PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)

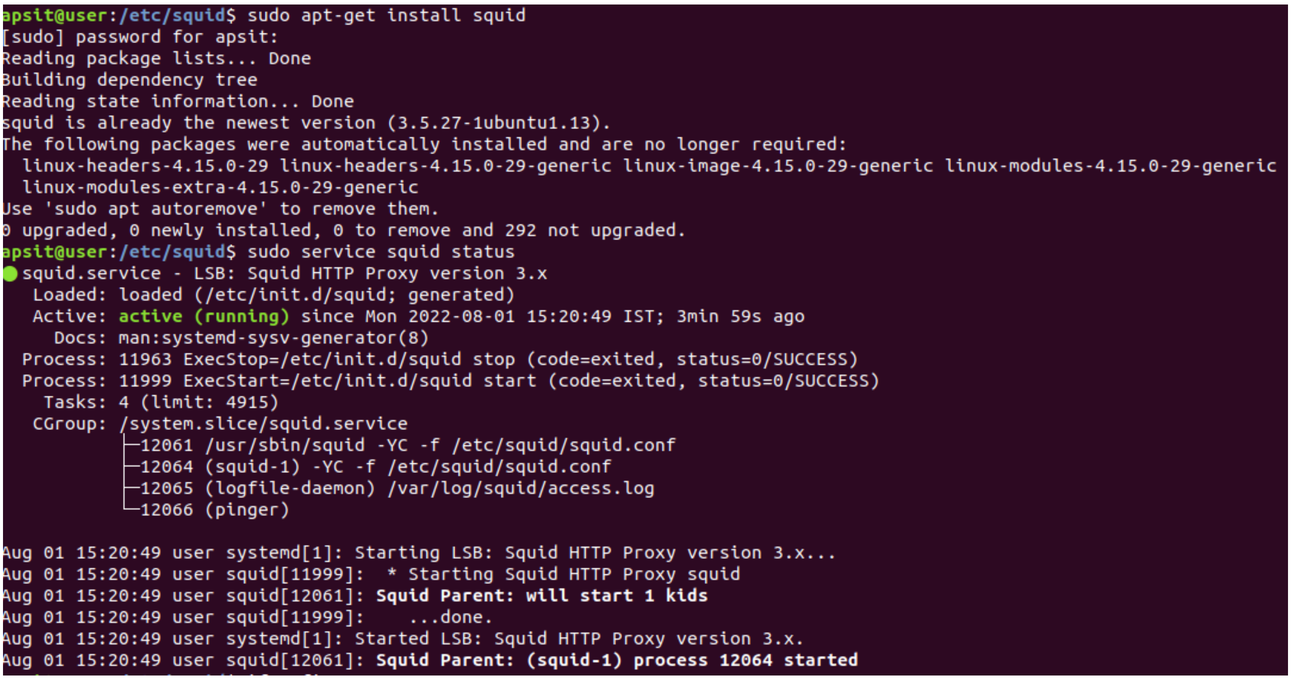
Department of Information Technology

Semester: V **Name of Student: visha**
Academic Year: 2022-23 **Student ID: 20104084**
Class / Branch: TE IT
Subject: Security Lab (SL)
Name of Instructor: Prof. Apeksha Mohite

EXPERIMENT NO. 2

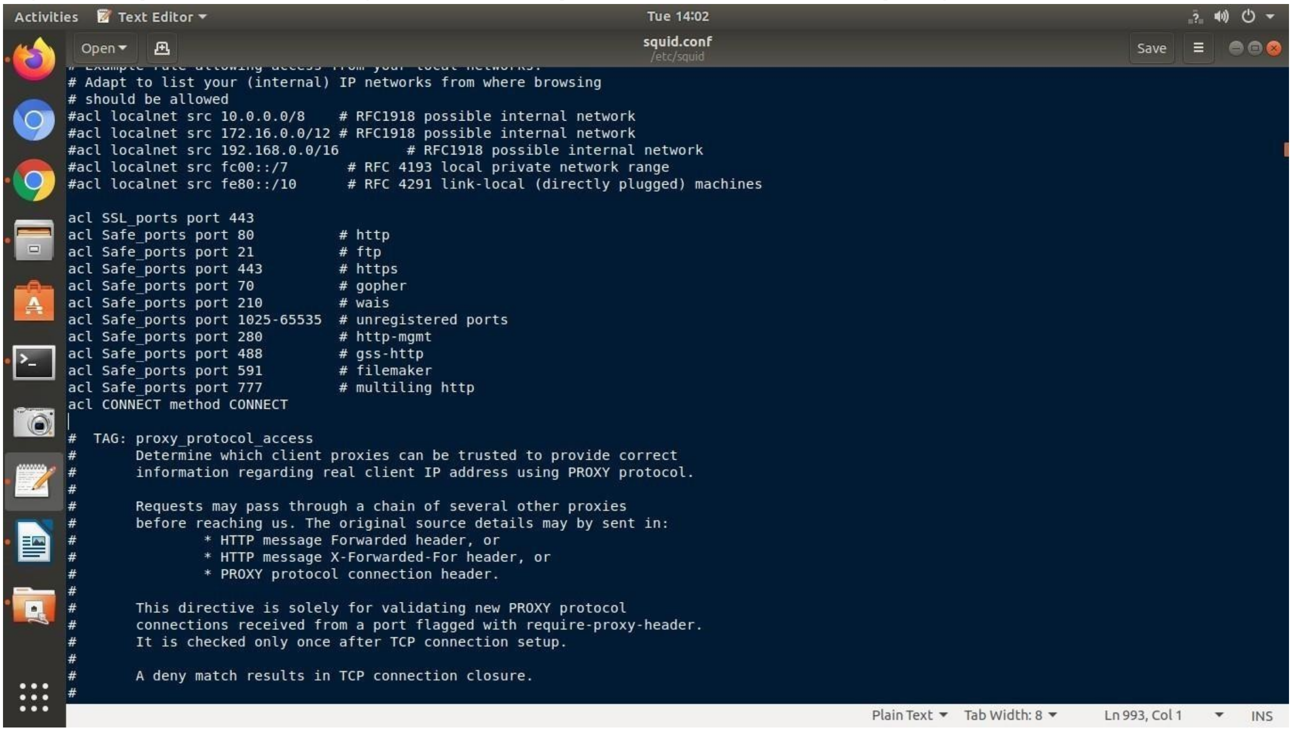
Aim: To Study use of access control Lists to deploy security policies of Web Acc

Verifying state of squid daemon and socket status after installation :



```
apsit@user:/etc/squid$ sudo apt-get install squid
[sudo] password for apsit:
Reading package lists... Done
Building dependency tree
Reading state information... Done
squid is already the newest version (3.5.27-1ubuntu1.13).
The following packages were automatically installed and are no longer required:
  linux-headers-4.15.0-29 linux-headers-4.15.0-29-generic linux-image-4.15.0-29-generic linux-modules-4.15.0-29-generic
  linux-modules-extra-4.15.0-29-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 292 not upgraded.
apsit@user:/etc/squid$ sudo service squid status
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; generated)
   Active: active (running) since Mon 2022-08-01 15:20:49 IST; 3min 59s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 11963 ExecStop=/etc/init.d/squid stop (code=exited, status=0/SUCCESS)
  Process: 11999 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/squid.service
           ├─12061 /usr/sbin/squid -YC -f /etc/squid/squid.conf
           ├─12064 (squid-1) -YC -f /etc/squid/squid.conf
           ├─12065 (logfile-daemon) /var/log/squid/access.log
           └─12066 (pinger)

Aug 01 15:20:49 user systemd[1]: Starting LSB: Squid HTTP Proxy version 3.x...
Aug 01 15:20:49 user squid[11999]:  * Starting Squid HTTP Proxy squid
Aug 01 15:20:49 user squid[12061]: Squid Parent: will start 1 kids
Aug 01 15:20:49 user squid[11999]:    ...done.
Aug 01 15:20:49 user systemd[1]: Started LSB: Squid HTTP Proxy version 3.x.
Aug 01 15:20:49 user squid[12061]: Squid Parent: (squid-1) process 12064 started
```

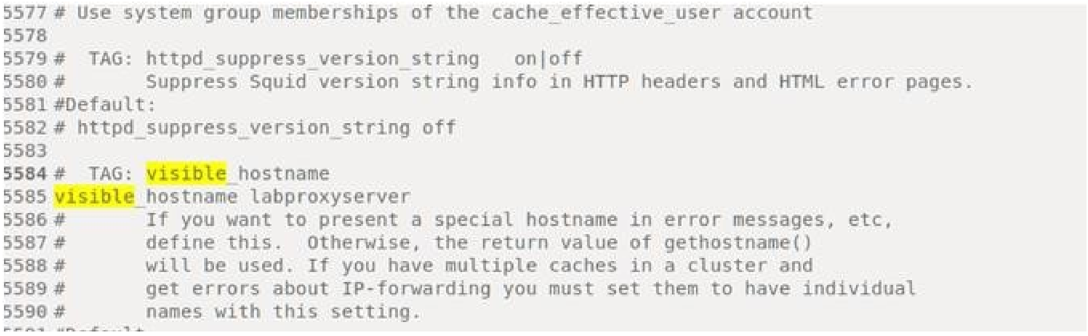
Squid Configuration file with required ACL directives and actions :
Log Analysis of Configured Proxy Server and verifying ACL directives working :



```
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
#acl localnet src 10.0.0.0/8    # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
#acl localnet src 192.168.0.0/16        # RFC1918 possible internal network
#acl localnet src fc00::/7       # RFC 4193 local private network range
#acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#  TAG: proxy_protocol_access
#       Determine which client proxies can be trusted to provide correct
#       information regarding real client IP address using PROXY protocol.
#
#       Requests may pass through a chain of several other proxies
#       before reaching us. The original source details may by sent in:
#               * HTTP message Forwarded header, or
#               * HTTP message X-Forwarded-For header, or
#               * PROXY protocol connection header.
#
#       This directive is solely for validating new PROXY protocol
#       connections received from a port flagged with require-proxy-header.
#       It is checked only once after TCP connection setup.
#
#       A deny match results in TCP connection closure.
#
```

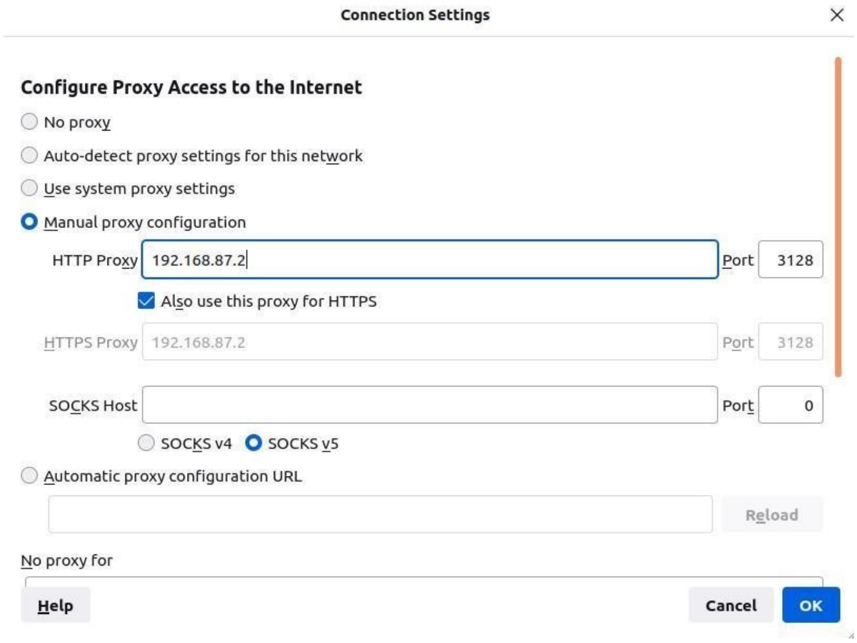
```
root@apsit-HP-245-G4-Notebook-PC:~# tail -f /var/log/squid/access.log

15/Apr/2017:15:51:48 +0530      155 192.168.3.140 TCP_MISS/200 3625 GET  ftp://192.168.25.25/ kzn/n
HIER_DIRECT/192.168.25.25 text/html
```

Changed Proxy Name



```
# Use system group memberships of the cache_effective_user account

#  TAG: httpd_suppress_version_string   on|off
#       Suppress Squid version string info in HTTP headers and HTML error pages.
#Default:
# httpd_suppress_version_string off

#  TAG: visible_hostname
visible_hostname labproxyserver
#       If you want to present a special hostname in error messages, etc,
#       define this.  Otherwise, the return value of gethostname()
#       will be used. If you have multiple caches in a cluster and
#       get errors about IP-forwarding you must set them to have individual
#       names with this setting.
```

FireFox Preference Changes



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 192.168.87.2 Port 3128

☑ Also use this proxy for HTTPS

HTTPS Proxy 192.168.87.2 Port 3128

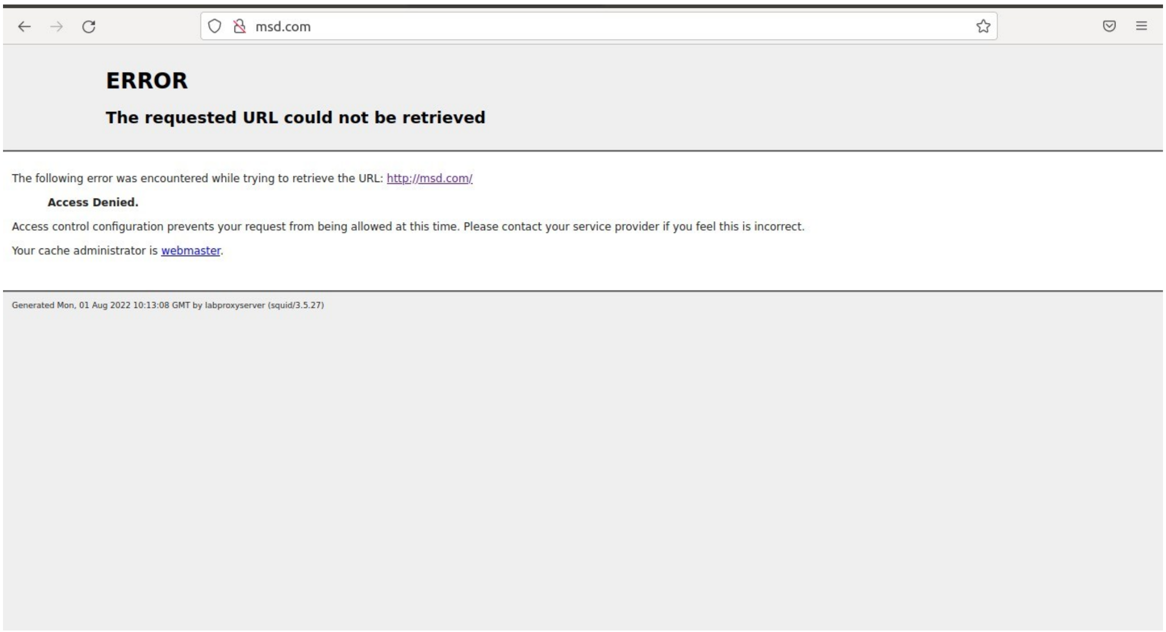
SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

firefox user Error



ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: http://msd.com/

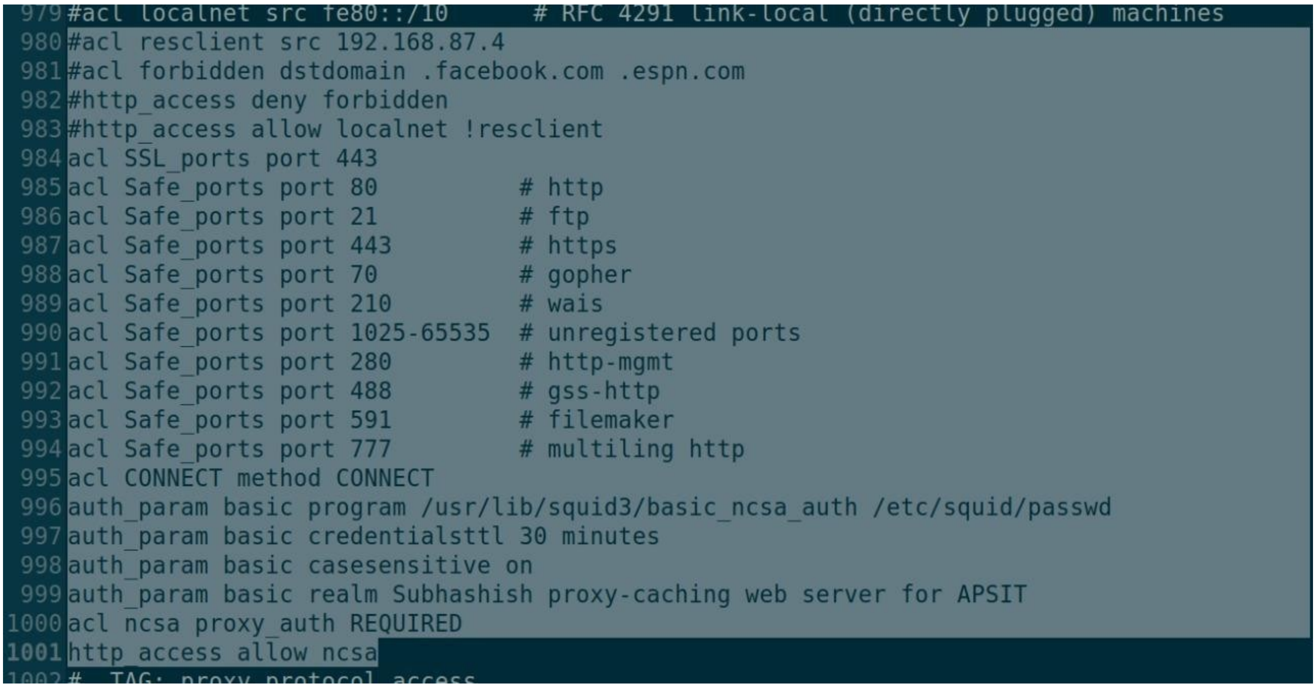
Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is webmaster.

Generated Mon, 01 Aug 2022 10:13:08 GMT by labproxyserver (squid/3.5.27)

Creating a Proxy By making Changes in Conf. files:



```
#acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines
#acl resclient src 192.168.87.4
#acl forbidden dstdomain .facebook.com .espn.com
#http_access deny forbidden
#http_access allow localnet !resclient
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid/passwd
auth_param basic credentialsttl 30 minutes
auth_param basic casesensitive on
auth_param basic realm Subhashish proxy-caching web server for APSIT
acl ncsa proxy_auth REQUIRED
http_access allow ncsa
#  TAG: proxy_protocol_access
```

Conclusion: Thus we have successfully studied use of access cont to deploy security policies of Web Access by configuring