

Practical Activity – Scanning Exercise

Brief

Perform scans against your assigned website using the tools available in [Kali Linux](#).

Answer as many of the following questions as you can:

- What Operating System does the web site utilise?
- What web server software is it running?
- Is it running a CMS (Wordpress, Drupal, etc?)
- What protection does it have (CDN, Proxy, Firewall?)
- Where is it hosted?
- Does it have any open ports?
- Does the site have any known vulnerabilities?
- What versions of software is it using? Are these patched so that they are up to date?

The following results were conducted against www.staffmatters.co.uk.

Results

What Operating System does the web site utilise?

- I used **nmap -O -sV** to scan for OS guesses:

```

root@kali:~# nmap -O -sV www.staffmatters.co.uk
Command 'nmap' not found, did you mean:
  command 'nama' from deb nama
  command 'pamp' from deb paml
  command 'nmap' from deb nmap
  command 'nam' from deb nam
  command 'wamp' from deb python3-autobahn
Try: apt install <deb name>

root@kali:~# nmap -O -sV www.staffmatters.co.uk
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 16:56 EST
Stats: 0:01:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 16:57 (0:00:14 remaining)
Stats: 0:03:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.61% done; ETC: 16:59 (0:00:00 remaining)
Nmap scan report for www.staffmatters.co.uk (68.66.247.187)
Host is up (0.014s latency).
rDNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  tcpwrapped
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)
110/tcp   open  tcpwrapped
143/tcp   open  tcpwrapped
443/tcp   open  ssl/https  imunify360-webshield/1.18
587/tcp   open  tcpwrapped
993/tcp   open  tcpwrapped
995/tcp   open  tcpwrapped
3306/tcp  open  tcpwrapped
5060/tcp  open  sip?
8080/tcp  open  http-proxy
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-s
service :
SF-Port8080-TCP:V=7.92XI=7XD=1/24Time=61EF209BXP=x86_64-pc-linux-gnuXr(Fo
SF:ur0hFourRequest,CC,"HTTP/1.1\x20403\x20Blocked\x20by\x20Bitdefender\r
SF:Content-Type:\x20text/html\r\nPragma:\x20no-cache\r\nCache-Control:\x2
SF:0no-store,\x20no-cache,\x20must-revalidate,\x20max-age=0\r\nExpires:\x2
SF:0Tue,\x2001\x20Jan\x201971\x2002:00:00\x20GMT\r\nContent-Length:\x200\r
SF:\n\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge[general purpose]switch
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%), Bay Networks embedded (88%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (88%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 200.63 seconds

root@kali:~#

```

The tool correctly detected the source operating hosted by Oracle VirtualBox which is correct given that Kali Linux was used inside VirtualBox, but incorrect because the tool did not detect the operating system of the website's host.

Using the **-PN** option with **nmap** ("no ping") the results are slightly different:

```

L-# nmap -O -PN 68.66.247.187
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 17:50 EST
Nmap scan report for 68.66.247.187.static.a2webhosting.com (68.66.247.187)
Host is up (0.020s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
5060/tcp  open  sip
8080/tcp  open  http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP phone|bridge
Running (JUST GUESSING): Cisco embedded (89%), Oracle Virtualbox (86%)
OS CPE: cpe:/h:cisco:unified_ip_phone_7912 cpe:/o:oracle:virtualbox
Aggressive OS guesses: Cisco IP Phone 7912-series (89%), Oracle Virtualbox (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.89 seconds

```

Now the operating system guess is Cisco Embedded.

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

- I used the tool **wpscan -url -random-user-agent**

```
(root@kali)-[~]
# wpscan --url www.staffmatters.co.uk --random-user-agent
```

WordPress Security Scanner by the WPScan Team
Version 3.8.20
Sponsored by Automattic - <https://automattic.com/>
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

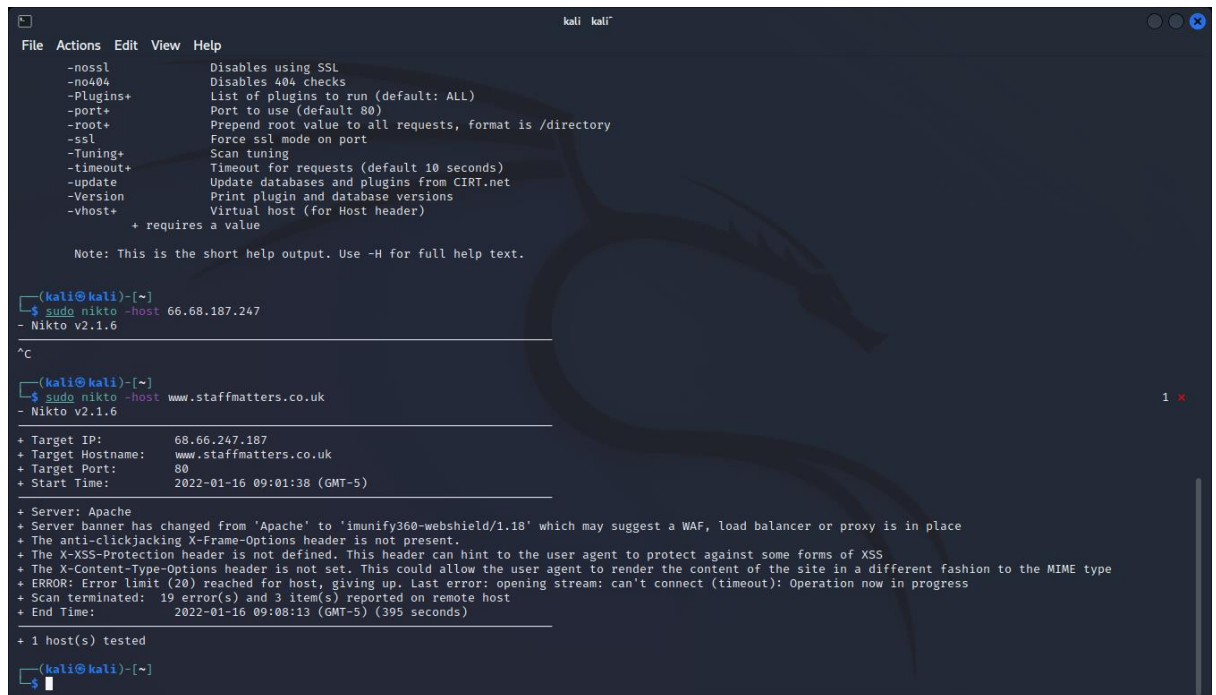
```
[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]Y
[i] Updating the Database ...
[i] Update completed.
```

Scan Aborted: The remote website is up, but does not seem to be running WordPress.

- I used the tool **killshot** (<https://www.geeksforgeeks.org/killshot-information-gathering-tool-in-kali-linux/>) and selected the option “{1} Web Technologies”

```
Basic WhatWeb Information :: http://staffmatters.co.uk [200 OK]
Bootstrap[3.3.6,3.3.7],
Cookies[cl-bypass-cache],
```


- I used the tool **nikto**



```

kali kali
File Actions Edit View Help
-nossl Disables using SSL
-no404 Disables 404 checks
-Plugins+ List of plugins to run (default: ALL)
-port+ Port to use (default 80)
-root+ Prepend root value to all requests, format is /directory
-ssl Force ssl mode on port
-Tuning+ Scan tuning
-timeout+ Timeout for requests (default 10 seconds)
-update Update databases and plugins from CIRT.net
-Version Print plugin and database versions
-vhost+ Virtual host (for Host header)
+ requires a value

Note: This is the short help output. Use -H for full help text.

(kali@kali)-[~]
└─$ sudo nikto -host 66.68.187.247
- Nikto v2.1.6

^C

(kali@kali)-[~]
└─$ sudo nikto -host www.staffmatters.co.uk
- Nikto v2.1.6

+ Target IP: 66.68.247.187
+ Target Hostname: www.staffmatters.co.uk
+ Target Port: 80
+ Start Time: 2022-01-16 09:01:38 (GMT-5)

+ Server: Apache
+ Server banner has changed from 'Apache' to 'imunify360-webshield/1.18' which may suggest a WAF, load balancer or proxy is in place
+ 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
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Operation now in progress
+ Scan terminated: 19 error(s) and 3 item(s) reported on remote host
+ End Time: 2022-01-16 09:08:13 (GMT-5) (395 seconds)

+ 1 host(s) tested

(kali@kali)-[~]
└─$
  
```

- I used the tool **wafW00f**



```

wafw00f www.staffmatters.co.uk

      { WOOF! }

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error

~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.staffmatters.co.uk
[+] Generic Detection results:
[*] The site https://www.staffmatters.co.uk seems to be behind a WAF or some sort of security solution
[~] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to a SQL injection attack is "403"
[~] Number of requests: 7
  
```

The site is potentially hosted behind a Web Application Firewall, but the tool could not correctly identify it.

Where is it hosted?

- I used the tool **WHOIS**

```

L# whois staffmatters.co.uk

Domain name:
  staffmatters.co.uk

Data validation:
  Nominet was not able to match the registrant's name and/or address against a 3rd party source on 21-Oct-2021

Registrar:
  eNom LLC [Tag = ENOM]
  URL: http://www.enom.com

Relevant dates:
  Registered on: 21-Oct-2021
  Expiry date: 21-Oct-2022
  Last updated: 21-Oct-2021

Registration status:
  Registered until expiry date.

Name servers:
  ns1.a2hosting.com
  ns2.a2hosting.com
  ns3.a2hosting.com
  ns4.a2hosting.com

WHOIS lookup made at 23:51:24 20-Jan-2022

--
This WHOIS information is provided for free by Nominet UK the central registry
for .uk domain names. This information and the .uk WHOIS are:

Copyright Nominet UK 1996 - 2022.
```

Nominet hold registration data for the hosted site but does not show the hosting location.

- I used the tool **IPGeolocation**

```

L# ./ipgeolocation.py -t 68.66.247.187

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

Target: 68.66.247.187
IP: 68.66.247.187
ASN: AS55293 A2 Hosting, Inc.
City: Amsterdam
Country: Netherlands
Country Code: NL
ISP: A2 Hosting, Inc.
Latitude: 52.3676
Longitude: 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
```

Does it have any open ports?

- I used the tool **ssllscan** to scan for SSL ports

```

root kali ~,killshot
File Actions Edit View Help
root@kali:~/killshot# sslscan www.staffmatters.co.uk
Version: 2.0.11-static
OpenSSL 1.1.1n-dev xx XXX xxxx

Connected to 100.96.1.229

Testing SSL server www.staffmatters.co.uk on port 443 using SNI name www.staffmatters.co.uk

SSL/TLS Protocols:
SSLv2 disabled
SSLv3 disabled
TLSv1.0 disabled
TLSv1.1 disabled
TLSv1.2 enabled
TLSv1.3 enabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):
Preferred TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253
Accepted TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253
Accepted TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253
Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve 25519 DHE 253

Server Key Exchange Group(s):
TLSv1.3 128 bits secp256r1 (NIST P-256)
TLSv1.3 192 bits secp384r1 (NIST P-384)
TLSv1.3 260 bits secp521r1 (NIST P-521)
TLSv1.3 128 bits x25519
TLSv1.3 224 bits x448
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 192 bits secp384r1 (NIST P-384)
TLSv1.2 260 bits secp521r1 (NIST P-521)
TLSv1.2 128 bits x25519
TLSv1.2 224 bits x448

SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject: staffmatters.co.uk
AltNames: DNS:staffmatters.co.uk, DNS:autodiscover.staffmatters.co.uk, DNS:cpanel.staffmatters.co.uk, DNS:cpcalendars.staffmatters.co.uk, DNS:cpcontacts.staffmatters.co.uk, DNS:mail.staffmatters.co.uk, DNS:webdisk.staffmatters.co.uk, DNS:webmail.staffmatters.co.uk, DNS:www.staffmatters.co.uk
Issuer: cPanel, Inc. Certification Authority

Not valid before: Jan 14 00:00:00 2022 GMT
Not valid after: Apr 14 23:59:59 2022 GMT

root@kali:~/killshot#

```

- I used the tool **Dmitry**


```

dmitry www.staffmatters.co.uk
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:100.96.1.229
HostName:www.staffmatters.co.uk

Gathered Inet-whois information for 100.96.1.229

inetnum:      98.158.239.0 - 101.55.255.255
netname:      NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:        IPv4 address block not managed by the RIPE NCC
remarks:
remarks:
remarks:      For registration information,
remarks:      you can consult the following sources:
remarks:
remarks:      IANA
remarks:      http://www.iana.org/assignments/ipv4-address-space
remarks:      http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:      http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:      AFRINIC (Africa)
remarks:      http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:      APNIC (Asia Pacific)
remarks:      http://www.apnic.net/ whois.apnic.net
remarks:
remarks:      ARIN (Northern America)
remarks:      http://www.arin.net/ whois.arin.net
remarks:
remarks:      LACNIC (Latin America and the Caribbean)
remarks:      http://www.lacnic.net/ whois.lacnic.net
remarks:
country:      EU # Country is really world wide
last-modified: 2021-03-29T13:41:55Z
source:        RIPE

role:          Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source:        RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.102.2 (WAGYU)

Gathered Inic-whois information for staffmatters.co.uk

Gathered Netcraft information for www.staffmatters.co.uk

Retrieving Netcraft.com information for www.staffmatters.co.uk
Netcraft.com Information gathered

Gathered Subdomain information for staffmatters.co.uk

Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 possible subdomain(s) for host staffmatters.co.uk, Searched 0 pages containing 0 results

Gathered E-Mail information for staffmatters.co.uk

Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host staffmatters.co.uk, Searched 0 pages containing 0 results

Gathered TCP Port information for 100.96.1.229

Port      State
1/tcp     open
2/tcp     open
3/tcp     open
4/tcp     open
5/tcp     open
6/tcp     open
7/tcp     open
8/tcp     open
9/tcp     open
10/tcp    open
11/tcp    open
12/tcp    open
13/tcp    open
14/tcp    open
15/tcp    open
16/tcp    open
17/tcp    open
18/tcp    open
19/tcp    open
20/tcp    open
21/tcp    open
19/tcp    open 60/tcp    open 110/tcp    open
20/tcp    open 61/tcp    open 111/tcp    open
21/tcp    open 62/tcp    open 112/tcp    open
22/tcp    open 63/tcp    open 113/tcp    open
23/tcp    open 64/tcp    open 114/tcp    open
24/tcp    open 65/tcp    open 115/tcp    open
25/tcp    open 66/tcp    open 116/tcp    open
26/tcp    open 67/tcp    open 117/tcp    open
27/tcp    open 68/tcp    open 118/tcp    open
28/tcp    open 69/tcp    open 119/tcp    open
29/tcp    open 70/tcp    open 120/tcp    open
30/tcp    open 71/tcp    open 121/tcp    open
31/tcp    open 72/tcp    open 122/tcp    open
32/tcp    open 73/tcp    open 123/tcp    open
33/tcp    open 74/tcp    open 124/tcp    open
34/tcp    open 75/tcp    open 125/tcp    open
35/tcp    open 76/tcp    open 126/tcp    open
36/tcp    open 77/tcp    open 127/tcp    open
37/tcp    open 78/tcp    open 128/tcp    open
38/tcp    open 79/tcp    open 129/tcp    open
39/tcp    open 80/tcp    open 130/tcp    open
40/tcp    open 81/tcp    open 131/tcp    open
41/tcp    open 82/tcp    open 132/tcp    open
42/tcp    open 83/tcp    open 133/tcp    open
43/tcp    open 84/tcp    open 134/tcp    open
44/tcp    open 85/tcp    open 135/tcp    open
45/tcp    open 86/tcp    open 136/tcp    open
46/tcp    open 87/tcp    open 137/tcp    open
47/tcp    open 88/tcp    open 138/tcp    open
48/tcp    open 89/tcp    open 139/tcp    open
49/tcp    open 90/tcp    open 140/tcp    open
50/tcp    open 91/tcp    open 141/tcp    open
51/tcp    open 92/tcp    open 142/tcp    open
52/tcp    open 93/tcp    open 143/tcp    open
54/tcp    open 94/tcp    open 144/tcp    open
55/tcp    open 95/tcp    open 145/tcp    open
56/tcp    open 96/tcp    open 146/tcp    open
57/tcp    open 97/tcp    open 147/tcp    open
58/tcp    open 98/tcp    open 148/tcp    open
59/tcp    open 99/tcp    open 149/tcp    open
100/tcp   open
101/tcp   open
102/tcp   open
103/tcp   open
104/tcp   open
105/tcp   open
106/tcp   open
107/tcp   open
108/tcp   open
109/tcp   open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed

```

- I used **nmap** to scan HTTP ports

```

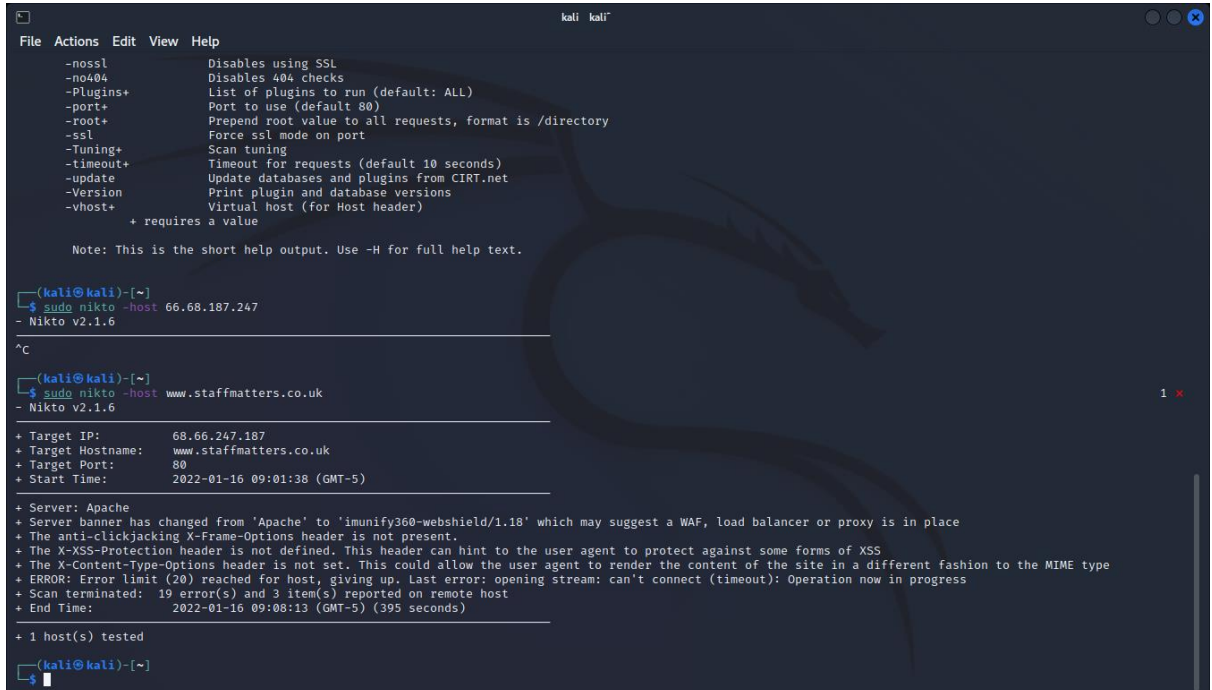
(root@kali)-[~]
# nmap -F www.staffmatters.co.uk
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-23 06:23 EST
Nmap scan report for www.staffmatters.co.uk (68.66.247.187)
Host is up (0.023s latency).
rDNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com
Not shown: 89 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
5060/tcp  open  sip
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 22.09 seconds

```


Does the site have any known vulnerabilities?

- I used the tool **nikto**



```
kali kali~  
File Actions Edit View Help  
-noss! Disables using SSL  
-no404 Disables 404 checks  
-Plugins+ List of plugins to run (default: ALL)  
-port+ Port to use (default 80)  
-root+ Prepend root value to all requests, format is /directory  
-ssl Force ssl mode on port  
-Tuning+ Scan tuning  
-timeout+ Timeout for requests (default 10 seconds)  
-update Update databases and plugins from CIRT.net  
-Version Print plugin and database versions  
-vhost+ Virtual host (for Host header)  
+ requires a value  
  
Note: This is the short help output. Use -H for full help text.  
  
(kali@kali)-[~]  
$ sudo nikto -host 66.68.187.247  
- Nikto v2.1.6  
^C  
  
(kali@kali)-[~]  
$ sudo nikto -host www.staffmatters.co.uk  
- Nikto v2.1.6  
  
+ Target IP: 66.66.247.187  
+ Target Hostname: www.staffmatters.co.uk  
+ Target Port: 80  
+ Start Time: 2022-01-16 09:01:38 (GMT-5)  
  
+ Server: Apache  
+ Server banner has changed from 'Apache' to 'imunify360-webshield/1.18' which may suggest a WAF, load balancer or proxy is in place  
+ 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  
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Operation now in progress  
+ Scan terminated: 19 error(s) and 3 item(s) reported on remote host  
+ End Time: 2022-01-16 09:08:13 (GMT-5) (395 seconds)  
  
+ 1 host(s) tested  
  
(kali@kali)-[~]  
$
```

- The response message contains “X-XSS-Protection” header
- The response message contains “X-Content-Type-Options”

- CVE vulnerabilities were provided by a fellow team member:

[Orangehrm : Security vulnerabilities \(cvedetails.com\)](https://www.cvedetails.com/)

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

I did not find a way to scan for software installations on the server