**Peer Response 1 (Dario)**

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 cybersecurity 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].

**Peer Response 2 (Czeska)**

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.

**Others**

Further to Jan’s point, firewalls may be able to identify the use of Traceroute and drop the traffic as the tool utilises UDP datagrams that reference an unusual port number <<TCP/IP. However, as Traceroute is utilised to test network connection issues, this is unlikely to be a blanket rule on a standard AWS firewall.

Whilst this exercise sought to replicate reconnaissance activities, there is a natural limitation in that a website not owned and run by a genuine business does not have peripheral services and users to mimic a genuine attack surface area (McNab, 2016).

When initially using Traceroute, 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 <<TCP/IP, Other.

Some peers in the team saw the largest delay in the hop between Europe, where our team members are based, and the US, where the website is hosted. Whilst AWS utilises edge computing to improve performance, this feature is unlikely to be used consistently for free websites, such as the one tested.