Peer Response

Thanks, Zihaad, it is an informative post about the scanning techniques and analysis result on the target website. Particularly identified the website services by Nmap and telnet commands.

Besides the scanning on the open port, Nmap could enable version detection during the scan with sV option (Nmap, N.D.). Version detection will try to elicit responses and gather information from the examined ports, just like one of the TCP/IP tools, telnet, does (Parziale et al, 2006). For example, if using telnet command on port 21, the target domain will show the welcome message of Pure-FTPd and with the system local time (Pure-FTPd, N.D). With the version detection by Nmap, the version information will list out automatically including the Apache version mentioned above. This kind of welcome message contains version information that crackers can use to detect vulnerabilities in a system, which should encourage organizations to change it before use.

On the other hand, there is another powerful command is Nmap Scripting Engine (NSE) which can perform a script scan (Nmap, N.D.). It provided the default scripts that could scan for useful information like the HTTP generator of the SSL certificate. For the scanning on loadedwithstuff.co.uk TCP 443 port, it shows that it used Loaded Commerce Community Edition v6.6 as the generator. Beyond reasonable doubt, this web likely used this software as the eCommerce Content Management System (CMS) platform on Softaculous (Softaculous, N.D.). In addition, some of the vulnerabilities can be executed by the shell with the NSE command like ftp-proftpd-backdoor (Mak, N.D.).

References:

Nmap (N.D.) Service and Version Detection. *Nmap Reference Guide*. Available from: https://nmap.org/book/man-version-detection.html [Accessed 10 December 2021].

Parziale, L. et al, (2006) *TCP/IP tutorial & technical overview*. IBM Redbooks. Available via the Vitalsource Bookshelf [Accessed 10 December 2021].

Pure-FTPd (N.D) Advanced Compilation. *Readme Documentation for version 1.0.48.* Available from: https://download.pureftpd.org/pub/pure-ftpd/doc/README [Accessed 10 December 2021].

Nmap (N.D.) Nmap Scripting Engine (NSE). *Nmap Reference Guide*. Available from: https://nmap.org/book/man-nse.html [Accessed 10 December 2021].

Softaculous (N.D.) Loaded Commerce. *E-Commerce*. Available from: https://www.softaculous.com/apps/ecommerce/Loaded\_Commerce [Accessed 10 December 2021].

Mak, K. (N.D.) File ftp-proftpd-backdoor. *NSEDoc: Scripts*. Available from: https://nmap.org/nsedoc/scripts/ftp-proftpd-backdoor.html [Accessed 10 December 2021].

<https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=289200>

Zihaad Khan