Collaborative Discussion 2 – Summary Post – Michael Geiger

When examining the website loadedwithstuff.co.uk with the help of CMD commands and various online tools as well as programs, some information about the website as well as insights into troubleshooting could be obtained.

The hops from the outgoing device via the respective router to the destination address and its latency could be determined with the CMD command tracert. Another possibility to determine this course can be achieved with the program WinMTR (dmanac & vlastanimir, 2013).

A variety of online tools are available to determine the main nameservers, the MX record and the registered contact on the website. Websites like dnstools.ch, who.is and hostingchecker.com offer the possibility to obtain this information. This information can also be examined using CMD commands. However, it was found that pre-installed CMD commands and their usability differ under the respective Operating System (OS) (source). For example, the Windows 10 OS does not offer the CMD commands dig and whois as standard, in contrast to OS such as Linux and macOS and must be installed manually. The results of these commands can be found in the appendix.

It was also found that the tracert command uses ICMP packets under Windows 10. In order to carry out TCP / UDP and ICMP packet examinations, examination programs such as NetScanTools are available, which provide several examination options (Northwest Perfomance Software, Inc., 2021).

The ports of a website can be examined with the program NetScanTools, as well as various online offers (e.g. nmap.org, pentest-tools.com or hackertarget.co). It should be noted here that the results made available differ in part. An investigation with the help of various tools can therefore be useful (O'reilly & Associates, 2002).

The fact that many of the troubleshooting options are free and freely accessible, as well as being possible without registration, enables a good threat analysis for website operators on the one hand. On the other hand, this also poses a risk, since hackers can also spy on websites for their vulnerabilities without in-depth knowledge. Website operators must therefore be aware of this threat.

References

Dmanac & vlasanimir (2013) WinMTR. Available from: https://sourceforge.net/projects/winmtr/ [Accessed: 13.12.2021]

Hacker Target. Available from: https://hackertarget.com/nmap-online-port-scanner/ [Accessed: 11.12.2021]

Hosting Checker (2021) Find out who is hosting any website. Available from: https://hostingchecker.com/ [Accessed:03.12.2021]

Nmap (N.D.).Fast Scan. Available from: https://nmap.online [Accessed: 11.12.2021]

Northwest Performance Software, Inc. (2021)Traceroute Tool. Available from: https://www.netscantools.com/nstpro_traceroute.html [Accessed: 13.12.2021]

Pentest Tools. Available from: https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap [Accessed: 11.12.2021]

Sitepoint GmbH(2021) DNStools. Available from:http://www.dnstools.ch/dns nameserver.html [Accessed: 03.12.2021]

Who.is (2021) WHOIS Search, Domain Name, Website, and IP Tools. Available from: https://who.is/whois-ip/ip-address/68.66.247.187 [Accessed: 03.12.2021]