domain enumeration

atg9999s.com

- Reconnaissance
  - whois scan on atg9999s.com

```
┌──(kali㉿kali)-[~]
└─$ whois atg9999s.com
 Domain Name: ATG9999S.COM
 Registry Domain ID: 2666292443_DOMAIN_COM-VRSN
 Registrar WHOIS Server: whois.godaddy.com
 Registrar URL: http://www.godaddy.com
 Updated Date: 2022-10-06T00:22:29Z
 Creation Date: 2022-01-05T20:23:49Z
 Registry Expiry Date: 2032-01-05T20:23:49Z
 Registrar: GoDaddy.com, LLC
 Registrar IANA ID: 146
 Registrar Abuse Contact Email: abuse@godaddy.com
 Registrar Abuse Contact Phone: 480-624-2505
 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
 Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
 Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
 Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
 Name Server: LELAND.NS.CLOUDFLARE.COM
 Name Server: OLLIE.NS.CLOUDFLARE.COM
 DNSSEC: unsigned
 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
Last update of whois database: 2023-11-17T21:06:24Z

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
```

```
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: atg9999s.com
Registry Domain ID: 2666292443_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2022-01-05T15:23:50Z
Creation Date: 2022-01-05T15:23:49Z
Registrar Registration Expiration Date: 2032-01-05T15:23:49Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 2155 E Warner Rd
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85284
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
```

```
Registrant Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=atg9999s.com
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 2155 E Warner Rd
Admin City: Tempe
Admin State/Province: Arizona
Admin Postal Code: 85284
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=atg9999s.com
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 2155 E Warner Rd
Tech City: Tempe
Tech State/Province: Arizona
Tech Postal Code: 85284
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=atg9999s.com
Name Server: LELAND.NS.CLOUDFLARE.COM
Name Server: OLLIE.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
Last update of WHOIS database: 2023-11-17T21:06:37Z
For more information on Whois status codes, please visit https://icann.org/epp

TERMS OF USE: The data contained in this registrar's Whois database, while believed by the
registrar to be reliable, is provided "as is" with no guarantee or warranties regarding its
accuracy. This information is provided for the sole purpose of assisting you in obtaining
information about domain name registration records. Any use of this data for any other purpose
is expressly forbidden without the prior written permission of this registrar. By submitting
an inquiry, you agree to these terms and limitations of warranty. In particular, you
```

```
agree not
to use this data to allow, enable, or otherwise support the dissemination or
collection of this
data, in part or in its entirety, for any purpose, such as transmission by e-mail,
telephone,
postal mail, facsimile or other means of mass unsolicited, commercial advertising or
solicitations
of any kind, including spam. You further agree not to use this data to enable high
volume, automated
or robotic electronic processes designed to collect or compile this data for any
purpose, including
mining this data for your own personal or commercial purposes. Failure to comply with
these terms
may result in termination of access to the Whois database. These terms may be subject
to modification
at any time without notice.
```

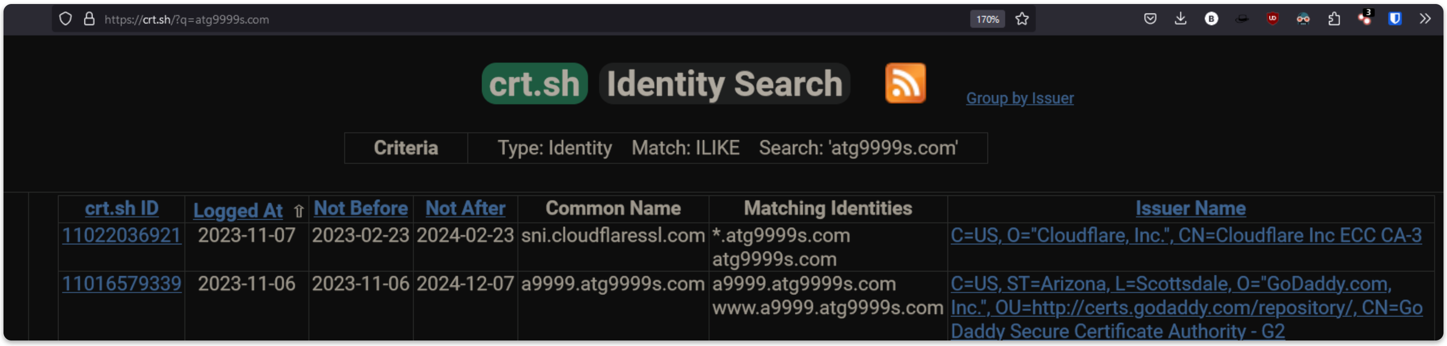
```

 - nslookup results reveal domain ip address of 34.102.136.180
```

```
┌──(kali㉿kali)-[~]
└─$ nslookup atg9999s.com
Server:         24.154.1.12
Address:        24.154.1.12#53

Non-authoritative answer:
Name:   atg9999s.com
Address: 34.102.136.180
```

- searched on https://crt.sh
  - results available at https://crt.sh/?q=atg9999s.com



https://crt.sh/?q=atg9999s.com

crt.sh Identity Search

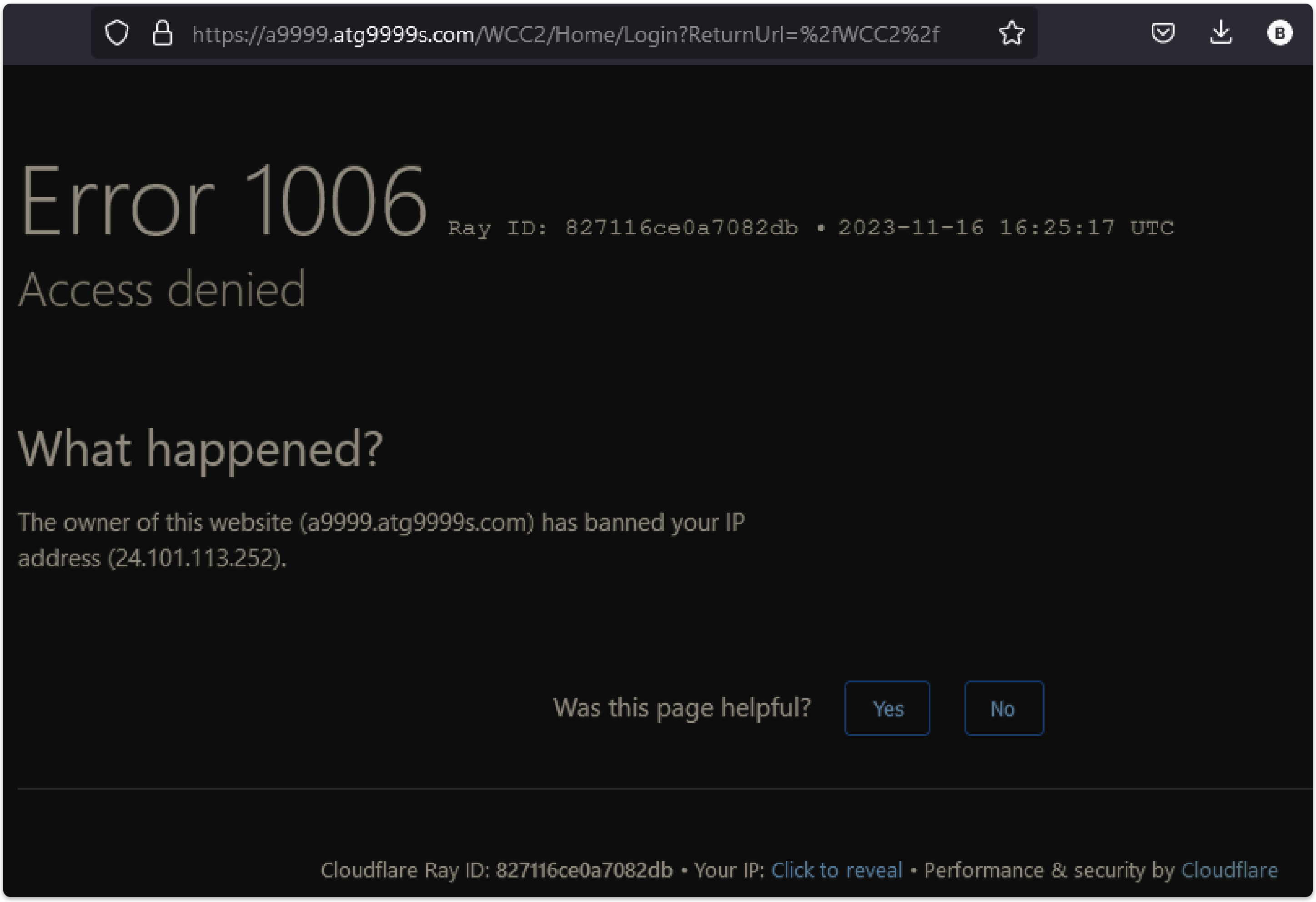
Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'atg9999s.com'

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
11022036921	2023-11-07	2023-02-23	2024-02-23	sni.cloudflaressl.com	*.atg9999s.com atg9999s.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
11016579339	2023-11-06	2023-11-06	2024-12-07	a9999.atg9999s.com	a9999.atg9999s.com www.a9999.atg9999s.com	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2

- Navigated to the 2nd url on the list and was immediately banned
- the website a9999.atg9999s.com may be banning all who connect

- My home ip 24.101.113.252



https://a9999.atg9999s.com/WCC2/Home/Login?ReturnUrl=%2fWCC2%2f

Error 1006

Ray ID: 827116ce0a7082db • 2023-11-16 16:25:17 UTC

Access denied

What happened?

The owner of this website (a9999.atg9999s.com) has banned your IP address (24.101.113.252).

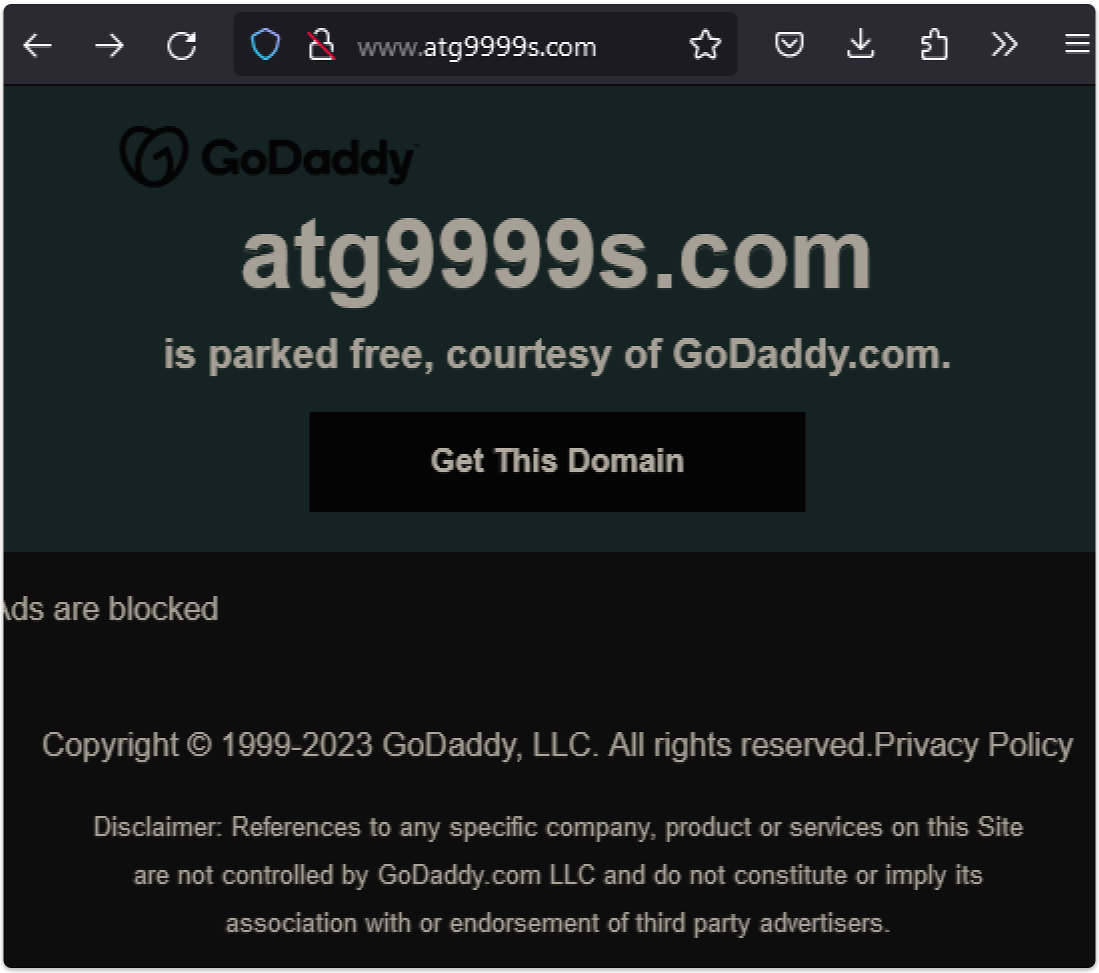
Was this page helpful?
Yes
No

Cloudflare Ray ID: 827116ce0a7082db • Your IP: Click to reveal • Performance & security by Cloudflare

no connection here to arcistg.com from Jeff's profile

- navigating to the TLD http://atg9999s.com and godaddy advertises that the domain is parked free
  - Parked for free means that the owner of the domain name hasn’t developed a site yet and temporarily he uses his domain registrar’s (ex. Godaddy) nameservers. Registrars usually promote their services on parked domains or they show ads.

- clicking through godaddy link reveals that the domain is not available. But could be?



GoDaddy

atg9999s.com

is parked free, courtesy of GoDaddy.com.

ds are blocked

Privacy Policy

Disclaimer: References to any specific company, product or services on this Site are not controlled by GoDaddy.com LLC and do not constitute or imply its association with or endorsement of third party advertisers.

- I changed my ip using a VPN - THM 10.6.9.143 and tried again

```
┌──(kali㉿kali)-[~]
└─$ ping atg9999s.com
PING atg9999s.com (34.102.136.180) 56(84) bytes of data.
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=1 ttl=117
time=21.3 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=2 ttl=117
time=20.0 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=3 ttl=117
time=22.6 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=4 ttl=117
time=16.6 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=5 ttl=117
time=14.7 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq=6 ttl=117
time=23.5 ms
^C
--- atg9999s.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 9103ms
rtt min/avg/max/mdev = 14.692/19.766/23.485/3.167 ms
```

- Need to run nmap to scan the ip but I'm concerned about being detected
- modifying my normal nmap scan down to avoid detection

- I couldn't remember the top 100 most common ports and discovered port 100 filtered with newacct service running on it.

```
┌──(root💀RCS-Response1)-[~]
└─# nmap -p100 -T2 -v -Pn 34.102.136.180
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be
slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-11-18 12:48 EST
Initiating Parallel DNS resolution of 1 host. at 12:48
Completed Parallel DNS resolution of 1 host. at 12:48, 0.09s elapsed
Initiating SYN Stealth Scan at 12:48
Scanning 180.136.102.34.bc.googleusercontent.com (34.102.136.180) [1 port]
Completed SYN Stealth Scan at 12:48, 2.41s elapsed (1 total ports)
Nmap scan report for 180.136.102.34.bc.googleusercontent.com (34.102.136.180)
Host is up.

PORT    STATE    SERVICE
100/tcp filtered newacct

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.68 seconds
           Raw packets sent: 2 (88B) | Rcvd: 0 (0B)
```

- `-F` top 100 most common ports scan reveals 80 and 443 open

```
┌──(root💀RCS-Response1)-[~]
└─# nmap -F -T2 -v -Pn 34.102.136.180
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be
slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-11-18 12:49 EST
Initiating Parallel DNS resolution of 1 host. at 12:49
Completed Parallel DNS resolution of 1 host. at 12:49, 0.02s elapsed
Initiating SYN Stealth Scan at 12:49
Scanning 180.136.102.34.bc.googleusercontent.com (34.102.136.180) [100 ports]
Discovered open port 80/tcp on 34.102.136.180
Discovered open port 443/tcp on 34.102.136.180
SYN Stealth Scan Timing: About 26.50% done; ETC: 12:51 (0:01:26 remaining)
SYN Stealth Scan Timing: About 60.50% done; ETC: 12:51 (0:00:40 remaining)
Completed SYN Stealth Scan at 12:51, 98.23s elapsed (100 total ports)
Nmap scan report for 180.136.102.34.bc.googleusercontent.com (34.102.136.180)
Host is up (0.089s latency).
Not shown: 98 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
```

```
443/tcp open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 98.38 seconds
           Raw packets sent: 217 (9.548KB) | Rcvd: 20 (880B)
```

- I also ran a long slow scan over the weekend to attempt to avoid detection.

```
┌──(root💀RCS-Response1)-[~]
└─# nmap -p- -T2 -v -Pn 34.102.136.180
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-11-18 14:20 EST
Initiating Parallel DNS resolution of 1 host. at 14:20
Completed Parallel DNS resolution of 1 host. at 14:20, 0.09s elapsed
Initiating SYN Stealth Scan at 14:20
Scanning 180.136.102.34.bc.googleusercontent.com (34.102.136.180) [65535 ports]
Discovered open port 443/tcp on 34.102.136.180
Discovered open port 80/tcp on 34.102.136.180
Increasing send delay for 34.102.136.180 from 400 to 800 due to 13 out of 43 dropped probes since last increase.
SYN Stealth Scan Timing: About 0.30% done
SYN Stealth Scan Timing: About 0.32% done
SYN Stealth Scan Timing: About 0.33% done
SYN Stealth Scan Timing: About 0.34% done
SYN Stealth Scan Timing: About 0.35% done
SYN Stealth Scan Timing: About 0.36% done
SYN Stealth Scan Timing: About 0.38% done
SYN Stealth Scan Timing: About 0.39% done
SYN Stealth Scan Timing: About 0.41% done
SYN Stealth Scan Timing: About 0.42% done
SYN Stealth Scan Timing: About 0.44% done
SYN Stealth Scan Timing: About 0.45% done
SYN Stealth Scan Timing: About 0.48% done
SYN Stealth Scan Timing: About 0.49% done
SYN Stealth Scan Timing: About 0.51% done
SYN Stealth Scan Timing: About 0.53% done
SYN Stealth Scan Timing: About 0.56% done
SYN Stealth Scan Timing: About 0.58% done
SYN Stealth Scan Timing: About 0.61% done
SYN Stealth Scan Timing: About 0.64% done
SYN Stealth Scan Timing: About 0.66% done
SYN Stealth Scan Timing: About 0.68% done
SYN Stealth Scan Timing: About 0.71% done
SYN Stealth Scan Timing: About 0.73% done
SYN Stealth Scan Timing: About 0.76% done
SYN Stealth Scan Timing: About 0.78% done
SYN Stealth Scan Timing: About 0.81% done
SYN Stealth Scan Timing: About 0.83% done
SYN Stealth Scan Timing: About 0.86% done
SYN Stealth Scan Timing: About 0.89% done
SYN Stealth Scan Timing: About 0.91% done
SYN Stealth Scan Timing: About 0.94% done
SYN Stealth Scan Timing: About 0.96% done
SYN Stealth Scan Timing: About 0.99% done
SYN Stealth Scan Timing: About 1.01% done; ETC: 05:04 (38:20:32 remaining)
SYN Stealth Scan Timing: About 1.41% done; ETC: 03:16 (36:23:54 remaining)
SYN Stealth Scan Timing: About 2.80% done; ETC: 01:53 (34:32:59 remaining)
SYN Stealth Scan Timing: About 4.47% done; ETC: 00:39 (32:46:08 remaining)
Stats: 2:21:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 7.02% done; ETC: 23:52 (31:10:12 remaining)
SYN Stealth Scan Timing: About 11.28% done; ETC: 23:35 (29:29:38 remaining)
SYN Stealth Scan Timing: About 16.53% done; ETC: 23:41 (27:49:52 remaining)
SYN Stealth Scan Timing: About 21.01% done; ETC: 23:28 (26:09:44 remaining)
SYN Stealth Scan Timing: About 26.12% done; ETC: 23:31 (24:30:22 remaining)
adjust_timeouts2: packet supposedly had rtt of 8448282 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 8448282 microseconds.  Ignoring time.
SYN Stealth Scan Timing: About 30.88% done; ETC: 23:24 (22:50:51 remaining)
SYN Stealth Scan Timing: About 35.86% done; ETC: 23:23 (21:11:37 remaining)
SYN Stealth Scan Timing: About 40.78% done; ETC: 23:20 (19:32:28 remaining)
SYN Stealth Scan Timing: About 45.63% done; ETC: 23:15 (17:53:28 remaining)
SYN Stealth Scan Timing: About 50.52% done; ETC: 23:10 (16:14:43 remaining)
SYN Stealth Scan Timing: About 55.44% done; ETC: 23:06 (14:36:13 remaining)
SYN Stealth Scan Timing: About 60.41% done; ETC: 23:05 (12:57:52 remaining)
SYN Stealth Scan Timing: About 65.37% done; ETC: 23:03 (11:19:35 remaining)
SYN Stealth Scan Timing: About 70.34% done; ETC: 23:01 (9:41:24 remaining)
SYN Stealth Scan Timing: About 75.32% done; ETC: 22:58 (8:03:21 remaining)
SYN Stealth Scan Timing: About 80.31% done; ETC: 22:58 (6:25:25 remaining)
SYN Stealth Scan Timing: About 85.32% done; ETC: 22:59 (4:47:31 remaining)
SYN Stealth Scan Timing: About 90.32% done; ETC: 22:58 (3:09:34 remaining)
SYN Stealth Scan Timing: About 95.32% done; ETC: 22:58 (1:31:38 remaining)
Completed SYN Stealth Scan at 22:57, 117409.93s elapsed (65535 total ports)
Nmap scan report for 180.136.102.34.bc.googleusercontent.com (34.102.136.180)
Host is up (0.052s latency).
Not shown: 65533 filtered ports
PORT    STATE SERVICE
```

```
80/tcp  open  http
443/tcp open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 117410.13 seconds
           Raw packets sent: 144174 (6.344MB) | Rcvd: 13143 (578.292KB)
```

- Another nmap scan to detect versions running on open ports.
-
- 80 openresty and 443 tcpwrapped
- robots.txt exists

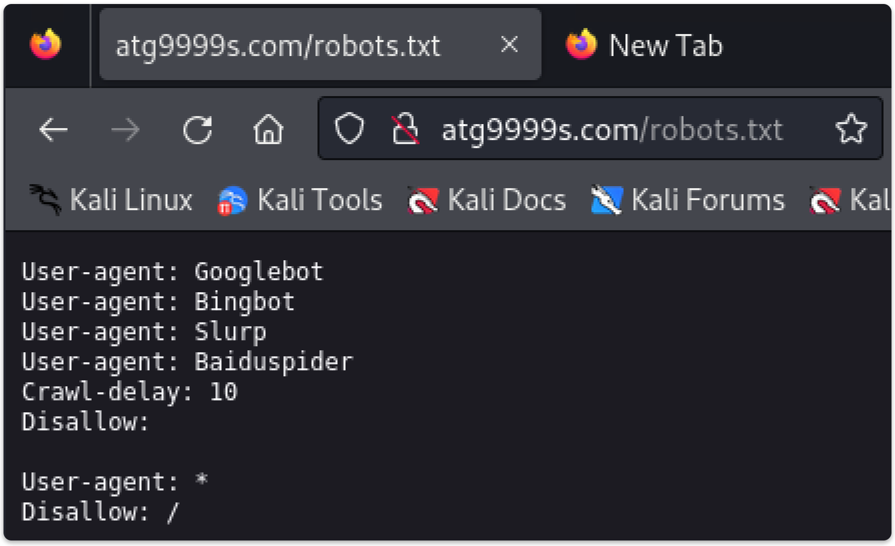
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80,443 -A 34.102.136.180
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 07:09 EST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 07:10 (0:00:28 remaining)
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 07:11 (0:00:43 remaining)
Nmap scan report for 180.136.102.34.bc.googleusercontent.com (34.102.136.180)
Host is up (0.022s latency).

PORT    STATE SERVICE    VERSION
80/tcp  open  http       openresty
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: openresty
|_http-title: Site doesn't have a title (text/html).
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 403 Forbidden
|     Server: openresty
|     Date: Mon, 20 Nov 2023 16:58:03 GMT
|     Content-Type: text/html
|     Content-Length: 291
|     ETag: "6552adee-123"
|     Via: 1.1 google
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta http-equiv="content-type" content="text/html;charset=utf-8" />
|     <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon" />
|     <title>Forbidden</title>
|     </head>
|     <body>
|     <h1>Access Forbidden</h1>
|     </body>
|     </html>
|   GetRequest:
|     HTTP/1.0 403 Forbidden
|     Server: openresty
|     Date: Mon, 20 Nov 2023 16:57:58 GMT
|     Content-Type: text/html
|     Content-Length: 291
|     ETag: "6552adee-123"
|     Via: 1.1 google
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta http-equiv="content-type" content="text/html;charset=utf-8" />
|     <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon" />
|     <title>Forbidden</title>
|     </head>
|     <body>
|     <h1>Access Forbidden</h1>
|     </body>
|     </html>
|   HTTPOptions:
|     HTTP/1.0 403 Forbidden
|     Server: openresty
|     Date: Mon, 20 Nov 2023 16:57:58 GMT
|     Content-Type: text/html
|     Content-Length: 150
|     Via: 1.1 google
|     <html>
|     <head><title>403 Forbidden</title></head>
|     <body>
|     <center><h1>403 Forbidden</h1></center>
|     <hr><center>openresty</center>
|     </body>
|     </html>
|   RTSPRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/html; charset=UTF-8
|     Referrer-Policy: no-referrer
|     Content-Length: 273
|     Date: Mon, 20 Nov 2023 16:57:58 GMT
|     <html><head>
|     <meta http-equiv="content-type" content="text/html;charset=utf-8">
|     <title>400 Bad Request</title>
|     </head>
|     <body text=#000000 bgcolor=#ffffff>
|     <h1>Error: Bad Request</h1>
|     <h2>Your client has issued a malformed or illegal request.</h2>
|     <h2></h2>
|_    </body></html>
443/tcp open  tcpwrapped
```

```
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-service :
SF-Port80-TCP:V=7.94%I=7%D=11/20%Time=655B4C8A%P=x86_64-pc-linux-gnu%r(Get
SF:Request,1CA,"HTTP/1\.0\x20403\x20Forbidden\r\nServer:\x20openresty\r\nD
SF:ate:\x20Mon,\x2020\x20Nov\x202023\x2016:57:58\x20GMT\r\nContent-Type:\x
SF:20text/html\r\nContent-Length:\x20291\r\nETag:\x20\"6552adee-123\"\r\nV
SF:ia:\x201\.1\x20google\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en\">\
SF:n\x20\x20<head>\n\x20\x20\x20\x20<meta\x20http-equiv=\"content-type\"\x
SF:20content=\"text/html;charset=utf-8\"\x20/>\n\x20\x20\x20\x20<link\x20r
SF:el=\"shortcut\x20icon\"\x20href=\"data:image/x-icon;,\"\x20type=\"image
SF:/x-icon\"\x20/>\n\x20\x20\x20\x20<title>Forbidden</title>\n\x20\x20</he
SF:ad>\n\x20\x20<body>\n\x20\x20\x20\x20<h1>Access\x20Forbidden</h1>\n\x20
SF:\x20</body>\n</html>\n")%r(HTTPOptions,127,"HTTP/1\.0\x20403\x20Forbidd
SF:en\r\nServer:\x20openresty\r\nDate:\x20Mon,\x2020\x20Nov\x202023\x2016:
SF:57:58\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x20150\r\
SF:nVia:\x201\.1\x20google\r\n\r\n<html>\r\n<head><title>403\x20Forbidden<
SF:/title></head>\r\n<body>\r\n<center><h1>403\x20Forbidden</h1></center>\
SF:r\n<hr><center>openresty</center>\r\n</body>\r\n</html>\r\n")%r(RTSPReq
SF:uest,1AD,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/h
SF:tml;\x20charset=UTF-8\r\nReferrer-Policy:\x20no-referrer\r\nContent-Len
SF:gth:\x20273\r\nDate:\x20Mon,\x2020\x20Nov\x202023\x2016:57:58\x20GMT\r\
SF:n\r\n\n<html><head>\n<meta\x20http-equiv=\"content-type\"\x20content=\"
SF:text/html;charset=utf-8\">\n<title>400\x20Bad\x20Request</title>\n</hea
SF:d>\n<body\x20text=#000000\x20bgcolor=#ffffff>\n<h1>Error:\x20Bad\x20Req
SF:uest</h1>\n<h2>Your\x20client\x20has\x20issued\x20a\x20malformed\x20or\
SF:x20illegal\x20request\.</h2>\n<h2></h2>\n</body></html>\n")%r(FourOhFou
SF:rRequest,1CA,"HTTP/1\.0\x20403\x20Forbidden\r\nServer:\x20openresty\r\n
SF:Date:\x20Mon,\x2020\x20Nov\x202023\x2016:58:03\x20GMT\r\nContent-Type:\
SF:x20text/html\r\nContent-Length:\x20291\r\nETag:\x20\"6552adee-123\"\r\n
SF:Via:\x201\.1\x20google\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en\">
SF:\n\x20\x20<head>\n\x20\x20\x20\x20<meta\x20http-equiv=\"content-type\"\
SF:x20content=\"text/html;charset=utf-8\"\x20/>\n\x20\x20\x20\x20<link\x20
SF:rel=\"shortcut\x20icon\"\x20href=\"data:image/x-icon;,\"\x20type=\"imag
SF:e/x-icon\"\x20/>\n\x20\x20\x20\x20<title>Forbidden</title>\n\x20\x20</h
SF:ead>\n\x20\x20<body>\n\x20\x20\x20\x20<h1>Access\x20Forbidden</h1>\n\x2
SF:0\x20</body>\n</html>\n");
```

- robots.txt reveals
  - user-agents - specifies rules for specific web crawlers, Googlebot, Bingbot, Slurp and Baiduspider
  - Crawl-delay - permitted to crawl with a delay of 10 sec between requests
  - Disallow: blank no specific paths are disallowed for theses bots
  - user-agent: * - all others
  - Disallow: / - not permitted to crawl any part of the site
  - Consider Disallowing all web crawlers to ensure that any bot regardless of it's identity, is barred

from accessing any part of the domain.



```
User-agent: Googlebot
User-agent: Bingbot
User-agent: Slurp
User-agent: Baiduspider
Crawl-delay: 10
Disallow:

User-agent: *
Disallow: /
```

- Quick search on metasploit and searchsploit did not yield any existing vulnerabilities.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole


     ,           ,
        /             \
((__---,,,---__))
(_) O O (_)_________
\ _ /            |\
o_o \   M S F   | \
\   _____  |  *
|||   WW|||
|||     |||



       =[ metasploit v6.3.31-dev                          ]
+ -- --=[ 2346 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1390 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search openresty
[-] No results from search
msf6 > tcpwrapped
[-] Unknown command: tcpwrapped
msf6 > search tcpwrapped
[-] No results from search
msf6 > exit

┌──(kali㉿kali)-[~]
└─$ searchsploit openresty
```

```
Exploits: No Results
Shellcodes: No Results
```