

System administrators are tasked with implementing robust security measures, including managing user permissions, configuring and monitoring firewalls (such as iptables and firewalld), and enforcing SELinux policies to prevent unauthorized access and ensure the system's integrity and protection.



The image consists of two terminal screenshots. The top screenshot shows the editing of the `/etc/sysconfig/selinux` file in a `VIM` editor. The file content includes comments about SELinux states (enforcing, permissive, disabled) and modes (targeted, minimum, mls). The current configuration is `SELINUX=disabled` and `SELINUXTYPE=targeted`. The bottom screenshot shows the output of the `firewalld` service status command. It indicates that the service is loaded but inactive. The output also shows the service's history, including its start and stop times, and the user who started it.

```
root@localhost:~ — /usr/bin/vim /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/changing_selinux_states_and_modes_using_selinux#changing_selinux_modes-at-boot-time_changing_selinux_states_and_modes
#
# NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted

-- INSERT --
```

```
root@localhost:~

target      prot opt source                destination
Chain FORWARD (policy ACCEPT)
target      prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target      prot opt source                destination
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target      prot opt source                destination
Chain FORWARD (policy ACCEPT)
target      prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target      prot opt source                destination
[root@localhost ~]# iptables -I INPUT -s 10.10.10.10 -j REJECT
[root@localhost ~]# iptables -I INPUT -s 10.10.10.11 -j ACCEPT
[root@localhost ~]# service firewalld stop
Redirecting to /bin/systemctl stop firewalld.service
[root@localhost ~]# service firewalld status
Redirecting to /bin/systemctl status firewalld.service
o firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
   Active: inactive (dead) since Tue 2024-10-01 20:38:06 IST; 44s ago
     Duration: 1h 15min 45.804s
    Docs: man:firewalld(1)
   Process: 1039 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (code=exited, status=0/SUCCESS)
   Main PID: 1039 (code=exited, status=0/SUCCESS)
      CPU: 484ms

Oct 01 19:22:16 localhost systemd[1]: Starting firewalld - dynamic firewall daemon...
Oct 01 19:22:20 localhost systemd[1]: Started firewalld - dynamic firewall daemon.
Oct 01 20:38:05 localhost.localdomain systemd[1]: Stopping firewalld - dynamic firewall daemon...
Oct 01 20:38:06 localhost.localdomain systemd[1]: firewalld.service: Deactivated successfully.
Oct 01 20:38:06 localhost.localdomain systemd[1]: Stopped firewalld - dynamic firewall daemon.
[root@localhost ~]# service firewalld start
Redirecting to /bin/systemctl start firewalld.service
[root@localhost ~]#
```

```
Oct 1 20:39 root@localhost:~ — /bin/systemctl status firewall.service
* firewall.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
  Active: active (running) since Tue 2024-10-01 20:39:02 IST; 36s ago
    Docs: man:firewalld(1)
  Main PID: 2986 (firewalld)
    Tasks: 2 (limit: 22944)
  Memory: 26.8M
    CPU: 322ms
  CGroup: /system.slice/firewalld.service
          └─2986 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

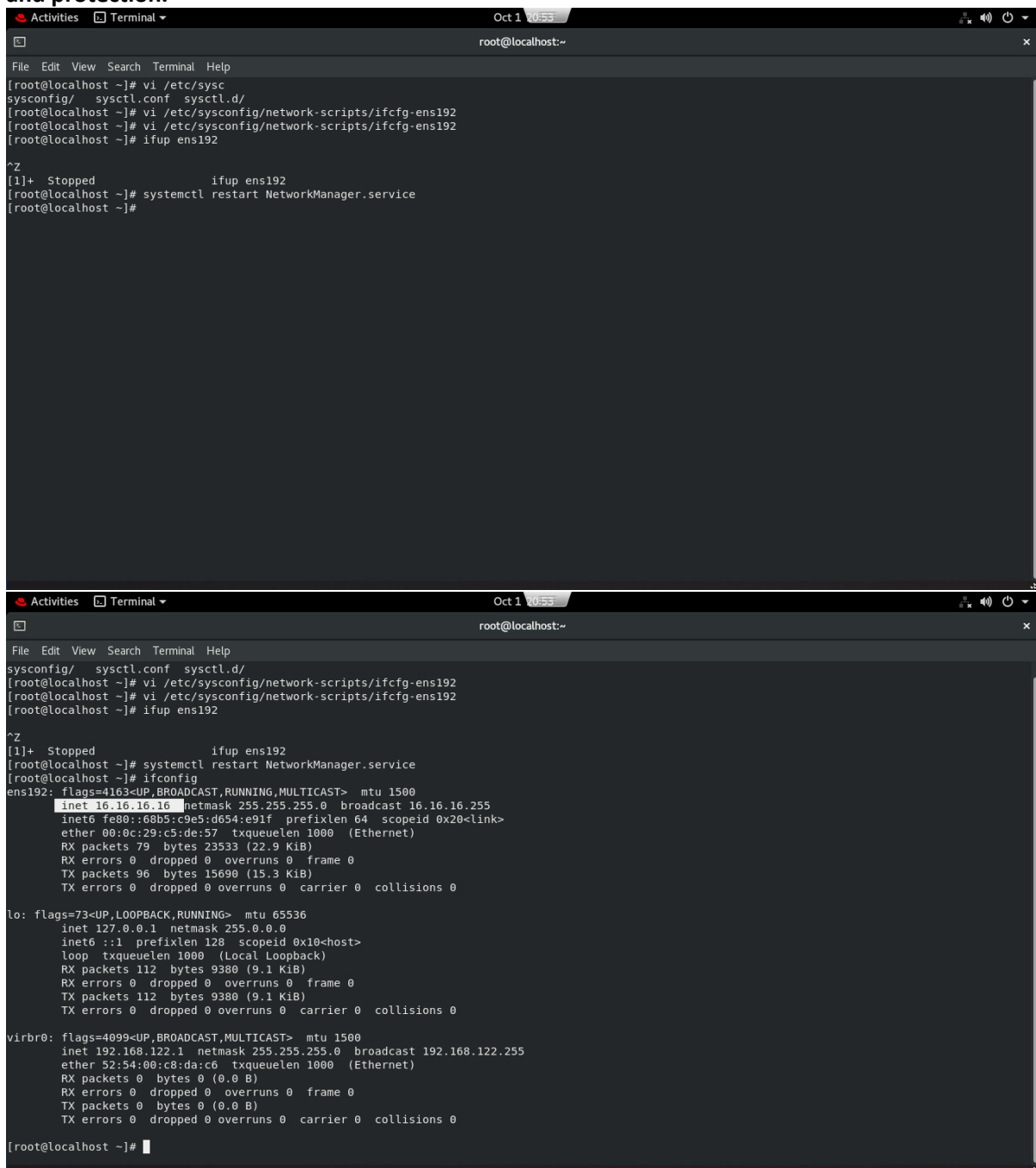
Oct 01 20:39:02 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...
Oct 01 20:39:02 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.

lines 1-13/13 (END)

Oct 1 20:59 root@localhost:~
File Edit View Search Terminal Help
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens192
UUID=4ffa4966-d231-4831-91a7-34225045de64
DEVICE=ens192
ONBOOT=yes
IPADDR=16.16.16.16
PREFIX=24
GATEWAY=16.16.16.1

:wq
```

System administrators are tasked with implementing robust security measures, including managing user permissions, configuring and monitoring firewalls (such as iptables and firewalld), and enforcing SELinux policies to prevent unauthorized access and ensure the system's integrity and protection.



The image displays two screenshots of a Linux terminal window, showing the configuration and verification of a network interface named ens192.

Top Screenshot: The terminal shows the user editing the `/etc/sysconfig/network-scripts/ifcfg-ens192` file using the `vi` editor. The file is set to `BOOTPROTO=none` and `ONBOOT=yes`. The user then runs `ifup ens192` to bring the interface up. The output shows the interface is now up and running.

```
root@localhost ~]# vi /etc/sysconfig/network-scripts/ifcfg-ens192
root@localhost ~]# ifup ens192
^Z
[1]+  Stopped                  ifup ens192
root@localhost ~]# systemctl restart NetworkManager.service
root@localhost ~]#
```

Bottom Screenshot: The terminal shows the user running `ifconfig` to verify the network configuration. The output shows the interface `ens192` is up and running, with the IP address `16.16.16.16` and netmask `255.255.255.0`. The user also runs `ifconfig lo` to verify the loopback interface, which is also up and running with the IP address `127.0.0.1`.

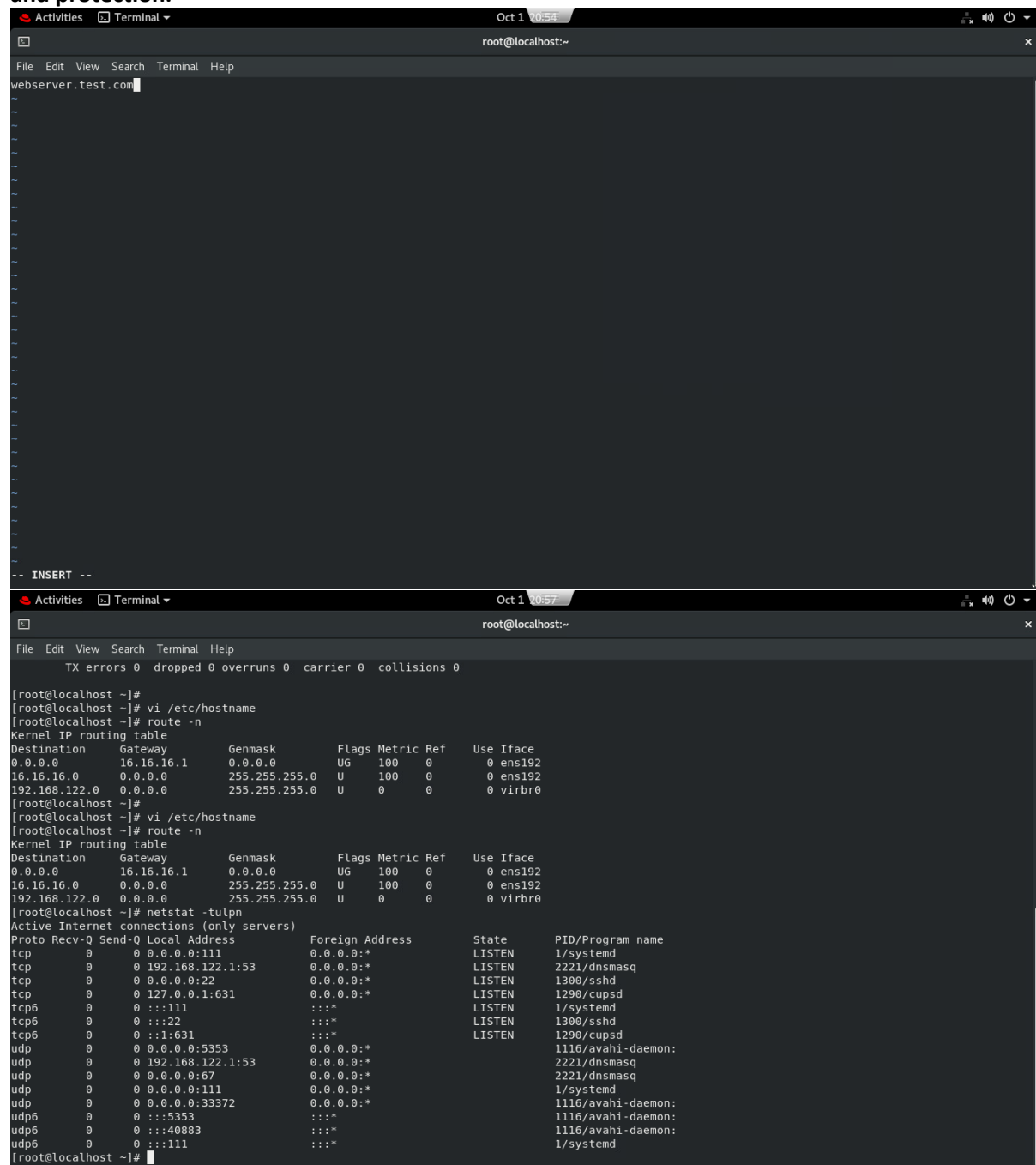
```
root@localhost ~]# ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 16.16.16.16  netmask 255.255.255.0  broadcast 16.16.16.255
    inet6 fe80::68b5:c9e5:d654:e91f  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:c5:de:57  txqueuelen 1000  (Ethernet)
    RX packets 79  bytes 23533 (22.9 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 96  bytes 15690 (15.3 KiB)
    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 112  bytes 9380 (9.1 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 112  bytes 9380 (9.1 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
    inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
    ether 52:54:00:c8:da:c6  txqueuelen 1000  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@localhost ~]#
```

System administrators are tasked with implementing robust security measures, including managing user permissions, configuring and monitoring firewalls (such as iptables and firewallld), and enforcing SELinux policies to prevent unauthorized access and ensure the system's integrity and protection.



The image displays two screenshots of a Linux terminal window, likely from a virtual machine, showing network configuration and status.

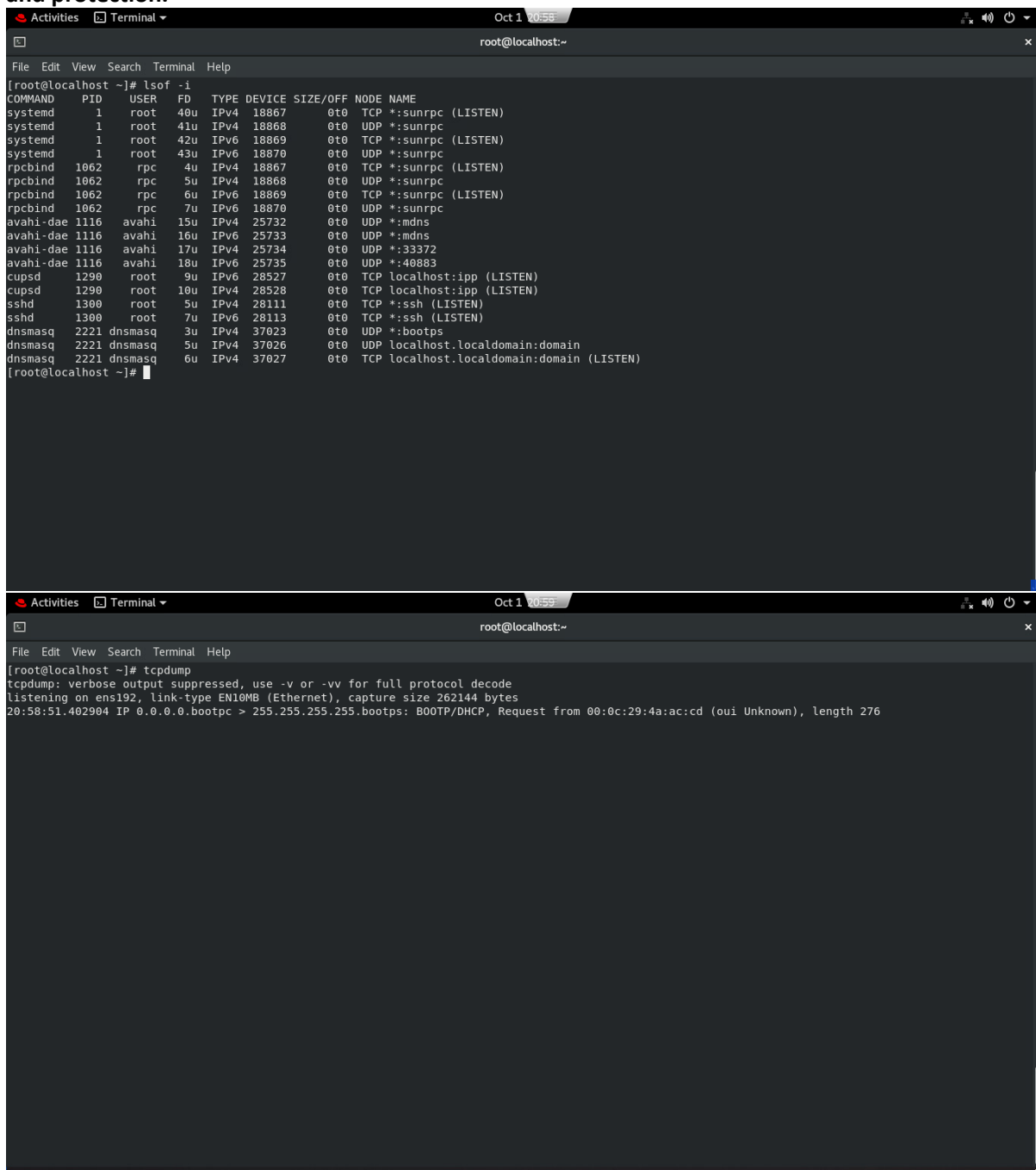
The top screenshot shows the terminal with the prompt `root@localhost:~`. The user has entered `webservice.test.com` and is at the prompt. The terminal title bar indicates the date is Oct 1, 2024, and the time is 10:54.

The bottom screenshot shows the terminal with the prompt `root@localhost:~`. The user has entered `TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0`. The terminal title bar indicates the date is Oct 1, 2024, and the time is 10:57.

The terminal output in the bottom screenshot shows the following commands and their results:

```
[root@localhost ~]#  
[root@localhost ~]# vi /etc/hostname  
[root@localhost ~]# route -n  
Kernel IP routing table  
Destination Gateway Genmask Flags Metric Ref Use Iface  
0.0.0.0 16.16.16.1 0.0.0.0 UG 100 0 0 ens192  
16.16.16.0 0.0.0.0 255.255.255.0 U 100 0 0 ens192  
192.168.122.0 0.0.0.0 255.255.255.0 U 0 0 0 virbr0  
[root@localhost ~]#  
[root@localhost ~]# vi /etc/hostname  
[root@localhost ~]# route -n  
Kernel IP routing table  
Destination Gateway Genmask Flags Metric Ref Use Iface  
0.0.0.0 16.16.16.1 0.0.0.0 UG 100 0 0 ens192  
16.16.16.0 0.0.0.0 255.255.255.0 U 100 0 0 ens192  
192.168.122.0 0.0.0.0 255.255.255.0 U 0 0 0 virbr0  
[root@localhost ~]# netstat -tulpn  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name  
tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN 1/systemd  
tcp 0 0 192.168.122.1:53 0.0.0.0:* LISTEN 2221/dnsmasq  
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 1300/sshd  
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN 1290/cupsd  
tcp6 0 0 :::111 :::* LISTEN 1/systemd  
tcp6 0 0 :::22 :::* LISTEN 1300/sshd  
tcp6 0 0 :::631 :::* LISTEN 1290/cupsd  
udp 0 0 0.0.0.0:5353 0.0.0.0:* 1116/avahi-daemon:  
udp 0 0 192.168.122.1:53 0.0.0.0:* 2221/dnsmasq  
udp 0 0 0.0.0.0:67 0.0.0.0:* 2221/dnsmasq  
udp 0 0 0.0.0.0:111 0.0.0.0:* 1/systemd  
udp 0 0 0.0.0.0:33372 0.0.0.0:* 1116/avahi-daemon:  
udp6 0 0 :::5353 :::* 1116/avahi-daemon:  
udp6 0 0 :::40883 :::* 1116/avahi-daemon:  
udp6 0 0 :::111 :::* 1/systemd
```

System administrators are tasked with implementing robust security measures, including managing user permissions, configuring and monitoring firewalls (such as iptables and firewallld), and enforcing SELinux policies to prevent unauthorized access and ensure the system's integrity and protection.



The image displays two screenshots of a Linux terminal window. The top screenshot shows the output of the `lsof -i` command, which lists all active network connections. The bottom screenshot shows the output of the `tcpdump` command, which captures network traffic on the `ens192` interface.

```
[root@localhost ~]# lsof -i
```

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
systemd	1	root	40u	IPv4	18867	0t0	TCP	*:sunrpc (LISTEN)
systemd	1	root	41u	IPv4	18868	0t0	UDP	*:sunrpc
systemd	1	root	42u	IPv6	18869	0t0	TCP	*:sunrpc (LISTEN)
systemd	1	root	43u	IPv6	18870	0t0	UDP	*:sunrpc
rpcbind	1062	rpc	4u	IPv4	18867	0t0	TCP	*:sunrpc (LISTEN)
rpcbind	1062	rpc	5u	IPv4	18868	0t0	UDP	*:sunrpc
rpcbind	1062	rpc	6u	IPv6	18869	0t0	TCP	*:sunrpc (LISTEN)
rpcbind	1062	rpc	7u	IPv6	18870	0t0	UDP	*:sunrpc
avahi-daemon	1116	avahi	15u	IPv4	25732	0t0	UDP	*:mdns
avahi-daemon	1116	avahi	16u	IPv6	25733	0t0	UDP	*:mdns
avahi-daemon	1116	avahi	17u	IPv4	25734	0t0	UDP	*:33372
avahi-daemon	1116	avahi	18u	IPv6	25735	0t0	UDP	*:40883
cupsd	1290	root	9u	IPv6	28527	0t0	TCP	localhost:ipp (LISTEN)
cupsd	1290	root	10u	IPv4	28528	0t0	TCP	localhost:ipp (LISTEN)
sshd	1300	root	5u	IPv4	28111	0t0	TCP	*:ssh (LISTEN)
sshd	1300	root	7u	IPv6	28113	0t0	TCP	*:ssh (LISTEN)
dnsmasq	2221	dnsmasq	3u	IPv4	37023	0t0	UDP	*:bootps
dnsmasq	2221	dnsmasq	5u	IPv4	37026	0t0	UDP	localhost.localdomain:domain
dnsmasq	2221	dnsmasq	6u	IPv4	37027	0t0	TCP	localhost.localdomain:domain (LISTEN)

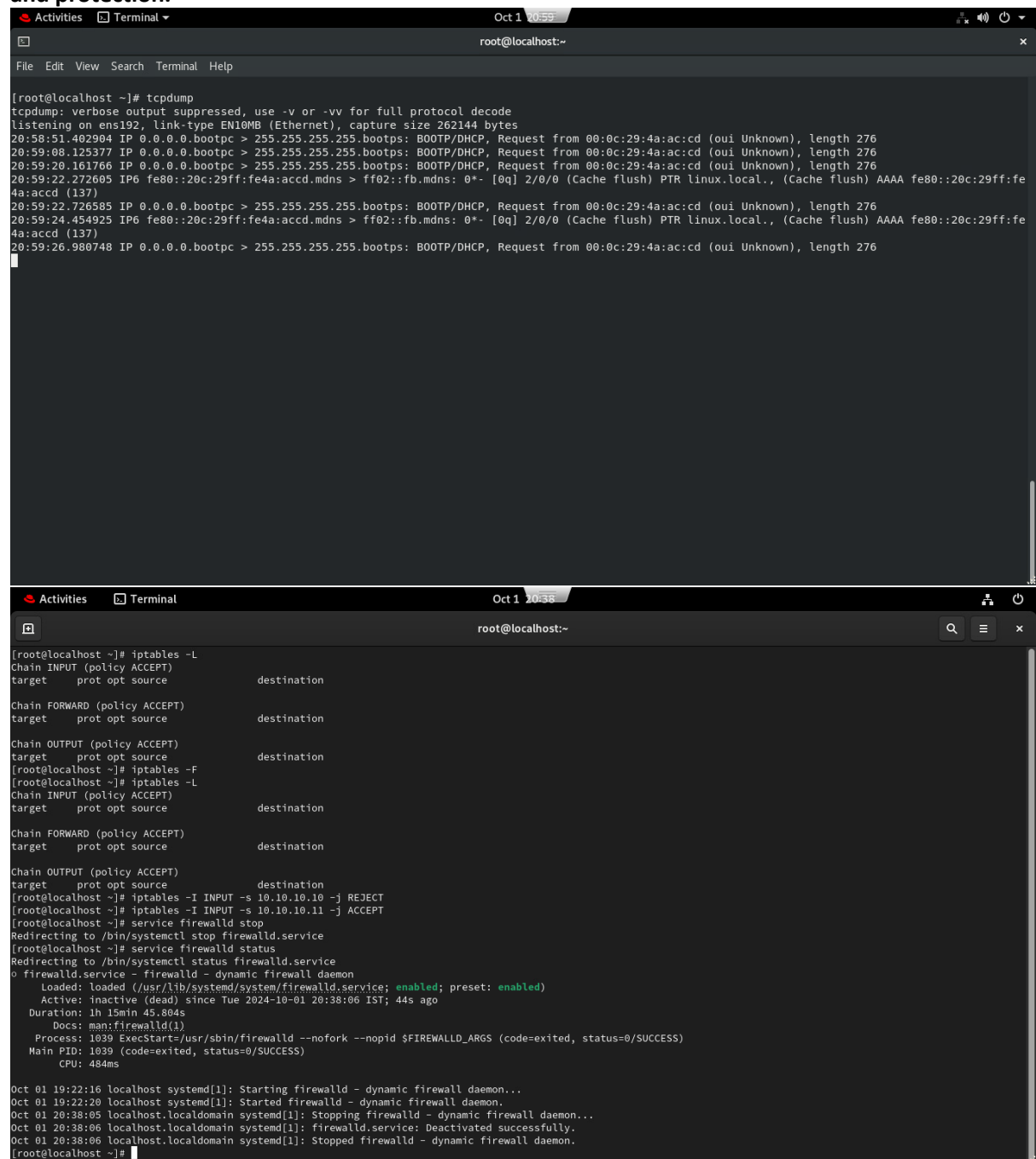
```
[root@localhost ~]#
```



```
[root@localhost ~]# tcpdump
```

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens192, link-type EN10MB (Ethernet), capture size 262144 bytes
20:58:51.402904 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 00:0c:29:4a:ac:cd (oui Unknown), length 276

System administrators are tasked with implementing robust security measures, including managing user permissions, configuring and monitoring firewalls (such as iptables and firewalld), and enforcing SELinux policies to prevent unauthorized access and ensure the system's integrity and protection.



The image consists of two terminal screenshots. The top screenshot shows a terminal window titled 'root@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The user has run the command 'tcpdump', and the output shows several DHCP requests from 00:0c:29:4a:ac:cd to 255.255.255.255. The bottom screenshot shows the same terminal window after running 'iptables -L', displaying the default rules for INPUT, FORWARD, and OUTPUT chains. Then, the user runs 'iptables -F' to flush the rules. Finally, the user runs 'service firewalld stop', and the terminal shows the service stopping successfully. The bottom of the screenshot shows system logs for the firewalld service starting and stopping.

```
[root@localhost ~]# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens192, link-type EN10MB (Ethernet), capture size 262144 bytes
20:58:51.402904 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 00:0c:29:4a:ac:cd (oui Unknown), length 276
20:59:08.125377 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 00:0c:29:4a:ac:cd (oui Unknown), length 276
20:59:20.161766 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 00:0c:29:4a:ac:cd (oui Unknown), length 276
20:59:22.272605 IP6 fe80::20c:29ff:fe4a:accd.mdns > ff02::fb.mdns: 0*- [0q] 2/0/0 (Cache flush) PTR linux.local., (Cache flush) AAAA fe80::20c:29ff:fe4a:accd (137)
20:59:22.726585 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 00:0c:29:4a:ac:cd (oui Unknown), length 276
20:59:24.454925 IP6 fe80::20c:29ff:fe4a:accd.mdns > ff02::fb.mdns: 0*- [0q] 2/0/0 (Cache flush) PTR linux.local., (Cache flush) AAAA fe80::20c:29ff:fe4a:accd (137)
20:59:26.980748 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 00:0c:29:4a:ac:cd (oui Unknown), length 276

[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source               destination

Chain FORWARD (policy ACCEPT)
target    prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source               destination
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source               destination

Chain FORWARD (policy ACCEPT)
target    prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source               destination
[root@localhost ~]# iptables -I INPUT -s 10.10.10.10 -j REJECT
[root@localhost ~]# iptables -I INPUT -s 10.10.10.11 -j ACCEPT
[root@localhost ~]# service firewalld stop
Redirecting to /bin/systemctl stop firewalld.service
[root@localhost ~]# service firewalld status
Redirecting to /bin/systemctl status firewalld.service
○ firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
   Active: inactive (dead) since Tue 2024-10-01 20:38:06 IST; 44s ago
   Duration: 1h 15min 45.804s
   Docs: man:firewalld(1)
   Process: 1039 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (code=exited, status=0/SUCCESS)
   Main PID: 1039 (code=exited, status=0/SUCCESS)
   CPU: 484ms

Oct 01 19:22:16 localhost systemd[1]: Starting firewalld - dynamic firewall daemon...
Oct 01 19:22:20 localhost systemd[1]: Started firewalld - dynamic firewall daemon.
Oct 01 20:38:05 localhost.localdomain systemd[1]: Stopping firewalld - dynamic firewall daemon...
Oct 01 20:38:06 localhost.localdomain systemd[1]: firewalld.service: Deactivated successfully.
Oct 01 20:38:06 localhost.localdomain systemd[1]: Stopped firewalld - dynamic firewall daemon.
[root@localhost ~]#
```