
TCP/IP SCAN
PENTESTING
GROUP 5

Basic TCP/IP Tool Scans

- **Ping** produces no results because requests are timed out
- **Tracert:** Each member has different result. Majority have **13-30 hops**, with **1-30ms TTL**

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

Tracing route to teamnebula.us-east-1.elasticbeanstalk.com [18.235.155.131]
over a maximum of 30 hops:
```

- **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.elasticbeanstalk.com
Address:  18.235.155.131
```

- **Whois:**

```
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
```

How it will shape future pen tests

- **Having collected the web site information, we can simulate the malicious activities to identify security holes in the web site. This helps us understand:**
  1. Vulnerabilities are in the web site
  2. How they could be exploited
  3. Impacts would be if an attacker were successful.

- **After having obtained the web site information, we can introduce a web app penetration test including:**
  1. Database Injections (If Have)
  2. Cross-site Scripting (XSS)
  3. Broken Authentication

References

1. A2 HOSTING(2021) Using nslookup on Microsoft Windows
Available from:
https://www.a2hosting.com/kb/getting-started-guide/internet-and-networking/troubleshooting-dns-with-dig-and-nslookup
[Accessed 25th May 2015]
2. Domain.com (2021) What is the traceroute command
Available from:
https://www.domain.com/help/article/using-the-traceroute-tracert-command
[Accessed 25 May 2015]