Experiment 4: SQUID

AIM: To create and configure Squid -proxy server

DESCRIPTION:

SQUID – PROXY SERVER

Squid is a full-featured web proxy cache server application which provides proxy and cache services for HyperText Transport Protocol (HTTP), File Transfer Protocol (FTP), and other popular network protocols. Squid can implement caching and proxying of Secure Sockets Layer (SSL) requests and caching of Domain Name Server (DNS) lookups, and perform transparent caching. Squid also supports a wide variety of caching protocols, such as Internet Cache Protocol (ICP), the HyperText Caching Protocol (HTCP), the Cache Array Routing Protocol (CARP), and the Web Cache Coordination Protocol (WCCP).

The Squid proxy cache server is an excellent solution to various proxy and caching server needs, and scales from the branch office to enterprise-level networks while providing extensive, granular access control mechanisms, and monitoring of critical parameters via the Simple Network Management Protocol (SNMP). When selecting a computer system for use as a dedicated Squid caching proxy server for many users ensure it is configured with a large amount of physical memory as Squid maintains an in-memory cache for increased performance.

Port No: 3128

Package name: squid

Configuration file: /etc/squid/squid.conf

PROCEDURE:

1. At a terminal prompt, enter the following command to install the Squid server:

$sudo apt install squid

2. Squid is configured by editing the directives contained within the /etc/squid/squid.conf configuration file.

3. Change the access as shown below:

acl localnet src 192.168.234.139(your ip address)

acl blocksite dstdomain "/etc/squid/blocksite"

http_access deny blocksite

http_access allow localnet

#http_access deny all

http_access allow all

4. To block access to the website we must configure using

"/etc/squid/blocksite”

we edit the file by running:

$cd /etc/squid

$sudo gedit blocksite

5. Add the websites to block:

in this case, I am blocking youtube, facebook, google

6. To check the actual functioning of the proxy server go to the browser and click settings, search proxy in connection settings.

7. To configure Proxy access to the internet

8. Select Manual Proxy configuration

9. Type your HTTP Proxy(IP Address) and Port number as 3128.

10. Select SOCKS v5

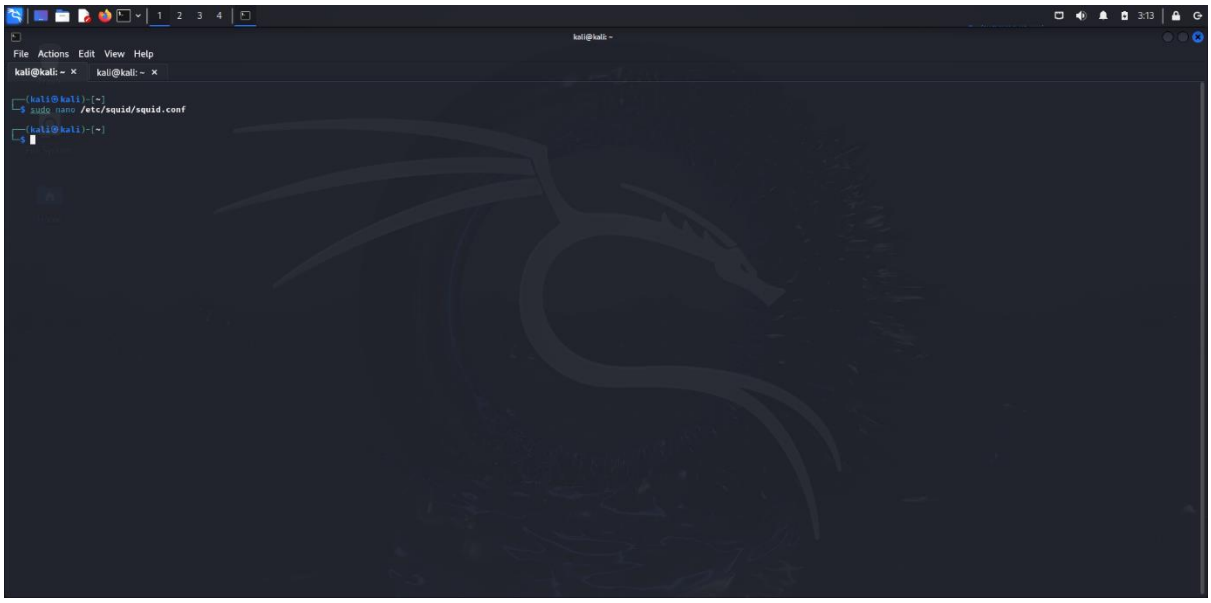
CONNECTING TO WEBSITE

11. Search for the blocked websites

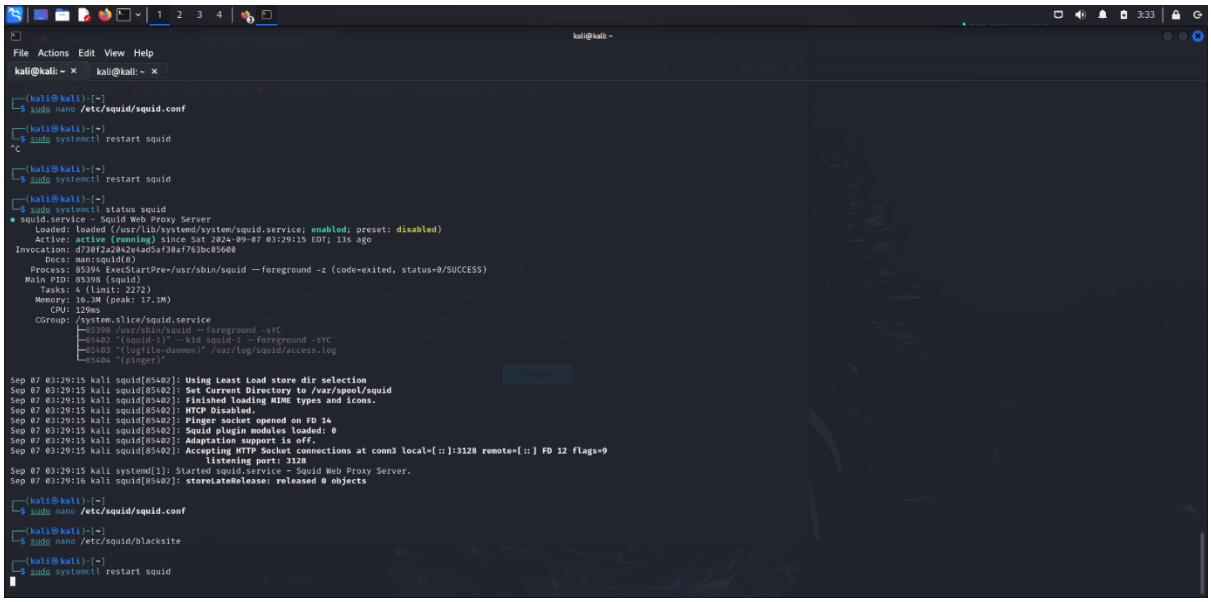
12. Access is denied to the above websites.

RESULT:

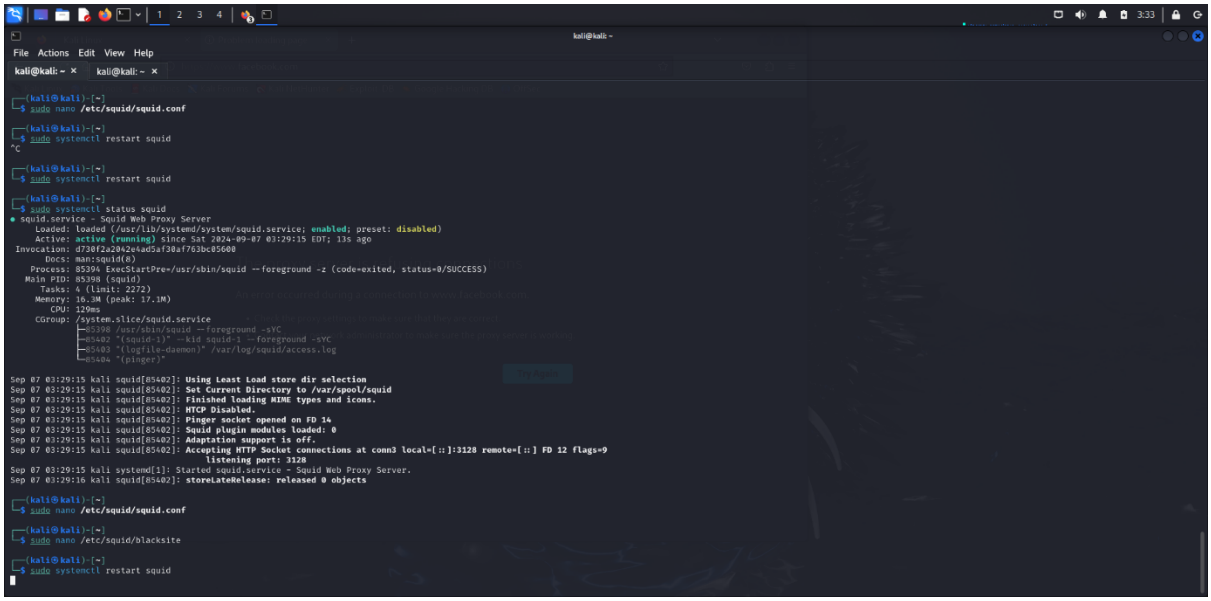

kali@kali: ~
File Actions Edit View Help
Processing triggers for libapache2-mod-php8.2 (8.2.21-1+b1) ...
(kali㉿kali)-[~]
$ sudo apt install squid
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
libavfilter9 libgeos3.12.1t64 libjxl0.7 libplacebo338 libpostproc57 libre2-10 libsvtav1enc1d1 libx265-199 openjdk-17-jre-headless python3-mistune0 python3-pytzdata rwhod samba-dsdb-modules
libdaxctl1 libjsoncpp25 libndctl6 libpmem1 libravie0 libroc0.3 libu2f-udev openjdk-17-jre python3-diskcache python3-pendulum rwho samba-ad-provision
Use 'sudo apt autoremove' to remove them.
Installing:
squid
Installing dependencies:
libecap3 squid-common squid-langpack
Suggested packages:
squidclient squid-cgi squid-purge resolvconf ufw winbind
Summary:
Upgrading: 0, Installing: 4, Removing: 0, Not Upgrading: 3
Download size: 3,385 kB
Space needed: 14.6 MB / 63.5 GB available
Continue? [Y/n] Y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libecap3 amd64 1.0.1-3.4+b1 [17.2 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 squid-langpack all 20220130-1 [169 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 squid-common all 6.10-1 [320 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 squid amd64 6.10-1 [2,879 kB]
Fetched 3,385 kB in 5s (733 kB/s)
Selecting previously unselected package libecap3:amd64.
(Reading database ... 403564 files and directories currently installed.)
Preparing to unpack .../libecap3_1.0.1-3.4+b1_amd64.deb ...
Unpacking libecap3:amd64 (1.0.1-3.4+b1) ...
Selecting previously unselected package squid-langpack.
Preparing to unpack .../squid-langpack_20220130-1_all.deb ...
Unpacking squid-langpack (20220130-1) ...
Selecting previously unselected package squid-common.
Preparing to unpack .../squid-common_6.10-1_all.deb ...
Unpacking squid-common (6.10-1) ...
Selecting previously unselected package squid.
Preparing to unpack .../squid_6.10-1_amd64.deb ...
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
Unpacking squid (6.10-1) ...
Setting up squid-langpack (20220130-1) ...
Setting up libecap3:amd64 (1.0.1-3.4+b1) ...
Setting up squid-common (6.10-1) ...
Setting up squid (6.10-1) ...
Setcap worked! /usr/lib/squid/pinger is not suid!
Skipping profile in /etc/apparmor.d/disable: usr.sbin.squid

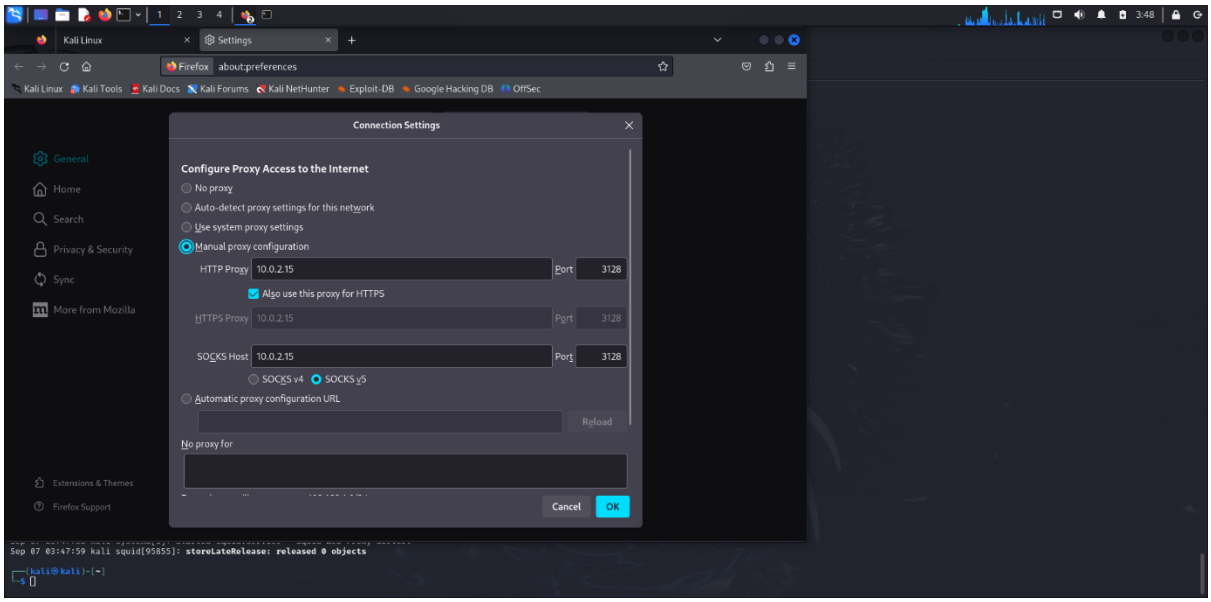

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
(kali㉿kali)-[~]
$ sudo nano /etc/squid/squid.conf
(kali㉿kali)-[~]
$

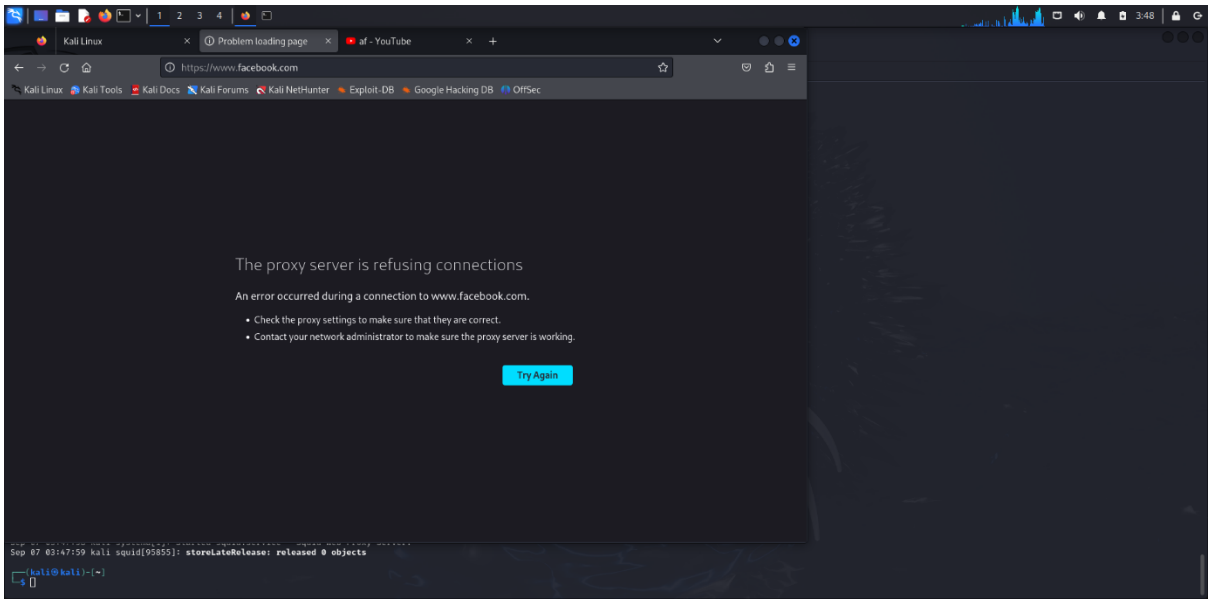

kali@kali: ~
File Actions Edit View Help
GNU nano 8.1 /etc/squid/squid.conf
The two deny rules below are unnecessary in this default configuration
because they are followed by a "deny all" rule. However, they may become
critically important when you start allowing external requests below them.
Protect web applications running on the same server as Squid. They often
assume that only local users can access them at "localhost" ports.
http_access deny to_localhost
Protect cloud servers that provide local users with sensitive info about
their server via certain well-known link-local (a.k.a. APIPA) addresses.
http_access deny to_linklocal
#
INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*.conf
For example, to allow access from your local networks, you may uncomment the
following rule (and/or add rules that match your definition of "local"):
http_access allow localnet
And finally deny all other access to this proxy
acl localnet src 10.0.2.15
acl blocksite dstdomain "/etc/squid/blocksite"
http_access deny blocksite
http_access allow localnet
#http_access deny all
http_access allow all
TAG: adapted_http_access
Allowing or Denying access based on defined access lists
#
Essentially identical to http_access, but runs after redirectors
and ICAP/eCAP adaptation. Allowing access control based on their
output.
#
If not set then only http_access is used.
#Default:
Allow, unless rules exist in squid.conf.
TAG: http_reply_access
Allow replies to client requests. This is complementary to http_access.
#
http_reply_access allow|deny [!] aclname ...
#
NOTE: if there are no access lines present, the default is to allow
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous ^B Back ^← Prev Word ^A Home
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-W Next ^F Forward ^→ Next Word ^E End


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nano /etc/squid/squid.conf
(kali㉿kali)-[~]
$ sudo systemctl restart squid
^C
(kali㉿kali)-[~]
$ sudo systemctl restart squid
(kali㉿kali)-[~]
$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; preset: disabled)
Active: active (running) since Sat 2024-09-07 03:29:15 EDT; 13s ago
Invocation: d730f2a204204ad5af30af763bc05600
Docs: man:squid(8)
Process: 85394 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
Main PID: 85398 (squid)
Tasks: 4 (limit: 2272)
Memory: 16.3M (peak: 17.1M)
CPU: 129ms
CGroup: /system.slice/squid.service
├─85398 /usr/sbin/squid --foreground -sYC
├─85402 "(squid-1)" --kid squid-1 --foreground -sYC
├─85403 "(logfile-daemon)" /var/log/squid/access.log
└─85404 "(pinger)"
Sep 07 03:29:15 kali squid[85402]: Using Least Load store dir selection
Sep 07 03:29:15 kali squid[85402]: Set Current Directory to /var/spool/squid
Sep 07 03:29:15 kali squid[85402]: Finished loading MIME types and icons.
Sep 07 03:29:15 kali squid[85402]: HTCP Disabled.
Sep 07 03:29:15 kali squid[85402]: Pinger socket opened on FD 14
Sep 07 03:29:15 kali squid[85402]: Squid plugin modules loaded: 0
Sep 07 03:29:15 kali squid[85402]: Adaptation support is off.
Sep 07 03:29:15 kali squid[85402]: Accepting HTTP Socket connections at conn3 local=[::]:3128 remote=[::] FD 12 flags=9
listening port: 3128
Sep 07 03:29:15 kali systemd[1]: Started squid.service - Squid Web Proxy Server.
Sep 07 03:29:16 kali squid[85402]: storeLateRelease: released 0 objects
(kali㉿kali)-[~]
$ sudo nano /etc/squid/squid.conf
(kali㉿kali)-[~]
$ sudo nano /etc/squid/blacksite
(kali㉿kali)-[~]
$ sudo systemctl restart squid


kali@kali: ~
File Actions Edit View Help
GNU nano 8.1 /etc/squid/blocksite
facebook.com
[Read 2 lines]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous ^B Back ^← Prev Word ^A Home
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-W Next ^F Forward ^→ Next Word ^E End


kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
$ sudo nano /etc/squid/squid.conf
$ sudo systemctl restart squid
^C
$ sudo systemctl restart squid
$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; preset: disabled)
Active: active (running) since Sat 2024-09-07 03:29:15 EDT; 13s ago
Invocation: d730f2a2042e4ad5af30af763bc05600
Docs: man:squid(8)
Process: 85394 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
Main PID: 85398 (squid)
Tasks: 4 (limit: 2272)
Memory: 16.3M (peak: 17.1M)
CPU: 129ms
CGroup: /system.slice/squid.service
Sep 07 03:29:15 kali squid[85402]: Using Least Load store dir selection
Sep 07 03:29:15 kali squid[85402]: Set Current Directory to /var/spool/squid
Sep 07 03:29:15 kali squid[85402]: Finished loading MIME types and icons.
Sep 07 03:29:15 kali squid[85402]: HTCP Disabled.
Sep 07 03:29:15 kali squid[85402]: Pinger socket opened on FD 14
Sep 07 03:29:15 kali squid[85402]: Squid plugin modules loaded: 0
Sep 07 03:29:15 kali squid[85402]: Adaptation support is off.
Sep 07 03:29:15 kali squid[85402]: Accepting HTTP Socket connections at conn3 local=[::]:3128 remote=[::] FD 12 flags=9
listening port: 3128
Sep 07 03:29:15 kali systemd[1]: Started squid.service - Squid Web Proxy Server.
Sep 07 03:29:16 kali squid[85402]: storeLateRelease: released 0 objects
$ sudo nano /etc/squid/squid.conf
$ sudo nano /etc/squid/blacksite
$ sudo systemctl restart squid


Kali Linux
Settings
Firefox about:preferences
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Extensions & Themes
Firefox Support
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 10.0.2.15 Port 3128
Also use this proxy for HTTPS
HTTPS Proxy 10.0.2.15 Port 3128
SOCKS Host 10.0.2.15 Port 3128
SOCKS v4 SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Cancel OK
Sep 07 03:47:59 kali squid[95855]: storeLateRelease: released 0 objects


Kali Linux
Problem loading page
af - YouTube
https://www.facebook.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
The proxy server is refusing connections
An error occurred during a connection to www.facebook.com.
Check the proxy settings to make sure that they are correct.
Contact your network administrator to make sure the proxy server is working.
Try Again
Sep 07 03:47:59 kali squid[95855]: storeLateRelease: released 0 objects

All the commands have been executed and the output has been obtained successfully.