Scanning Exercises: Peer Responses

Course: MSc Computer Science

Module: Network and Information Security Management

Assignment: ePortfolio

Date: Saturday 30th October 2021

Student ID: 126853

Peer Response 1:

In response to:

Uzayr Parak

Initial Post (Team A)

48 days ago

2 replies

Last now

Collaborative Discussion 2 – Initial Post (Team A)

Modules

Kieron Hol

How many hops from your machine to your assigned website?

For this we used the traceroute tool, which is available on MacOS, Windows, and Linux machines. This tool reports information about each hop taken by a packet between a computer and remote host. We initially struggled to get a result using traceroute on the provided AWS URL, however increasing the maximum number of hops from 30 to 64 allowed a full traceroute to be completed without timing out. It took 37 hops from our machine to the assigned website (*How to troubleshoot network connectivity using ping and traceroute*, no date; Tetz, 2011; Broad and Bindner, 2014; Edwards and Bramante, 2015).

What are the main nameservers for the website?

To find the information on the main nameservers we used both dig and nslookup. Both tools can be used to retrieve various DNS information for a given website. Setting the record type to NS returns the appropriate information. Windows machines use nslookup, Linux machines use sig, and MacOS machines can use both (*How to troubleshoot DNS with dig and nslookup*, no date).

Who is the registered contact?

Similarly to the nameservers above, the registered contact can be found by using the nslookup or dig tools and setting the DNS record type to RP. These tools did not reveal any useful information relating to the registered contact. We therefore used the whois command(Bruen, 2015) to determine the registered contact- Amazon

What is the MX record for the website?

Similarly to the nameservers above, the registered contact can be found by using the nslookup or dig tools and setting the DNS record type to MX. We did not identify any information using this command, and therefore used the whois command (Bruen, 2015).

Where is the website hosted?

Similarly to the nameservers above, the registered contact can be found by using the nslookup or dig tools and setting the DNS record type to LOC. This command was not able to determine the location, therefore a whois command was performed to determine the location- Reno, Nevada, USA

References

Broad, J. and Bindner, A. (2014) 'Chapter 8 - Scanning', in Broad, J. and Bindner, A. (eds) *Hacking with Kali*. Boston: Syngress, pp. 103–130. doi: https://doi.org/10.1016/B978-0-12-407749-2.00008-2.

Bruen, G. O. (2015) *WHOIS Running the Internet: Protocol, Policy, and Privacy*. Wiley. Available at: https://books.google.co.za/books?id=mgmeCAAAQBAJ.

Edwards, J. and Bramante, R. (2015) *Networking Self-Teaching Guide: OSI, TCP/IP, LANs, MANs, WANs, Implementation, Management, and Maintenance*. Wiley. Available at: https://books.google.co.za/books?id=YSPPBwAAQBAJ.

How to troubleshoot DNS with dig and nslookup (no date). Available at: https://www.a2hosting.co.uk/kb/getting-started-guide/internet-and-networking/troubleshooting-dns-with-dig-and-nslookup#Using-dig-on-Apple-Mac-OS-X-and-Linux (Accessed: 10 September 2021).

How to troubleshoot network connectivity using ping and traceroute (no date). Available at: https://www.a2hosting.com/kb/getting-started-guide/internet-and-networking/troubleshooting-network-connectivity-with-ping-and-traceroute#Testing-the-path-to-a-remote-host-with-traceroute (Accessed: 11 September 2021).

Tetz, E. (2011) *Cisco Networking All-in-One For Dummies*. Wiley (--For dummies). Available at: https://books.google.co.za/books?id=7DVtgcZVOYIC.

Reply

Post:

Hi Team,

An excellent point was raised above. Many of the services provided by Amazon Web Services will, by default, offer subdomains indicating the Region/Availability Zone, as well as the resource name (Amazon, n.d.). However, generally speaking, the WHOIS service is only available for primary domains (Kailash1, 2009). In cases like this, the

most appropriate way of identifying domain details is to look up the main domain (elasticbeanstalk.com).

It is also worth considering the usage of services such as AnyCast for DNS with large cloud providers. The Nameservers chosen to handle your request will likely be those located geographically closest (Cloudflare, n.d.), meaning different team members will likely experience different results.

References:

Amazon. (n.d.) Your Elastic Beanstalk environment's Domain Name. Available from: https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/customdomains.html [Accessed 30th October 2021].

Cloudflare. (n.d.) What is Anycast DNS?. Available from: https://www.cloudflare.com/en-gb/learning/dns/what-is-anycast-dns [Accessed 30th October 2021].

Kailash1. (2009) Whois for Subdomain. Available from: https://forums.cpanel.net/threads/whois-for-subdomain.129273/ [Accessed 30th October 2021].

Screenshot:

Post by **Kieron Holmes** now

Peer Response

Hi Team,

An excellent point was raised above. Many of the services provided by Amazon Web Services will, by default, offer subdomains indicating the Region/Availability Zone, as well as the resource name (Amazon, n.d.). However, generally speaking, the WHOIS service is only available for primary domains (Kailash1, 2009). In cases like this, the most appropriate way of identifying domain details is to look up the main domain (elasticbeanstalk.com).

It is also worth considering the usage of services such as AnyCast for DNS with large cloud providers. The Nameservers chosen to handle your request will likely be those located geographically closest (Cloudflare, n.d.), meaning different team members will likely experience different results.

References:

Amazon. (n.d.) Your Elastic Beanstalk environment's Domain Name. Available from: https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/customdomains.html [Accessed 30th October 2021].
Cloudflare. (n.d.) What is Anycast DNS?. Available from: https://www.cloudflare.com/en-gb/learning/dns/what-is-anycast-dns [Accessed 30th October 2021].
Kailash1. (2009) Whois for Subdomain. Available from: https://forums.cpanel.net/threads/whois-for-subdomain.129273/ [Accessed 30th October 2021].

Peer Response 2:

In response to:

Kikelomo Obayemi

Initial Post

56 days ago

3 replies

Last 14 secs ago

For Team B

Network troubleshooting can be defined as an activity carried out to diagnose a network problem (a2hosting, n.d) Its success is largely dependent on the quality of information collected and the efficiency with which the information is collected (Sloan, 2021). An example of network troubleshooting can be seen in the Unit 3 formative activity which required the use of basic networking tools to collect information from Team A's AWS url and IP address.

The specific information to be gathered from this exercise are as follows:

Number of hops from tester's machine to the assigned website?

This can be achieved using the **traceroute** tool which is used to determine the path between two connections (a2hosting, n.d). It can be executed by typing into the command prompt:

PC: tracert "url" or tracert "IP address"

Mac: traceroute "url" or traceroute "IP address"

In this exercise, we were unable to reach the destination IP address.

Which step causes the biggest delay in the route? What is the average duration of that delay?

The **ping** tool was used for this question. The ping tool is usually the first tool used by a system administrator to test for network connectivity and is executed using this syntax

"ping IP address"(Sloan, 2021). Since It shows the duration to reach a route, by pinging the IP address of the hop with the longest delay, we were able to get the average duration of that delay.

What are the main nameservers for the website?

Information on Domain Name Servers (DNS) can be found using the nslookup tool (Sloan, 2021). However, for this task, nslookup did not provide much information. Whois website was used instead.

Who is the registered contact?

My Modules

Kieron

What is the MX record for the website?

nslookup tool can be used to get this information (trendmicro, 2021) however No MX records found in this scenario.

Where is the website hosted?

Information found on the whois website

References

a2hosting (n.d) How to troubleshoot network connectivity using ping and traceroute. Available from: https://www.a2hosting.com/kb/getting-started-guide/internet-and-networking/troubleshooting-network-connectivity-with-ping-and-traceroute [accessed 25 August 2021]

a2hosting (n.d) Introduction to Network Troubleshooting. Available from: https://www.a2hosting.com/kb/getting-started-guide/internet-and-networking/introduction-to-network-troubleshooting [Accessed 25 August 2021]

Sloan, J.D. (2001). Network Troubleshooting Tools: Help for Network Administrators. " O'Reilly Media, Inc.".

Trendmicro (2021) Available from: https://success.trendmicro.com/solution/1034632-using-nslookup-to-view-mail-exchange-mx-records-for-hosted-email-security-hes-and-email-reputati [Accessed 03 September 2021]

Team B Network Troubleshooting Activity.pdf

Reply

Post:

Hi Kike/Team,

In general, you've produced a great post detailing the tools that can be used for specific host identification tasks, as well as the associated commands.

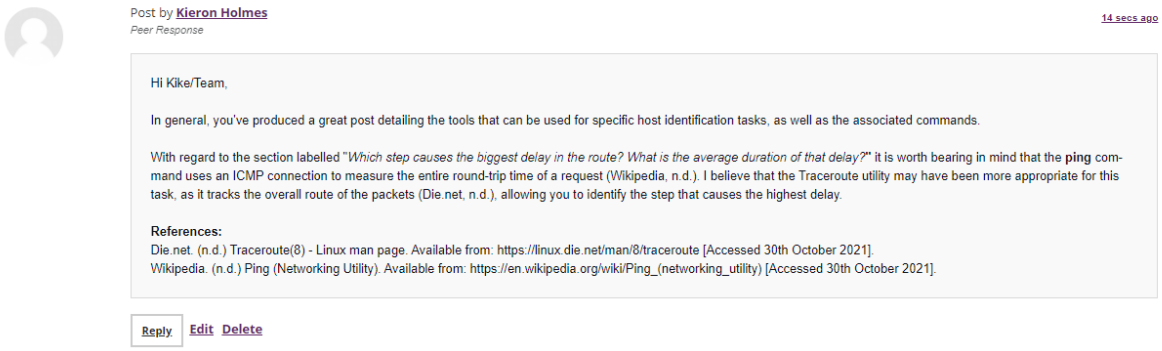
With regard to the section labelled "Which step causes the biggest delay in the route? What is the average duration of that delay?" it is worth bearing in mind that the ping command uses an ICMP connection to measure the entire round-trip time of a request (Wikipedia, n.d.). I believe that the Traceroute utility may have been more appropriate for this task, as it tracks the overall route of the packets (Die.net, n.d.), allowing you to identify the step that causes the highest delay.

References:

Die.net. (n.d.) Traceroute(8) - Linux man page. Available from: https://linux.die.net/man/8/traceroute [Accessed 30th October 2021].

Wikipedia. (n.d.) Ping (Networking Utility). Available from: https://en.wikipedia.org/wiki/Ping_(networking_utility) [Accessed 30th October 2021].

Screenshot:



Post by **Kieron Holmes** 14 secs ago

Peer Response

Hi Kike/Team,

In general, you've produced a great post detailing the tools that can be used for specific host identification tasks, as well as the associated commands.

With regard to the section labelled "*Which step causes the biggest delay in the route? What is the average duration of that delay?*" it is worth bearing in mind that the **ping** command uses an ICMP connection to measure the entire round-trip time of a request (Wikipedia, n.d.). I believe that the Traceroute utility may have been more appropriate for this task, as it tracks the overall route of the packets (Die.net, n.d.), allowing you to identify the step that causes the highest delay.

References:

Die.net. (n.d.) Traceroute(8) - Linux man page. Available from: https://linux.die.net/man/8/traceroute [Accessed 30th October 2021].

Wikipedia. (n.d.) Ping (Networking Utility). Available from: https://en.wikipedia.org/wiki/Ping_(networking_utility) [Accessed 30th October 2021].

Reply Edit Delete