TEAM NEBULA

NETWORK AND INFORMATION SECURITY MANAGEMENT

SEMINAR 2: TCP/IP V ISO/OSI

26/05/21

TOOLS, SCANS & RESULTS

Target

Team 4 Website

URL: nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com

Tools

- Kali Linux
  - Nmap
  - Traceroute
  - MTR
  - Ping
  - Dig
  - Nslookup
  - Whois
- Windows 10
  - Tracert

Scan Variations

- ICMP/TCP
- Home router/Mobile hotspot
- IP address/hostname

Results

Hops:

- From 13 to 30+

Maximum latency examples:

- 142ms - 34.193.11.248 (destination)
- 144ms – UK to US hop

Hosting Location:

- ec2-34-193-11-248.compute-1.amazonaws.com
- Virginia, US

Registered Contact:

- Amazon Technologies Inc.

Nameservers:

- ns-1011.awsdns-62.net
- ns-1219.awsdns-24.org
- ns-1846.awsdns-38.co.uk
- ns-59.awsdns-07.com

MX Record:

- awsdns-hostmaster.amazon.com

ISSUES, CHALLENGES & PLANNING

Issue/Challenge	Resolution
Setting up Kali Linux	• Windows App • VM Image from Offensive Security • Browser-based
30+ hops and request timeouts common with ICMP Traceroute	• Use mobile hotspot instead of home router • Adjust max hops to beyond 30 • Use TCP traceroute • Browser option – https://geotraceroute.com/
Only one hop shown using Traceroute with TCP	Use Kali Linux on cloud server in US
WHOIS not working with hostname	Use IP address instead
Different physical hosting locations found	N/A
MX Record not available response	N/A

How will the issues and challenges affect your final report?

- Regular blocking of certain traffic types may be an issue – there is likely a firewall in front of AWS.
- All team members can now set up and use Kali Linux for the next steps.