INTRODUCTION:

For this part of the practical, the aim was to perform penetration testing on 2 websites, one being bbc.co.uk and the second one I chose was a website for a codelab called Google Gruyere. The purpose was to gather as much information as possible using resources ranging from a myriad of search engines, to using tools such as nmap, nslookup, whois, robtex, etc.

1. **bbc.co.uk**

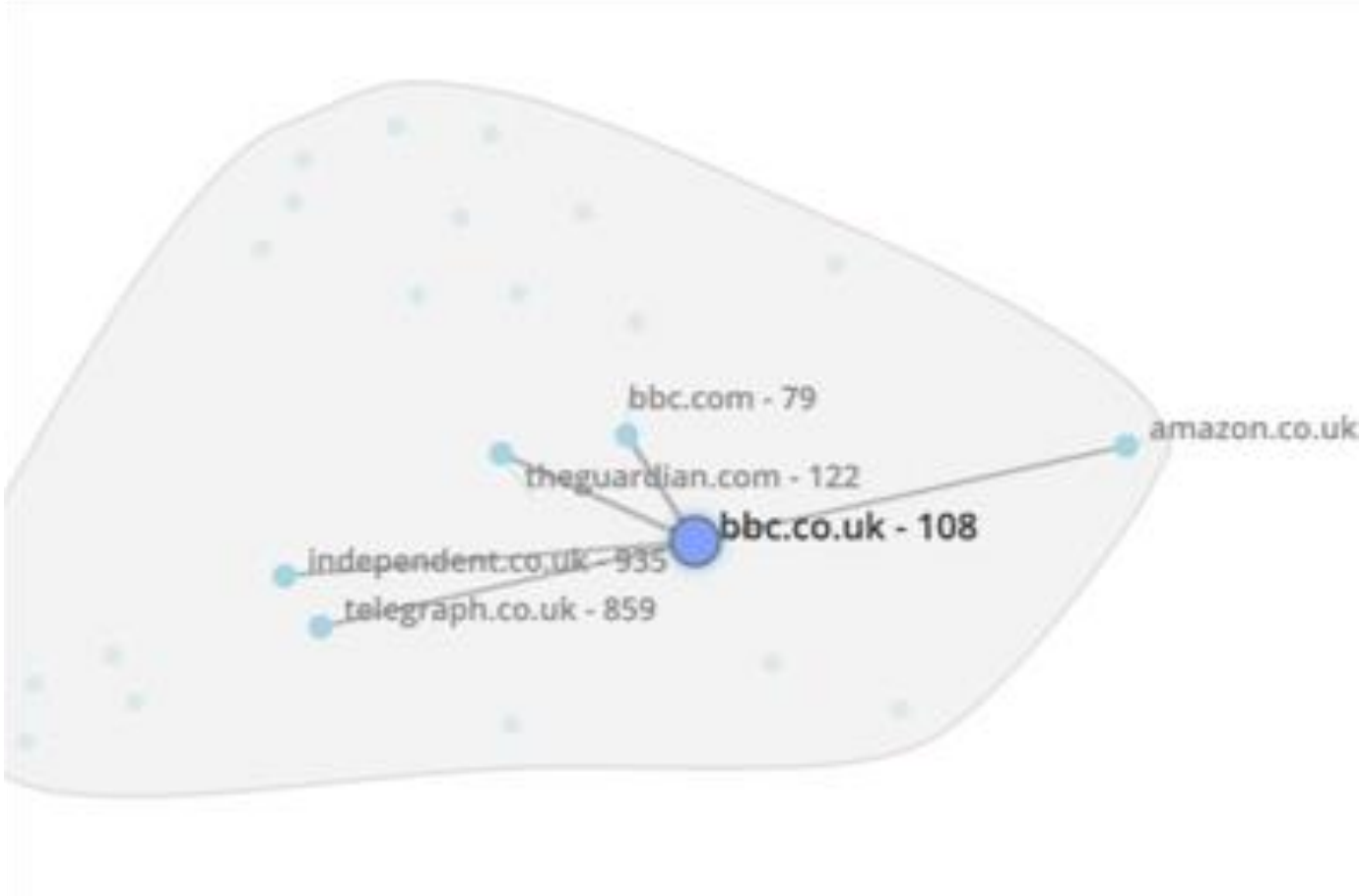
Corporate Owner:	British Broadcasting Corporation

Mail Server ID: Found through (**Tool used:** nslookup -type=mx)	• 10 cluster1.eu.messagelabs.com • 20cluster1a.eu.messagelab.com
Cloud Service provider:	Fastly (SKYCA-3) – San Francisco, CA
Operating System used: (nmap OS guesses)	• Linux 2.6.18-2.6.22 • OpenBSD 4.6
Net Worth: (resource used: w3snoop)	$986,166,903
Visitors (Unique):	Daily: Monthly: Yearly:
Websites Linking in:	Compared to its competitors there are 220,213 websites that link to bbc.co.uk. Quite a few of these sites linking in are Chinese search engines like Baidu, Baike, youdao, which are scraping data from the bbc.co.uk, other websites such as someone's Wix website, is mentioned to increase the number of viewers to the website. One interesting website linked is "ruTracker" which is a torrent portal that people majorly in Russia use to grab millions of downloads, even after being completely banned from the country.Hence, it seems like these were linked to other sites simply to increase the number of people visiting the site, or maybe randomly added by users who were obliged to give in their website details upon registration, that deemed that the website wasn't popular enough and hence "safe" to use. This is, of course, among a myriad of other possible reasons.

Interaction of visitors on website (alexa.org)	Daily Pageviews per visitor: 3.84 Daily Time on Site: 3:20(mm:ss) Bounce Rate (when visitors enter the site and leave rather than browsing through other pages within the website): 42%
Google Search:	**bbc.co.uk-** About 557,000,000 results (0.46 seconds). This returns more results but after browsing through the first couple search pages results on Google, the search results start displaying websites that might mention or link to bbc.co.uk at some point. **site:bbc.co.uk-** About 11,500,000 results (0.30 seconds). This returns comparatively less results, however the search results only lead to bbc.co.uk.

NSlookup	• **dig**: After performing a dig (on the website's name servers, it was interesting to note that AAAA server records aren't displayed, meaning that IPv6 address records aren't updated. This could a starting point for occurrence of vulnerabilities in the system. • **soa**: The SOA. Serial number is revealed, which can be quite handy for a hacker. This increases every time DNS settings for a domain get modified, and by watching the serial number, one can see the moment the entry changes are made, and get prompted about tampering with credentials. The expiration dates and the details of the admin are also displayed which gives away information like email addresses. • **mx: "**10 cluster1.eu.messagelabs.com" and "20cluster1a.eu.messagelab.com" are the two mail servers, which ensures that if the primary mail server is down, then the mail is not lost due to single point of failure as the backup server will become active.
Premier Network Detection: Nmap	I primarily used nmap to search if there were any vulnerabilities in bbc.co.uk: To check and gather the information about the services we do map -sS, and then further it shows us that HTTP port versions are **Varnish** which is an HTTP accelerator designed for content-heavy websites which are content heavy as well as APIs. Also varnish is generally ideal to run on Linux/Unix OS like BSD (belonging to Unix family) environments, so that helped shortlist the operating systems being used. I made use of NSE(Nmap Scripting Engine) feature that could be used with nmap, to perform a various networking tasks. One common thing that I noticed was that after running most of the NSE Scripts, the services running for port 443 was resulting in "tcpwrapped". Looking up what it meant, I found that the behavior of the port is protected. The tcpwrapper serves the purpose of protecting the website here and not the port, as it might indicate that a real network service is available, however I'm not an authorized host to talk with the service.
Vulnerabilities detected using nmap: The scripts I found vulnerabilities with were:	• **Nmap-Vulners:** It's a script that searches for the target's vulnerabilities. It first scans through targets versions and services, and then scans them against CVE's through multiple databases provided online, like Nessus, Exploit-DB, etc. Screenshot of vulnerabilities found are further down in this report. • **http-slowloris-check:** These checks for the case if the web server is actually vulnerable to the slowloris DOS attack without actually executing the aforementioned attack. After running this script with bbc's IP the result came out to be "LIKELY VUILNERABLE" which means that the server might be vulnerable to timeout-extension attack.

Screenshots:
Alexa.com:



AUDIENCE OVERLAP WITH BBC.CO.UK

Audience Geography

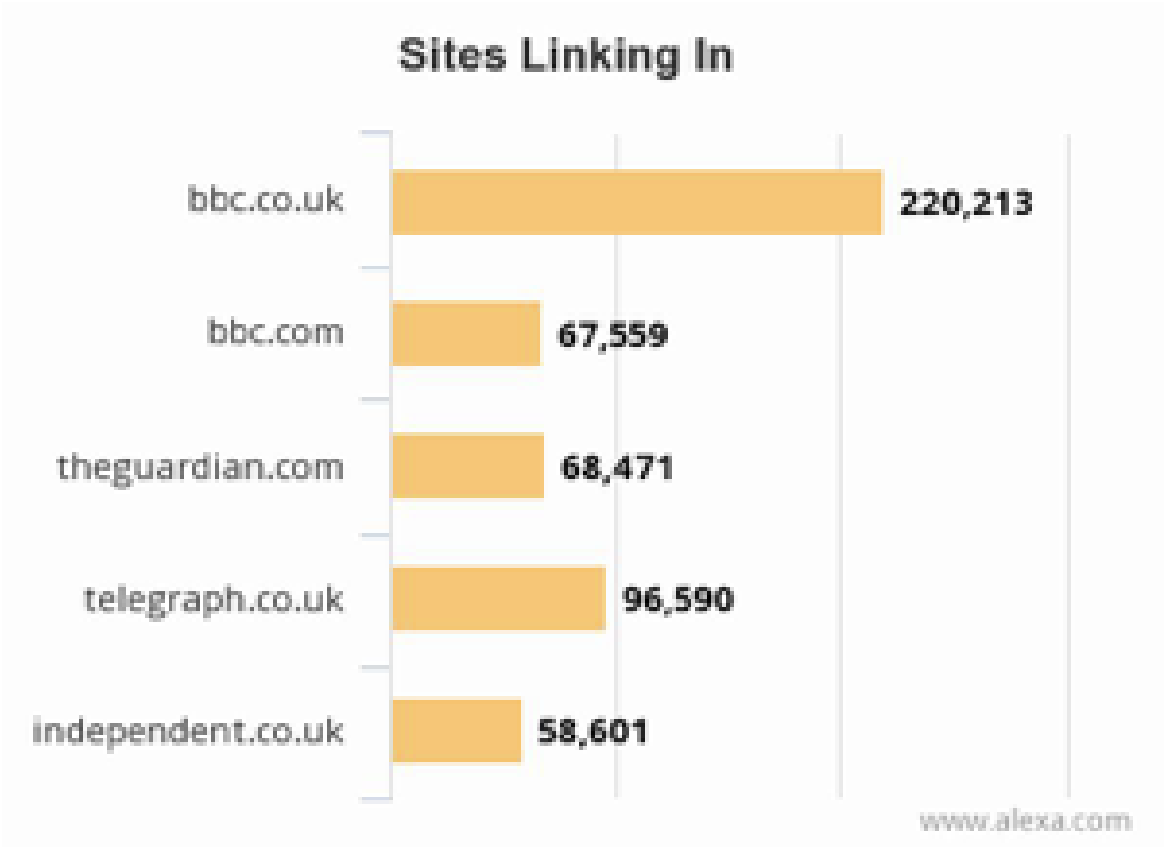
Estimate

All visitors to this site in the past 30 days

Visitors by Country

United Kingdom	48.7%
United States	18.0%
Japan	10.3%
South Korea	5.8%
Taiwan	1.6%

FIRST 5 COUNTRIES CONTRIBUTING TO THIS WEBSITES TRAFFIC


Sites Linking In
bbc.co.uk
220,213
bbc.com
67,559
theguardian.com
68,471
telegraph.co.uk
96,590
independent.co.uk
58,601
www.alexa.com

All visitors to this site

Engagement

Past 90 Days

3.84	3:20	42.0%
Daily Pageviews per Visitor	Daily Time on Site	Bounce rate

Traffic Sources

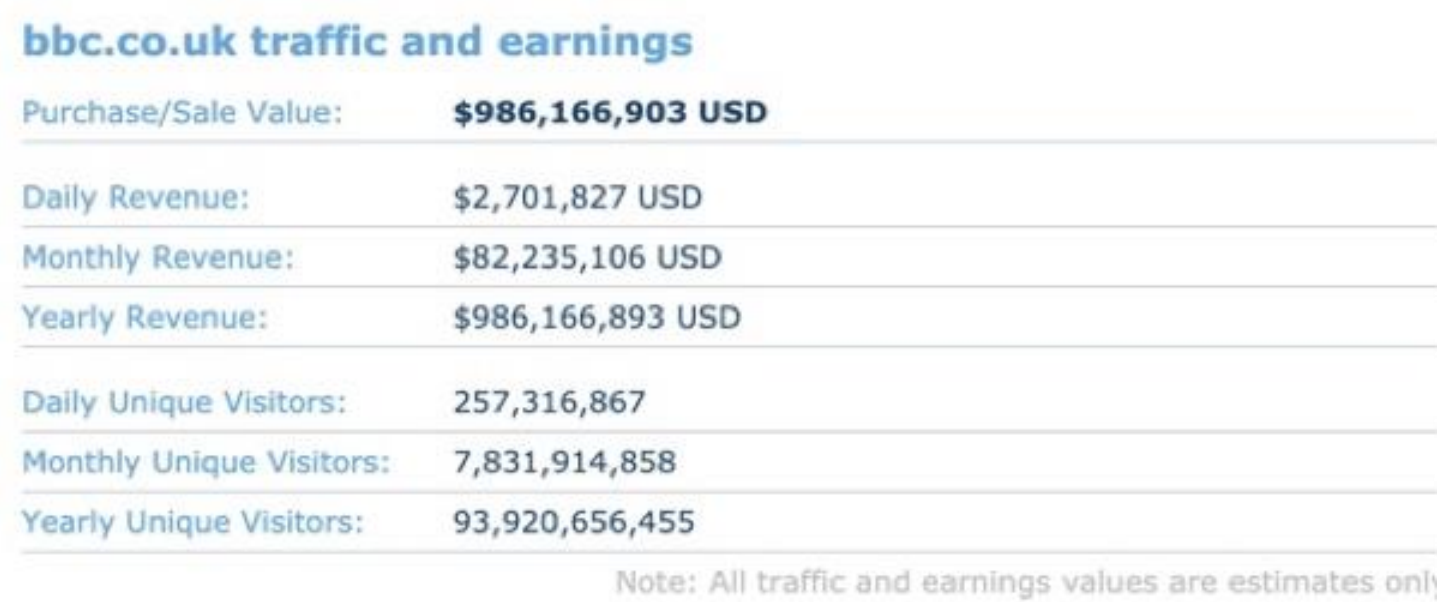
Past 30 Days

Site Flow

Past 60 Days

Visited just before		Visited right after	
27.3%	google.com	20.8%	google.com
5.37%	bbc.com	16%	bbc.com
3.88%	login.tmall.com	4.72%	login.tmall.com
3.38%	facebook.com	3.89%	youtube.com
3.07%	youtube.com	3.42%	facebook.com

W3snoop:



bbc.co.uk traffic and earnings

Purchase/Sale Value:	**$986,166,903 USD**
Daily Revenue:	$2,701,827 USD
Monthly Revenue:	$82,235,106 USD
Yearly Revenue:	$986,166,893 USD
Daily Unique Visitors:	257,316,867
Monthly Unique Visitors:	7,831,914,858
Yearly Unique Visitors:	93,920,656,455

Note: All traffic and earnings values are estimates onl

WORTH & VISITORS

```
# whois.nic.uk

    Domain name:
        bbc.co.uk

    Data validation:
        Nominet was able to match the registrant's name and address against a 3rd party data source on 12-Jun-2014

    Registrar:
        British Broadcasting Corporation [Tag = BBC]
        URL: http://www.bbc.co.uk

    Relevant dates:
        Registered on: before Aug-1996
        Expiry date:  13-Dec-2025
        Last updated:  29-Oct-2016

    Registration status:
        Registered until expiry date.

    Name servers:
        ns3.bbc.co.uk             156.154.66.17  2610:a1:1015::17
        ns3.bbc.net.uk
        ns4.bbc.co.uk             156.154.67.17  2001:502:4612::17
        ns4.bbc.net.uk

    WHOIS lookup made at 14:47:03 26-Nov-2019
```

WHOISLOOKUP

```
gopaljuneja@Gopals-MacBook-Pro ~ % nslookup -type=mx bbc.co.uk
Server:         192.168.22.22
Address:        192.168.22.22#53

Non-authoritative answer:
bbc.co.uk       mail exchanger = 10 cluster1.eu.messagelabs.com.
bbc.co.uk       mail exchanger = 20 cluster1a.eu.messagelabs.com.
```

MAIL SERVERS

```
gopaljuneja@Gopals-MacBook-Pro ~ % dig ns4 bbc.co.uk

; <<>> DiG 9.10.6 <<>> ns4 bbc.co.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19050
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ns4.                           IN      A

;; ANSWER SECTION:
ns4.                    300     IN      A       92.242.132.30

;; AUTHORITY SECTION:
.                       900     IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2019112600 1800 900 604800 86400

;; Query time: 32 msec
;; SERVER: 192.168.22.22#53(192.168.22.22)
;; WHEN: Tue Nov 26 14:54:31 GMT 2019
;; MSG SIZE  rcvd: 123

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27666
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;bbc.co.uk.                     IN      A

;; ANSWER SECTION:
bbc.co.uk.              268     IN      A       151.101.0.81
bbc.co.uk.              268     IN      A       151.101.128.81
bbc.co.uk.              268     IN      A       151.101.192.81
bbc.co.uk.              268     IN      A       151.101.64.81

;; Query time: 13 msec
;; SERVER: 192.168.22.22#53(192.168.22.22)
;; WHEN: Tue Nov 26 14:54:31 GMT 2019
;; MSG SIZE  rcvd: 102
```

NSlookup Dig

```
gopaljuneja@Gopals-MacBook-Pro ~ % nslookup -type=soa bbc.co.uk
Server:         192.168.22.22
Address:        192.168.22.22#53

Non-authoritative answer:
bbc.co.uk
        origin = ns.bbc.co.uk
        mail addr = hostmaster.bbc.co.uk
        serial = 2019112001
        refresh = 1800
        retry = 600
        expire = 864000
        minimum = 900
```

STATE OF AUTHORITY

```
gopaljuneja@Gopals-MacBook-Pro ~ % sudo nmap -sS 151.101.64.81
Password:
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-26 16:05 GMT
Nmap scan report for 151.101.64.81
Host is up (0.025s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds
gopaljuneja@Gopals-MacBook-Pro ~ % sudo nmap -sS -sV 151.101.64.81
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-26 16:06 GMT
Nmap scan report for 151.101.64.81
Host is up (0.026s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE        VERSION
21/tcp  open  tcpwrapped
80/tcp  open  http-proxy     Varnish
443/tcp open  ssl/http-proxy Varnish

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 132.33 seconds
```

NMAP

```
gopaljuneja@Gopals-MacBook-Pro ~ % sudo nmap -A -T4 151.101.64.81
Password:
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-26 16:08 GMT
Nmap scan report for 151.101.64.81
Host is up (0.029s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE        VERSION
21/tcp  open  tcpwrapped
80/tcp  open  http-proxy     Varnish
|_http-title: Fastly error: unknown domain 151.101.64.81
443/tcp open  ssl/http-proxy Varnish
|_http-title: Fastly error: unknown domain 151.101.64.81
| ssl-cert: Subject: commonName=www.bbc.com/organizationName=British Broadcasting Corporation/stateOrProvinceName=London/countryName=GB
| Subject Alternative Name: DNS:www.bbc.com, DNS:fig.bbc.co.uk, DNS:bbc.co.uk, DNS:www.bbc.co.uk, DNS:bbc.com
| Not valid before: 2019-05-28T12:30:02
|_Not valid after:  2020-08-05T09:36:04
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|_  http/1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 2.6.X (86%), OpenBSD 4.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: Linux 2.6.18 - 2.6.22 (86%), OpenBSD 4.0 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   19.26 ms 100.109.0.1
2   18.39 ms 192.168.194.246
3   23.47 ms 192.168.118.1
4   22.03 ms 192.168.202.17
5   23.46 ms 213.120.179.202
6   28.57 ms acc2-xe-2-1-2.sf.21cn-ipp.bt.net (109.159.255.225)
7   28.59 ms 217.32.170.14
8   24.03 ms 194.72.16.54
9   ...
10  25.11 ms 151.101.64.81

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 166.33 seconds
gopaljuneja@Gopals-MacBook-Pro ~ %
```

NMAP AGGRESSIVE SCAN

http-slowloris-check

```
gopaljuneja@Gopals-MacBook-Pro ~ % nmap --script http-slowloris-check -sV -v -p443,80 151.101.64.81
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-26 21:38 GMT
NSE: Loaded 46 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:38
Completed NSE at 21:38, 0.00s elapsed
Initiating NSE at 21:38
Completed NSE at 21:38, 0.00s elapsed
Initiating Ping Scan at 21:38
Scanning 151.101.64.81 [2 ports]
Completed Ping Scan at 21:38, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:38
Completed Parallel DNS resolution of 1 host. at 21:38, 0.01s elapsed
Initiating Connect Scan at 21:38
Scanning 151.101.64.81 [2 ports]
Discovered open port 443/tcp on 151.101.64.81
Discovered open port 80/tcp on 151.101.64.81
Completed Connect Scan at 21:38, 0.02s elapsed (2 total ports)
Initiating Service scan at 21:38
Scanning 2 services on 151.101.64.81
Completed Service scan at 21:38, 12.20s elapsed (2 services on 1 host)
NSE: Script scanning 151.101.64.81.
Initiating NSE at 21:38
NSE Timing: About 93.48% done; ETC: 21:46 (0:00:30 remaining)
NSE Timing: About 93.48% done; ETC: 21:46 (0:00:32 remaining)
NSE Timing: About 93.48% done; ETC: 21:47 (0:00:35 remaining)
Completed NSE at 21:47, 511.52s elapsed
Initiating NSE at 21:47
Completed NSE at 21:47, 0.23s elapsed
Nmap scan report for 151.101.64.81
Host is up (0.029s latency).

PORT    STATE SERVICE       VERSION
80/tcp  open  http-proxy    Varnish
| http-slowloris-check:
```

```
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web
server open and hold
|       them open as long as possible.  It accomplishes this by
opening connections to
|       the target web server and sending a partial request. By doing
so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-
6750
|_      http://ha.ckers.org/slowloris/
443/tcp open  ssl/http-proxy Varnish
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web
server open and hold
|       them open as long as possible.  It accomplishes this by
opening connections to
|       the target web server and sending a partial request. By doing
so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-
6750
|_      http://ha.ckers.org/slowloris/

NSE: Script Post-scanning.
Initiating NSE at 21:47
Completed NSE at 21:47, 0.00s elapsed
Initiating NSE at 21:47
Completed NSE at 21:47, 0.00s elapsed
```

Read data files from: /usr/local/bin/../share/nmap

Service detection performed. Please report any incorrect results at

https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 524.63 seconds

Nmap-vulners(shortened the output since it was too big)

gopaljuneja@Gopals-MacBook-Pro updater % nmap --script nmap-vulners -sV -p443 151.101.64.81/24
Starting Nmap 7.80 (https://nmap.org) at 2019-11-26 18:26 GMT
Nmap scan report for 151.101.64.0
Host is up (0.12s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.1
Host is up (0.028s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.2
Host is up (0.029s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.3
Host is up (0.027s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.4
Host is up (0.029s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.5
Host is up (0.032s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.6

Host is up (0.032s latency).

PORT STATE SERVICE VERSION

443/tcp open tcpwrapped

Nmap scan report for 151.101.64.7

Host is up (0.034s latency).

PORT STATE SERVICE VERSION

443/tcp open tcpwrapped

Nmap scan report for 151.101.64.8

Host is up (0.034s latency).

PORT STATE SERVICE VERSION

443/tcp open tcpwrapped

Nmap scan report for 151.101.64.9

Host is up (0.038s latency).

PORT STATE SERVICE VERSION

443/tcp open tcpwrapped

Nmap scan report for 151.101.64.45

Host is up (0.029s latency).

PORT STATE SERVICE VERSION

443/tcp open tcpwrapped

PORT STATE SERVICE VERSION

443/tcp open tcpwrapped

Nmap scan report for 151.101.64.58

Host is up (0.032s latency).

PORT STATE SERVICE VERSION

443/tcp open tcpwrapped

Nmap scan report for 151.101.64.59

Host is up (0.034s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.60
Host is up (0.043s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.61
Host is up (0.087s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.62
Host is up (0.12s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.63
Host is up (0.042s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.64
Host is up (0.040s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish

Nmap scan report for 151.101.64.65
Host is up (0.13s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish

Nmap scan report for 151.101.64.66
Host is up (0.093s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish

Nmap scan report for 151.101.64.67
Host is up (0.042s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish

Nmap scan report for 151.101.64.68
Host is up (0.045s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish

Nmap scan report for 151.101.64.69
Host is up (0.11s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish

Nmap scan report for 151.101.64.70
Host is up (0.13s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish

Nmap scan report for 151.101.64.71
Host is up (0.033s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.72
Host is up (0.032s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish

Nmap scan report for 151.101.64.73
Host is up (0.091s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.74
Host is up (0.092s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish

Nmap scan report for 151.101.64.75
Host is up (0.041s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.76
Host is up (0.042s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.77
Host is up (0.11s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.78
Host is up (0.13s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.91
Host is up (0.035s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.103
Host is up (0.096s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.104
Host is up (0.10s latency).

443/tcp open tcpwrapped

Nmap scan report for 151.101.64.111
Host is up (0.094s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.112
Host is up (0.095s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.113
Host is up (0.047s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish

Nmap scan report for 151.101.64.114
Host is up (0.048s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish

Nmap scan report for 151.101.64.115
Host is up (0.12s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.116
Host is up (0.12s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish

Nmap scan report for 151.101.64.117
Host is up (0.053s latency).

PORT STATE SERVICE VERSION
443/tcp open tcpwrapped

Nmap scan report for 151.101.64.118
Host is up (0.056s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http T-Home Telekom Media Receiver httpd
|_http-server-header: api-gateway/1.9.3.1
Service Info: Device: media device

Nmap scan report for 151.101.64.119
Host is up (0.052s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http T-Home Telekom Media Receiver httpd
Service Info: Device: media device

Nmap scan report for 151.101.64.120
Host is up (0.052s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish

Nmap scan report for 151.101.64.133
Host is up (0.10s latency).

PORT STATE SERVICE VERSION
443/tcp open ssl/http-proxy Varnish
|_http-server-header: GitHub.com

Nmap scan report for 151.101.64.134
Host is up (0.11s latency).

PORT STATE SERVICE VERSION

443/tcp open ssl/http Apache httpd 2.2.15 ((CentOS))

|_http-server-header: Apache/2.2.15 (CentOS)

| vulners:

| cpe:/a:apache:http_server:2.2.15:

| CVE-2011-3192 7.8 https://vulners.com/cve/CVE-2011-3192

| CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679

| CVE-2017-7668 7.5 https://vulners.com/cve/CVE-2017-7668

| CVE-2017-3169 7.5 https://vulners.com/cve/CVE-2017-3169

| CVE-2017-3167 7.5 https://vulners.com/cve/CVE-2017-3167

| CVE-2013-2249 7.5 https://vulners.com/cve/CVE-2013-2249

| CVE-2012-0883 6.9 https://vulners.com/cve/CVE-2012-0883

| CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312

| CVE-2017-12171 6.4 https://vulners.com/cve/CVE-2017-12171

| CVE-2013-1862 5.1 https://vulners.com/cve/CVE-2013-1862

| CVE-2014-0231 5.0 https://vulners.com/cve/CVE-2014-0231

| CVE-2014-0098 5.0 https://vulners.com/cve/CVE-2014-0098

| CVE-2013-6438 5.0 https://vulners.com/cve/CVE-2013-6438

| CVE-2012-4557 5.0 https://vulners.com/cve/CVE-2012-4557

| CVE-2011-3368 5.0 https://vulners.com/cve/CVE-2011-3368

| CVE-2010-2068 5.0 https://vulners.com/cve/CVE-2010-2068

| CVE-2010-1452 5.0 https://vulners.com/cve/CVE-2010-1452

| CVE-2012-0031 4.6 https://vulners.com/cve/CVE-2012-0031

| CVE-2011-3607 4.4 https://vulners.com/cve/CVE-2011-3607
| CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975
| CVE-2013-1896 4.3 https://vulners.com/cve/CVE-2013-1896
| CVE-2012-4558 4.3 https://vulners.com/cve/CVE-2012-4558
| CVE-2012-3499 4.3 https://vulners.com/cve/CVE-2012-3499
| CVE-2012-0053 4.3 https://vulners.com/cve/CVE-2012-0053
| CVE-2011-4317 4.3 https://vulners.com/cve/CVE-2011-4317
| CVE-2011-3639 4.3 https://vulners.com/cve/CVE-2011-3639
| CVE-2011-3348 4.3 https://vulners.com/cve/CVE-2011-3348
| CVE-2011-0419 4.3 https://vulners.com/cve/CVE-2011-0419
| CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612
| CVE-2012-2687 2.6 https://vulners.com/cve/CVE-2012-2687
|_ CVE-2011-4415 1.2 https://vulners.com/cve/CVE-2011-4415

2.Website 2:bestbuy.com

Corporate Owner:	VeriSign Global Registry Services
Mail Server ID: Found through (**Tool used:** nslookup -type=mx)	• 10 mxb-002a6b01.gslb.pphosted.com • 10 mxa-002a6b01.gslb.pphosted.com
Operating System used: (nmap OS guesses)	• Linksys BEFW11S4 WAP (92%) • Palo Alto PA-500 firewall (89%) • Linksys BEFSR41 router (88%) • Asus RT-53N WAP (87%) • Cisco ACE load balancer (87%) • Tripp Lite NetOS 7.5.2tl (85%) • Essentia OpenWifless ESS (85%) • Linux 2.6.11 - 2.6.18 (85%)
Net Worth: (resource used: w3snoop)	$109,988,635
Visitors (Unique):	Daily: Monthly: Yearly:
Websites Linking in:	9,110
IP Address:	23.209.52.32
Cloud Storage:	Akamai Technologies, Inc. (AKAMAI)

Vulnerabilities detected using nmap:	**Attempt to find vulnerabilities with:** **1.** Nmap-vulners **2.** Vuln **3.** http-slowloris.nse **4.** mysql.query **5.** ssl-heartbleed **No vulnerabilities found** **Screenshots attached below**

Interaction of visitors on website (alexa.org)	Daily Pageviews per visitor: 4.34 Daily Time on Site: 3:29(mm:ss) Bounce Rate (when visitors enter the site and leave rather than browsing through other pages within the website): 25.6%, as it's a e-market, people tend to spend more time browsing through products
Google Search:	**bestbuy.com-** 181,000,000 results (0.59 seconds) This returns more results but after browsing through the first couple search pages results on Google, the search results start displaying websites that might mention or link to bbc.co.uk at some point. **inurl:bestbuy.com-** About 7 results (0.42 seconds) This returns comparatively less results, however the search results only lead to bestbuy.com plus its extensions like bestbuy.com.mx, etc.

Whoislookup:

```
gopaljuneja@8afbcf9e ~ % whois www.bestbuy.com
% IANA WHOIS server
% for more information on IANA, visit http://www.iana
% This query returned 1 object

refer:        whois.verisign-grs.com

domain:       COM

organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States

contact:      administrative
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

contact:      technical
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

nserver:      A.GTLD-SERVERS.NET 192.5.6.30 2001:503:
nserver:      B.GTLD-SERVERS.NET 192.33.14.30 2001:50
nserver:      C.GTLD-SERVERS.NET 192.26.92.30 2001:50
nserver:      D.GTLD-SERVERS.NET 192.31.80.30 2001:50
nserver:      E.GTLD-SERVERS.NET 192.12.94.30 2001:50
nserver:      F.GTLD-SERVERS.NET 192.35.51.30 2001:50
nserver:      G.GTLD-SERVERS.NET 192.42.93.30 2001:50
nserver:      H.GTLD-SERVERS.NET 192.54.112.30 2001:5
nserver:      I.GTLD-SERVERS.NET 192.43.172.30 2001:5
nserver:      J.GTLD-SERVERS.NET 192.48.79.30 2001:50
nserver:      K.GTLD-SERVERS.NET 192.52.178.30 2001:5
nserver:      L.GTLD-SERVERS.NET 192.41.162.30 2001:5
nserver:      M.GTLD-SERVERS.NET 192.55.83.30 2001:50
ds-rdata:     30909 8 2 E2D3C916F6DEEAC73294E8268FB58

whois:        whois.verisign-grs.com

status:       ACTIVE
remarks:      Registration information: http://www.ve

created:      1985-01-01
changed:      2017-10-05
source:       IANA

# whois.verisign-grs.com

No match for domain "WWW.BESTBUY.COM".
>>> Last update of whois database: 2019-11-28T19:10:3
```

```
gopaljuneja@8afbcf9e ~ % nslookup set type=soa bestbuy.com
nslookup: couldn't get address for 'type=soa': not found
gopaljuneja@8afbcf9e ~ % nslookup -type=soa bestbuy.com
Server:         138.251.10.53
Address:        138.251.10.53#53

Non-authoritative answer:
bestbuy.com
        origin = tag1.bestbuy.com
        mail addr = please_set_email.absolutely.nowhere
        serial = 2008066051
        refresh = 10800
        retry = 3600
        expire = 2592000
        minimum = 900

Authoritative answers can be found from:
bestbuy.com     nameserver = use1.akam.net.
bestbuy.com     nameserver = eur2.akam.net.
bestbuy.com     nameserver = ns1-118.akam.net.
bestbuy.com     nameserver = asia3.akam.net.
bestbuy.com     nameserver = ns1-119.akam.net.
bestbuy.com     nameserver = eur1.akam.net.
bestbuy.com     nameserver = usw2.akam.net.
bestbuy.com     nameserver = usc2.akam.net.
eur1.akam.net   internet address = 2.16.130.64
eur2.akam.net   internet address = 95.100.173.64
usc2.akam.net   internet address = 184.26.160.64
use1.akam.net   internet address = 72.246.46.64
usw2.akam.net   internet address = 184.26.161.64
asia3.akam.net  internet address = 23.211.61.64
```

nslookup: SOA

```
gopaljuneja@8afbcf9e ~ % nslookup -type=mx bestbuy.com
Server:         138.251.10.53
Address:        138.251.10.53#53

Non-authoritative answer:
bestbuy.com     mail exchanger = 10 mxb-002a6b01.gslb.pphosted.com.
bestbuy.com     mail exchanger = 10 mxa-002a6b01.gslb.pphosted.com.

Authoritative answers can be found from:
bestbuy.com     nameserver = ns1-119.akam.net.
bestbuy.com     nameserver = eur1.akam.net.
bestbuy.com     nameserver = usc2.akam.net.
bestbuy.com     nameserver = usw2.akam.net.
bestbuy.com     nameserver = eur2.akam.net.
bestbuy.com     nameserver = asia3.akam.net.
bestbuy.com     nameserver = ns1-118.akam.net.
bestbuy.com     nameserver = use1.akam.net.
eur1.akam.net   internet address = 2.16.130.64
eur2.akam.net   internet address = 95.100.173.64
usc2.akam.net   internet address = 184.26.160.64
use1.akam.net   internet address = 72.246.46.64
usw2.akam.net   internet address = 184.26.161.64
asia3.akam.net  internet address = 23.211.61.64
```

Nslookup: -type=mx Message exchange servers

```
gopaljuneja@8afbcf9e ~ % dig bestbuy.com

; <<>> DiG 9.10.6 <<>> bestbuy.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12842
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 8, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;bestbuy.com.                   IN      A

;; ANSWER SECTION:
bestbuy.com.            20      IN      A       104.127.39.115

;; AUTHORITY SECTION:
bestbuy.com.            150294  IN      NS      ns1-119.akam.net.
bestbuy.com.            150294  IN      NS      eur1.akam.net.
bestbuy.com.            150294  IN      NS      use1.akam.net.
bestbuy.com.            150294  IN      NS      asia3.akam.net.
bestbuy.com.            150294  IN      NS      usc2.akam.net.
bestbuy.com.            150294  IN      NS      ns1-118.akam.net.
bestbuy.com.            150294  IN      NS      eur2.akam.net.
bestbuy.com.            150294  IN      NS      usw2.akam.net.

;; ADDITIONAL SECTION:
eur1.akam.net.          62266   IN      A       2.16.130.64
eur2.akam.net.          100685  IN      A       95.100.173.64
usc2.akam.net.          62266   IN      A       184.26.160.64
use1.akam.net.          72625   IN      A       72.246.46.64
usw2.akam.net.          72625   IN      A       184.26.161.64
asia3.akam.net.         72779   IN      A       23.211.61.64

;; Query time: 17 msec
;; SERVER: 138.251.10.53#53(138.251.10.53)
;; WHEN: Thu Nov 28 19:17:39 GMT 2019
;; MSG SIZE  rcvd: 319
```

Dig

```
gopaljuneja@8afbcf9e ~ % nslookup -debug bestbuy.com
Server:         138.251.10.53
Address:        138.251.10.53#53

------------
    QUESTIONS:
        bestbuy.com, type = A, class = IN
    ANSWERS:
    ->  bestbuy.com
        internet address = 104.127.39.115
        ttl = 20
    AUTHORITY RECORDS:
    ->  bestbuy.com
        nameserver = usc2.akam.net.
        ttl = 150173
    ->  bestbuy.com
        nameserver = asia3.akam.net.
        ttl = 150173
    ->  bestbuy.com
        nameserver = eur2.akam.net.
        ttl = 150173
    ->  bestbuy.com
        nameserver = usw2.akam.net.
        ttl = 150173
    ->  bestbuy.com
        nameserver = ns1-119.akam.net.
        ttl = 150173
    ->  bestbuy.com
        nameserver = eur1.akam.net.
        ttl = 150173
    ->  bestbuy.com
        nameserver = ns1-118.akam.net.
        ttl = 150173
    ->  bestbuy.com
        nameserver = use1.akam.net.
        ttl = 150173
    ADDITIONAL RECORDS:
    ->  eur1.akam.net
        internet address = 2.16.130.64
        ttl = 62145
    ->  eur2.akam.net
        internet address = 95.100.173.64
        ttl = 100564
    ->  usc2.akam.net
        internet address = 184.26.160.64
        ttl = 62145
    ->  use1.akam.net
        internet address = 72.246.46.64
        ttl = 72504
    ->  usw2.akam.net
        internet address = 184.26.161.64
        ttl = 72504
    ->  asia3.akam.net
        internet address = 23.211.61.64
        ttl = 72658
------------
Non-authoritative answer:
Name:   bestbuy.com
Address: 104.127.39.115
```

Nslookup-debug

```
gopaljuneja@8afbcf9e ~ %  sudo nmap -sS -sV -sC -T4 -A 23.209.52.32
Password:
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-28 19:24 GMT
Nmap scan report for a23-209-52-32.deploy.static.akamaitechnologies.com (23.209.52.32)
Host is up (0.026s latency).
Not shown: 990 filtered ports
PORT      STATE  SERVICE      VERSION
25/tcp    closed smtp
53/tcp    closed domain
80/tcp    open   http         AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-title: Invalid URL
111/tcp   closed rpcbind
135/tcp   closed msrpc
139/tcp   closed netbios-ssn
443/tcp   open   ssl/http     AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-title: Invalid URL
| ssl-cert: Subject: commonName=www.bestbuy.com/organizationName=Best Buy Co, Inc./stateOrProvinceName=Minnesota/countryName=US
| Subject Alternative Name: DNS:www.bestbuy.com, DNS:bestbuy.com, DNS:mexico.bbystatic.com, DNS:assets.bbystatic.com, DNS:css-ssl.bbystatic.com, DNS:msi.bbycastatic.ca, DNS:deals.bestbuy.com, DNS:m.bestbu
y.ca, DNS:www.bestbuy.ca, DNS:www-ssl.bestbuy.ca, DNS:m-ssl.bestbuy.ca, DNS:app.bestbuy.com, DNS:app-ssl.bestbuy.com, DNS:bestbuy.com.mx, DNS:images-ssl.bbystatic.com, DNS:context.bestbuy.com, DNS:api-ssl
.bestbuy.ca, DNS:www-ssl.bestbuy.com, DNS:js-ssl.bbystatic.com, DNS:kiosk.bestbuy.ca, DNS:misc-ssl.bbystatic.com, DNS:bestbuy.ca, DNS:pisces.bbystatic.com, DNS:api.bestbuy.ca, DNS:img.bbystatic.com, DNS:i
mages.bestbuy.com, DNS:www.bestbuy.com.mx, DNS:pisces-ssl.bbystatic.com
| Not valid before: 2018-12-03T00:00:00
|_Not valid after:  2020-03-26T12:00:00
445/tcp   closed microsoft-ds
2049/tcp  closed nfs
31337/tcp closed Elite
Device type: WAP|firewall|router|load balancer|specialized|general purpose
Running (JUST GUESSING): Linksys embedded (92%), Palo Alto embedded (89%), Asus embedded (87%), Cisco embedded (87%), Tripp Lite NetOS 7.X (85%), Essentia embedded (85%), Linux 2.6.X (85%)
OS CPE: cpe:/h:linksys:befw11s4 cpe:/h:paloalto:pa-500 cpe:/h:linksys:befsr41 cpe:/h:asus:rt-53n cpe:/o:tripplite:netos:7.5.2tl cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linksys BEFW11S4 WAP (92%), Palo Alto PA-500 firewall (89%), Linksys BEFSR41 router (88%), Asus RT-53N WAP (87%), Cisco ACE load balancer (87%), Tripp Lite NetOS 7.5.2tl (85%), Esse
ntia OpenWifless ESS (85%), Linux 2.6.11 - 2.6.18 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 3 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   4.35 ms 138.251.207.2
2   4.37 ms 138.251.1.42
3   4.39 ms a23-209-52-32.deploy.static.akamaitechnologies.com (23.209.52.32)

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 41.97 seconds
gopaljuneja@8afbcf9e ~ %
```

Aggressive nmap scan

DNS Lookup

IP Address: 23.209.52.32

Geolocation: US (United States), MA, Massachusetts, 02142 Cambridge - Google Maps

Reverse DNS: a23-209-52-32.deploy.static.akamaitechnologies.com

Title:	Best Buy
Description:	International retailer of consumer electronics and entertainment software under the names Best Buy, Magnolia, and Future Shop. Also offers online shopping. Store locator, investor information, career opportunities.
Domain Name:	**bestbuy.com**
Domain Extension:	.com
Domain Age:	25.7 years old
Domain Length:	7 characters
Fav Icon:	
Average Load Time:	3.76 seconds
Alexa Rank:	220
Moz Rank:	0/10
Page Authority:	0/100
Domain Authority:	0/100
IP Address:	23.209.52.32
Local Language:	English
Local Currency:	USD
Backlinks / Links In:	Approx. 8,399 inbound links

bestbuy.com traffic and earnings

Purchase/Sale Value:	**$109,988,635 USD**
Daily Revenue:	$301,339 USD
Monthly Revenue:	$9,171,801 USD
Yearly Revenue:	$109,988,625 USD
Daily Unique Visitors:	46,719,178
Monthly Unique Visitors:	1,421,984,608
Yearly Unique Visitors:	17,052,499,970

Note: All traffic and earnings values are estimates only.

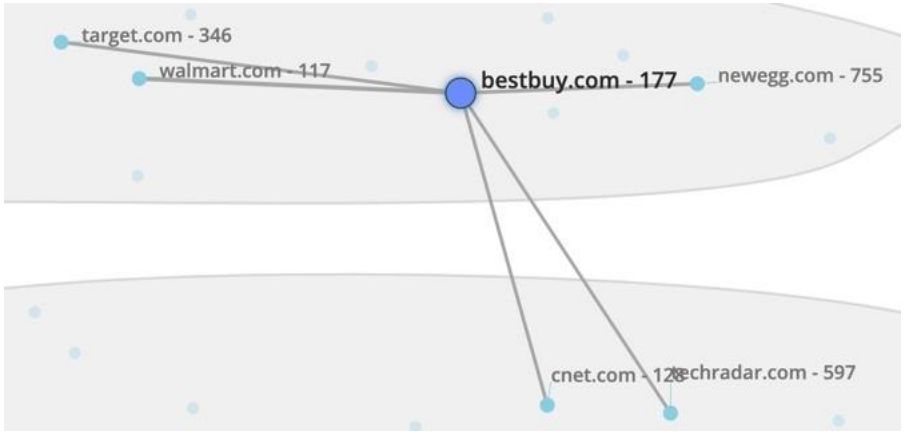
Audience Geography

Estimate

All visitors to this site in the past 30 days

Visitors by Country

United States	64.1%
Japan	14.8%
South Korea	8.4%
Taiwan	2.3%
Canada	1.9%
India	1.5%



Search Engine Optimization information
bestbuy.com SEO data
Ranked as #357 according to Alexa
Ranked as #9278 according to Cisco Umbrella
Ranked as #1009 according to Majestic

SEMrush

Common keywords	Domain
354402	newegg.com
943716	walmart.com
305542	staples.com
517568	cnet.com
454511	target.com
231242	pcmag.com
198182	bhphotovideo.com
1017216	ebay.com
232563	sears.com
158785	techradar.com

Phrase	Ranking
best buy	1
bestbuy	1
best buy credit card	1
geek squad	1
best buy hours	1
refrigerator	1
laptop	1
bestbuy.com	1
best	1
bestbuy com	1

More detailed SEO data at semrush

```
gopaljuneja@8afbcf9e ~ % nmap --script vuln -sV -p80 23.209.52.32
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-28 20:06 GMT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Stats: 0:01:39 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.32% done; ETC: 20:07 (0:00:00 remaining)
Stats: 0:01:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.32% done; ETC: 20:08 (0:00:00 remaining)
Stats: 0:05:44 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.32% done; ETC: 20:12 (0:00:02 remaining)
Nmap scan report for a23-209-52-32.deploy.static.akamaitechnologies.com (23.209.52.32)
Host is up (0.11s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 543.14 seconds
```

Nmap Vuln

```
Nmap scan report for a23-209-52-32.deploy.static.akamaitechnologies.com (23.209.52.32)
Host is up (0.074s latency).
Not shown: 990 filtered ports
PORT      STATE  SERVICE      VERSION
25/tcp    closed smtp
53/tcp    closed domain
80/tcp    open   http         AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
| vulscan: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| No findings
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| No findings
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| No findings
|
| Exploit-DB - https://www.exploit-db.com:
| No findings
|
| OpenVAS (Nessus) - http://www.openvas.org:
| No findings
|
| SecurityTracker - https://www.securitytracker.com:
| No findings
|
| OSVDB - http://www.osvdb.org:
| No findings
|_
111/tcp   closed rpcbind
135/tcp   closed msrpc
139/tcp   closed netbios-ssn
443/tcp   open   ssl/http     AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
| vulscan: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| No findings
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| No findings
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| No findings
|
| Exploit-DB - https://www.exploit-db.com:
| No findings
|
| OpenVAS (Nessus) - http://www.openvas.org:
| No findings
|
| SecurityTracker - https://www.securitytracker.com:
| No findings
|
| OSVDB - http://www.osvdb.org:
| No findings
|_
445/tcp   closed microsoft-ds
2049/tcp  closed nfs
```

Nmap Vulscan

Resources & Websites used:

https://www.alexa.com/
https://ipinfo.info/html/ip_checker.php
https://w3snoop.com/
https://www.robtex.com/