Collaborative Discussion 2 – Peer Response 2 – Michael Geiger

When examining the ports used by the loadedwithstuff.co.uk website with various online tools, it is noticeable that they provide different results. The online tool offers compared below are: nmap.online, pentest-tools.com and hackertarget.com. The respective results of the tests can be found in the appendices.

When comparing the results of the respective ports found, it is noticeable that the results differ. The website hackertarget.com only finds eight ports. However, this online tool is the only one to show the filtered ports 23 (telnet) and 3389 (ms-wbt-server). These ports are not listed in the other two scans. The online tool nmap.online lists 21 ports, but also indicates that no response was received from 72 filtered ports and 7 filtered ports could not be reached.

A comparison with the online tool pentest-tools.com shows that the results largely overlap. However, this tool also recognizes port 25 (smtp), which is not listed in the other two results. The program NetScanTools Pro (Northwest Performance Software, Inc., 2021) was used to validate this result. During this investigation, it was also possible to determine port 25 as the active port.

This comparison of online tools and their results suggests that online tools can be useful for examining a website and troubleshooting, but that they do not always deliver complete results. It can therefore make sense to use several tools. It should also be noted that only the free offer was used in each case. If these tools are used for a fee, more detailed results can be expected. On the other hand, this research shows how easy it is for hackers with freely accessible tools to examine websites for potential vulnerabilities.

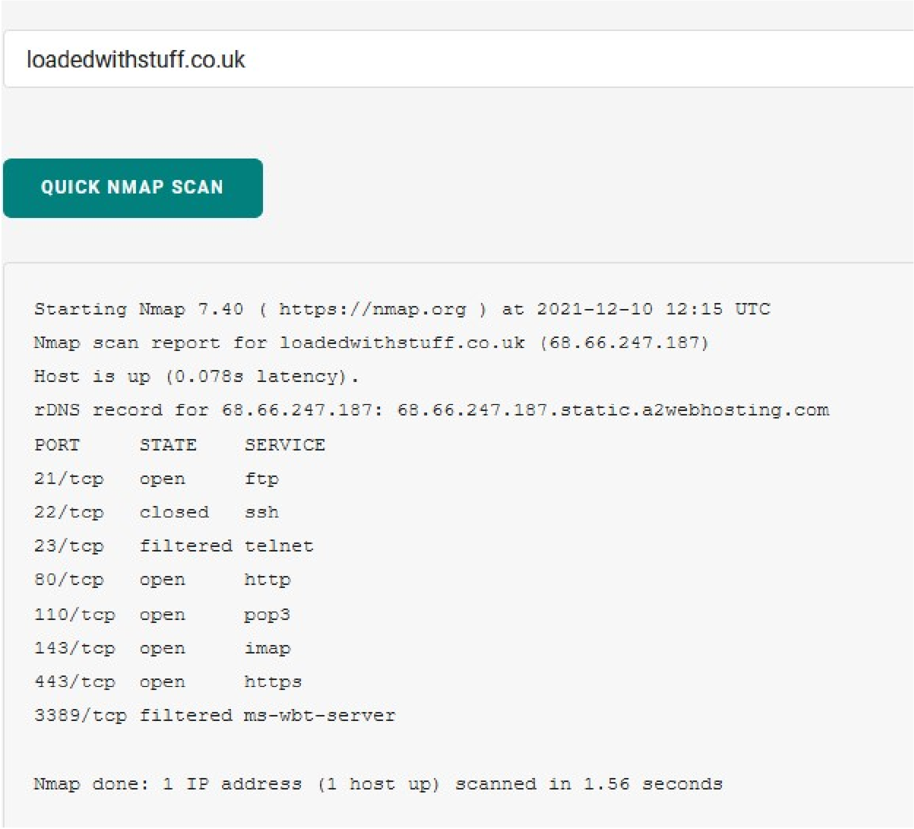
References:

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

Nmap. Available from: https://nmap.online [Accessed: 11.12.2021]

Northwest Performance Software, Inc. (2021) NetScanTools. Available from: https://www.netscantools.com/index.html [Accessed: 09.12.2021]

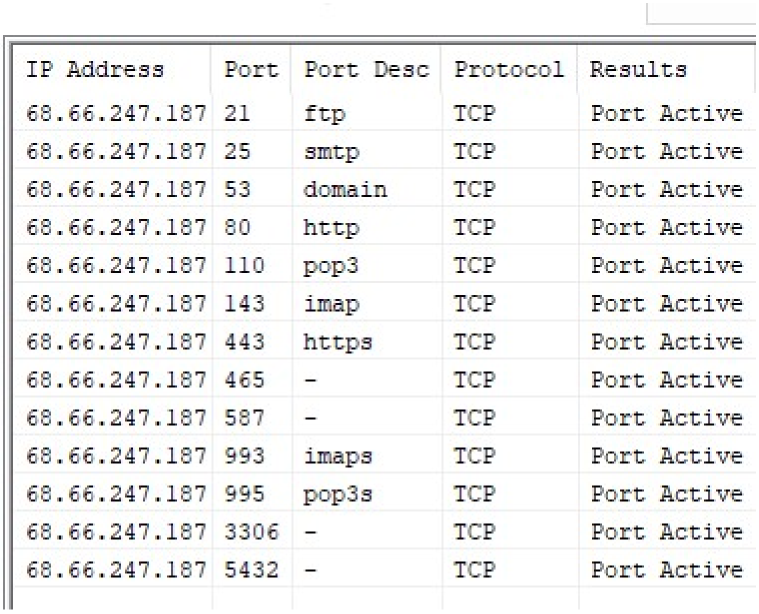
Pentest Tools. Available from: https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap [Accessed: 11.12.2021]



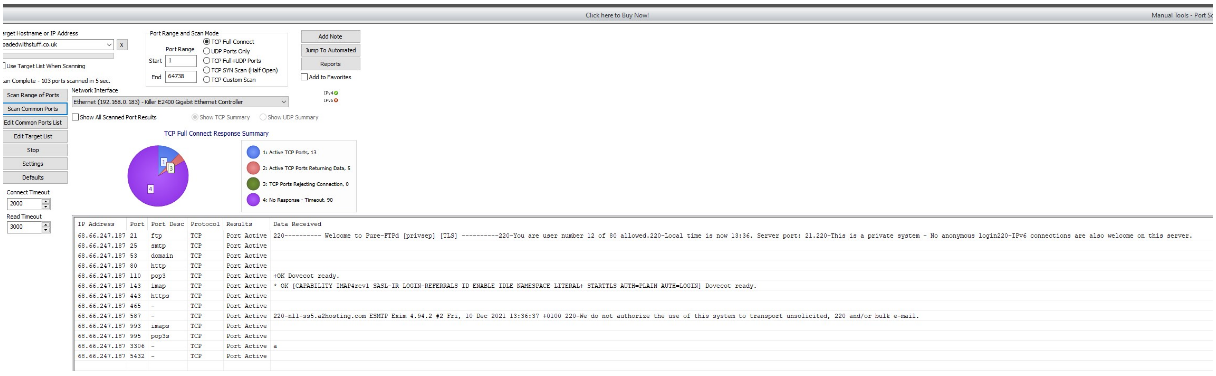
loadedwithstuff.co.uk

```
Starting Nmap 7.40 ( https://nmap.org ) at 2021-12-10 12:15 UTC
Nmap scan report for loadedwithstuff.co.uk (68.66.247.187)
Host is up (0.078s latency).
rDNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   closed   ssh
23/tcp   filtered telnet
80/tcp   open     http
110/tcp  open     pop3
143/tcp  open     imap
443/tcp  open     https
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds
```



IP Address	Port	Port Desc	Protocol	Results
68.66.247.187	21	ftp	TCP	Port Active
68.66.247.187	25	smtp	TCP	Port Active
68.66.247.187	53	domain	TCP	Port Active
68.66.247.187	80	http	TCP	Port Active
68.66.247.187	110	pop3	TCP	Port Active
68.66.247.187	143	imap	TCP	Port Active
68.66.247.187	443	https	TCP	Port Active
68.66.247.187	465	-	TCP	Port Active
68.66.247.187	587	-	TCP	Port Active
68.66.247.187	993	imaps	TCP	Port Active
68.66.247.187	995	pop3s	TCP	Port Active
68.66.247.187	3306	-	TCP	Port Active
68.66.247.187	5432	-	TCP	Port Active



arget Hostname or IP Address: oadedwithstuff.co.uk

□ Use Target List When Scanning

can Complete - 103 ports scanned in 5 sec.

Port Range and Scan Mode

Port Range

Start: 1

End: 64738

● TCP Full Connect
○ UDP Ports Only
○ TCP Full+UDP Ports
○ TCP SYN Scan (Half Open)
○ TCP Custom Scan

□ Add to Favorites

Network Interface: Ethernet (192.168.0.183) - Killer E2400 Gigabit Ethernet Controller

□ Show All Scanned Port Results ● Show TCP Summary ○ Show UDP Summary

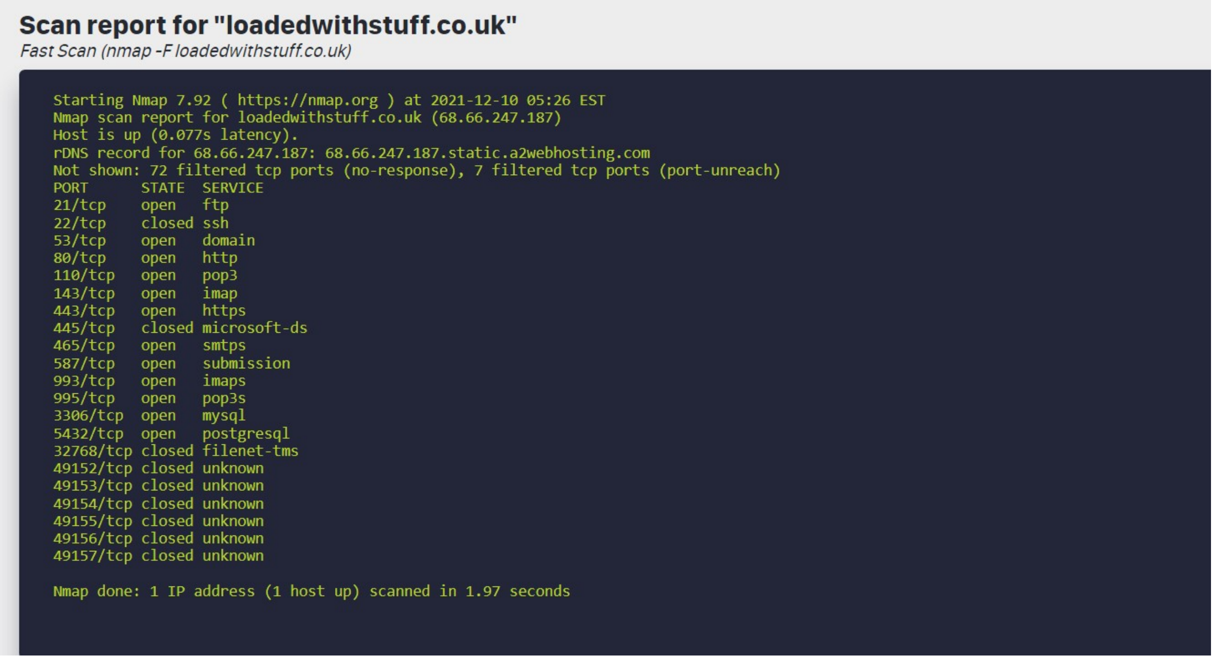
Connect Timeout: 2000

Read Timeout: 3000

TCP Full Connect Response Summary

- 1: Active TCP Ports, 13
- 2: Active TCP Ports Returning Data, 5
- 3: TCP Ports Rejecting Connection, 0
- 4: No Response - Timeout, 90

IP Address	Port	Port Desc	Protocol	Results	Data Received
68.66.247.187	21	ftp	TCP	Port Active	220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 12 of 80 allowed.220-Local time is now 13:36. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.
68.66.247.187	25	smtp	TCP	Port Active	
68.66.247.187	53	domain	TCP	Port Active	
68.66.247.187	80	http	TCP	Port Active	
68.66.247.187	110	pop3	TCP	Port Active	+OK Dovecot ready.
68.66.247.187	143	imap	TCP	Port Active	* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
68.66.247.187	443	https	TCP	Port Active	
68.66.247.187	465	-	TCP	Port Active	
68.66.247.187	587	-	TCP	Port Active	220-nll-ss5.a2hosting.com ESMTP Exim 4.94.2 #2 Fri, 10 Dec 2021 13:36:37 +0100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
68.66.247.187	993	imaps	TCP	Port Active	
68.66.247.187	995	pop3s	TCP	Port Active	
68.66.247.187	3306	-	TCP	Port Active	a
68.66.247.187	5432	-	TCP	Port Active	

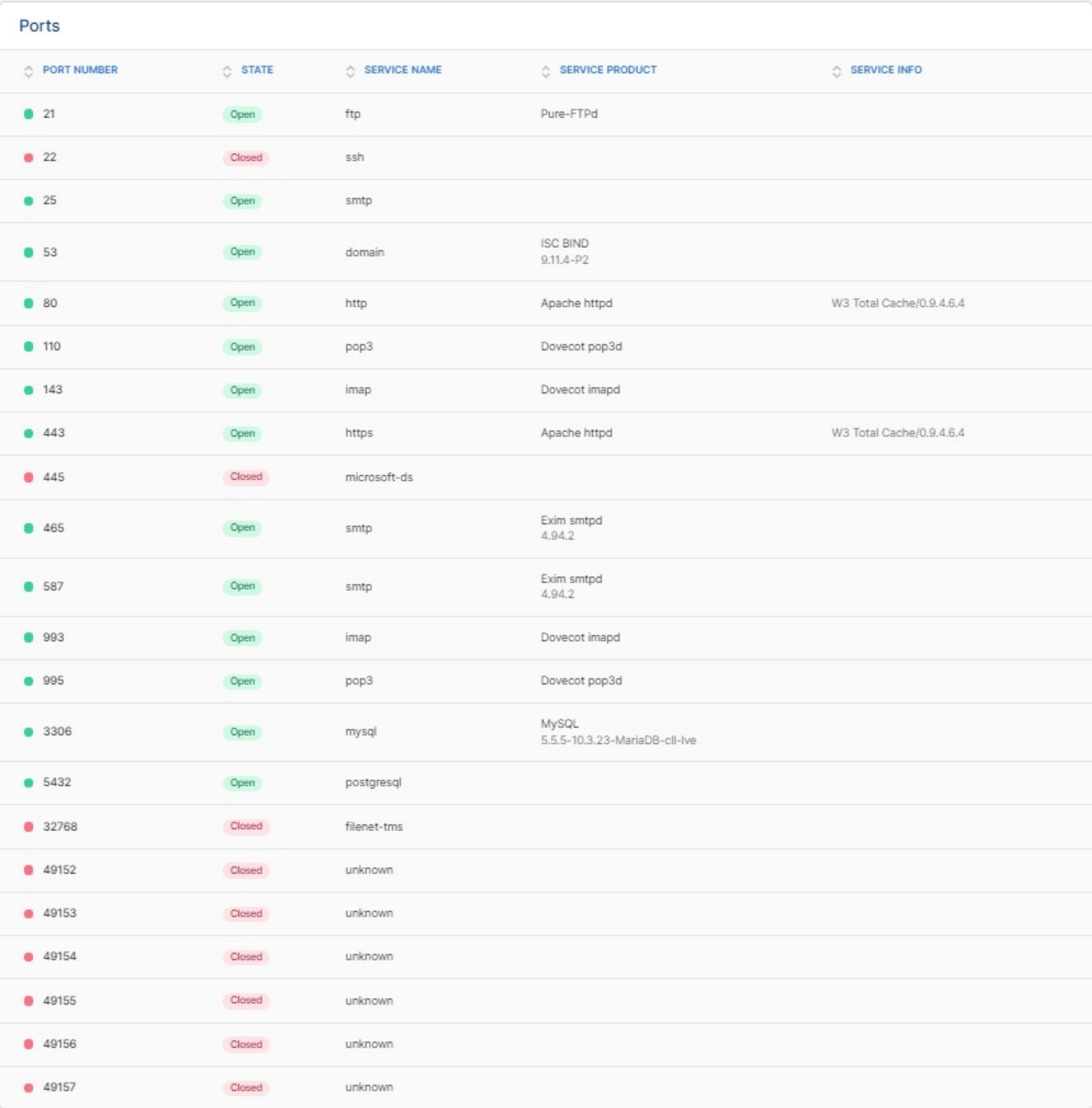


Scan report for "loadedwithstuff.co.uk"

Fast Scan (nmap -F loadedwithstuff.co.uk)

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-10 05:26 EST
Nmap scan report for loadedwithstuff.co.uk (68.66.247.187)
Host is up (0.077s latency).
rDNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com
Not shown: 72 filtered tcp ports (no-response), 7 filtered tcp ports (port-unreach)
PORT      STATE  SERVICE
21/tcp    open   ftp
22/tcp    closed ssh
53/tcp    open   domain
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
445/tcp   closed microsoft-ds
465/tcp   open   smtps
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
3306/tcp  open   mysql
5432/tcp  open   postgresql
32768/tcp closed filenet-tms
49152/tcp closed unknown
49153/tcp closed unknown
49154/tcp closed unknown
49155/tcp closed unknown
49156/tcp closed unknown
49157/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 1.97 seconds
```



Ports

PORT NUMBER	STATE	SERVICE NAME	SERVICE PRODUCT	SERVICE INFO
● 21	Open	ftp	Pure-FTPd	
● 22	Closed	ssh		
● 25	Open	smtp		
● 53	Open	domain	ISC BIND 9.11.4-P2	
● 80	Open	http	Apache httpd	W3 Total Cache/0.9.4.6.4
● 110	Open	pop3	Dovecot pop3d	
● 143	Open	imap	Dovecot imapd	
● 443	Open	https	Apache httpd	W3 Total Cache/0.9.4.6.4
● 445	Closed	microsoft-ds		
● 465	Open	smtp	Exim smtpd 4.94.2	
● 587	Open	smtp	Exim smtpd 4.94.2	
● 993	Open	imap	Dovecot imapd	
● 995	Open	pop3	Dovecot pop3d	
● 3306	Open	mysql	MySQL 5.5.5-10.3.23-MariaDB-cll-lve	
● 5432	Open	postgresql		
● 32768	Closed	filenet-tms		
● 49152	Closed	unknown		
● 49153	Closed	unknown		
● 49154	Closed	unknown		
● 49155	Closed	unknown		
● 49156	Closed	unknown		
● 49157	Closed	unknown		