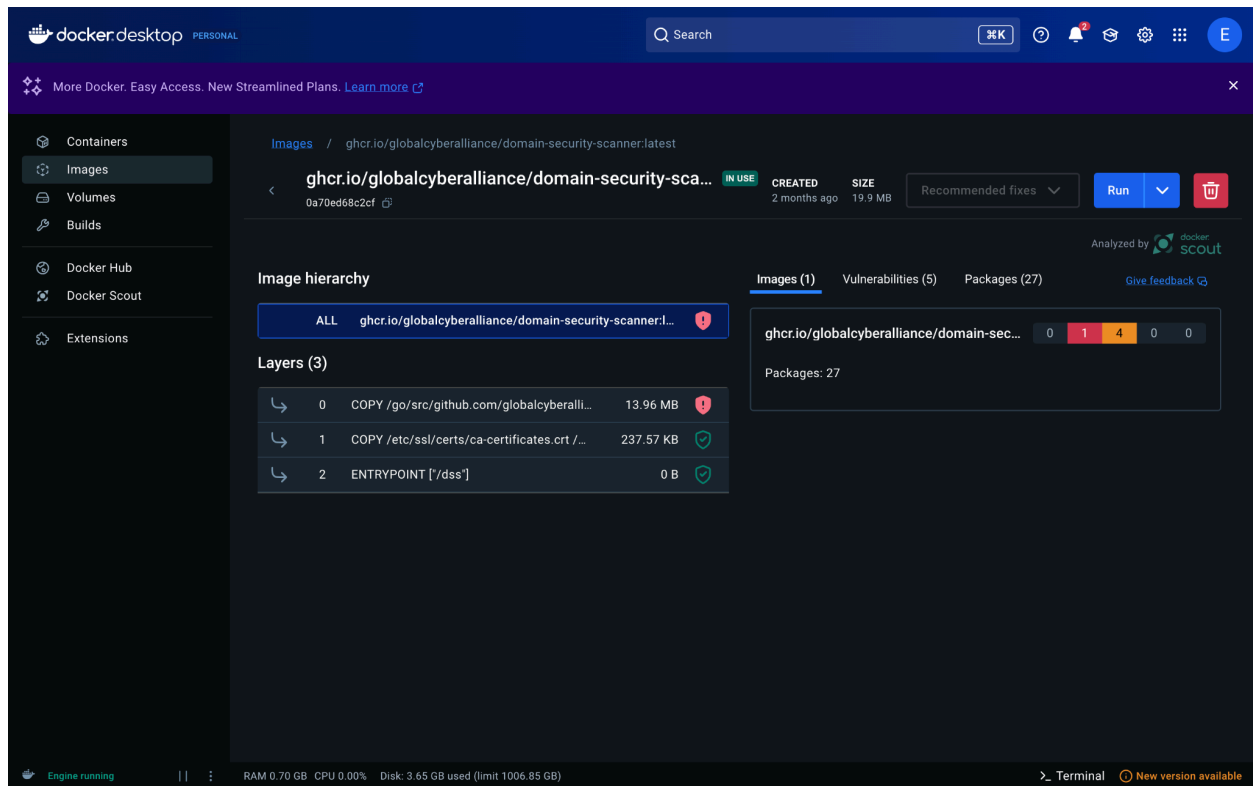


## Domain-Security-Scanner: ([GitHub Page](#))

This open-source program by *Global Cyber Alliance* can be used to perform scans against domains for DKIM, DMARC, and SPF DNS records. Making it an ideal comparison for Spoofy.

Something about this program is very bizarre. I don't really understand why it refuses to work. This program is intended for Docker. I have gotten this Docker running, however, you can see that this program refuses to work inside of Docker. I will launch it and it immediately closes, additionally I don't have Docker premium. Setting it up on a macOS machine with Go is also impossible because the program can't access Python script. Maybe a bug? Whatever.

You can see here an analysis of the vulnerabilities in this program; none of them are very significant with the exception of [CVE-2025 22869](#) for DDoS attacks. This is not very important, just a note about the status of the program, there is no fix for this CVE.



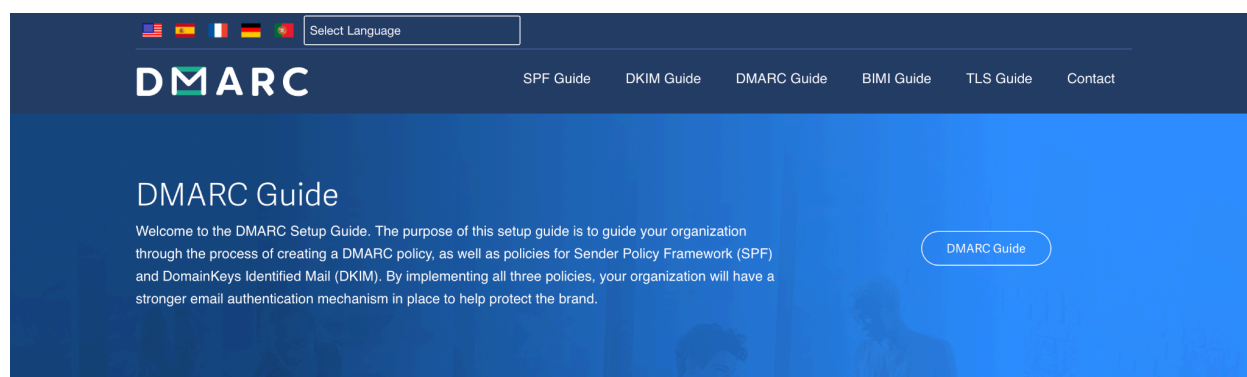
```

2025-03-18 23:10:14 Scan a domain's DNS records.
2025-03-18 23:10:14 https://github.com/globalcyberalliance/domain-security-scanner
2025-03-18 23:10:14
2025-03-18 23:10:14 Usage:
2025-03-18 23:10:14   dss [command]
2025-03-18 23:10:14
2025-03-18 23:10:14 Available Commands:
2025-03-18 23:10:14   completion  Generate the autocompletion script for the specified shell
2025-03-18 23:10:14   config       Configure your DSS instance
2025-03-18 23:10:14   help        Help about any command
2025-03-18 23:10:14   scan        Scan DNS records for one or multiple domains.
2025-03-18 23:10:14   serve       Serve the scanner via a REST API or dedicated mailbox
2025-03-18 23:10:14
2025-03-18 23:10:14 Flags:
2025-03-18 23:10:14   -a, --advise          Provide suggestions for incorrect/missing mail security features
2025-03-18 23:10:14   --cache duration      Specify how long to cache results for (default 3m0s)
2025-03-18 23:10:14   --checkTLS            Check the TLS connectivity and cert validity of domains
2025-03-18 23:10:14   -c, --concurrent uint16 The number of domains to scan concurrently (default 8)
2025-03-18 23:10:14   -d, --debug           Print debug logs
2025-03-18 23:10:14   --dkimSelector strings Specify a DKIM selector
2025-03-18 23:10:14   --dnsBuffer uint16    Specify the allocated buffer for DNS responses (default 4096)
2025-03-18 23:10:14   --dnsProtocol string  Protocol to use for DNS queries (udp, tcp, tcp-tls) (default "udp")
2025-03-18 23:10:14   -f, --format string   Format to print results in (yaml, json) (default "yaml")
2025-03-18 23:10:14   -h, --help            help for dss
2025-03-18 23:10:14   -n, --nameservers host[:port] Use specific nameservers, in host[:port] format; may be specified multiple times
2025-03-18 23:10:14   -o, --outputFile string Output the results to a specified file (creates a file with the current unix timestamp if n
o file is specified)
2025-03-18 23:10:14   --prettyLog           Pretty print logs to console (default true)
2025-03-18 23:10:14   -t, --timeout duration Timeout duration for queries (default 15s)
2025-03-18 23:10:14   -v, --version         version for dss
2025-03-18 23:10:14   -z, --zoneFile        Input file/pipe containing an RFC 1035 zone file

```

You can see the intended tool usage here. A user can use the ‘dss’ command to check any domain similarly to Spoofy. You can see that Domain-Security-Scanner has some additional functionality in the form of the ‘-a’ and ‘--checkTLS’ functions. Spoofy has no ability to advise potential fixes; it only gives basic information about the DKIM, DMARC, and SPF DNS records. Additionally, Spoofy has no TLS analysis functions which would be a significant boon for the platform. Potentially, something we can consider adding to Spoofy in the future. Unfortunately, I can’t run any tests based on the status of the program in Docker.

Thankfully this program can be run in a browser. Mind you with significantly less features than its Docker counterpart. We will run our comparison test through this platform ([Webpage for Domain-Security-Scanner](#)).



Enter your domain

The first step is confirming whether not your organization is using any of the three policies.

Please input the domain from your organization's email address, exactly as it appears after the @ symbol in the email address.

[Bulk Scan](#)

For example, the following email address, `domainsecurityscanner@globalcyberalliance.org`.

You can see the webpage here. It's fairly straightforward, the top of the page has some links to pages that explain SPF, DKIM, DMARC, BIMI, and TLS accordingly. You also have the options for a simple scan and a bulk scan (for checking multiple domains). The results for my tests on the webpage can be seen below. I did a very simple test on the TAMUSA domains.

Overall, I think this tool is useful but its implementation is bad unfortunately. It's good inspiration but it's awful to use. This website has terrible ping and some errors when loading webpages. Maybe I would have liked this tool more if it worked in Docker.

TAMUSA.EDU:

✓

SPF

SPF seems to be setup correctly! No further action needed.

SPF Guide

✓

DMARC

You are currently at the lowest level and receiving reports, which is a great starting point. Please make sure to review the reports.

DMARC Guide

✓

DKIM

DKIM is setup for this email server. However, if you have other 3rd party systems, please send a test email to confirm DKIM is setup

DKIM Guide

✗

BIMI

We couldn't detect any active BIMI record for your domain. Please visit <https://dmarcguide.globalcyberalliance.org> to fix this.

BIMI Guide

✓

TLS

Your domain is using TLS 1.3, no further action needed!  
You have a single mail server setup, but it's recommended

TLS Guide

Advanced ▼

SPF Record

v=spf1 include:spf.protection.outlook.com include:\_tuf-spf.touchnet.com include:illiad.oclc.org include:outboundmail.blackbaud.net -all

DMARC Record

v=DMARC1;p=none;rua=mailto:dmarc-monitor@tamusa.edu,mailto:dmarc\_agg@vall.email

DKIM Record

v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC79iPvavR1MznIsIa6OIVk5SfHCVhxLLDwaS43NRjthA023x6QQdc

MX Records

tamusa-edu.mail.protection.outlook.com.

NS Records

ns1.tamusa.edu.  
ns2.tamusa.edu.

JAGUAR.TAMU.EDU:

✓

SPF

SPF seems to be setup correctly! No further action needed.

SPF Guide

✗

DMARC

You do not have DMARC setup!

DMARC Guide

✓

DKIM

server. However, if you have other 3rd party systems, please send a test email to confirm DKIM is setup properly.

DKIM Guide

✗

BIMI

We couldn't detect any active BIMI record for your domain. Please visit <https://dmarcguide.globalcyberalliance.org> to fix this.

BIMI Guide

✓

TLS

You have a single mail server setup, but it's recommended that you have at least two setup in case the first one fails.

TLS Guide

Advanced ▼

SPF Record

v=spf1 include:spf.protection.outlook.com include:sendgrid.net -all

DKIM Record

v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC32znxCXGewJwYB9TDhkkWXFdnftOGFNh8pYqI75pAzXShf9haj

MX Records

jaguar-tamu-edu.mail.protection.outlook.com.

NS Records

ns2.tamusa.tamus.edu.  
ns2.tamusa.edu.  
ns1.tamusa.tamus.edu.  
ns1.tamusa.edu.

Start Over

Share

## MXToolBox Network Tools ([Website](#)):

MXToolBox is an online diagnostic tool used for email and network troubleshooting. It has a suite of utilities including Email and DNS troubleshooting, network diagnostics, performance and security analysis. These use cases make it an ideal comparison for Spoofy. Specifically for its capability to check SPF, DKIM, and DMARC records for email security settings. These settings, as established, allow us to determine the spoofability of a domain. Additionally the MX check and Blacklist Check functions can give us a better idea of how the domain functions. Specifically, what IPs the chosen domain is blacklisting. For the majority of blocked domains you'll notice they present critical vulnerabilities that need to be avoided.

**MX TOOLBOX®**  
SUPERTOOL

SuperTool Beta9

Lookup anything... Mx Lookup

### ABOUT THE SUPERTOOL!

All of your MX record, DNS, blacklist and SMTP diagnostics in one integrated tool. Input a **domain name** or **IP Address** or **Host Name**. Links in the results will guide you to other relevant tools and information. And you'll have a chronological history of your results.

If you already know exactly what you want, you can force a particular test or lookup. Try some of these examples:

(e.g. "blacklist: 127.0.0.2" will do a blacklist lookup)

Command	Explanation
blacklist:	Check IP or host for reputation
smtp:	Test mail server SMTP (port 25)
mx:	DNS MX records for domain
a:	DNS A record IP address for host name
spf:	Check SPF records on a domain
txt:	Check TXT records on a domain
ptr:	DNS PTR record for host name
cname:	DNS canonical host name to IP address
whois:	Get domain registration information
arin:	Get IP address block information
soa:	Get Start of Authority record for a domain
tcp:	Verify an IP Address allows tcp connections
http:	Verify a URL allows http connections
https:	Verify a URL allows secure http connections
ping:	Perform a standard ICMP ping
trace:	Perform a standard ICMP trace route
dns:	Check your DNS Servers for possible problems <b>New!</b>

Other tools

**Feedback:** If you run into any problems with the site or have an idea that you think would make it better, we would appreciate your feedback. Please leave us some [Feedback](#).

Your IP is: 98.46.160.13 | [Contact](#) [Terms & Conditions](#) [Site Map](#) [Security API](#) [Privacy](#) [Phone: \(866\)-698-6652](#) | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 1083553 B2 & 11461738 B2

For our example we're going to do an analysis on the TAMUSA domains, similarly to the previous tool. This should give us a good point of reference for our discussion of MXToolBox. What's especially curious in comparison to the previous test you'll notice is that this website states that tamusa.edu does not have a DMARC policy. Further analysis points to the DMARC policy being p=none. This leads me to believe that the tool we previously tested could potentially be inaccurate. You'll notice looking at the previous images that tamusa.edu's DMARC policy is confirmed by the other tool to also be p=none. Meaning there is no DMARC security. For security, this DMARC policy should be p=quarantine, but it is not so we should state that there is no DMARC policy. That is misleading, because though the domain has a DMARC policy because mail domains are required to list a policy to be legitimate that does not necessarily mean the policy is secure. Especially considering that with Gmail and Yahoo domains they're making a move away from zero policy.

mx:tamusa.edu

Find Problems

Solve Email Delivery Problems

mx



## Google and Yahoo! require DMARC

get to the Inbox with MxToolbox Delivery Center

Learn More

Pref	Hostname	IP Address	TTL	
10	tamusa-edu.mail.protection.outlook.com	52.101.10.10 Microsoft Corporation (AS8075)	60 min	Blacklist Check SMTP Test
10	tamusa-edu.mail.protection.outlook.com	2a01:111:f403:c946::6	60 min	Blacklist Check

	Test	Result	
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	<a href="#">More Info</a>
✓	DMARC Record Published	DMARC Record found	
✓	DNS Record Published	DNS Record found	

Your email service provider is "Microsoft Office" [Need Bulk Email Provider Data?](#)

[dns lookup](#) [dns check](#) [dmarc lookup](#) [spf lookup](#) [dns propagation](#)

Reported by ns1.tamusa.edu on 3/20/2025 at 9:29:31 PM (UTC -5), [just for you.](#)

[Transcript](#)

dmarc:tamusa.edu

Solve Email Delivery Problems

dmarc



## Think that you are on Google's Blacklist?

It's more complicated than that...

Learn More

v=DMARC1;p=none;rua=mailto:dmarc-monitor@tamusa.edu,mailto:dmarc\_agg@vali.email

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	none	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
rua	mailto:dmarc-monitor@tamusa.edu,mailto:dmarc_agg@vali.email	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.

	Test	Result	
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	<a href="#">More Info</a>
✓	DMARC Record Published	DMARC Record found	
✓	DMARC Syntax Check	The record is valid	
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.	
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.	

[dns lookup](#) [dns check](#) [mx lookup](#) [spf lookup](#) [dns propagation](#)

Reported by ns2.tamusa.edu on 3/20/2025 at 9:31:25 PM (UTC -5), [just for you.](#)

[Transcript](#)

Tool	SPF Support	DKIM Support	DMARC Support	TLS Support	Notes
Spoofy	✔ Yes	✗ No	✔ Yes	✗ No	CLI tool that checks SPF & DMARC only. Outputs spoofability score based on 198 DNS policy combinations. No DKIM/TLS functionality included.
MXToolbox	✔ Yes	✔ Yes	✔ Yes	✔ Yes	Web-based suite with tools for DNS, email, blacklist checks, and TLS diagnostics. Accurate SPF, DKIM, and DMARC analysis with enforcement status.
Domain-Security-Scanner	✔ Yes	✔ Yes	✔ Yes	✔ Yes	Open-source CLI and web tool. Supports `--checkTLS`. Web version is limited and slow; Docker implementation has reliability issues.