JADHUSAN M S

11/3/2021

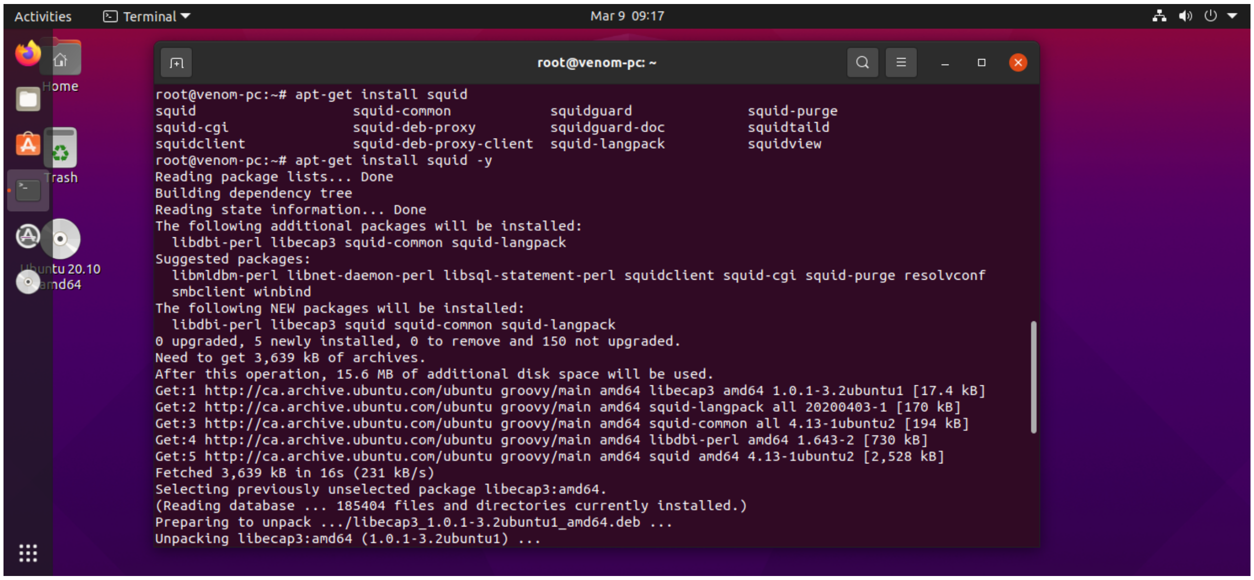
Proxy Server

System Administration

Jadhusan M.S

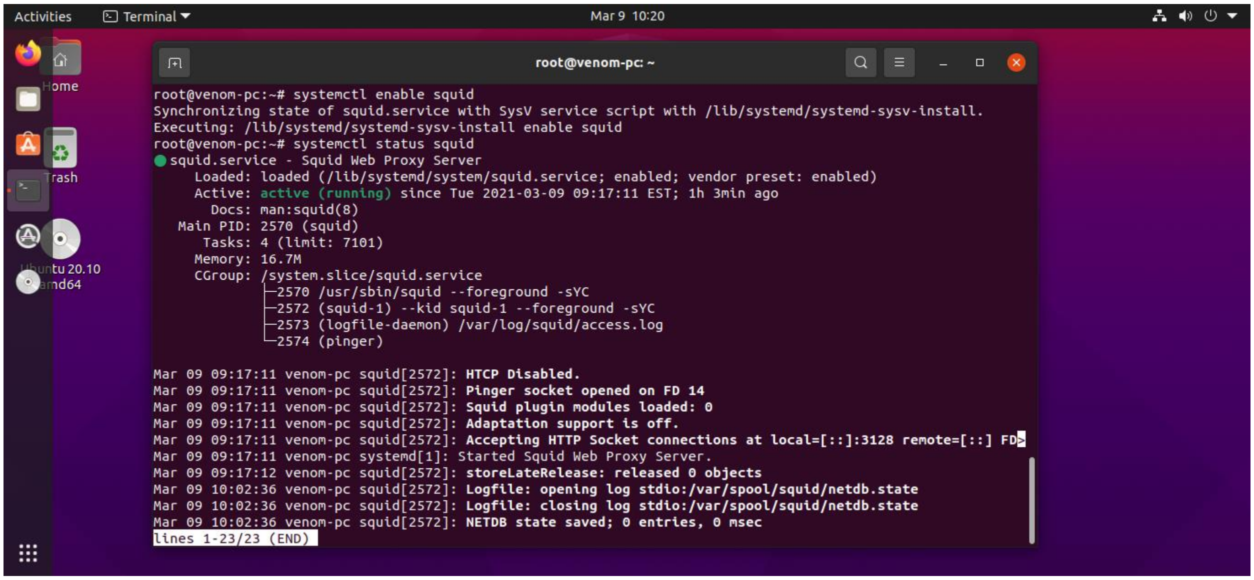
SQUID SERVICE

Installing Squid Service in Ubuntu Machine



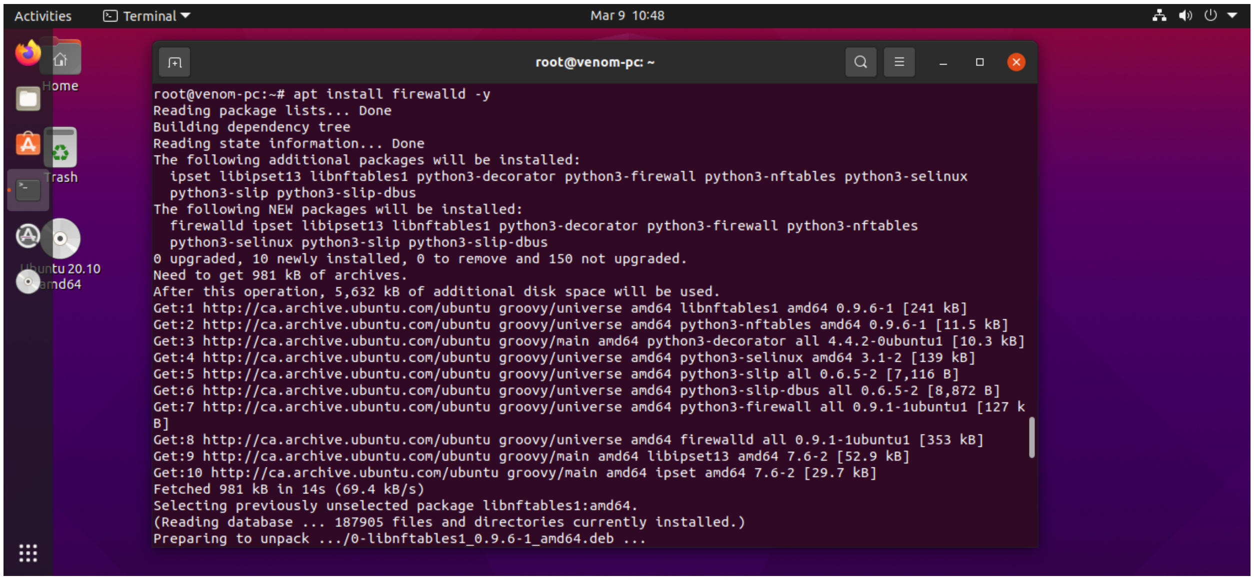
```
root@venom-pc:~# apt-get install squid
squid                  squid-common           squidguard             squid-purge
squid-cgi              squid-deb-proxy        squidguard-doc         squidtaild
squidclient            squid-deb-proxy-client squid-langpack         squidview
root@venom-pc:~# apt-get install squid -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdbi-perl libecap3 squid-common squid-langpack
Suggested packages:
  libmldbm-perl libnet-daemon-perl libsql-statement-perl squidclient squid-cgi squid-purge resolvconf
  smbclient winbind
The following NEW packages will be installed:
  libdbi-perl libecap3 squid squid-common squid-langpack
0 upgraded, 5 newly installed, 0 to remove and 150 not upgraded.
Need to get 3,639 kB of archives.
After this operation, 15.6 MB of additional disk space will be used.
Get:1 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 libecap3 amd64 1.0.1-3.2ubuntu1 [17.4 kB]
Get:2 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 squid-langpack all 20200403-1 [170 kB]
Get:3 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 squid-common all 4.13-1ubuntu2 [194 kB]
Get:4 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 libdbi-perl amd64 1.643-2 [730 kB]
Get:5 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 squid amd64 4.13-1ubuntu2 [2,528 kB]
Fetched 3,639 kB in 16s (231 kB/s)
Selecting previously unselected package libecap3:amd64.
(Reading database ... 185404 files and directories currently installed.)
Preparing to unpack .../libecap3_1.0.1-3.2ubuntu1_amd64.deb ...
Unpacking libecap3:amd64 (1.0.1-3.2ubuntu1) ...
```

Start / Enable and Check the status of Squid Service.



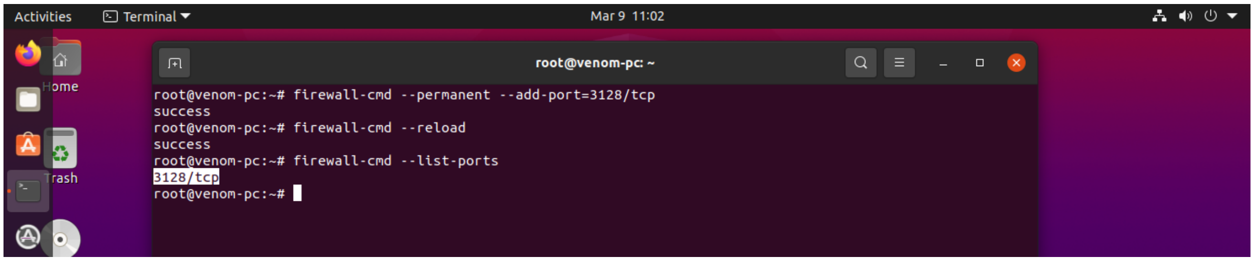
```
root@venom-pc:~# systemctl enable squid
Synchronizing state of squid.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable squid
root@venom-pc:~# systemctl status squid
● squid.service - Squid Web Proxy Server
     Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2021-03-09 09:17:11 EST; 1h 3min ago
       Docs: man:squid(8)
   Main PID: 2570 (squid)
      Tasks: 4 (limit: 7101)
     Memory: 16.7M
     CGroup: /system.slice/squid.service
             ├─2570 /usr/sbin/squid --foreground -sYC
             ├─2572 (squid-1) --kid squid-1 --foreground -sYC
             ├─2573 (logfile-daemon) /var/log/squid/access.log
             └─2574 (pinger)

Mar 09 09:17:11 venom-pc squid[2572]: HTCP Disabled.
Mar 09 09:17:11 venom-pc squid[2572]: Pinger socket opened on FD 14
Mar 09 09:17:11 venom-pc squid[2572]: Squid plugin modules loaded: 0
Mar 09 09:17:11 venom-pc squid[2572]: Adaptation support is off.
Mar 09 09:17:11 venom-pc squid[2572]: Accepting HTTP Socket connections at local=[::]:3128 remote=[::] FD>
Mar 09 09:17:11 venom-pc systemd[1]: Started Squid Web Proxy Server.
Mar 09 09:17:12 venom-pc squid[2572]: storeLateRelease: released 0 objects
Mar 09 10:02:36 venom-pc squid[2572]: Logfile: opening log stdio:/var/spool/squid/netdb.state
Mar 09 10:02:36 venom-pc squid[2572]: Logfile: closing log stdio:/var/spool/squid/netdb.state
Mar 09 10:02:36 venom-pc squid[2572]: NETDB state saved; 0 entries, 0 msec
lines 1-23/23 (END)
```

Install Firewall .



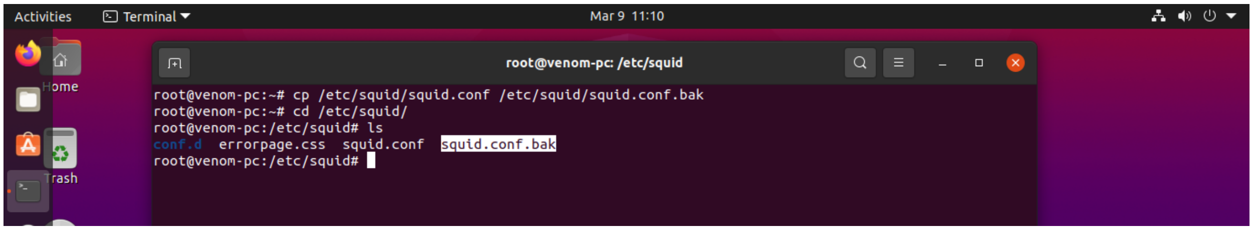
```
root@venom-pc:~# apt install firewalld -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ipset libipset13 libnftables1 python3-decorator python3-firewall python3-nftables python3-selinux
  python3-slip python3-slip-dbus
The following NEW packages will be installed:
  firewalld ipset libipset13 libnftables1 python3-decorator python3-firewall python3-nftables
  python3-selinux python3-slip python3-slip-dbus
0 upgraded, 10 newly installed, 0 to remove and 150 not upgraded.
Need to get 981 kB of archives.
After this operation, 5,632 kB of additional disk space will be used.
Get:1 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 libnftables1 amd64 0.9.6-1 [241 kB]
Get:2 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 python3-nftables amd64 0.9.6-1 [11.5 kB]
Get:3 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 python3-decorator all 4.4.2-0ubuntu1 [10.3 kB]
Get:4 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 python3-selinux amd64 3.1-2 [139 kB]
Get:5 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 python3-slip all 0.6.5-2 [7,116 B]
Get:6 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 python3-slip-dbus all 0.6.5-2 [8,872 B]
Get:7 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 python3-firewall all 0.9.1-1ubuntu1 [127 k
B]
Get:8 http://ca.archive.ubuntu.com/ubuntu groovy/universe amd64 firewalld all 0.9.1-1ubuntu1 [353 kB]
Get:9 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 libipset13 amd64 7.6-2 [52.9 kB]
Get:10 http://ca.archive.ubuntu.com/ubuntu groovy/main amd64 ipset amd64 7.6-2 [29.7 kB]
Fetched 981 kB in 14s (69.4 kB/s)
Selecting previously unselected package libnftables1:amd64.
(Reading database ... 187905 files and directories currently installed.)
Preparing to unpack .../0-libnftables1_0.9.6-1_amd64.deb ...
```

Assign the squid service port number to firewall.



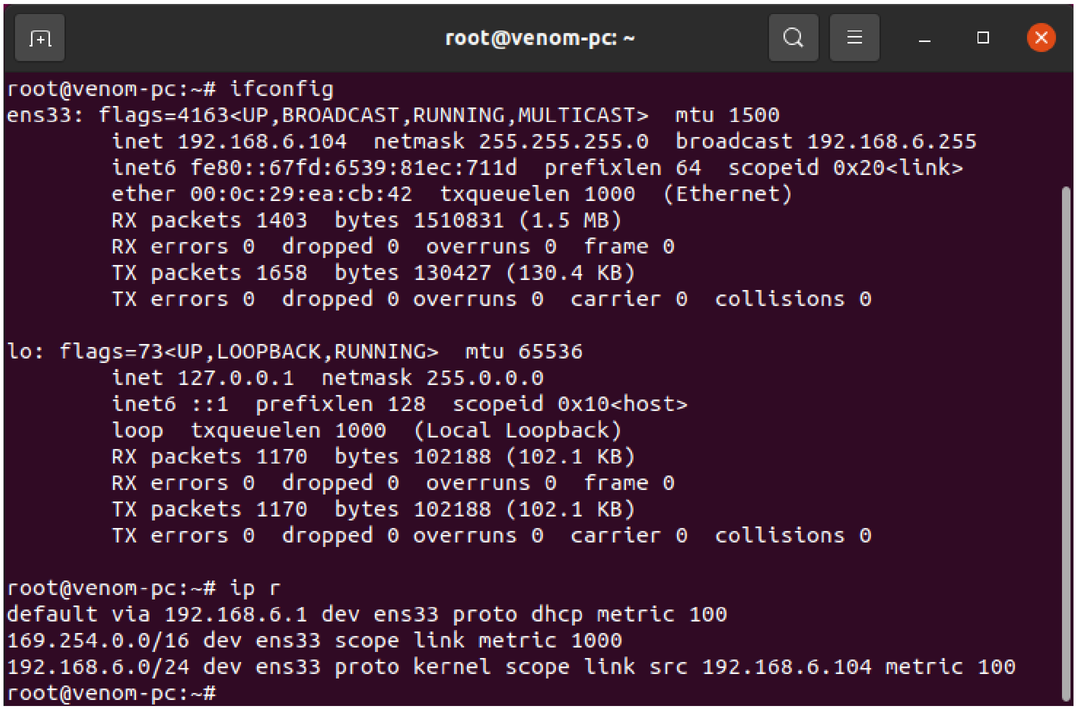
```
root@venom-pc:~# firewall-cmd --permanent --add-port=3128/tcp
success
root@venom-pc:~# firewall-cmd --reload
success
root@venom-pc:~# firewall-cmd --list-ports
3128/tcp
root@venom-pc:~# 
```

Before Configuring the squid service, get a backup of the config file.



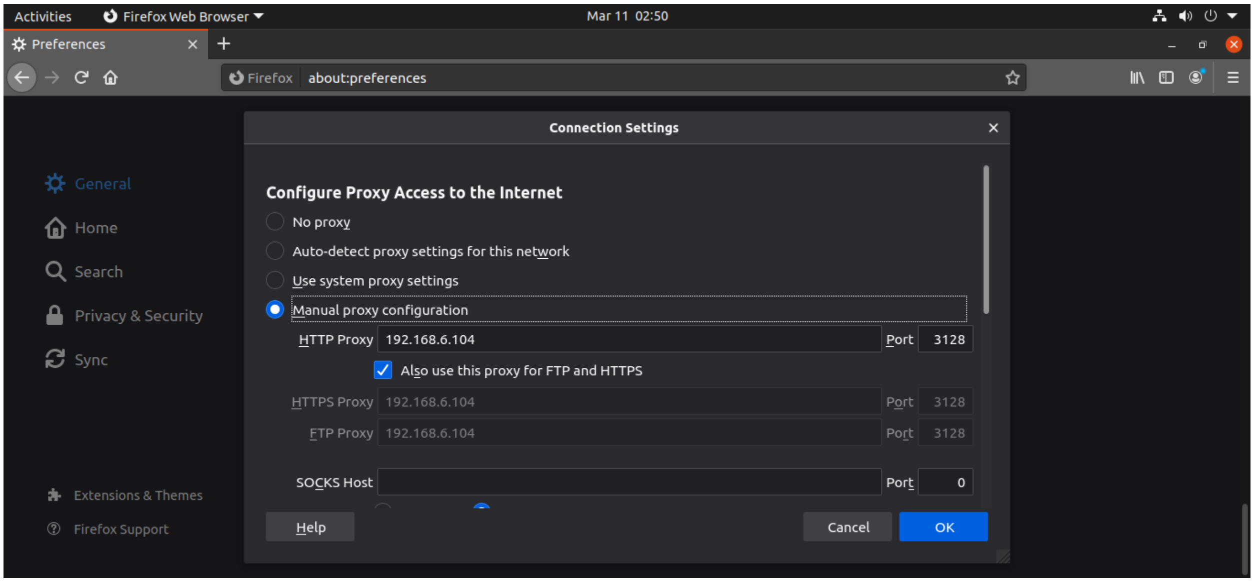
```
root@venom-pc:~# cp /etc/squid/squid.conf /etc/squid/squid.conf.bak
root@venom-pc:~# cd /etc/squid/
root@venom-pc:/etc/squid# ls
conf.d  errorpage.css  squid.conf  squid.conf.bak
root@venom-pc:/etc/squid# 
```

Ipaddress verifying in ubuntu.



```
root@venom-pc:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.6.104  netmask 255.255.255.0  broadcast 192.168.6.255
        inet6 fe80::67fd:6539:81ec:711d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ea:cb:42  txqueuelen 1000  (Ethernet)
        RX packets 1403  bytes 1510831 (1.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1658  bytes 130427 (130.4 KB)
        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 1170  bytes 102188 (102.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1170  bytes 102188 (102.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@venom-pc:~# ip r
default via 192.168.6.1 dev ens33 proto dhcp metric 100
169.254.0.0/16 dev ens33 scope link metric 1000
192.168.6.0/24 dev ens33 proto kernel scope link src 192.168.6.104 metric 100
root@venom-pc:~#
```

Manually Assinging Proxy Server to firefox.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 192.168.6.104 Port 3128

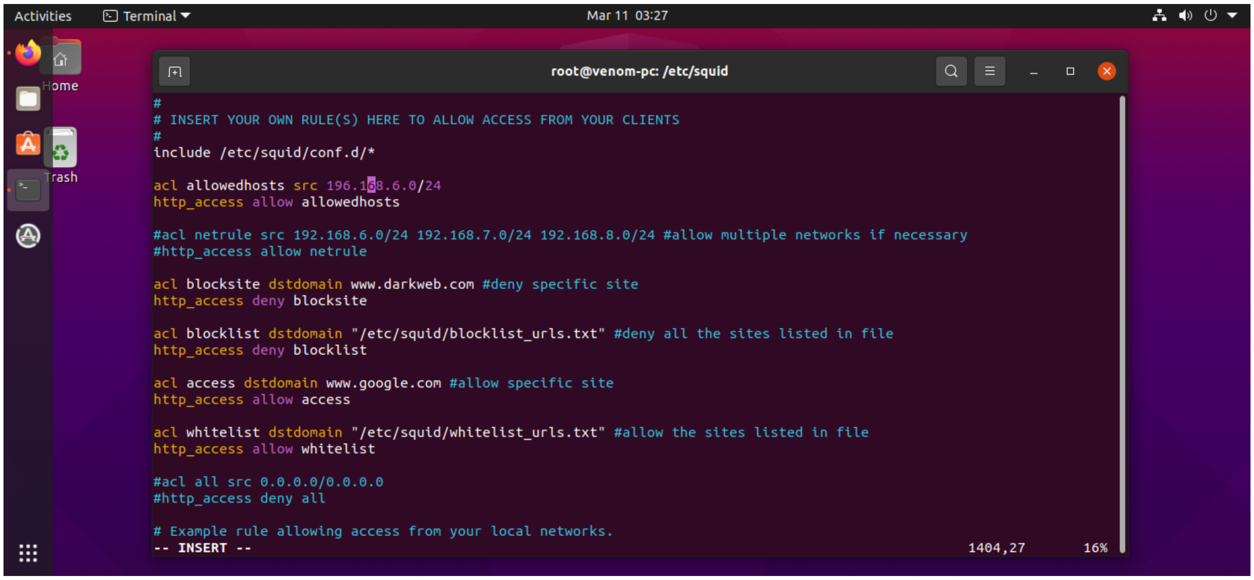
☑ Also use this proxy for FTP and HTTPS

HTTPS Proxy 192.168.6.104 Port 3128

FTP Proxy 192.168.6.104 Port 3128

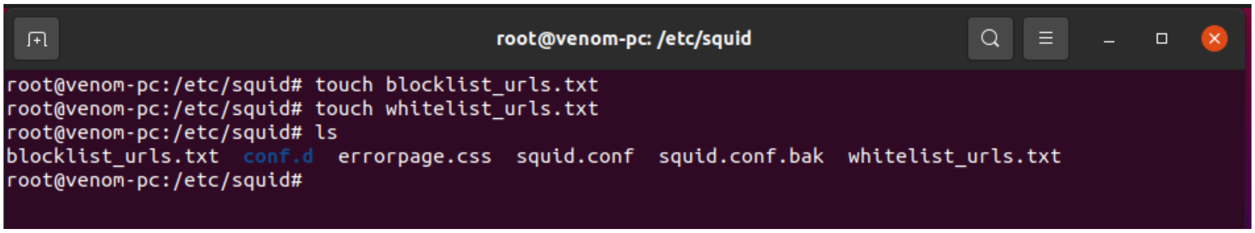
SOCKS Host Port 0

Configuring the SQUID SERVICES.



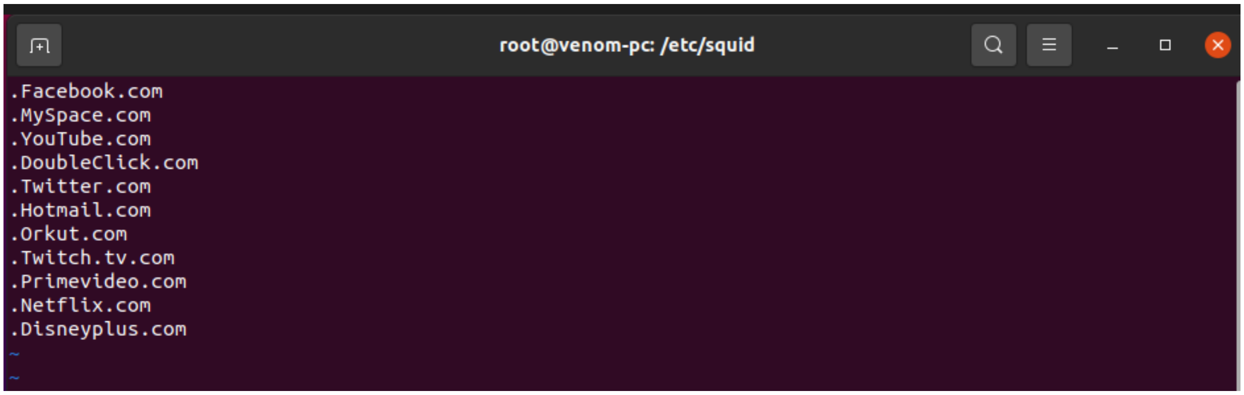
```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*

acl allowedhosts src 196.168.6.0/24
http_access allow allowedhosts

#acl netrule src 192.168.6.0/24 192.168.7.0/24 192.168.8.0/24 #allow multiple networks if necessary
#http_access allow netrule

acl blocksite dstdomain www.darkweb.com #deny specific site
http_access deny blocksite

acl blocklist dstdomain "/etc/squid/blocklist_urls.txt" #deny all the sites listed in file
http_access deny blocklist

acl access dstdomain www.google.com #allow specific site
http_access allow access

acl whitelist dstdomain "/etc/squid/whitelist_urls.txt" #allow the sites listed in file
http_access allow whitelist

#acl all src 0.0.0.0/0.0.0.0
#http_access deny all

# Example rule allowing access from your local networks.
-- INSERT --                                                                            1404,27        16%
```

Creating URL files.



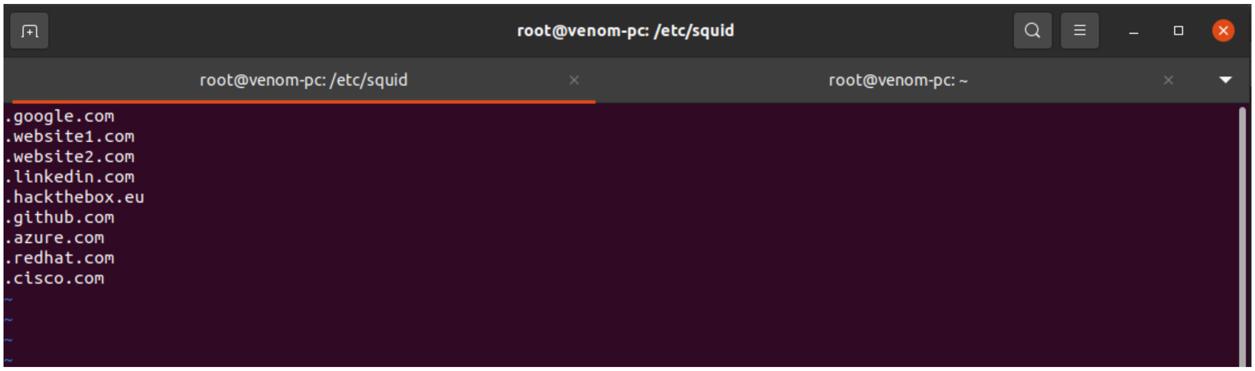
```
root@venom-pc:/etc/squid# touch blocklist_urls.txt
root@venom-pc:/etc/squid# touch whitelist_urls.txt
root@venom-pc:/etc/squid# ls
blocklist_urls.txt  conf.d  errorpage.css  squid.conf  squid.conf.bak  whitelist_urls.txt
root@venom-pc:/etc/squid#
```

Vim blocklist_urls.txt



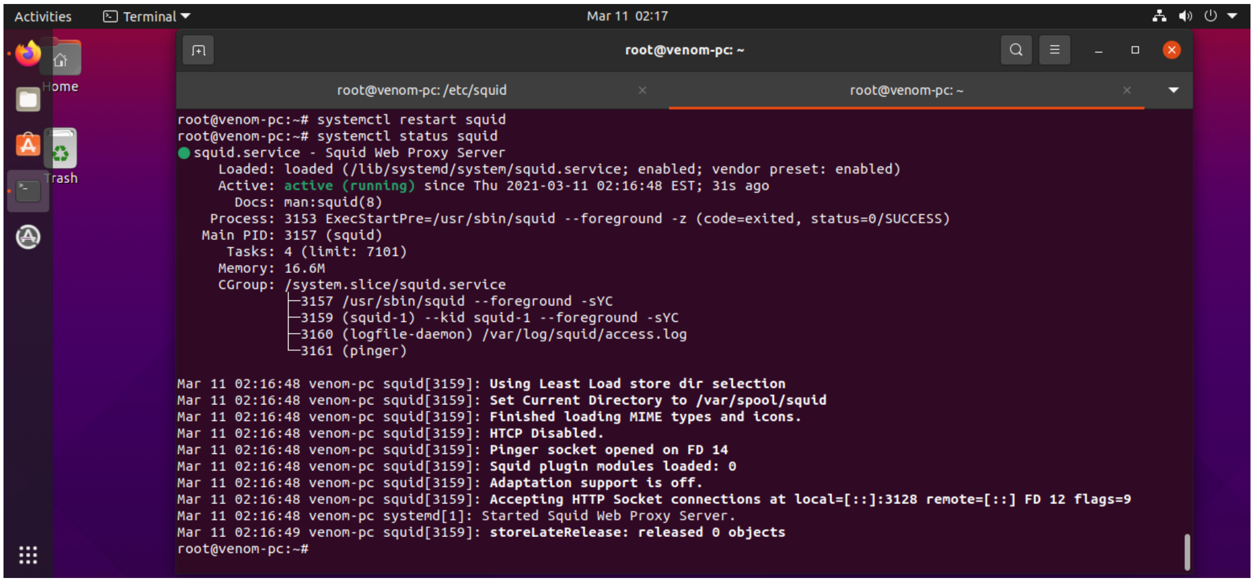
```
.Facebook.com
.MySpace.com
.YouTube.com
.DoubleClick.com
.Twitter.com
.Hotmail.com
.Orkut.com
.Twitch.tv.com
.Primevideo.com
.Netflix.com
.Disneyplus.com
~
~
```

vim whitelist_urls.txt.



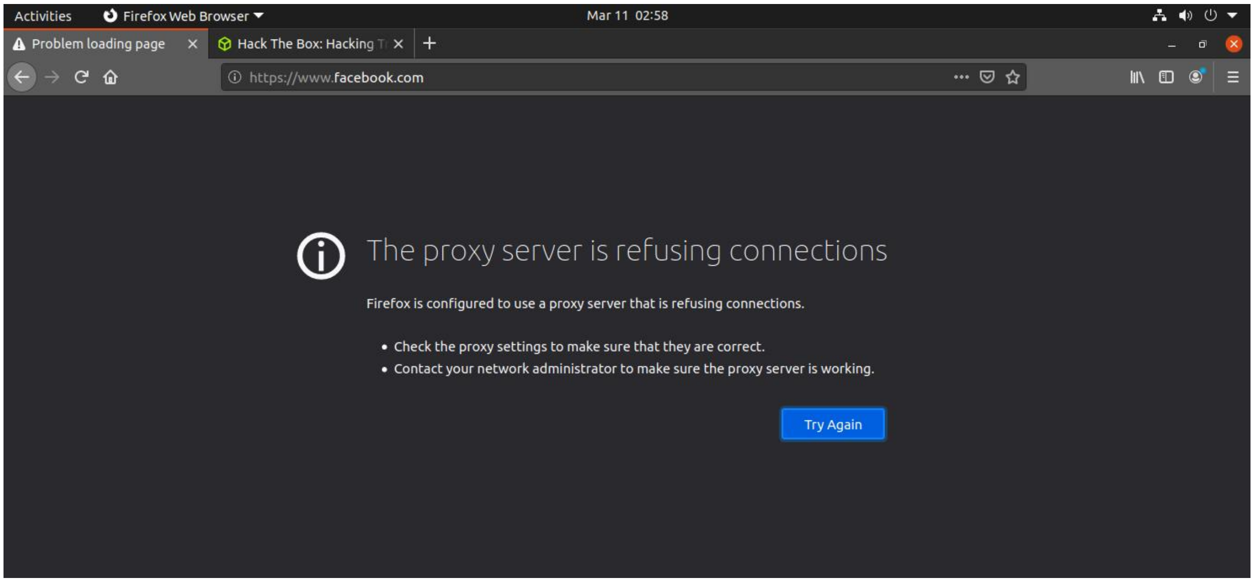
```
.google.com
.website1.com
.website2.com
.linkedin.com
.hackthebox.eu
.github.com
.azure.com
.redhat.com
.cisco.com
~
~
~
~
```

Restart the services And Check the status.



```
root@venom-pc:~# systemctl restart squid
root@venom-pc:~# systemctl status squid
● squid.service - Squid Web Proxy Server
     Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2021-03-11 02:16:48 EST; 31s ago
       Docs: man:squid(8)
    Process: 3153 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
   Main PID: 3157 (squid)
      Tasks: 4 (limit: 7101)
     Memory: 16.6M
     CGroup: /system.slice/squid.service
             ├─3157 /usr/sbin/squid --foreground -sYC
             ├─3159 (squid-1) --kid squid-1 --foreground -sYC
             ├─3160 (logfile-daemon) /var/log/squid/access.log
             └─3161 (pinger)

Mar 11 02:16:48 venom-pc squid[3159]: Using Least Load store dir selection
Mar 11 02:16:48 venom-pc squid[3159]: Set Current Directory to /var/spool/squid
Mar 11 02:16:48 venom-pc squid[3159]: Finished loading MIME types and icons.
Mar 11 02:16:48 venom-pc squid[3159]: HTCP Disabled.
Mar 11 02:16:48 venom-pc squid[3159]: Pinger socket opened on FD 14
Mar 11 02:16:48 venom-pc squid[3159]: Squid plugin modules loaded: 0
Mar 11 02:16:48 venom-pc squid[3159]: Adaptation support is off.
Mar 11 02:16:48 venom-pc squid[3159]: Accepting HTTP Socket connections at local=[::]:3128 remote=[::] FD 12 flags=9
Mar 11 02:16:48 venom-pc systemd[1]: Started Squid Web Proxy Server.
Mar 11 02:16:49 venom-pc squid[3159]: storeLateRelease: released 0 objects
root@venom-pc:~#
```

DENIED SITE

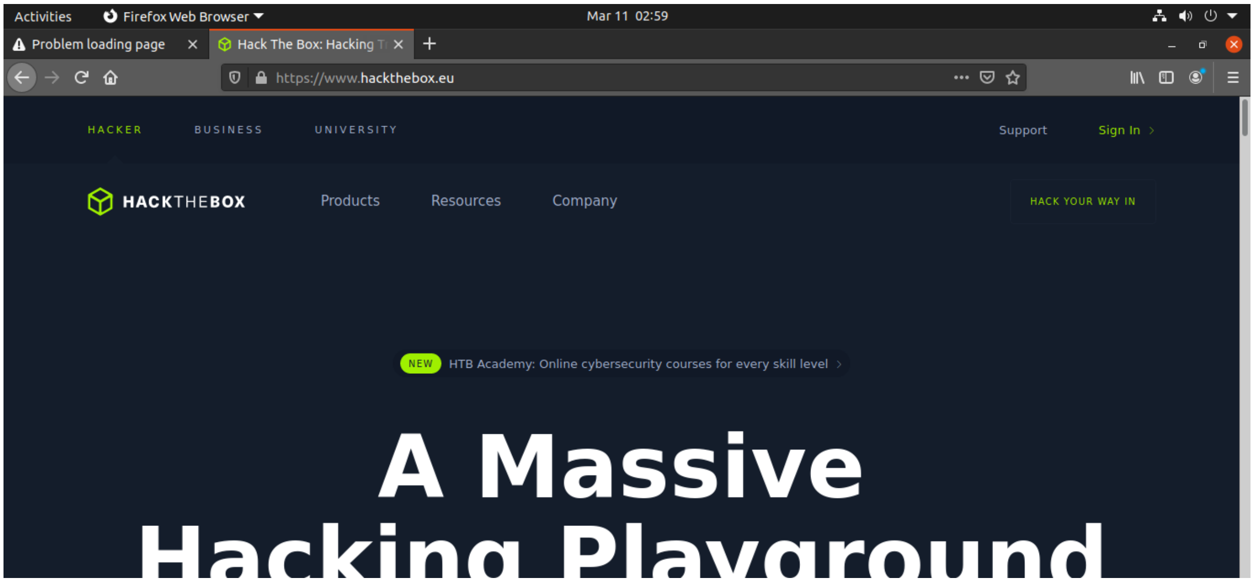


The proxy server is refusing connections

Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

ALLOWED SITE



HTB Academy: Online cybersecurity courses for every skill level

A Massive Hacking Playground