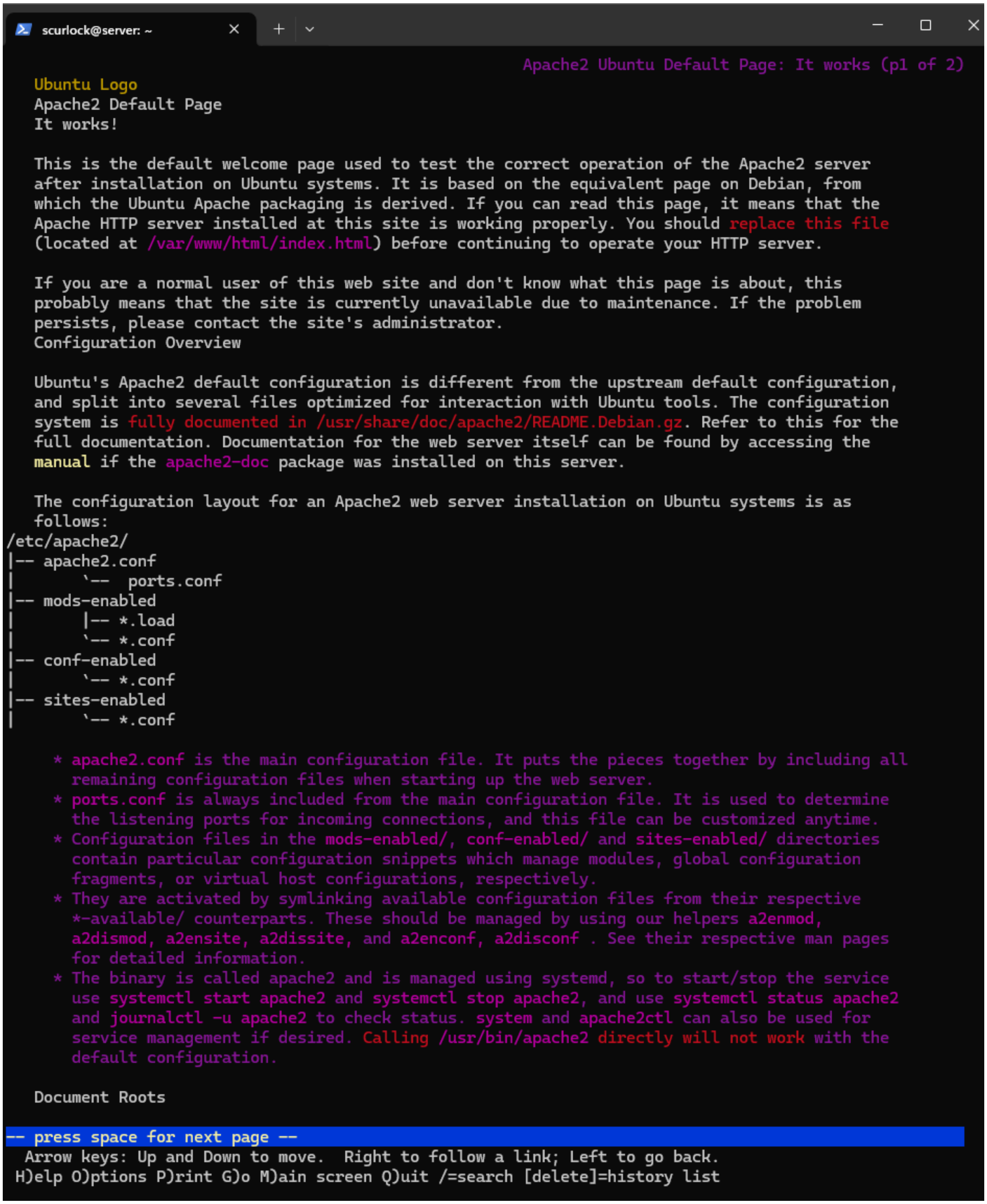
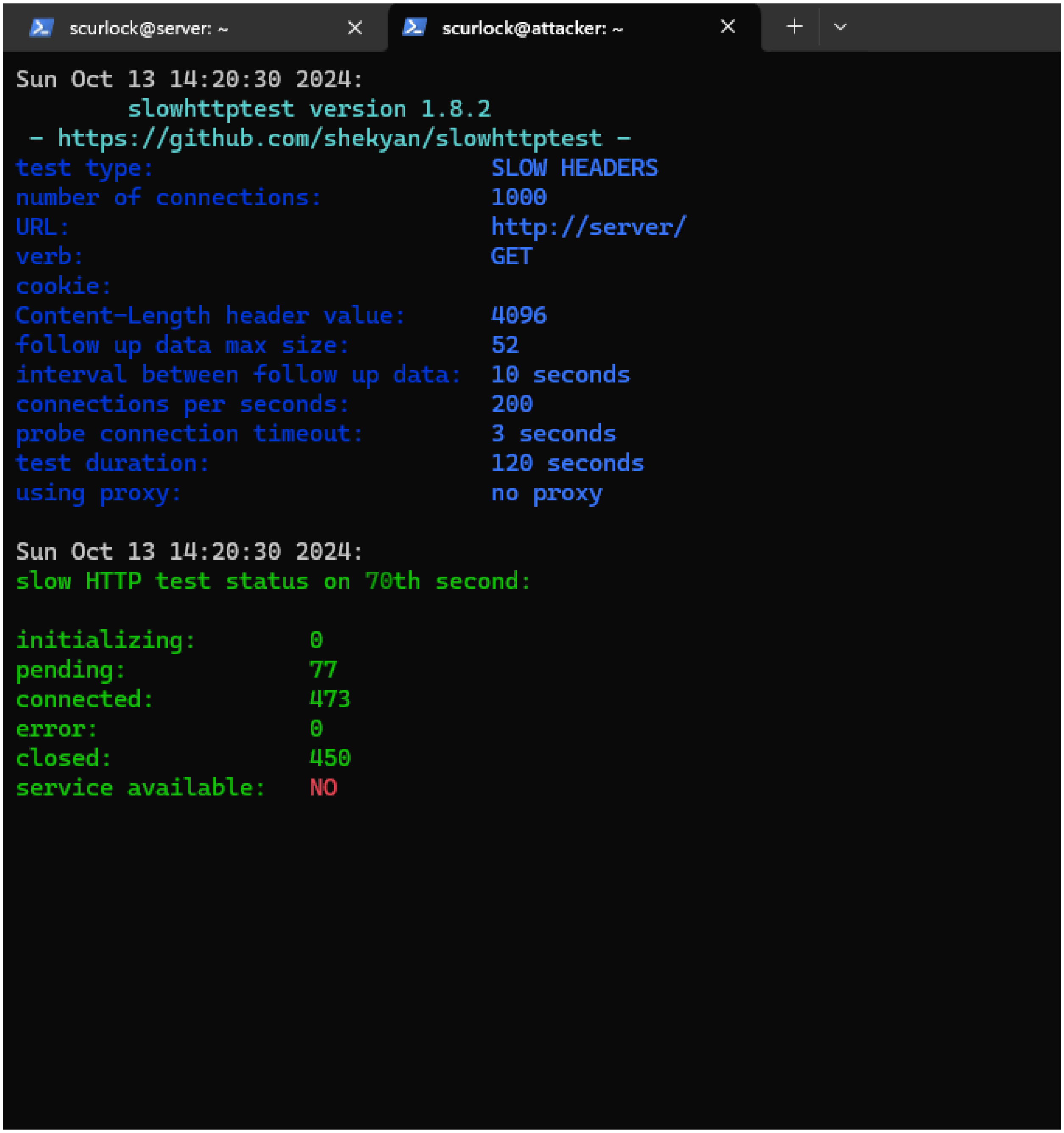
Zach Scurlock

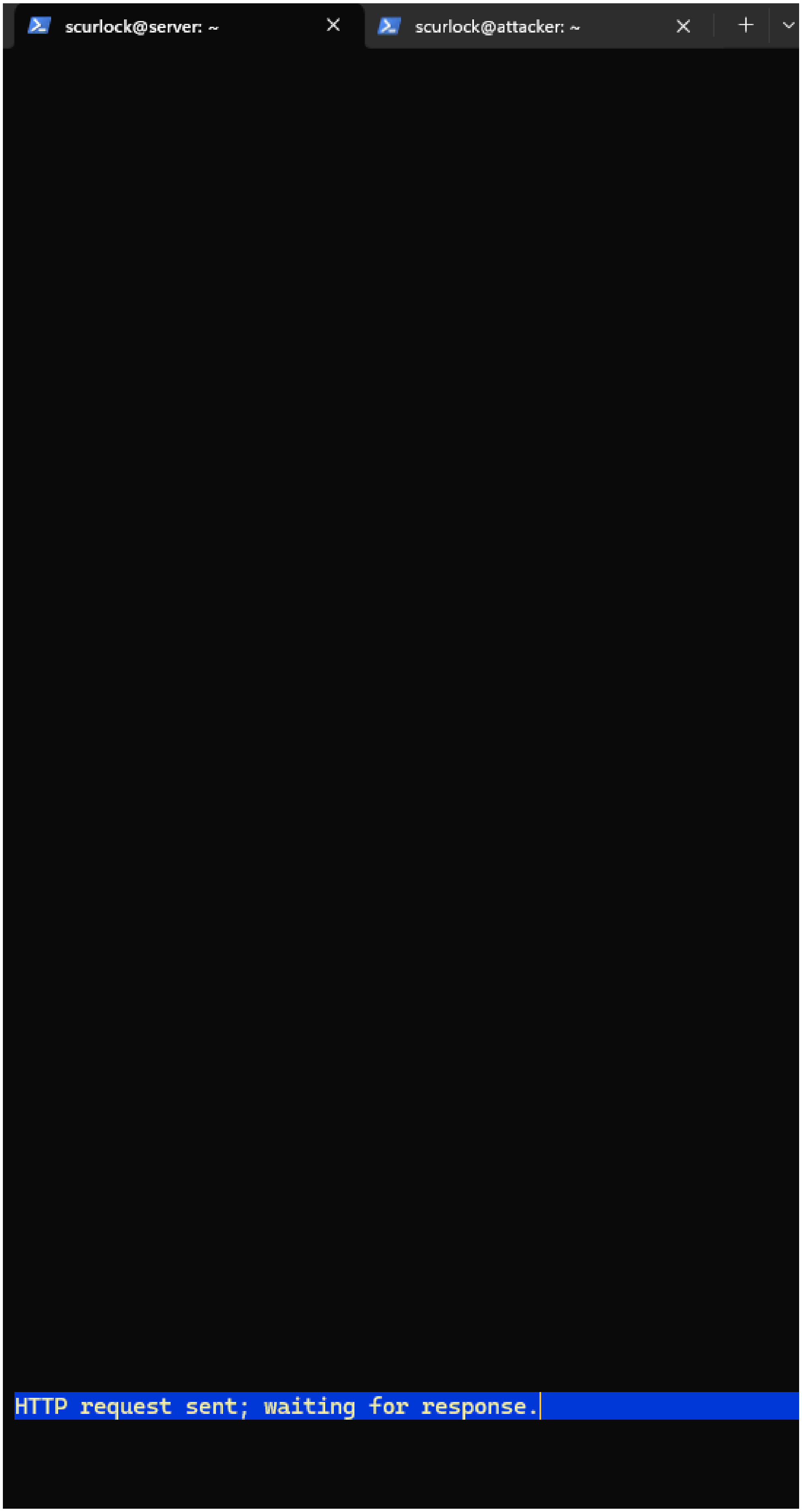
CprE 431 Module 4 Lab HW



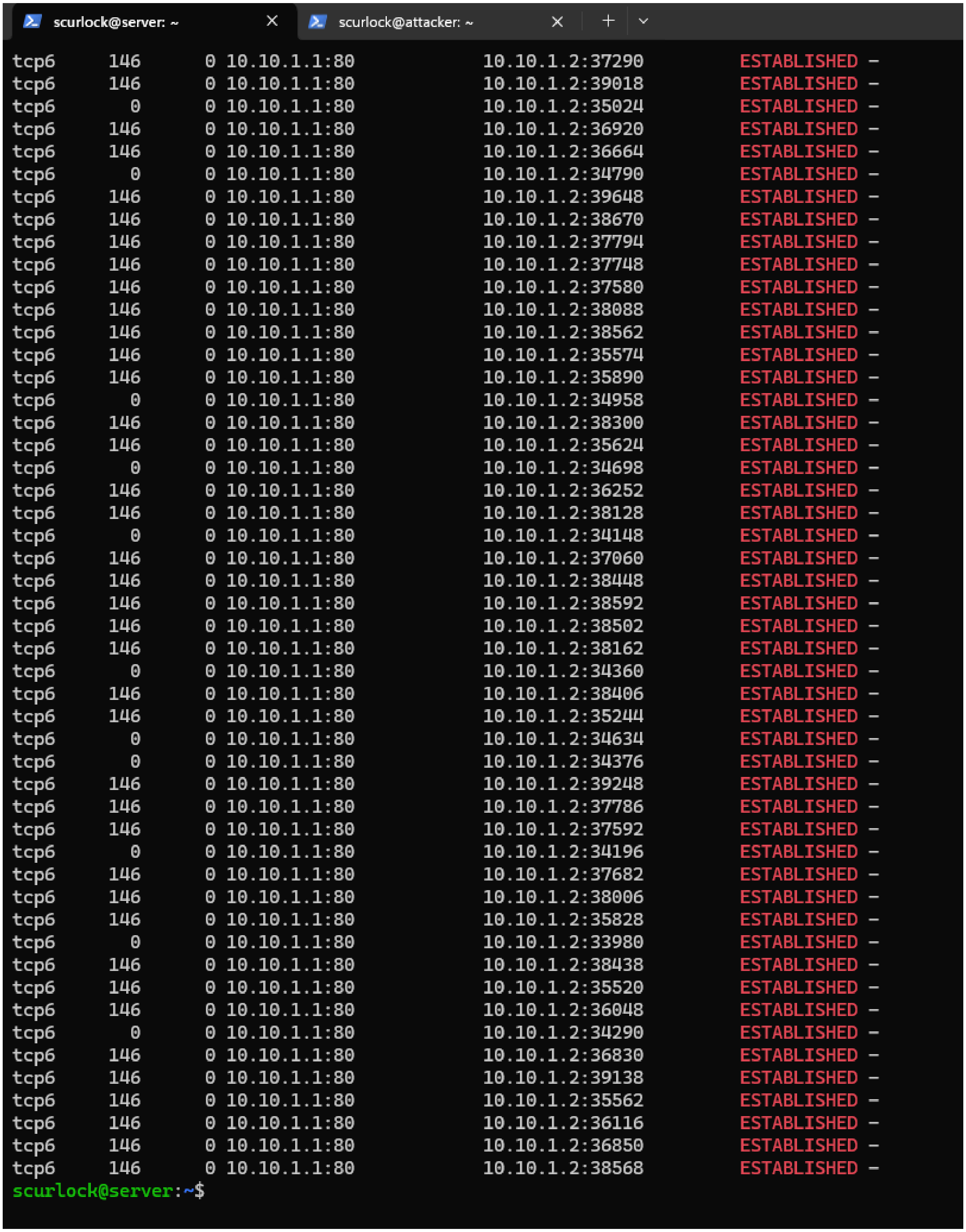
```
                                                Apache2 Ubuntu Default Page: It works (p1 of 2)
   Ubuntu Logo
   Apache2 Default Page
   It works!

   This is the default welcome page used to test the correct operation of the Apache2 server
   after installation on Ubuntu systems. It is based on the equivalent page on Debian, from
   which the Ubuntu Apache packaging is derived. If you can read this page, it means that the
   Apache HTTP server installed at this site is working properly. You should replace this file
   (located at /var/www/html/index.html) before continuing to operate your HTTP server.

   If you are a normal user of this web site and don't know what this page is about, this
   probably means that the site is currently unavailable due to maintenance. If the problem
   persists, please contact the site's administrator.
   Configuration Overview

   Ubuntu's Apache2 default configuration is different from the upstream default configuration,
   and split into several files optimized for interaction with Ubuntu tools. The configuration
   system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the
   full documentation. Documentation for the web server itself can be found by accessing the
   manual if the apache2-doc package was installed on this server.

   The configuration layout for an Apache2 web server installation on Ubuntu systems is as
   follows:
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf

     * apache2.conf is the main configuration file. It puts the pieces together by including all
       remaining configuration files when starting up the web server.
     * ports.conf is always included from the main configuration file. It is used to determine
       the listening ports for incoming connections, and this file can be customized anytime.
     * Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories
       contain particular configuration snippets which manage modules, global configuration
       fragments, or virtual host configurations, respectively.
     * They are activated by symlinking available configuration files from their respective
       *-available/ counterparts. These should be managed by using our helpers a2enmod,
       a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages
       for detailed information.
     * The binary is called apache2 and is managed using systemd, so to start/stop the service
       use systemctl start apache2 and systemctl stop apache2, and use systemctl status apache2
       and journalctl -u apache2 to check status. system and apache2ctl can also be used for
       service management if desired. Calling /usr/bin/apache2 directly will not work with the
       default configuration.

   Document Roots

-- press space for next page --
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```



```
Sun Oct 13 14:20:30 2024:
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            1000
URL:                              http://server/
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    120 seconds
using proxy:                      no proxy

Sun Oct 13 14:20:30 2024:
slow HTTP test status on 70th second:

initializing:        0
pending:             77
connected:           473
error:               0
closed:              450
service available:   NO
```

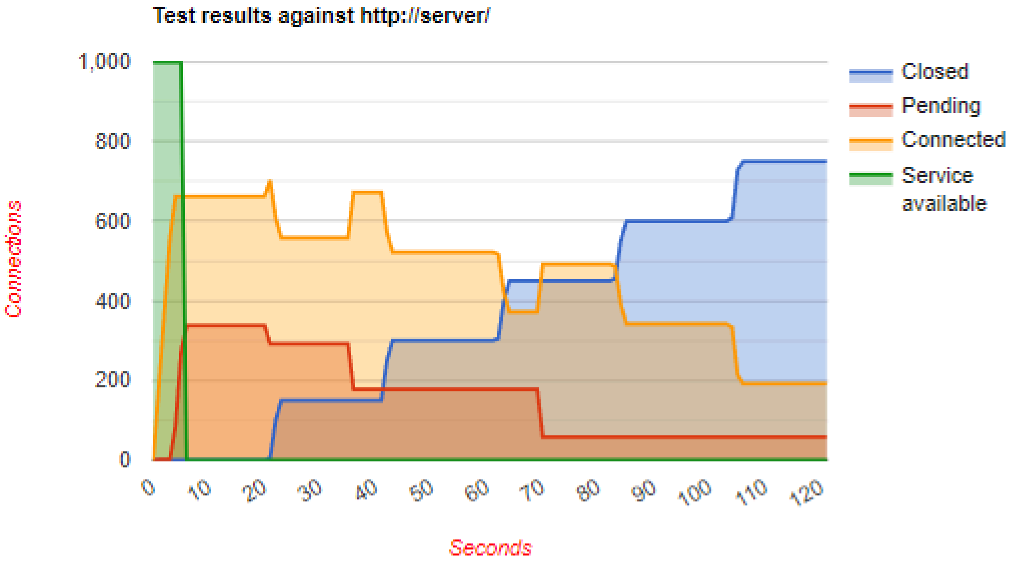


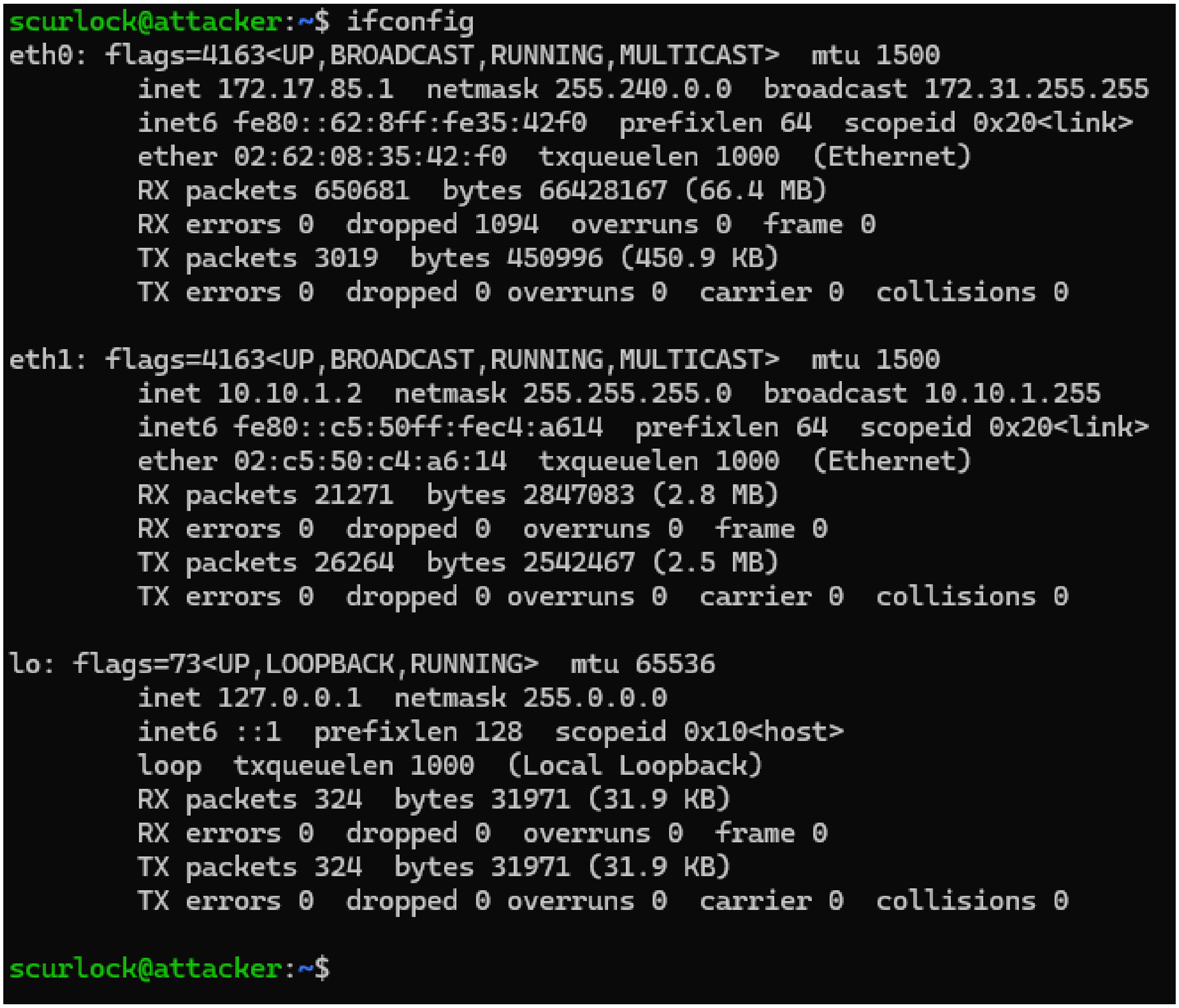
```
HTTP request sent; waiting for response.
```



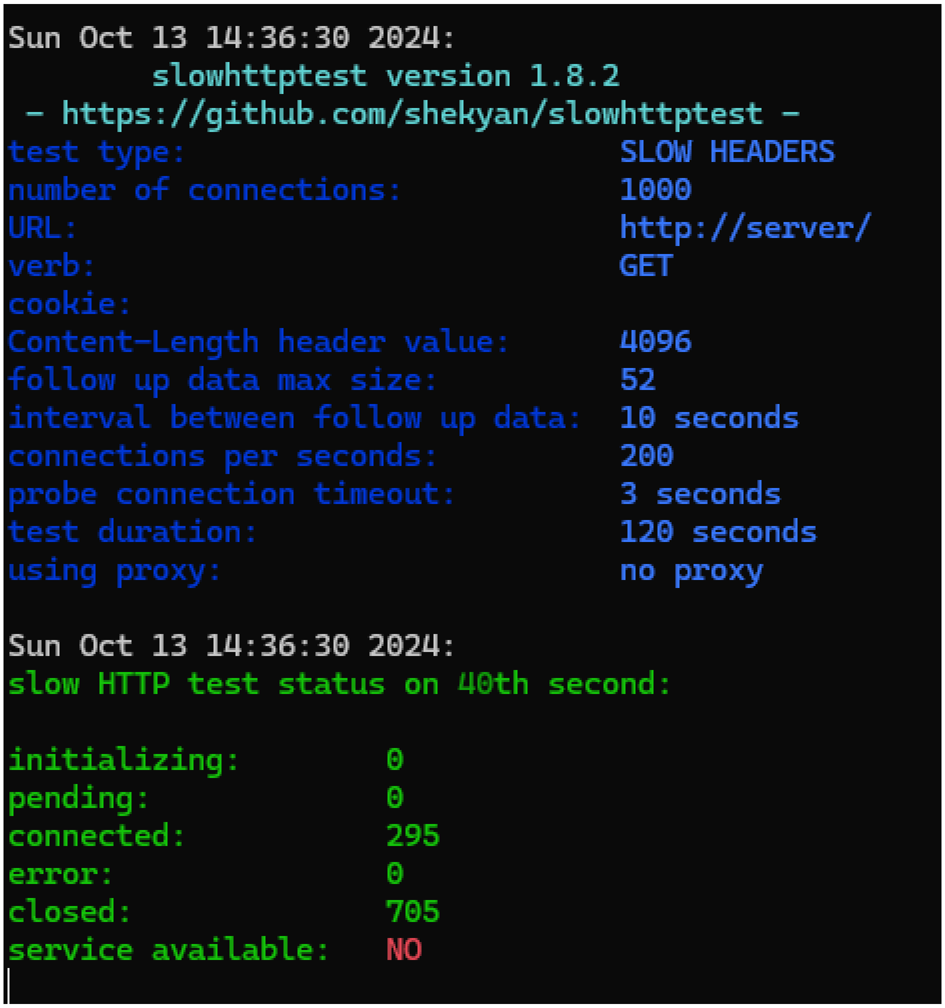
```
tcp6     146      0 10.10.1.1:80            10.10.1.2:37290         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:39018         ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:35024         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:36920         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:36664         ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:34790         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:39648         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:38670         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:37794         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:37748         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:37580         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:38088         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:38562         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:35574         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:35890         ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:34958         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:38300         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:35624         ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:34698         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:36252         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:38128         ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:34148         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:37060         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:38448         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:38592         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:38502         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:38162         ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:34360         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:38406         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:35244         ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:34634         ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:34376         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:39248         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:37786         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:37592         ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:34196         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:37682         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:38006         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:35828         ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:33980         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:38438         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:35520         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:36048         ESTABLISHED -
tcp6       0      0 10.10.1.1:80            10.10.1.2:34290         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:36830         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:39138         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:35562         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:36116         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:36850         ESTABLISHED -
tcp6     146      0 10.10.1.1:80            10.10.1.2:38568         ESTABLISHED -
scurlock@server:~$
```

Test parameters	
Test type	SLOW HEADERS
Number of connections	1000
Verb	GET
Content-Length header value	4096
Cookie	
Extra data max length	52
Interval between follow up data	10 seconds
Connections per seconds	200
Timeout for probe connection	3
Target test duration	120 seconds
Using proxy	no proxy

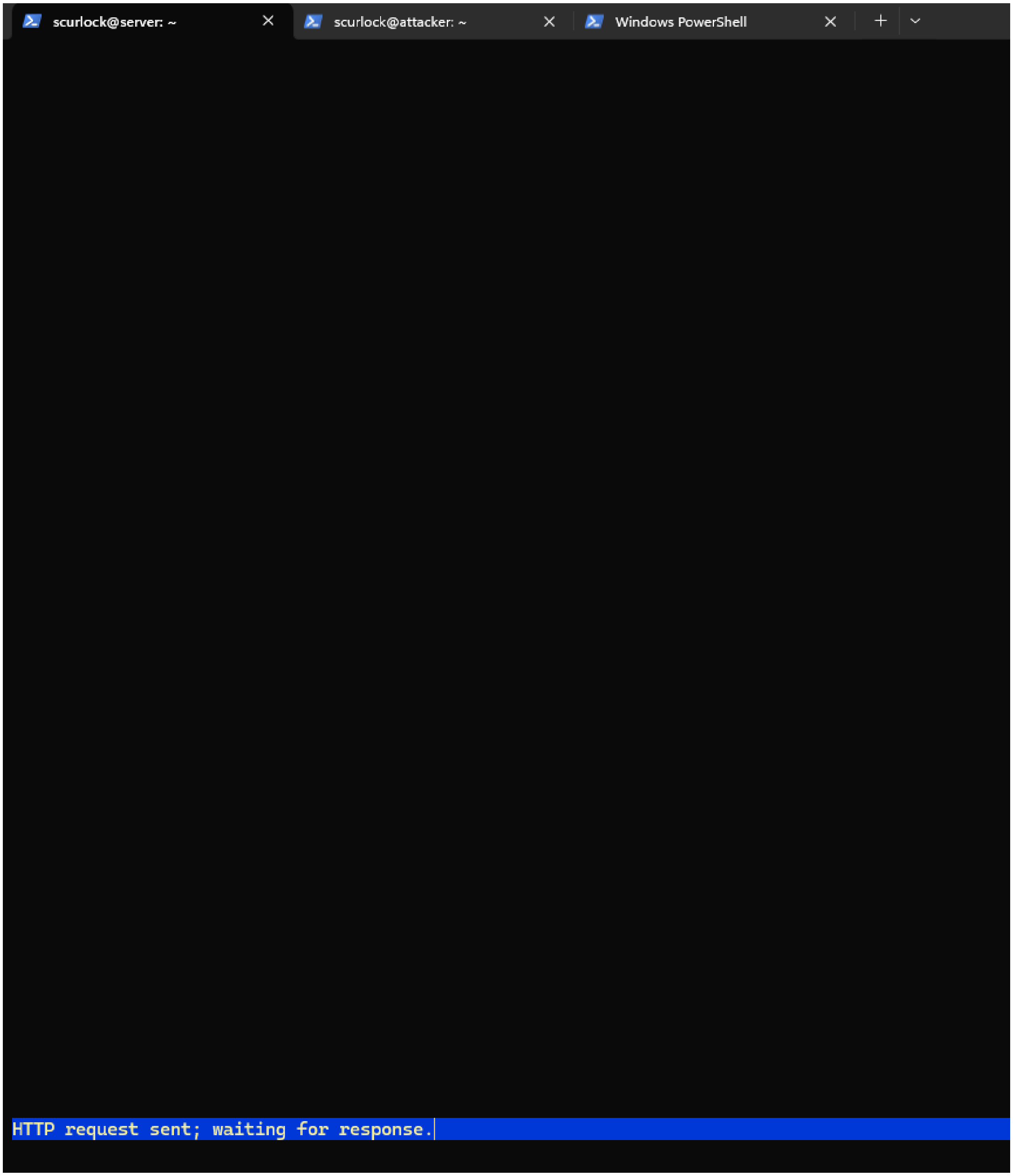




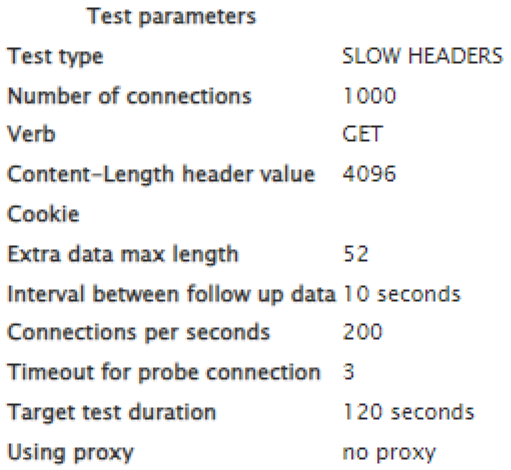
```
scurlock@attacker:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.85.1  netmask 255.240.0.0  broadcast 172.31.255.255
        inet6 fe80::62:8ff:fe35:42f0  prefixlen 64  scopeid 0x20<link>
        ether 02:62:08:35:42:f0  txqueuelen 1000  (Ethernet)
        RX packets 650681  bytes 66428167 (66.4 MB)
        RX errors 0  dropped 1094  overruns 0  frame 0
        TX packets 3019  bytes 450996 (450.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.1.2  netmask 255.255.255.0  broadcast 10.10.1.255
        inet6 fe80::c5:50ff:fec4:a614  prefixlen 64  scopeid 0x20<link>
        ether 02:c5:50:c4:a6:14  txqueuelen 1000  (Ethernet)
        RX packets 21271  bytes 2847083 (2.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26264  bytes 2542467 (2.5 MB)
        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 324  bytes 31971 (31.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 324  bytes 31971 (31.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

scurlock@attacker:~$
```



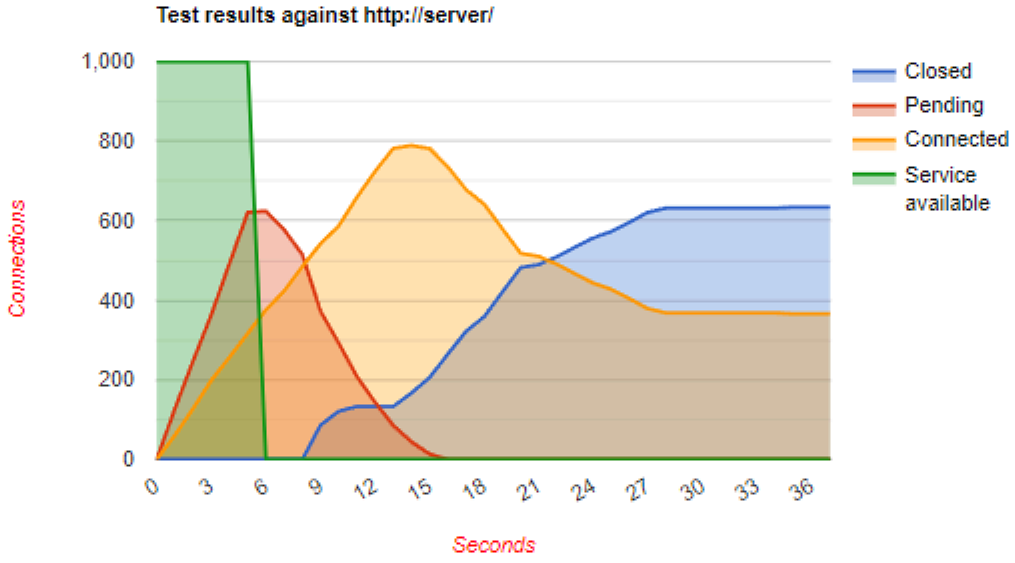
```
Sun Oct 13 14:36:30 2024:
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            1000
URL:                              http://server/
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    120 seconds
using proxy:                      no proxy

Sun Oct 13 14:36:30 2024:
slow HTTP test status on 40th second:

initializing:        0
pending:             0
connected:           295
error:               0
closed:              705
service available:   NO
```



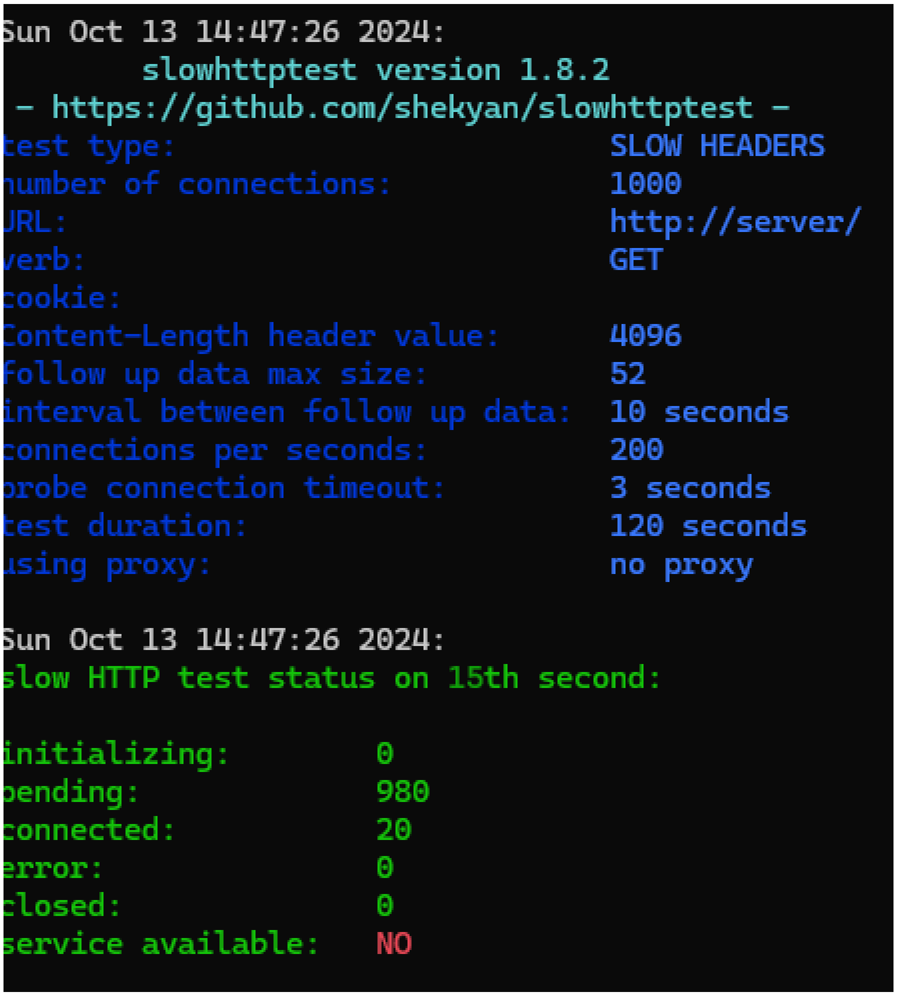
```
HTTP request sent; waiting for response.
```



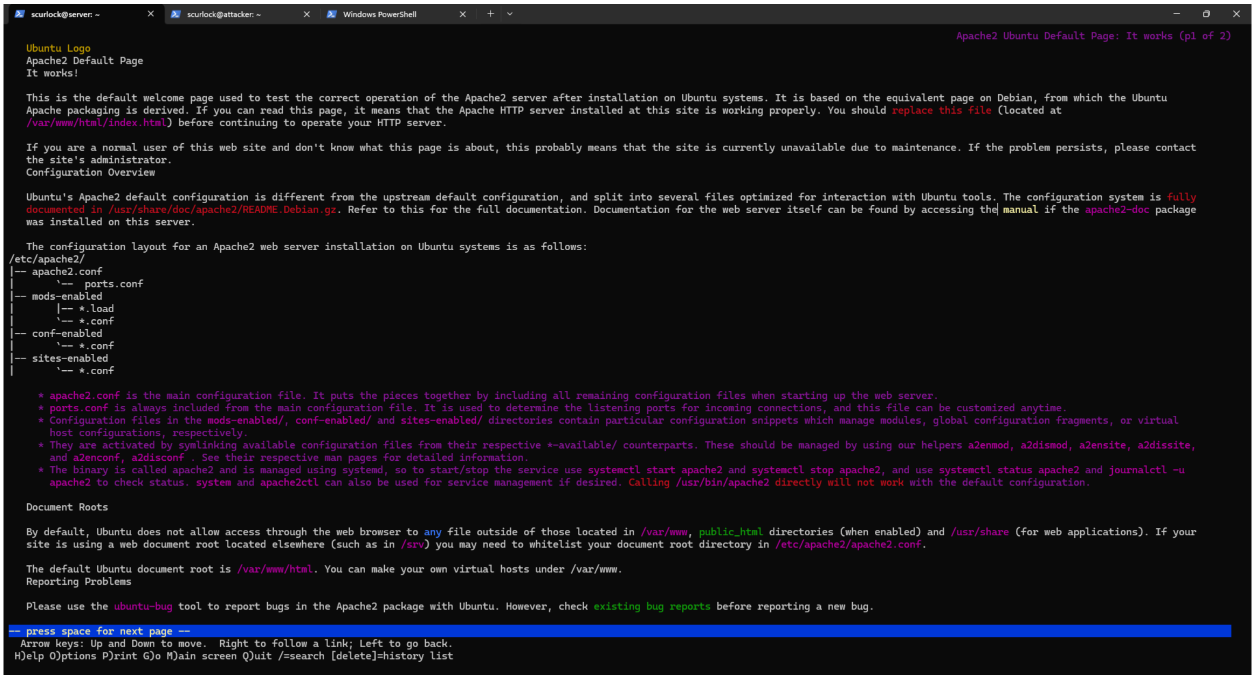
Test parameters	
Test type	SLOW HEADERS
Number of connections	1000
Verb	GET
Content-Length header value	4096
Cookie	
Extra data max length	52
Interval between follow up data	10 seconds
Connections per seconds	200
Timeout for probe connection	3
Target test duration	120 seconds
Using proxy	no proxy



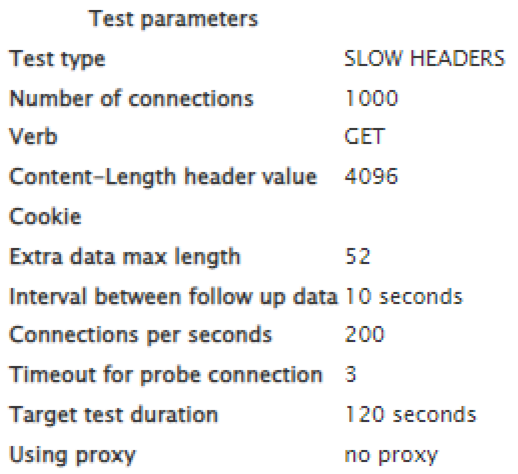
Test results against http://server/



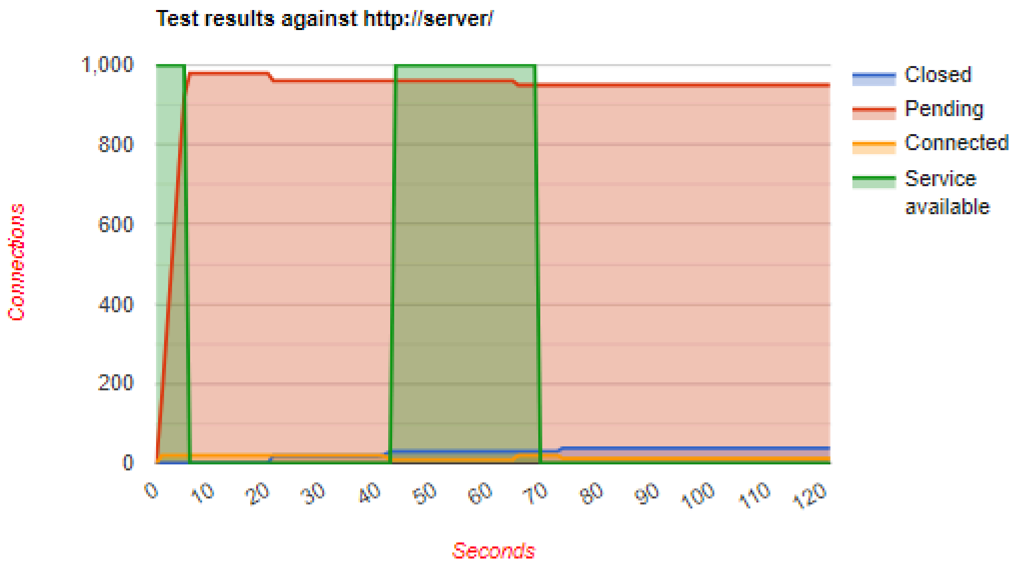
```
Sun Oct 13 14:47:26 2024:
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            1000
URL:                              http://server/
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    120 seconds
using proxy:                      no proxy

Sun Oct 13 14:47:26 2024:
slow HTTP test status on 15th second:

initializing:        0
pending:             980
connected:           20
error:               0
closed:              0
service available:   NO
```



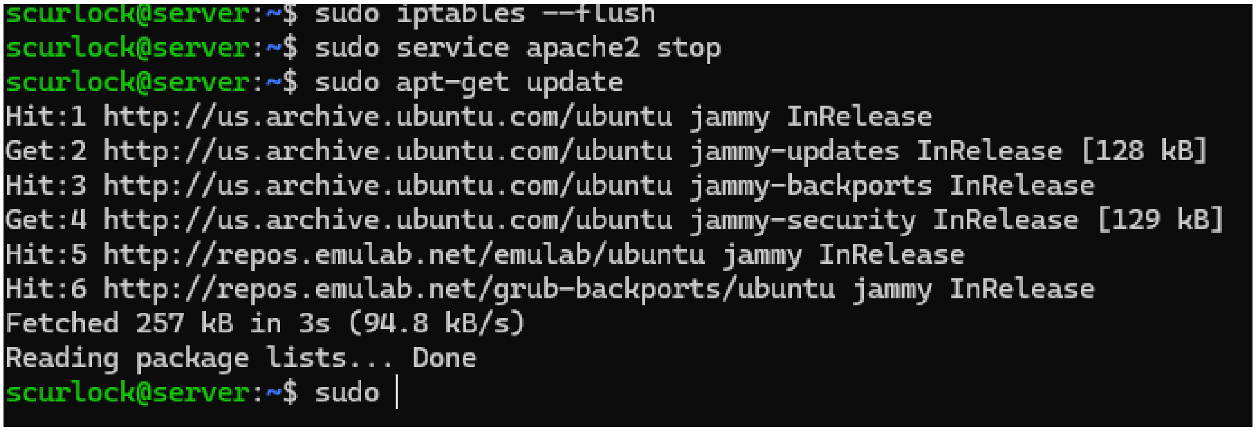
```
                                                                      Apache2 Ubuntu Default Page: It works (p1 of 2)
   Ubuntu Logo
   Apache2 Default Page
   It works!

   This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu
   Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at
   /var/www/html/index.html) before continuing to operate your HTTP server.

   If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact
   the site's administrator.
   Configuration Overview

   Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully
   documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package
   was installed on this server.

   The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf

     * apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
     * ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
     * Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual
       host configurations, respectively.
     * They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite,
       and a2enconf, a2disconf . See their respective man pages for detailed information.
     * The binary is called apache2 and is managed using systemd, so to start/stop the service use systemctl start apache2 and systemctl stop apache2, and use systemctl status apache2 and journalctl -u
       apache2 to check status. system and apache2ctl can also be used for service management if desired. Calling /usr/bin/apache2 directly will not work with the default configuration.

   Document Roots

   By default, Ubuntu does not allow access through the web browser to any file outside of those located in /var/www, public_html directories (when enabled) and /usr/share (for web applications). If your
   site is using a web document root located elsewhere (such as in /srv) you may need to whitelist your document root directory in /etc/apache2/apache2.conf.

   The default Ubuntu document root is /var/www/html. You can make your own virtual hosts under /var/www.
   Reporting Problems

   Please use the ubuntu-bug tool to report bugs in the Apache2 package with Ubuntu. However, check existing bug reports before reporting a new bug.

-- press space for next page --
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```



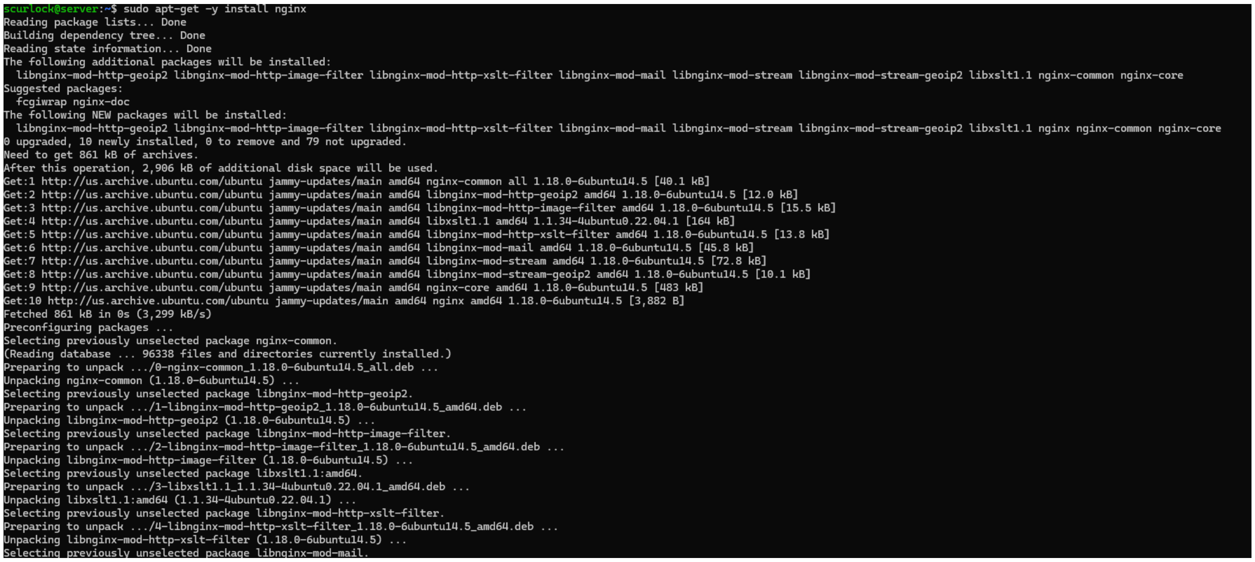
Test parameters	
Test type	SLOW HEADERS
Number of connections	1000
Verb	GET
Content-Length header value	4096
Cookie	
Extra data max length	52
Interval between follow up data	10 seconds
Connections per seconds	200
Timeout for probe connection	3
Target test duration	120 seconds
Using proxy	no proxy



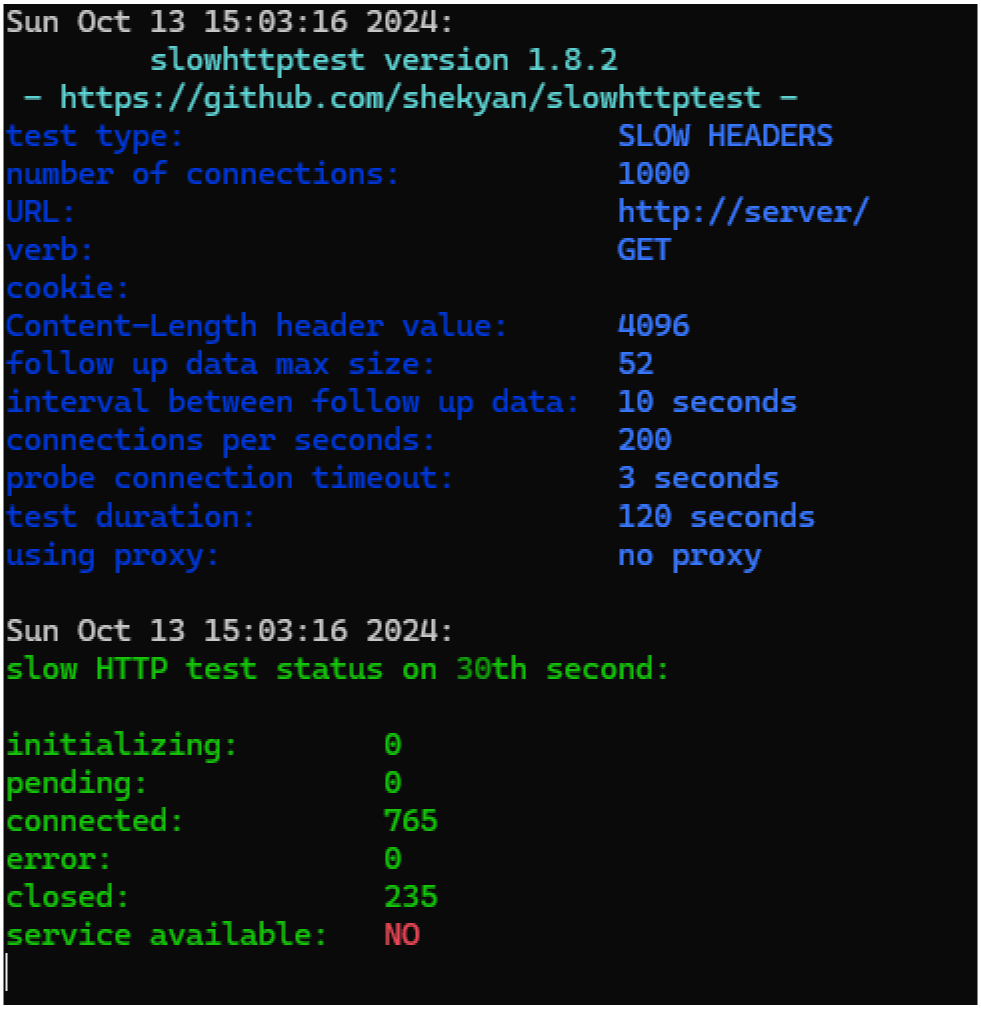
I’m not sure why the service became available but it kept happening.



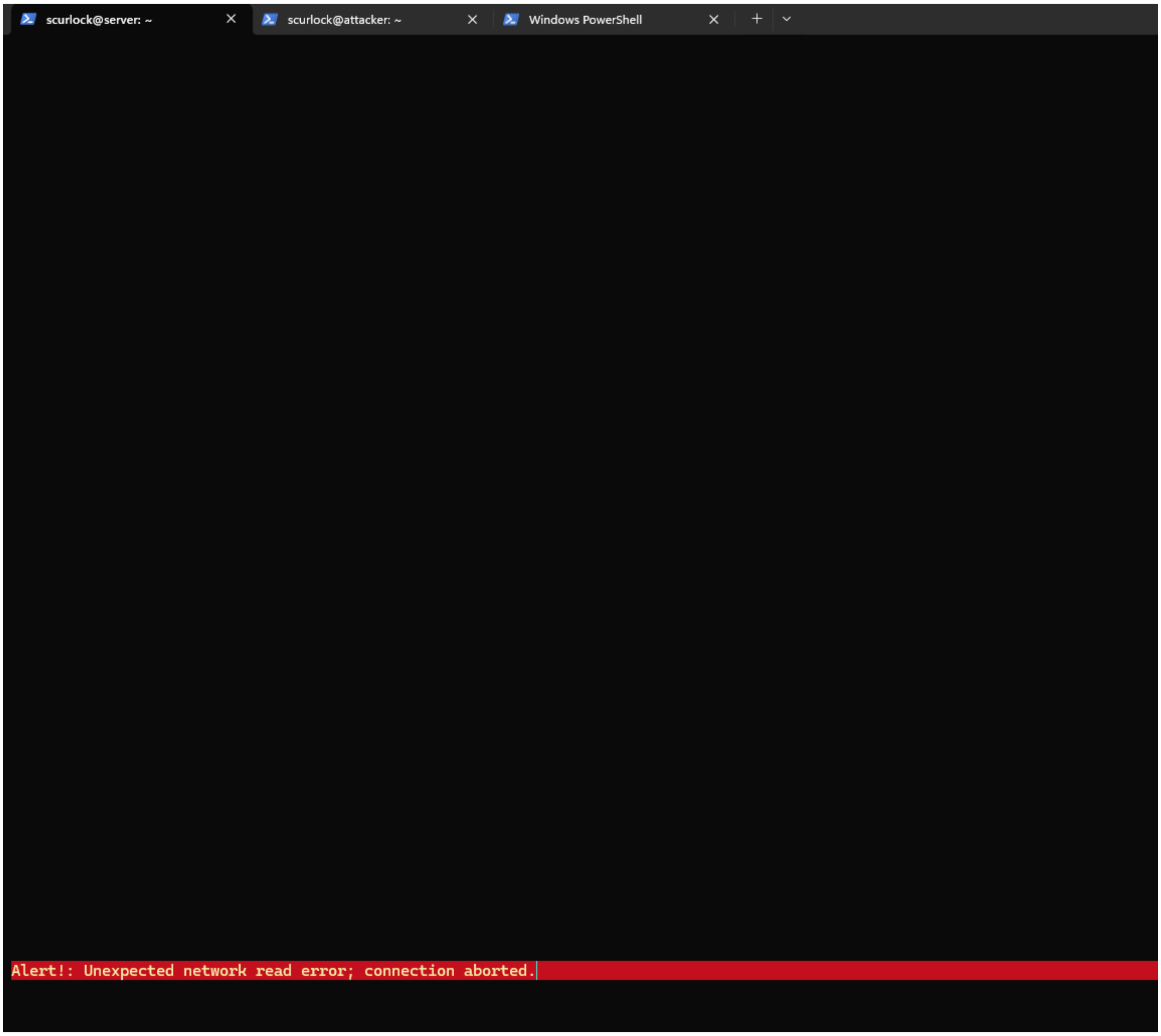
```
scurlock@server:~$ sudo iptables --flush
scurlock@server:~$ sudo service apache2 stop
scurlock@server:~$ sudo apt-get update
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Hit:3 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 http://us.archive.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:5 http://repos.emulab.net/emulab/ubuntu jammy InRelease
Hit:6 http://repos.emulab.net/grub-backports/ubuntu jammy InRelease
Fetched 257 kB in 3s (94.8 kB/s)
Reading package lists... Done
scurlock@server:~$ sudo 
```



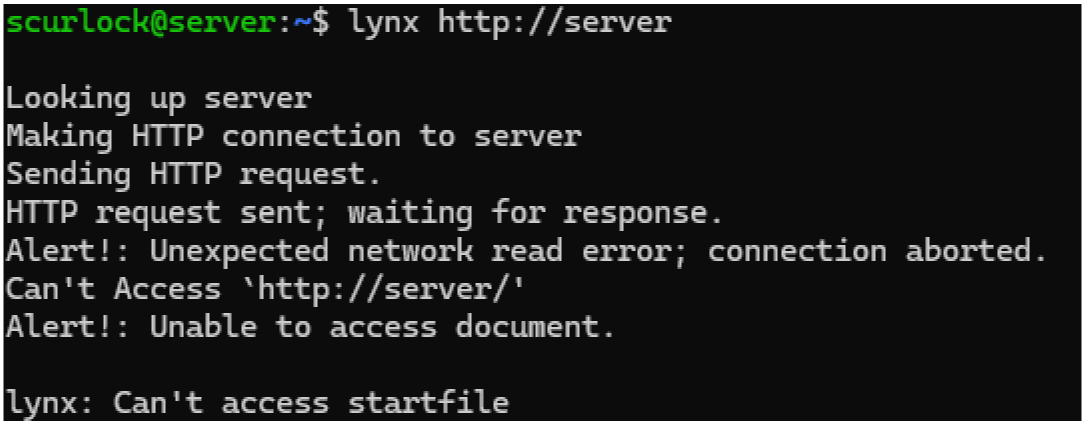
```
scurlock@server:~$ sudo apt-get -y install nginx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libnginx-mod-http-geoip2 libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip2 libxslt1.1 nginx-common nginx-core
Suggested packages:
  fcgiwrap nginx-doc
The following NEW packages will be installed:
  libnginx-mod-http-geoip2 libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip2 libxslt1.1 nginx nginx-common nginx-core
0 upgraded, 10 newly installed, 0 to remove and 79 not upgraded.
Need to get 861 kB of archives.
After this operation, 2,906 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 nginx-common all 1.18.0-6ubuntu14.5 [40.1 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libnginx-mod-http-geoip2 amd64 1.18.0-6ubuntu14.5 [12.0 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libnginx-mod-http-image-filter amd64 1.18.0-6ubuntu14.5 [15.5 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libxslt1.1 amd64 1.1.34-4ubuntu0.22.04.1 [164 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libnginx-mod-http-xslt-filter amd64 1.18.0-6ubuntu14.5 [13.8 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libnginx-mod-mail amd64 1.18.0-6ubuntu14.5 [45.8 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libnginx-mod-stream amd64 1.18.0-6ubuntu14.5 [72.8 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libnginx-mod-stream-geoip2 amd64 1.18.0-6ubuntu14.5 [10.1 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 nginx-core amd64 1.18.0-6ubuntu14.5 [483 kB]
Get:10 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 nginx amd64 1.18.0-6ubuntu14.5 [3,882 B]
Fetched 861 kB in 0s (3,299 kB/s)
Preconfiguring packages ...
Selecting previously unselected package nginx-common.
(Reading database ... 96338 files and directories currently installed.)
Preparing to unpack .../0-nginx-common_1.18.0-6ubuntu14.5_all.deb ...
Unpacking nginx-common (1.18.0-6ubuntu14.5) ...
Selecting previously unselected package libnginx-mod-http-geoip2.
Preparing to unpack .../1-libnginx-mod-http-geoip2_1.18.0-6ubuntu14.5_amd64.deb ...
Unpacking libnginx-mod-http-geoip2 (1.18.0-6ubuntu14.5) ...
Selecting previously unselected package libnginx-mod-http-image-filter.
Preparing to unpack .../2-libnginx-mod-http-image-filter_1.18.0-6ubuntu14.5_amd64.deb ...
Unpacking libnginx-mod-http-image-filter (1.18.0-6ubuntu14.5) ...
Selecting previously unselected package libxslt1.1:amd64.
Preparing to unpack .../3-libxslt1.1_1.1.34-4ubuntu0.22.04.1_amd64.deb ...
Unpacking libxslt1.1:amd64 (1.1.34-4ubuntu0.22.04.1) ...
Selecting previously unselected package libnginx-mod-http-xslt-filter.
Preparing to unpack .../4-libnginx-mod-http-xslt-filter_1.18.0-6ubuntu14.5_amd64.deb ...
Unpacking libnginx-mod-http-xslt-filter (1.18.0-6ubuntu14.5) ...
Selecting previously unselected package libnginx-mod-mail.
```



```
Sun Oct 13 15:03:16 2024:
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            1000
URL:                              http://server/
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    120 seconds
using proxy:                      no proxy

Sun Oct 13 15:03:16 2024:
slow HTTP test status on 30th second:

initializing:        0
pending:             0
connected:           765
error:               0
closed:              235
service available:   NO
```

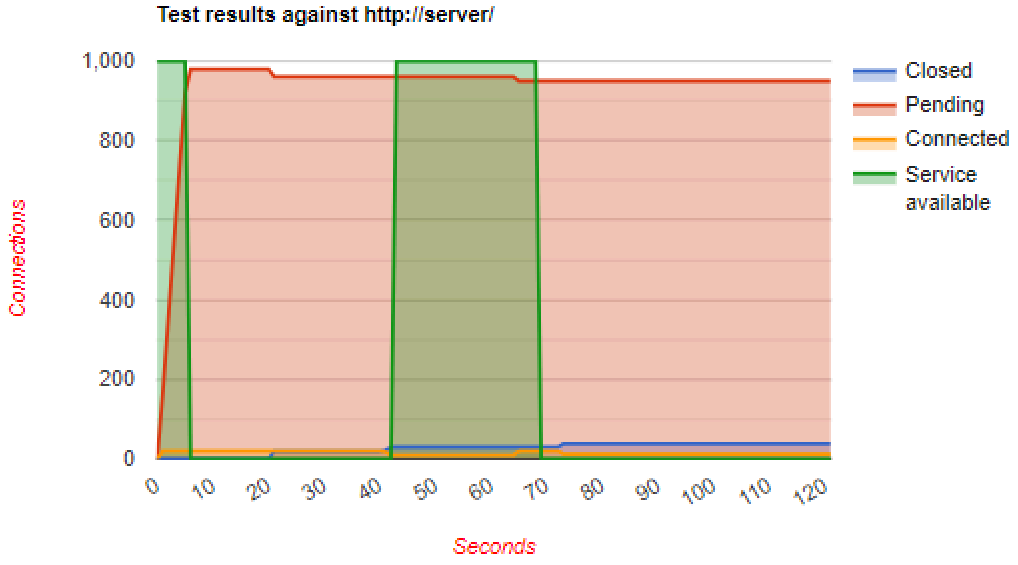


```
Alert!: Unexpected network read error; connection aborted.
```



```
scurlock@server:~$ lynx http://server

Looking up server
Making HTTP connection to server
Sending HTTP request.
HTTP request sent; waiting for response.
Alert!: Unexpected network read error; connection aborted.
Can't Access `http://server/'
Alert!: Unable to access document.

lynx: Can't access startfile
```

Test parameters	
Test type	SLOW HEADERS
Number of connections	1000
Verb	GET
Content-Length header value	4096
Cookie	
Extra data max length	52
Interval between follow up data	10 seconds
Connections per seconds	200
Timeout for probe connection	3
Target test duration	120 seconds
Using proxy	no proxy


Test results against http://server/
Connections
Seconds
Closed
Pending
Connected
Service available