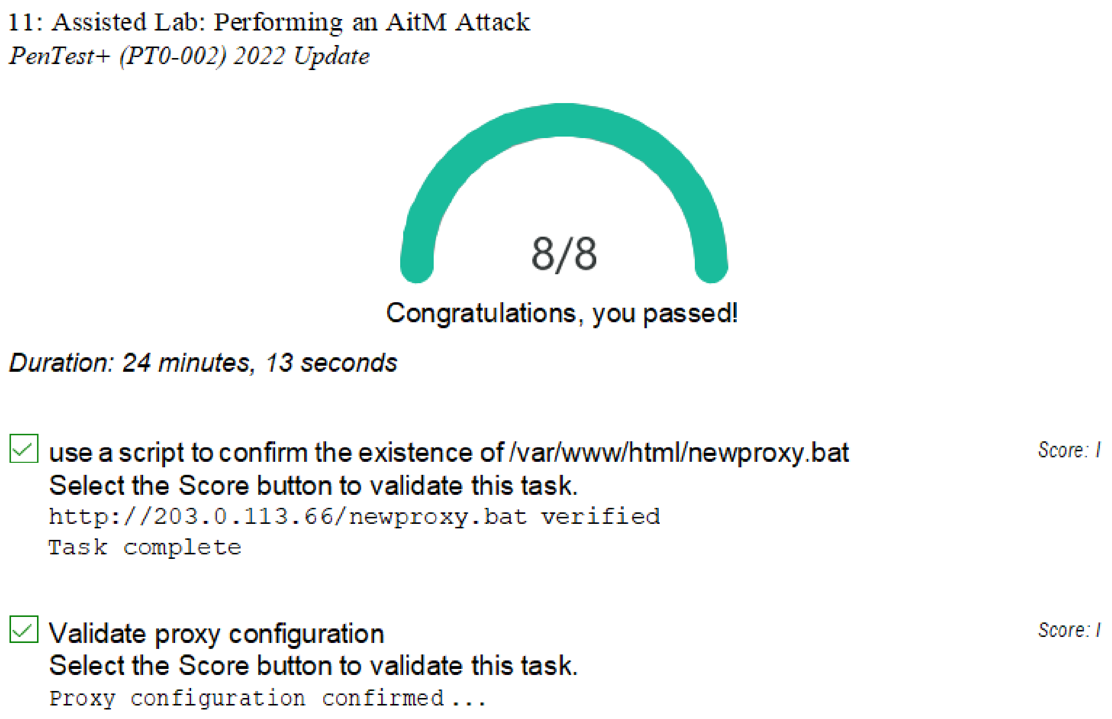
# WEEK 6 ASSIGNMENT



11: Assisted Lab: Performing an AitM Attack

*PenTest+ (PT0-002) 2022 Update*

8/8

Congratulations, you passed!

*Duration: 24 minutes, 13 seconds*

☑ use a script to confirm the existence of /var/www/html/newproxy.bat *Score: 1*

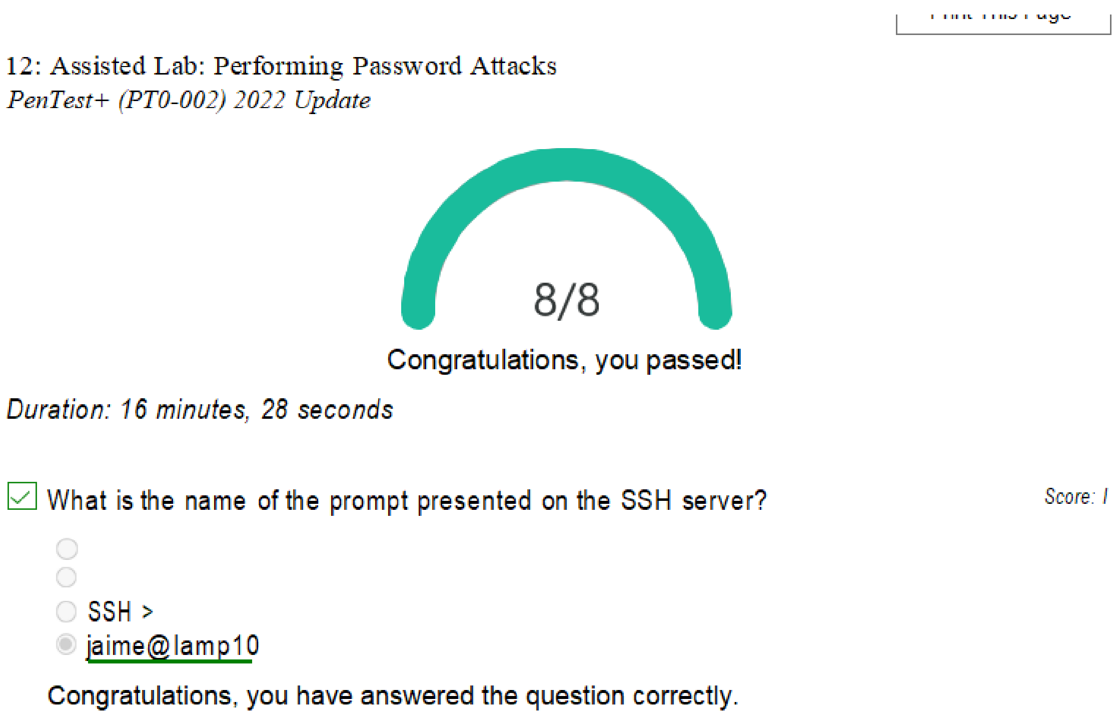
Select the Score button to validate this task.

```
http://203.0.113.66/newproxy.bat verified
Task complete
```

☑ Validate proxy configuration *Score: 1*

Select the Score button to validate this task.

```
Proxy configuration confirmed...
```



12: Assisted Lab: Performing Password Attacks

*PenTest+ (PT0-002) 2022 Update*

8/8

Congratulations, you passed!

*Duration: 16 minutes, 28 seconds*

☑ What is the name of the prompt presented on the SSH server? *Score: 1*

○

○

○ SSH >

● jaime@lamp10

Congratulations, you have answered the question correctly.

1) **Have you had any experience with Burp Suite before?**

   **What were the use cases if so?**

Certainly, I do possess experience with Burp Suite. Specifically, I utilized it in a web application security testing course where I was charged with scrutinizing vulnerabilities in a web application. Burp Suite presented a vast number of use cases, one of which entailed intercepting and modifying HTTP requests and responses exchanged between the browser and the web application. This enabled me to identify potential security flaws such as SQL injection and cross-site scripting (XSS) vulnerabilities in the web application.

Moreover, another use case of Burp Suite encompassed the manual and automated security testing of the web application. This involved utilizing the diverse range of tools and modules available within Burp Suite, including the Scanner and Intruder tools, to expose and exploit potential vulnerabilities in the web application.

Overall, my experience with Burp Suite was immensely enlightening and contributed greatly to my understanding of web application security testing. I perceived Burp Suite as an incredibly potent and versatile tool that can effectively identify and resolve security issues in web applications.

2) **Why do you think Burp Suite is a pen-testers favorite tool for web application hacking?**

Burp Suite is highly favored by pen-testers for web application hacking due to its versatility, flexibility, and automation capabilities. Its comprehensive range of tools and modules enable pen-testers to detect and exploit vulnerabilities such as SQL injection and cross-site scripting efficiently. Moreover, its user-friendly interface and detailed reporting capabilities allow pen-testers to easily communicate their findings to stakeholders. All these features make Burp Suite an indispensable tool for pen-testers, especially when it comes to web application security testing.

3) **What type off password attacks can John the Ripper perform?**

   **What are the 3 types of password hashes John the Ripper can crack?**

   **Do you think there is value in using generic word lists to crack passwords or would you choose to create your own?**

John the Ripper, the ubiquitous password cracking tool, boasts a smorgasbord of tactics to infiltrate even the most impregnable of passwords. These tactics include the dictionary attack, wherein John employs a vast list of commonly used words and phrases to discern the password; the brute-force attack, in which John endeavours to test every conceivable combination of characters to breach the password; and the hybrid attack, which sees John merge the dictionary and brute-force attacks by appending numbers, symbols, or other characters to the words or phrases in the dictionary. What's more, John the Ripper can crack a plethora of password hashes, including DES-based, MD5-based, and Blowfish-based password hashes, which utilize the Data Encryption Standard, MD5 hashing algorithm, and Blowfish algorithm, respectively, for encryption.

When it comes to cracking passwords using word lists, one can derive value from generic word lists to begin with, but creating a bespoke word list can yield even greater success. A custom word list enables one to incorporate words and phrases specific to the target audience or organization, thus heightening the likelihood of cracking the password. Additionally, it allows one to introduce commonly used passwords or phrases, misspellings, or other variations to the word list to augment the probability of success. However, it's vital to bear in mind that using password cracking tools to gain unauthorized access to someone's account is both illegal and unethical.