**Unit 7 Scanning Activity**

<http://ehealth-env.eba-d6shft2m.us-east-1.elasticbeanstalk.com/>

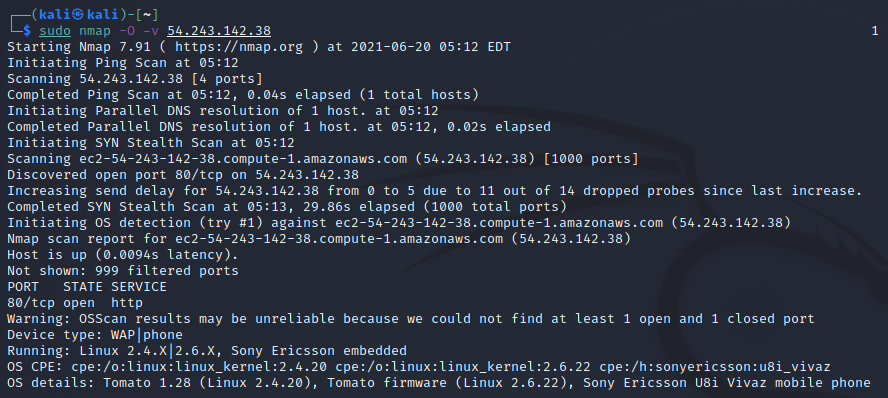
54.243.142.38

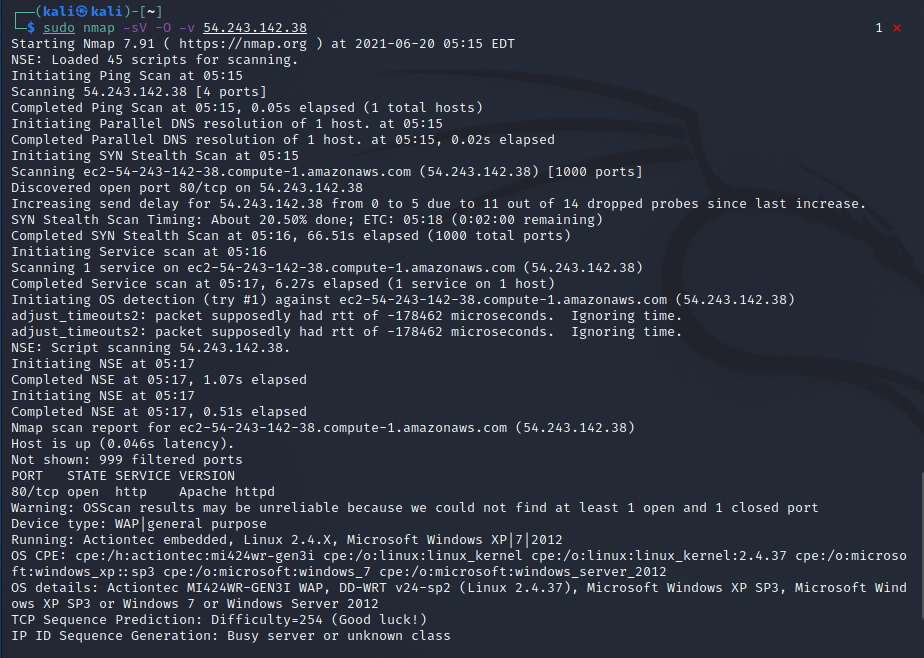
<http://teamnebula.us-east-1.elasticbeanstalk.com/>

107.20.143.245

**What Operating System does the website utilise?**

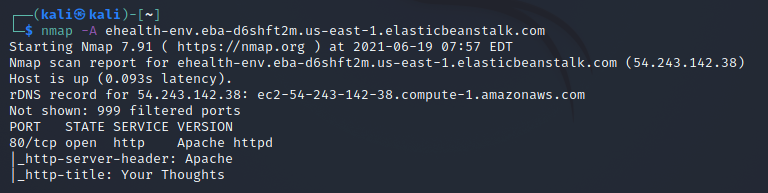
Several inconsistent results across different internet connections and commands due to non-ideal conditions but the most common guess appears to be Linux 2.4.20.

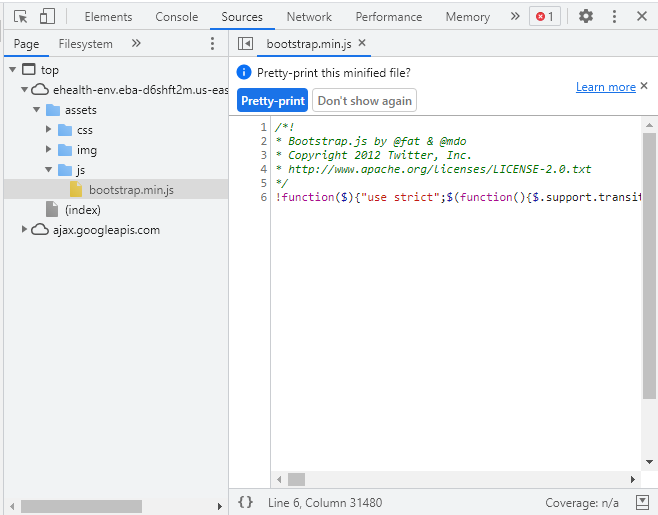




**What web server software is it running?**

Apache httpd v2.0





**Is it running a CMS (Wordpress, Drupal, etc?)**

No – webpage source inspected.

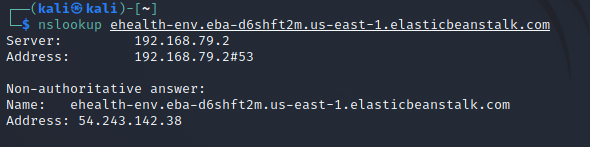
**What protection does it have (CDN, Proxy, Firewall?)**

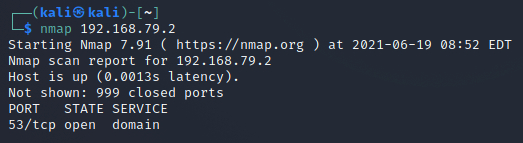
Unknown – traceroute suggests some protection on AWS but not specified.

**Where is it hosted?**

rDNS record: ec2-54-243-142-38.compute-1.amazonaws.com

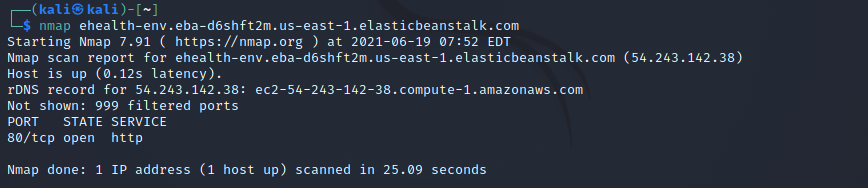
Server: 192.168.79.2

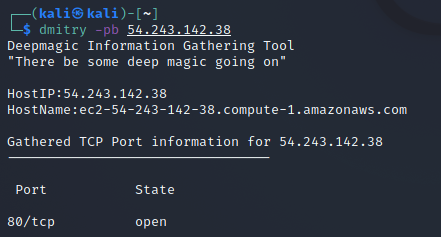


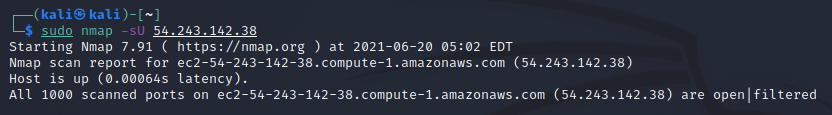


**Does it have any open ports?**

Yes - Port 80

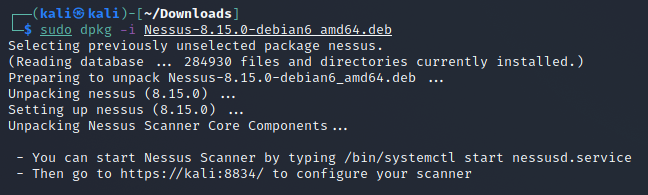


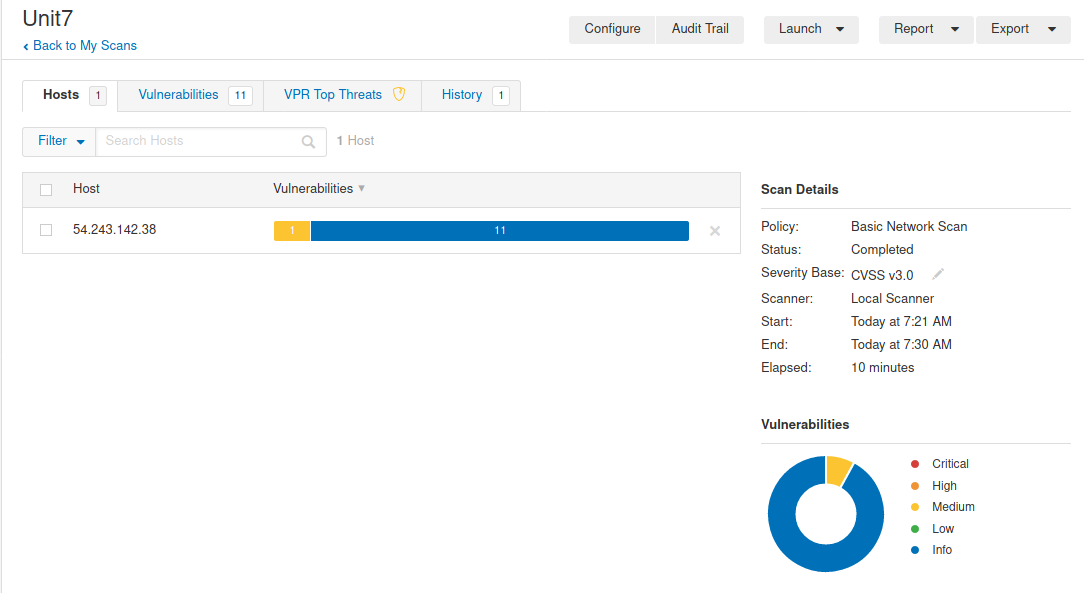




**Does the site have any known vulnerabilities?**

CVE-2001-1446 – according to Nessus Essentials basic network scan.

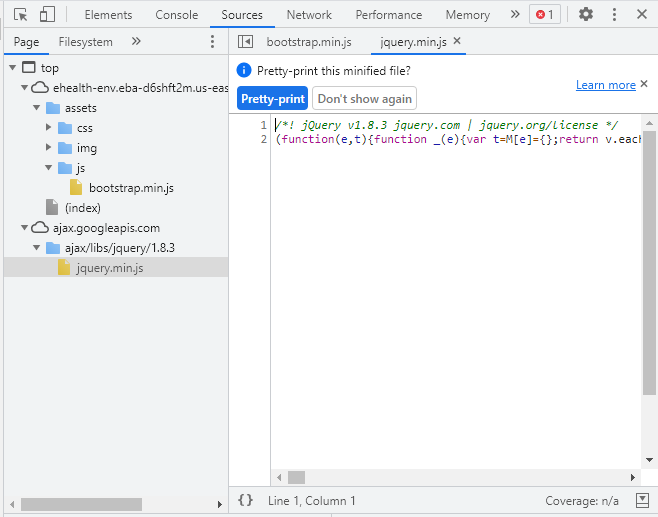


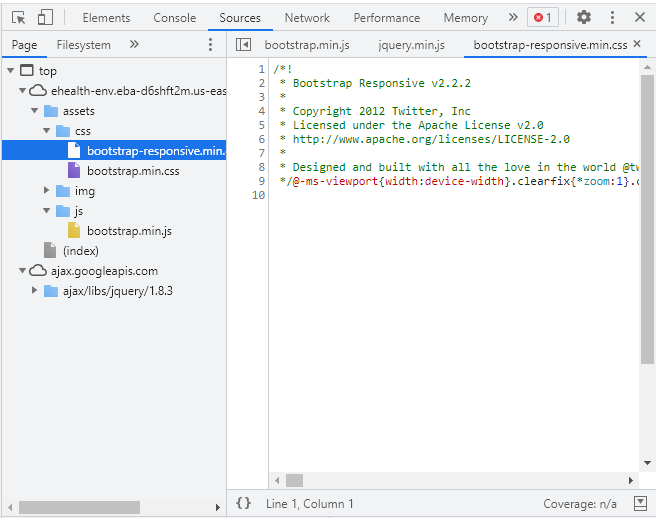


**What versions of software is it using? Are these patched so that they are up to date?**

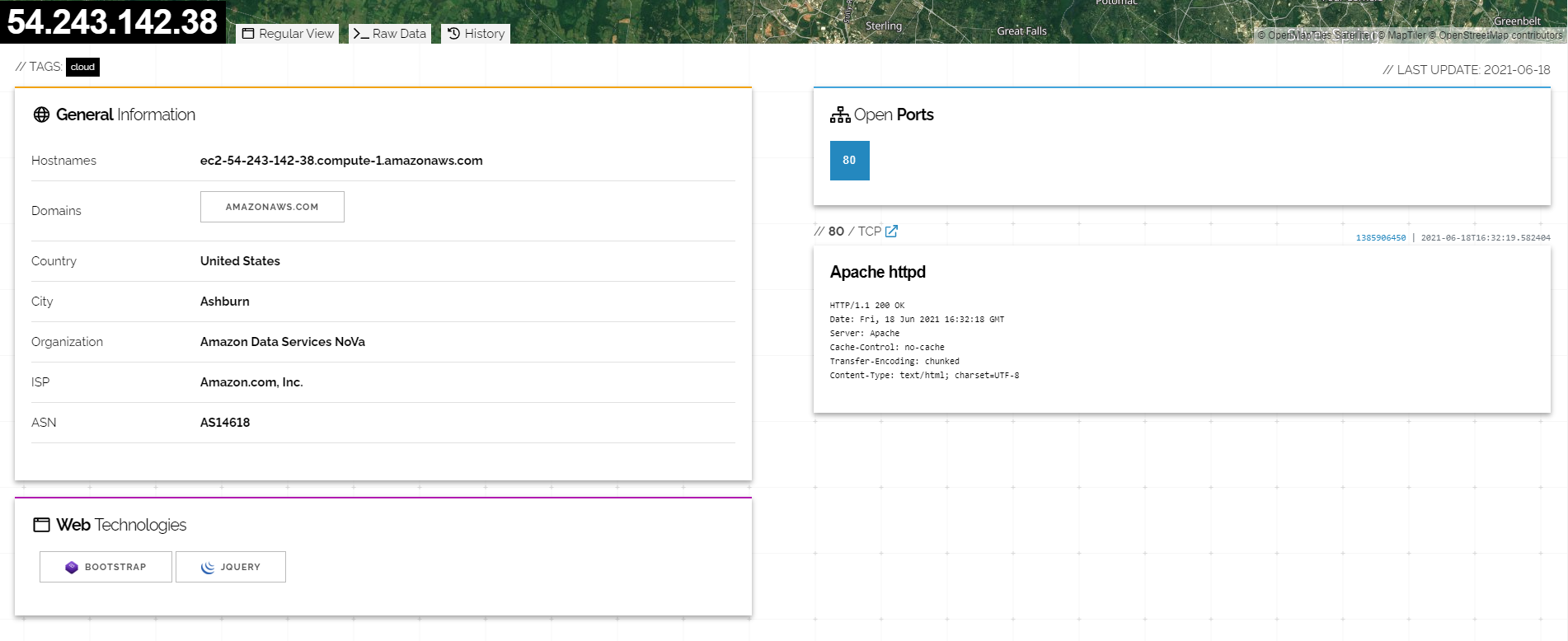
jQuery v1.8.3

Bootstrap Responsive v2.2.2





**Other Sources**



Bibliography:

<https://serpstat.com/blog/how-to-detect-which-cms-a-website-is-using-8-easy-ways/>

Bhatt, D. (2018) Modern Day Penetration Testing Distribution Open Source Platform - Kali Linux - Study Paper. *International Journal of Scientific & Technology Research* 7(4): 233-237.

Bhingardeve, N. & Franklin, S. (2018) A Comparison Study of Open Source Penetration Testing Tools. *International Journal of Trend in Scientific Research and Development* 2(4): 2595-2597.

Hertzog, R., O'Gorman, J. and Aharoni, M. (2017) *Kali Linux Revealed*. 1st ed. Cornelius: Offset Press.

Kaur, G., Kaur, N. (2017) Penetration Testing - Reconnaissance with NMAP Tool. *International Journal of Advanced Research in Computer Science* 8(3): 844-846.

McNab, C. (2004) *Network Security Assessment: Know Your Network*. Sebastopol, CA: O’Reilly Media.

<https://nmap.org/>

<https://www.cloudns.net/blog/traceroute-command-tracert/>

<https://linuxhint.com/nessus_installation_kali_linux/>