Network and Information Security Management November 2021 B

« Collaborative Learning Discussion 2

Pavendran Wimalendran

Initial Post

58 days ago

1 reply

Last 16 days ago

I used the following tools in order to identify a variety of information relating to the blog site
"readmyblog.co.uk".
Traceroute
nslookup
WHOIS

Here are the ways the above tools were used to answer the questions that were set in Unit 3 of
this module and the outcomes.

How many hops from your machine to your assigned website?
Used TRACERT to count the hops and it took 11 hops to reach the intended website.

Which step causes the biggest delay in the route? What is the average duration of that delay?
Routing between https://cogentco.com/ network and the average delay is 17.63 ms.

What are the main nameservers for the website?
Used nslookup to query the name server details and found the following name servers.
ns1.a2hosting.com
ns2.a2hosting.com
ns3.a2hosting.com
ns4.a2hosting.com

Who is the registered contact?
Used whois for this activity and was able to find the following related to the blog site:
Registrar: eNom LLC [Tag = ENOM] (http://www.enom.com)

What is the MX record for the website?

Used nslookup by setting "set type=mx" to query the MX record for this website and found the following MX record.
MX preference = 0
mail exchanger = mail.readmyblog.co.uk

Where is the website hosted?
Since pinging is not recommended, I used "whatismyipaddress.com" to get the IP address using the hostname and then used "ipinfo.io" to find the location of the server. It appears from the above steps that the website is hosted in Amsterdam, the Netherland

References:

Pandit, P. (2021). A Study of Network Reconnaissance Tools.

University of Essex Online. (2021) Network Fundamentals [Lecturecast]. NISM_PCOM7E November 2021 B, Network and Information Security Management. University of Essex Online.

Reply

Maximum rating: -

1 reply

1   Post by **Taylor Edgell**

16 days ago

Responce

> Hi Pavendran.
> Thank you for your output, what did you find to be the most useful and easiest to use tools within this exercise ?
>
> I do find it interesting that many of us found the wesites to be hosted in different locations. As all websites are provided through a name based hosting system they should all be hosted in the same location. The two primary locations I have seen people to have determined they are hosted are the Netherlands (such as you have found) and the USA. It can be seen that "Despite considerable efforts, accurate measurement-based geolocation remains an open problem." (Eriksson & Crovella, 2013). This may be a bit of an open question, but how do you think we could gain a better accuracy level of where the website is actually hosted ?
>
> References:
>
> Eriksson, B. and Crovella, M., 2013, April. Understanding geolocation accuracy using network geometry. In *2013 Proceedings IEEE INFOCOM* (pp. 75-79). IEEE.

Reply

Add your reply

Your subject

Type your post

Choose files   No file chosen

Submit

Use advanced editor and additional options

OLDER DISCUSSION

NEWER DISCUSSION

Initial Post

Summary