

Lab 04 Requirements

- VM Snapshots from Lab 03

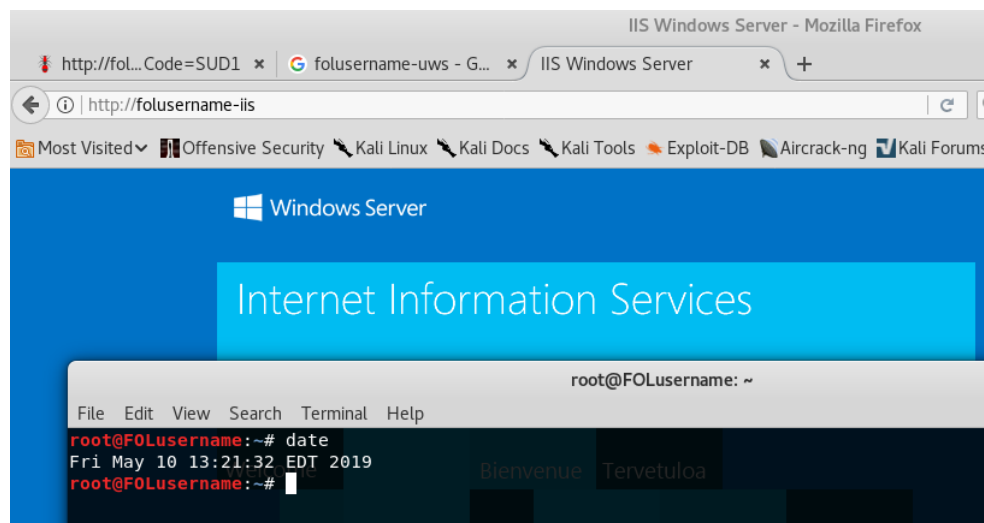
Part 01: IIS 10.0 Role set up

Start your Windows Server 2016 VM

Go to **Server Manager -> Manage -> Add Roles and Features**

- ✓ Role based or Feature based installation
- ✓ Select the current server .201
- ✓ Select Web Server (IIS)
- ✓ Under Role Services, add FTP Server -> FTP Services
- ✓ Confirm and Install

Once the installation finishes, ensure you can reach the default IIS web page from Kali Linux by navigating to <http://folusername-iis> and issue the **date** command in the terminal



Slide 1:

- **Show Firefox on Kali with the default IIS page loaded**
- **Ensure your FOLusername is in the URL**
- **Issue the date command in a terminal window**

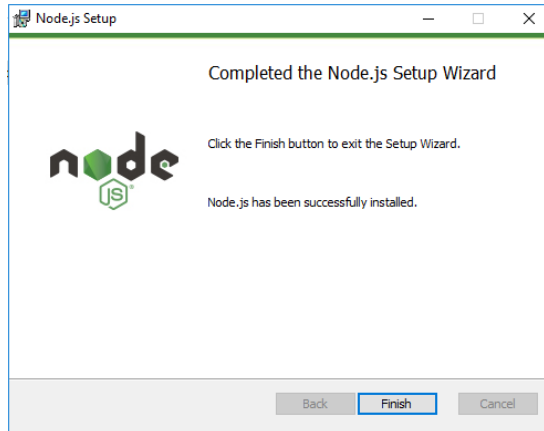
Part 02: Install OWASP Juice Shop on the Windows 2016 Web Server

Add another network adapter to Windows Server 2016 so that it has internet access

Download nodejs from <https://nodejs.org/en/download/>

Ensure you select the Windows x64 Edition and run the **.msi** installer

Run the installer and ensure it finishes successfully



Download Git for Windows using the x64-bit.exe file

<https://gitforwindows.org/>

Install Git using the installer .exe file

Once installed, open Git and run the following command:

```
git clone https://github.com/bkimminich/juice-shop.git
```

```
cmd MINGW64; c:/Users/FOLusername

FOLusername@WIN-6E2FPE30QPN MINGW64 ~
$

FOLusername@WIN-6E2FPE30QPN MINGW64 ~
$ git clone https://github.com/bkimminich/juice-shop.git
Cloning into 'juice-shop'...
remote: Enumerating objects: 48101, done.
remote: Total 48101 (delta 0), reused 0 (delta 0), pack-reused 48101
Receiving objects: 100% (48101/48101), 102.25 MiB | 6.67 MiB/s, done.
Resolving deltas: 100% (34578/34578), done.
Checking out files: 100% (526/526), done.

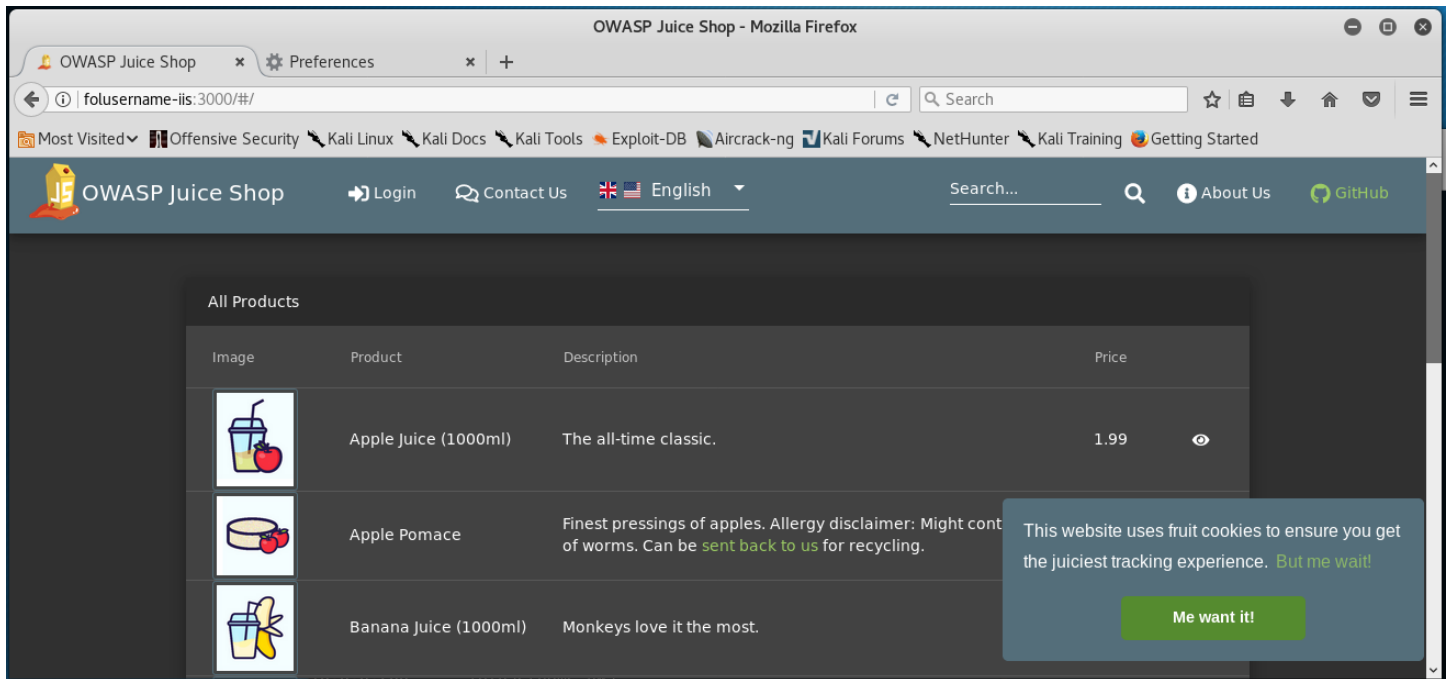
FOLusername@WIN-6E2FPE30QPN MINGW64 ~
$
```

Navigate to the C:\users\FOLusername\juice-shop directory. Right click on the blank space and select **Get Shell Here**. Once the Git shell opens, issue the following two commands:

Run **npm install** (This may take some time)

Run **npm start**


Once completed, you should be able to navigate to <http://folusername-iis:3000> from your Kali Linux VM and see the OWASP Juice Shop page as shown below:

**Slide 02:**

Take a screenshot showing the OWASP Juice Shop working and place it into slide 02

Part 03: Set up Burp Suite

On Kali Linux

 Open the free version (Free Edition) of Burp Suite from the menu on the left side of the screen

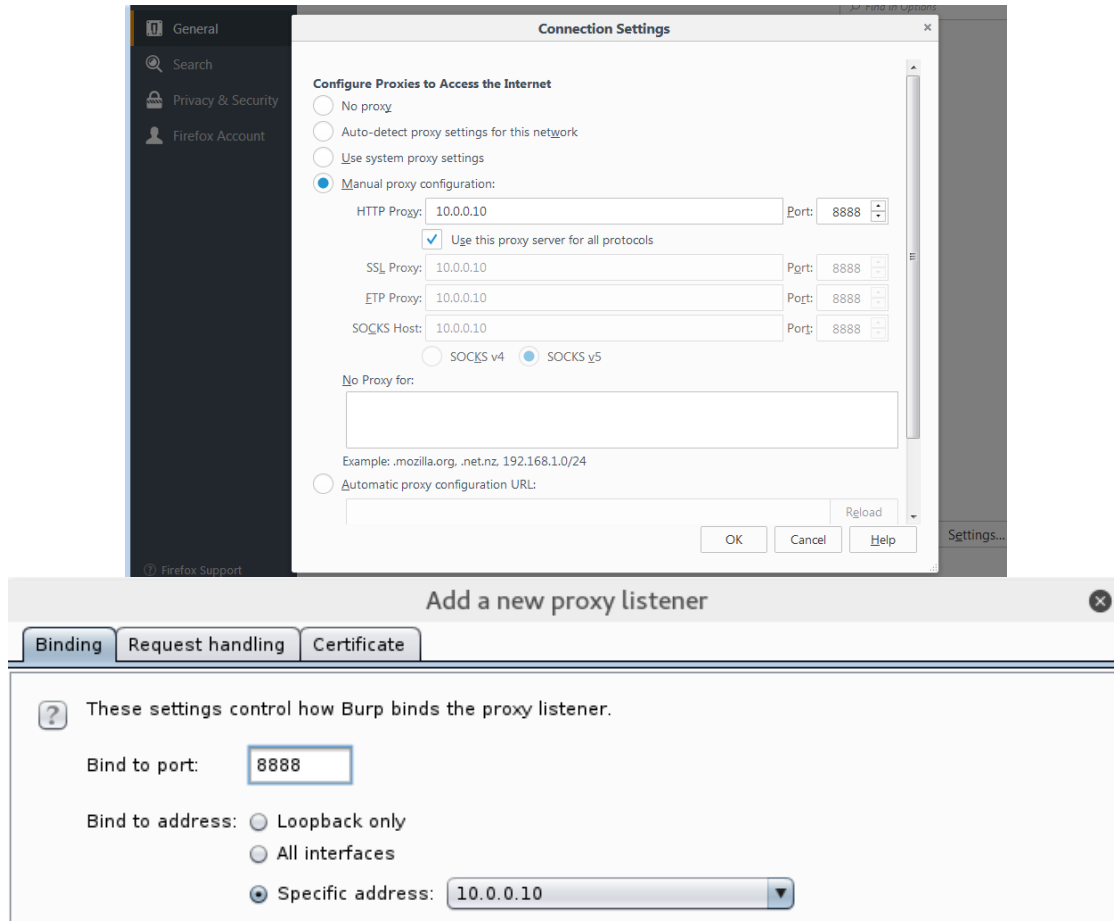
Select a **Temporary project** and **Use Burp defaults**

Navigate to the **Proxy** tab, then the **Options** sub-tab and make a note of the proxy Interface.

Click “Add” under Proxy Listeners to make a new entry in the list

Bind to port # 8888

Select Bind to Specific address: 10.0.0.10 (**See the following example**)



Click Ok to accept these values. You should now have two entries in the list

Navigate to the **Intercept** sub-tab and verify that **Intercept is on**
Leave Burp Suite Open (you can minimize the window).

Configure Firefox to Work with Burp Suite

On Windows 10

Under the Firefox menu, go to: **Options -> General -> Network Proxy -> Settings**
(Depending on the version of FF you are using, the menus might differ slightly)

Select **Manual Proxy Configuration** and configure your settings as shown below:
Enter HTTP Proxy: IP address and Port from the Burp Suite (10.0.0.10) and 8888.

Remove everything from the **No Proxy for:** section and check "Use this proxy server for all protocols".

Click OK

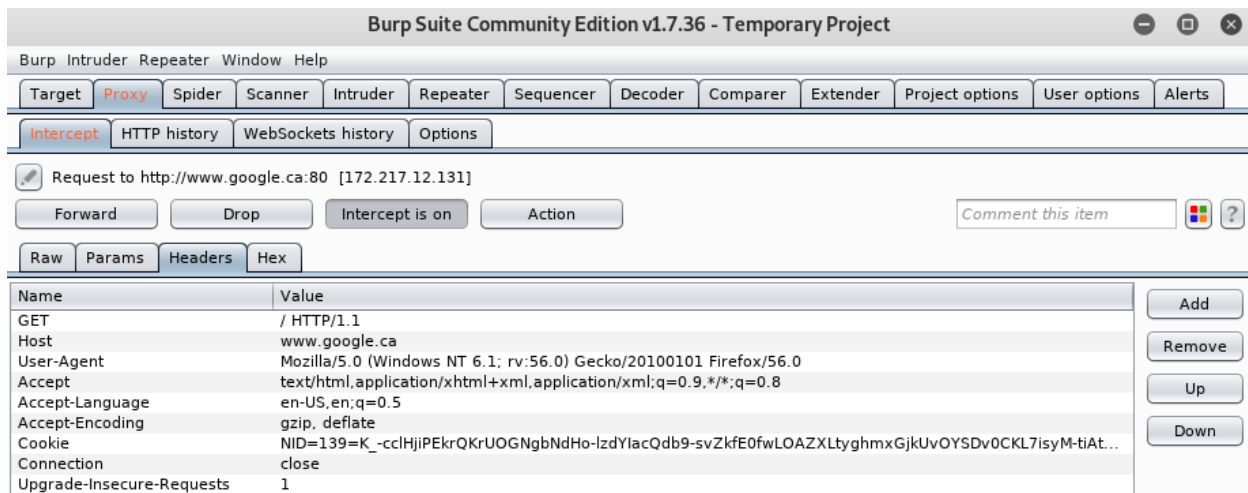
In Firefox open a new tab and enter www.google.ca in the address bar. You should see Firefox waiting for the server to respond to its request for this URL

On Kali Linux

The Burp Suite window should pop up. If not, go back to the Burp Suite window that you minimized, click on the **Proxy** tab and then the **Intercept** sub-tab

Notice that **Intercept** is still **on** and Burp Suite intercepted the HTTP GET request from the Windows 10 Firefox VM?

You should also see a raw data of the HTTP GET request. Click on the **Headers** sub-tab



Slide 03:

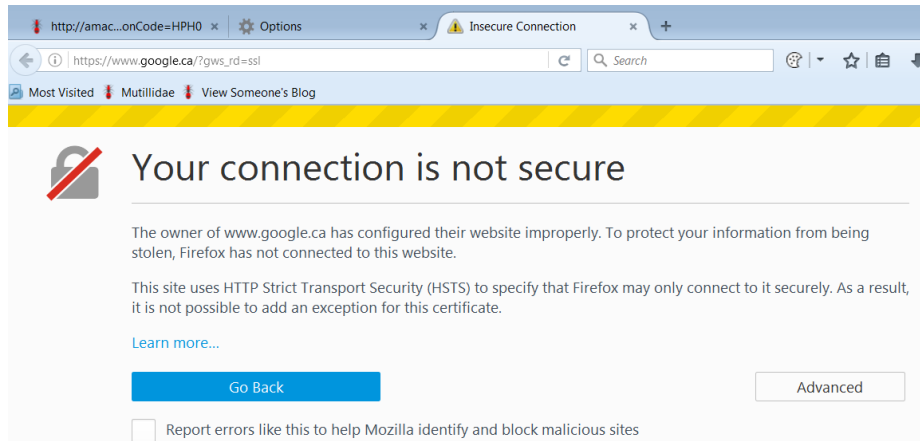
Take a screenshot showing all of the above and place it into slide 03

If you bring the Firefox window forward, you will see either "The connection has timed out" message or connecting

Click on the **"Intercept is on"** button in Burp Suite (**Proxy** tab -> **Intercept** sub-tab). This will toggle interception off.

On Windows 10

Refresh the www.google.ca page. If everything is done properly you should see a certificate error. Why?



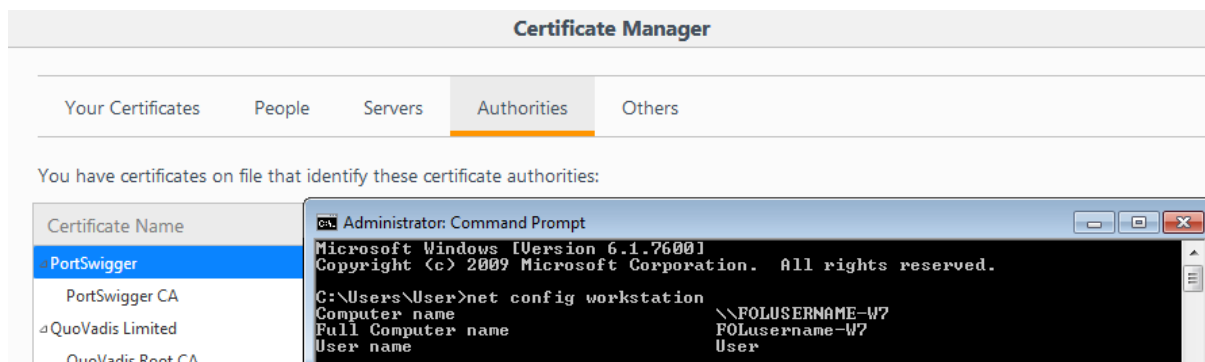
Export Burp Suite (PortSwigger) Certificate

- Navigate to `http://burp`
- Click on the CA Certificate Link and save it to your desktop
- Save the Certificate, then move it to your desktop

Install the PortSwigger Certificate

- Open FireFox menu -> **Options** -> **Privacy & Security** -> **Certificates**
 - Click on **View Certificates...** The **Certificate Manager** window should open
- Chose the **Authorities** tab and click on **Import** button and import the **cacert** certificate
- Select the option: **Trust this CA to identify websites** and click OK
- Click OK until you are back at the main Firefox page then refresh the `www.google.ca` page

Open the **Certificate Manager** window again and highlight PortSwigger CA certificate as shown below



Slide 04:

Take a screenshot showing all of the above and place it into slide 04

Part 04: Directory Traversal

On your Kali VM:

- Open Firefox and go to Mutillidae home page
- Make sure the hostname is FOLusername-uws – i.e you should see `http://folusername-uws/mutillidae`
- Reset Database to make sure your Mutillidae is set to its defaults (use the ResetDB link)
- Disable (Hide) Popup Hints if it's not done already

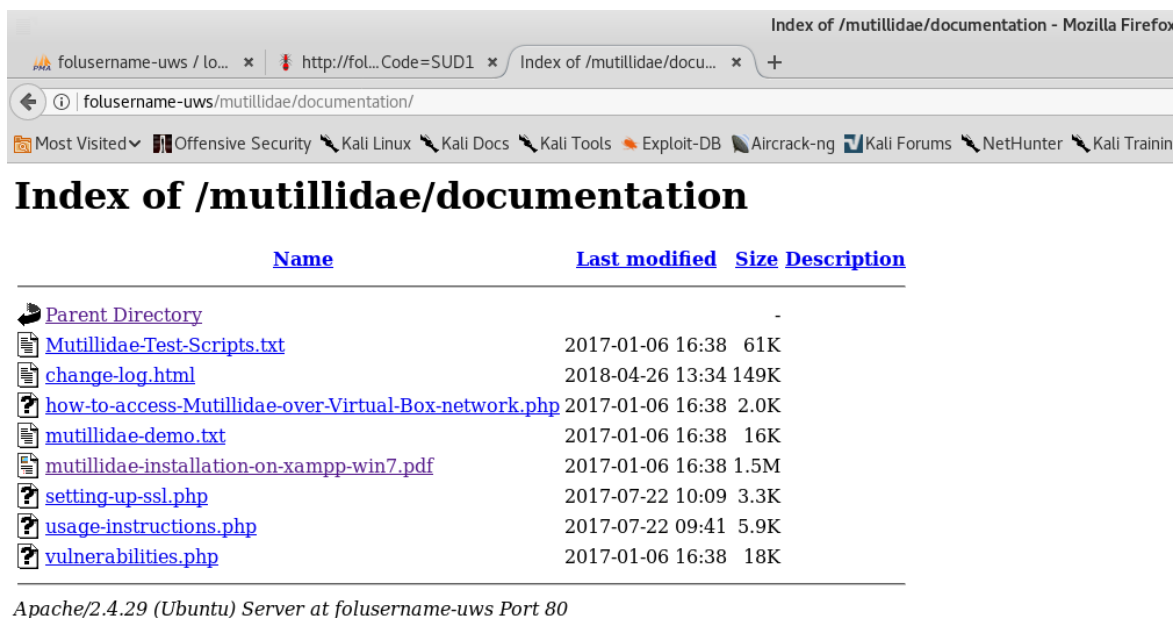
Often web applications are misconfigured.

We are going to take advantage of that fact to explore the directory structure of the Mutillidae page

Click on the **Installation Instructions: Windows 7 (PDF)** listed under the **Documentation** menu on the left. You may be prompted to save the file. Do not save the file. We are only interested in where this file is located on the server.

Check the URL for the PDF file. If you look at the URL you will see that it is located in a folder called **documentation**. Let's see what else is located in this folder.

Delete everything after **...documentation/** and hit enter. You will be presented with an index of that directory. Ideally web visitors should not be able to see directories on a web server.



| Name | Last modified | Size | Description |
|---|------------------|------|-------------|
| Parent Directory | - | - | - |
| Mutillidae-Test-Scripts.txt | 2017-01-06 16:38 | 61K | |
| change-log.html | 2018-04-26 13:34 | 149K | |
| how-to-access-Mutillidae-over-Virtual-Box-network.php | 2017-01-06 16:38 | 2.0K | |
| mutillidae-demo.txt | 2017-01-06 16:38 | 16K | |
| mutillidae-installation-on-xampp-win7.pdf | 2017-01-06 16:38 | 1.5M | |
| setting-up-ssl.php | 2017-07-22 10:09 | 3.3K | |
| usage-instructions.php | 2017-07-22 09:41 | 5.9K | |
| vulnerabilities.php | 2017-01-06 16:38 | 18K | |

Apache/2.4.29 (Ubuntu) Server at folusername-uws Port 80

Slide 05:

Take a screenshot showing all of the above and place it into slide 05

- ✓ Figure out where a list of users is stored on an Ubuntu Server
- ✓ Replace the **file:///** portion of the entry to reference that directory/file location

Highlight your FOLusername user as shown in the example below:

Validate XML

–XML Submitted–

```
<!DOCTYPE foo [ <!ENTITY testref SYSTEM [REDACTED] <somexml><message>&testref;</message></somexml>
```

–Text Content Parsed From XML–

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin messagebus:x:103:107::/nonexistent:/usr/sbin/nologin _apt:x:104:65534::/nonexistent:/usr/sbin/nologin lxd:x:105:65534::/var/lib/lxd:/bin/false uidd:x:106:110::/run/uidd:/usr/sbin/nologin dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin pollinate:x:109:1::/var/cache/pollinate:/bin/false sshd:x:110:65534::/run/sshd:/usr/sbin/nologin folusername:x:1000:1004:FOLusername:/home/folusername:/bin/bash mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false ftp:x:112:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
```

Slide 06:

Take a screenshot showing all of the above and place it into slide 06

***** Shutdown the VM and take a snapshot called After Lab 04 *****