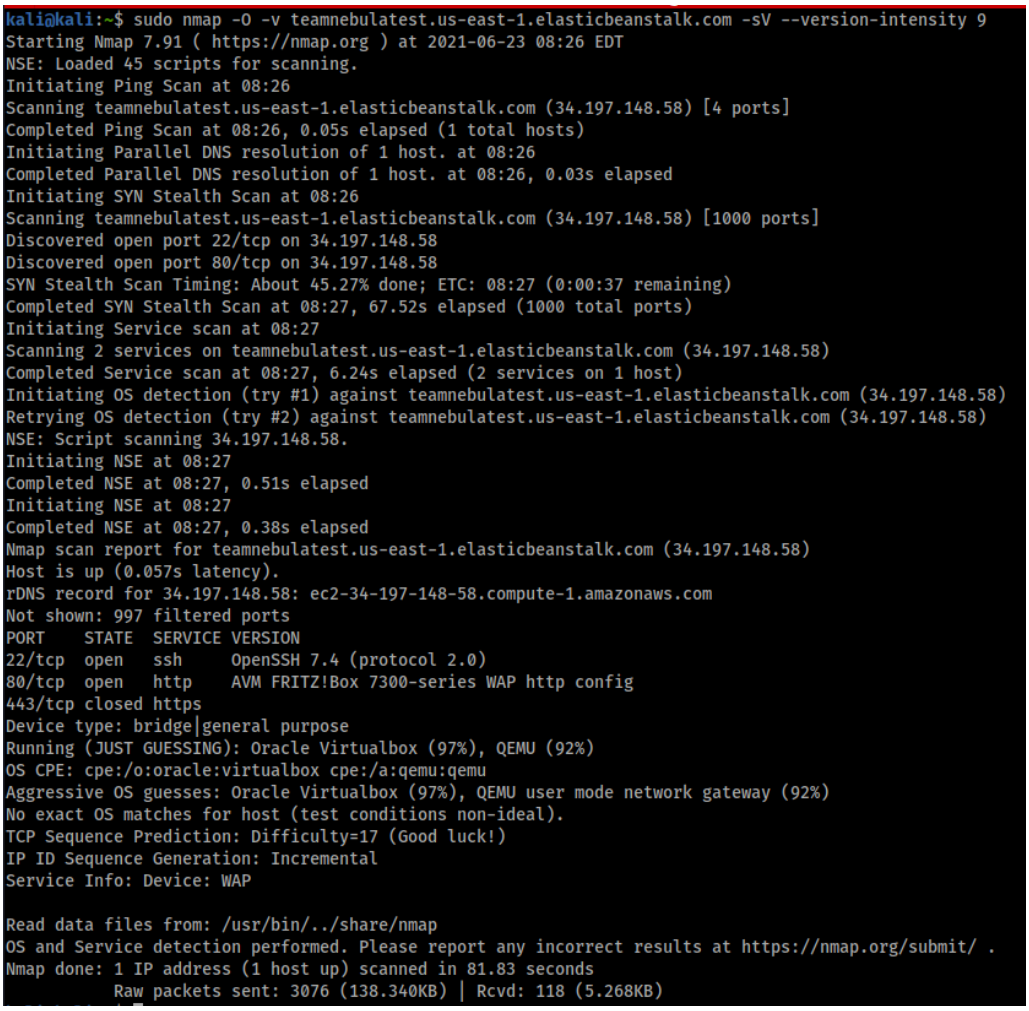
1 Inhaltsverzeichnis

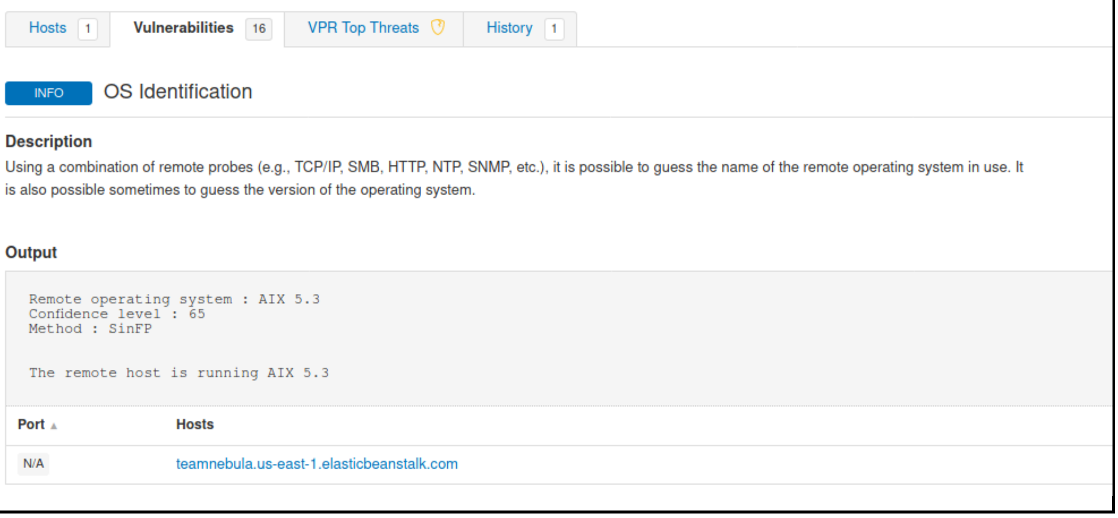
Author: Jan Küfner

2 What Operating System does the web site utilise?

<table>
<tr><td><b>Answer</b></td><td><b>Oracle VirtualBox</b></td></tr>
<tr><td>Tool</td><td>Nmap, Nessus Essentials</td></tr>
<tr><td>Proof of Concept</td><td>



```
kali@kali:~$ sudo nmap -O -v teamnebulatest.us-east-1.elasticbeanstalk.com -sV --version-intensity 9
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-23 08:26 EDT
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 08:26
Scanning teamnebulatest.us-east-1.elasticbeanstalk.com (34.197.148.58) [4 ports]
Completed Ping Scan at 08:26, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:26
Completed Parallel DNS resolution of 1 host. at 08:26, 0.03s elapsed
Initiating SYN Stealth Scan at 08:26
Scanning teamnebulatest.us-east-1.elasticbeanstalk.com (34.197.148.58) [1000 ports]
Discovered open port 22/tcp on 34.197.148.58
Discovered open port 80/tcp on 34.197.148.58
SYN Stealth Scan Timing: About 45.27% done; ETC: 08:27 (0:00:37 remaining)
Completed SYN Stealth Scan at 08:27, 67.52s elapsed (1000 total ports)
Initiating Service scan at 08:27
Scanning 2 services on teamnebulatest.us-east-1.elasticbeanstalk.com (34.197.148.58)
Completed Service scan at 08:27, 6.24s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against teamnebulatest.us-east-1.elasticbeanstalk.com (34.197.148.58)
Retrying OS detection (try #2) against teamnebulatest.us-east-1.elasticbeanstalk.com (34.197.148.58)
NSE: Script scanning 34.197.148.58.
Initiating NSE at 08:27
Completed NSE at 08:27, 0.51s elapsed
Initiating NSE at 08:27
Completed NSE at 08:27, 0.38s elapsed
Nmap scan report for teamnebulatest.us-east-1.elasticbeanstalk.com (34.197.148.58)
Host is up (0.057s latency).
rDNS record for 34.197.148.58: ec2-34-197-148-58.compute-1.amazonaws.com
Not shown: 997 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 7.4 (protocol 2.0)
80/tcp  open   http    AVM FRITZ!Box 7300-series WAP http config
443/tcp closed https
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Device: WAP

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.83 seconds
           Raw packets sent: 3076 (138.340KB) | Rcvd: 118 (5.268KB)
```



INFO OS Identification

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Output

```
Remote operating system : AIX 5.3
Confidence level : 65
Method : SinFP


The remote host is running AIX 5.3
```

Port	Hosts
N/A	teamnebula.us-east-1.elasticbeanstalk.com

</td></tr>
</table>

3 What web server software is it running?

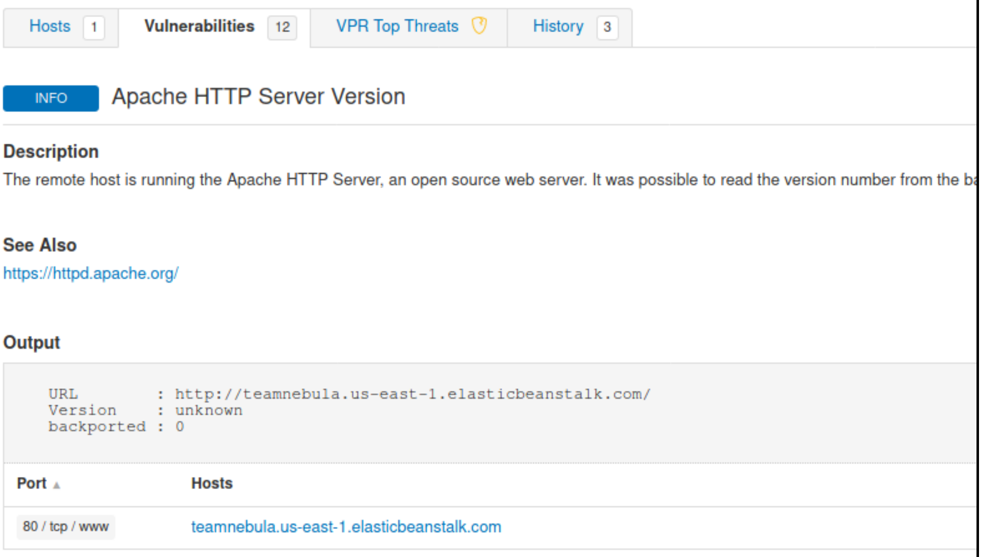
Answer

- **Apache (Version unknown)**
- **Jquery 1.8.3**
- **Bootstrap v2.2.2**

Tool

Nessus Essentials, Burpsuite Community Edition, visual code inspection

Proof of Concept



Apache HTTP Server Version

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the ba

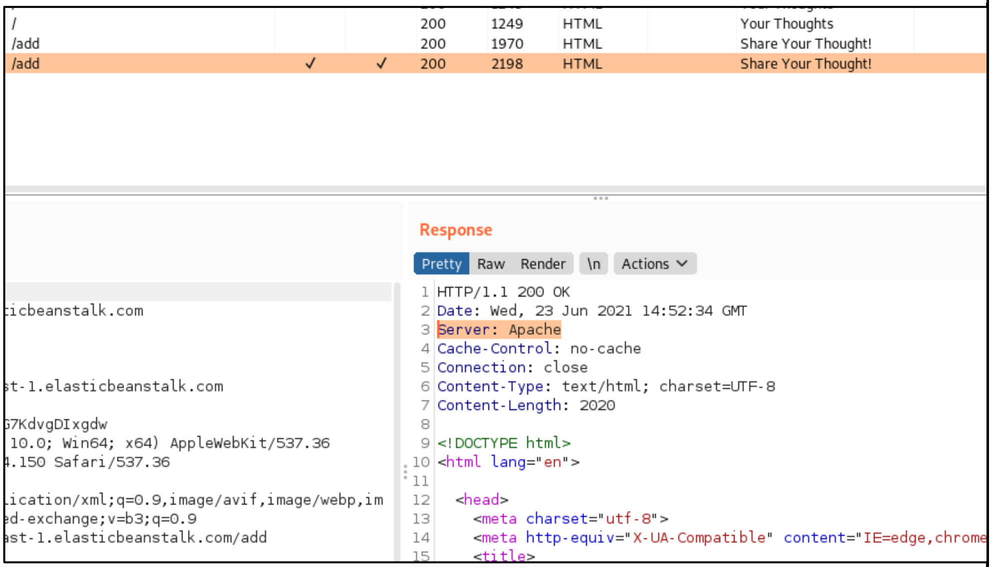
See Also

https://httpd.apache.org/

Output

```
URL        : http://teamnebula.us-east-1.elasticbeanstalk.com/
Version    : unknown
backported : 0
```

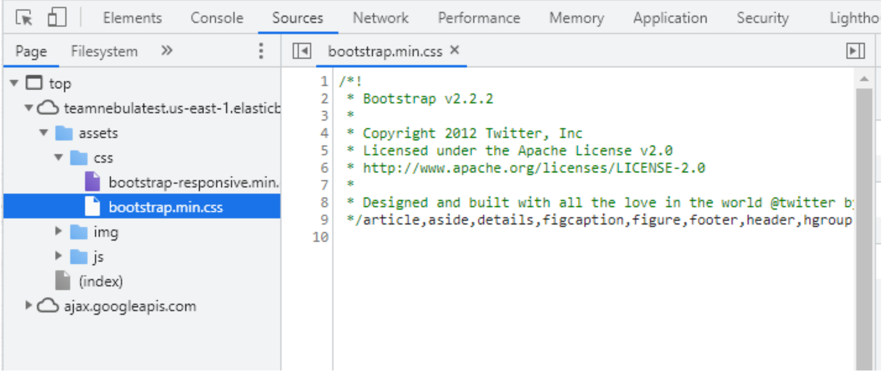
Port	Hosts
80 / tcp / www	teamnebula.us-east-1.elasticbeanstalk.com



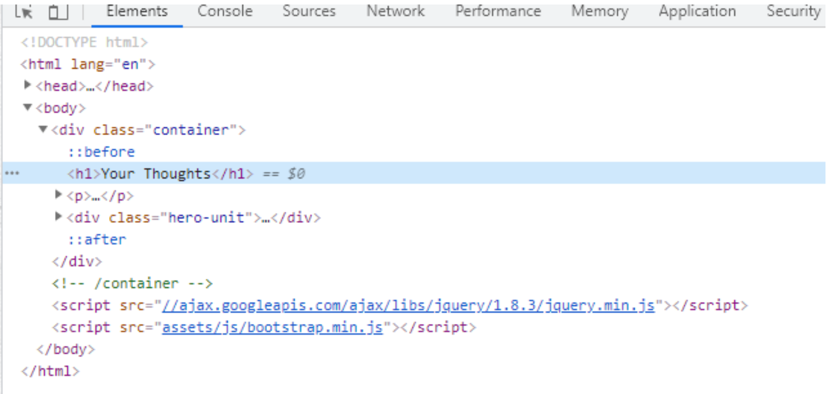
/			200	1249	HTML	Your Thoughts
/add			200	1970	HTML	Share Your Thought!
/add	✓	✓	200	2198	HTML	Share Your Thought!

```
icbeanstalk.com

st-1.elasticbeanstalk.com

57KdvgDIxgdw
 10.0; Win64; x64) AppleWebKit/537.36
4.150 Safari/537.36

ication/xml;q=0.9,image/avif,image/webp,im
ed-exchange;v=b3;q=0.9
ast-1.elasticbeanstalk.com/add
```

```
HTTP/1.1 200 OK
Date: Wed, 23 Jun 2021 14:52:34 GMT
Server: Apache
Cache-Control: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 2020

<!DOCTYPE html>
<html lang="en">

  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome
    <title>
```



```
/*!
 * Bootstrap v2.2.2
 *
 * Copyright 2012 Twitter, Inc
 * Licensed under the Apache License v2.0
 * http://www.apache.org/licenses/LICENSE-2.0
 *
 * Designed and built with all the love in the world @twitter b
 */article,aside,details,figcaption,figure,footer,header,hgroup
```

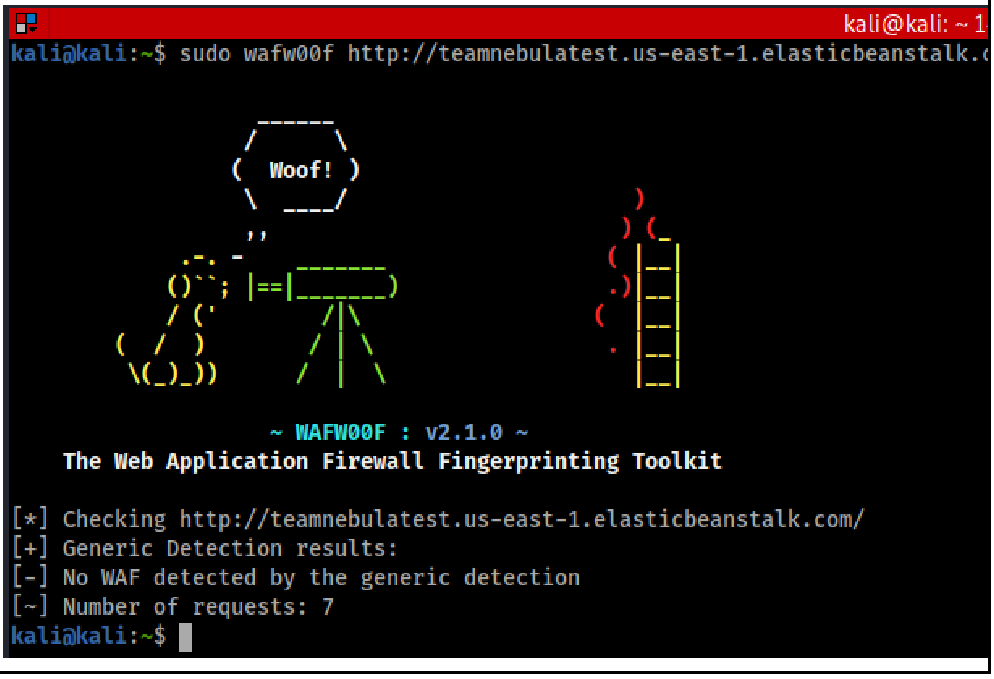
	

```
<!DOCTYPE html>
<html lang="en">
▶<head>…</head>
▼<body>
  ▼<div class="container">
      ::before
...   <h1>Your Thoughts</h1> == $0
    ▶<p>…</p>
    ▶<div class="hero-unit">…</div>
      ::after
    </div>
    <!-- /container -->
    <script src="//ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js"></script>
    <script src="assets/js/bootstrap.min.js"></script>
  </body>
</html>
```

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

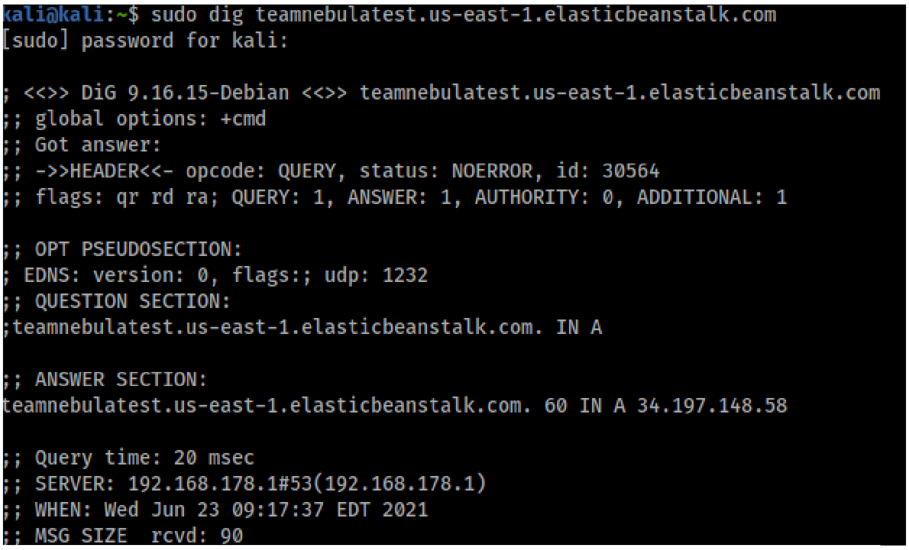
Answer	**Non detected**
Tool	Code inspection (BlindElephant not used, though)
Proof of Concept	NA

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

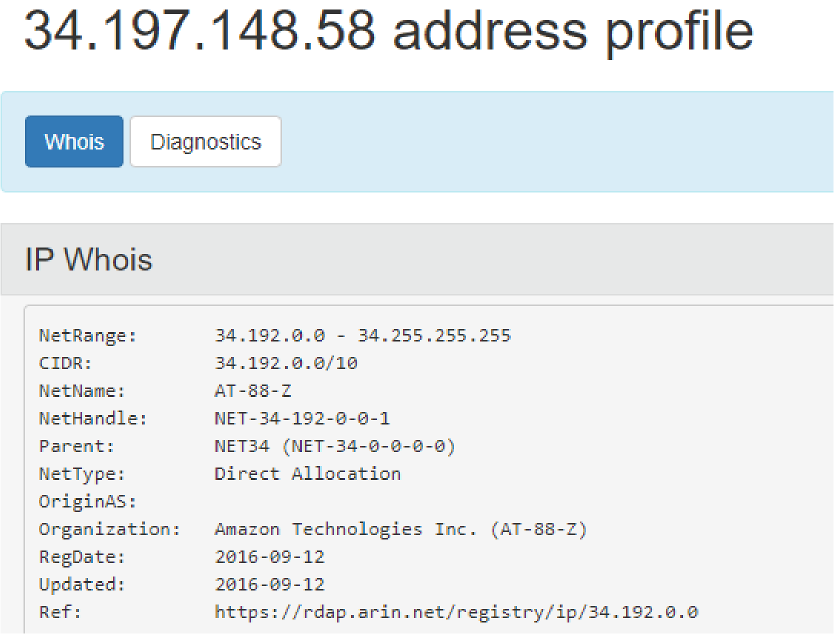
Answer	**CDN: yes, since it is an Amazon server (see chapter 6 for proof of concept) the target content is however currently only cached on one AWS server.** **Proxy: a CDN typically consists of various proxies, so yes. Also our TCP traceroute, conducted in the first scan, did reveal AWS proxies.** **WAF: none detected**
Tool	Wafw00f
Proof of Concept	 kali@kali: ~ 1 kali@kali:~$ sudo wafw00f http://teamnebulatest.us-east-1.elasticbeanstalk.c Woof! ~ WAFW00F : v2.1.0 ~ The Web Application Firewall Fingerprinting Toolkit [*] Checking http://teamnebulatest.us-east-1.elasticbeanstalk.com/ [+] Generic Detection results: [-] No WAF detected by the generic detection [~] Number of requests: 7 kali@kali:~$

6 Where is it hosted?

<table>
<tr><td><b>Answer</b></td><td><b>IP: 34.197.148.58</b>
<b>OrgName: Amazon Technologies Inc.</b></td></tr>
<tr><td>Tool</td><td>Dig, https://who.is/</td></tr>
<tr><td>Proof of Concept</td><td>



```
kali@kali:~$ sudo dig teamnebulatest.us-east-1.elasticbeanstalk.com
[sudo] password for kali:

; <<>> DiG 9.16.15-Debian <<>> teamnebulatest.us-east-1.elasticbeanstalk.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30564
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;teamnebulatest.us-east-1.elasticbeanstalk.com. IN A

;; ANSWER SECTION:
teamnebulatest.us-east-1.elasticbeanstalk.com. 60 IN A 34.197.148.58

;; Query time: 20 msec
;; SERVER: 192.168.178.1#53(192.168.178.1)
;; WHEN: Wed Jun 23 09:17:37 EDT 2021
;; MSG SIZE  rcvd: 90
```



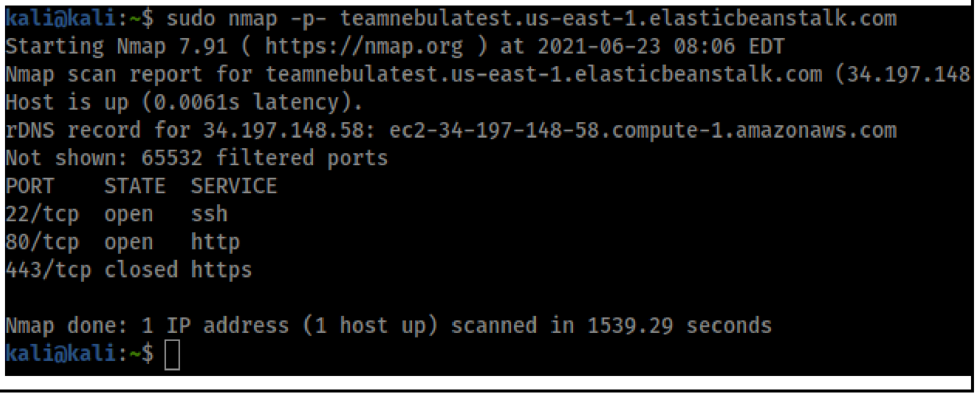
34.197.148.58 address profile

IP Whois

```
NetRange:       34.192.0.0 - 34.255.255.255
CIDR:           34.192.0.0/10
NetName:        AT-88-Z
NetHandle:      NET-34-192-0-0-1
Parent:         NET34 (NET-34-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        2016-09-12
Updated:        2016-09-12
Ref:            https://rdap.arin.net/registry/ip/34.192.0.0
```

</td></tr>
</table>

7 Does it have any open ports?

Answer	**open ports are as following:** **22/tcp open ssh** **80/tcp open http** **443/tcp closed https**
Tool	nmap
Proof of Concept	

```
kali@kali:~$ sudo nmap -p- teamnebulatest.us-east-1.elasticbeanstalk.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-23 08:06 EDT
Nmap scan report for teamnebulatest.us-east-1.elasticbeanstalk.com (34.197.148
Host is up (0.0061s latency).
rDNS record for 34.197.148.58: ec2-34-197-148-58.compute-1.amazonaws.com
Not shown: 65532 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 1539.29 seconds
kali@kali:~$ 
```

8 Does the site have any known vulnerabilities?

Yes, e.g. the following:

CVE-2020-7656	CVE-2019-6111	CVE-2001-1446	CVE-2020-7066	CVE-2019-11049	CVE-2019-11040	CVE-2019-9639	CVE-2019-6977
CVE-2020-11022	CVE-2019-6110	CWE: 693	CVE-2020-7065	CVE-2019-11047	CVE-2019-11039	CVE-2019-9638	CVE-2013-2220
CVE-2020-11023	CVE-2019-6109	CVE-2021-21702	CVE-2020-7064	CVE-2019-11046	CVE-2019-11038	CVE-2019-9637	CVE-2007-3205
CVE-2019-11358	CVE-2018-20685	CVE-2020-7071	CVE-2020-7063	CVE-2019-11045	CVE-2019-11036	CVE-2019-9025	CVE-2019-8331
CVE-2015-9251	CVE-2018-15919	CVE-2020-7070	CVE-2020-7062	CVE-2019-11044	CVE-2019-11035	CVE-2019-9024	CVE-2018-20677
CVE-2012-6708	CVE-2018-15473	CVE-2020-7069	CVE-2020-7061	CVE-2019-19246	CVE-2019-11034	CVE-2019-9023	CVE-2018-20676
CVE - 2008-5161	CVE-2017-15906	CVE-2020-7068	CVE-2020-7060	CVE-2019-11043	CVE-2019-9675	CVE-2019-9022	CVE-2018-14042
CVE-2020-15778	CVE-2008-3844	CVE-2019-11048	CVE-2020-7059	CVE-2019-11042	CVE-2019-9641	CVE-2019-9021	CVE-2018-14040
CVE-2020-14145	CVE-2007-2768	CVE-2020-7067	CVE-2019-11050	CVE-2019-11041	CVE-2019-9640	CVE-2019-9020	

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

See chapters three and four for version identifiers. The software is not up to date / patched as it should be. Many vulnerabilities are present due to this (compare chapter 8).