Scanning Activity

nikto and nmap were mainly used to complete this activity. To get the host location, IPGeoLocation was used (maldevel, 2016). Some questions could not be answered in greater detail as the protection software used (immunify360-webshield) would ban my IP address while scans were still being completed.

Scan outputs:

nikto:

```
┌──(shan㉿kali)-[~]
└─$ nikto -host www.readmyblog.co.uk
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          68.66.247.187
+ Target Hostname:    www.readmyblog.co.uk
+ Target Port:        80
+ Start Time:         2022-02-19 21:58:08 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user
agent to protect against some forms of XSS
+ Server banner has changed from 'Apache' to 'imunify360-webshield/1.18' which may
suggest a WAF, load balancer or proxy is in place
```

Note: more content should appear after the last line of the results displayed above, however, I got banned shortly after that line was displayed in my terminal.

nmap:

```
┌──(shan㉿kali)-[~]
└─$ sudo nmap -O -v readmyblog.co.uk
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-19 22:24 GMT
Initiating Ping Scan at 22:24
Scanning readmyblog.co.uk (68.66.247.187) [4 ports]
Completed Ping Scan at 22:24, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:24
Completed Parallel DNS resolution of 1 host. at 22:24, 0.01s elapsed
Initiating SYN Stealth Scan at 22:24
Scanning readmyblog.co.uk (68.66.247.187) [1000 ports]
Discovered open port 110/tcp on 68.66.247.187
Discovered open port 143/tcp on 68.66.247.187
Discovered open port 587/tcp on 68.66.247.187
Discovered open port 53/tcp on 68.66.247.187
Discovered open port 995/tcp on 68.66.247.187
Discovered open port 993/tcp on 68.66.247.187
Discovered open port 3306/tcp on 68.66.247.187
Discovered open port 443/tcp on 68.66.247.187
Discovered open port 21/tcp on 68.66.247.187
Discovered open port 25/tcp on 68.66.247.187
Discovered open port 80/tcp on 68.66.247.187
Discovered open port 465/tcp on 68.66.247.187
Discovered open port 2525/tcp on 68.66.247.187
Discovered open port 5432/tcp on 68.66.247.187
Completed SYN Stealth Scan at 22:24, 3.66s elapsed (1000 total ports)
Initiating OS detection (try #1) against readmyblog.co.uk (68.66.247.187)
Retrying OS detection (try #2) against readmyblog.co.uk (68.66.247.187)
Nmap scan report for readmyblog.co.uk (68.66.247.187)
Host is up (0.013s latency).
DNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com
Not shown: 907 filtered tcp ports (no-response), 9 filtered tcp ports (port-
unreach), 70 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2525/tcp open  ms-v-worlds
3306/tcp open  mysql
5432/tcp open  postgresql
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X (88%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4.4
Aggressive OS guesses: Linux 3.10 - 3.12 (88%), Linux 4.4 (88%), Linux 4.9 (87%),
Linux 4.0 (86%), Linux 3.10 (85%), Linux 3.10 - 3.16 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 37.647 days (since Thu Jan 13 06:53:01 2022)
Network Distance: 20 hops
TCP Sequence Prediction: Difficulty=266 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.86 seconds
           Raw packets sent: 1974 (88.740KB) | Rcvd: 116 (6.352KB)
```

`ipgeolocation`:

```
┌──(shan㉿kali)-[~/IPGeoLocation]
└─$ ./ipgeolocation.py -t readmyblog.co.uk

IPGeolocation 2.0.4
```

```
--[ Retrieve IP Geolocation information from ip-api.com
--[ Copyright (c) 2015-2016 maldevel (@maldevel)
--[ ip-api.com service will automatically ban any IP addresses doing over 150
requests per minute.

Target: readmyblog.co.uk
IP: 68.66.247.187
ASN: AS55293 A2 Hosting, Inc.
City: Amsterdam
Country: Netherlands
Country Code: NL
ISP: A2 Hosting, Inc.
Latitude: 52.3676
Longtitude: 4.90414
Organization: A2 Hosting, Inc
Region Code: NH
Region Name: North Holland
Timezone: Europe/Amsterdam
Zip Code: 1012
Google Maps: http://www.google.com/maps/place/52.3676,4.90414/@52.3676,4.90414,16z
```

What Operating System does the web site utilise?

Certainly Linux, but it is not clear which distribution.

What web server software is it running?

Apache.

Is it running a CMS (Wordpress, Drupal, etc?)

Yes, it is using NucleusCMS.

What protection does it have (CDN, Proxy, Firewall?)

It uses imunify360-webshield, which acts as a firewall (imunify360, n.d.).

Where is it hosted?

It is hosted in the Netherlands.

Does it have any open ports?

Yes, namely: 21, 25, 53, 80, 110, 143, 443, 465, 587, 993, 995, 2525, 3306, and 5432.

Does the site have any known vulnerabilities?

Yes, there are some publicly disclosed vulnerabilities viewable on the Github issues page for NucleusCMS (Github, n.d.). These include 3 XSS vulnerabilities, 1 injection vulnerability, a file upload vulnerability, and one undisclosed vulnerability.

What versions of software is it using? Are these patched so that they are up to date?

The website is running an outdated version of NucleusCMS (v3.70, compared to the latest version which is 3.71). This software has not been patched on the website. That said, NucleusCMS itself hasn't been updated since 2018.

References

Github. (n.d.) Available from: https://github.com/NucleusCMS/NucleusCMS/issues [Accessed 19 February 2022]. imunify360. (n.d.) Imunify360. https://www.imunify360.com/ [Accessed 19 February 2022]. maldevel. (2016) IPGeoLocation. Available from: https://github.com/maldevel/IPGeoLocation [Accessed 19 February 2022].