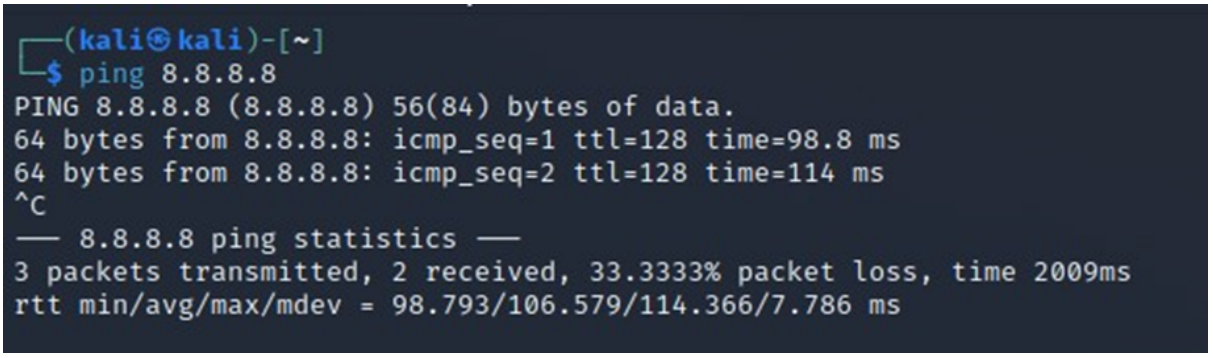
Squid

> This lab introduces the installation and configuration of Squid proxy, along with the analysis of Squid logs

Ping Test:

1. Open the command line interface.
2. Enter the command `ping 8.8.8.8` to check the connection to the IP address 8.8.8.8.



Finding Kali Linux IP Address:

1. Open the command line interface.
2. Enter the command `ifconfig` to display the network interfaces and their corresponding IP addresses.

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.128  netmask 255.255.255.0  broadcast 192.168.32.255
        inet6 fe80::6fd3:e042:78b9:61d7  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:28:b1:f6  txqueuelen 1000  (Ethernet)
        RX packets 4  bytes 598 (598.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27  bytes 3450 (3.3 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 24  bytes 1240 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1240 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Enabling Website Logging in Squid Proxy:

1. Open the Squid configuration file (typically located at `/etc/squid/squid.conf`) using a text editor.
2. Add the following lines after the last line in the "http_access" section:

````
acl localnet src 192.168.32.128/24
http_access allow localnet
```
Comment out the lines by adding a `#` at the beginning.
````

3. Uncomment the line that starts with `logformat` to enable logging of requested websites.
4. Save the changes to the configuration file and exit the text editor.

```
1187 # should be allowed
1188 #acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
1189 #acl localnet src 10.0.0.0/8            # RFC 1918 local private network (LAN)
1190 #acl localnet src 100.64.0.0/10         # RFC 6598 shared address space (CGN)
1191 #acl localnet src 169.254.0.0/16        # RFC 3927 link-local (directly plugged) machines
1192 #acl localnet src 172.16.0.0/12         # RFC 1918 local private network (LAN)
1193 #acl localnet src 192.168.0.0/16               # RFC 1918 local private network (LAN)
1194 #acl localnet src fc00::/7              # RFC 4193 local private network range
1195 #acl localnet src fe80::/10             # RFC 4291 link-local (directly plugged) machines
1196 acl localnet src 192.168.32.128
1197 http_access allow localnet
1198
```
```

```
4173 #
4174 #logformat squid      %ts.%03tu %6tr %>a %Ss/%03>Hs %<st %rm %ru %[un %Sh/%<a %mt
4175 #logformat common     %>a %[ui %[un [%tl] "%rm %ru HTTP/%rv" %>Hs %<st %Ss:%Sh
4176 logformat combined   %>a %[ui %[un [%tl] "%rm %ru HTTP/%rv" %>Hs %<st "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh
4177 access_log daemon:/var/log/squid/access.log combined
4178 #logformat referrer   %ts.%03tu %>a %{Referer}>h %ru
4179 #logformat useragent  %>a [%tl] "%{User-Agent}>h"
```

```
4176 logformat combined   %>a %[ui %[un [%tl] "%rm %ru HTTP/%rv" %>Hs %<st "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh
4177 access_log daemon:/var/log/squid/access.log combined
```

Enabling and Starting Squid Service:

1. Enter the command to enable the Squid service: `systemctl enable squid`.
2. Enter the command to start the Squid service: `systemctl start squid`.

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable squid.service
Synchronizing state of squid.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable squid
Created symlink /etc/systemd/system/multi-user.target.wants/squid.service → /lib/systemd/system/squid.service.
```

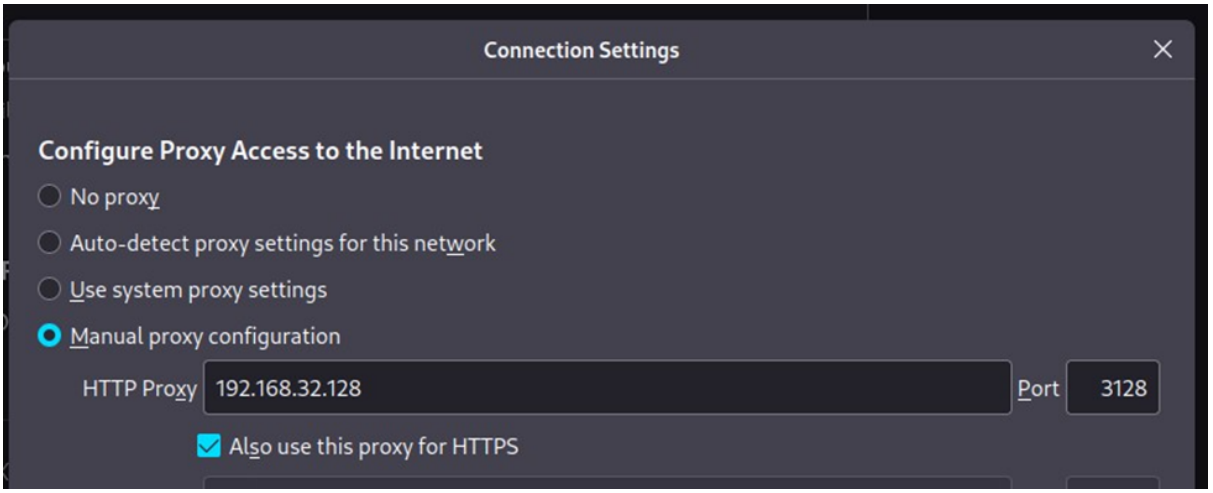
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start squid.service

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status squid.service
● squid.service - Squid Web Proxy Server
     Loaded: loaded (/lib/systemd/system/squid.service; enabled; preset: disabled)
     Active: active (running) since Mon 2023-01-30 17:49:20 EST; 5s ago
       Docs: man:squid(8)
    Process: 6034 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
    Process: 6037 ExecStart=/usr/sbin/squid -sYC (code=exited, status=0/SUCCESS)
   Main PID: 6043 (squid)
      Tasks: 4 (limit: 4500)
     Memory: 15.1M
        CPU: 724ms
     CGroup: /system.slice/squid.service
             ├─6043 /usr/sbin/squid -sYC
             ├─6045 "(squid-1)" --kid squid-1 -sYC
             ├─6047 "(logfile-daemon)" /var/log/squid/access.log
             └─6048 "(pinger)"
```

Checking Open Ports

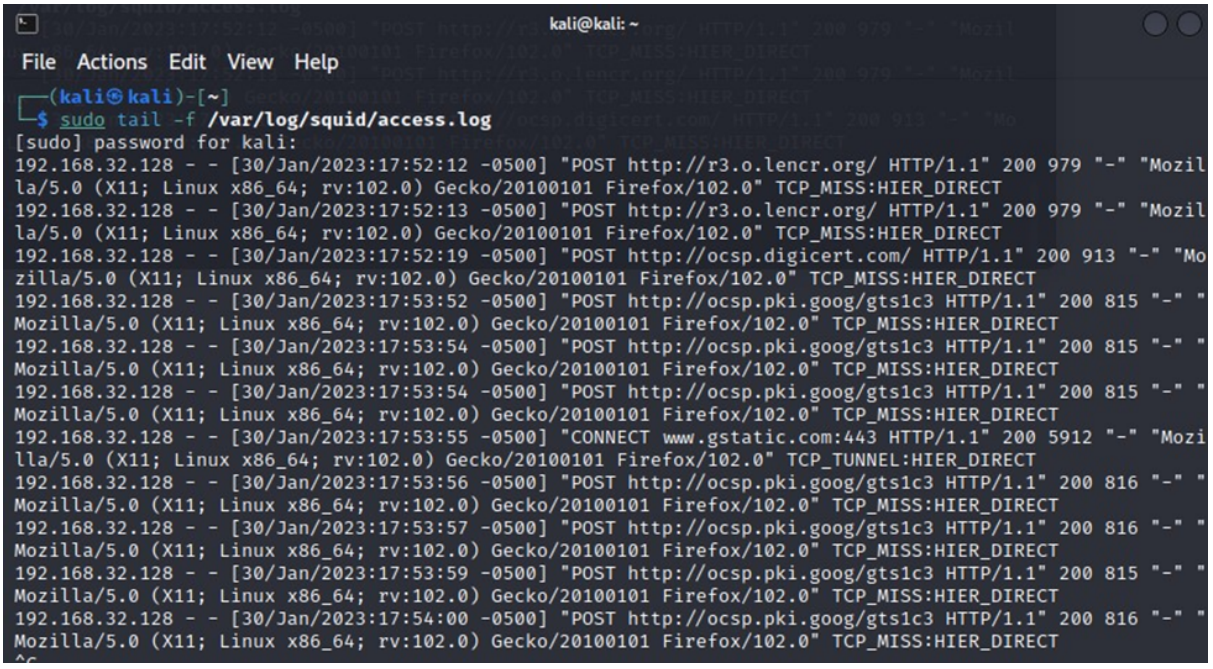
```
┌──(kali㉿kali)-[~]
└─$ sudo lsof -i -P -n | grep LISTEN
squid     6045 proxy   12u  IPv6  32452      0t0  TCP *:3128 (LISTEN)
```

By correctly configuring this settings you will have visibility of visited websites on your network. This allows you to analyze these websites and block/filter as necessary



Monitoring Access.log:

1. Use a log analysis tool or open the `access.log` file in a text editor to monitor the requested websites.



To display the most frequently-requested websites in squid proxy log:

```
┌──(kali㉿kali)-[~]
└─$ sudo grep "CONNECT" /var/log/squid/access.log | awk '{print $7}' | sort| uniq -c | sort -nr | head -n
 20
     18 www.moi.gov.sa:443
     17 www.uj.edu.sa:443
     14 prg-apac.smartadserver.com:443
     14 prebid.a-mo.net:443
     14 oss.maxcdn.com:443
     13 px.vliplatform.com:443
     12 prebid.media.net:443
     11 tlx.3lift.com:443
     11 prebid-asia.creativecdn.com:443
     11 pbjs.e-planning.net:443
     11 moe.gov.sa:443
     10 ib.adnxs.com:443
     10 cdnjs.cloudflare.com:443
      9 targeting.unrulymedia.com:443
      9 safebrowsing.googleapis.com:443
      7 kaust.edu.sa:443
      7 abs.twimg.com:443
      6 www.moe.gov.sa:443
      6 vk.com:443
      6 useast.quantumdex.io:443
```

To display IP addresses that used the proxy and how many requests each IP address made:

```
┌──(kali㉿kali)-[~]
└─$ sudo grep "CONNECT" /var/log/squid/access.log | awk '{print $1}' | sort| uniq -c | sort -nr
   503 192.168.32.128
```

To display the most frequently-requested Saudi (.sa) domains/websites in the access.log:

```
┌──(kali㉿kali)-[~]
└─$ sudo grep "CONNECT" /var/log/squid/access.log | awk '{print $7}' | grep \.sa | sort | uniq -c | sort
-nr | head
     18 www.moi.gov.sa:443
     17 www.uj.edu.sa:443
     14 moe.gov.sa:443
      9 www.moj.gov.sa:443
      7 kaust.edu.sa:443
      6 www.moe.gov.sa:443
      6 university-president.uj.edu.sa:443
      6 ssum-sec.casalemedia.com:443
      6 med.uj.edu.sa:443
      5 apmeum.moe.gov.sa:443
```

To display the most frequently-requested .gov domains (websites) in the access.log:

```
┌──(kali㉿kali)-[~]
└─$ sudo grep "CONNECT" /var/log/squid/access.log | awk '{print $7}' | grep \.gov | sort | uniq -c | sort
 -nr | head
     18 www.moi.gov.sa:443
     14 moe.gov.sa:443
      9 www.moj.gov.sa:443
      6 www.moe.gov.sa:443
      5 apmeum.moe.gov.sa:443
      3 portaleservices.moj.gov.sa:443
      1 moj.gov.sa:443
      1 moi.gov.sa:443
```

To display how many times each IP address opens www.google.com :

```
┌──(kali㉿kali)-[~]
└─$ sudo grep google.com /var/log/squid/access.log | awk '{print $1}' | sort | uniq -c | sort -nr
     14 192.168.32.128
```

Find all systems that requested a particular resource (download file):

```
┌──(kali㉿kali)-[~]
└─$ sudo grep "\"GET" /var/log/squid/access.log | awk '{print $7}' | sort | uniq -c | sort -nr | head
     10 http://192.168.8.1/api/monitoring/status
      8 http://192.168.8.1/api/device/basic_information
      6 http://192.168.8.1/api/user/web-feature-switch
      4 http://192.168.8.1/config/global/config.xml
      4 http://192.168.8.1/api/user/state-login
      4 http://192.168.8.1/api/system/devcapacity
      4 http://192.168.8.1/api/pin/status
      2 http://pastebin.com/
      2 http://192.168.8.1/res/submiting.gif
      2 http://192.168.8.1/res/logo.png
```

To display all requested websites by specific IP address

```
┌──(kali㉿kali)-[~]
└─$ sudo grep "^192.168.32.128" /var/log/squid/access.log | awk '{print $7}' | sort | uniq -c | sort -nr
     41 http://ocsp.digicert.com/
     18 www.moi.gov.sa:443
     17 www.uj.edu.sa:443
     14 prg-apac.smartadserver.com:443
     14 prebid.a-mo.net:443
     14 oss.maxcdn.com:443
     14 moe.gov.sa:443
     13 px.vliplatform.com:443
     12 prebid.media.net:443
     12 error:transaction-end-before-headers
     12 cdnjs.cloudflare.com:443
     11 tlx.3lift.com:443
     11 prebid-asia.creativecdn.com:443
     11 pbjs.e-planning.net:443
     11 http://ocsp.pki.goog/gts1c3
     10 ib.adnxs.com:443
     10 http://192.168.8.1/api/monitoring/status
      9 www.moj.gov.sa:443
      9 targeting.unrulymedia.com:443
      9 safebrowsing.googleapis.com:443
      9 http://ocsp.sca1b.amazontrust.com/
      8 http://r3.o.lencr.org/
      8 http://ocsp.sectigo.com/
      8 http://192.168.8.1/api/device/basic_information
      7 kaust.edu.sa:443
      7 abs.twimg.com:443
      6 www.moe.gov.sa:443
      6 vk.com:443
```

To find who used pastebin.com website in your network and how many times this website has been requested:

```
┌──(kali㉿kali)-[~]
└─$ sudo grep "CONNECT" /var/log/squid/access.log | awk '{print $1,$7}' | grep pastebin.com | sort | uniq
 -c | sort -nr
      2 192.168.32.128 pastebin.com:443
```

To find what time pastebin.com website was requested in your network:

Conclusion

This lab has provided me with hands-on experience in setting up Squid proxy, analyzing Squid logs, and improving network security through web inspection and monitoring of website requests.