Network and Information Security Management May 2021 A

« Collaborative Learning Discussion 2

Czeska Stanley

Initial post

14 days ago

5 replies

Last 7 days ago

Good evening all,

In our group, we agreed that each individual person would conduct a basic scan each on the opposing groups website so that we could compare the results with each other. This proved to be fairly different between the members when it came to the hop count. Some of the results were vastly different across the board.

In regards to my own individual results, there was a max number of 30 hops with some of them returning blank results, however the longest hop was on step/hop 7 that consisted of 100ms. The blank results that were returned, the ones that consisted of asterisks, were due to a router and its corresponding firewall blocking my computer (Pickaweb, 2021).

The main name servers for the website that I found during my searches via 'Whois' found 'markmonitor.com' to be the name server and the registered contact turned out to be 'Amazon host master legal department'.
Despite having found the aforementioned, I did struggle to find where the website was hosted despite using 'MX lookup' and the 'OSINT framework', however I did find that the domain is 'Elasticbeanstalk.com'

Some of the tools used consist of :

- command prompt
- MX toolbox / look up
- OSINT frame work
- WHOis
- traceroute

References

Pickaweb. (2021). What Is A Traceroute?. Available at: https://www.pickaweb.co.uk/kb/what-is-a-traceroute/. [Accessed 03 June 2021].

Bibliography

Hacking Articles. (2021). Working of Traceroute using Wireshark. Available at: https://www.hackingarticles.in/working-of-traceroute-using-wireshark/. [Accessed 03 June 2021].

Pickaweb. (2021). What Is A Traceroute?. Available at: https://www.pickaweb.co.uk/kb/what-is-a-traceroute/. [Accessed 03 June 2021].

Reply

5 replies

1 Post by **Aimalohi Odia**

12 days ago

Peer Response

The “ping” command is a subset of the Internet Control Message Protocol (ICMP), and it is used to test for internet connectivity issues on the network layer resulting in problems such as latency and packet loss which may be as a result of bandwidth saturation over a link ,a bad network cable or a port on a switch. Other reasons for unsuccessful pings are the presence of proxy servers or firewalls.(Jacobson, 2009).

Reference

Jacobson, D. (2009) Introduction to Network Security. (1st ed.). Chapman and Hall.

Reply

2  Post by **Freya Basey**

10 days ago

Peer Response

Further to Aimalohi’s point, Traceroute also utilises the Internet Control Message Protocol (ICMP) as standard (Parziale et al., 2006). The deprioritisation of ICMP packets by modern routers can lead to distorted and unreliable delay data when using Traceroute (NetBrain, 2017). When initially using Traceroute, I found the requests timed out before reaching the destination. Switching to an internet connection via a mobile hotspot returned better results as the traffic took a different route and was not limited by the manufacturer’s settings on the residential gateway.

NetBrain (2017) Traceroute Limitations Explained. Available from: **https://www.netbraintech.com/blog/limitations-of-traceroute/** [Accessed 7 June 2021].

Parziale, L., Britt, D., Davis, C., Forrester, J., Lui, W., Matthews, C. & Rosselot, N. (2006) *TCP/IP Tutorial And Technical Overview.* 8th ed. New York: IBM.

Reply

3  Post by **Jan Küfner**

10 days ago

peer response

Blank results consisting of asterisks followed by further hops does not mean that a firewall is blocking your computer totally. It only means that rules are in place at that node, that will not deliver an ICMP response to you, stating that time to live (TTL) has expired. Traffic with a TTL > 1 will be forwarded without any blocking. (Parziale et al 2006)

References:
Parziale, L. et al, (2006) - TCP/IP tutorial & technical overview Available from https://www.redbooks.ibm.com/abstracts/gg243376.html?Open Accessed on 2021-06-01

Reply

Maximum rating: -

4  Post by **David Luvaha**

8 days ago

Peer Response

As discussed above Stanton (2019) says that Pinging is an excellent command to test network connectivity, however when used on windows operating systems it sometimes returns “Ping transmit failed. General Failure” on Windows 7, 8/8.1, and 10. The problem may be attributed Virtual Machine (VM) issues, lack resent network drivers or firmware, Domain Name System (DNS) problems or poorly configured firewalls.

References

Stanton, W.(2019)Ping Transmit Failed General Failure – What To Do

Available from:

https://www.alphr.com/ping-transmit-failed-general-failure/

[Accessed 3 June 2021]

Reply

5  Post by **Shiraj Ali**

7 days ago

Peer Response

We want to extend on hop count difference between the members. (Fei et al., 1988) measured Hop-Count and Round Trip Time (RTT) distribution from one host in the USA to about 3000 hosts scattered in four continents. They found out that RTT and HC to international hosts depend on the hosts' countries.

The Hop-Count distribution seen from the six sources to all the destinations is calculated. Although the Hop-Count values vary between 6 and 30, more than 83% of the Hop-Count values are located between 11 and 21 hops only (Mukaddam and Elhajj, 2011).

To expand on the OSINT framework, (Lee and Shon, 2016) explains that it is challenging to apply the OSINT procedure to inspect vulnerabilities in the general IT environment since the system boundary and communication patterns are ambiguous and various. However, it is possible to efficiently apply OSINT procedure to a critical infrastructure network because of its character of communication patterns and environments.

Therefore, the improvement of security level is expected by applying the OSINT framework to inspect cybersecurity threats, which are not discovered and considered in critical infrastructures of energy, industrial, and financial networks (Lee and Shon, 2016).

- Team TLL (Amy, Chris, Laura, Shiraj)

Reference:
Fei, A., Zhang, L., Pei, G. and Liu, R., 1998. Measurements on Delay and Hop-count of the Internet. [online] Web.cs.ucla.edu. Available at: **http://web.cs.ucla.edu/~lixia/papers/98Globcom.pdf** [Accessed 10 June 2021].

Mukaddam, A. and Elhajj, I., 2011. Hop Count Variability. In: International Conference on Internet Technology and Secured Transactions,. [online] Abu Dhabi, United Arab Emirates: American University of Beirut, pp.240-244. Available at: **https://ieeexplore.ieee.org/document/6148450** [Accessed 11 June 2021].

Lee, S. and Shon, T., 2016. Open Source Intelligence Base Cyber Threat Inspection Framework for Critical Infrastructures. In: Future Technologies Conference 2016. [online] San Francisco, United States: Department of Cyber Security Ajou University, pp.1030-1033. Available at: https://ieeexplore.ieee.org/document/7821730 [Accessed 11 June 2021].

Reply

Add your reply

Your subject

Type your post

Dateien auswählen Keine ausgewählt

Submit

Use advanced editor and additional options

Older discussion

Initial Post

Newer discussion

Team initial post