SQUID

Experiment: 4

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.

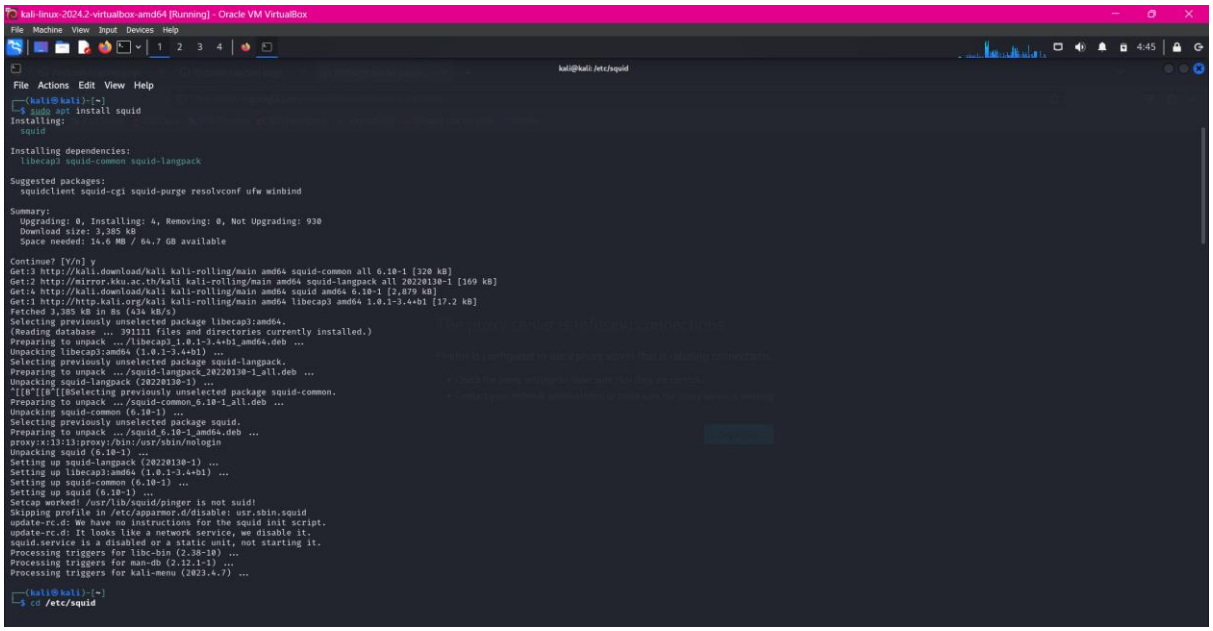
10. Select SOCKS v5

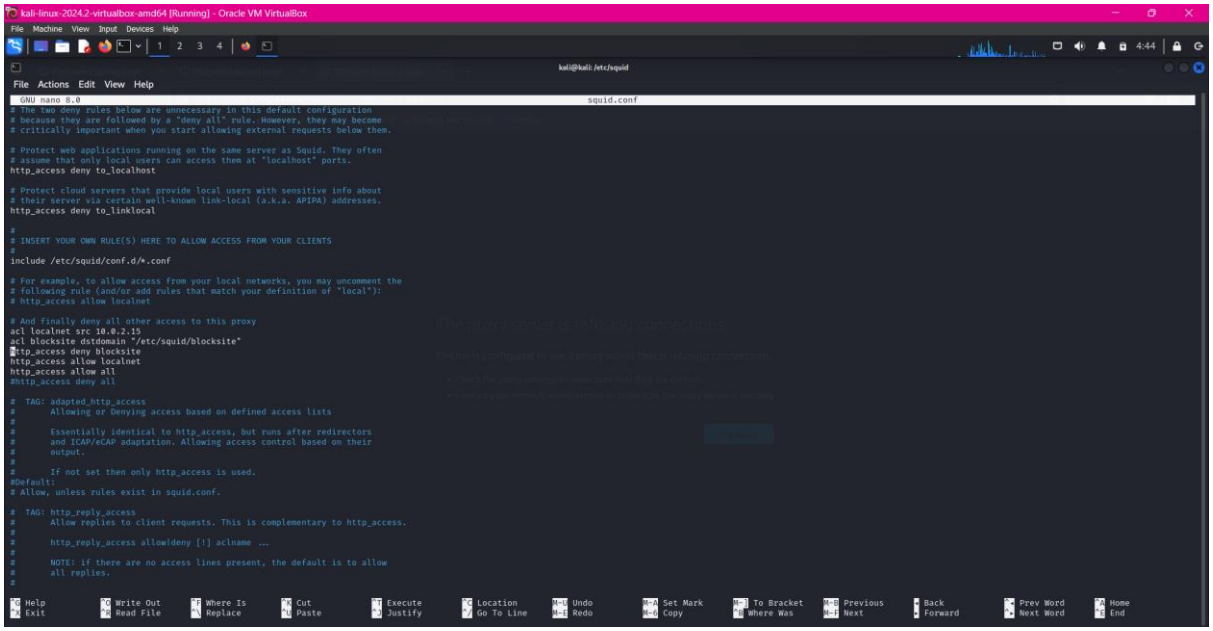
CONNECTING TO WEBSITE

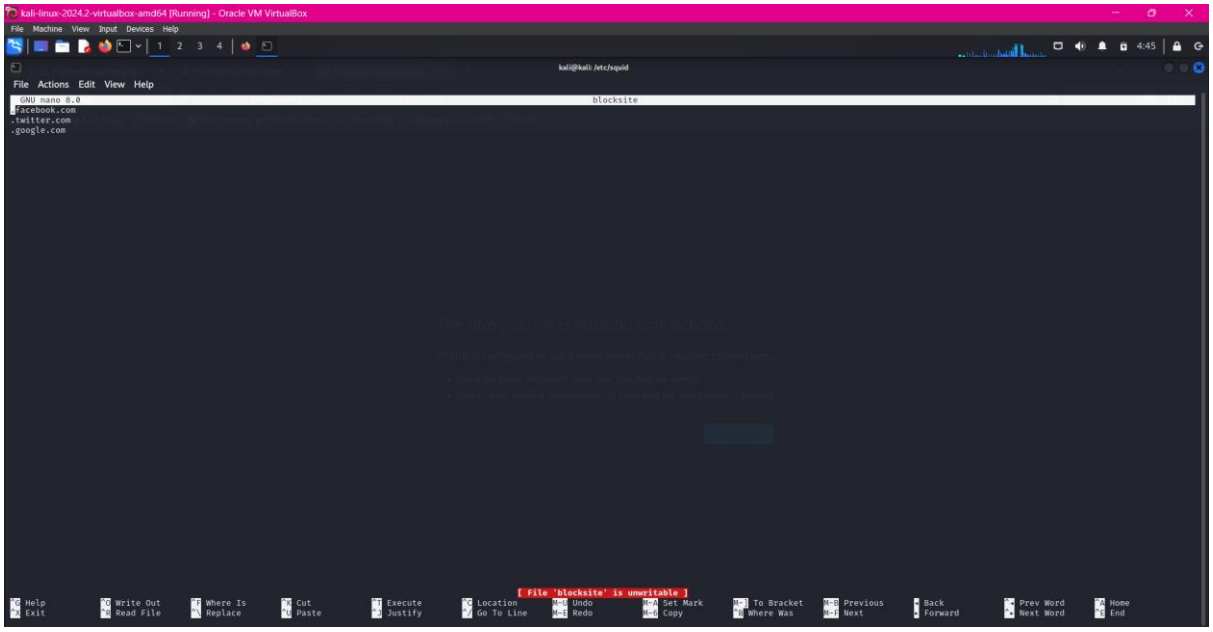
11. Search for the blocked websites

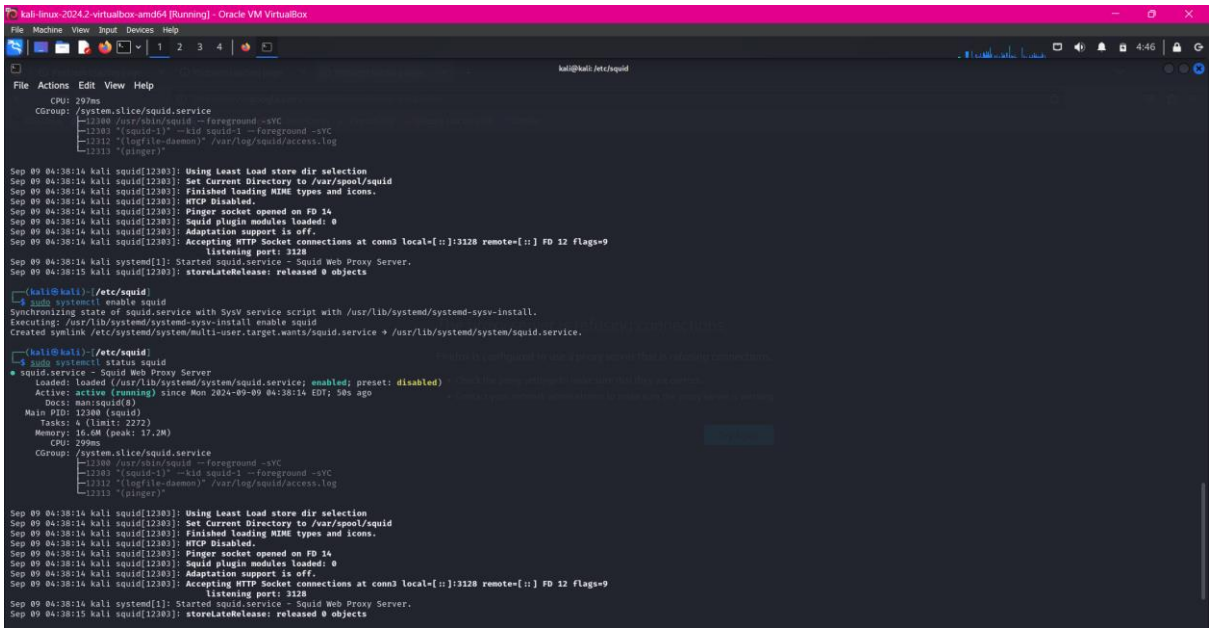
12. Access is denied to the above websites

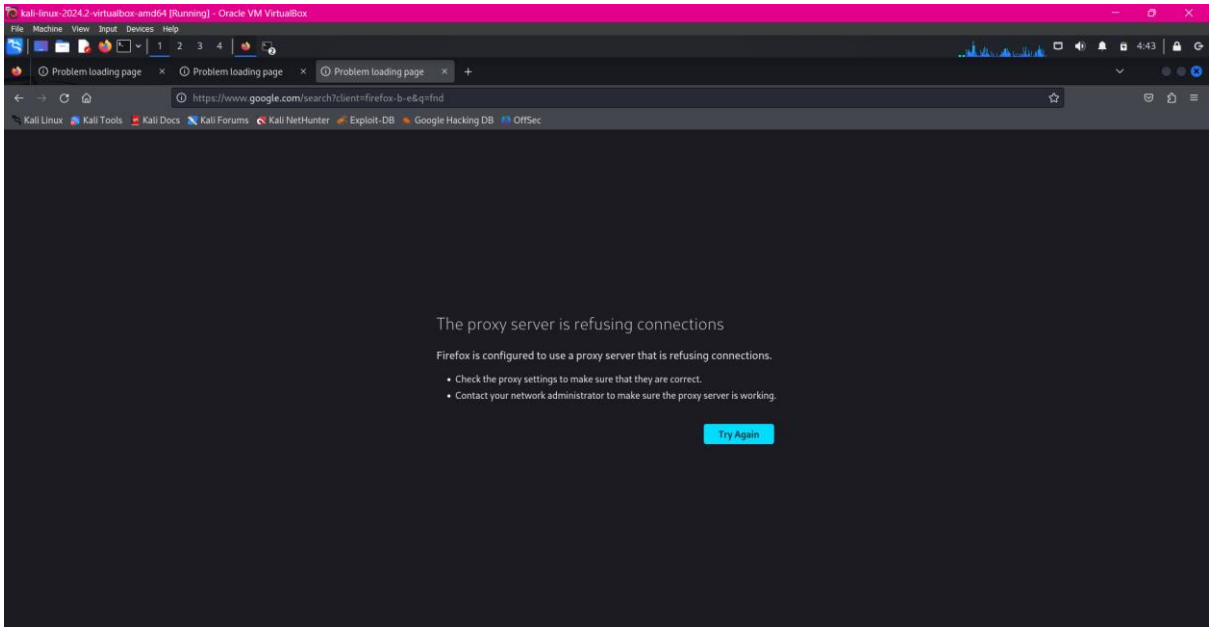
Result:

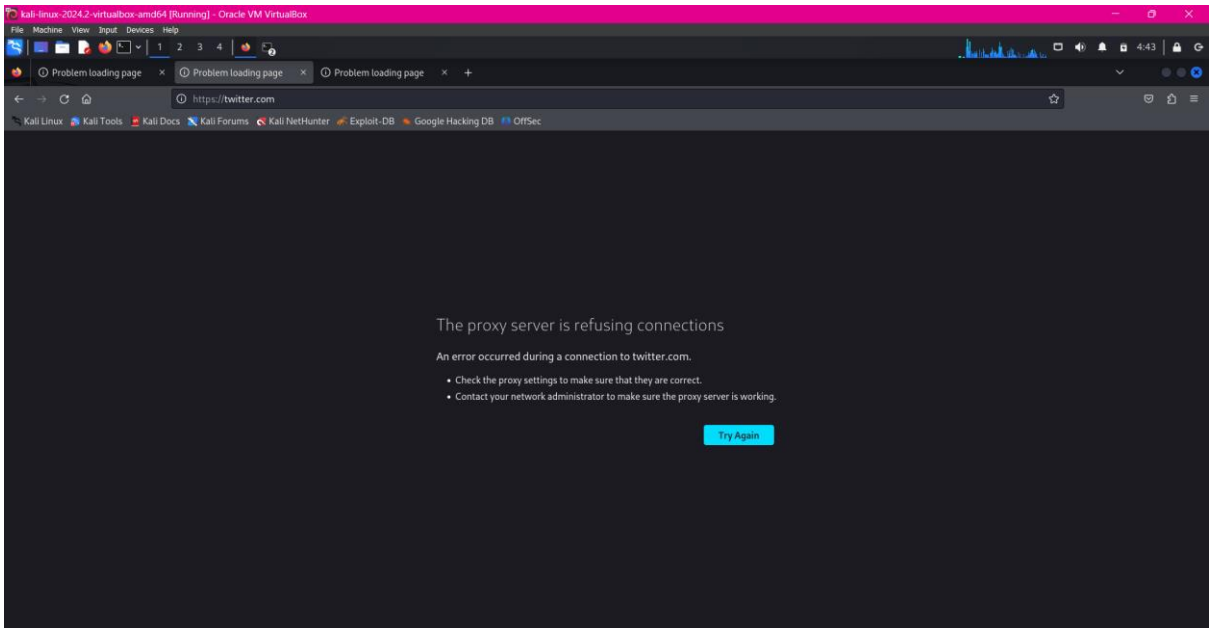

kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: /etc/squid
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt install squid
Installing:
squid
Installing dependencies:
libecap3 squid-common squid-langpack
Suggested packages:
squidclient squid-cgi squid-purge resolvconf ufw winbind
Summary:
Upgrading: 0, Installing: 4, Removing: 0, Not Upgrading: 930
Download size: 3,385 kB
Space needed: 14.6 MB / 64.7 GB available
Continue? [Y/n] y
Get:3 http://kali.download/kali kali-rolling/main amd64 squid-common all 6.10-1 [320 kB]
Get:2 http://mirror.kku.ac.th/kali kali-rolling/main amd64 squid-langpack all 20220130-1 [169 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 squid amd64 6.10-1 [2,879 kB]
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libecap3 amd64 1.0.1-3.4+b1 [17.2 kB]
Fetched 3,385 kB in 8s (434 kB/s)
Selecting previously unselected package libecap3:amd64.
(Reading database ... 391111 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
update-rc.d: We have no instructions for the squid init script.
update-rc.d: It looks like a network service, we disable it.
squid.service is a disabled or a static unit, not starting it.
Processing triggers for libc-bin (2.38-10) ...
Processing triggers for man-db (2.12.1-1) ...
Processing triggers for kali-menu (2023.4.7) ...
(kali㉿kali)-[~]
$ cd /etc/squid

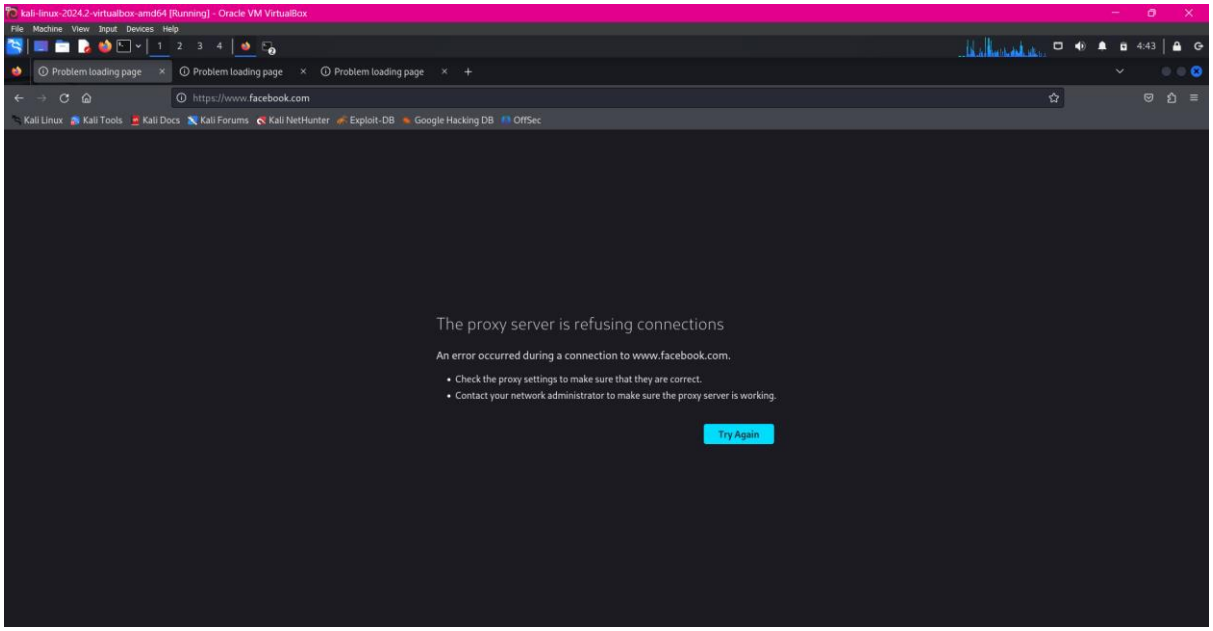

kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: /etc/squid
File Actions Edit View Help
GNU nano 8.0 squid.conf
The two deny rules below are unnecessary in this default configuration
because they are followed by a "deny all" rule. However, 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 allow all
#http_access deny 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
all replies.
#
^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-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: /etc/squid
File Actions Edit View Help
GNU nano 8.0 blocksite
.facebook.com
.twitter.com
.google.com
[File 'blocksite' is unwritable]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket ^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 ^W Where Was ^V Next ^F Forward ^→ Next Word ^E End


kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: /etc/squid
File Actions Edit View Help
CPU: 297ms
CGroup: /system.slice/squid.service
├─12300 /usr/sbin/squid --foreground -sYC
├─12303 "(squid-1)" --kid squid-1 --foreground -sYC
├─12312 "(logfile-daemon)" /var/log/squid/access.log
└─12313 "(pinger)"
Sep 09 04:38:14 kali squid[12303]: Using Least Load store dir selection
Sep 09 04:38:14 kali squid[12303]: Set Current Directory to /var/spool/squid
Sep 09 04:38:14 kali squid[12303]: Finished loading MIME types and icons.
Sep 09 04:38:14 kali squid[12303]: HTCP Disabled.
Sep 09 04:38:14 kali squid[12303]: Pinger socket opened on FD 14
Sep 09 04:38:14 kali squid[12303]: Squid plugin modules loaded: 0
Sep 09 04:38:14 kali squid[12303]: Adaptation support is off.
Sep 09 04:38:14 kali squid[12303]: Accepting HTTP Socket connections at conn3 local=[::]:3128 remote=[::] FD 12 flags=9
listening port: 3128
Sep 09 04:38:14 kali systemd[1]: Started squid.service - Squid Web Proxy Server.
Sep 09 04:38:15 kali squid[12303]: storeLateRelease: released 0 objects
(kali㉿kali)-[/etc/squid]
$ sudo systemctl enable squid
Synchronizing state of squid.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable squid
Created symlink /etc/systemd/system/multi-user.target.wants/squid.service → /usr/lib/systemd/system/squid.service.
(kali㉿kali)-[/etc/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 Mon 2024-09-09 04:38:14 EDT; 50s ago
Docs: man:squid(8)
Main PID: 12300 (squid)
Tasks: 4 (limit: 2272)
Memory: 16.6M (peak: 17.2M)
CPU: 299ms
CGroup: /system.slice/squid.service
├─12300 /usr/sbin/squid --foreground -sYC
├─12303 "(squid-1)" --kid squid-1 --foreground -sYC
├─12312 "(logfile-daemon)" /var/log/squid/access.log
└─12313 "(pinger)"
Sep 09 04:38:14 kali squid[12303]: Using Least Load store dir selection
Sep 09 04:38:14 kali squid[12303]: Set Current Directory to /var/spool/squid
Sep 09 04:38:14 kali squid[12303]: Finished loading MIME types and icons.
Sep 09 04:38:14 kali squid[12303]: HTCP Disabled.
Sep 09 04:38:14 kali squid[12303]: Pinger socket opened on FD 14
Sep 09 04:38:14 kali squid[12303]: Squid plugin modules loaded: 0
Sep 09 04:38:14 kali squid[12303]: Adaptation support is off.
Sep 09 04:38:14 kali squid[12303]: Accepting HTTP Socket connections at conn3 local=[::]:3128 remote=[::] FD 12 flags=9
listening port: 3128
Sep 09 04:38:14 kali systemd[1]: Started squid.service - Squid Web Proxy Server.
Sep 09 04:38:15 kali squid[12303]: storeLateRelease: released 0 objects


kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Problem loading page
Problem loading page
Problem loading page
https://www.google.com/search?client=firefox-b-e&q=fnd
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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.
Try Again


kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Problem loading page
Problem loading page
Problem loading page
https://twitter.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 twitter.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



.

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