

TECHNICAL REPORT



Passive Security Audit *for Email*

The Acme Corporation Ltd.



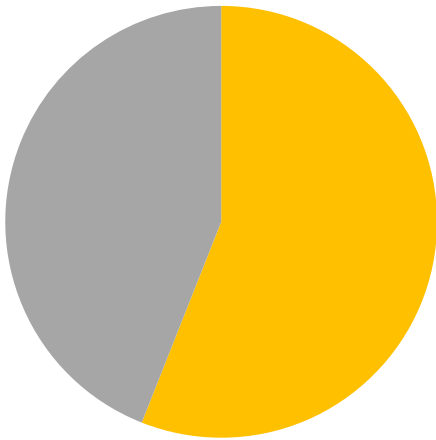
2020 September, 7

Gianandrea Daverio
Cybersecurity & Compliance Manager

M +39 342 9928782

E gianandrea.daverio@nposistemi.it

THEACMECORPORATION.ORG



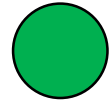
56%





















AVERAGE
SECURITY

TEST		
MX Connection Test	●	PASSED
Reverse DNS Test	●	FAILED
DNSBL Verification Test	●	PASSED
SPF Server Test	●	FAILED
SPF Client Test	●	NO INFO
Open Relay and Email Format Test	●	PASSED
SMTP Plain Text Authentication Test	●	PASSED
POP3 Connection Test	●	NO INFO
IMAP Connection Test	●	NO INFO
Domain Reputation Test	●	FAILED

MX Connection Test

Connected to at least one of your MX(s) on at least one of the ports.



HOSTNAME	SMTP (25)	SMTP (465)	SMTP (587)	AUTH (587)
ALT1.ASPMX.L.GOOGLE.COM				
ALT2.ASPMX.L.GOOGLE.COM				
ALT3.ASPMX.L.GOOGLE.COM				
ALT4.ASPMX.L.GOOGLE.COM				
ASPMX.L.GOOGLE.COM				

TEST DETAILS

WHY ARE WE TESTING IT

- 1) A mail exchange (MX or SMTP) server must make port 25 available externally to receive messages from other public SMTP servers.
- 2) Local users may also use port 25 to submit messages to be relayed (sent) to their recipients.

RISK FACTORS

If port 25 is blocked from external access on the MX server itself, the server cannot receive incoming messages (sending servers will never look for an alternate port). The port must at least be available via a proxy server or router.

WHAT ARE WE TESTING

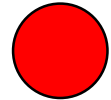
A secure mail server will force local users to authenticate prior to sending mail and will use either ports 465 or 587 for message encryption and submission.






Therefore we will test the following:

- 1) Attempt to connect to ports 25, 465 and 587 to verify that all three ports are open;
- 2) Test that authentication (i.e. an AUTH command) is additionally required on port 587

Reverse DNS Test

Your MX(s) IP(s) either do not resolve to name(s), or the name(s) that they resolve to do not resolve to the same MX(s) IP(s)



HOSTNAME	STATE
ALT1.ASPMX.L.GOOGLE.COM	
ALT2.ASPMX.L.GOOGLE.COM	
ALT3.ASPMX.L.GOOGLE.COM	
ALT4.ASPMX.L.GOOGLE.COM	
ASPMX.L.GOOGLE.COM	

TEST DETAILS

WHY ARE WE TESTING IT

To properly send and receive email, a valid domain should have a corresponding MX record in the DNS that contains 3 pieces of information: the domain name, the hostname (e.g. servername.domain.com) and the IP. Querying a hostname to resolve the address to its IP is called forward lookup. Reverse lookup is the opposite process: resolving the IP to its hostname.

RISK FACTORS

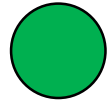
Many mail servers conduct reverse lookups to validate the authenticity of the sender domain. If the test fails, communication from the sending server can be blocked. Various reputation services may also give your system a lower score if the reverse record is missing.






WHAT ARE WE TESTING

- 1) A reverse lookup is attempted on your IP to see if it resolves to your hostname,
- 2) A forward lookup is attempted on your hostname to make sure it returns the matching IP from Test 1

DNS Black List Verification Test

Your MX(s) do not appear in the majority of RBLs



HOSTNAME	RBL
ALT1.ASPMX.L.GOOGLE.COM	
ALT2.ASPMX.L.GOOGLE.COM	
ALT3.ASPMX.L.GOOGLE.COM	
ALT4.ASPMX.L.GOOGLE.COM	
ASPMX.L.GOOGLE.COM	

TEST DETAILS

WHY ARE WE TESTING IT

A DNSBL (DNS-based Blacklist) publicly lists the IP addresses of computers and networks associated with sending spam and other malware.

RISK FACTORS

If any IP belonging to your network is blacklisted, mail servers that subscribe to DNSBLs will block communication from your server.

WHAT ARE WE TESTING

We will check the IPs associated with your MX against multiple DNSBL lists to verify whether or not any of your IPs are listed.

DNS Black List Verification Test

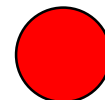
DNSBL	SERVER 1	SERVER 2	SERVER 3	SERVER 4	SERVER 5
bl.deadbeef.com	●	●	●	●	●
bl.emailbasura.org	●	●	●	●	●
bl.spamcop.net	●	●	●	●	●
blackholes.five-ten-sg.com	●	●	●	●	●
blacklist.woody.ch	●	●	●	●	●
bogons.cymru.com	●	●	●	●	●
cbl.abuseat.org	●	●	●	●	●
cdl.anti-spam.org.cn	●	●	●	●	●
combined.abuse.ch	●	●	●	●	●
combined.rbl.msrb1.net	●	●	●	●	●
db.wpbl.info	●	●	●	●	●
dnsbl-1.uceprotect.net	●	●	●	●	●
dnsbl-2.uceprotect.net	●	●	●	●	●
dnsbl-3.uceprotect.net	●	●	●	●	●
dnsbl.cyberlogic.net	●	●	●	●	●
dnsbl.inps.de	●	●	●	●	●
dnsbl.njabl.org	●	●	●	●	●
dnsbl.sorbs.net	●	●	●	●	●
drone.abuse.ch	●	●	●	●	●
duinv.aupads.org	●	●	●	●	●
dul.dnsbl.sorbs.net	●	●	●	●	●
dul.ru	●	●	●	●	●
dyna.spamrats.com	●	●	●	●	●
dynip.rothen.com	●	●	●	●	●
http.dnsbl.sorbs.net	●	●	●	●	●
images.rbl.msrb1.net	●	●	●	●	●
ips.backscatterer.org	●	●	●	●	●
ix.dnsbl.manitu.net	●	●	●	●	●
korea.services.net	●	●	●	●	●
misc.dnsbl.sorbs.net	●	●	●	●	●
noptr.spamrats.com	●	●	●	●	●
ohps.dnsbl.net.au	●	●	●	●	●
omrs.dnsbl.net.au	●	●	●	●	●
orvedb.aupads.org	●	●	●	●	●
osps.dnsbl.net.au	●	●	●	●	●
osrs.dnsbl.net.au	●	●	●	●	●
owfs.dnsbl.net.au	●	●	●	●	●
owps.dnsbl.net.au	●	●	●	●	●

DNS Black List Verification Test

DNSBL	SERVER 1	SERVER 2	SERVER 3	SERVER 4	SERVER 5
pbl.spamhaus.org	●	●	●	●	●
phishing.rbl.msrbl.net	●	●	●	●	●
probes.dnsbl.net.au	●	●	●	●	●
proxy.bl.gweep.ca	●	●	●	●	●
proxy.block.transip.nl	●	●	●	●	●
psbl.surriel.com	●	●	●	●	●
rbl.interserver.net	●	●	●	●	●
rdts.dnsbl.net.au	●	●	●	●	●
relays.bl.gweep.ca	●	●	●	●	●
relays.bl.kundenserver.de	●	●	●	●	●
relays.nether.net	●	●	●	●	●
residential.block.transip.nl	●	●	●	●	●
ricn.dnsbl.net.au	●	●	●	●	●
rmst.dnsbl.net.au	●	●	●	●	●
sbl.spamhaus.org	●	●	●	●	●
short.rbl.jp	●	●	●	●	●
smtp.dnsbl.sorbs.net	●	●	●	●	●
socks.dnsbl.sorbs.net	●	●	●	●	●
spam.abuse.ch	●	●	●	●	●
spam.rbl.msrbl.net	●	●	●	●	●
spam.spamrats.com	●	●	●	●	●
spamlist.or.kr	●	●	●	●	●
spamrbl.imp.ch	●	●	●	●	●
t3direct.dnsbl.net.au	●	●	●	●	●
tor.dnsbl.sectoor.de	●	●	●	●	●
torservers.tor.dnsbl.sectoor.de	●	●	●	●	●
ubl.lashback.com	●	●	●	●	●
ubl.unsubscore.com	●	●	●	●	●
virbl.bit.nl	●	●	●	●	●
virus.rbl.jp	●	●	●	●	●
virus.rbl.msrbl.net	●	●	●	●	●
web.dnsbl.sorbs.net	●	●	●	●	●
wormrbl.imp.ch	●	●	●	●	●
xbl.spamhaus.org	●	●	●	●	●
zombie.dnsbl.sorbs.net	●	●	●	●	●
zen.spamhaus.org	●	●	●	●	●
reputation.vircom.com	●	●	●	●	●
b.barracudacentral.org	●	●	●	●	●

SPF Server Test

Your SPF record has an invalid syntax or is non existent. Note that this test only checks for the syntax validity.



HOSTNAME

STATE

THEACMECORPORATION.ORG



TEST DETAILS

WHY ARE WE TESTING IT

This test examines whether or not you validate your local sender addresses. A common spam-sending practice involves spoofing (forging) the email address used in the FROM field. Sender Policy Framework (SPF) is a method used to prevent this type of spoofing: you create the SPF record on your DNS server to specify and limit which host addresses are allowed to send email using your domain name.

RISK FACTORS

Today, nearly all abusive e-mail messages carry fake sender addresses. The victims whose addresses are being abused often suffer from the consequences, because their reputation gets diminished and they have to disclaim liability for the abuse, or waste their time sorting out misdirected bounce messages

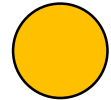
WHAT ARE WE TESTING






This test and the score are based on the following two criteria:

- 1) Whether or not your domain has a corresponding SPF record in the DNS
- 2) The syntax of the record.

SPF Client Test

Could not conclusively decide if you are enforcing an SPF connection test as some servers tag SPF violators instead of rejecting them at a connection level.



HOSTNAME	STATE
ALT1.ASPMX.L.GOOGLE.COM	
ALT2.ASPMX.L.GOOGLE.COM	
ALT3.ASPMX.L.GOOGLE.COM	
ALT4.ASPMX.L.GOOGLE.COM	
ASPMX.L.GOOGLE.COM	

TEST DETAILS

WHY ARE WE TESTING IT

This test examines what happens when a message arrives at the receiving server's end:

- 1) Will it check the sending server's domain for the existence of the SPF record?
- 2) Will it apply the rules as specified, e.g. block the connection (called a hard fail) or allow the connection (a soft fail)?

RISK FACTORS

If your server does not support SPF verification, the resulting problems can be twofold:

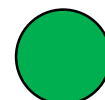
- 1) You risk accepting and having to process greater amounts of spam, putting increased pressure on your system resources and a greater number of invalid delivery failures and bounces, known as backscatter.






WHAT ARE WE TESTING

This test will verify whether or not your server supports SPF lookup and connection rejection. The test is done using an EHLO and MAIL FROM from a known domain whose SPF record is set up to reject any connection not originating from its mail servers. We connect to your server from a different domain than the aforementioned one and spoof the return path. A rejected connection will result in a Pass.

Open Relay & Email Format Test

More than half the open relay tests passed



HOSTNAME	STATE
ALT1.ASPMX.L.GOOGLE.COM	
ALT2.ASPMX.L.GOOGLE.COM	
ALT3.ASPMX.L.GOOGLE.COM	
ALT4.ASPMX.L.GOOGLE.COM	
ASPMX.L.GOOGLE.COM	

TEST DETAILS

WHY ARE WE TESTING IT

An open relay allows anyone to send email through it. This used to be the norm in the old days but spammers reroute their mail through these open relays to avoid detection.

RISK FACTORS

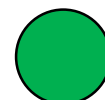
If the server allows messages to be sent to non-local addresses (by unauthenticated senders or non trusted IPs), it is considered an open relay. The server can therefore be exploited by spammers and consequently get blacklisted.











WHAT ARE WE TESTING

The server is tested using various combinations of MAIL FROM and RCPT TO addresses, none of which should be considered valid on your system. Various invalid address formats (e.g. the % hack) are also tried.

SMTP Plain Text Authentication Test

Your MX does not supports plain text AUTH



HOSTNAME	SMTP	SMTP SSL
ALT1.ASPMX.L.GOOGLE.COM		
ALT2.ASPMX.L.GOOGLE.COM		
ALT3.ASPMX.L.GOOGLE.COM		
ALT4.ASPMX.L.GOOGLE.COM		
ASPMX.L.GOOGLE.COM		

TEST DETAILS

WHY ARE WE TESTING IT

A mail exchange server is more vulnerable to abuse if the system is not configured to a) authenticate and verify local users before allowing them to submit messages to the SMTP server, and b) to encrypt the login criteria using a Secure Socket Layer (SSL) connection between the mail client and the server.

RISK FACTORS

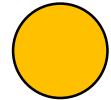
Spammers can potentially hack users' accounts by collecting passwords that are transmitted to the server in clear text via PLAIN or AUTH LOGIN mechanisms.











WHAT ARE WE TESTING

This test attempts to connect to the mail server on ports 25 and 465. For each connection it checks the list of available authentication (AUTH) methods. The server will receive the lowest score if PLAIN or AUTH LOGIN are supported on port 25. The highest score is awarded if SMTP SSL is enabled, and the PLAIN and AUTH LOGIN mechanisms are not available on port 25. Note that if AUTH is not supported, your MX passes the test as plain text passwords cannot be sniffed.

POP3 Connection Test

Could not connect to a POP3/POP3s server on your MX



HOSTNAME	POP3	POP3 SSL
ALT1.ASPMX.L.GOOGLE.COM		
ALT2.ASPMX.L.GOOGLE.COM		
ALT3.ASPMX.L.GOOGLE.COM		
ALT4.ASPMX.L.GOOGLE.COM		
ASPMX.L.GOOGLE.COM		

TEST DETAILS

WHY ARE WE TESTING IT

The POP3 connection natively downloads messages from the server and stores them on the mail client. The standard configuration uses port 110, but messages are transferred in plain text. The more secure method is to use an encrypted transmission connection (POP3s) on port 995, to protect the data while in transit.

RISK FACTORS

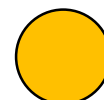
If the POP3 connection uses the standard port 110, the connection is not secure and can be breached, leading to a potential loss of messages and privacy.

WHAT ARE WE TESTING

We will check whether the POP3 Service responds on port 995 and 110 on the mail exchange server: 1) If port 995 is found, you are using a secure POP3s connection and will be awarded full marks; 2) If port 110 is found, this indicates that the plain text version of POP3 is visible from outside your network and marks will be deducted

IMAP Connection Test

Could not connect to your IMAP ports and thus cannot conclude anything about this test.



HOSTNAME	IMAP	IMAP Cleartext	IMAP SSL
ALT1.ASPMX.L.GOOGLE.COM	●	●	●
ALT2.ASPMX.L.GOOGLE.COM	●	●	●
ALT3.ASPMX.L.GOOGLE.COM	●	●	●
ALT4.ASPMX.L.GOOGLE.COM	●	●	●
ASPMX.L.GOOGLE.COM	●	●	●

TEST DETAILS

WHY ARE WE TESTING IT

IMAP differs from POP3 in that messages remain stored on the server; allowing for access from multiple mail clients (e.g. Outlook and webmail clients like Gmail). The standard, non-secure port for IMAP connections is 143. The secure, encrypted port is 993.

RISK FACTORS

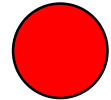
IMAP natively supports encrypted login mechanisms, but this security can be bypassed if plain text login on port 143 is used. Message content is therefore vulnerable to exposure and loss of privacy.





















WHAT ARE WE TESTING

We will check whether the IMAP service responds on port 993 or 143 on the mail exchange server. If the ports are available, the IMAP server's capabilities are examined: If AUTH=login or AUTH=plain are supported on port 143, then the IMAP server allows for plain text login and points are deducted. The highest score goes to servers that have ports 143 and 993 enabled and require an encrypted login (e.g., neither AUTH=login nor AUTH=plain are supported on 143)

Email Reputation Test

Could not connect to your IMAP ports and thus cannot conclude anything about this test.



IP Address Information				Domain/IP			Overall IP		
IP Address	ISP	ISP Domain	Ctry	Rep.	Good	Bad	Rep.	Good	Bad
155.231.210.253	NHSMail	hscic.gov.	GB		82%	18%		3%	97%
155.231.210.221	NHSMail	hscic.gov.	GB		76%	24%		3%	97%
51.163.158.103	Equinix	equinix.co	DE		93%	7%		98%	2%
62.140.7.103	E-Shelter Servi	e-shelter.	DE		95%	5%		100%	0%
51.163.158.237	Equinix	equinix.co	DE		100%	0%		100%	0%
62.140.7.237	E-Shelter Servi	e-shelter.	DE		100%	0%		100%	0%
104.47.59.177	Microsoft Corpo	microsoft.	US		50%	50%		68%	32%
104.47.46.53	Microsoft Corpo	microsoft.	US		100%	0%		62%	38%
94.75.244.176	LeaseWeb Nether	leaseweb.c	NL		0%	100%		70%	30%
104.47.36.51	Microsoft Corpo	microsoft.	US		100%	0%		65%	35%

TEST DETAILS

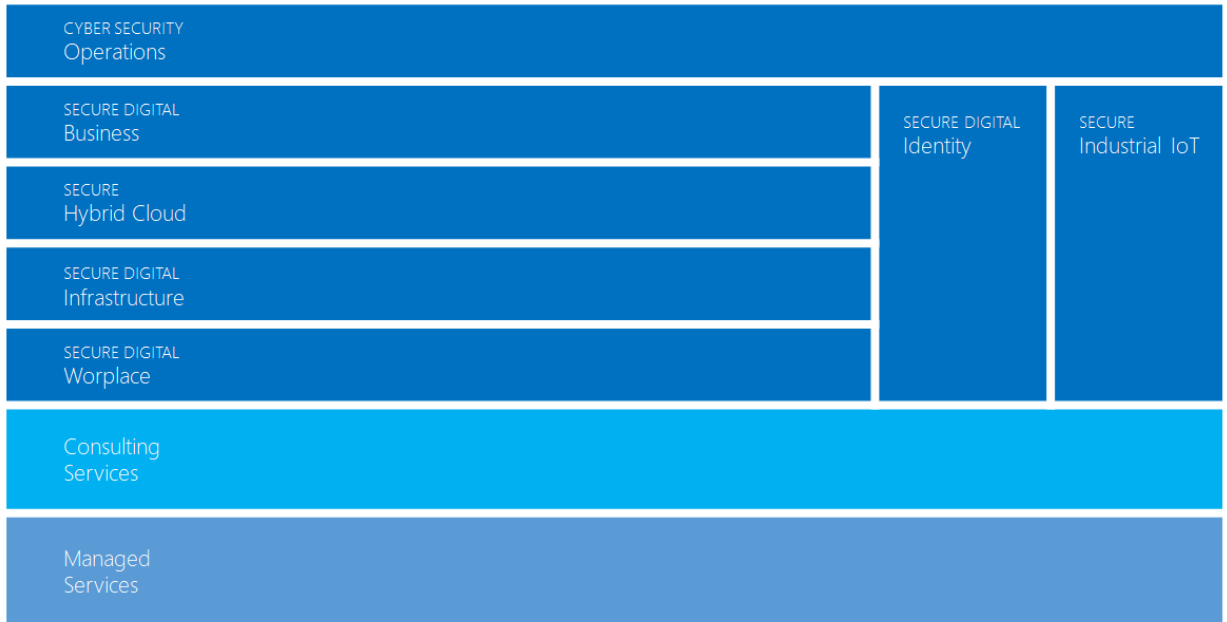
WHY ARE WE TESTING IT

Domain Reputation examines not only the IP reputation of a sender, but also the domain and sender information from that IP address. A domain can receive a reputation independent of the behavior of the IP address from which it originates, and independent from other domains originating from the same IP address.

For example, if joe@example.com sends email from the same server and same IP address as mary@example2.com, the behavior of those two domains will be tracked separately for that IP address. Subsequent mail sent from the same IP address from example.com will be compared to the history for example.com only and will not be affected by behavior from example2.com. If there is insufficient observed data for a domain, the domain reputation will be averaged with the overall IP reputation.

Note that not all of these IP addresses may be recognized as your servers, as the list also includes legitimate users sending from home ISPs or remote sites, and also spammers spoofing your domain from arbitrary locations.

Cybersecurity portfolio



Email Security offering



NPO SISTEMI S.R.L.

Viale Martesana, 12 20090 Vimodrone (MI)

Telefono: +39 02 925961 - Fax: +39 02 92590092

Sede Legale: Via Vittor Pisani, 6 - 20124 Milano (MI)

P.IVA e C.F. 08820850967 - Cap.Soc. € 2.100.284,00 i.v.

Filiale di Torino

Lungo Dora Colletta 81 10153 Torino

Tel. +39 011 19701225

Filiale di Roma

Via Mario Bianchini, 15 00142 Roma

Tel. +39 06 837881.1

Agenzia di Padova

Via Medoaco 2 (via Po) 35135 Padova

Tel. +39 049 865 0862