CNIT 123 Proj 3: HTTP Basic Authentication (10 pts.)

What You Need

A Linux machine, such as Kali.

Starting Apache

In a Terminal window, execute this command:

```
service apache2 start
```

If you see an error saying Apache is not installed, follow the instructions on your screen to install it.

In a Terminal window, execute this command:

```
ip addr
```

(Note: ifconfig is deprecated and ip is preferred.)

Find your IP address.

Click **Applications**, **Internet**, "**Firefox Web Browser**" and enter your IP address in the URL. You should see a Web page--if your Apache is newly installed, it will be an Apache default page.

Making the secret Page

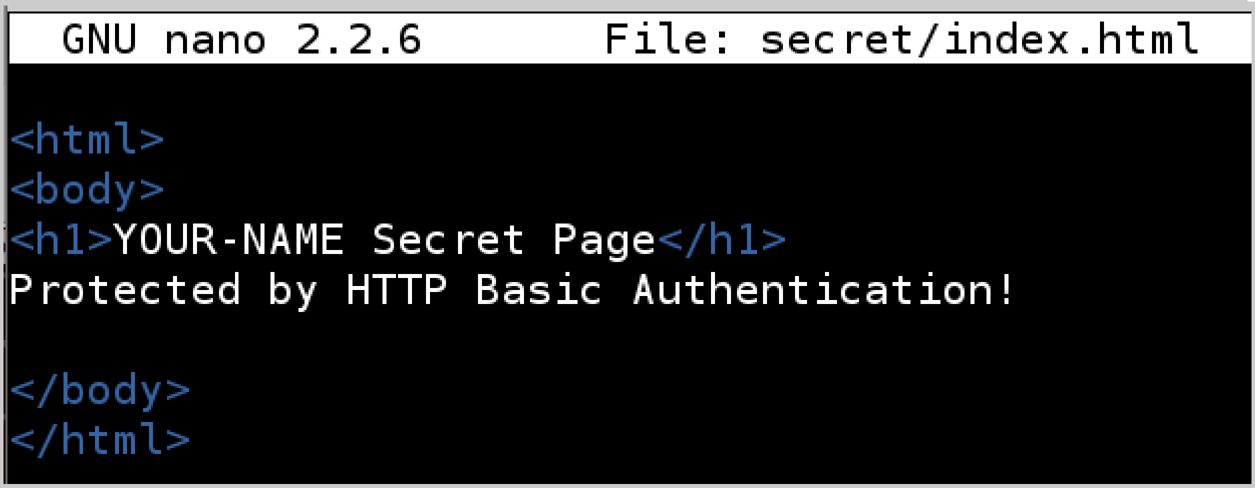
In a Terminal window, execute these commands:

```
mkdir /var/www/html/secret

nano /var/www/html/secret/index.html
```

In nano, enter the HTML code shown below, replacing YOUR-NAME with your own name:

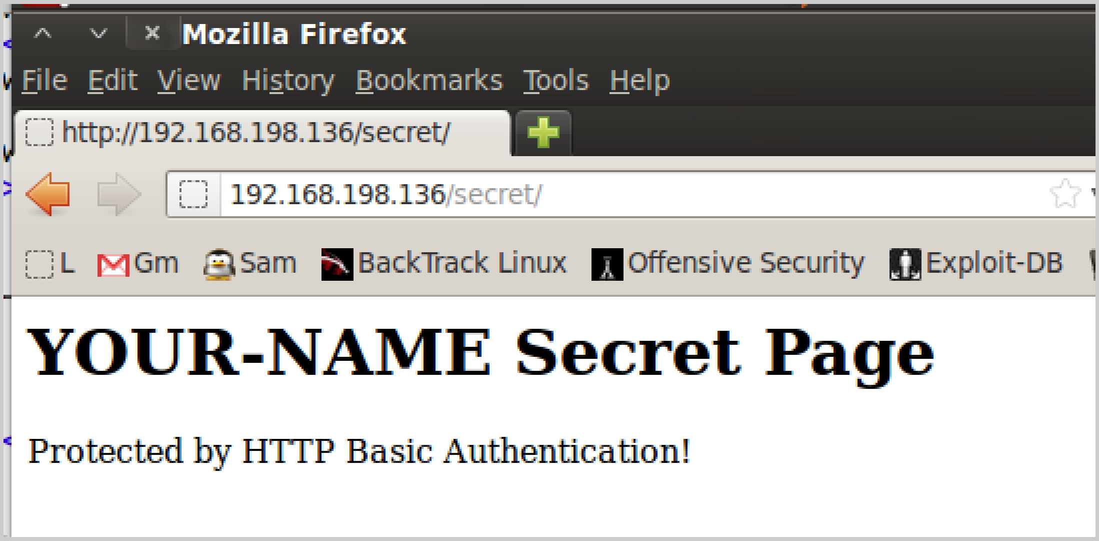
```
<html>
<body>
<h1>YOUR-NAME Secret Page</h1>

Protected by HTTP Basic Authentication!

</body>
</html>
```

Save the file with **Ctrl+X**, **Y**, **Enter**.



```
  GNU nano 2.2.6          File: secret/index.html

<html>
<body>
<h1>YOUR-NAME Secret Page</h1>
Protected by HTTP Basic Authentication!

</body>
</html>
```

In Firefox, append **/secret** to the IP address to view your page, as shown below:



Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.198.136/secret/
192.168.198.136/secret/
L Gm Sam BackTrack Linux Offensive Security Exploit-DB

YOUR-NAME Secret Page

Protected by HTTP Basic Authentication!

There was no password required to see this page.

Configuring Basic Authentication

In a Terminal window, execute this command:

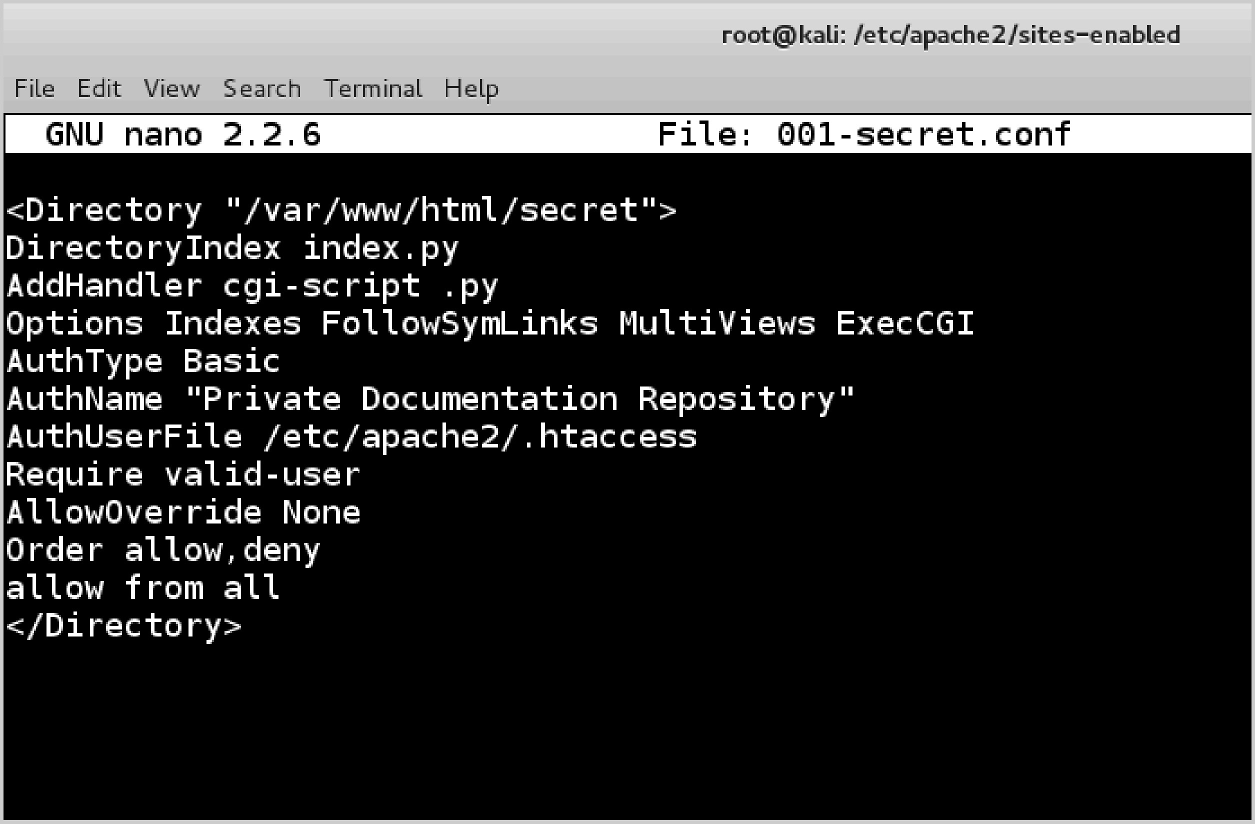
```
nano /etc/apache2/sites-enabled/001-secret.conf
```

In nano, enter the code shown below:

```
<Directory "/var/www/html/secret">
DirectoryIndex index.py
AddHandler cgi-script .py
Options Indexes FollowSymLinks MultiViews ExecCGI
```

```
AuthType Basic
AuthName "Private Documentation Repository"
AuthUserFile /etc/apache2/.htaccess
Require valid-user
AllowOverride None
Order allow,deny
allow from all
</Directory>
```

Save the file with **Ctrl+X**, **Y**, Enter.

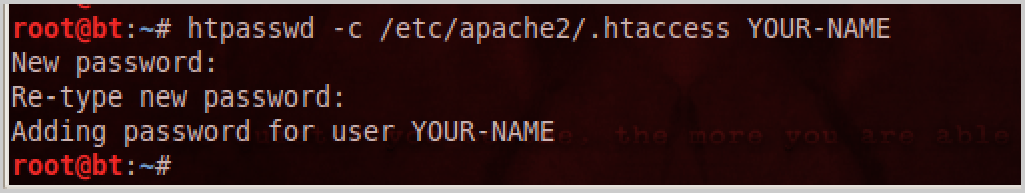

root@kali: /etc/apache2/sites-enabled
File Edit View Search Terminal Help

```
  GNU nano 2.2.6                File: 001-secret.conf

<Directory "/var/www/html/secret">
DirectoryIndex index.py
AddHandler cgi-script .py
Options Indexes FollowSymLinks MultiViews ExecCGI
AuthType Basic
AuthName "Private Documentation Repository"
AuthUserFile /etc/apache2/.htaccess
Require valid-user
AllowOverride None
Order allow,deny
allow from all
</Directory>
```

Specifying Username and Password

In a Terminal window, execute this command replacing "YOUR-NAME with your own name. When you are prompted for a password, enter **secretpassword** twice.

```
htpasswd -c /etc/apache2/.htaccess YOUR-NAME
```



```
root@bt:~# htpasswd -c /etc/apache2/.htaccess YOUR-NAME
New password:
Re-type new password:
Adding password for user YOUR-NAME
root@bt:~#
```

Restart Apache

In a Terminal window, execute this command:

```
service apache2 restart
```

Troubleshooting

If Apache won't start, and you see an error message, execute this command to get more information about the problem:

```
tail /var/log/syslog
```

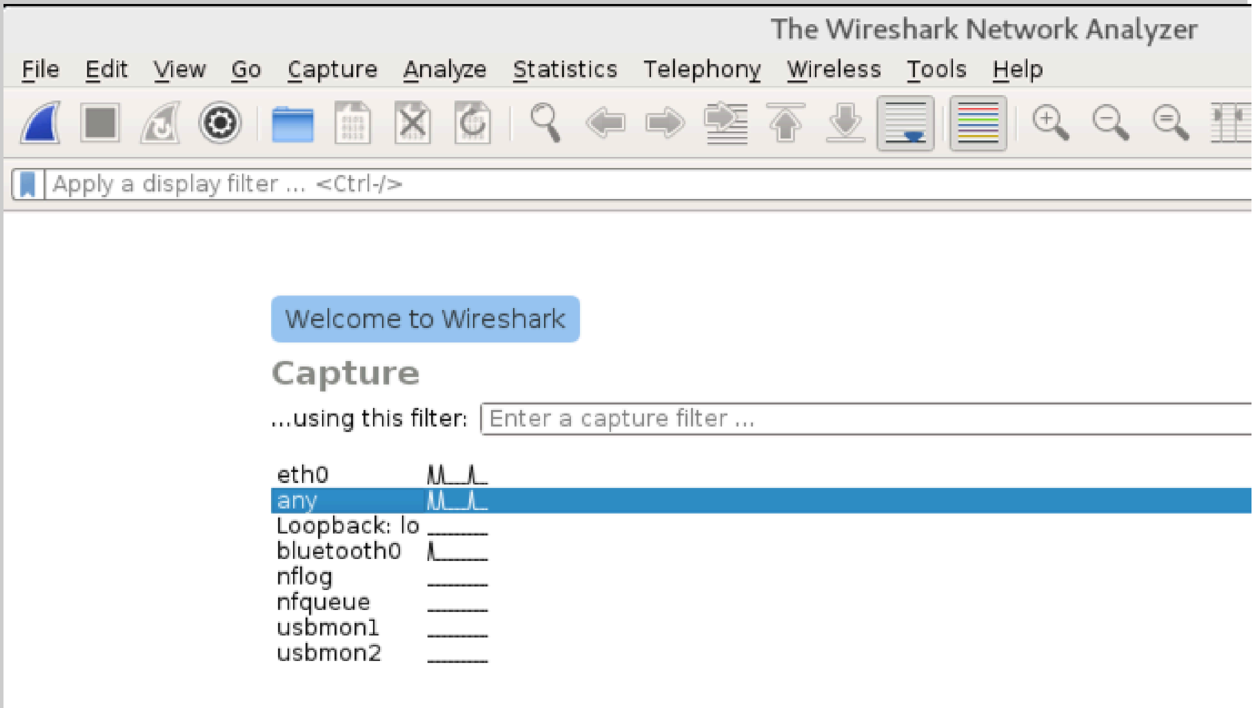
Starting Wireshark

In a Terminal window, execute this command:

```
wireshark
```

A box pops up saying "Lua: Error during loading". Press **Enter**.

In Wireshark, double-click **any**, as shown below.

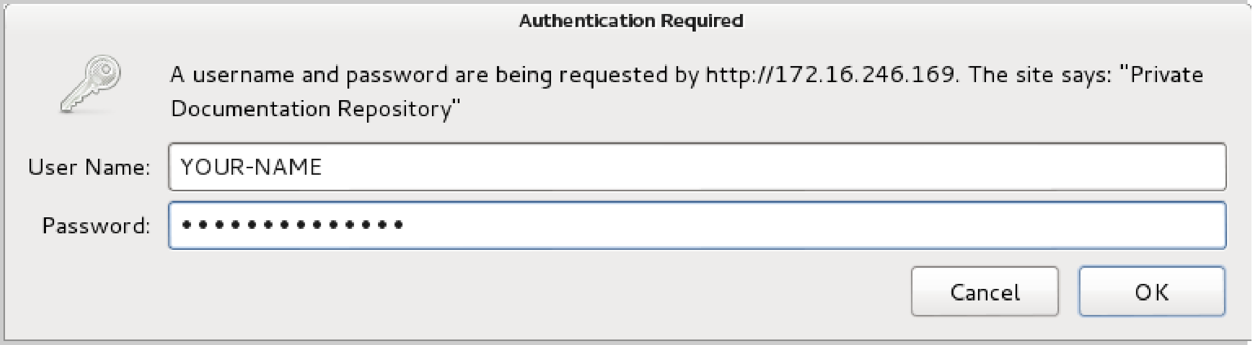

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
eth0
any
Loopback: lo
bluetooth0
nflog
nfqueue
usbmon1
usbmon2

Click **Start**.

Authenticating

In Firefox, refresh the page with your IP address followed by **/secret**

An "Authentication Required" box pops up, as shown below. Log in with your name and the password **secretpassword**



Authentication Required

A username and password are being requested by http://172.16.246.169. The site says: "Private Documentation Repository"

User Name: YOUR-NAME

Password: ••••••••••••••

In Wireshark, click **Capture**, **Stop**.

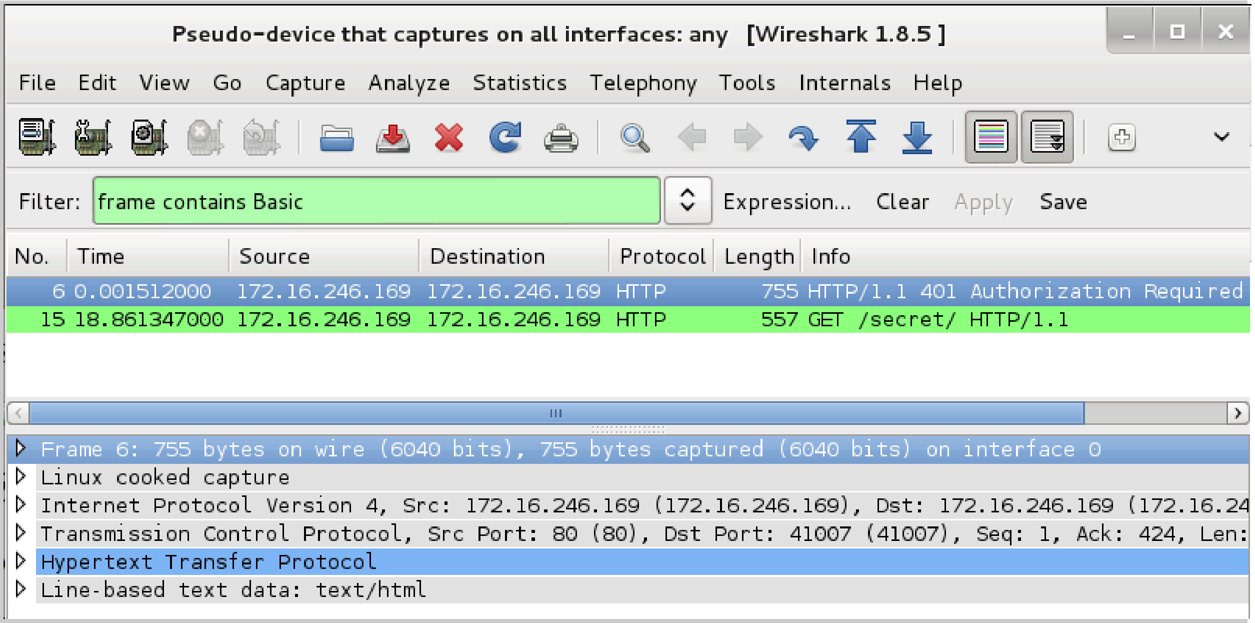
In the top section of the Wireshark window, in the Filter bar, erase the text there and type in this filter.

```
frame contains Basic
```

Press Enter.

Two packets are visible, as shown below.

In the Info column, the first one is labelled "HTTP/1.1 401 Authorization Required", and the second one is labelled "GET /secret/ HTTP/1.1", as shown below.



Pseudo-device that captures on all interfaces: any [Wireshark 1.8.5]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

Filter: frame contains Basic

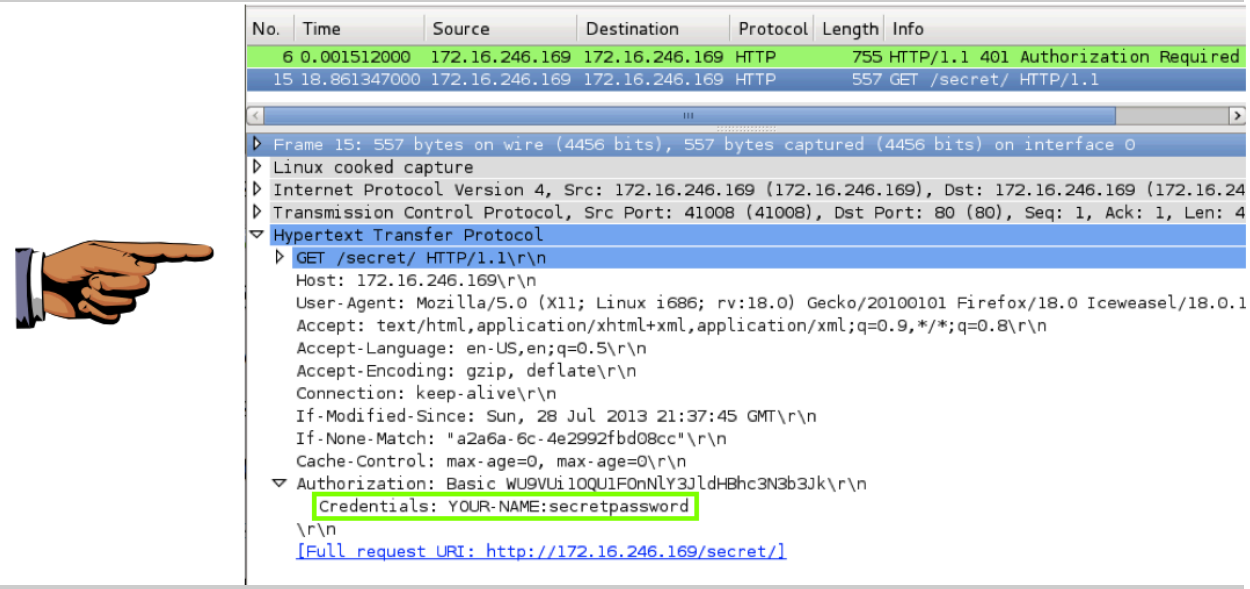
```
No. Time          Source          Destination     Protocol Length Info
  6 0.001512000   172.16.246.169  172.16.246.169  HTTP        755 HTTP/1.1 401 Authorization Required
 15 18.861347000  172.16.246.169  172.16.246.169  HTTP        557 GET /secret/ HTTP/1.1

▷ Frame 6: 755 bytes on wire (6040 bits), 755 bytes captured (6040 bits) on interface 0
▷ Linux cooked capture
▷ Internet Protocol Version 4, Src: 172.16.246.169 (172.16.246.169), Dst: 172.16.246.169 (172.16.24
▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 41007 (41007), Seq: 1, Ack: 424, Len:
▷ Hypertext Transfer Protocol
▷ Line-based text data: text/html
```

In the top pane of Wireshark, click "**GET /secret/ HTTP/1.1**".

In the middle pane, expand the "**Hypertext Tranfer Protocol**" section.

Scroll down and expand the **Authorization** section.

The credentials are shown in cleartext, showing your name and the secret password, as shown below:



```
No. Time          Source          Destination     Protocol Length Info
  6 0.001512000   172.16.246.169  172.16.246.169  HTTP        755 HTTP/1.1 401 Authorization Required
 15 18.861347000  172.16.246.169  172.16.246.169  HTTP        557 GET /secret/ HTTP/1.1

▷ Frame 15: 557 bytes on wire (4456 bits), 557 bytes captured (4456 bits) on interface 0
▷ Linux cooked capture
▷ Internet Protocol Version 4, Src: 172.16.246.169 (172.16.246.169), Dst: 172.16.246.169 (172.16.24
▷ Transmission Control Protocol, Src Port: 41008 (41008), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 4
▽ Hypertext Transfer Protocol
  ▷ GET /secret/ HTTP/1.1\r\n
    Host: 172.16.246.169\r\n
    User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Sun, 28 Jul 2013 21:37:45 GMT\r\n
    If-None-Match: "a2a6a-6c-4e2992fbd08cc"\r\n
    Cache-Control: max-age=0, max-age=0\r\n
  ▽ Authorization: Basic WU9VUi1OQU1FOnNlY3JldHBhc3N3b3Jk\r\n
      Credentials: YOUR-NAME:secretpassword
    \r\n
    [Full request URI: http://172.16.246.169/secret/]
```

Saving the Screen Image

Make sure **YOUR-NAME** and **secretpassword** are visible, as shown above.

Click the host computer's desktop. Press the PrntScrn key to capture the entire desktop.

YOU MUST SUBMIT A WHOLE-DESKTOP IMAGE FOR FULL CREDIT

Save this image as a PNG file, named "**Proj 3 from YOUR NAME**"

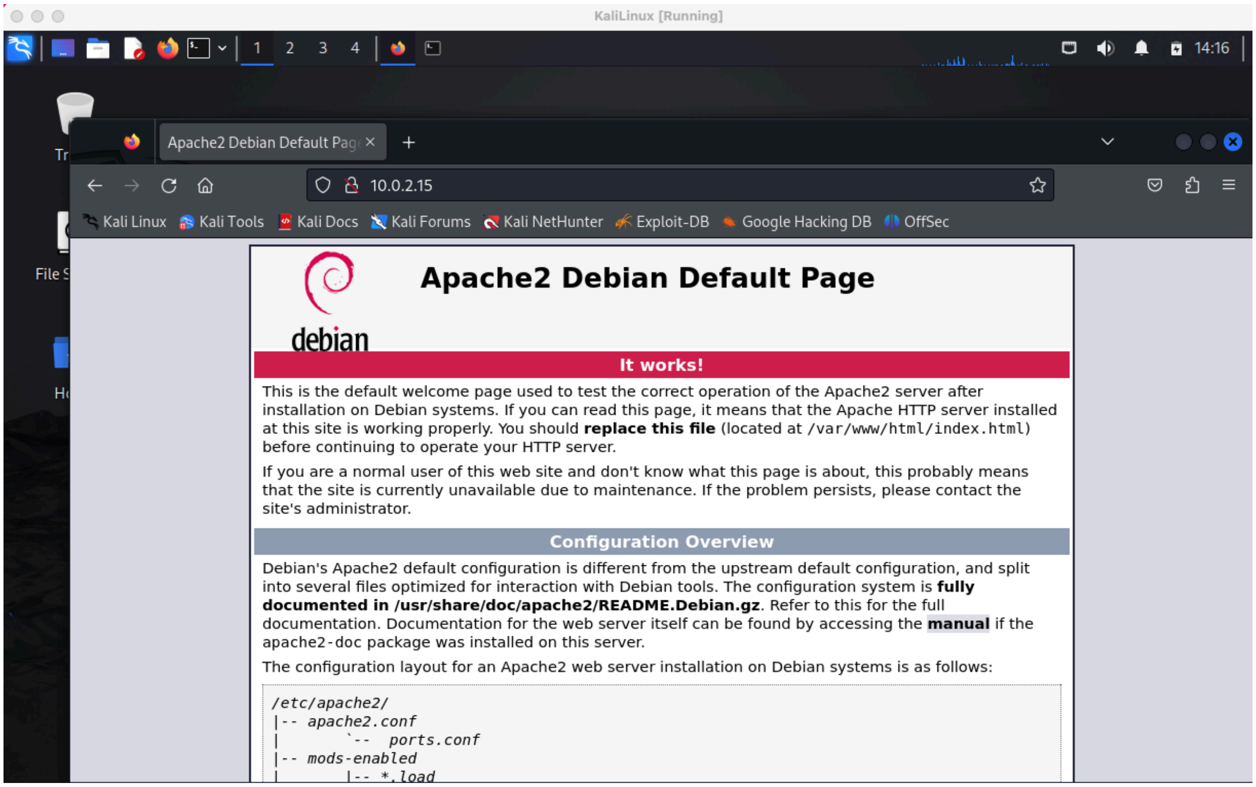
Turning in Your Project

Email the image to **cnit.123@gmail.com** with a subject of "**Proj 3 from YOUR NAME**".

Source

http://doc.norang.ca/apache-basic-auth.html

Last modified 2-9-17
Sam Bowne



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. 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.

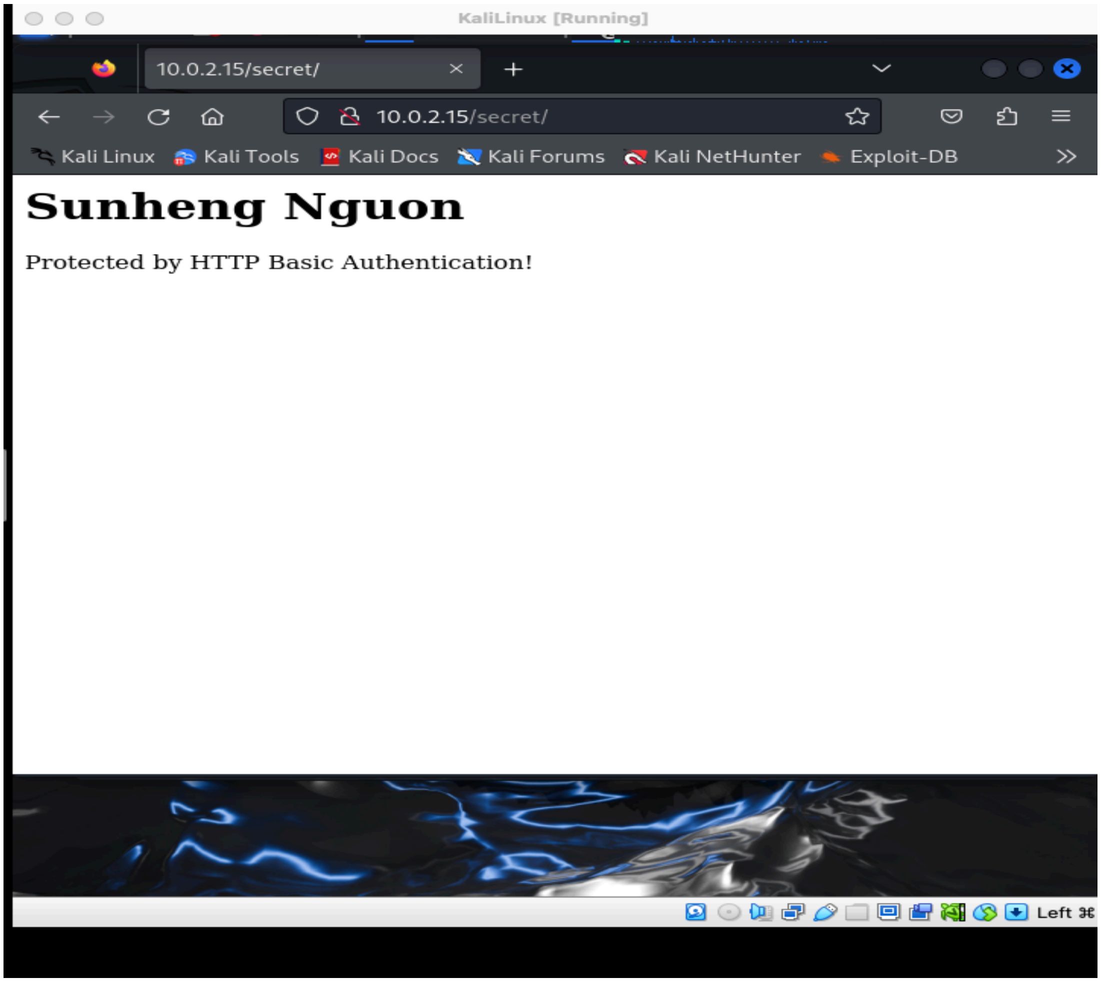
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian 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.

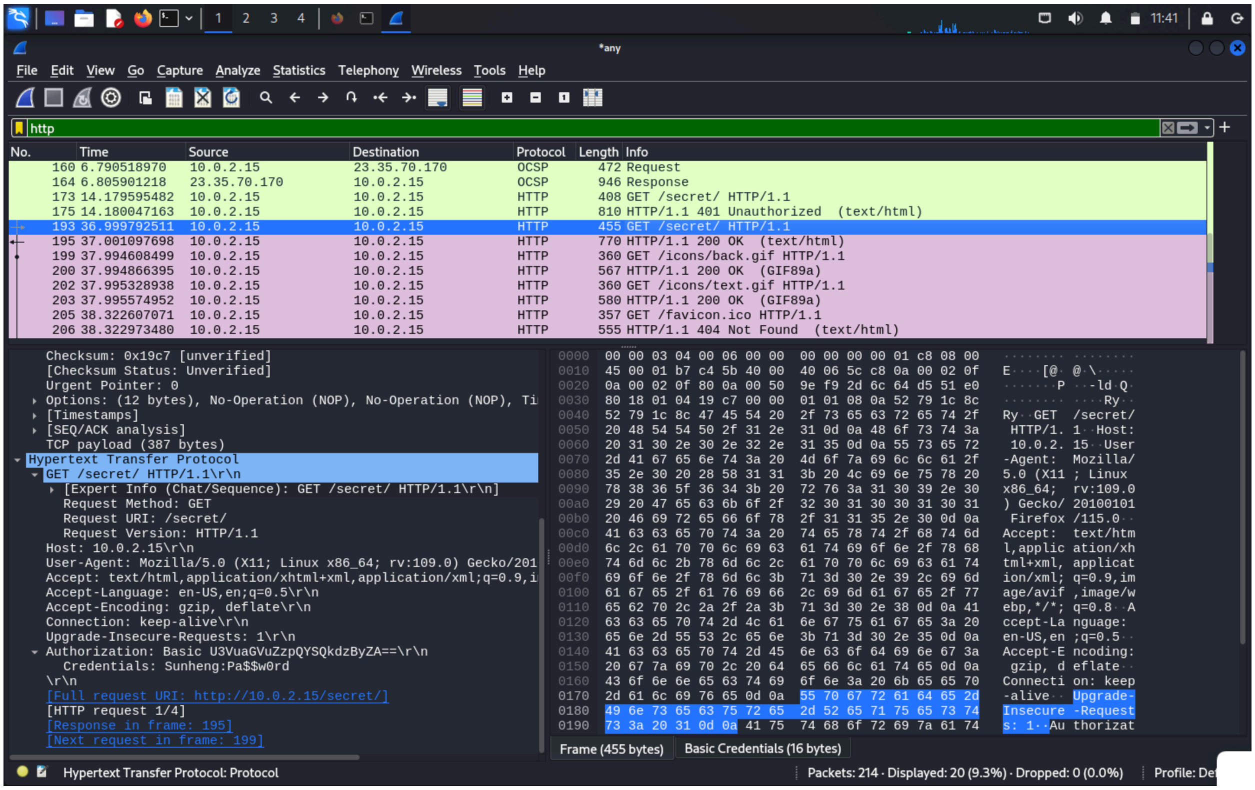
The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
```



Sunheng Nguon

Protected by HTTP Basic Authentication!



```
No.   Time          Source        Destination    Protocol Length Info
  160 6.790518970   10.0.2.15     23.35.70.170   OCSP      472 Request
  164 6.805901218   23.35.70.170  10.0.2.15      OCSP      946 Response
  173 14.179595482  10.0.2.15     10.0.2.15      HTTP      408 GET /secret/ HTTP/1.1
  175 14.180047163  10.0.2.15     10.0.2.15      HTTP      810 HTTP/1.1 401 Unauthorized  (text/html)
  193 36.999792511  10.0.2.15     10.0.2.15      HTTP      455 GET /secret/ HTTP/1.1
  195 37.001097698  10.0.2.15     10.0.2.15      HTTP      770 HTTP/1.1 200 OK  (text/html)
  199 37.994608499  10.0.2.15     10.0.2.15      HTTP      360 GET /icons/back.gif HTTP/1.1
  200 37.994866395  10.0.2.15     10.0.2.15      HTTP      567 HTTP/1.1 200 OK  (GIF89a)
  202 37.995328938  10.0.2.15     10.0.2.15      HTTP      360 GET /icons/text.gif HTTP/1.1
  203 37.995574952  10.0.2.15     10.0.2.15      HTTP      580 HTTP/1.1 200 OK  (GIF89a)
  205 38.322607071  10.0.2.15     10.0.2.15      HTTP      357 GET /favicon.ico HTTP/1.1
  206 38.322973480  10.0.2.15     10.0.2.15      HTTP      555 HTTP/1.1 404 Not Found  (text/html)
```

```
    Checksum: 0x19c7 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Ti
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (387 bytes)
▾ Hypertext Transfer Protocol
  ▾ GET /secret/ HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /secret/ HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /secret/
      Request Version: HTTP/1.1
    Host: 10.0.2.15\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/201
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,i
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
  ▾ Authorization: Basic U3VuaGVuZzpQYSQkdzByZA==\r\n
      Credentials: Sunheng:Pa$$w0rd
    \r\n
    [Full request URI: http://10.0.2.15/secret/]
    [HTTP request 1/4]
    [Response in frame: 195]
    [Next request in frame: 199]
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 01 c8 08 00   ········ ········
0010  45 00 01 b7 c4 5b 40 00  40 06 5c c8 0a 00 02 0f   E····[@· @·\·····
0020  0a 00 02 0f 80 0a 00 50  9e f9 2d 6c 64 d5 51 e0   ·······P ··-ld·Q·
0030  80 18 01 04 19 c7 00 00  01 01 08 0a 52 79 1c 8c   ········ ····Ry··
0040  52 79 1c 8c 47 45 54 20  2f 73 65 63 72 65 74 2f   Ry··GET  /secret/
0050  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
0060  20 31 30 2e 30 2e 32 2e  31 35 0d 0a 55 73 65 72    10.0.2. 15··User
0070  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0080  35 2e 30 20 28 58 31 31  3b 20 4c 69 6e 75 78 20   5.0 (X11 ; Linux
0090  78 38 36 5f 36 34 3b 20  72 76 3a 31 30 39 2e 30   x86_64;  rv:109.0
00a0  29 20 47 65 63 6b 6f 2f  32 30 31 30 30 31 30 31   ) Gecko/ 20100101
00b0  20 46 69 72 65 66 6f 78  2f 31 31 35 2e 30 0d 0a    Firefox /115.0··
00c0  41 63 63 65 70 74 3a 20  74 65 78 74 2f 68 74 6d   Accept:  text/htm
00d0  6c 2c 61 70 70 6c 69 63  61 74 69 6f 6e 2f 78 68   l,applic ation/xh
00e0  74 6d 6c 2b 78 6d 6c 2c  61 70 70 6c 69 63 61 74   tml+xml, applicat
00f0  69 6f 6e 2f 78 6d 6c 3b  71 3d 30 2e 39 2c 69 6d   ion/xml; q=0.9,im
0100  61 67 65 2f 61 76 69 66  2c 69 6d 61 67 65 2f 77   age/avif ,image/w
0110  65 62 70 2c 2a 2f 2a 3b  71 3d 30 2e 38 0d 0a 41   ebp,*/*; q=0.8··A
0120  63 63 65 70 74 2d 4c 61  6e 67 75 61 67 65 3a 20   ccept-La nguage:
0130  65 6e 2d 55 53 2c 65 6e  3b 71 3d 30 2e 35 0d 0a   en-US,en ;q=0.5··
0140  41 63 63 65 70 74 2d 45  6e 63 6f 64 69 6e 67 3a   Accept-E ncoding:
0150  20 67 7a 69 70 2c 20 64  65 66 6c 61 74 65 0d 0a    gzip, d eflate··
0160  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 6b 65 65 70   Connecti on: keep
0170  2d 61 6c 69 76 65 0d 0a  55 70 67 72 61 64 65 2d   -alive·· Upgrade-
0180  49 6e 73 65 63 75 72 65  2d 52 65 71 75 65 73 74   Insecure -Request
0190  73 3a 20 31 0d 0a 41 75  74 68 6f 72 69 7a 61 74   s: 1··Au thorizat
```

```
Hypertext Transfer Protocol: Protocol    Packets: 214 · Displayed: 20 (9.3%) · Dropped: 0 (0.0%)    Profile: Def
```