Auditing an Email server

Patrick Mattson

May 2019

patrick@dk-systems.com

Table of Contents

Proposal notes

Auditing an Email server

Understanding an email server, and how to secure it

Presentation title: Understanding an email server and how to review and secure one

Condensed Title for Promotional Use: Review and secure an email server

Target Audience: Beginner

Short description: Email is a service that is used by every business, verifying it is setup properly can help prevent a server from sending spam and reducing dangerous emails from entering your business.

Learning objective 1: After completing this session, the participate will have a basic understanding of the components in an email server and how an email is sent through the server.

Learning objective 2: After completing this session, the participate will understand what command line tools they can utilize to verify the settings on an email server.

Learning objective 3: After completing this session, the participate will understand industry best practices used to verify and reduce the risk that their domain is spoofed.

Learning objective 4: After completing this session, the participate will be able to describe risks associated with an unsecured mail server.

Abstract:
Email is a service that is used by every business and it is a primary way to communicate with others. There are some industry standards/settings that a company should have implemented. Missing a setting or two can cause a server to receive large amounts of spam or allow someone to send spam from their server(s). This presentation will discuss standard components of any mail server and how a message passes through the server. Today spammers will try to impersonate your domain when sending spam, we will discuss ways to reduce the risk by implementing DKIM, SPF, and DMARC records. An unsecure mail server can become a spamming host, we will discuss ways to check this. By explaining and demonstrating various command line tools and other resources the audience can see how to verify current settings. In a final demonstration I will pretend to be a spammer using an open source tool to spoof an email showing whatever information I would like.

Audience Engagement:
The presentation will cover the topic, I will add in experiences I have had dealing with my mail server. The presentation will continually be reviewed in the event there are new settings that should be implemented. I also plan to demonstrate on a live mail server the commands to show current settings and using an open source tool send an email from a live server.

Additional information:

A company I own hosts email for businesses. We have 75+ customers and 800+ users that we need to ensure they are protected. At Northwestern Mutual I work with teams to fix audit issues, currently I am assisting a team that has several email issues.

When it comes to sending and receiving a mail server uses the same basic components, how the email software uses those components varies. Understanding the component's role in as it relates to the server will help when reviewing your server's settings.

Attackers today can spoof almost any email address using free tools and can send large amounts of spam with these free tools. By implementing industry best practices, you can reduce your exposure to these threats. We will discuss how to reduce these risks.

Some companies have set up their servers with the default settings. These companies might be at risk of spreading spam and viruses. There are industry standards you should verify are not configured, we will discuss a few of these.

For the demonstration portion of the topic attendees will see various command line tools found in Linux (Kali Linux) or Windows to show current settings and how someone can send an email if they find an unsecured mail server. Attendees will also see various web sites that can verify settings. It is important an auditor or an IT security administrator understands the same tools a bad actor can use against them.

Learning objective 1: After completing this session, the participate will have a basic understanding of the components in an email server and how an email is sent through the server.

Learning objective 2: After completing this session, the participate will understand what command line tools they can utilize to verify the settings on an email server.

Learning objective 3: After completing this session, the participate will understand industry best practices used to verify and reduce the risk that their domain is spoofed.

Learning objective 4: After completing this session, the participate will be able to describe risks associated with an unsecured mail server.

What are the components of an email server.

There are only a few components related to a mail server. It does not matter whether it is a Microsoft Exchange or some form of a Linux email server. Some servers are composed of all of these in one box, others break it down into several servers. To add to the complexity some companies will utilize cloud-based components.

These are terms you will see in most cases:
Mail User Agent (MUA) is the application which is used to create, send, and receive emails. Examples: Microsoft Outlook, Lotus Notes, Mozilla Thunderbird, Eudora Mail, or Incredimail.

Mail Transfer Agent (MTA) - the service that sends and receives the email. This is the service that communicates using SMTP between other mail servers.

- Microsoft Exchange refers to this as the Edge server

Mail Delivery Agent (MDA) is the service that gets the email from the MTA and sorts it to the user's mailbox. This is an inbound function, not an outbound.

- Microsoft Exchange refers to this as the internal Exchange Mailbox server.

Often MTA and MDA are the same server.

Mail Host is the server that is the email server

Mailbox is the folder associated with a user, all email is received by the Mail Host and delivered to a mailbox.

The MUA communicates with the MTA using POP, IMAP, or SMTP. The MUA will go to the MDA to retrieve the new email.

Microsoft Exchange Components

Edge Transport - Mail Transfer Agent (MTA)

Edge Transport servers handle all inbound and outbound Internet mail flow by providing mail relay and smart host services for your Exchange organization. In addition, it provides additional layers of message protection and security, such as spam filtering and virus scanning, and apply Transport rules. Transport rule conditions are based on data, such as specific words or text patterns in the message subject, body, header, or from address; the spam confidence level (SCL); or the attachment type.

Incoming mail -> Edge Transport Server -> Front End Transport service -> Transport service -> Exchange Mailbox Server -> user retrieves

Client Access Server
Mailbox Server (Spam filtering)
Hub Transport

Getting the Spam settings

```
[PS] C:\Windows\system32>Get-TransportAgent

Identity                                                Enabled
--------                                                -------
Transport Rule Agent                                    True
Malware Agent                                           True
Text Messaging Routing Agent                            True
Text Messaging Delivery Agent                           True
Content Filter Agent                                    True
Sender Id Agent                                         True
Sender Filter Agent                                     True
Recipient Filter Agent                                  True
Protocol Analysis Agent                                 True
```

EdgeSync

https://docs.microsoft.com/en-us/exchange/exchange-server?view=exchserver-2019

- The Edge Transport server should never be an Active Directory (AD) domain controller or in the domain. It needs your AD data, so it gets data synchronized from AD.
- This data is synchronized to the Edge Transport server by the Microsoft Exchange EdgeSync service (EdgeSync). EdgeSync establishes a one-way replication from AD to the Mailbox server. It utilizes Active Directory Lightweight Directory Services (AD LDS). The only information that is transferred is used to perform antispam configuration tasks and to enable end-to-end mail flow. Data is sync'd on a schedule to get updates so the information in AD LDS remains current.

Other components:

DNS Settings

An important component, if your settings are incorrect you may not receive email, or it may be intermittent. We will discuss later additional settings you can add to help secure your server. The following are important:

DNS record - **MX** record, stands for **M**ail e**X**changer

When someone wants to send you an email, their MTA will query the DNS servers you have specified for your domain name to get a list of MX records. The MX record is the name of the host/server the sender will communicate with when sending email, it is a good idea to have more than one. If this record does not exist or is incorrect, they may receive a message no mail server found. If there is more than one, it looks at the weight and talks to the lowest number first.

Verify you have an MX record(s) for each domain name your organization owns.

As an auditor, you should review what MX records your DNS servers have, compare that to what servers you have, they should match. If you find one that does not match, it should be noted and investigated. The entry will consist of a names and weight of your mail servers. There should also be an A record that points a name to an IP. Some companies may only have one record, this means they have one mail server. It is a good idea to have multiple MX records, but this also means you need multiple mail servers. If you find an MX record that no one seems to know about, has this server been secured recently?

The weight, sometimes referred to as a preference, is the order in which the MX server is chosen, the lower the weight the higher the priority. If for some reason MX server 1 is down, it will move to the next lowest number MX address.

For my customers I have a backup server, if for some reason my primary server is down email will go to my backup server. Once the primary comes back online, it will check the backup server for any emails it collected while it was unavailable. This works great when I need to perform maintenance emails are not lost.

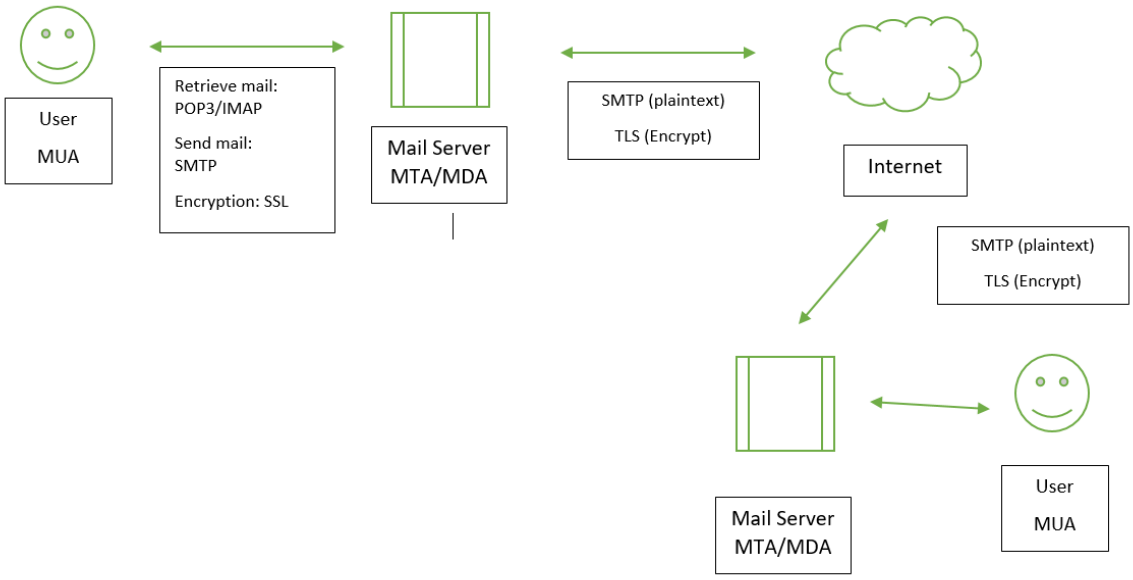
Sample BIND record

example.com.	3600	IN	MX	0	mail.example.com.
example.com.	3600	IN	MX	20	mail2.example.com.
mail.example.com.	3600	IN	A	10.0.0.10	
mail2.example.com.	3600	IN	A	10.0.0.20	

With the records above the domain example.com's primary mail server is mail.example.com (IP 10.0.0.10), but if that is not available mail2.example.com (IP 10.0.0.20) will step in and receive email.

Note, this backup server(s) may not deliver email to the mailboxes, that is a more advanced topic.

Diagram



Quick checks:

- Have you checked who has administrative access?
- When was the last time the administrator(s) password(s) were changed?
- Logging, each server is different, but they still save the logs.
  - What policies and procedures do they have to set up server?
  - Where are the logs located?
  - How long are the logs saved?
  - Are the logs sent to an application like Splunk (paid) or ELK (open source)?
  - What are the permissions on the log files?
  - Is detailed set or is it's minimal reporting, more detail is better for reviewing, but takes up more space?

Server Logs

- SMTP, will the connections, it will show failed login attempts
- Delivery, how the email is delivered to the end user

Backup server

- Does your organization have a backup mail server in case the primary does down?
- Is there an MX record for the server, what is the weight/priority?

The email

Components of an email

- Header
- Body

The header contains information about the security checks and the from address. Different mail servers provide different information about the email and its delivery. By default, the header information is not shown, but it can be viewed.

Reading a header, start at the bottom and work your way up.

Why look at the header?

- Is your Spam filtering picking up Spam?
- Is your email security set up properly?

Sample header (Gmail showing security)
When testing if you use a Gmail account and someone sends a secure email you will see a yellow/gold arrow.

Sample email full source downloaded from a Gmail account, this email had all pieces of security (SPF, DKIM, and DMARC)

Header reader/translater: https://toolbox.googleapps.com/apps/messageheader/

Communication methods

POP3 - Post Office Protocol - Version 3

- MUA communicates with server and retrieves email from the server
- Default port 110 (plaintext)
- Default port 995 (secured)

IMAP - Internet Message Access Protocol Version 4 (latest)

- MUA communicates with server and displays email on the server. Like a web client (Gmail, yahoo, etc.). If an email is removed it is removed from the server.
- Default port 143 (plaintext)
- Default port 993 (secured)

SMTP - Simple Mail Transport Protocol

- MUA sends emails to MTA using SMTP
- Used to communicate server to server, sending email back and forth
- Default port 25 (plaintext)
- Default port 465 (secured)
- Vulnerable to relay attacks

Secured using an SSL or TLS certificate:

- SSL should be used for Ports: 465, 993, and 995
- TLS should be used for Ports: 25, 110, and 143

Industry standards are you implementing encryption to be compliant
- Record retention
- Encryption (HIPAA)

Which ports are open on your mail servers?

Command to run to see what IPs and ports are listening/open on your server(s):

Windows
- From an administrative command prompt type: **netstat -aon | find /i "listening"**
- To send to a file type: **netstat -aon | find /i "listening" > filename.txt**
    - Change the file name from filename.txt to something else

Linux
Widen the PuTTY screen
- **sudo netstat -plnt**
- Pipe to a file: **sudo netstat -plnt > filename**

If you ask an administrator to run this command have them send you the file you created so you can review it at a later time. This does not impact a system.

Defenses against email spoofing

SPF - Sender Policy Framework

The first step in reducing a Spammers chance of impersonating your domain.

Used to verify which server(s) can **send** email for this domain, it is used to prevent others from sending email from other servers. For example, a spammer is spoofing your domain but send from their PC. Because the receiving server looks up and your SPF record and notices it is not a verified IP to send from, depending on the setting they may reject the email. This is a DNS text (TXT) record and it can contain an IP address, an IP range, or DNS names.

It is your company's sending policy, you are saying which servers can send your company's email. This can be a fully qualified domain name (FQDN), an IP address, or even a range (CIDR notation)

What if your company utilizes a service such as Constant Contact to send out newsletters? If you forget to add them to your SPF record, the emails might get flagged a spam and be deleted or go to the junk folder.

Items to add:
A mail server that has an MX record already existing: a:server1.example.com
Two or more servers: a:server1.example.com server2.example.com
A single IP: ipv4:2.3.4.5
A range use CIDR: ipv4:1.2.3.0/24

A range and a single IP: ipv4:1.2.3.0/24 ipv4:2.3.4.5

Sample entry:
This is an example for a BIND record
example.com. TXT "v=spf1 a mx a:mail.example.com include:_spf.google.com -all"

v=spf1 a mx ip4:1.2.3.4 include:_spf.google.com ~all

If you wanted to add a mass mailing company like constant contact you would add:
include:spf.constantcontact.com

So looking at our sample above, the DNS record would look like:
v=spf1 a mx ip4:1.2.3.4 include:_spf.google.com include:spf.constantcontact.com ~all

Breakdown:
v=spf1 - This is the version of the SPF standard, they are currently only on 1
mx - **M**ail e**X**changer, the server responsible for sending email
a: an A record in DNS terminology

Qualifiers of the **all**:
"+" Pass
- The SPF record states that the host is permitted to send

"-" Fail
- The SPF record states that the host is NOT permitted to send

"~" SoftFail
- The SPF record states that the host is NOT permitted to send but is in transition

"?" Neutral
- The SPF record states explicitly that no judgement is made on the validity of the host

Be careful with the all, if you set it to the "-" and you forget to add a record to SPF record email will fail.

To utilize the all, the receiver needs to have that as part of their checks, most companies do. So if you send someone an email, their mail server will query your DNS for the SPF record. If the sending IP or domain name is not in the record and you have the "-" set, they will reject your email.

To give an example, if you added a new IP 1.2.3.4 and you have the - set.
SPF creation tool, there are many here is just one: https://mxtoolbox.com/SPFRecordGenerator.aspx

What is your company's SPF record?

The dig command
dig (domain information groper) a command-line tool for querying Domain Name System (DNS) servers.

Testing SPF
Linux via dig command
The command is **dig** (@DNS server) (domain name) (record type)

Test through your name servers (DNS Servers)
dig @ns1.yourdomain.com example.com txt

Test through Google
dig @8.8.8.8 example.com txt

Reference:
http://www.openspf.org/
https://support.dnsimple.com/articles/spf-record/
http://www.openspf.org/Mechanisms
https://postmarkapp.com/blog/explaining-spf

DKIM - DomainKeys Identified Mail

DKIM provides a method for validating a domain name identity that is associated with a message through cryptographic authentication (public and private keys).

When an email leaves your mail server it is given a digital signature. It verifies who you are.

This is generated by the MTA sending the email, the signature is generated by using your public key. When the receiving MTA receives the email, it can perform a query to your mail server and compare your public key signature.

DNS record is a TXT
Sample DNS record: v=DKIM1;k=rsa;p=MIGfM

The p= is the public key created by your mail server, the private key is on your server.

Reference:
http://www.dkim.org/

DMARC - Domain-based Message Authentication, Reporting, and Conformance

The DMARC requires a domain has both an SPF and DKIM record. Your DMARC record tells the receiver what to do if your message does not pass.

Reference with picture: https://blog.returnpath.com/how-to-explain-dmarc-in-plain-english/

Create a DMARC Record: https://blog.returnpath.com/build-your-dmarc-record-in-15-minutes-v2/

Test
dig _dmarc.example.org txt

DKIM - Domain Keys Identified Mail

Test
dig google._domainkey.example.com txt

Sample output:

_dmarc.example.com. 300 IN TXT "v=DMARC1; p=reject; aspf=s; fo=1; ri=3600; rua=mailto:dmarc_rua@example.com; ruf=mailto:dmarc_ruf@example.com"

Breakdown

Here are the common tags used:

Tag name	Required	Purpose	Example
v	Required	Protocol versions	v=DMARC1
p	Required	Protocol for domain	p=quarantine
pct	Optional	% of message to filter	pct=100
rua	Optional	Report UTI of aggregate report	Rua=mailto:postmaster@example.com
aspf	Optional	Alignment mode for SPF	aspf=r
sp	Optional	Policy for subdomains	sp=r

(p) Policy Tag options

- None - Do nothing, send the log of messages in the daily report
- Quarantine - Mark the message as Spam
- Reject - Reject the message at the SMTP layer

Deploying the DMARC

Start slowly, if you start too high you could block legitimate email

Suggested start:

Step	Suggested	p tag value	pct tag value
1	Monitor all	p=none	Leave blank
2	Quarantine 1%	p=quarantine	pct=1
3	Quarantine 10%	p=quarantine	pct=10
4	Quarantine 25%	p=quarantine	pct=25
5	Quarantine 50%	p=quarantine	pct=50
6	Reject all	p=quarantine	pct=100
7	Reject 1%	p=reject	pct=1
8	Reject 10%	p=reject	pct=10
9	Reject 25%	p=reject	pct=25
10	Reject 50%	p=reject	pct=50
11	Reject all	p=reject	pct=100

How to start DMARC
Start collecting data safely

Publish “p=none” DMARC for all domains

Receivers can enforce a policy against unauthenticated email
- None (also known as monitor mode, will not impact mail)
- Quarantine (should send to the Spam/Junk folder)
- Reject (never sees any mailbox)

The “pct” tag
- Start with “pct-10”, apply policy to 10% of unauthroized email
- If a policy is not applied due to pct tag, “next lesser” policy is applied

Reference: http://www.zytrax.com/books/dns/ch9/dmarc.html

Reading a DMARC record

Created in an XML format.
https://dmarcian.com/xml-to-human-converter/

Defensive domains

A defensive domain is used defend your domain name. Often the defensive domain names are very similar to your primary. First need to know all the domains your company uses, maybe it is one.

Depending on how big you are or what your company does, for example Google might buy gooogle.com. Scammers will try to register domains like yours. They will try send out emails and when someone looks at it, since it is close to yours people might think it is really you.

Unsecured email server

There are many things that can impact your company with an unsecured server.

Authentication

A big problem, but with most modern email servers this is an email server being an open relay, this can be solved by requiring authentication in order to send email from your server. An open relay allows anyone to send email.

If authentication is not turned on, your mail server(s) could become an open relay. This means anyone on the internet can send email. These are also known as a spamming box.

Does your mail server require authentication to send email?

Usually a setting to turn on. What is your mail server settings at?

Spam filtering

Today what is the one thing we most dislike about our email, it is all the junk mail we get, best known as Spam.

Spam is the unwanted email, can contain viruses, phishing scams, and just fills up an inbox.

Some examples of unwanted mail, bulk mail, junk mail, you get the picture.

- Lose weight
- The CEO is stuck and needs help
- You won money
- I got robbed in London, send money

Is your company filtering out bad email?
Larger companies will use companies like IronPort, Proofpoint, etc. Smaller companies may use a combination of Spamassassin, Barracuda, and Realtime Black Lists (RBLs). It is often on a separate server, in some cases it is up in the cloud. A layer before it reaches your mail server.

In any of these cases, email is filtered based on criteria that is defined. Here are some examples of the different types of criteria:

- Content filters - review the content within a message
- Header filters - review the email header information
- General blacklist filters - block email based on known bad IPs of known spammers
- Rules-based filters - user-defined criteria – keywords, email address(es), or domain names

Types of filters:

- Gateway, physical machine, often in house, that all email passes through. Set in front of your mail server to act as a first line of defense.
- Hosted, email goes up into the cloud and gets processed
- Desktop, not as popular, on a user's desktop device

An email gets a score based on certain things. At the end if an email has a certain score it is often: marked as Spam, quarantined, moves to junk mail, or deleted.

Just like some companies use Realtime Black Lists, you need to check your sending IPs to see if they are on blacklists. As an auditor you will want to check this a simple tool for this is mxtoolbox.com. If you find yourself on one of these blacklists, you will want to make a note in your report. This could prevent your recipients from receiving your organization's email, if the receiver uses that blacklist as a check.

How do you get on a blacklist?
That all depends on the blacklisting organization's criteria, if a spammer blasted several thousand emails from one of your servers. You do not have validation in-place, SPF, DKIM, DMARC, etc. When on a blacklist, and you are sending legitimate email, it may get rejected by the receiver if your company's IP(s) are blacklisted.

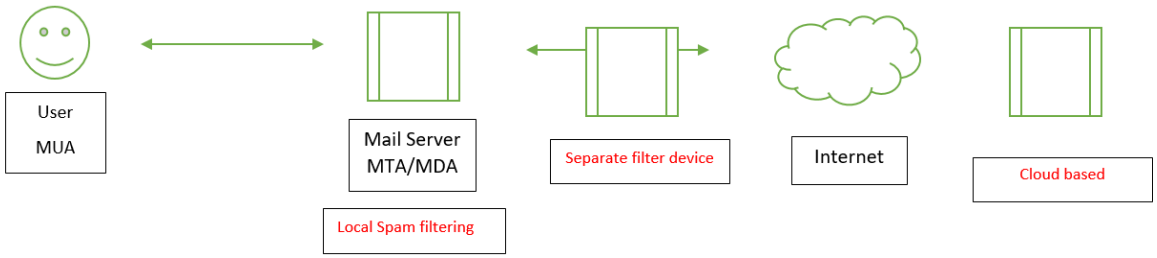
Many countries have some form of Spam law, you can be fined.

The United States
Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003

Many different providers available, the better the service and features the higher the cost.

- Locally hosted:

    - Spamassassin (free, we will be discussing)
    - Untangle
    - Barracuda, subscription based
    - There are others
- Cloud based or SaaS Anti-Spam:
    - Barracuda, they offer both options
    - ProofPoint
    - IronPort
    - Mimecast
    - MailCleaner
    - Many others



Retry sending emails

Does your server attempt to make additional attempts after the first attempt? Maybe the receiving server is down or is busy. What happens, if you have not set up your mail server to retry the message will fail that one time. If the organization has a backup mail server your email will get delivered there because the first server did not respond back.

It is important to have a retry of several days.

Microsoft Exchange uses the Edge server to perform Spam filtering.

Disabling VRFY/EXPN

These commands can return if a user exists on the server.

VRFY - Will verify an ID on the mail server, hackers will use this to discover potential email accounts and system accounts.

By default, many mail servers disable this, there is always that one that might not. Exchange began disabling with Exchange 2000. We will see commands to test later and if any IDs can be identified it will be important to disable immediately.

EXPN - Will expand a mailing list, in Exchange a distribution list.

Just like VRFY, this should be disabled and is by default on most mail servers.

Collect logs

Without audit logs you cannot see what has been going on. For example, failed login attempts or a login from a strange IP at a strange time of day.

Are your logs copied off of your server?

There are services like Splunk and ELK that allow you to collect logs from various sources and report issues found and alerts can be sent out.

Auditing mailboxes in Microsoft Exchange

If you want to see activity on a mailbox, auditing needs to be turned on.

Exchange can audit mailboxes for activity, if you need to monitor activity for PII or other sensitive information being processed you should verify this is enabled.

Review the following logs:

- Administrator - Activities on the server
- Mailbox - Mailbox activities

To see the status of an account, you can run the following command in a PowerShell:

- Get-Mailbox [user name] | FL
- Replace [user name] with the name of the user
- Part of the results will show AuditEnabled it will be False or True

Defenses

SSL Certificate

Before going to deep, the term SSL Certificate has been used for years. We will be using this certificate with protocols: SSL and TLS. SSL is an older version and has many vulnerabilities. TLS is the newer technology when it comes to secure protocols. SSL stopped at version 3.0, TLS 1.0 took over.

By default, an email server sends its information via plaintext. What does plaintext mean and why could this be an issue? Anything sent through plaintext is visible to anyone who might be collecting packets from a network. It would show everything from passwords to the body of the message.

By verifying you an SSL certificate has been installed and is current it will ensure communications are secure. It will scramble the content, not the header and will make no sense to anyone collecting packets.

So what communications are secured? IMAP, POP, SMTP, and if you have a web interface the interface.

Something I learned. To secure my mail server I discovered some protocols open. Wanting a secure server, I disabled some older SSL protocols. Next day started getting calls. Turns out older versions of Outlook use the older SSL protocols. People were getting a message they could not talk to my server.

Options for getting an SSL certificate:

- Paid version, offers insurance
- Free through https://letsencrypt.org/

Test your server's SSL: https://www.ssllabs.com/ssltest/

- Type your domain name(s), I would check the box to not publish results

Test your server's TLS: https://www.checktls.com/TestReceiver

- Type your domain name(s)

Installing and automatically updating Let's Encrypt. Look at this tool: https://certbot.eff.org

SSL, TLS, and STARTTLS Email Encryption

SSL and TLS are transport-layer protocols (Layer 4), there some documentation saying the session-layer (Layer 5), and application-layer (Layer 7). Since it is encryption, the OSI model never really discusses encryption.

SSL and TLS encrypt the traffic, sometimes the application will initiate the security.

STARTTLS an email protocol command that tells an email server it wants to change from an existing insecure connection into a secure one. When one server communicates I have a connection I am using TLS it is sending a STARTTLS command. If the other server is using TLS the entire session is encrypted from end to end between the two servers.

TLS is newer than SSL
TLS 1.0 was unofficially known as SSL 3.1

By default the emails are sent unencrypted and are therefore in plain text.

Google sends via TLS, if the receiver is not listening for secure connections Google will send insecurely.

Do not confuse this with truly encrypted email. This is often a service. If you are sending someone a secure email the most secure way is through a third-party. The sender sends to a server, then depending on the service will only allow the receipt to come to the server to get the email.

A good practice is to encrypt: SSL on ports465 (SMTP), 993 (IMAP), and 995 (POP3) and TLS on ports 25 (SMTP), 110 (POP3), and 143 (IMAP)

Spam filtering

We discussed above

Block file extensions

Some companies have decided to block extensions like: exe, bat, com, and vbs

Blocking .zip files could impact your users, but there is a trade-off, viruses can be delivered in a zip file.

Virus scanning

Is your server scanning for viruses as they come into the network?

Test by emailing a file from http://www.eicar.org/

- Eicar is a test virus file that gets flagged by good virus scanner. It is not harmful.
- It will tell you if your antivirus is working.

Greylisting

Reference: https://www.greylisting.org/

An email comes to your mail transfer agent (MTA) when greylisting is enabled, your server will send back a response “Try Again later”. It gives a "temporarily reject" from an unknown sender. This action occurs at the SMTP layer.

A new email comes into your MTA, if your server has not seen this sender’s IP before, it will reply to the sending MTA server please try again in X minutes. If the sending server is configured properly it will attempt to resend the message at the time set by the receiving email administrator.

So how does this help, a spammer will never see the message because they do not have an RFC compliant server, they have already moved on to the next spamming target. The result the message is not resent. If a legitimate server sends the email a second time, that address will be added to a list. There is a downside, if you are expecting an email from someone it may get delayed. You can add items to a whitelist, a trusted/safe list.

Ways to by-pass a greylisting

- Add the sender’s IP address or IP range, also known as whitelisting
- Add an email address to a whitelist
- Add an entire domain to a whitelist

One issue I was starting to see with my hosting company, the sending servers were not retrying. They must have been set up wrong and never retry sending. I had to disable it, hosting about 80 companies I did not want to run the risk of losing email.

Outbound scanning for Spam

Retry sending emails. Look for a lot of bounces, this will tell you someone is sending to an invalid email. A sign this account sending out spam.

Cyrillic characters

Throttling/Message Limits

Restricts outbound email if a certain threshold is met. On my servers I set a limit of 2000 messages in a certain period of time for one customer and others I set 300 messages in that same time frame.

What does this tell me? 9 out of 10 times someone’s password was compromised and a spammer is blasting out large amounts.

So what happens when my thresholds are met, it will wait about 10 minutes before sending the next batch of emails.

If you send out to many bad emails in a certain timeframe your IP could be flagged as a spammer and put on blacklists.

References for Microsoft Exchange:
https://docs.microsoft.com/en-us/exchange/mail-flow/message-rate-limits?view=exchserver-2019
https://docs.microsoft.com/en-us/office365/securitycompliance/outbound-spam-controls

Avoiding being a Spammer

Provide an unsubscribe link, can be tough because some people do not know if they can trust your link. This should get appended automatically to any bulk email your company sends.

Checking if your servers are on blacklists

What is a blacklist and what if my server is on one?
There are sites that collect information on IP and domain name activity. If an IP address or domain name has been sending out too many messages at one time, it may get added to a list. Many email services look at these lists during Spam checks.

The website mxtoolbox.com does a nice job of summarizing all of the most common blacklisting sites.

Here are some sites you and your email administrators can use:
http://postmaster.google.com/ (to verify your domain name)
https://www.senderscore.org/ (Need to register a domain, but can look up stats on your IPs)
https://www.talosintelligence.com/ (Look up your domain and IP reputation)
http://multirbl.valli.org/lookup/ (Look up if your IP is on any blacklists)

Reference:
https://postmarkapp.com/blog/how-to-check-your-ip-reputation

Tools/Demo

I registered two (2) domain names for this presentation:

- mymxdemo.com
- mymxdemo.net (the one that will show misconfigurations)

For both domains you as a guest can send and receive emails for testing purposes:
Website:

- https://mail.mymxdemo.com
- https://mail.mymxdemo.net

Username: isacademo
Password: NACACS2019!

During my demonstrations I will be using Kali Linux. Remember if you are using a Linux operating system it is case sensitive. So this command: dig and Dig would be two different commands. The same is with the switches.

Basic connection

I prefer to use PuTTY (**putty.exe**, 32-bit is fine, it is a standalone file no installation needed), I use it for SSH, too.

Download: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

During these demonstrations you will not a need a username and password until I note it.

Basic connection

```
220 mail.mymxdemo.com ESMTP Postfix
ehlo mail.patrick.com
250-mail.mymxdemo.com
250-SIZE 15728640
250-STARTTLS
250 DSN
```

I send it anything with the ehlo, it needs to be domain name correct or not
Size is how big of an email the server will accept in bytes (15MB)
StartTLS means the server offers TLS communication

Demonstration

Dig commands through Linux, can get dig for Windows or use NSLOOKUP

MX record look up

Looking up your MX records using the name servers on your computer
Run the following command: **dig example.com MX**

To use another name server, for example Google's public IP
dig @8.8.8.8 example.com MX

dig mymxdemo.com MX

```
root@kali1:/# dig mymxdemo.com MX

; <<>> DiG 9.11.4-P2-3-Debian <<>> mymxdemo.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 69
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1452
;; QUESTION SECTION:
;mymxdemo.com.                  IN      MX

;; ANSWER SECTION:
mymxdemo.com.           300     IN      MX      0 mail.mymxdemo.com.

;; Query time: 54 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Fri Mar 08 06:31:40 CST 2019
;; MSG SIZE  rcvd: 62
```

The command we just ran uses the DNS servers you have defined on the computer you are currently using, in my case I am using 1.1.1.1 (CloudFlare's public DNS server). You can see the priority is 0 and the name of my server.

If you want to use another DNS server, add it with the @IP, in the example below I am using one of Google's public IPs.
dig @8.8.8.8 mymxdemo.com MX

That was a boring example, let us see one with a backup server:

```
root@kali1:/# dig gmail.com MX

; <<>> DiG 9.11.4-P2-3-Debian <<>> gmail.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3237
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1452
;; QUESTION SECTION:
;gmail.com.                     IN      MX

;; ANSWER SECTION:
gmail.com.              2100    IN      MX      30 alt3.gmail-smtp-in.l.google.c
om.
gmail.com.              2100    IN      MX      40 alt4.gmail-smtp-in.l.google.c
om.
gmail.com.              2100    IN      MX      5 gmail-smtp-in.l.google.com.
gmail.com.              2100    IN      MX      10 alt1.gmail-smtp-in.l.google.c
om.
gmail.com.              2100    IN      MX      20 alt2.gmail-smtp-in.l.google.c
om.
```

One box shows the weights/priority the box is the servers.

NSLOOKUP (Windows), look up an MX record
From a command prompt, type **nslookup**

Type: **set type=mx**

- This gives a lookup of the MX type there are others

Type the domain name

```
PS C:\> nslookup
Default Server:  one.one.one.one
Address:  1.1.1.1

> set type=mx
> mymxdemo.com
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
mymxdemo.com    MX preference = 0, mail exchanger = mail.mymxdemo.com
>
```

The non-authoritative answer is saying this is not your primary DNS server. The primary is the one you use for your registration.

Example with more than one record:

```
> set type=mx
> dk-systems.com
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
dk-systems.com  MX preference = 30, mail exchanger = mail2.dk-systems.com
dk-systems.com  MX preference = 10, mail exchanger = mail.dk-systems.com
>
```

IP/A record of your mail server

CNAME (Mail server names)
dig mail.example.com

From our previous example: dig mail.mymxdemo.com

```
root@kali1:/# dig mail.mymxdemo.com

; <<>> DiG 9.11.4-P2-3-Debian <<>> mail.mymxdemo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38117
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1452
;; QUESTION SECTION:
;mail.mymxdemo.com.             IN      A

;; ANSWER SECTION:
mail.mymxdemo.com.      300     IN      A       66.195.55.226

;; Query time: 38 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Fri Mar 08 06:38:43 CST 2019
;; MSG SIZE  rcvd: 62
```

Are these IPs owned by your company?

NSLOOKUP
Type: **set type=a**

```
> set type=a
> mail.mymxdemo.com
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    mail.mymxdemo.com
Address:  66.195.55.226
```

By adding a **+short** to the end we get less information

dig Short example

To see less information, add a **+short** to the end of the command

dig mymxdemo.com MX +short

```
root@kali1:/# dig mymxdemo.com MX +short
0 mail.mymxdemo.com.
root@kali1:/#
```

To use another DNS server
dig @8.8.8.8 mymxdemo.com MX +short

Back to gmail example:

```
root@kali1:/# dig gmail.com MX +short
10 alt1.gmail-smtp-in.l.google.com.
20 alt2.gmail-smtp-in.l.google.com.
30 alt3.gmail-smtp-in.l.google.com.
40 alt4.gmail-smtp-in.l.google.com.
5 gmail-smtp-in.l.google.com.
```

Look ups
Mail servers

dig SPF/TXT record

dig isaca.org TXT

```
root@kali1:/# dig isaca.org TXT

; <<>> DiG 9.11.4-P2-3-Debian <<>> isaca.org TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19259
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1452
;; QUESTION SECTION:
;isaca.org.                     IN      TXT

;; ANSWER SECTION:
isaca.org.              300     IN      TXT     "v=spf1 ip4:50.31.141.71 include
:spf.protection.outlook.com include:spf.exclaimer.net include:_spf.salesforce.co
m include:rnmk.com ip4:192.254.116.40 -all"
isaca.org.              300     IN      TXT     "google-site-verification=KneeQl
P_vGGTE-kpXaC2hGIYxg7a3Vfh0XSWVr9Qy2c"

;; Query time: 6 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Sat Mar 09 08:45:30 CST 2019
;; MSG SIZE  rcvd: 285
```

NSLOOKUP SPF/TXT record

Type: **set type=txt**
Type the domain name

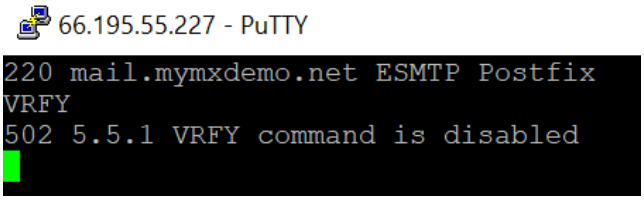
```
PS C:\> nslookup
Default Server:  one.one.one.one
Address:  1.1.1.1

> set type=txt
> isaca.org
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
isaca.org       text =

        "google-site-verification=KneeQlP_vGGTE-kpXaC2hGIYxg7a3Vfh0XSWVr9Qy2c"
isaca.org       text =

        "v=spf1 ip4:50.31.141.71 include:spf.protection.outlook.com include:spf.exclaimer.net include:_spf.salesforce.co
m include:rnmk.com ip4:192.254.116.40 -all"
>
```

For DMARC record
Add **_domain.**<domain name>

```
root@kali1:/# dig _dmarc.isaca.org txt +short
"v=DMARC1; p=quarantine; sp=none; adkim=s; aspf=s; rua=mailto:dmarc_rua@isaca.or
g; ruf=mailto:dmarc_ruf@isaca.org; rf=afrf; pct=100; ri=604800"
root@kali1:/#
```

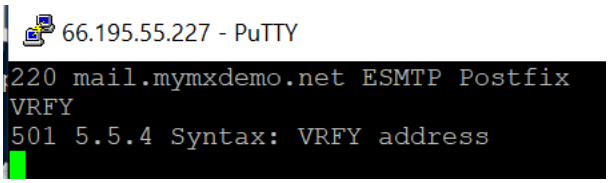
Testing VRFY

After the mail server greats you just type: VRFY

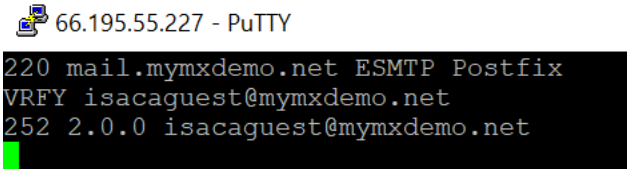


This tells us the command is disabled.

With the command enabled, I can see this command is active I just did not type it right:



Now I will test against an address I know exists:



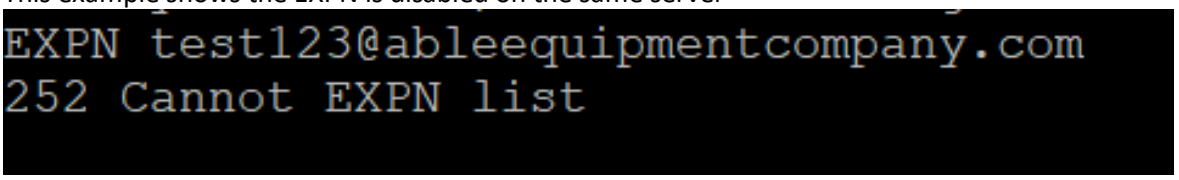
Success or failure depending on who you are!

Testing EXPN

EXPN shows the members of a group, this can be bad because it provides someone a potential list of valid email addresses.

This example shows EXPN is enabled

This example shows the EXPN is disabled on the same server



Open relay

If any of your SMTP servers are set to be an “open relay” a spammer can take advantage of this. What they will do is send email using your SMTP server. Having an open relay can put your public IP address on too many different blacklists.

The best defense is to verify anyone using your SMTP server to send email is set to use authentication. Meaning the sender must provide a valid user name and password.

If your server is open to be a relay, you can use a simple program like Blat and send emails using any name and email you want.

What you should see, notice the not permitted to relay

```
220-host.teensouq.com ESMTP Exim 4.91 #1 Fri, 15 Mar 2019 23:27:55 +0530
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
HELO mail.iamdoingademo.com
MAIL FROM: bobsmith@oddnamed.com
RC250 host.teensouq.com Hello mail.iamdoingademo.com [216.20.176.8]
PT TO: isacaguest@mymxdemo.net
250 OK
DATA
SUBJECT: Hello this was sent through a demo
550-Please turn on SMTP Authentication in your mail client.
550-(mail.iamdoingademo.com) [216.20.176.8]:52191 is not permitted to relay
550 through this server without authentication.
503-All RCPT commands were rejected with this error:
```

Running an Open Relay against a machine

Open relays are bad, it allows someone to send email without authenticating to your server. Hint spammers love these servers.

If you can run the following commands and send yourself an email, not good.

Note there is a period (.) between the quit command

telnet mail.example.com 25

HELO mail.iamdoingademo.com
MAIL FROM: bobsmith@oddnamed.com
RCPT TO: isacaguest@mymxdemo.net

DATA
SUBJECT: Hello this was sent through a demo

This is the body of my email and I did not authenticate.

Took me a while to find an open relay to demonstrate.

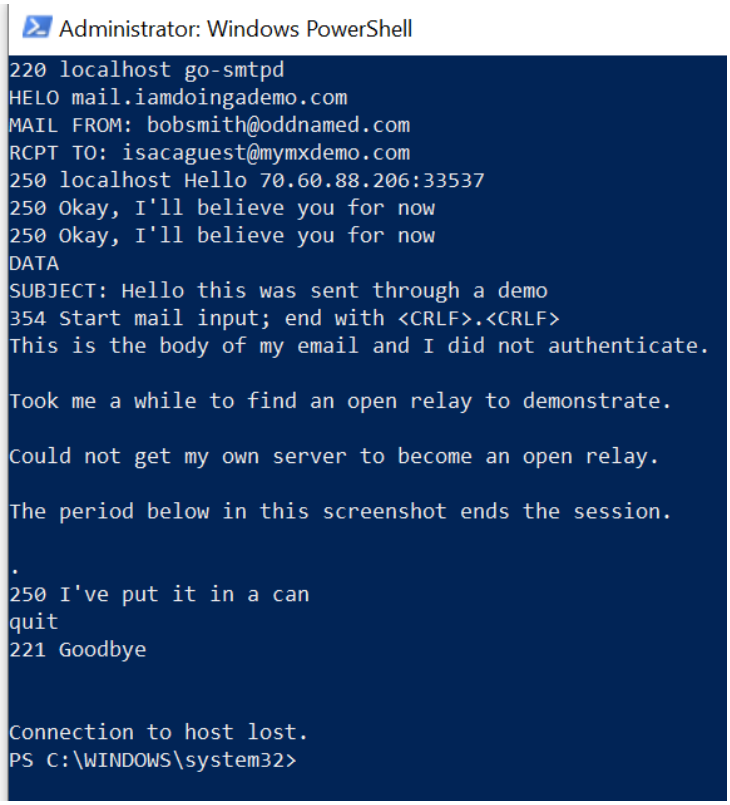
Could not get my own server to become an open relay.

The period below in this screenshot ends the session.

.

quit

Not good, the 250 in the image below is everything went through ok. This was a domain I found sending my server spam. I never received the email because my spam filtering blocked it. The server's IP was on a blacklist.



Tools
Mxtoolbox.com

Kali Linux
iSMTP
smtp-user-enum (disable vrfy response) (EXPN)

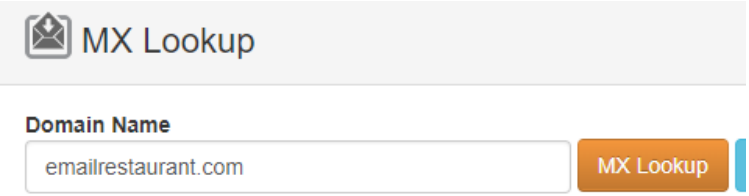
Section 3.5.2 https://www.ietf.org/proceedings/50/I-D/drums-smtpupd-13.txt

Mxtoolbox.com

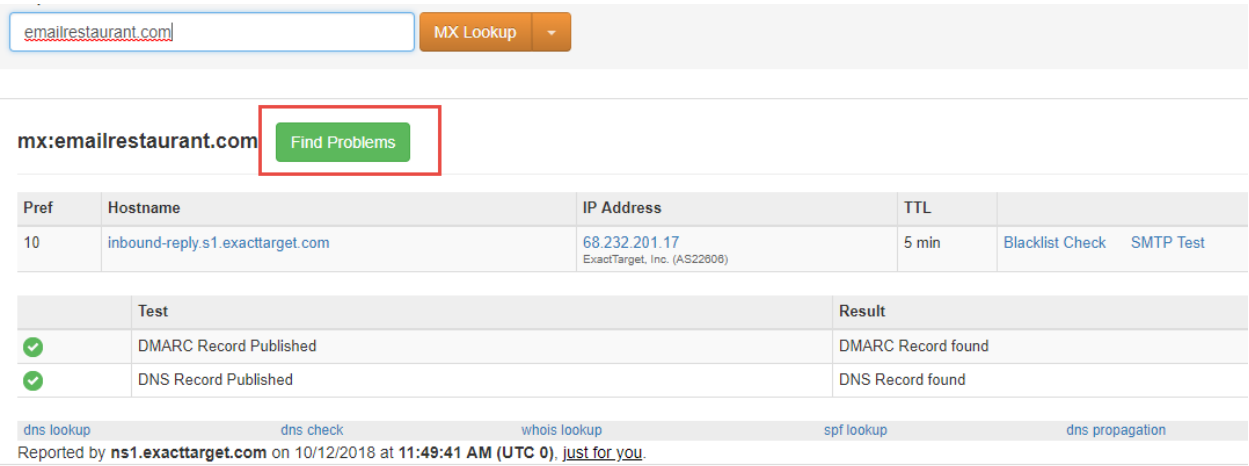
Will provide a lot of information about your company and a sending company.

A basic lookup can help show potential issues, the very blatant problems.

Basic lookup:



Shows all the servers that respond to the MX DNS record lookup.



Click Find Problems, this will show misconfigurations.

Here we see there are three (3) potential problems. The open relay could be a really big one.

3 Problems

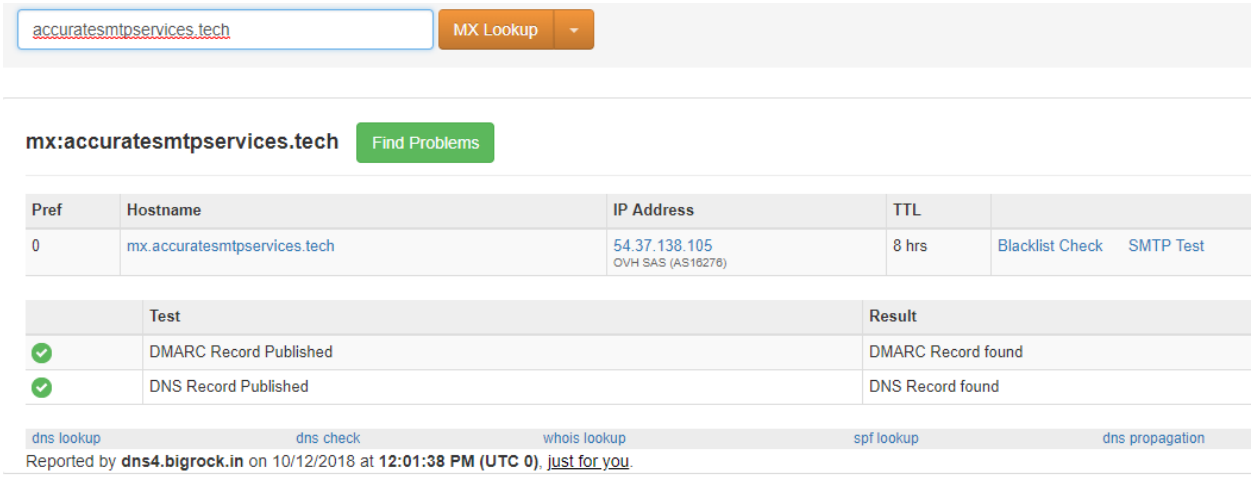
	Category	Host	Result
✖	http	emailrestaurant.com	The remote name could not be resolved: 'emailrestaurant.com' (http://emailrestaurant.com)
!	dns	emailrestaurant.com	Local NS list does not match Parent NS list
!	smtp	inbound-reply.s1.exacttarget.com	May be an open relay.

MXToolbox helps and you can pay for a service from them. For additional details, click on the More Info icon.

Let's look at one that has been sending Spam as an example. We will pretend this is our domain.

accuratesmtpservices.tech

So far so good



Click on Find Problems

7 Problems

	Category	Host	Result
✖	http	accuratesmtpservices.tech	The remote name could not be resolved: 'accuratesmtpservices.tech' (http://accuratesmtpservices.tech)
✖	blacklist	accuratesmtpservices.tech	Blacklisted by ivmURI
✖	blacklist	accuratesmtpservices.tech	Blacklisted by Spamhaus DBL
✖	blacklist	mx.accuratesmtpservices.tech	Blacklisted by ivmURI
✖	blacklist	mx.accuratesmtpservices.tech	Blacklisted by Spamhaus DBL
!	dns	accuratesmtpservices.tech	Name Servers are on the Same Subnet
!	dns	accuratesmtpservices.tech	SOA Expire Value out of recommended range

We did find a few issues, so if this was our domain, we can see what needs fixing. One major issue is being on the Blacklists.

Checking SSL security

Nice site to show the security of your server: https://www.ssllabs.com/ssltest/

Enter your site: https://example.com

Analyze, what's the score.

Testing checklist:

- ☐ HELO Greeting
- ☐ Reverse DNS
- ☐ DNSBL (RBL)
- ☐ SPF
- ☐ Domain Keys
- ☐ SPAMAssassin Content Checks
- ☐ BATV (Bounce Address Tag Validation)
- ☐ Greylisting
- ☐ URIBL

Demonstration
Mxtoolbox.com
Domain name registered

- mymxdemo.com
- mymxdemo.net

Both servers are running Ubuntu Linux and Postfix as my mail server software.

Both servers

- Let's encrypt for a certificate

References

http://www.emailarchivestaskforce.org/documents/email-security-standards-and-protocols/

http://www.openspf.org/Tools

http://www.openspf.org/SPF_Record_Syntax

http://exchange.sembee.info/network/openrelaytest.asp

https://emailmarketing.comm100.com/email-marketing-ebook/email-spam.aspx

https://space.dmarcian.com/videos-on-all-things-dmarc

How to configure Spam settings in Exchange 2019: https://docs.microsoft.com/en-us/exchange/antispam-and-antimalware/antispam-protection/configure-antispam-settings?view=exchserver-2019