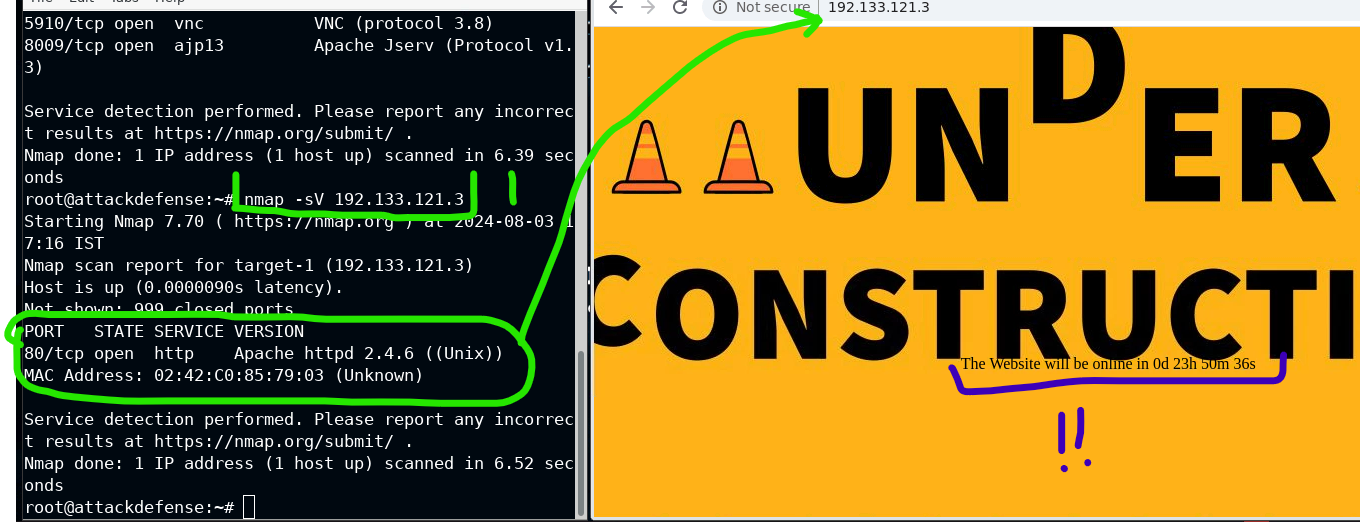
Nmap service version scan on the target reveals port 80 and apache httpd 2.4.6 running some kind of unix system

With port 80 running, this means a browser can open the IP address, as shown in the page.

Oddly enough, there’s an active timer for the website, counting down how long until it will be online…



Looking into the page source, we find a cgi script. The pathing is straightforward, allowing up to simply add /gettime.cgi to the end of the url address to witness the calculation/text all on its own.

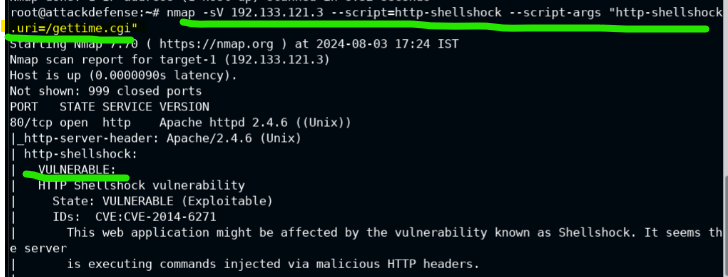
Cgi scripts like this could help us infiltrate.



The shellshock script can take advantage of http uri things. In this case, gettime.cgi will fulfill the uri parameter, as shown in the highlight example below.

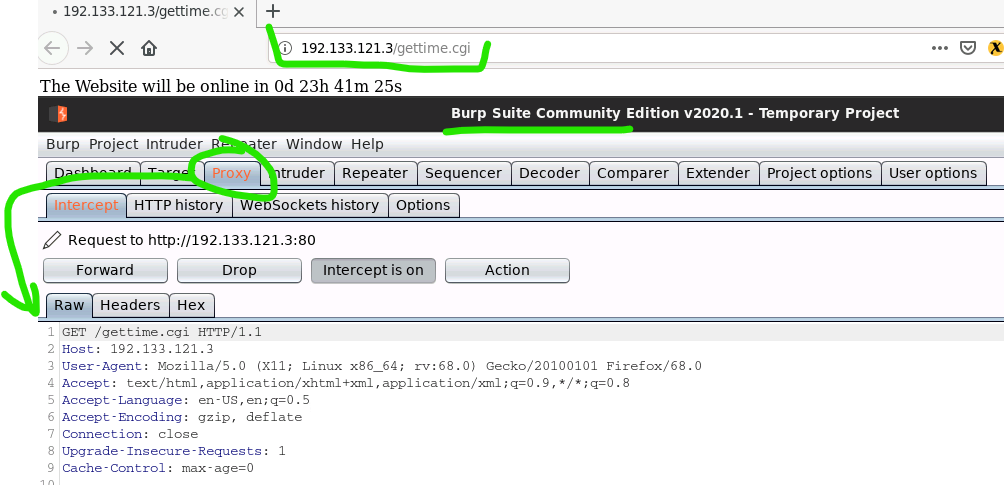
Command: nmap -V 192.133.121.3 –script=http-shellshock –script-args “http-shellshock.uri=/gettime.cgi”

This only scans for the shellshock vulnerability and won’t be a can-opener to the process at hand. It should maintain your concealment.



Switching over to burpsuite, we set up the proxy intercept and navigate to the cgi indicated in the url.

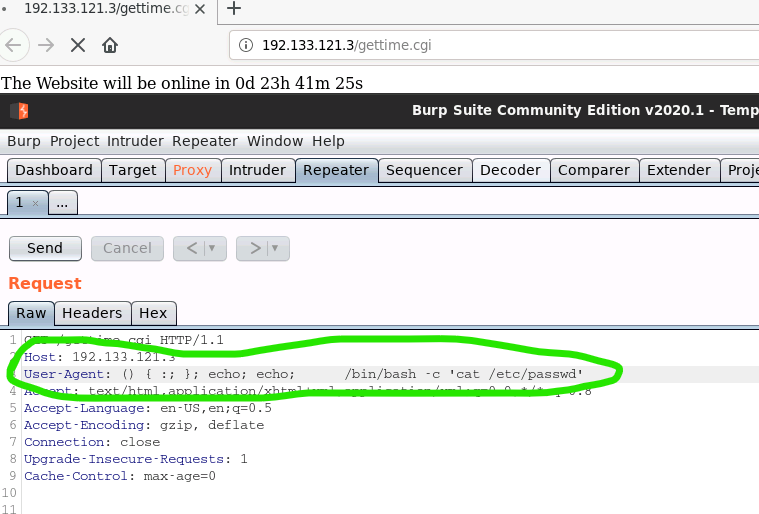
This gives us access to the user agent being used on port 80; User agents let the service know what kind of device is accessing it. In some of the spiders I’ve made, I’ve had to spoof user agents to make requests look as if they are coming from different devices to lower suspicion. In this case, we’re going to alter the user agent as a means to an end for command injection, which is a whole different ball game.



Below, showing command injection for

Payload in user-agents:

() { :; } ; echo; echo; /bin/bash -c ‘cat /etc/passwd’



This gets us the contents of the passwd file, if we can grab it on the host.

This is very similar to an sql injection in terms of reaching out to another system and getting info through a type of command injection. Only, we’re working with a server instead of a database… I think. The teacher wasn’t too clear in their lecture on this.

That’s all for this lab. Other code execution is out of scope, since this is more about methodology in general.