



A Toolbox for Ethical Hacking

Model Answer

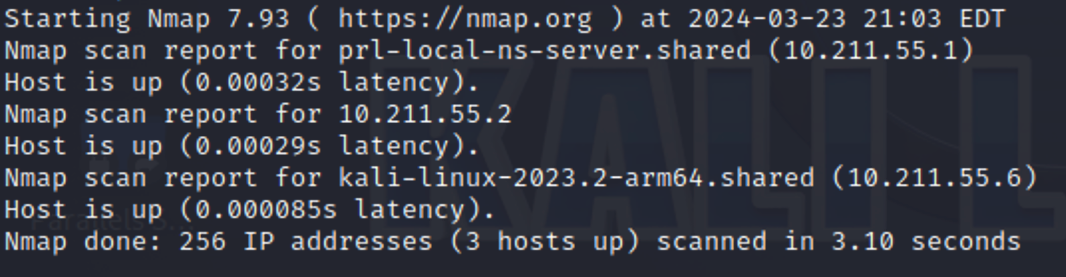
[](http://www.hyperiondev.com/portal/)

# Auto-graded task

1. Mapping out the network topology:
2. The correct tool for this task is **Nmap**.
3. To perform a comprehensive scan of your local network and identify active hosts, you can use the following command:

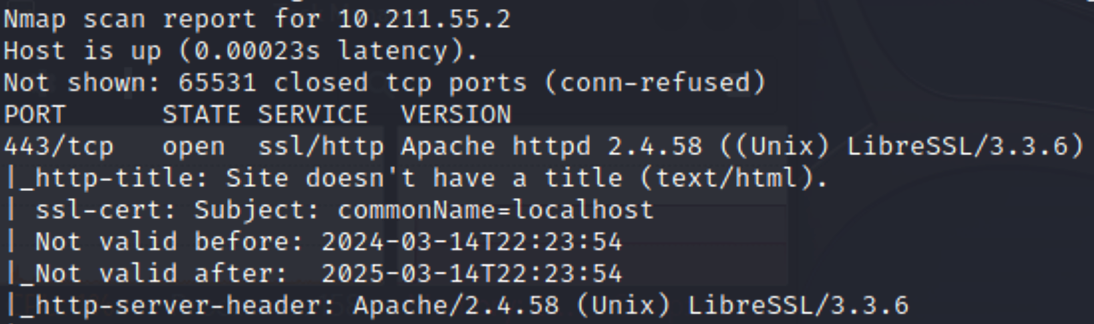
| nmap -sn 10.211.55.0/24 |
| --- |

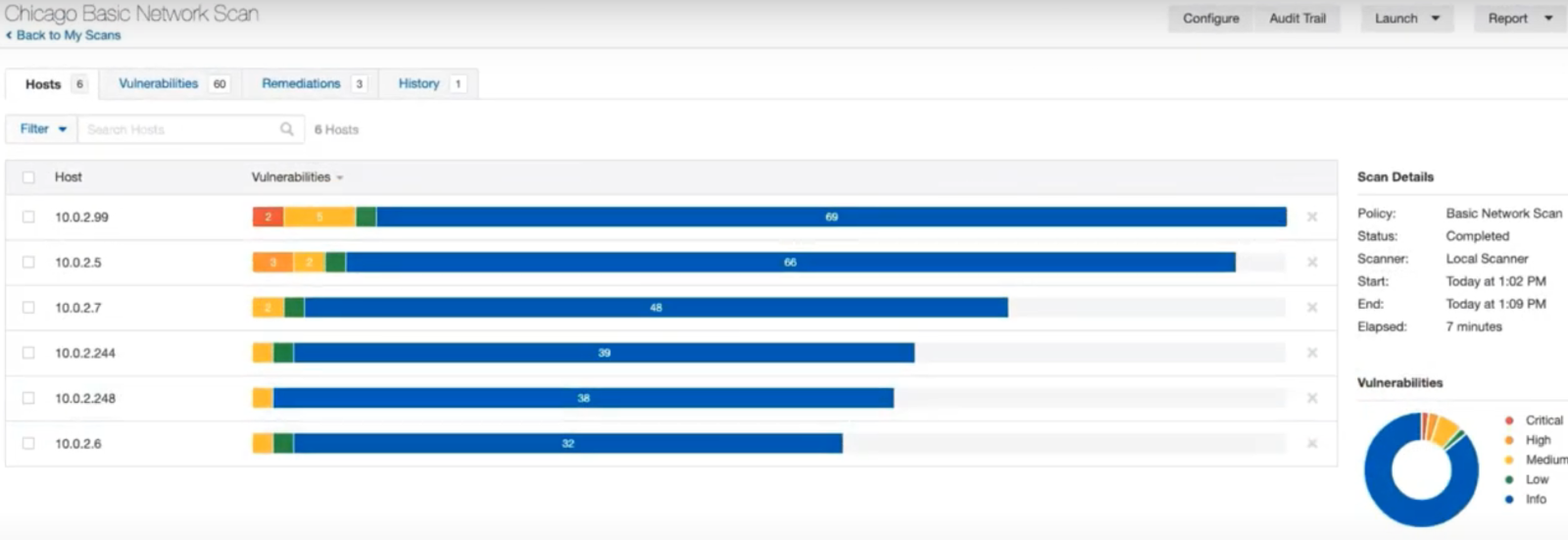
In this command, the target IP address range 10.211.55.0/24 specifies the network address and the subnet mask. **Replace this with the appropriate IP address range for your local network.** Here is a sample output:

To identify open ports and services running on those ports, use the following command:

| nmap -p- -A -T4 10.211.55.2 |
| --- |

Replace this address 10.211.55.2 with your own IP address. Here is a sample output showing a poorly configured web server:



1. Vulnerability scan:
2. The correct tool for the vulnerability scan is **Nessus**.
3. Here is a sample screenshot of a basic scan of a local network:

Notice that the scan provides results for each host, with the criticality of each discovered vulnerability clearly marked. Continue to investigate your results by clicking on each host’s results to obtain more information about each vulnerability.

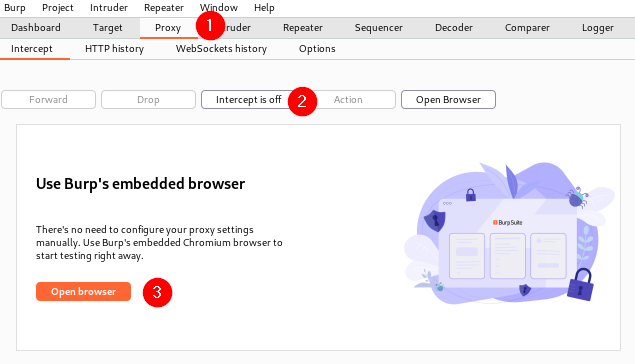
1. Numbers in each category (critical, high, medium, and low) will depend on the individual network scanned. The criticality numbers are shown in the scan results.

# Optional task

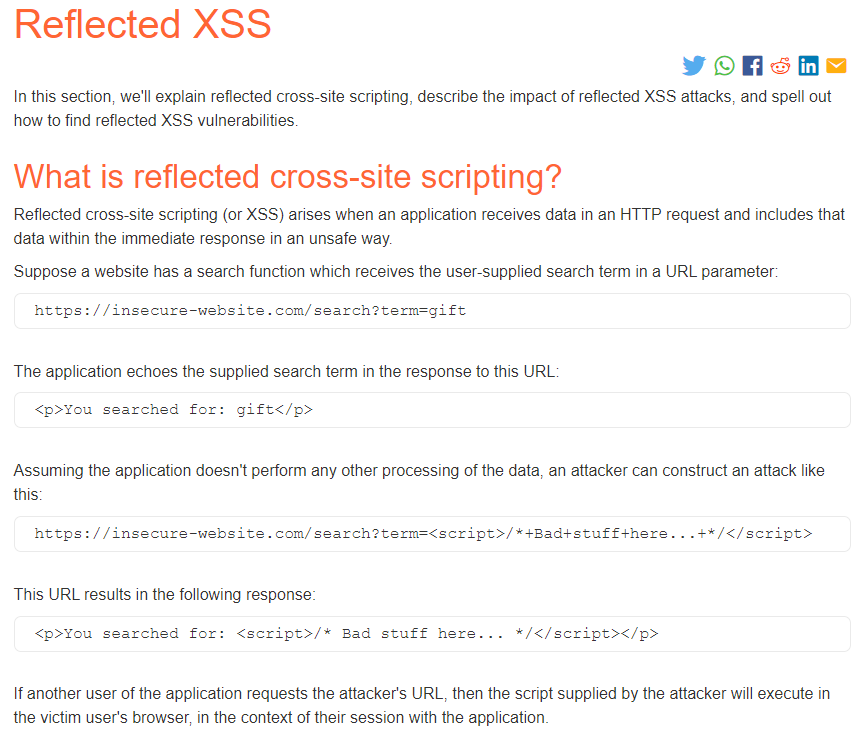
1. Go to Kali Linux and open Burp Suite.
2. Remember to update Burp suite before using it

| sudo apt upgrade burpsuite |
| --- |

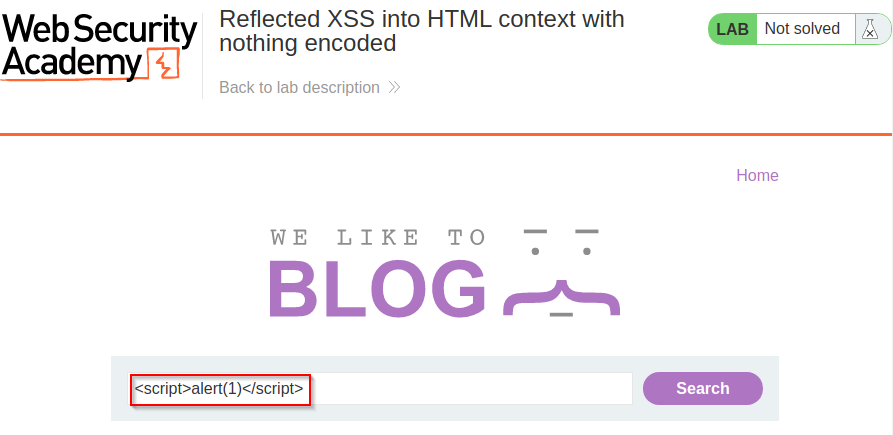
1. On Burp Suite, locate the “Proxy” tab and ensure the intercept is off, then open the embedded browser.



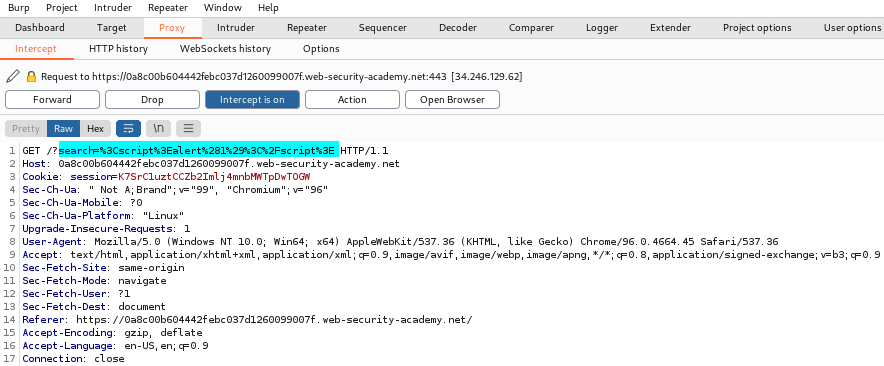
1. Please visit [**Reflected XSS**](https://portswigger.net/web-security/cross-site-scripting/reflected) to read up on the topic.



1. After reading about reflected XSS, log in to your Burp Suite account and complete the [**lab on reflected XSS**](https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded).
2. Turn on the intercept and refresh the webpage once you have copied and pasted <script>alert(1)</script> into the blog search box.

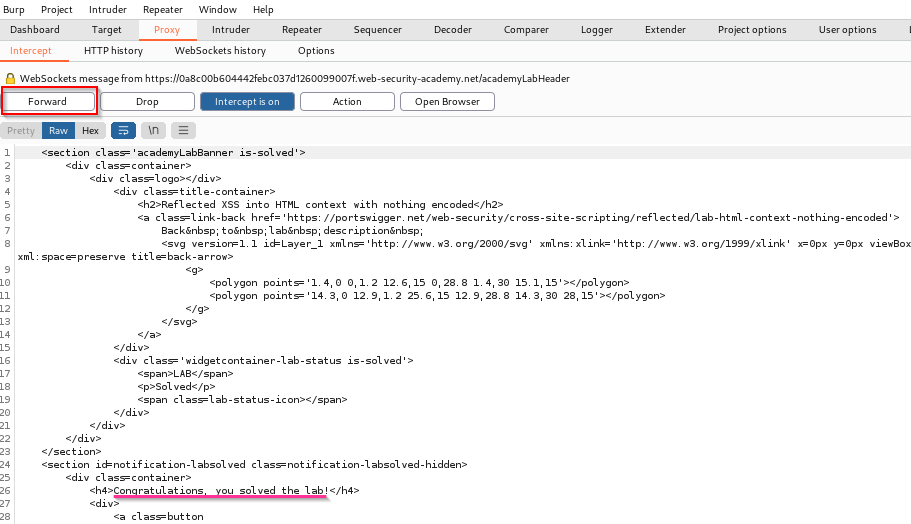


1. Look at the response captured by Burp Suite.



1. Click on “Forward” and check the responses on both Burp Suite and the lab (example screenshots on the next page).

**Burp Suite:**



**Lab:**

