

Unit 4 Scanning Activity

Kali Linux	nmap	whatweb
wpscan	Joomscan	curl
whois	dig	Nikto

Perform scans against your assigned website using the tools available in Kali Linux.

Question One

Command Used: `nmap -O ginandjuice.shop -O` Enables OS detection

What Operating System does the website utilise?

OS detection in Nmap relies on fingerprinting network responses from the target.

Nmap requires at least one open and one closed port to get a reliable OS guess.

The scan shows a warning that OS detection may be unreliable due to not meeting these conditions.

Because of this limitation, Nmap seems to be guessing the OS of the scanning system instead of the actual server.

```
(kali㉿kali)-[~]
$ nmap -O ginandjuice.shop
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-04 17:25 EST
Nmap scan report for ginandjuice.shop (34.249.203.140)
Host is up (0.0078s latency).
Other addresses for ginandjuice.shop (not scanned): 34.246.169.176
rDNS record for 34.249.203.140: ec2-34-249-203-140.eu-west-1.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (94%)
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 10.04 seconds
```

Question Two

Command Used: `nmap -sV ginandjuice.shop -sV` Enables service version detection

Command Used: `whatweb ginandjuice.shop`

Command Used: `nikto -h ginandjuice.shop -h` Specifies the host to scan

What web server software is it running?

The server is running AWS Elastic Load Balancer (awselb/2.0), using AWS ALB to distribute traffic to multiple backend instances. The backend could be running any OS (Linux or Windows), but AWS ELB masks it.

Open ports detected:

- Port 80 (HTTP) → Running AWS ELB.
- Port 443 (HTTPS) → Running SSL/TLS.

Identified security issues:

- X-Frame-Options header missing → Website could be vulnerable to clickjacking attacks.
- X-Content-Type-Options header missing → Could allow MIME-type confusion attacks.

```
(kali㉿kali)-[~]
└─$ nmap -sV ginandjuice.shop
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-04 17:31 EST
Nmap scan report for ginandjuice.shop (34.246.169.176)
Host is up (0.0031s latency).
Other addresses for ginandjuice.shop (not scanned): 34.249.203.140
rDNS record for 34.246.169.176: ec2-34-246-169-176.eu-west-1.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         awselb/2.0
443/tcp   open  ssl/https
```

```
(kali㉿kali)-[~]
└─$ whatweb ginandjuice.shop
http://ginandjuice.shop [302 Found] Country[UNITED STATES][US], HTTPServer[awselb/2.0], IP[34.249.203.140], RedirectLocation[https://ginandjuice.shop:443/], Title[302 Found]
https://ginandjuice.shop/ [200 OK] Cookies[AWSALB,AWSALBCORS,session], Country[UNITED STATES][US], HTML5, HttpOnly[session], IP[34.249.203.140], Script[text/javascript], Title[Home - Gin & Juice Shop], UncommonHeaders[x-backend], X-Backend[df6723c9-42b6-45b3-b0f4-446693d6bbca], X-Frame-Options[SAMEORIGIN]
```

```
(kali㉿kali)-[~]
└─$ nikto -h ginandjuice.shop
- Nikto v2.5.0

+ Multiple IPs found: 34.249.203.140, 34.246.169.176
+ Target IP: 34.249.203.140
+ Target Hostname: ginandjuice.shop
+ Target Port: 80
+ Start Time: 2025-03-04 17:33:51 (GMT-5)

+ Server: awselb/2.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://ginandjuice.shop:443/
```

Question Three

Command Used:	<code>wpscan -url ginandjuice.shop --enumerate ap</code>	<code>--enumerate ap</code>	Tries to list all installed plugins on the site.
Command Used:	<code>joomscan -u ginandjuice.shop</code>	<code>-u</code>	Specifies the host to scan

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

The scan detected that ginandjuice.shop is NOT running WordPress.

The scan confirmed that ginandjuice.shop is NOT running Joomla.

WhatWeb results showed that the server is using AWS Elastic Load Balancer (awselb/2.0), but did not indicate a known CMS.

Nikto results showed missing security headers but did not indicate a CMS presence.

```
(kali㉿kali)-[~]
$ wpscan --url ginandjuice.shop --enumerate ap

WordPress Security Scanner by the WPScan Team
Version 3.8.27
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

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

Question Four

Command Used:	<code>nmap --script https-waf-detect ginandjuie.shop</code>	<code>--script https-waf-detect</code>	Uses the https-waf-detect script
Command Used:	<code>curl -I ginandjuice.shop</code>	<code>-I</code>	Fetches only the HTTP headers

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

No explicit Web Application Firewall (WAF) was detected.

Only HTTP (port 80) and HTTPS (port 443) are open.

No additional security mechanisms were identified.

The AWS Elastic Load Balancer is handling incoming traffic.

The actual backend server OS is still unknown, as AWS ELB masks it.

```
(kali㉿kali)-[~]  
$ curl -I ginandjuice.shop  
HTTP/1.1 302 Moved Temporarily  
Server: awselb/2.0  
Date: Tue, 04 Mar 2025 22:48:26 GMT  
Content-Type: text/html  
Content-Length: 110  
Connection: keep-alive  
Location: https://ginandjuice.shop:443/
```

```
(kali㉿kali)-[~]  
$ nmap --script http-waf-detect ginandjuice.shop  
  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-04 17:45 EST  
Nmap scan report for ginandjuice.shop (34.246.169.176)  
Host is up (0.0032s latency).  
Other addresses for ginandjuice.shop (not scanned): 34.249.203.140  
rDNS record for 34.246.169.176: ec2-34-246-169-176.eu-west-1.compute.amazonaws.com  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 5.41 seconds
```


Question Five

Command Used:	whois 43.249.203.140		
Command Used:	dig +short ginandjuice.shop	+short	Returns only the direct answer
Command Used:	curl https://ipinfo.io/34.246.169.176		
Command Used:	curl https://ipinfo.io/34.249.203.140		

Where is it hosted?

Hosting Provider:

- Amazon Web Services (AWS)
- Amazon Data Services Ireland Limited (ADSIL)

Data centre Location:

- Region: AWS eu-west-1
- City: Dublin, Ireland
- Country: Ireland (IE)

IP Addresses Associated with the Website:

- 34.246.169.176
- 34.249.203.140

Network & ASN Information:

- ASN (Autonomous System Number): AS16509
- Network Range: 34.248.0.0 - 34.255.255.255
- Service Type: AWS Elastic Compute Cloud

```
NetRange: 34.248.0.0 - 34.255.255.255
CIDR: 34.248.0.0/13
NetName: AMAZON-DUB
NetHandle: NET-34-248-0-0-1
Parent: AT-88-Z (NET-34-192-0-0-1)
NetType: Reallocated
OriginAS: AS16509
Organization: Amazon Data Services Ireland Limited (ADSIL-1)
RegDate: 2016-11-30
Updated: 2016-11-30
Ref: https://rdap.arin.net/registry/ip/34.248.0.0

OrgName: Amazon Data Services Ireland Limited
OrgId: ADSIL-1
Address: Unit 4033, Citywest Avenue Citywest Business Park
City: Dublin
StateProv: D24
PostalCode:
Country: IE
RegDate: 2014-07-18
Updated: 2014-07-18
Ref: https://rdap.arin.net/registry/entity/ADSIL-1
```

```
(kali㉿kali)-[~]
$ dig +short ginandjuice.shop

34.246.169.176
34.249.203.140

(kali㉿kali)-[~]
$ curl https://ipinfo.io/34.246.169.176
{
  "ip": "34.246.169.176",
  "hostname": "ec2-34-246-169-176.eu-west-1.compute.amazonaws.com",
  "city": "Dublin",
  "region": "Leinster",
  "country": "IE",
  "loc": "53.3331,-6.2489",
  "org": "AS16509 Amazon.com, Inc.",
  "postal": "D02",
  "timezone": "Europe/Dublin",
  "readme": "https://ipinfo.io/missingauth"
}

(kali㉿kali)-[~]
$ curl https://ipinfo.io/34.249.203.140
{
  "ip": "34.249.203.140",
  "hostname": "ec2-34-249-203-140.eu-west-1.compute.amazonaws.com",
  "city": "Dublin",
  "region": "Leinster",
  "country": "IE",
  "loc": "53.3331,-6.2489",
  "org": "AS16509 Amazon.com, Inc.",
  "postal": "D02",
  "timezone": "Europe/Dublin",
  "readme": "https://ipinfo.io/missingauth"
}
```

Question Six

Command Used: `nmap -p- ginandjuice.shop` `-p-` Scans all 65,535 TCP ports

Does it have any open ports? Which did you expect to be open?

Only two ports are open:

- Port 80 (HTTP) → Web server
- Port 443 (HTTPS) → Secure web traffic

The website is strictly limited to web services, meaning no other exposed services like SSH (22), FTP (21), or databases (3306, 5432).

AWS Security Groups are actively blocking all non-web traffic.

No misconfigured or open high-risk ports detected

```
(kali㉿kali)-[~]
└─$ nmap -p- ginandjuice.shop
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-04 17:53 EST
Nmap scan report for ginandjuice.shop (34.246.169.176)
Host is up (0.032s latency).
Other addresses for ginandjuice.shop (not scanned): 34.249.203.140
rDNS record for 34.246.169.176: ec2-34-246-169-176.eu-west-1.compute.amazonaws.com
Not shown: 54054 filtered tcp ports (net-unreach), 11479 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 53.71 seconds
```

Question Seven

Command Used: Nmap --script vuln ginandjuice.shop --script vuln
Command Used: Nikto -h ginandjuice.shop -h

Uses Nmap's vulnerability detection scripts
Specifies the target hostname

Does the site have any known vulnerabilities?

No stored or DOM-based XSS vulnerabilities were detected.

No CSRF vulnerabilities were found in automated testing.

Potential CSRF vulnerabilities were identified in various forms:

- /catalog/product/stock
- /catalog/cart
- /catalog
- /blog

These forms may be susceptible to CSRF attacks, meaning an attacker could potentially trick a user into submitting unintended actions.

Security headers are missing, specifically:

- X-Frame-Options is not set → The site is potentially vulnerable to Clickjacking attacks.
- X-Content-Type-Options is not set → This could allow MIME-type confusion attacks.

```
(kali@kali)-[~]
$ nmap --script vuln ginandjuice.shop
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-04 18:04 EST
Nmap scan report for ginandjuice.shop (34.249.203.140)
Host is up (0.0042s latency).
Other addresses for ginandjuice.shop (not scanned): 34.246.169.176
rDNS record for 34.249.203.140: ec2-34-249-203-140.eu-west-1.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp   open  https
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf:
|_Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=ginandjuice.shop
|_Found the following possible CSRF vulnerabilities:

Path: https://ginandjuice.shop:443/catalog/product?productId=2
Form id: stockcheckform
Form action: /catalog/product/stock

Path: https://ginandjuice.shop:443/catalog/product?productId=2
Form id: addtocartform
Form action: /catalog/cart

Path: https://ginandjuice.shop:443/catalog/product?productId=1
Form id: stockcheckform
Form action: /catalog/product/stock

Path: https://ginandjuice.shop:443/catalog/product?productId=1
Form id: addtocartform
Form action: /catalog/cart

Path: https://ginandjuice.shop:443/catalog
Form id: searchbar
Form action: /catalog

Path: https://ginandjuice.shop:443/blog
Form id:
Form action: /blog/

Path: https://ginandjuice.shop:443/catalog/product?productId=3
Form id: stockcheckform
Form action: /catalog/product/stock

Path: https://ginandjuice.shop:443/catalog/product?productId=3
Form id: addtocartform
Form action: /catalog/cart

Nmap done: 1 IP address (1 host up) scanned in 169.65 seconds
```

```
(kali@kali)-[~]
$ nikto -h ginandjuice.shop
- Nikto v2.5.0

+ Multiple IPs found: 34.249.203.140, 34.246.169.176
+ Target IP: 34.249.203.140
+ Target Hostname: ginandjuice.shop
+ Target Port: 80
+ Start Time: 2025-03-04 18:07:29 (GMT-5)

+ Server: awselb/2.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://ginandjuice.shop:443/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Question Eight

Command Used: `whatweb ginandjuice.shop`

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

Web Server:

- awselb/2.0 (AWS Elastic Load Balancer)
- This is not a traditional web server (like Apache or Nginx) but a load balancer used in AWS to distribute traffic.

Backend Technology:

- X-Backend header present → Suggests a backend server behind AWS ELB, but its software/version is unknown.
- HTML5 is used, indicating a modern web application.

Security Headers Detected:

- X-Frame-Options: SAMEORIGIN → Protects against Clickjacking attacks.
- Cookies (AWSALB, AWSALBCORS) → Indicate AWS session management.

```
(kali@kali)-[~]
$ whatweb ginandjuice.shop
http://ginandjuice.shop [302 Found] Country[UNITED STATES][US], HTTPServer[awselb/2.0], IP[34.249.203.140], RedirectLocation[https://ginandjuice.shop:443/], Title[302 Found]
https://ginandjuice.shop/ [200 OK] Cookies[AWSALB,AWSALBCORS,session], Country[UNITED STATES][US], HTML5, HttpOnly[session], IP[34.246.169.176], Script[text/javascript], Title[Home - Gin & Juice Shop], UncommonHeaders[x-backend], X-Backend[df6723c9-42b6-45b3-b0f4-446693d6bbca], X-Frame-Options[SAMEORIGIN]
```


References

Kali Linux. (no date). *Kali Linux – Penetration Testing and Ethical Hacking Linux Distribution*. Available at: <https://www.kali.org/> [Accessed 3 Mar. 2025].

Microsoft. (no date). *Whois v1.20*. Microsoft Learn. Available at: <https://learn.microsoft.com/en-us/sysinternals/downloads/whois#introduction> [Accessed 3 Mar. 2025].

Microsoft. (no date). *nslookup*. Microsoft Learn. Available at: <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup> [Accessed 3 Mar. 2025].

Microsoft. (no date). *tracert*. Microsoft Learn. Available at: <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/tracert> [Accessed 3 Mar. 2025].

Whois.com. (no date). *WHOIS Lookup*. Available at: <https://www.whois.com/whois/> [Accessed 3 Mar. 2025].