Week 3

Session 2

Web Services

Olga Chernukhina

Install Apache web Server on your Server

Run `sudo apt-get install apache2` in the terminal

Configure 3 websites on your server as following:

`www.innopolis.local`
`www.blocksec.innopolis.local`
`www.robotics.innopolis.local`

First, I created a folder for source files for each website

```
user1@cli2-VirtualBox:~$ sudo mkdir -p /var/www/blocksec.innopolis/public_html
user1@cli2-VirtualBox:~$ sudo mkdir -p /var/www/innopolis.local/public_html
user1@cli2-VirtualBox:~$ sudo mkdir -p /var/www/robotics.innopolis/public_html
```

Then I created a default file that will load at the moment the site is accessed

```
user1@cli2-VirtualBox:~$ sudo nano /var/www/robotics.innopolis/public_html/inde
x.html
user1@cli2-VirtualBox:~$ sudo nano /var/www/blocksec.innopolis/public_html/inde
x.html
user1@cli2-VirtualBox:~$ sudo nano /var/www/innopolis.local/public_html/index.h
tml
```

I copied the default site configuration file into each newly created website .conf

```
user1@cli2-VirtualBox:~$ sudo cp /etc/apache2/sites-available/000-default.conf
/etc/apache2/sites-available/innopolis.local.conf
user1@cli2-VirtualBox:~$ sudo cp /etc/apache2/sites-available/000-default.conf
/etc/apache2/sites-available/blocksec.innopolis.conf
user1@cli2-VirtualBox:~$ sudo cp /etc/apache2/sites-available/000-default.conf
/etc/apache2/sites-available/robotics.innopolis.conf
```

The configuration for each site is the same with Server Name, Document Root and Server Alias fields modified respectively to the appropriate names

```
        /etc/apache2/sites-available/robotics.innopolis.conf

<VirtualHost *:80>

        ServerAdmin webmaster@localhost
        ServerName www.robotics.innopolis.local
        ServerAlias robotics.innopolis.local
        DocumentRoot /var/www/robotics.innopolis/public_html

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
```

I modified `/etc/hosts` file to handle the requests to access the newly created sites (later on the aliases were also added to the configuration)

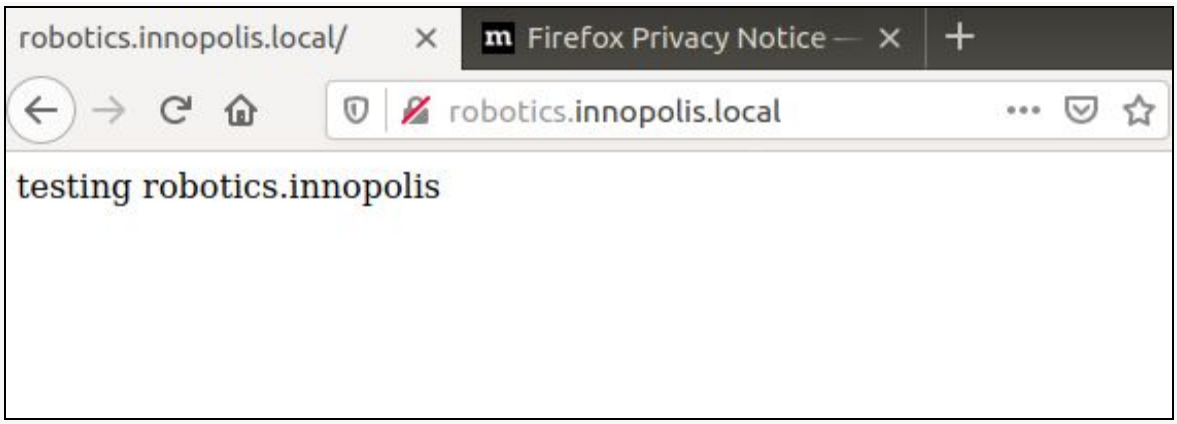
```
  GNU nano 2.9.3                        /etc/hosts

127.0.0.1       localhost
127.0.1.1       cli2-VirtualBox

127.0.0.1       www.innopolis.local
127.0.0.1       www.robotics.innopolis.local
127.0.0.1       www.blocksec.innopolis.local
```

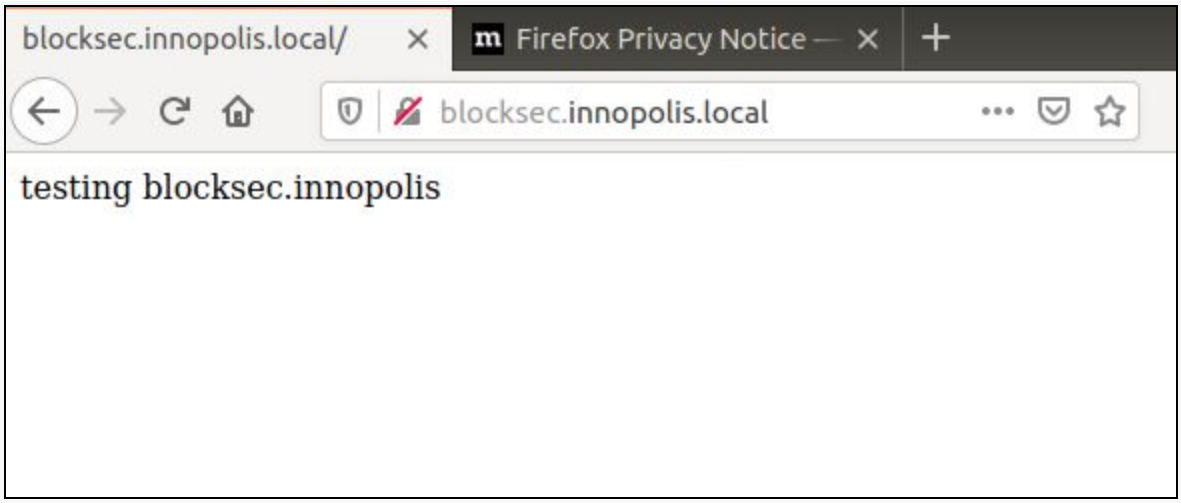
I enabled each site in the following way

```
user1@cli2-VirtualBox:~$ sudo a2ensite innopolis.local.conf
Enabling site innopolis.local.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

Then restarted apache server with `systemctl restart apache2`

Check that everything works fine:





Configure Page not found and forbidden special pages for “www.innopolis.local”.

I added the following lines to the configuration file of innopolis.local

```
ErrorDocument 404 /custom_404.html
ErrorDocument 403 /custom_403.html
```

```
<Files *.txt>
Order Deny,Allow
Deny from All
</Files>
```

Then I created and configured these files in the site’s sources directory mentioned above

```
cli2@cli2-VirtualBox:/var/www/innopolis.loca
custom_403.html  custom_404.html  file.txt
```

Then restarted apache server with `systemctl restart apache2`

Now testing that everything works as it should:

1) accessing a directory that doesn’t exist

2) accessing a .txt file that is forbidden to access in innopolis.local.conf

Create one more website on port 9090 in the “www.innopolis.local” website as if it is your service monitoring website.

I created a new configuration file on the apache server and connected it with the existing source files of innopolis.local

```
        /etc/apache2/sites-available/innopolis.local.9090.conf

<VirtualHost *:9090>
        ServerAdmin     webmaster@localhost
        DocumentRoot    /var/www/innopolis.local/public_html
        ServerName      www.innopolis.local
        ServerAlias     innopolis.local
</VirtualHost>
```

Then I added 9090 port to the list of “listened” in `/etc/apache2/ports.conf`

```
  GNU nano 2.9.3                        ports.conf

# If you just change the port or add more ports here, you wi
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80
Listen 9090

<IHelpule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>
```

Turned off and again on innopolis.local

```
user1@cli2-VirtualBox:/etc/apache2$ sudo a2ensite innopolis.local.9090.conf
Enabling site innopolis.local.9090.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

Then restarted apache server with `systemctl restart apache2` and tested the result

Protect the “www.innopolis.local/special/” with additional password.

I created a directory “special/” in the sources on innopolis.local and added its password protection to the configuration file

```
 GNU nano 2.9.3  /etc/apache2/sites-available/innopolis.local.conf  Modified

        ServerAlias innopolis.local
        DocumentRoot /var/www/innopolis.local/public_html

        <Files *.txt>
        Order Deny,Allow
        Deny from All
        </Files>

        <Directory /var/www/innopolis.local/public_html/special>
                AuthType Basic
                AuthName "Basic Authentication"
                AuthUserFile /var/www/innopolis.local/public_html/.htpasswd
                require valid-user
        </Directory>
```

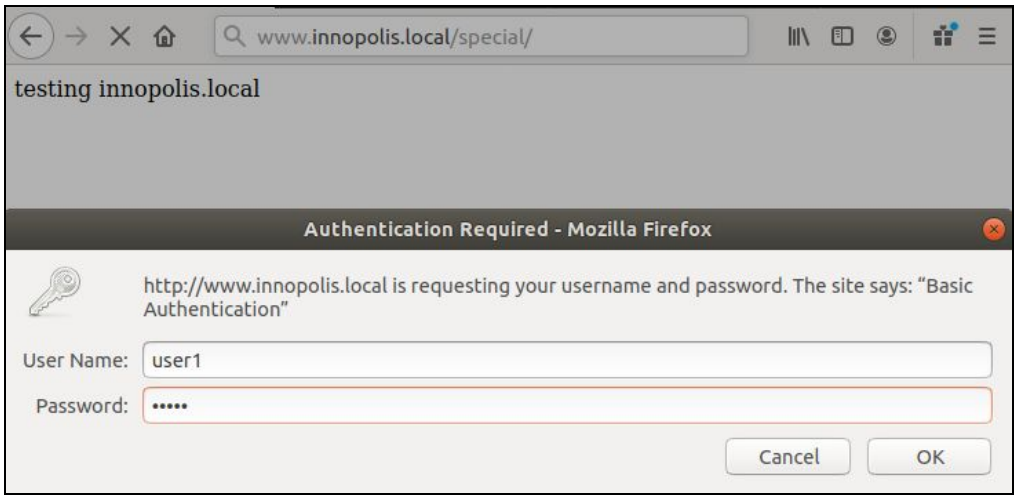
I created a user with a password in .htpasswd file in the same location that was mentioned in the .conf file

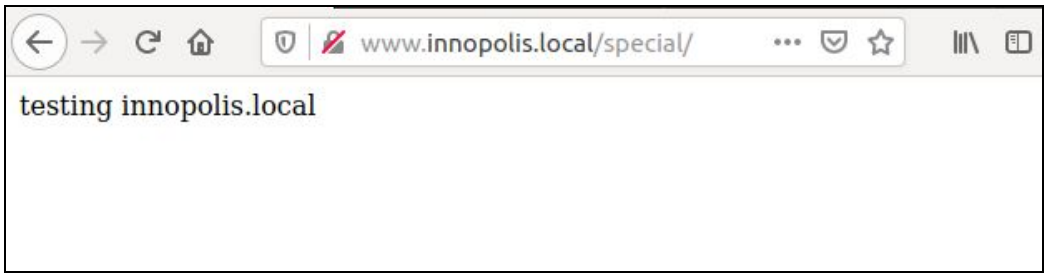
```
user1@cli2-VirtualBox:~$ sudo htpasswd -c /var/www/innopolis.local/public_html/
.htpasswd user1
New password:
Re-type new password:
Adding password for user user1
```

Then restarted apache server with `systemctl restart apache2`

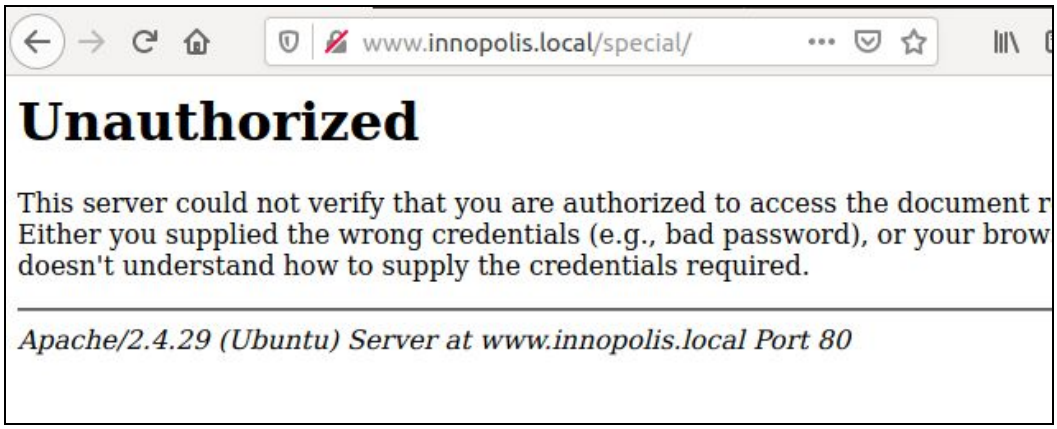
Testing:

1) accessing with valid credentials





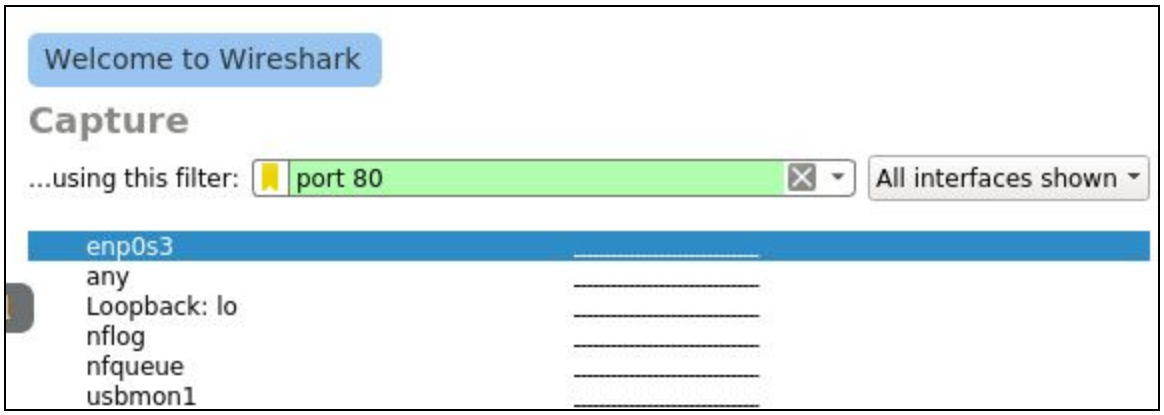
2) accessing with empty fields of user name and password gives the following



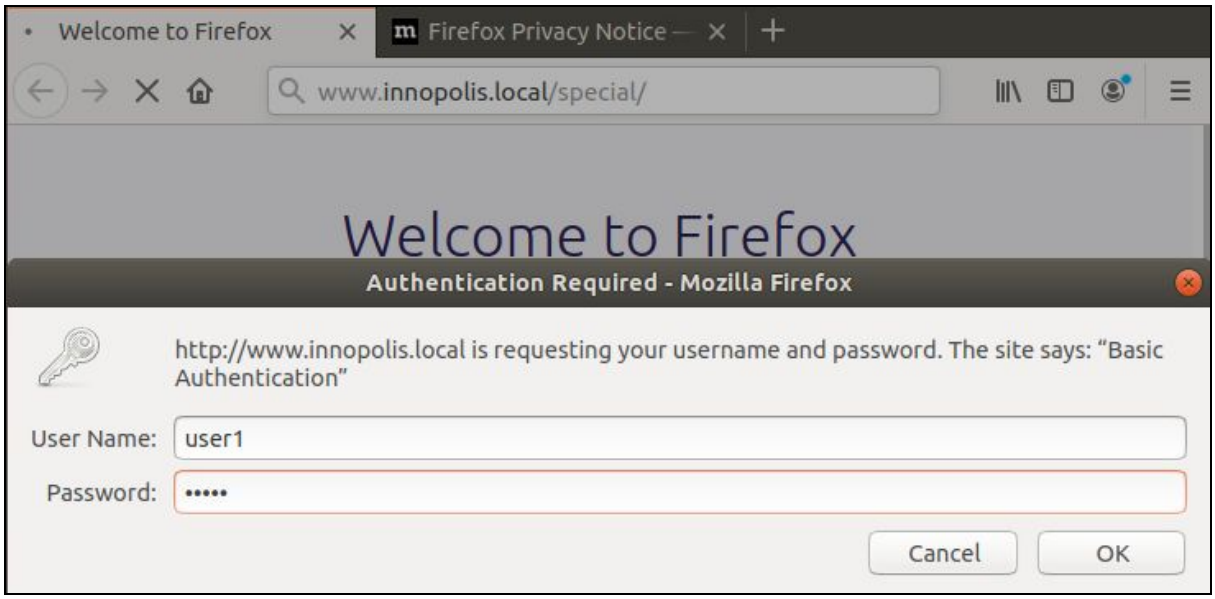
Capture this additional password using wireshark.

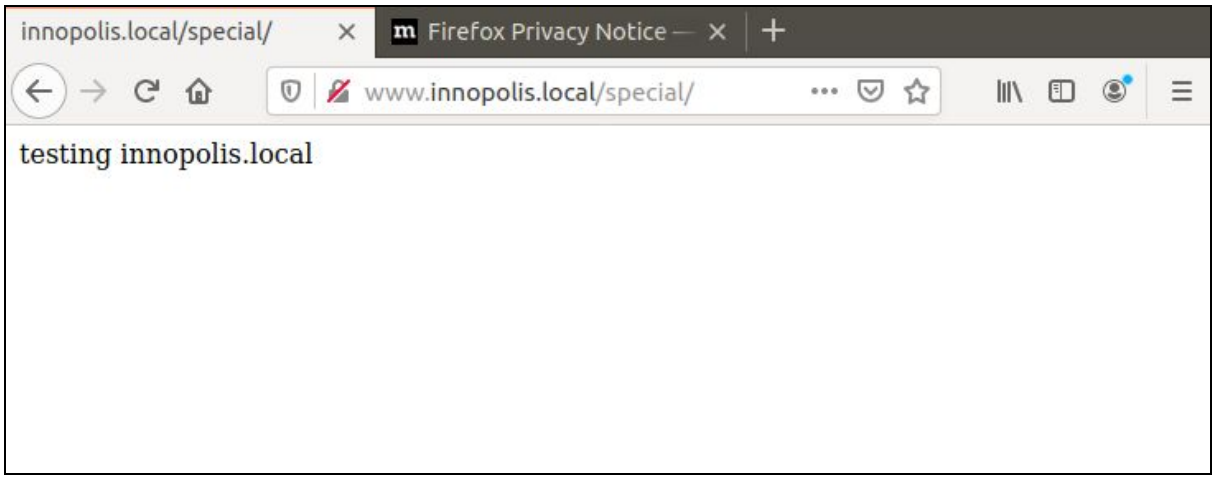
On the client machine run sudo apt-get install wireshark

Configure it to listen on the appropriate interface on port 80:

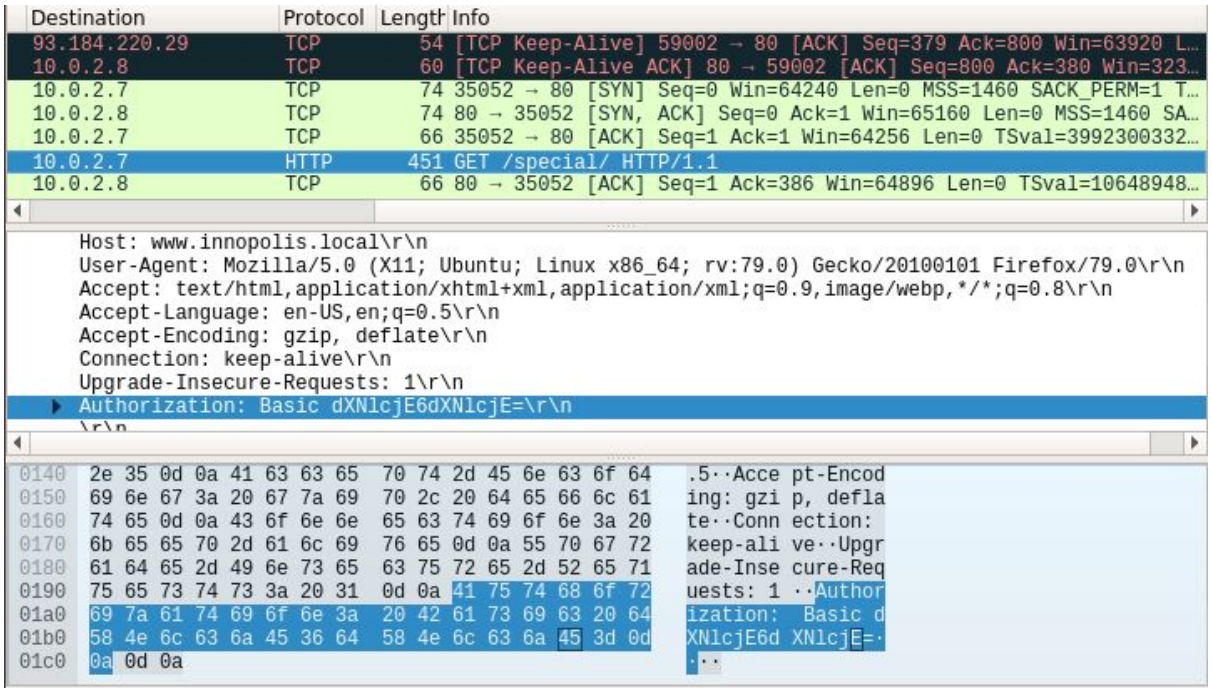


Access the protected directory providing username and password:





Analyze the transmitted packets:

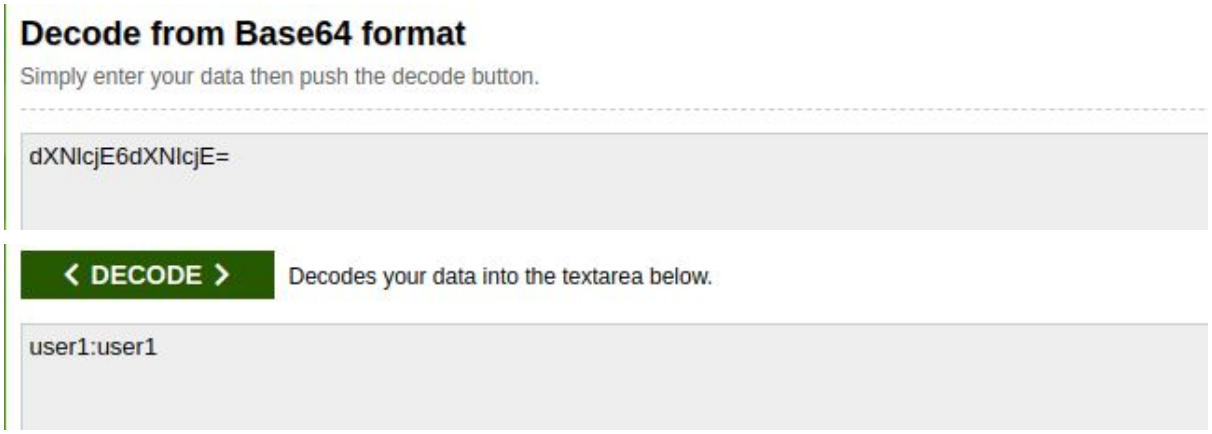


In the official documentation the following information is given regarding HTTP basic access authentication protocol:

In the client side, the HTTP basic access authentication protocol implies the following:

1. *The username and password are concatenated with a colon in between them to generate a single string, preferably using UTF-8,*
2. *The resulting string in the previous step is then encoded using a variant of Base64, and*
3. *The encoded string is included in every HTTP request as the authorization header as: Authorization: Basic dXNlcjE6dXNlcjE=, where dXNlcjE6dXNlcjE= is the encoded security token.*

So, processing the obtained encoded password in the online tool https://www.base64decode.org/



Enable HTTPS for all three websites

The procedure is shown for www.blocksec.innopolis.local
Since it is the same for all websites, it is not repeated in the report

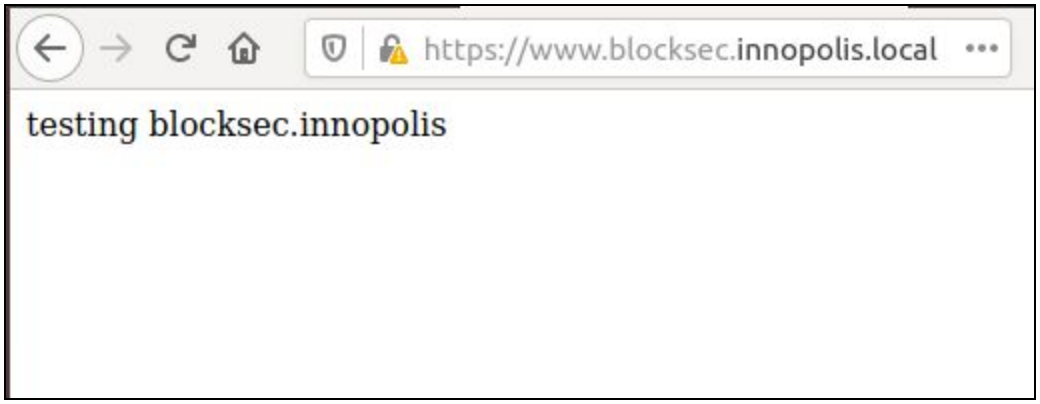
I created a folder `ssl` in the `/etc/apache2/` and created certificates via `openssl`

```
cli2@cli2-VirtualBox:/etc/apache2/ssl$ sudo openssl req -new -x509 -days 365 -n
odes -out key.pem -keyout key.key
```

In the configuration file I added port 443 and all the necessary configs

```
<VirtualHost *:443>
        DocumentRoot /var/www/blocksec.innopolis/public_html
        ServerName www.blocksec.innopolis.local
        ServerAlias blocksec.innopolis.local
        SSLEngine on
        SSLCertificateFile ssl/key.pem
        SSLCertificateKeyFile ssl/key.key
</VirtualHost>
```

Testing that it works



Redirect the users if they used HTTP instead of HTTPS

I added rewrite mod via `a2enmod rewrite`

Then added rewriting for clients that try to access the website on port 80:

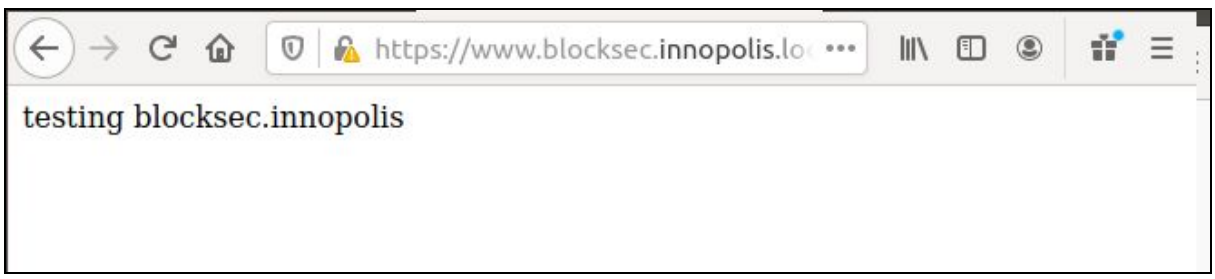
```
 GNU nano 2.9.3        sites-enabled/blocksec.innopolis.conf

<VirtualHost *:80>

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/blocksec.innopolis/public_html
        ServerName www.blocksec.innopolis.local
        ServerAlias blocksec.innopolis.local

        RewriteEngine On
        RewriteCond %{HTTPS} off
        RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Then restarted apache server with `systemctl restart apache2`

Testing:

1) accessing via http

2) getting redirected



Setup and Configure SQUID for “www.blocksec.innopolis.local” website

Run `sudo apt-get install squid3`

In the configuration file:

1) Set Squid in reverse proxy mode by

   ```
   http_port 3128 accel defaultsite=www.blocksec.innopolis.local vhost
   ```

2) Define the Web Server

   ```
   cache_peer 127.0.0.1 parent 80 0 no-query originserver
   name=blocksec.innopolis
   ```

3) Assign permissions

   ```
   acl known_hosts dstdomain www.blocksec.innopolis.local
   http_access allow known_hosts
   cache_peer_access blocksec.innopolis allow known_hosts
   cache_peer_access blocksec.innopolis deny all
   ```

Overall the configuration file should look like this:

```
  GNU nano 2.9.3                    squid.conf                         Modified

http_port 3128 accel defaultsite=www.blocksec.innopolis.local vhost
cache_peer 127.0.0.1 parent 80 0 no-query originserver name=blocksec.innopolis
acl known_hosts dstdomain www.blocksec.innopolis.local
http_access allow known_hosts
cache_peer_access blocksec.innopolis allow known_hosts
cache_peer_access blocksec.innopolis deny all
```

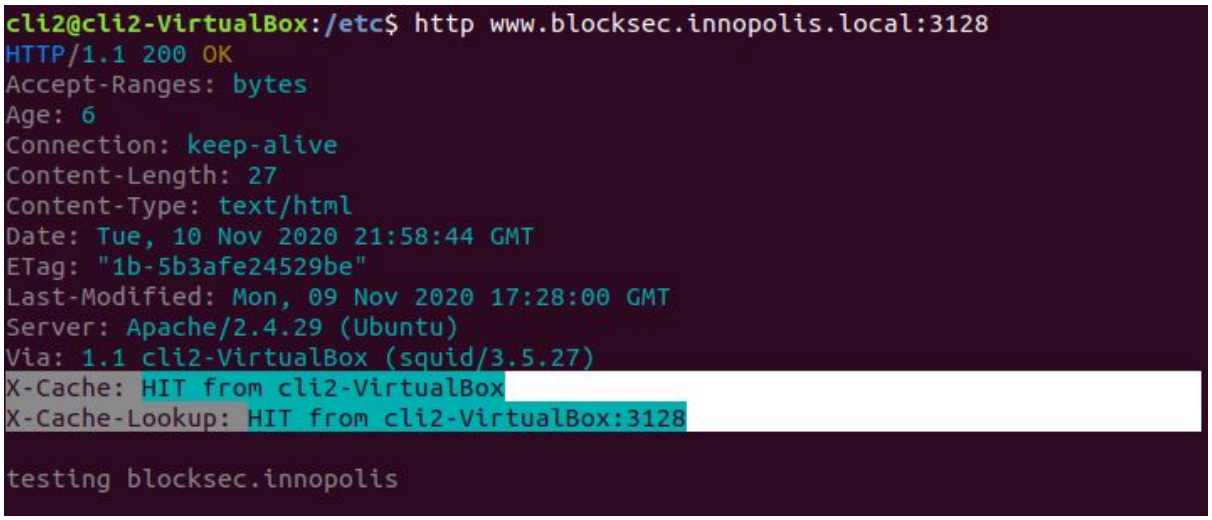
Restart squid - `sudo /etc/init.d/squid restart`

Testing:

1) try to access the file via SQUID
   Result - it is not in cache yet, still it is accessible

```
cli2@cli2-VirtualBox:/etc$ http www.blocksec.innopolis.local:3128
HTTP/1.1 200 OK
Accept-Ranges: bytes
Connection: keep-alive
Content-Length: 27
Content-Type: text/html
Date: Tue, 10 Nov 2020 21:58:44 GMT
ETag: "1b-5b3afe24529be"
Last-Modified: Mon, 09 Nov 2020 17:28:00 GMT
Server: Apache/2.4.29 (Ubuntu)
Via: 1.1 cli2-VirtualBox (squid/3.5.27)
X-Cache: MISS from cli2-VirtualBox
X-Cache-Lookup: MISS from cli2-VirtualBox:3128

testing blocksec.innopolis
```

2) try to access the same site for the second time
Result - it is in cache now



Bonus

What is Google dorks? give 3 examples.

This is a set of special queries to identify security holes. This type of requests to the search engine provide direct links to confidential data and lists of vulnerable network nodes.

Examples:

FILETYPE: or EXT:
Search by file extension. You can search for photos, archives, text files, logs, databases, and so on.
Example: filetype: sql
The result: http://www.namesurname.com/personal_data_wrd2.sql

INTITLE:
Search on the site between the <title>tagsFind this text< / title>

SIZE:
Search by file size\pages.
size:512000 will find content larger than 500 KB.

What is DirBuster?

DirBuster is a multithreaded Java application designed to brute force directory and file names of web applications and web servers. DirBuster tries to find hidden directories and files.

In addition, this tool is very valuable for its lists of directories and files. This program comes with several dictionaries (in the latest version - 9), which were collected from the actual names of files and directories. But DirBuster can also do pure brute force.

Sources:

https://www.liquidweb.com/kb/configure-apache-virtual-hosts-ubuntu-18-04/

https://www.digitalocean.com/community/tutorials/how-to-configure-apache-to-use-custom-error-pages-on-ubuntu-14-04

https://webmasters.stackexchange.com/questions/20306/how-to-set-up-a-403-forbidden

https://computingforgeeks.com/how-to-configure-apache-web-page-authentication/

https://httpd.apache.org/docs/2.4/howto/auth.html

https://www.dmosk.ru/miniinstruktions.php?mini=apache-ssl

http://cosmolinux.no-ip.org/raconetlinux/html/17-squid.html