Network and Information Security Management May 2021 A

« Collaborative Learning Discussion 2

David Luvaha

Initial Post

23 days ago

2 replies


Last 10 days ago

Domain.com (2021) says that tracert is used for trouble shooting network connection. It gives a list of 'hops' that data packets take along their route to the destination IP address or domain. The scan produced a maximum of 30 hops, the biggest delay was at step 14 with an average delay duration of 222ms**.** Norton life lock & Steve (2021) indicates that along delay indicates heavy traffic on the website making it unavailable.

According to Elsevier (2021) Pathping just like tracert provides statistics on network latency and loss between two communicating nodes by ascertain the number of hops between them. The scan produced a maximum of 30 hops and a Round Trip Time (RTT) of 10ms.

A2 Hosting (2021) indicates that Microsoft Windows uses nslookup software instead of dig software. Nslookup revealed a number of Domain Name System (DNS) that support the website. According to Security Trails (2021) such information might be maliciously used for DNS hijacking or redirection where hackers redirect your traffic to a malicious website. DNS poisoning/spoofing may also be conducted by maliciously redirecting traffic to the web server.

The scan produced, the registered contact and the host of the website to be Amazon.com, Inc however the MX record was found to be empty. Such information might make the website susceptible to Phishing attacks and ransomware attacks.

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]

3. Elsevier(2021) Pathping

Available from:

https://www.sciencedirect.com/topics/computer-science/tracert-command

[Accessed 25 May 2015]

4. Norton life lock & Steve,W. (2021) What are Denial of Service (DoS) attacks? DoS attacks explained.

Available from:

https://us.norton.com/internetsecurity-emerging-threats-dos-attacks- explained.html

[Accessed 25 May 2021].

5. Thompson, J. & AT&T Business(2021) How to Prevent DNS Poisoning and DNS Spoofing

Available from:

https://cybersecurity.att.com/blogs/security-essentials/dns-poisoning

[Accessed 25 May 2015]

Reply

2 replies

1  Post by **Charlotte Wilson**

11 days ago

Peer Response

The lack of MX record in this instance can mean the site is susceptible to phishing attacks. Having a MX record in place can ensure that only authorised emails are sent from this particular domain. Unfortunately, cyber criminals tend to set up fake domains that resemble legitimate companies in an attempt to attack individuals with phishing emails and other attacks. A legitimate MX record could help improve the reputation of your domain and in turn, ensure that emails are directed to others correctly knowing they will pass any MX check (Fraud Watch, 2016). It is becoming necessary for organisations to follow these security practices to continue running their business. Many now expect these good security measures to be in place as a standard.

References

Fraud Watch (2016) Email Security: MX Records. Available from:
https://fraudwatchinternational.com/phishing/email-security-mx-records/

[Accessed 5 June 2021]

Reply

2 

Post by **Jan Küfner**

10 days ago

peer response

Tracert uses ICMP packages, which have lower priority in routing. Results obtained with this tool will therefore not reflect http traffic, since this is for example send with higher priority TCP packages. (Parziale et al 2006)

Having heavy traffic on AWS websites is rather unlikely, since they have a lot of bandwidth. If step 14 was not the end destination, which is likely with an ICMP route, than this also indicates, that the delay isn't created at the destination / at a website. A more likely explanation for delay could be that this node is busy and is only slowly forwarding ICMP packages. Another explanation could also be that this is a node connected to a node in great distance. It could for example be that this hop connects two continents. Information about the geolocation of those two nodes could provide more information. (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: -

Add your reply

Your subject

Type your post

Dateien auswählen Keine ausgewählt

Submit

Use advanced editor and additional options

NEWER DISCUSSION

Initial Post