

Contents

1. Setting up a password-protected page on your group's web server using the HTTP Basic Authentication method.....	1
2. Installing with the apt-get password-cracking utility Hydra on your client (the computer in the cloud that has a GUI).....	3
3. Testing that we can access our password-protected Web site:.....	3
4. Trying to access the http://172.16.0.49 password-protected Web site:.....	3

1. Setting up a password-protected page on your group's web server using the HTTP Basic Authentication method

Installing the Apache Utilities Package

You can use a utility called `htpasswd`, part of the `apache2-utils` package, to create the file and manage the username and passwords needed to access restricted content.

- `sudo apt-get update`
- `sudo apt-get install apache2-utils`

Creating the Password File

You now have access to the `htpasswd` command. You can use this to create a password file that Apache can use to authenticate users. You will create a hidden file for this purpose called `.htpasswd` within our `/etc/apache2` configuration directory.

The first time you use this utility, you need to add the `-c` option to create the specified file. We specify a username (`labb6` in this example) at the end of the command to create a new entry within the file:

- `sudo htpasswd -c /etc/apache2/.htpasswd labb6`

You will be asked to supply and confirm a password for the user.

If you view the contents of the file, you can see the username and the encrypted password for each record:

- `cat /etc/apache2/.htpasswd`

Output:

Laboration 6 - Password security, "hacking" of web pages

```
labb6:$apr1$J/zCRZ6g$GPYluqeL8cFIWjWRnVYDr.
```

Configuring Access Control within the Virtual Host Definition

Modify the following listing (in 000-default.conf) to only target a specific directory within the web space:

```
<Directory "/var/www/html">  
</Directory>
```

```
sudo nano /etc/apache2/sites-enabled/000-default.conf
```

```
<Directory "/var/www/html">  
    AuthType Basic  
    AuthName "Restricted Content"  
    AuthUserFile /etc/apache2/.htpasswd  
    Require valid-user  
</Directory>
```

Before restarting the web server, you can check the configuration with the following command:

- `sudo apache2ctl configtest`

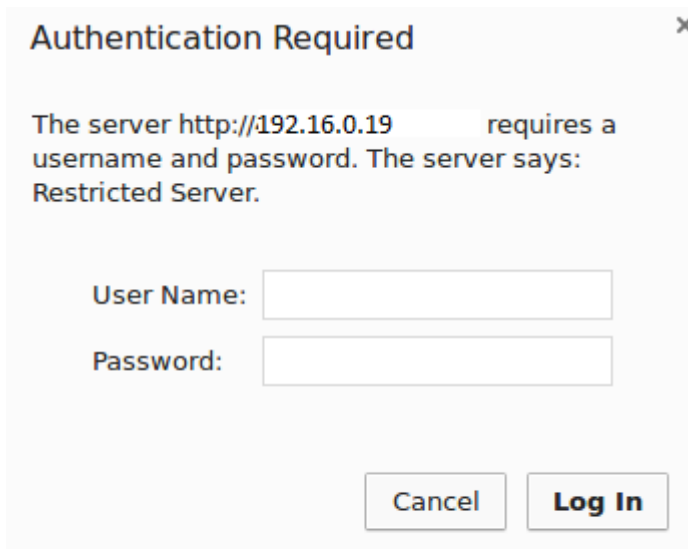
If everything checks out and you get Syntax OK, then restart the server to implement your password policy. I used the the status to be sure the server is running:

- `sudo systemctl restart apache2`
- `sudo systemctl status apache2`

Now, the directory you specified should now be password protected.

Confirming Password Authentication

To confirm that your content is protected, try to access your restricted content in a web browser. You should be presented with a username and password prompt that looks like this:



If you enter the correct credentials, you will be allowed to access the content. If you enter the wrong credentials or hit "Cancel", you will see the "Unauthorized" error page:

2. Installing with the apt-get password-cracking utility Hydra on your client (the computer in the cloud that has a GUI)

You can install hydra by

```
sudo apt-get update  
sudo apt-get install hydra
```

3. Testing that we can access our password-protected Web site:

I downloaded rockyou.txt from the internet and copied it into my client with the command below:

```
scp ./rockyou.txt gr13@172.16.0.103:/home/gr13  
  
hydra -l root -P /home/ubuntu/rockyou.txt -t 1 192.168.159.130 http-get  
var/www/html/admin/
```

4. Trying to access the http://172.16.0.49 password-protected Web site:

```
hydra -l root -P /home/ubuntu/rockyou.txt -t 1 192.168.159.49 http-get  
var/www/html/admin/
```