Network Security Practices
CY 5150 – Fall 2020
Alexander Semaan

Open-Source Intelligence Reconnaissance

Grantham, Mayo, Van Otterloo & Co. LLC

I. Executive Summary

From a general perspective, GMO has a good cybersecurity posture when it comes to open source intelligence reconnaissance. However, there are quite a few security controls that should be put in place to mitigate the damage from some information's exposure. For instance, it appears that about 103 subdomains for gmo.com are publicly available, some of which should not. Investing in a CDN service (Content Delivery Network service) as well as a DDoS protection service (such as Cloudfare) can go a long way in protecting GMO's domain and subdomains. If such a service already exists, as soon as new subdomains are added, make sure you are declaring them that service.

Looking at social media exposure and emails exposure, the only outstanding elements are LinkedIn Profiles and the email contact information for the 'gmo.com' domain WHOIS. To protect against social media attacks, include social media policies in employees' Security Awareness, Training and Education program, and encourage employees to configure their privacy settings on these platforms appropriately. Do not put a GMO email address as the contact information on the domain's WHOIS; instead, register a different email, and forward the emails to the current contact on the WHOIS (Mike T.).

Concerning the 'gmo.com' web server, it appears that it allows outdated protocols (TLS 1.0 and 1,1) and should omit these protocols if there are no business requirements for them. Additionally, make sure that exposed subdomains have a requirement to be open to the internet. In the case where they do, make sure that services or apps on these subdomains are protected by DDoS mitigation services, and that any login forms or authentication processes use MFA (Multi-Factor Authentication). Also, to protect against OS fingerprinting and scanning attacks on your internet-facing servers, make sure that you install the appropriate kernel modules on those servers, which protect against most detection and scanning tools.

Finally, regarding the DNS servers, DNSSec should be implemented to prevent DNS cache poisoning or spoofing attacks. Furthermore, remove all TXT records, because all they do is advertise machine types and services running and they result in giving out unnecessary information. If not implemented already, split your DNS Zone into an External and Internal DNS Zone, so that apps and services that shouldn't have external access are not advertised on the internet, and limit DNS Zone transfers.

II. Introduction

Grantham, Mayo, Van Otterloo & Co. (GMO for short), is an investments management company providing portfolio management and consulting services to pooled investment vehicles and private investment funds. They've handled about 70 billion dollars in 2019 as AUM (Assets Under Management). GMO has about 600 employees to date and their headquarters are located in Downtown Boston, but they also have branches all over the world: in Sydney, London, Amsterdam, Singapore, San Francisco and Tokyo.

GMO's web app domain is 'www.gmo.com' and it is the domain that will be used for most tools, as well as 'gmo.com'.

III. Tools and Findings

1. Sublist3r

a. Tool Description

Sublist3r is a domain harvesting tool that uses different search engine APIs (Google, Yahoo, Bing, Ask, Baidu, and many more) to enumerate sub-domains. Sublist3r strictly uses search engines and returns data that is publicly available on the internet. The format of the data output by the tool is simple: it returns the number of total unique subdomains found, followed by a list of all these subdomains.

b. Information Discovered

By running GMO's domain name on Sublist3r, I discovered that gmo.com has 103 subdomains. The list of these subdomains can be found in *Appendix 1*. Some examples of notable subdomains found are: adfs.gmo.com, apps.gmo.com, as-mobile.gmo.com, as-mobiledev.gmo.com, directaccessmar.gmo.com, remote.gmo.com, ftp.gmo.com, ftps.gmo.com, itapps.gmo.com, zix01.gmo.com.

c. Negative Impact

By getting a list of gmo.com's subdomains, a potential threat actor can get his hands on a larger surface area to attack. Additionally, subdomains can reveal a substantial amount of information and can help threat actors understand GMO's network infrastructure, including which applications are running. The attacker can then target specific applications that might have unpatched vulnerabilities, or even attempt DDoS attacks on certain apps or services.

d. Suggested Controls

Investing in a CDN service (Content Delivery Network service) as well as a DDoS protection service can go a long way in protecting GMO's domain and subdomains. One of the best services in the security industry for DDoS mitigation and CDN is offered by Cloudfare. The damage is already done for subdomains that are already created and available on the internet, however what one can do is make sure that the subdomain is only accessible internally if there is no requirements for remote use or external network access. Furthermore, when creating or activating new subdomains, immediate use of a CDN/DDoS mitigation service will protect your subdomains against passive and sometimes active reconnaissance techniques.

2. theHarvester

a. Tool Description

theHarvester is an information gathering tool that queries multiple search engines APIs (Google, Yahoo, Bing, Ask, Baidu, and many more) looking for email addresses, employee names, usernames, hosts, IPs and more. This tool can also be used for active reconnaissance to scan ports of detected hosts and attempt Takeover attacks, however for the purpose of this assignment only publicly available information (passive reconnaissance) will be used. Like Sublist3r, this tool completes its searches based on the domain address (gmo.com) that one inputs.

b. Information Discovered

First, the positive side is that no IPs, emails, Trello URLs, Github code, VirusTotal results were found. The only information harvested was LinkedIn Profile URLs, and it found 91 of them. Please refer to Appendix 2 for the list of URLs.

c. Negative Impact

Being able to view GMO employees' LinkedIn profiles can help attackers increase their attack surface, as they can now target employees via LinkedIn by setting up phishing scams, that can use employee impersonation to get the victim to click on malicious links or perform certain tasks. Additionally, being able to see employees' profiles can help an attacker better understand the hierarchy within GMO and see the role of employees or how long they've been working at GMO to figure out the ideal target.

d. Suggested Controls

With the quick growth of social media, most companies and individuals need to have a presence on LinkedIn, so there is no way around having LinkedIn profiles available to the public. However, there are profile privacy settings that should be well configured to limit the exposure of your profile and make it available only to your network. GMO should include LinkedIn in their Security Awareness, Training and Education program, and should encourage employees to configure their privacy settings appropriately.

3. Qualys' SSL Server Test

a. Tool Description

The Qualys SSL Server Test gives TLS certificate information including the TLS version, all possible cipher suites being used for key exchange, possible vulnerabilities (scans for multiple CVEs) and if mitigation controls are in place for vulnerabilities (for TLS downgrade attacks for example). It also gives the tested server a rating and generates a report.

b. Information Discovered

First off, I tested 'www.gmo.com' and the results of the scan were near perfect with an overall rating of A+. The server supports TLS 1.3 and 1.2 and has TLS 1.1, TLS 1.0, SSL 3 and SSL 2 disabled, which is compliant with best security practices for web app protocols.

Additionally, the server key and certificate appear to be trusted and valid, and the cipher suites used for TLS are strong overall.
On another note, I tested ‘gmo.com’ and the results of the scan weren’t too great with an overall rating of B, mainly because it supports TLS 1.0 and 1.1.
Please refer to Appendix 3 for detailed findings.

c. Negative Impact
With this information, the attacker cannot do anything to attack ‘www.gmo.com’. However, the attacker can see that ‘gmo.com’ is not as secure and might be able to leverage certain attacks on TLS 1.0 and 1.1

d. Suggested Controls
Disable TLS 1.0 and 1.1, and enable TLS 1.2 and 1.3 if possible. Otherwise, make sure that requests coming to ‘gmo.com’ are redirected to ‘www.gmo.com’ by configuring the DNS records appropriately.

4. Shodan

a. Tool Description
Shodan is a search engine similar to Google, Yahoo and others, except that it searches for specific devices that are connected to the internet. It does that by collecting the service banners, considered a type of metadata that servers return when a request is sent to it. This data includes IP addresses, open ports, application/processes running with their version, server certificates and more.

b. Information Discovered
By looking up ‘gmo’ and ‘gmo.com’, the results that come back are pretty clean and do not contain a lot of information on GMO’s servers. The information found through Shodan is limited to the organization’s name (Grantham, Mayo, Van Otterloo & Co. LLC), GMO’s TLS certificate issuer (Certificate Authority – DigiCert Inc. in this case), the TLS version supported (TLSv1.2) and the IPv6 address for www.gmo.com (2606:4700::6813:f051 which appears to be owned by Cloudflare).

c. Negative Impact
An attacker cannot do much with the information gathered from Shodan, other than get the IPv6 address for ‘www.gmo.com’ and know that GMO uses Cloudfare as a CDN and DDoS Mitigation service. There are no ports exposed or services/apps running exposed nor their versions for that matter.

d. Suggested Controls
None are needed.

5. Censys

a. Tool Description

Used for similar purposes as Shodan, Censys is considered a public search engine that reveals the information that internet-facing hosts give out. This information includes IP addresses, open ports, application/processes running with their version, server certificates and can give insights on the network infrastructure behind the hosts, all while listing potential vulnerabilities for these hosts.

b. Information Discovered

Censys returned 15 results for ‘gmo.com’, 2 of which are Cloudfare hosts for ‘www.gmo.com’, which only reveal IP addresses (104.19.239.81 and 104.19.240.81) and standard HTTP and HTTPS ports open (80, 8080 and 443). However, the other results are from DNS relays and databases that expose multiple subdomains, IPs and the geo-location of the servers. Some examples: apps.gmo.com, citrixcallback1.gmo.com, citrixcallback2.gmo.com - 13.75.139.155 – Sydney, Australia | directaccessbedv2.gmo.com - 69.147.188.45 – Marlborough, MA, USA. Refer to Appendix 4 for additional details.

c. Negative Impact

The discovery of the Cloudfare hosts is nothing to be worried about as they offer assurance on their services. More importantly, the information that DNS relays and databases exposes is a bit more worrisome but not as bad as it may seem. In fact, a threat actor can gather intel on subdomains, their IP addresses, their physical location, as well as open ports that subdomains respond to. This information can reveal the application running on that subdomain and potential vulnerabilities targeting certain ports, applications or services.

d. Suggested Controls

Make sure that the exposed subdomains are not open to the internet, unless it is a requirement for the application or service running on it to be accessed remotely. In the latter’s case, you cannot prevent the subdomain from being stored by DNS relays or databases. However, what you can do is make sure that those services or apps open to the internet are protected by DDoS mitigation services, and that any login forms or authentication processes use MFA (Multi-Factor Authentication).

6. DNSRecon

a. Tool Description

As its name implies, DNSRecon is a DNS reconnaissance tool that looks up NS records for a given domain or subdomain. It also searches DNS servers and relays’ cache for all types of DNS Records (MX, NS, A, AAAA, SPF, CNAME and more). For this tool, we will be using ‘gmo.com’ as well as some other domains discovered by the Sublist3r tool, to get an idea on the DNS records exposure for GMO.

b. Information Gathered

Substantial Information was gathered by the tool: most importantly, it appears that GMO does not sign its DNS Zone (DNSSec is not configured). Additionally, the MX records (mail exchange) reveal 11 different IPs that are subdomains of messagelabs.com, and the TXT records reveal information about services that GMO uses (such as Cisco Domain Verification, Agari, Webex Domain Verification and Docusign). Furthermore, the tool was able to resolve certain subdomains to IP addresses, such as: apps.gmo.com – 216.57.159.24 | directaccessmar.gmo.com – 69.147.188.85 | zix01.gmo.com – 216.57.159.38, and they are all pingable.

c. Negative Impact

Using the information found above, an attacker can better understand the layout of GMO's security infrastructure and he can tell what email security software and services are being used (Zix, Agari, Broadcom's messagelabs). Additionally, the attacker has the IP addresses of the servers running the applications which he can use to exploit vulnerabilities for each of the apps or just simply perform DoS attacks. Most importantly, an attacker can leverage DNS cache poisoning attacks among other DNS attacks, because GMO does not have DNSSec. Refer to Appendix 5 for more.

d. Suggested Controls

Implementing DNSSec would be a great start to prevent DNS cache poisoning or DNS spoofing attacks. Furthermore, attempt to remove all TXT records, because all they do is advertise machine types and services running and they result in you giving out unnecessary information. If not implemented already, split your DNS Zone into an External and Internal DNS Zone, so that apps and services that shouldn't have external access are not advertised on the internet, and limit DNS Zone transfers.

7. Spiderfoot

a. Tool Description

Spiderfoot is an OSINT (Open Source Intelligence) recon tool that automatically sends queries to more than 100 public data sources, such as HaveIBeenPwned, and several other search engines and services, to gather several different types of information such as IP addresses, subdomains and domain names, hacked emails, social media presence, DNS records, and much more.

b. Information Gathered

The most notable information that this tool discovered, and that was not discovered by previous tools, is Web Server info, Cloud Buckets (that indicate what cloud services GMO is using – AWS and Azure) and the domain WHOIS record (containing company details, such as address, contact information, email, and Contact Name, among other details). Web server info reveal the service running on several GMO servers with their IP. For instance, 'gmo.com' is running Nginx and it is hosted by Cloudfare, other web servers are running

Big-IP (F5 product that provides application delivery services, access control and other security services). Refer to Appendix 6 for additional information regarding WHOIS record)

c. Negative Impact

Again, the impact here is intelligence gathering and understanding GMO's infrastructure better, and what type of products, software and security controls it has deployed. An attacker can figure out that GMO is running Nginx and Big-IP, so any time there is a vulnerability related to either, the attacker will attempt to exploit it. Additionally, an attacker can predict that GMO is using other F5 products. Regarding the WHOIS record, the attacker can get the physical address of GMO, the phone number of a GMO contact, their email and their name.

d. Suggested Controls

There are no controls regarding the WHOIS record, as it should be as accurate as possible. Concerning the exposure of Operating Systems and services that are running on servers, these are available on Leakix, and were likely leaked on the internet through active reconnaissance but are now public knowledge. The only thing to do now is to make sure to install certain kernel modules on the exposed servers, that will scramble future active recon that seek to do OS fingerprinting.

8. Maltego

a. Tool Description

Maltego is more than just a tool, it is a OSINT framework, that specializes in gathering information on individuals (or companies) using publicly available information through search engines, social media services and more. I am mostly interested in its ability to find emails and scout specific individuals' social media presence.

b. Information Gathered

Maltego was able to give me 4 relevant email addresses: Michael_zeoli@gmo.com, jack_cunnif@gmo.com, martha_mixson@gmo.com, mike.theriault@gmo.com. The good news is that Maltego did not find any social media information other than LinkedIn profiles which were already mentioned earlier.

c. Negative Impact

Getting a valid employee email address can be very beneficial for attackers, especially if they are looking to use phishing emails as a malware delivery method. For instance, now that an attacker knows the format of emails for GMO, which is FirstName_LastName@gmo.com or FirstName.LastName@gmo.com, he can combine that knowledge with the names of employees that he can find on LinkedIn or by googling 'GMO board members' the name of C-level executives. This will allow an attacker to have the email address of VIPs and whichever target at the company, that has their name on the internet and that work for GMO.

d. Suggested Controls

One of the emails discovered was from the WHOIS record (mike.theriault@gmo.com), and I think that WHOIS should not include a @gmo.com email address, but another address that might forward to the contact's business email. Additionally, make sure you train and educate employees against phishing attacks.

IV. References

[1] E. Skoudis. *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses.* Second Edition. 2005.

[2] R. Beggs, V.K. Velu. *Mastering Kali Linux for Advanced Penetration Testing*. Third Edition. 2019

V. Appendix

Appendix 1 – Sublist3r

Subdomains
www.gmo.com
Artifactory.gmo.com
Artifactorystg.gmo.com
aaa.gmo.com
adfs.gmo.com
adfs2.gmo.com
airwatch.gmo.com
app-mobile.gmo.com
app-mobiledev.gmo.com
apps.gmo.com
apps2.gmo.com
as-mobile.gmo.com
as-mobiledev.gmo.com
autodiscover.gmo.com
bedexc034.gmo.com
bkp.gmo.com
blk-mobile.gmo.com
apps.gmo.com<BR>citrixcallback1.gmo.com<BR>citrixcallback2.gmo.com<BR>citrixcallback3.gmo.com<BR>citrixcallback4.gmo.com
gmoqliksenseinternal.gmo.com<BR>gmoqliksenseuatsaml.gmo.com
app-mobile.gmo.com<BR>as-mobile.gmo.com<BR>mobile.gmo.com
portal-dev.gmo.com<BR>portal.gmo.com<BR>portal-prd.gmo.com<BR>portal-qa.gmo.com<BR>portal-uat.gmo.com

portal.gmo.com<BR>portal-uat.gmo.com
apps.gmo.com<BR>secureapps.gmo.com
autodiscover.gmo.com<BR>mail.gmo.com<BR>smtp.gmo.com
autodiscover.gmo.com<BR>hybrid.gmo.com<BR>mail.gmo.com<BR>oos.gmo.com<BR>smtp.gmo.com
app-mobile.gmo.com<BR>as-mobile.gmo.com<BR>mobile.gmo.com<BR>syd-app-mobile.gmo.com<BR>syd-as-mobile.gmo.com
sydmail2.gmo.com<BR>sydmail.gmo.com
gmo.com<BR>vcsedge.gmo.com
bedvcsedge.gmo.com<BR>sngvcsedge.gmo.com<BR>vcsedge.gmo.com
sngvcsedge.gmo.com<BR>vcsedge.gmo.com
mail.gmo.com<BR>webmail.gmo.com
app-mobiledev.gmo.com<BR>as-mobiledev.gmo.com<BR>mobiledev.gmo.com<BR>win-mobiledev.gmo.com
dc.gmo.com<BR>dev.gmo.com<BR>gmo.com<BR>prd.gmo.com<BR>qa.gmo.com<BR>uat.gmo.com<BR>www.gmo.com
dev.gmo.com<BR>prd.gmo.com<BR>qa.gmo.com<BR>uat.gmo.com<BR>www.gmo.com
connect.gmo.com
dc.gmo.com
www.dc.gmo.com
dev.gmo.com
directaccessbed.gmo.com
directaccessbedtst.gmo.com
directaccessbedv2.gmo.com
directaccessmar.gmo.com
directaccessmartst.gmo.com
directaccessmarv2.gmo.com
directaccessnrd.gmo.com
directaccessnrdtst.gmo.com
directaccesssng.gmo.com
directaccesssyd.gmo.com
docs.gmo.com
email.gmo.com
ep.gmo.com
events.gmo.com
ftp.gmo.com
ftps.gmo.com
ftps-dev.gmo.com
fw.gmo.com
gmojpm.gmo.com
gmoqliksenseinternal.gmo.com

gmoqliksenseuatsaml.gmo.com
hybrid.gmo.com
itapps.gmo.com
london.gmo.com
mail.gmo.com
maintenance.gmo.com
mgway.gmo.com
mgway1.gmo.com
mgway3.gmo.com
mgway4.gmo.com
mobile.gmo.com
mobiledev.gmo.com
mysecuremail.gmo.com
ns1.gmo.com
ns2.gmo.com
portal.gmo.com
portal-uat.gmo.com
prd.gmo.com
o114.ptr926.gmo.com
qa.gmo.com
remote.gmo.com
sdc.gmo.com
secureapps.gmo.com
secureapps2.gmo.com
singapore.gmo.com
smtp.gmo.com
sngapps.gmo.com
sydapps.gmo.com
sydexc002.gmo.com
sydmail.gmo.com
sydmail2.gmo.com
sydney.gmo.com
sydneydr.gmo.com
ftps.test.gmo.com
uat.gmo.com
us.gmo.com
vcsedge.gmo.com
video.gmo.com
view.gmo.com
wberguest.gmo.com

webmail.gmo.com
wguest.gmo.com
win-mobiledev.gmo.com
zix01.gmo.com
zix02.gmo.com

Appendix 2 – theHarvester

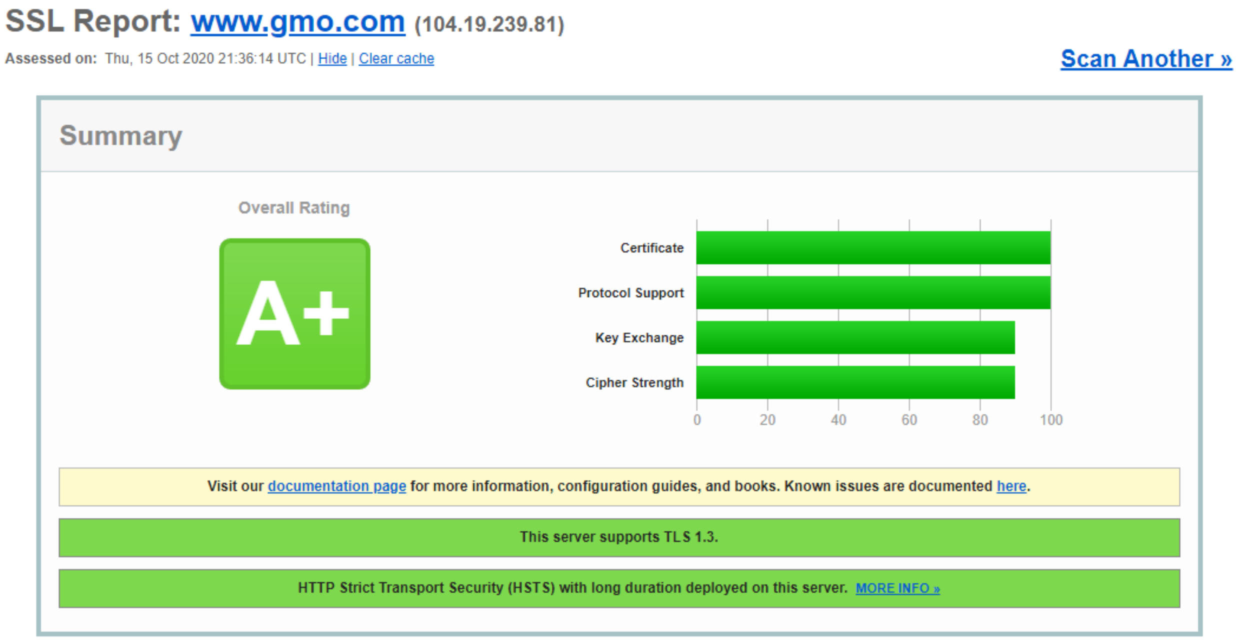
LinkedIn URLs
https://www.linkedin.com/in/acabral3
https://www.linkedin.com/in/adammachanic
https://www.linkedin.com/in/alexandrawatkins
https://www.linkedin.com/in/alexhebert1
https://www.linkedin.com/in/allison-davis-718bb287
https://www.linkedin.com/in/alongirmonsky
https://www.linkedin.com/in/amar-reganti-897421
https://www.linkedin.com/in/anna-chetoukhina-cfa-8031013
https://www.linkedin.com/in/anshuljain2
https://www.linkedin.com/in/anton-honikman-213470
https://www.linkedin.com/in/antoniograceffo
https://www.linkedin.com/in/aprilvharris
https://www.linkedin.com/in/arcady
https://www.linkedin.com/in/barbarabickham
https://www.linkedin.com/in/bayao
https://www.linkedin.com/in/bobangell
https://www.linkedin.com/in/brian-smith-5444948
https://www.linkedin.com/in/carl-ross-33354348
https://www.linkedin.com/in/catharinearnston
https://www.linkedin.com/in/chad-sarno-4a890a51
https://www.linkedin.com/in/charlesandersen
https://www.linkedin.com/in/ckaiwu
https://www.linkedin.com/in/court-west-53079514
https://www.linkedin.com/in/dan-mahoney-0257135
https://www.linkedin.com/in/danielzakowski
https://www.linkedin.com/in/edodson
https://www.linkedin.com/in/elizabeth-pinone-8357712a
https://www.linkedin.com/in/eric-schnell-b133a425
https://www.linkedin.com/in/fasol/

https://www.linkedin.com/in/fenglinzhu1991
https://www.linkedin.com/in/filipp-chebotarev-385a472a
https://www.linkedin.com/in/gayleoconnor
https://www.linkedin.com/in/georgiossakoulis
https://www.linkedin.com/in/greg-pottle-42757a5
https://www.linkedin.com/in/harpreet-dang-cfa-39b8411
https://www.linkedin.com/in/heather-schirmer-mahoney-jd
https://www.linkedin.com/in/hudsongr
https://www.linkedin.com/in/itsmeadamyee
https://www.linkedin.com/in/jack-cunniff-524a57165
https://www.linkedin.com/in/jack-roddy-4477026
https://www.linkedin.com/in/jamshed-khan-a62a568
https://www.linkedin.com/in/janiceperson
https://www.linkedin.com/in/jaynacantor
https://www.linkedin.com/in/jeremy-roll-655107
https://www.linkedin.com/in/jimis
https://www.linkedin.com/in/johnroulac
https://www.linkedin.com/in/jonodo
https://www.linkedin.com/in/jorge-heraud-704b945
https://www.linkedin.com/in/joseph-stanley-44325a16
https://www.linkedin.com/in/jthorndike
https://www.linkedin.com/in/karen-suber-96427612
https://www.linkedin.com/in/karimtoubba
https://www.linkedin.com/in/karl-kratzke-ab9bb516
https://www.linkedin.com/in/keith-r-mccullough-426a195
https://www.linkedin.com/in/kelleejames
https://www.linkedin.com/in/ken-nakamura
https://www.linkedin.com/in/kevin-berry-b81b1a3b
https://www.linkedin.com/in/kevin-folta-8856502b
https://www.linkedin.com/in/larrykaufmanlinkedinspeaker
https://www.linkedin.com/in/lisa-galassi-7a70773a
https://www.linkedin.com/in/loren-brill-56887121
https://www.linkedin.com/in/madeline-haydon-b721474
https://www.linkedin.com/in/maevewebster
https://www.linkedin.com/in/mattmckibbin
https://www.linkedin.com/in/maxkuzkin
https://www.linkedin.com/in/meganethompson
https://www.linkedin.com/in/melanie-rudoy-ph-d-805ba44
https://www.linkedin.com/in/michael-ellis-14aa785

https://www.linkedin.com/in/michael-herald-672b5b21
https://www.linkedin.com/in/michael-w-oleary
https://www.linkedin.com/in/mike-mccormack-1ba23a7
https://www.linkedin.com/in/nadjapiatka
https://www.linkedin.com/in/nateguggia
https://www.linkedin.com/in/nickrunyon
https://www.linkedin.com/in/nicole-atchison-ph-d-74244318
https://www.linkedin.com/in/nicole-zimmerman-8ab6aa3
https://www.linkedin.com/in/nitzberg
https://www.linkedin.com/in/organiccookingcoach
https://www.linkedin.com/in/perezaj
https://www.linkedin.com/in/roy-dinicola-72224a11
https://www.linkedin.com/in/ryan-dawley-490112a
https://www.linkedin.com/in/sachin-todur-09061114
https://www.linkedin.com/in/scott-hayward-239253a
https://www.linkedin.com/in/senagalazzi/%3Fppe%3D1
https://www.linkedin.com/in/shon-r-hiatt-a874327
https://www.linkedin.com/in/sinisaradovcic
https://www.linkedin.com/in/ssimms2
https://www.linkedin.com/in/stacie-orell-66934761
https://www.linkedin.com/in/tamibhaumik
https://www.linkedin.com/in/ty-cobb-432b2114
https://www.linkedin.com/in/unnabakery

Appendix 3 – Qualys SSL Server Test

Network Security Practices
CY 5150 – Fall 2020
Alexander Semaan



SSL Report: www.gmo.com (104.19.239.81)

Assessed on: Thu, 15 Oct 2020 21:36:14 UTC | Hide | Clear cache

Scan Another »

Summary

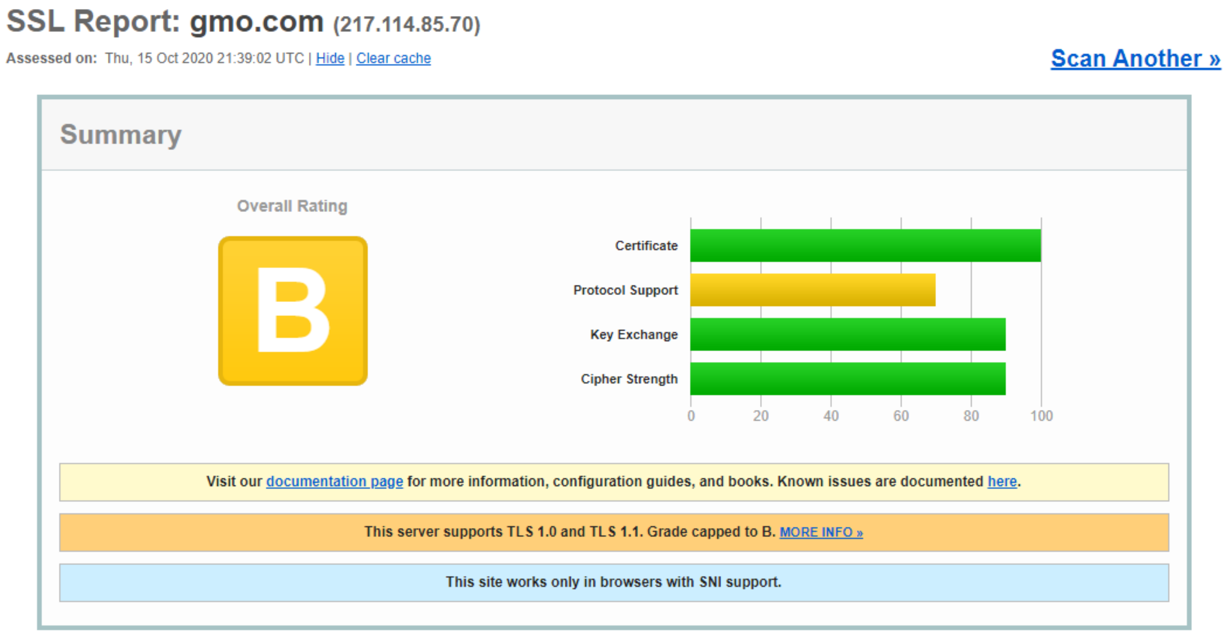
Overall Rating

A+

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »



SSL Report: gmo.com (217.114.85.70)

Assessed on: Thu, 15 Oct 2020 21:39:02 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

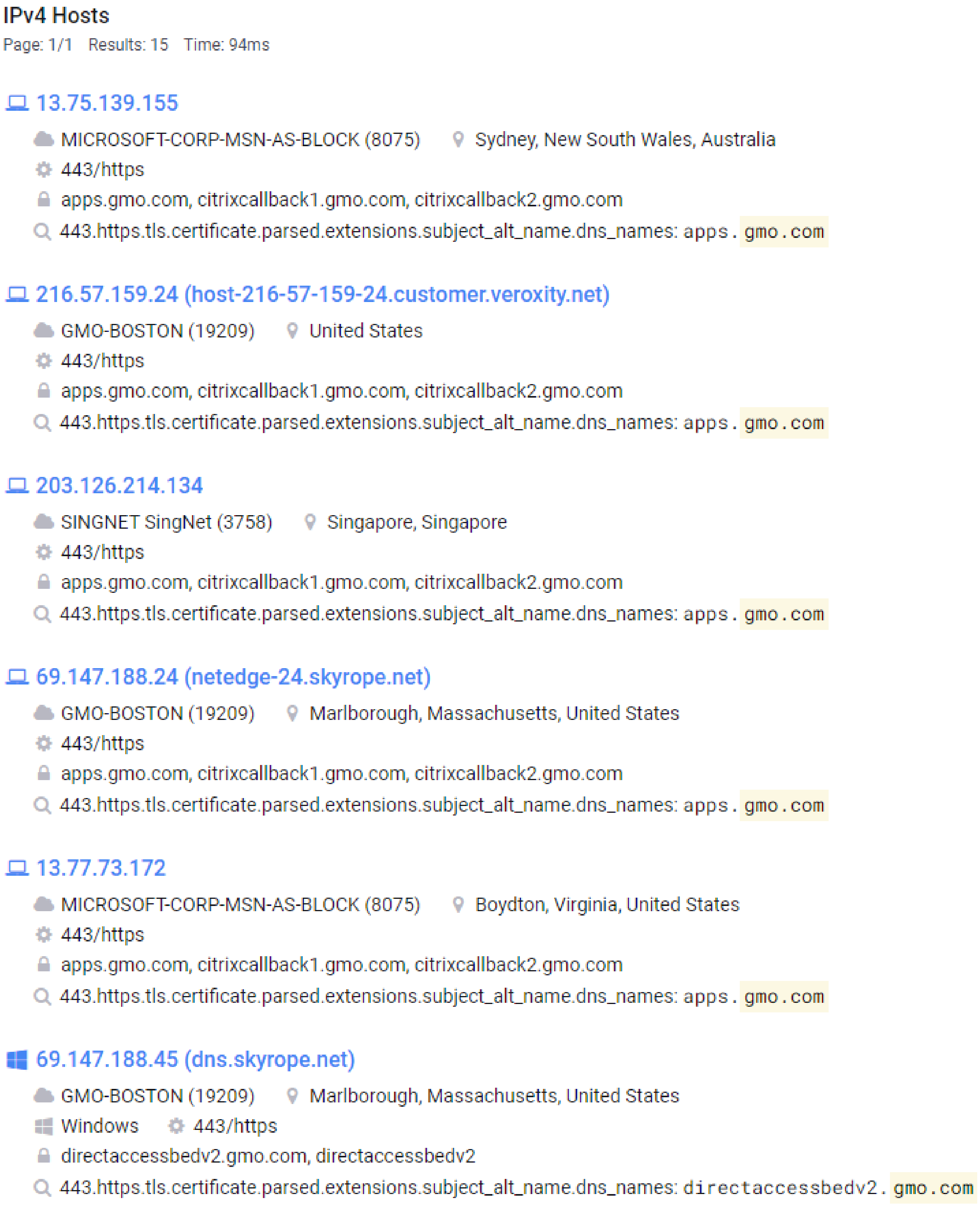
B

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This site works only in browsers with SNI support.

Appendix 4 – Censys



IPv4 Hosts

Page: 1/1   Results: 15   Time: 94ms

13.75.139.155
MICROSOFT-CORP-MSN-AS-BLOCK (8075)   Sydney, New South Wales, Australia
443/https
apps.gmo.com, citrixcallback1.gmo.com, citrixcallback2.gmo.com
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: apps.gmo.com

216.57.159.24 (host-216-57-159-24.customer.veroxity.net)
GMO-BOSTON (19209)   United States
443/https
apps.gmo.com, citrixcallback1.gmo.com, citrixcallback2.gmo.com
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: apps.gmo.com

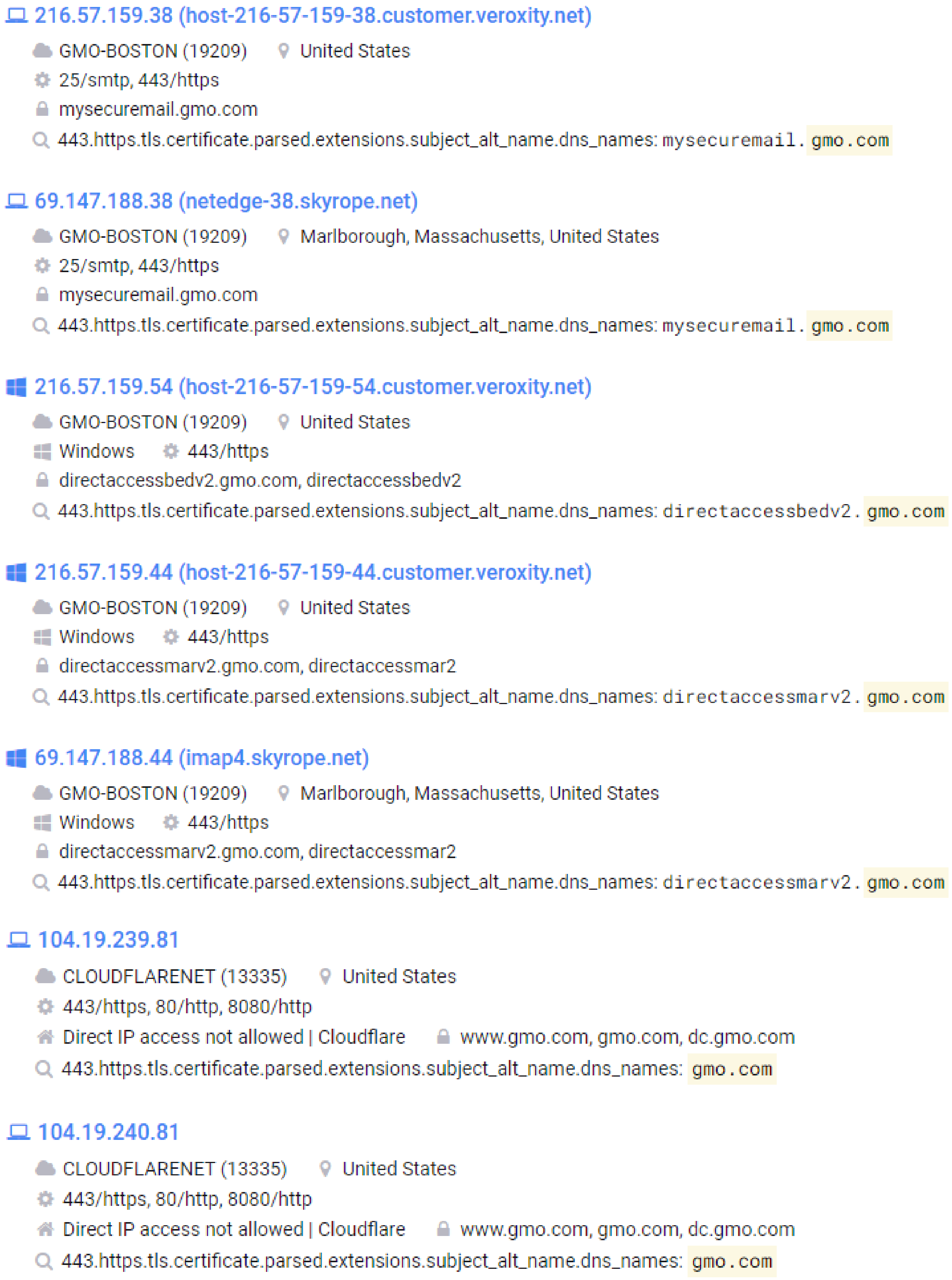
203.126.214.134
SINGNET SingNet (3758)   Singapore, Singapore
443/https
apps.gmo.com, citrixcallback1.gmo.com, citrixcallback2.gmo.com
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: apps.gmo.com

69.147.188.24 (netedge-24.skyrope.net)
GMO-BOSTON (19209)   Marlborough, Massachusetts, United States
443/https
apps.gmo.com, citrixcallback1.gmo.com, citrixcallback2.gmo.com
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: apps.gmo.com

13.77.73.172
MICROSOFT-CORP-MSN-AS-BLOCK (8075)   Boydton, Virginia, United States
443/https
apps.gmo.com, citrixcallback1.gmo.com, citrixcallback2.gmo.com
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: apps.gmo.com

69.147.188.45 (dns.skyrope.net)
GMO-BOSTON (19209)   Marlborough, Massachusetts, United States
Windows   443/https
directaccessbedv2.gmo.com, directaccessbedv2
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: directaccessbedv2.gmo.com

Network Security Practices
CY 5150 – Fall 2020
Alexander Semaan



216.57.159.38 (host-216-57-159-38.customer.veroxity.net)

GMO-BOSTON (19209) United States
25/smtp, 443/https
mysecuremail.gmo.com
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: mysecuremail.gmo.com

69.147.188.38 (netedge-38.skyrope.net)

GMO-BOSTON (19209) Marlborough, Massachusetts, United States
25/smtp, 443/https
mysecuremail.gmo.com
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: mysecuremail.gmo.com

216.57.159.54 (host-216-57-159-54.customer.veroxity.net)

GMO-BOSTON (19209) United States
Windows 443/https
directaccessbedv2.gmo.com, directaccessbedv2
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: directaccessbedv2.gmo.com

216.57.159.44 (host-216-57-159-44.customer.veroxity.net)

GMO-BOSTON (19209) United States
Windows 443/https
directaccessmarv2.gmo.com, directaccessmar2
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: directaccessmarv2.gmo.com

69.147.188.44 (imap4.skyrope.net)

GMO-BOSTON (19209) Marlborough, Massachusetts, United States
Windows 443/https
directaccessmarv2.gmo.com, directaccessmar2
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: directaccessmarv2.gmo.com

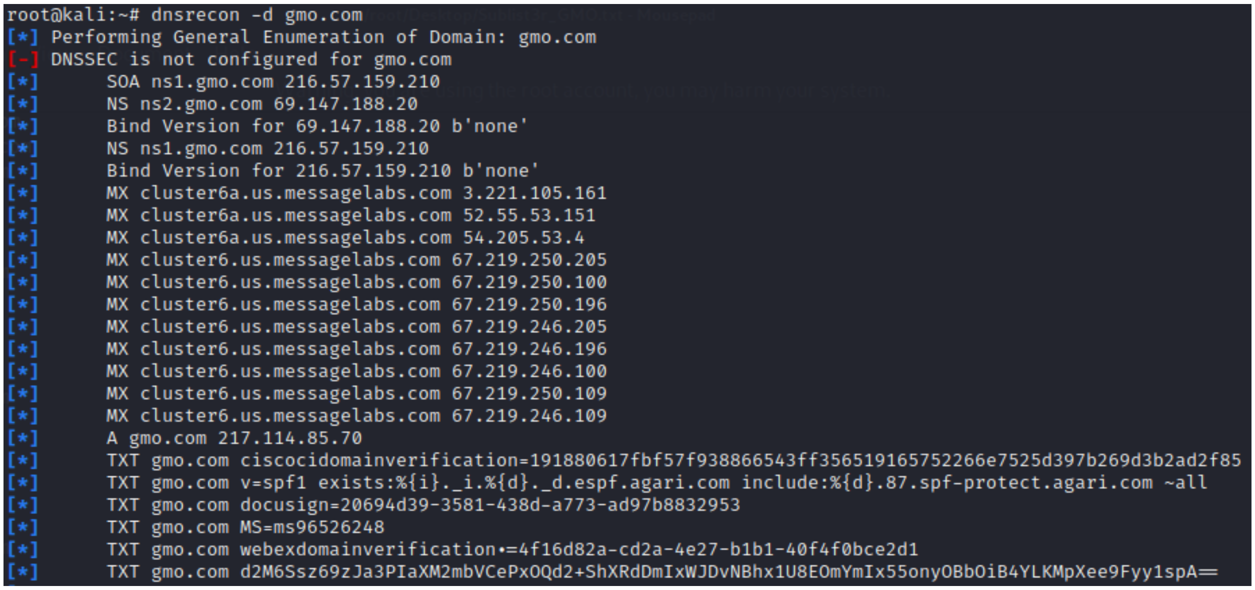
104.19.239.81

CLOUDFLARENET (13335) United States
443/https, 80/http, 8080/http
Direct IP access not allowed | Cloudflare www.gmo.com, gmo.com, dc.gmo.com
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: gmo.com

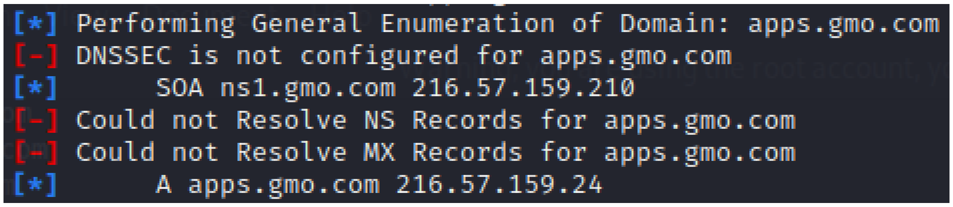
104.19.240.81

CLOUDFLARENET (13335) United States
443/https, 80/http, 8080/http
Direct IP access not allowed | Cloudflare www.gmo.com, gmo.com, dc.gmo.com
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: gmo.com

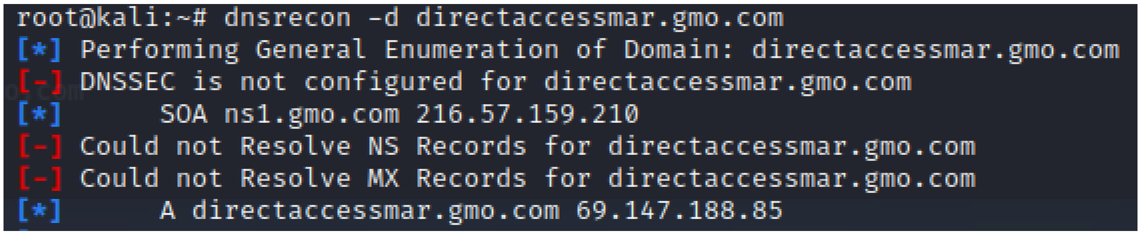
Appendix 5 – DNSRecon



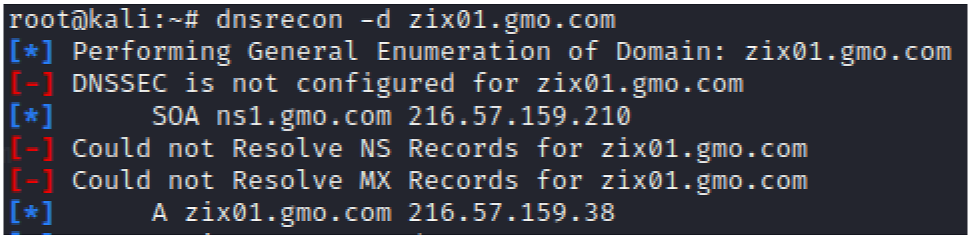
```
root@kali:~# dnsrecon -d gmo.com
[*] Performing General Enumeration of Domain: gmo.com
[-] DNSSEC is not configured for gmo.com
[*]      SOA ns1.gmo.com 216.57.159.210
[*]      NS ns2.gmo.com 69.147.188.20
[*]      Bind Version for 69.147.188.20 b'none'
[*]      NS ns1.gmo.com 216.57.159.210
[*]      Bind Version for 216.57.159.210 b'none'
[*]      MX cluster6a.us.messagelabs.com 3.221.105.161
[*]      MX cluster6a.us.messagelabs.com 52.55.53.151
[*]      MX cluster6a.us.messagelabs.com 54.205.53.4
[*]      MX cluster6.us.messagelabs.com 67.219.250.205
[*]      MX cluster6.us.messagelabs.com 67.219.250.100
[*]      MX cluster6.us.messagelabs.com 67.219.250.196
[*]      MX cluster6.us.messagelabs.com 67.219.246.205
[*]      MX cluster6.us.messagelabs.com 67.219.246.196
[*]      MX cluster6.us.messagelabs.com 67.219.246.100
[*]      MX cluster6.us.messagelabs.com 67.219.250.109
[*]      MX cluster6.us.messagelabs.com 67.219.246.109
[*]      A gmo.com 217.114.85.70
[*]      TXT gmo.com ciscocidomainverification=191880617fbf57f938866543ff356519165752266e7525d397b269d3b2ad2f85
[*]      TXT gmo.com v=spf1 exists:%{i}._i.%{d}._d.espf.agari.com include:%{d}.87.spf-protect.agari.com ~all
[*]      TXT gmo.com docusign=20694d39-3581-438d-a773-ad97b8832953
[*]      TXT gmo.com MS=ms96526248
[*]      TXT gmo.com webexdomainverification•=4f16d82a-cd2a-4e27-b1b1-40f4f0bce2d1
[*]      TXT gmo.com d2M6Ssz69zJa3PIaXM2mbVCePxOQd2+ShXRdDmIxWJDvNBhx1U8EOmYmIx55onyOBbOiB4YLKMpXee9Fyy1spA==
```



```
[*] Performing General Enumeration of Domain: apps.gmo.com
[-] DNSSEC is not configured for apps.gmo.com
[*]      SOA ns1.gmo.com 216.57.159.210
[-] Could not Resolve NS Records for apps.gmo.com
[-] Could not Resolve MX Records for apps.gmo.com
[*]      A apps.gmo.com 216.57.159.24
```

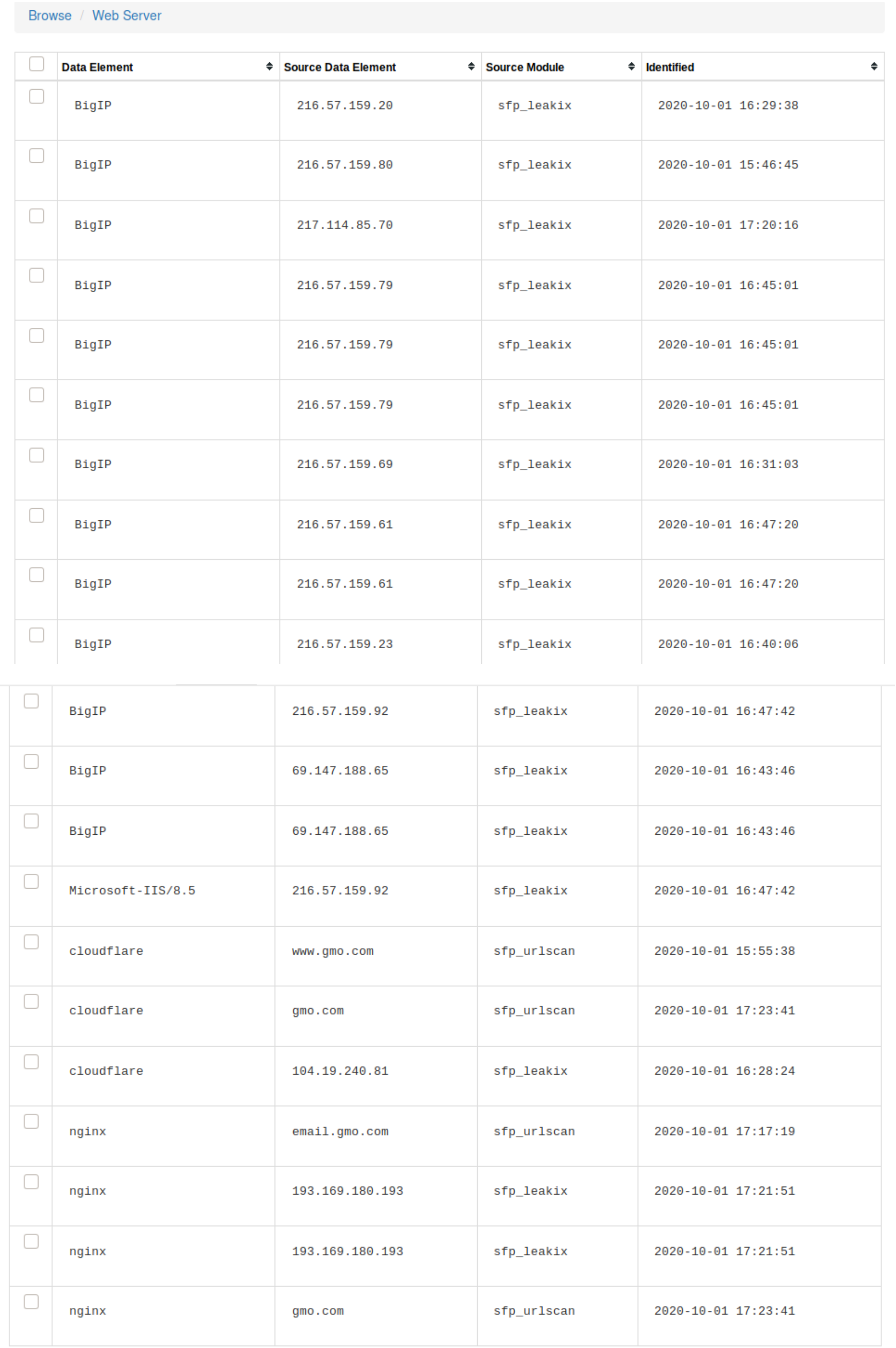


```
root@kali:~# dnsrecon -d directaccessmar.gmo.com
[*] Performing General Enumeration of Domain: directaccessmar.gmo.com
[-] DNSSEC is not configured for directaccessmar.gmo.com
[*]      SOA ns1.gmo.com 216.57.159.210
[-] Could not Resolve NS Records for directaccessmar.gmo.com
[-] Could not Resolve MX Records for directaccessmar.gmo.com
[*]      A directaccessmar.gmo.com 69.147.188.85
```



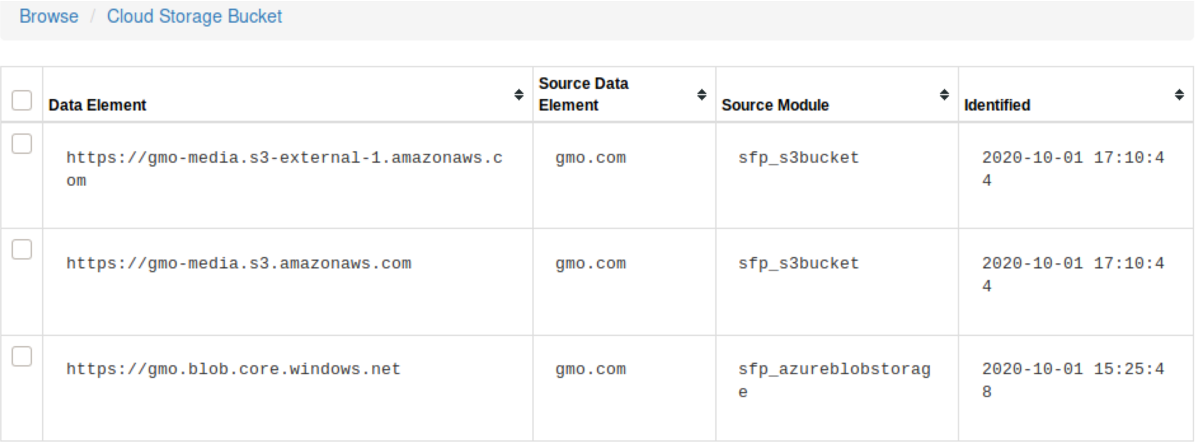
```
root@kali:~# dnsrecon -d zix01.gmo.com
[*] Performing General Enumeration of Domain: zix01.gmo.com
[-] DNSSEC is not configured for zix01.gmo.com
[*]      SOA ns1.gmo.com 216.57.159.210
[-] Could not Resolve NS Records for zix01.gmo.com
[-] Could not Resolve MX Records for zix01.gmo.com
[*]      A zix01.gmo.com 216.57.159.38
```

Appendix 6 – Spiderfoot



Browse / Web Server

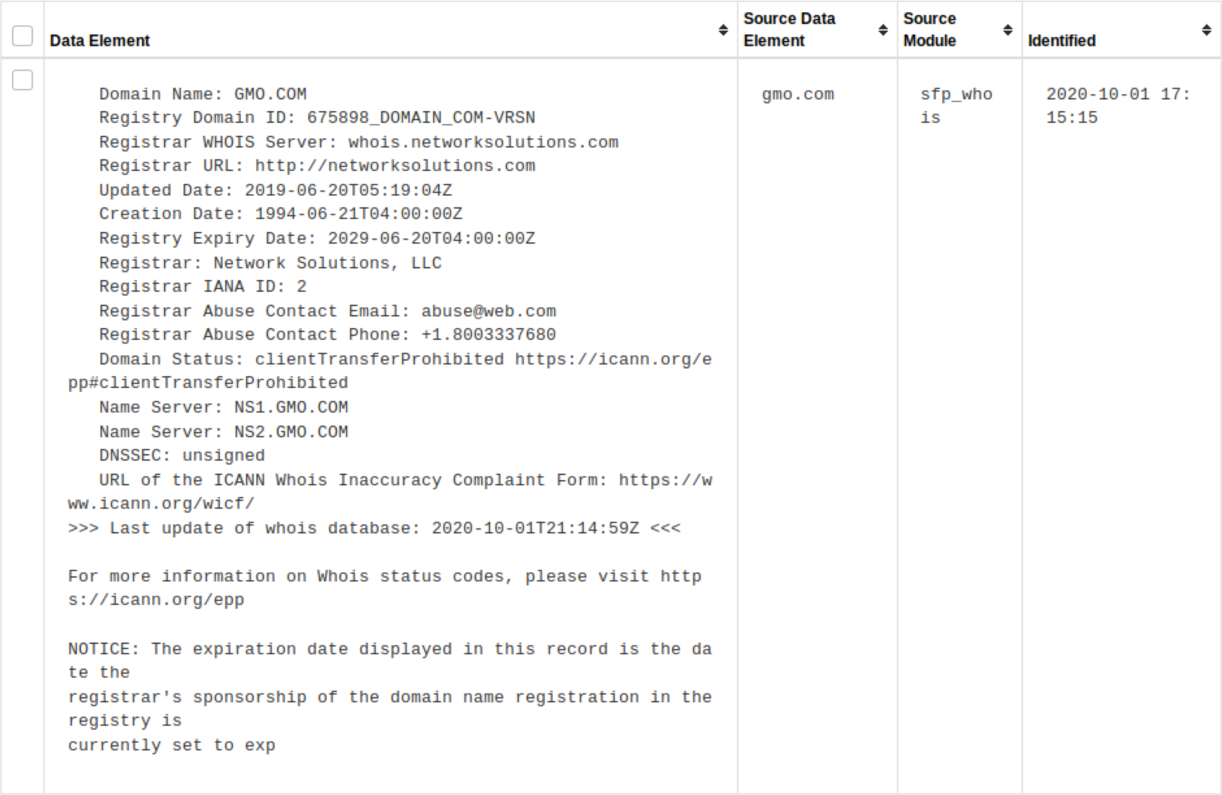
□	Data Element	Source Data Element	Source Module	Identified
□	BigIP	216.57.159.20	sfp_leakix	2020-10-01 16:29:38
□	BigIP	216.57.159.80	sfp_leakix	2020-10-01 15:46:45
□	BigIP	217.114.85.70	sfp_leakix	2020-10-01 17:20:16
□	BigIP	216.57.159.79	sfp_leakix	2020-10-01 16:45:01
□	BigIP	216.57.159.79	sfp_leakix	2020-10-01 16:45:01
□	BigIP	216.57.159.79	sfp_leakix	2020-10-01 16:45:01
□	BigIP	216.57.159.69	sfp_leakix	2020-10-01 16:31:03
□	BigIP	216.57.159.61	sfp_leakix	2020-10-01 16:47:20
□	BigIP	216.57.159.61	sfp_leakix	2020-10-01 16:47:20
□	BigIP	216.57.159.23	sfp_leakix	2020-10-01 16:40:06
□	BigIP	216.57.159.92	sfp_leakix	2020-10-01 16:47:42
□	BigIP	69.147.188.65	sfp_leakix	2020-10-01 16:43:46
□	BigIP	69.147.188.65	sfp_leakix	2020-10-01 16:43:46
□	Microsoft-IIS/8.5	216.57.159.92	sfp_leakix	2020-10-01 16:47:42
□	cloudflare	www.gmo.com	sfp_urlscan	2020-10-01 15:55:38
□	cloudflare	gmo.com	sfp_urlscan	2020-10-01 17:23:41
□	cloudflare	104.19.240.81	sfp_leakix	2020-10-01 16:28:24
□	nginx	email.gmo.com	sfp_urlscan	2020-10-01 17:17:19
□	nginx	193.169.180.193	sfp_leakix	2020-10-01 17:21:51
□	nginx	193.169.180.193	sfp_leakix	2020-10-01 17:21:51
□	nginx	gmo.com	sfp_urlscan	2020-10-01 17:23:41



Browse / Cloud Storage Bucket

□	Data Element	Source Data Element	Source Module	Identified
□	https://gmo-media.s3-external-1.amazonaws.com	gmo.com	sfp_s3bucket	2020-10-01 17:10:44
□	https://gmo-media.s3.amazonaws.com	gmo.com	sfp_s3bucket	2020-10-01 17:10:44
□	https://gmo.blob.core.windows.net	gmo.com	sfp_azureblobstorage	2020-10-01 15:25:48

WHOIS:



□	Data Element	Source Data Element	Source Module	Identified
□	Domain Name: GMO.COM Registry Domain ID: 675898_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.networksolutions.com Registrar URL: http://networksolutions.com Updated Date: 2019-06-20T05:19:04Z Creation Date: 1994-06-21T04:00:00Z Registry Expiry Date: 2029-06-20T04:00:00Z 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: NS1.GMO.COM Name Server: NS2.GMO.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2020-10-01T21:14:59Z <<< 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 exp	gmo.com	sfp_whois	2020-10-01 17:15:15