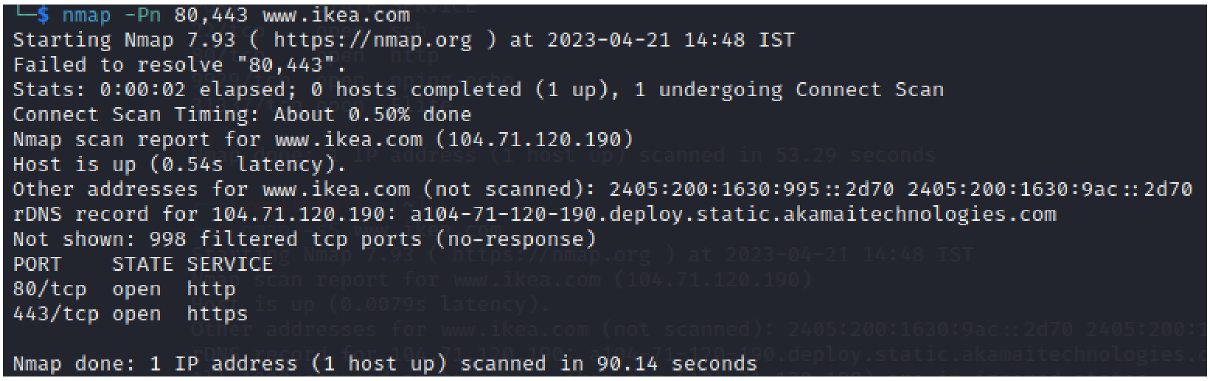
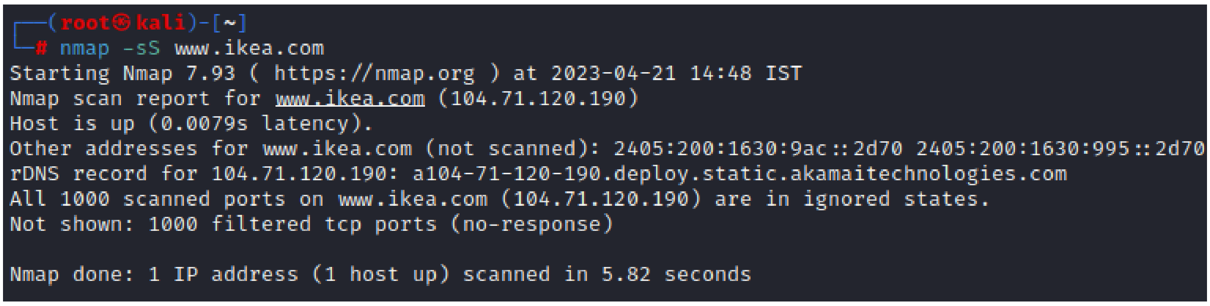
Assignment - 5

All of you have to perform the information gathering techniques on below listed domains. For this you have to use nmap, nmap scripts, robots.txt file, dns lookup, Whois, lookup and way back machine

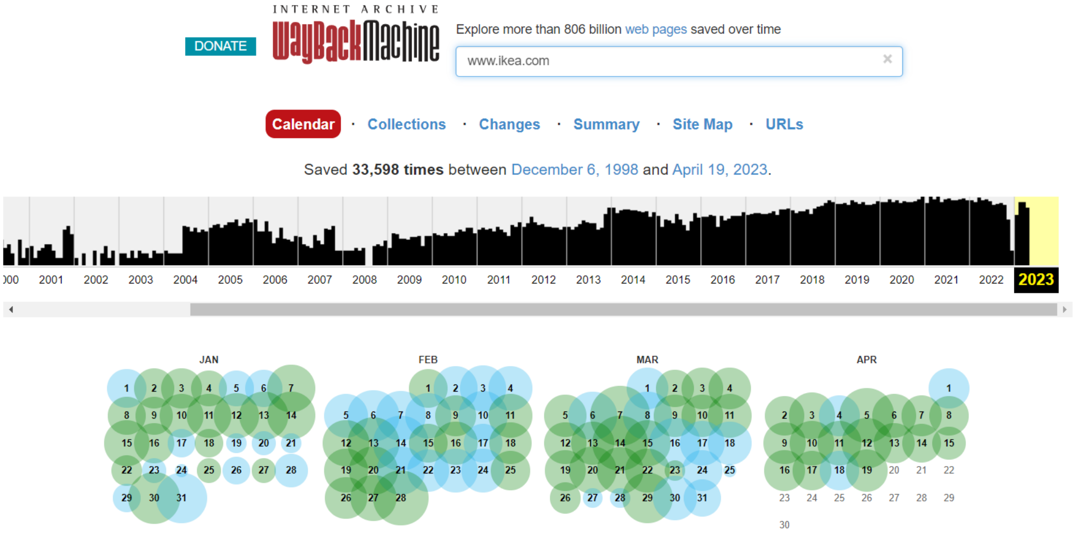
1. www.ikea.com



```
└─$ nmap -Pn 80,443 www.ikea.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-21 14:48 IST
Failed to resolve "80,443".
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.50% done
Nmap scan report for www.ikea.com (104.71.120.190)
Host is up (0.54s latency).
Other addresses for www.ikea.com (not scanned): 2405:200:1630:995::2d70 2405:200:1630:9ac::2d70
rDNS record for 104.71.120.190: a104-71-120-190.deploy.static.akamaitechnologies.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 90.14 seconds
```

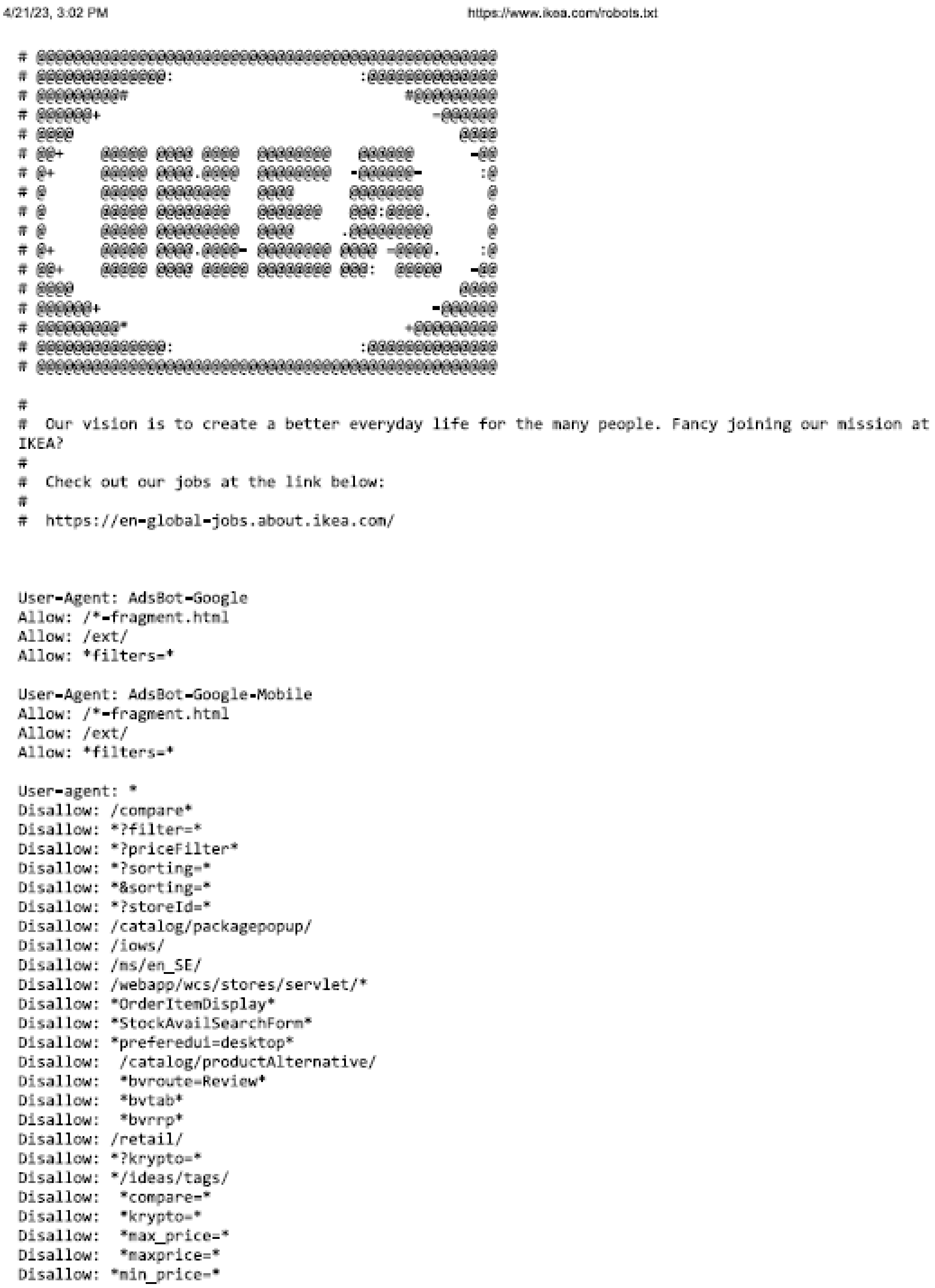


```
┌──(root㉿kali)-[~]
└─# nmap -sS www.ikea.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-21 14:48 IST
Nmap scan report for www.ikea.com (104.71.120.190)
Host is up (0.0079s latency).
Other addresses for www.ikea.com (not scanned): 2405:200:1630:9ac::2d70 2405:200:1630:995::2d70
rDNS record for 104.71.120.190: a104-71-120-190.deploy.static.akamaitechnologies.com
All 1000 scanned ports on www.ikea.com (104.71.120.190) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 5.82 seconds
```



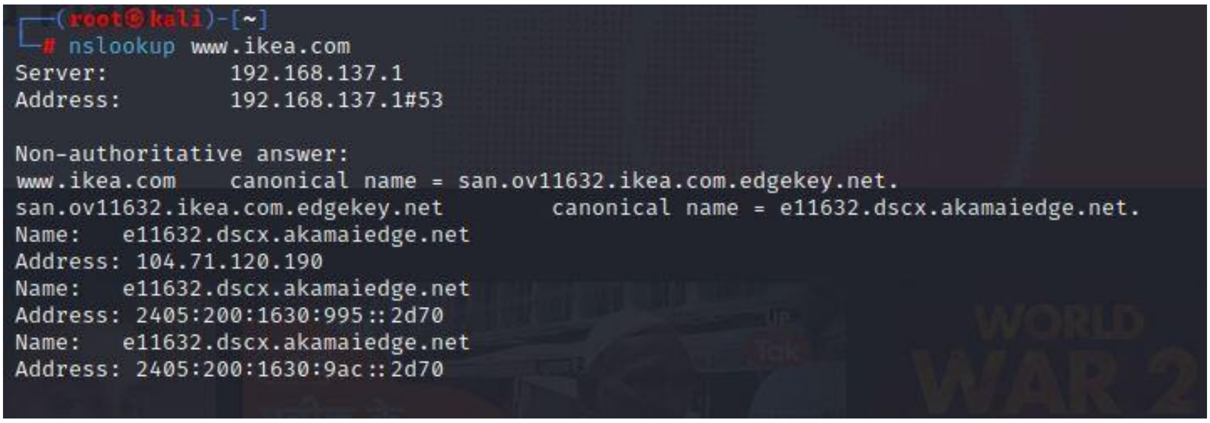
Saved 33,598 times between December 6, 1998 and April 19, 2023.

robots.txt



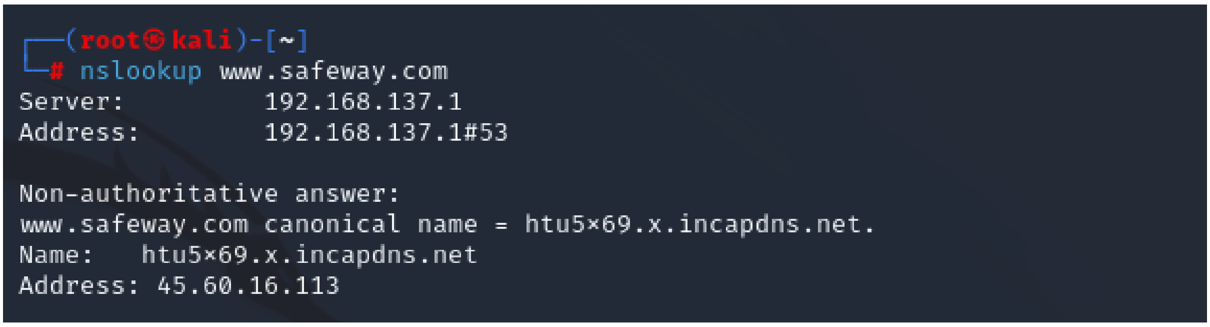
4/21/23, 3:02 PM https://www.ikea.com/robots.txt

```
# @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
# @@@@@@@@@@@@@@:                    :@@@@@@@@@@@@@@
# @@@@@@@@@#                              #@@@@@@@@@
# @@@@@@+                                    -@@@@@@
# @@@@                                          @@@@
# @@+    @@@@@ @@@@ @@@@  @@@@@@@@   @@@@@@      -@@
# @+     @@@@@ @@@@.@@@@  @@@@@@@@  -@@@@@@-      :@
# @      @@@@@ @@@@@@@@   @@@@      @@@@@@@@       @
# @      @@@@@ @@@@@@@@   @@@@@@@   @@@:@@@@.      @
# @      @@@@@ @@@@@@@@@  @@@@     .@@@@@@@@@      @
# @+     @@@@@ @@@@.@@@@- @@@@@@@@ @@@@ -@@@@.    :@
# @@+    @@@@@ @@@@ @@@@@ @@@@@@@@ @@@:  @@@@@   -@@
# @@@@                                          @@@@
# @@@@@@+                                    -@@@@@@
# @@@@@@@@@*                              +@@@@@@@@@
# @@@@@@@@@@@@@@:                    :@@@@@@@@@@@@@@
# @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

#
#  Our vision is to create a better everyday life for the many people. Fancy joining our mission at
IKEA?
#
#  Check out our jobs at the link below:
#
#  https://en-global-jobs.about.ikea.com/



User-Agent: AdsBot-Google
Allow: /*-fragment.html
Allow: /ext/
Allow: *filters=*

User-Agent: AdsBot-Google-Mobile
Allow: /*-fragment.html
Allow: /ext/
Allow: *filters=*

User-agent: *
Disallow: /compare*
Disallow: *?filter=*
Disallow: *?priceFilter*
Disallow: *?sorting=*
Disallow: *&sorting=*
Disallow: *?storeId=*
Disallow: /catalog/packagepopup/
Disallow: /iows/
Disallow: /ms/en_SE/
Disallow: /webapp/wcs/stores/servlet/*
Disallow: *OrderItemDisplay*
Disallow: *StockAvailSearchForm*
Disallow: *preferedui=desktop*
Disallow:  /catalog/productAlternative/
Disallow:  *bvroute=Review*
Disallow:  *bvtab*
Disallow:  *bvrrp*
Disallow: /retail/
Disallow: *?krypto=*
Disallow: */ideas/tags/
Disallow:  *compare=*
Disallow:  *krypto=*
Disallow:  *max_price=*
Disallow:  *maxprice=*
Disallow: *min_price=*
```

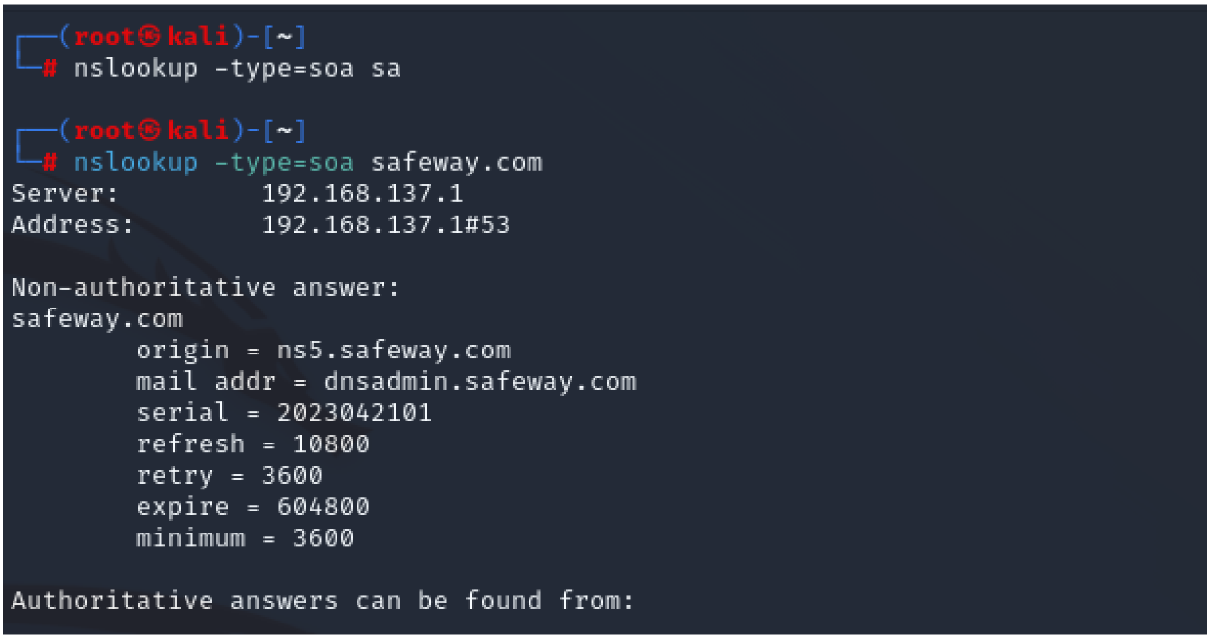


```
┌──(root㉿kali)-[~]
└─# nslookup www.ikea.com
Server:         192.168.137.1
Address:        192.168.137.1#53

Non-authoritative answer:
www.ikea.com    canonical name = san.ov11632.ikea.com.edgekey.net.
san.ov11632.ikea.com.edgekey.net        canonical name = e11632.dscx.akamaiedge.net.
Name:   e11632.dscx.akamaiedge.net
Address: 104.71.120.190
Name:   e11632.dscx.akamaiedge.net
Address: 2405:200:1630:995::2d70
Name:   e11632.dscx.akamaiedge.net
Address: 2405:200:1630:9ac::2d70
```

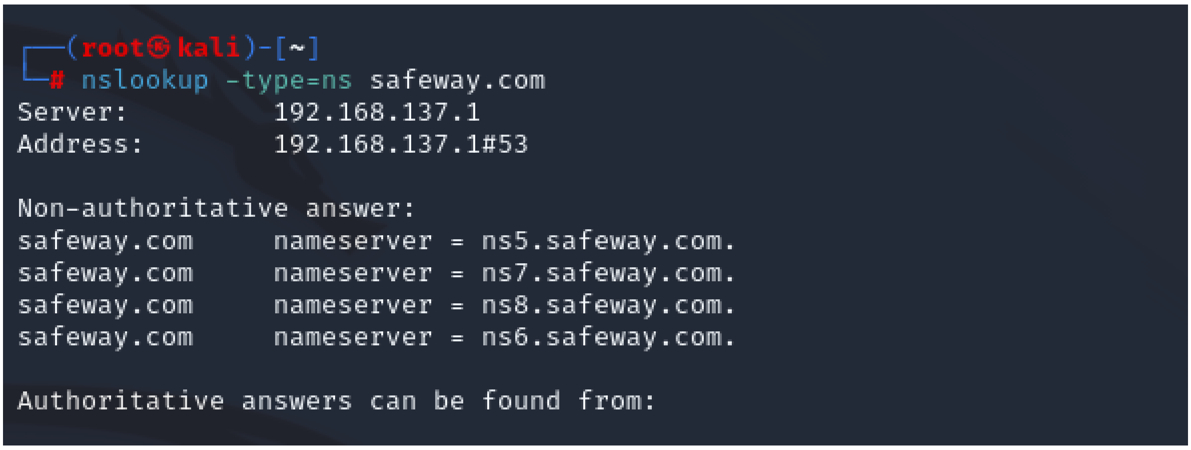
2. www.safeway.com



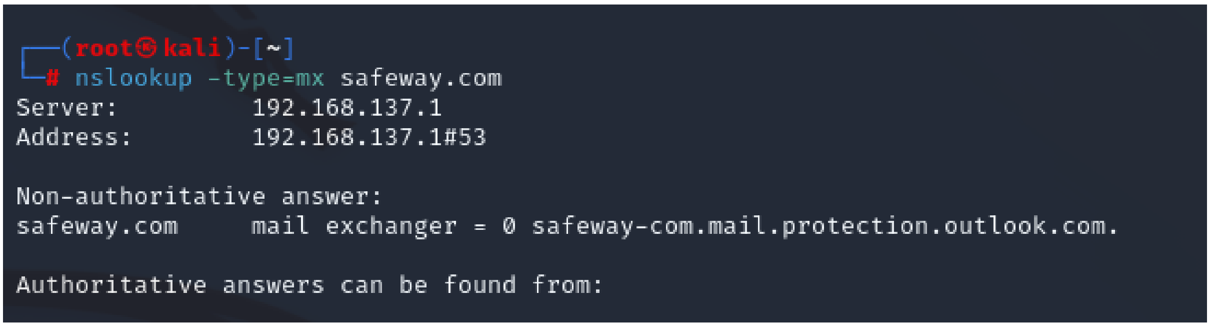
```
┌──(root㉿kali)-[~]
└─# nslookup www.safeway.com
Server:         192.168.137.1
Address:        192.168.137.1#53

Non-authoritative answer:
www.safeway.com canonical name = htu5×69.x.incapdns.net.
Name:   htu5×69.x.incapdns.net
Address: 45.60.16.113
```



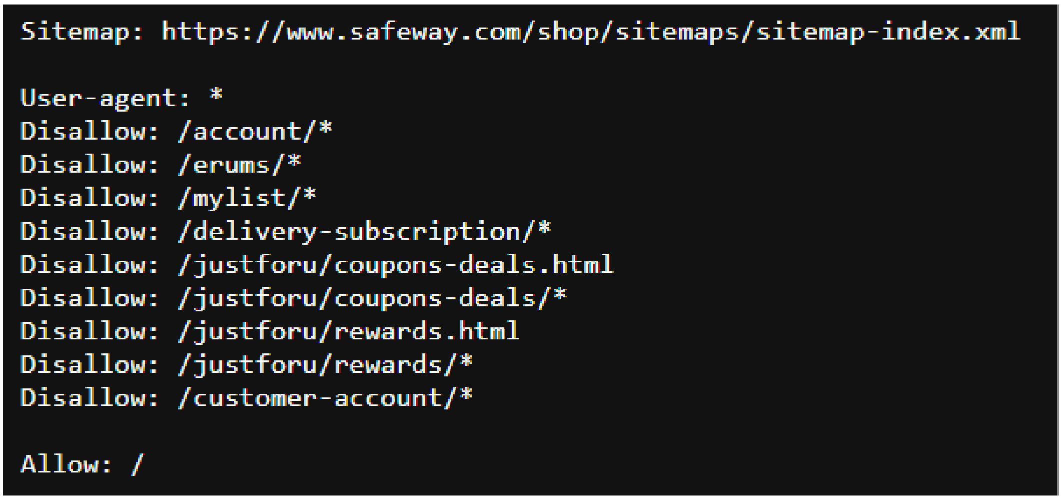
```
┌──(root㉿kali)-[~]
└─# nslookup -type=soa sa

┌──(root㉿kali)-[~]
└─# nslookup -type=soa safeway.com
Server:         192.168.137.1
Address:        192.168.137.1#53

Non-authoritative answer:
safeway.com
        origin = ns5.safeway.com
        mail addr = dnsadmin.safeway.com
        serial = 2023042101
        refresh = 10800
        retry = 3600
        expire = 604800
        minimum = 3600

Authoritative answers can be found from:
```



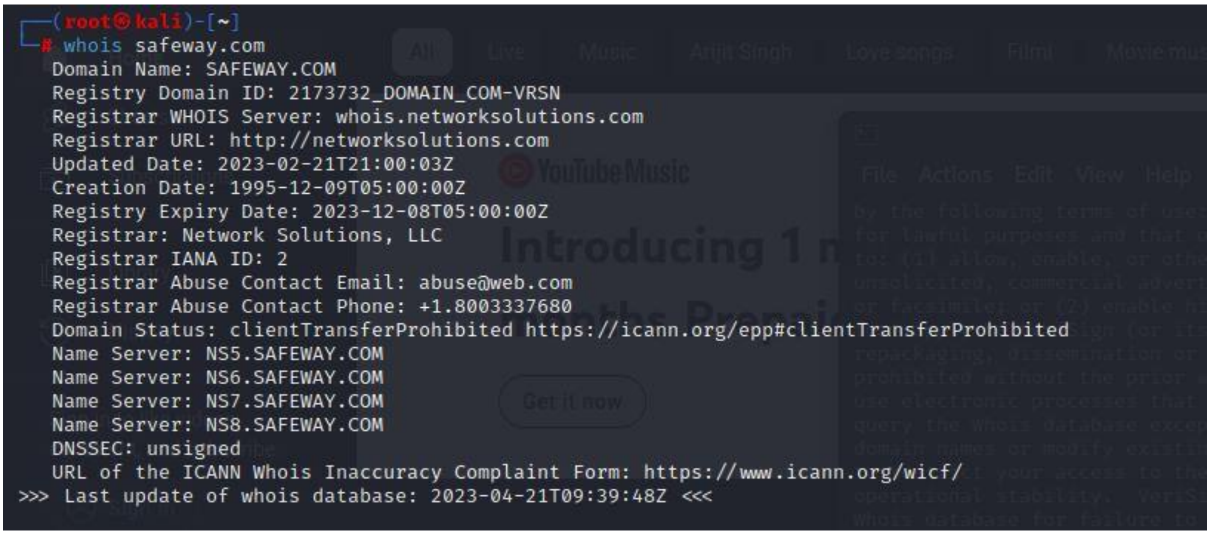
```
┌──(root㉿kali)-[~]
└─# nslookup -type=ns safeway.com
Server:         192.168.137.1
Address:        192.168.137.1#53

Non-authoritative answer:
safeway.com     nameserver = ns5.safeway.com.
safeway.com     nameserver = ns7.safeway.com.
safeway.com     nameserver = ns8.safeway.com.
safeway.com     nameserver = ns6.safeway.com.

Authoritative answers can be found from:
```



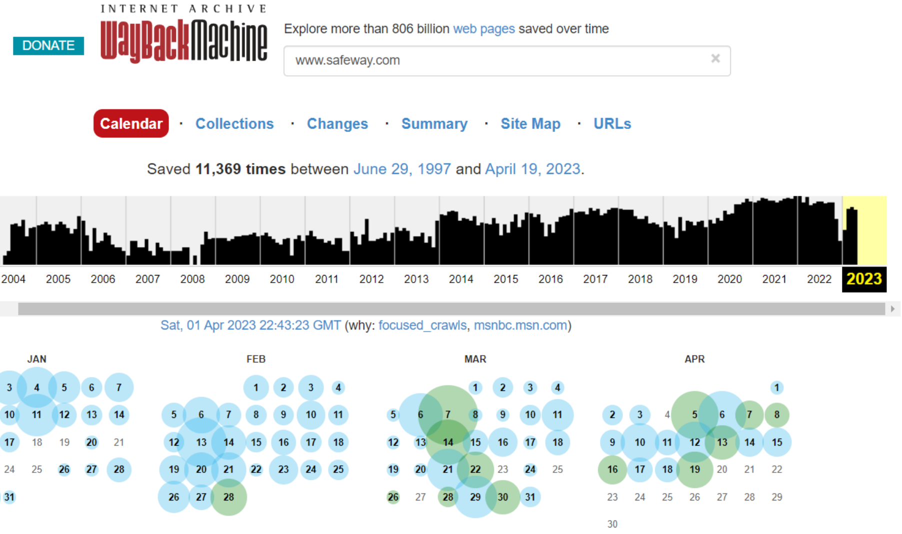
```
┌──(root㉿kali)-[~]
└─# nslookup -type=mx safeway.com
Server:         192.168.137.1
Address:        192.168.137.1#53

Non-authoritative answer:
safeway.com     mail exchanger = 0 safeway-com.mail.protection.outlook.com.

Authoritative answers can be found from:
```



```
Sitemap: https://www.safeway.com/shop/sitemaps/sitemap-index.xml

User-agent: *
Disallow: /account/*
Disallow: /erums/*
Disallow: /mylist/*
Disallow: /delivery-subscription/*
Disallow: /justforu/coupons-deals.html
Disallow: /justforu/coupons-deals/*
Disallow: /justforu/rewards.html
Disallow: /justforu/rewards/*
Disallow: /customer-account/*

Allow: /
```



```
┌──(root㉿kali)-[~]
└─# whois safeway.com
   Domain Name: SAFEWAY.COM
   Registry Domain ID: 2173732_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.networksolutions.com
   Registrar URL: http://networksolutions.com
   Updated Date: 2023-02-21T21:00:03Z
   Creation Date: 1995-12-09T05:00:00Z
   Registry Expiry Date: 2023-12-08T05:00:00Z
   Registrar: Network Solutions, LLC
   Registrar IANA ID: 2
   Registrar Abuse Contact Email: abuse@web.com
   Registrar Abuse Contact Phone: +1.8003337680
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS5.SAFEWAY.COM
   Name Server: NS6.SAFEWAY.COM
   Name Server: NS7.SAFEWAY.COM
   Name Server: NS8.SAFEWAY.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-04-21T09:39:48Z <<<
```



Explore more than 806 billion web pages saved over time

www.safeway.com

Calendar · Collections · Changes · Summary · Site Map · URLs

Saved **11,369 times** between June 29, 1997 and April 19, 2023.

Sat, 01 Apr 2023 22:43:23 GMT (why: focused_crawls, msnbc.msn.com)