Network and Information Security Management May 2021 A

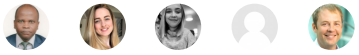
« Collaborative Learning Discussion 2

Dario De Giorgi

Initial Post

24 days ago

5 replies



Last 8 days ago

During the scan of the website of the opposite team, the use of traceroute allows to see the distance between my machine and the website it was 30 hops, with the biggest delay of 97 ms, the average is 80 ms. A lot of asterisks were founded on my result, it means it's returns a time out and the destination device is reached (Behrens, 2018)

The use of the dig command allows to have a lot of information's, for example the IP address that the website has. Exposing the public IP address provides an entry point for hackers (Shatilin, 2018).

The whois command gives information about the nameservers that the website uses or information about the person or organisation that registered the website. This part can be susceptible to DDOS attacks, a good way to protect against this would be to use name server protection (Imperva, N.D).

No MX record was found regarding the scan, it is possible to use fake mx records to avoid sending spam emails to the users concerned, spam emails are dangerous as they can contain malware or ransomware (TitanHQ, N.D).

Website hosting location information can also be found, during the scan the location of the team opposite is in Ashburn in Virginia in the US.

References:

Behrens, S. (2018) What you need to know about traceroute. Available from: https://blog.paessler.com/what-you-need-to-know-about-traceroute [Accessed 24 May 2021].

Shatilin, I. (2018) The dangers of public Ips. Available from: https://www.kaspersky.com/blog/public-ip-dangers/24745/ [Accessed 24 May 2021].

Iperva. (N.D) DDoS Portection for DNS. Available from: https://www.imperva.com/products/dns-ddos-protection-services/ [Accessed 24 May 2021].

TitanHQ. (N.D) MX Spam filter. Available from: https://www.titanhq.com/security-articles/mx-spam-filter/ [Accessed 24 May 2021].

Reply

5 replies

1 

Post by **Jan Küfner**

15 days ago

Peer Response

30 hops indicates that a programm was used that utilized ICMP packages. ICMP packages do have a different behaviour than standard TCP traffic, since it has lower priority in the internet. Due to this lower priority ICMP packages usually are not send the shortest way, which will result in a higher hop count compared to TCP/IP. If a more realistic traceroute needs to be conducted tools such as NMAP or MTR can be used, since they can do tracerouting via TCP/IP. Parziale et al (2006)

Asterisks in tracerouting typically does mean that no response at all is send back. Some routers are simply configured to not send information in return when the TTL expires. 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: -

2

Post by **Aimalohi Odia**

12 days ago

Peer Response

There are several reasons why a “Request timed out” message may appear at the end of a trace route. It could be because a device isn’t programmed to re-spond to the Internet Control Message Protocol (ICMP) or traceroute requests, it could also be due to the presence of a firewall or other security device which may be blocking the request (Jacobson, 2009).

Reference

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

Reply

3  Post by **Charlotte Wilson**

11 days ago

Peer Response

Information found during this initial stage of assessment can be useful, determining which tools to be used and what risks need mitigation. Whois in particular can be a useful tool to find information for future attacks. For example, the Whois tool can identify who owns the domain, and typically contact information if contact is required (Domain Tools, 2017). You could use this information to conduct targeted social engineering attacks on said individual / corporation, as unfortunately it only takes a few pieces of validity information to make an attack seem legitimate.

References

Domain Tools (2017) What is Whois Information and Why is it Valuable? Available from: https://www.domaintools.com/support/what-is-whois-information-and-why-is-it-valuable#:~:text=Whois%20is%20a%20widely%20used,domain%20name%20registration%20and%20ownership [Accessed 5 June 2021]

Reply

4  Post by **Freya Basey**

10 days ago

Peer Response

Further to Charlotte's point, when performing reconnaissance on a genuine digital asset, search engines and various other sites, such as LinkedIn, can aid the process (McNab, 2016). The information held on these sites can expose other potential vectors for attack that should be considered, including users. However, when including social engineering in vulnerability assessments, the scope of the activity must be clearly agreed with the client (Tang, 2014).

Assessments on the basis of social engineering are not limited to external testing. Phishing testing is completed by businesses internally to test the awareness and training of colleagues (Wright & Thacker, 2021). Due consideration should be given to the content of these emails in order to save on any potential reputational damage, as experienced by West Midlands Trains when the content of their phishing test emails attracted ethical questions from unions (Topham, 2021).

References

McNab, C. (2016) *Network Security Assessment: Know Your Network*. 3rd ed. O'Reilly Media.

Tang, A. (2014) A guide to penetration testing. *Network Security* 2014(8): 8-11.

Topham, G. (May 10, 2021) Train firm's 'worker bonus' email is actually cyber-security test. *The Guardian*. Available from: **https://www.theguardian.com/uk-news/2021/may/10/train-firms-worker-bonus-email-is-actually-cyber-security-test** [Accessed 7 June 2021].

Wright, R. & Thacker, J. (2021) Phishing Tests Are Necessary. But They Don't Need to Be Evil. Available from: **https://hbr.org/2021/04/phishing-tests-are-necessary-but-they-dont-need-to-be-evil** [Accessed 7 June 2021].

Reply

5 

Post by **David Luvaha**

8 days ago

Re: Initial Post

With reference to WHOIS command, Ehost Web Services (2021) says that WHOIS is a repository of your email address, name, domain name and IP address block. When such data is available to the public, it may cause problems. Privacy can be guaranteed by procuring privacy controls. Unfortunately, not all folks understands why it is valuable to keep website ownership information private. On the one hand, keeping WHOIS information private reduces spam attacks and prevent identity theft. On the other hand it makes the business look doubtful. Sometimes registrars may release this information anyway without informing the domain owner.

References

Ehost Web Services.(2021) WHOIS Protection on Domains

Available from:

https://www.ehost.co.za/blog/whois-protection-domains/

[Accessed 3 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

Initial post