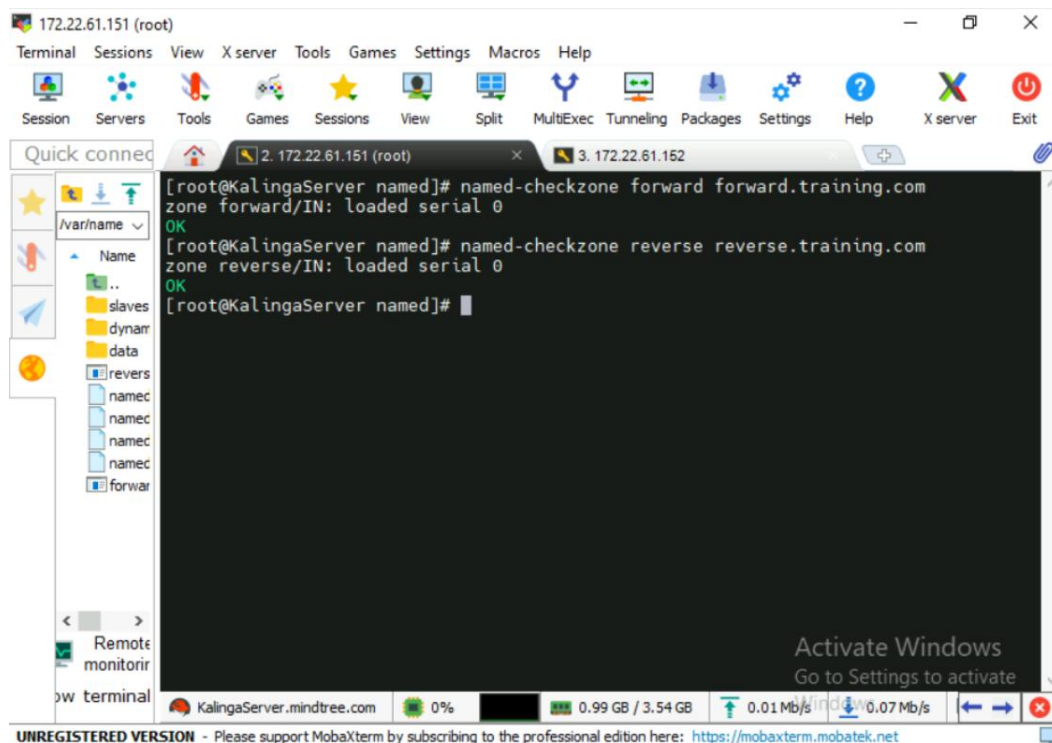
```
[root@KalingaServer named]# systemctl restart named; systemctl status named
```

The output of the `systemctl status named` command is as follows:

```
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; preset: disabled)
   Active: active (running) since Tue 2025-09-23 09:45:52 IST; 17ms ago
     Process: 2049959 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" ==>
     Process: 2049963 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS
   Main PID: 2049964 (named)
    Tasks: 8 (limit: 22780)
   Memory: 25.9M
      CPU: 84ms
   CGroup: /system.slice/named.service
           └─2049964 /usr/sbin/named -u named -c /etc/named.conf

Sep 23 09:45:52 KalingaServer.mindtree.com named[2049964]: network unreachable re>
Sep 23 09:45:52 KalingaServer.mindtree.com named[2049964]: network unreachable re>
Sep 23 09:45:52 KalingaServer.mindtree.com named[2049964]: network unreachable re>
Sep 23 09:45:52 KalingaServer.mindtree.com named[2049964]: network unreachable re>
Sep 23 09:45:52 KalingaServer.mindtree.com named[2049964]: zone localhost/IN: loa>
Sep 23 09:45:52 KalingaServer.mindtree.com named[2049964]: all zones loaded
Sep 23 09:45:52 KalingaServer.mindtree.com named[2049964]: running
Sep 23 09:45:52 KalingaServer.mindtree.com named[2049964]: zone training.com/IN: >
Sep 23 09:45:52 KalingaServer.mindtree.com named[2049964]: zone 61.22.172.in-addr>
Sep 23 09:45:52 KalingaServer.mindtree.com systemd[1]: Started Berkeley Internet
```

The terminal also shows a list of files in the `/var/name` directory on the left sidebar.



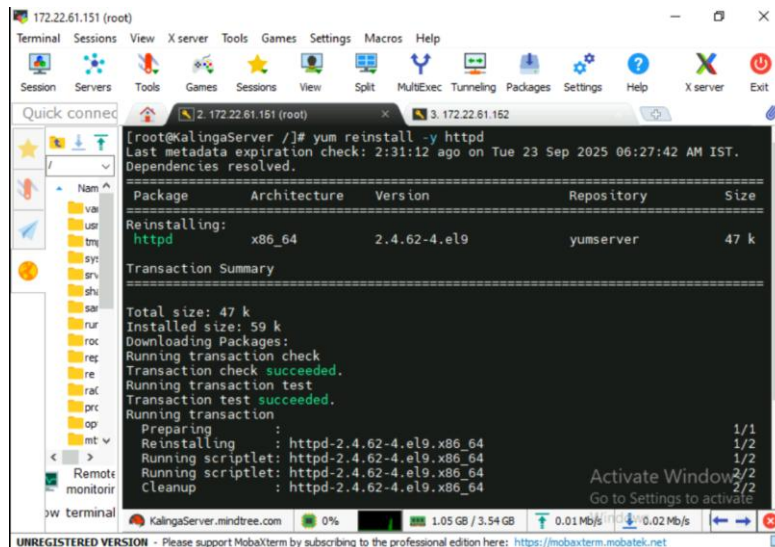
The screenshot shows a MobaXterm window with a terminal session on a Kali Linux server (172.22.61.151). The user has executed the following commands:

```
[root@KalingaServer named]# named-checkzone forward forward.training.com
zone forward/IN: loaded serial 0
OK
[root@KalingaServer named]# named-checkzone reverse reverse.training.com
zone reverse/IN: loaded serial 0
OK
[root@KalingaServer named]#
```

The terminal also shows a list of files in the `/var/name` directory on the left sidebar.

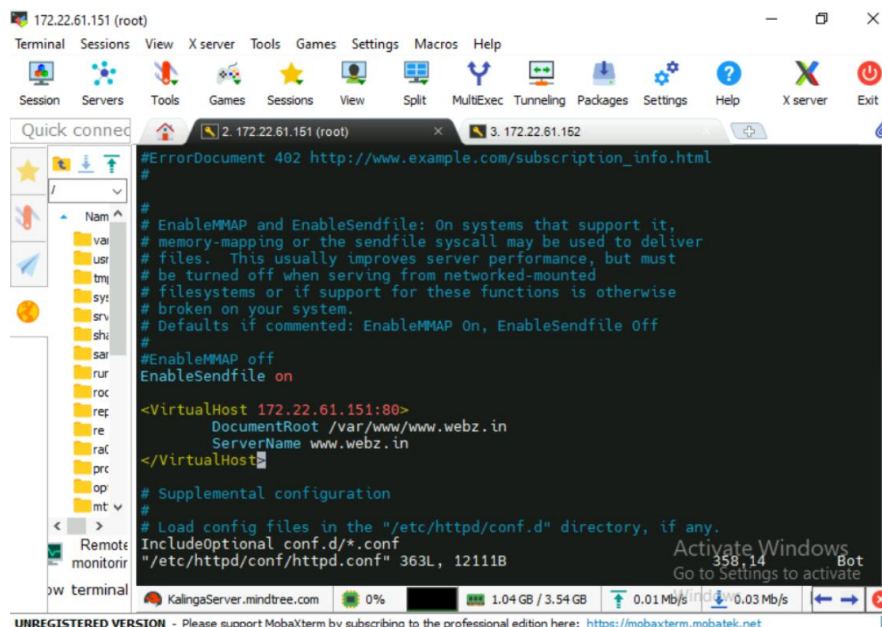
2. Create a website by using httpd and host a webpage so that that can accessed from Jump server.

- Install package httpd



```
[root@KalingaServer /]# yum reinstall -y httpd
Last metadata expiration check: 2:31:12 ago on Tue 23 Sep 2025 06:27:42 AM IST.
Dependencies resolved.
=====
Package             Architecture Version      Repository    Size
Reinstalling:
httpd                x86_64      2.4.62-4.el9 yumserver     47 k
=====
Transaction Summary
=====
Total size: 47 k
Installed size: 59 k
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing                : 1/1
Reinstalling             : httpd-2.4.62-4.el9.x86_64 1/2
Running scriptlet        : httpd-2.4.62-4.el9.x86_64 1/2
Running scriptlet        : httpd-2.4.62-4.el9.x86_64 2/2
Cleanup                  : httpd-2.4.62-4.el9.x86_64 2/2
=====
```

- Configure the file httpd.conf at path: /etc/httpd/conf with details of servername and document root



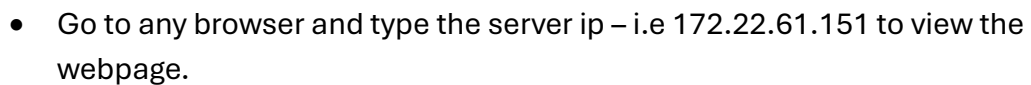
```
#ErrorDocument 402 http://www.example.com/subscription_info.html
#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on

<VirtualHost 172.22.61.151:80>
    DocumentRoot /var/www/www.webz.in
    ServerName www.webz.in
</VirtualHost>

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
"/etc/httpd/conf/httpd.conf" 363L, 12111B
```

- Create a html file→index.html at /var/www/www.webz.in





- Securely copy the files of /opt directory of server machine to /opt directory in client machine using SCP
  - Install packages vsftpd and ftp



172.22.61.151 (root)

Terminal Sessions View X server Tools Games Settings Macros Help

Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit

Quick connect

2. 172.22.61.151 (root) 3. 172.22.61.152

```
[root@KalingaServer /]# yum reinstall -y vsftpd ftp
Last metadata expiration check: 2:43:48 ago on Tue 23 Sep 2025 06:27:42 AM IST.
Dependencies resolved.

=====
Package             Architecture Version      Repository    Size
=====
Reinstalling:
ftp                  x86_64      0.17-89.el9  yumserver     62 k
vsftpd               x86_64      3.0.5-6.el9  yumserver     168 k
=====

Transaction Summary
=====
Total size: 230 k
Installed size: 459 k
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing :
Reinstalling : vsftpd-3.0.5-6.el9.x86_64 1/1
Running scriptlet: vsftpd-3.0.5-6.el9.x86_64 1/4
Reinstalling : ftp-0.17-89.el9.x86_64 2/4
=====
```

Activate Windows  
Go to Settings to activate

KalingaServer.mindtree.com 0% 1.03 GB / 3.54 GB 0.01 Mb/s 0.02 Mb/s

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

- Create files t1,t2 in /opt and using command #scp – a secured copy of these files are transferred to the client machine's /opt

172.22.61.151 (root)

Terminal Sessions View X server Tools Games Settings Macros Help

Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit

Quick connect

2. 172.22.61.151 (root) 3. 172.22.61.152

```
[root@KalingaServer /]# cd /opt
[root@KalingaServer /opt]# ls
t1 t2
[root@KalingaServer /opt]# scp /opt/t2 root@172.22.61.152:/opt
root@172.22.61.152's password:
100% 0 0.0KB/s 00:00
[root@KalingaServer /opt]# scp /opt/t1 root@172.22.61.152:/opt
root@172.22.61.152's password:
Permission denied, please try again.
root@172.22.61.152's password:
100% 0 0.0KB/s 00:00
[root@KalingaServer /opt]#
```

Activate Windows  
Go to Settings to activate

KalingaServer.mindtree.com 0% 0.99 GB / 3.54 GB 0.01 Mb/s 0.02 Mb/s

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

- Now going to the client machine's /opt directory we can clearly see the t1,t2 files .

