HTTP. Web Lab 2

Tabla de Contenido

This lab will set up virtual servers where authentication tests will be carried out.

> ❗ The network values used in this lab are *general*. You must adapt both the network and the IP addresses of the machines to your classroom network and to the IP addresses you have reserved for your machines. If you do this lab at home, these network values *might* work without changes.

> 💡 You can use the virtual machines created in *HTTP. Web Lab 1*

Initial configuration

Start from the following network configuration:

a. The hosts are on the network `192.168.56.0/24`

b. The first Linux VM will be called `dns` and will be a DNS server. It will have authority over the domain `sistema.sol.` Its IP address will be `192.168.56.100`.

c. Likewise it will act as the master server and will have authority over the reverse resolution zone of the network `192.168.56.0/24`. Therefore the DNS server for the domain will be `dns.sistema.sol`.

d. The second Linux VM will belong to the above network with IP `192.168.56.101`, with an appropriate gateway and `tierra` as the hostname. The role of `tierra` will be that of a web server.

In summary, the hostnames and their IPs will be:

`dns.sistema.sol`	`192.168.56.100`	Linux DNS server
`tierra.sistema.sol`	`192.168.56.101`	Linux Web server

1. Both VMs will use the DNS server installed on `dns` and will add the suffix `sistema.sol` to non-FQDN names.
2. Test with the `nslookup` or `dig` command from both VMs that the domain names resolve correctly.

> ❗ If the DNS service does not work, you cannot continue with the lab.

`discovery.sistema.sol`

We want to create and enable a web server for the domain `discovery.sistema.sol` hosted on the host `tierra.sistema.sol`. This server will be used for authentication tests.

1. Configure the DNS server so that the name `discovery.sistema.sol` resolves as an alias for `tierra.sistema.sol`.
2. Then test with `nslookup` or `dig` that the domain name resolves correctly.

Provisioning

1. Create the web root directory for the server, `/var/www/discovery.sistema.sol`.
2. Add an `index.html` file to the above directory with any desired HTML content.
3. Create the following directory and file structure.

Ejemplo 1. Root document tree for `discovery.sistema.sol`

```
discovery.sistema.sol/
├── basic
│   ├── desarrollo
│   │   └── index.html
│   ├── ventas
│   │   └── index.html
│   └── index.html
├── digest
│   └── hello.html
└── index.html
```

4. Create an Apache virtual host for the domain. The configuration file will be `discovery.sistema.sol.conf` and will be located in `/etc/apache2/sites-available`.
5. Once created, enable the virtual host.

Verification

1. http://discovery.sistema.sol should show the `index.html` page.
2. http://discovery.sistema.sol/basic should show the `index.html` page inside the `basic` directory.
3. http://discovery.sistema.sol/basic/ventas should show the `index.html` page inside the `ventas` directory.

4. http://discovery.sistema.sol/basic/desarrollo should show the `index.html` page inside the `desarrollo` directory.
5. http://discovery.sistema.sol/digest should show the `index.html` page inside the `digest` directory.

Virtual hosting with HTTP Basic authentication

We will set up and configure the virtual hosting of a website where some directories are protected by HTTP Basic authentication.

Configuration

Following the notes *Web Servers. Apache*, perform the following configuration:

1. The `basic` directory will use basic authentication.
2. The user password file will be at `/etc/apache2/.htpasswd_basic`. Encryption will be the default.
3. We will create the following users

user	**password**
arturo	arturo
ana	ana
maria	maria

4. We will create a user groups file located at `/etc/apache2/.htgroups`.
5. We will create the following groups with their assigned users

Group	**Members**
ventas	arturo
desarrollo	ana

6. Any user present in the database and who authenticates may enter the `basic` directory.
7. Only users in the `desarrollo` group may enter the `desarrollo` directory.
8. Only users in the `ventas` group may enter the `ventas` directory.

Verification

> To avoid caching of usernames and passwords, try accessing in a browser's private/incognito mode. After testing, close the browser.

1. http://discovery.sistema.sol/ All users can access without authentication.
2. http://discovery.sistema.sol/basic Only `ana`, `maria` and `arturo` can enter. Other users cannot

access.

3. http://discovery.sistema.sol/basic/desarrollo Only ana can enter. Users maria and arturo cannot enter.
4. http://discovery.sistema.sol/basic/ventas Only arturo can enter. Users maria and ana cannot enter.

Virtual hosting with HTTP Digest authentication

Set up and configure the virtual hosting of a website in Apache on Linux using HTTP Digest authentication for that site.

When Apache receives a request for a site it checks whether the request is authorized, so that only authorized users can access the site. Specifically it performs three steps:

Authentication

It checks the identity of the user using a username and password to see if those credentials match those stored in its database. There are basically two HTTP authentication methods: *basic* and *digest*.

Authorization

Afterwards the server checks whether the previously validated user has authorization for the requested information. Apache manages these authorizations through directives in the `<Directory>` section.

Access control

Finally, it establishes and controls which hosts have access to a resource, regardless of the user accessing it. Apache manages access control through directives in the `<Directory>`, `<Files>` and `<Location>` sections.

Taking the above into account, we want to add HTTP Digest authentication to the domain `discovery.sistema.sol` using the document root `/var/www/discovery.sistema.sol/digest`. Only the user `commander` will be allowed to access this website.

Configuration

The steps to follow are:

1. Configure the DNS server so that `discovery.sistema.sol` resolves.
2. Create the directory `/var/www/discovery.sistema.sol/digest` containing a `hello.html` file with a welcome message for the website.
3. The default file to be served in this directory will be `hello.html`.
4. Enable the `auth_digest` module. Using the command:

   ```
   a2enmod auth_digest
   ```

5. For Digest authentication you must create a file accessible by Apache where users, groups and passwords will be stored. For this the htdigest command is used as follows:

   ```
   htdigest -c /etc/apache2/password_file realm user
   ```

   With the -c option you allow creation of a key file (*password_file*); with *realm* the group or realm the user belongs to; and with *user* the name of a user to add to the key file (If you want to add more users later, repeat the command without the -c option since the key file has already been created). When executing the command a password for the user will be requested.

   In our case we will create the key file named .htpasswd_digest, adding the user commander to the user group or realm astronauts (We will later see that the group or realm must match the AuthName given in the site configuration).

6. Inspect the digest key file which should contain a line similar to the following:

   ```
   commander:astronauts:19c426e5b25e9bd568eaa17b5f0a6503
   ```

7. In the <Directory> section for the digest directory, add the necessary directives as follows:

   Ejemplo 2. File /etc/apache2/sites-available/discovery.sistema.sol.conf

   ```
   AuthType Digest
   AuthName "astronauts"
   AuthUserFile "/etc/apache2/.htpasswd_digest"
   Require user commander
   ```

8. Enable the virtual host and then restart the Apache service.

Verification

1. From the web browser access http://discovery.sistema.sol/digest
2. An authentication window will be presented where the user's credentials are entered, and then the content of the hello.html file will be displayed.

Submission

Submit a screenshot of:

- discovery.sistema.sol.conf
- /etc/apache2/.htpasswd_basic
- /etc/apache2/.htgroups
- /etc/apache2/.htpasswd_digest