

Unit 7 - Scanning Exercise and Collaborative Learning

Website: <https://loadedwithstuff.co.uk>

- The OS used for the website is the Red-Hat Enterprise Linux 7

```
Nmap scan report for loadedwithstuff.co.uk (68.66.247.187)
Host is up (0.20s latency).
Not shown: 900 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach), 84 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Pure-FTPd
25/tcp    open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
53/tcp    open  domain       ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp    open  http         Apache httpd (W3 Total Cache/0.9.4.6.4)
|_http-title: Site doesn't have a title (application/octet-stream).
|_http-server-header: imunify360-webshield/1.18
110/tcp   open  pop3         Dovecot pop3d
143/tcp   open  imap         Dovecot imapd
443/tcp   open  ssl/http     Apache httpd (W3 Total Cache/0.9.4.6.4)
```

- The web server used is an Apache web server:

```
curl -v http://loadedwithstuff.co.uk
* Trying 68.66.247.187:80 ...
* Connected to loadedwithstuff.co.uk (68.66.247.187) port 80 (#0)
> GET / HTTP/1.1
> Host: loadedwithstuff.co.uk
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 301 Moved Permanently
< Date: Sun, 16 Jan 2022 08:51:06 GMT
< Server: Apache
< X-Powered-By: PHP/7.3.33
< Strict-Transport-Security: max-age=63072000; includeSubDomains
< X-Frame-Options: SAMEORIGIN
< X-Content-Type-Options: nosniff
< Upgrade: h2,h2c
< Connection: Upgrade
< Location: https://loadedwithstuff.co.uk/
< Content-Length: 0
< Content-Type: text/html; charset=UTF-8
<
* Connection #0 to host loadedwithstuff.co.uk left intact
```

- In the screenshot below, it is visible that CMS (Content Management System) is present

```

$ whatweb loadedwithstuff.co.uk
http://loadedwithstuff.co.uk [301 Moved Permanently] Apache, Country[UNITED STATES][US], HTTPServer[Apache], IP[68.66.247.187], PHP[7.3.3], RedirectLocation[https://loadedwithstuff.co.uk/], Strict-Transport-Security[max-age=63072000; includeSubDomains], UncommonHeaders[x-content-type-options,upgrade], X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/7.3.33]
https://loadedwithstuff.co.uk/ [403 Forbidden] Apache, Bootstrap, Cookies[lcsid], Country[UNITED STATES][US], Email[sales@example.com,sales@loadedwithstuff.co.uk], HTML5, HTTPServer[Apache], IP[68.66.247.187], JQuery[3.4.1], MetaGenerator[Loaded Commerce Community Edition v6.6], PHP[7.3.33], Script[javascript,text/javascript], Strict-Transport-Security[max-age=63072000; includeSubDomains], Title[Loaded Commerce 6.6 - Powerful Ecommerce Shopping Cart], UncommonHeaders[x-content-type-options,upgrade], X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/7.3.33]

```

- The scanning tools used, the screenshot below shows that Immunity360 was used and this combines an Intrusion Prevention/detection system , a web application firewall and patch management components.

```

$ nikto -h loadedwithstuff.co.uk
- Nikto v2.1.6

+ Target IP: 68.66.247.187
+ Target Hostname: loadedwithstuff.co.uk
+ Target Port: 80
+ Start Time: 2022-01-15 16:26:57 (GMT2)

+ Server: immunity360-webshield/1.18
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

```

- The website was hosted in Amsterdam

To find out where a website is hosted enter the URL address:

It is hosted by: A2 Hosting, Inc.

WHOIS information: [Click here](#)

Organization name: A2 Hosting, Inc

IP address: 68.66.247.187

AS(autonomous system) number and organization: AS55293 A2 Hosting, Inc.

AS name: A2HOSTING

Reverse DNS of the IP: 68.66.247.187.static.a2webhosting.com

City: Amsterdam

Country: Netherlands

- A total of 1000 ports were open

```
└─$ nmap -v -A loadedwithstuff.co.uk
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-14 23:47 SAST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:47
Completed NSE at 23:47, 0.00s elapsed
Initiating NSE at 23:47
Completed NSE at 23:47, 0.00s elapsed
Initiating NSE at 23:47
Completed NSE at 23:47, 0.00s elapsed
Initiating Ping Scan at 23:48
Scanning loadedwithstuff.co.uk (68.66.247.187) [2 ports]
Completed Ping Scan at 23:48, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:48
Completed Parallel DNS resolution of 1 host. at 23:48, 0.01s elapsed
Initiating Connect Scan at 23:48
Scanning loadedwithstuff.co.uk (68.66.247.187) [1000 ports]
Discovered open port 80/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 3306/tcp on 68.66.247.187
Discovered open port 25/tcp on 68.66.247.187
Discovered open port 993/tcp on 68.66.247.187
Discovered open port 143/tcp on 68.66.247.187
Discovered open port 110/tcp on 68.66.247.187
Discovered open port 21/tcp on 68.66.247.187
Discovered open port 995/tcp on 68.66.247.187
Discovered open port 443/tcp on 68.66.247.187
Discovered open port 465/tcp on 68.66.247.187
Discovered open port 5432/tcp on 68.66.247.187
Discovered open port 2525/tcp on 68.66.247.187
Completed Connect Scan at 23:48, 8.96s elapsed (1000 total ports)
```

- The version of software used are below;

Jquery v.3.4.1