

basic tools/ scans we have used:

Windows CMD:

1. Ping

Information: The web site cannot be pinged

```
Microsoft Windows [Version 10.0.19042.804]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping teamnebula.us-east-1.elasticbeanstalk.com

Pinging teamnebula.us-east-1.elasticbeanstalk.com [52.85.160.100]:
Request timed out.
Request timed out.
Request timed out.
```

2. Tracert

```
C:\WINDOWS\system32>tracert teamnebula.us-east-1.elasticbeanstalk.com

Tracing route to teamnebula.us-east-1.elasticbeanstalk.com
over a maximum of 30 hops:

  0  1 ms    1 ms    1 ms    172.30.11.1
  1  1 ms    1 ms    1 ms    10.6.0.57
  2  2 ms    2 ms    4 ms    10.5.31.90
  3  1 ms    1 ms    2 ms    10.5.31.89
  4  1 ms    1 ms    1 ms    10.5.31.94
  5  2 ms    1 ms    1 ms    82.203.71.14
  6  1 ms    1 ms    1 ms    10.5.31.114
  7  2 ms    2 ms    1 ms    82.203.70.13
  8  3 ms    3 ms    3 ms    82.203.70.13
  9  3 ms    4 ms    4 ms    10.10.0.118
 10  5 ms    5 ms    5 ms    213.86.121.1
 11  *        *        *        Request time
 12  *        *        *        Request time
 13  *        *        *        Request time
 14  *        *        *        Request time
 15  *        *        *        Request time
 16  *
```

Information: Each member has different result. Usually 13-30 hops, with 1-30ms TTL:

3. Nslookup: The ip of the website is easy to find via nslookup, which is 18.235.155.131:

```
Non-authoritative answer:  
Name:      teamnebula.us-east-1.elasticbeansta  
Address:   18.235.155.131
```

4. Other Whois records:
All this information can be discovered by accessing domaintools.com

Whois Record (last updated on 2021-05-26)

Domain Name: elasticbeanstalk.com
Registry Domain ID: 1633430775_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: <http://www.markmonitor.com>
Updated Date: 2019-08-26T12:19:56-0700
Creation Date: 2011-01-04T15:11:58-0800
Registrar Registration Expiration Date: 2024-01-04T00:00:00-0800
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (<https://www.icann.org/epp#clientUpdateProhibited>)
Domain Status: clientTransferProhibited (<https://www.icann.org/epp#clientTransferProhibited>)
Domain Status: clientDeleteProhibited (<https://www.icann.org/epp#clientDeleteProhibited>)
Domain Status: serverUpdateProhibited (<https://www.icann.org/epp#serverUpdateProhibited>)
Domain Status: serverTransferProhibited (<https://www.icann.org/epp#serverTransferProhibited>)
Domain Status: serverDeleteProhibited (<https://www.icann.org/epp#serverDeleteProhibited>)
Registry Registrant ID:
Registrant Name: Hostmaster, Amazon Legal Dept.
Registrant Organization: Amazon Technologies, Inc.
Registrant Street: P.O. Box 8102
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89507
Registrant Country: US
Registrant Phone: +1.2062664064
Registrant Phone Ext:
Registrant Fax: +1.2062667010
Registrant Fax Ext:
Registrant Email: hostmaster@amazon.com
Registry Admin ID:
Admin Name: Hostmaster, Amazon Legal Dept.
Admin Organization: Amazon Technologies, Inc.
Admin Street: P.O. Box 8102
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89507
Admin Country: US
Admin Phone: +1.2062664064
Admin Phone Ext:
Admin Fax: +1.2062667010
Admin Fax Ext:
Admin Email: hostmaster@amazon.com
Registry Tech ID:
Tech Name: Hostmaster, Amazon Legal Dept.
Tech Organization: Amazon Technologies, Inc.
Tech Street: P.O. Box 8102
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89507
Tech Country: US
Tech Phone: +1.2062664064
Tech Phone Ext:
Tech Fax: +1.2062667010
Tech Fax Ext:
Tech Email: hostmaster@amazon.com
Name Server: ns-1235.awsdns-26.org
Name Server: ns-416.awsdns-52.com
Name Server: ns-846.awsdns-41.net
Name Server: ns-1537.awsdns-00.co.uk
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>

For more information on WHOIS status codes, please visit:

How this will shape the type of pen tests you will undertake after your initial report:

External Pen test: With the web site information, we can simulate the malicious activities to identify security holes in the web site. This helps us understand:

- vulnerabilities are in the web site
- how they could be exploited
- impacts would be if an attacker were successful.

Web application penetration testing: After having obtained the web site information, we can introduce a web app penetration test including:

- database injections (if have)
- cross-site scripting (XSS)
- broken authentication