ERP-SEC
HARMONIZING BUSINESS AND SECURITY

You’ve got mail

Owning an SAP running business via email

Agenda

- Introduction
- State of SAP security
- Mail & SAP
- Vulnerabilities
- Solutions

ERP-SEC
HARMONIZING BUSINESS AND SECURITY

Introduction

- Company specialised in securing SAP systems and infrastructures
- SAP Security consulting
- Regular presenters on SAP Security in Security conferences
- Research: In worldwide top 5 for found SAP Security vulnerabilities
- Developer Protect4S - Security Analyser for SAP™
- SAP Development Partner
- Our mission is to raise the security of mission–critical SAP platforms with minimal impact on day–to–day business.

Fred van de Langenberg

Robin Vleeschhouwer

Joris van de Vis

SAP Partner
BIZEC BUSINESS SECURITY
SAP® Certified Powered by SAP NetWeaver®
VNSG

State of SAP Security

- SAP platform security at customer side used to be really bad
- But nowadays there is more awareness of customers to work on this
- From awareness to action still not the default
- SAP has done a lot to improve security
- Action now really needed from customers
- Customers that actively work on SAP security are mainly large customers
- Big group of customers stays behind, especially ones outside fortune 2000
- In the light of upcoming GDPR this might impact your organization
- In >90% of our conducted SAP Security assessments we found even the most basic vulnerabilities like SAP default accounts.

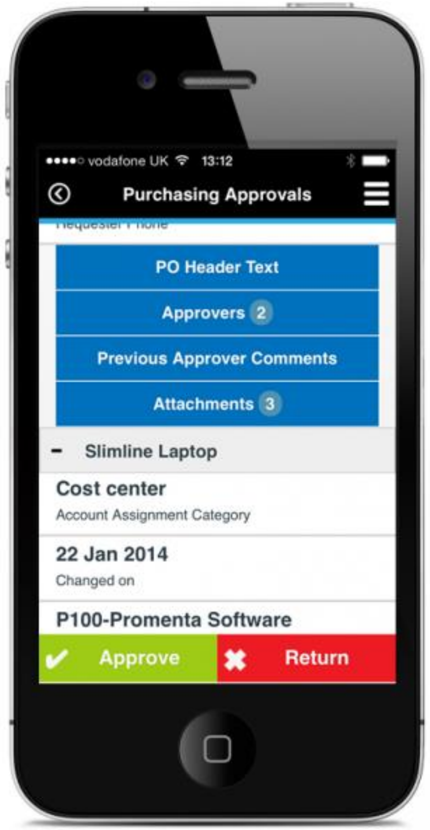
So, SAP and email processing…

- Many topics in SAP security have been discussed previously
- This is a new area in terms of SAP security
- Rather common scenario for SAP running organizations
- Unauthenticated as we've seen typically deployed
- So a logical choice to dig deeper…
- Still work in Progress

SAP inbound email scenarios

There are many business scenario’s that lean on inbound mail processing:

- Processing and approval of purchase orders
- Processing and approval of leave requests
- Processing and approval of expenses
- SRM shopping cart approvals
- Processing of inbound office documents
- Processing of digital invoices
- Processing of inbound interactive PDF’s
- Processing of CRM surveys
- Processing of Customer response messages in Support scenario’s
- And many, many more…



SAP Email configuration types

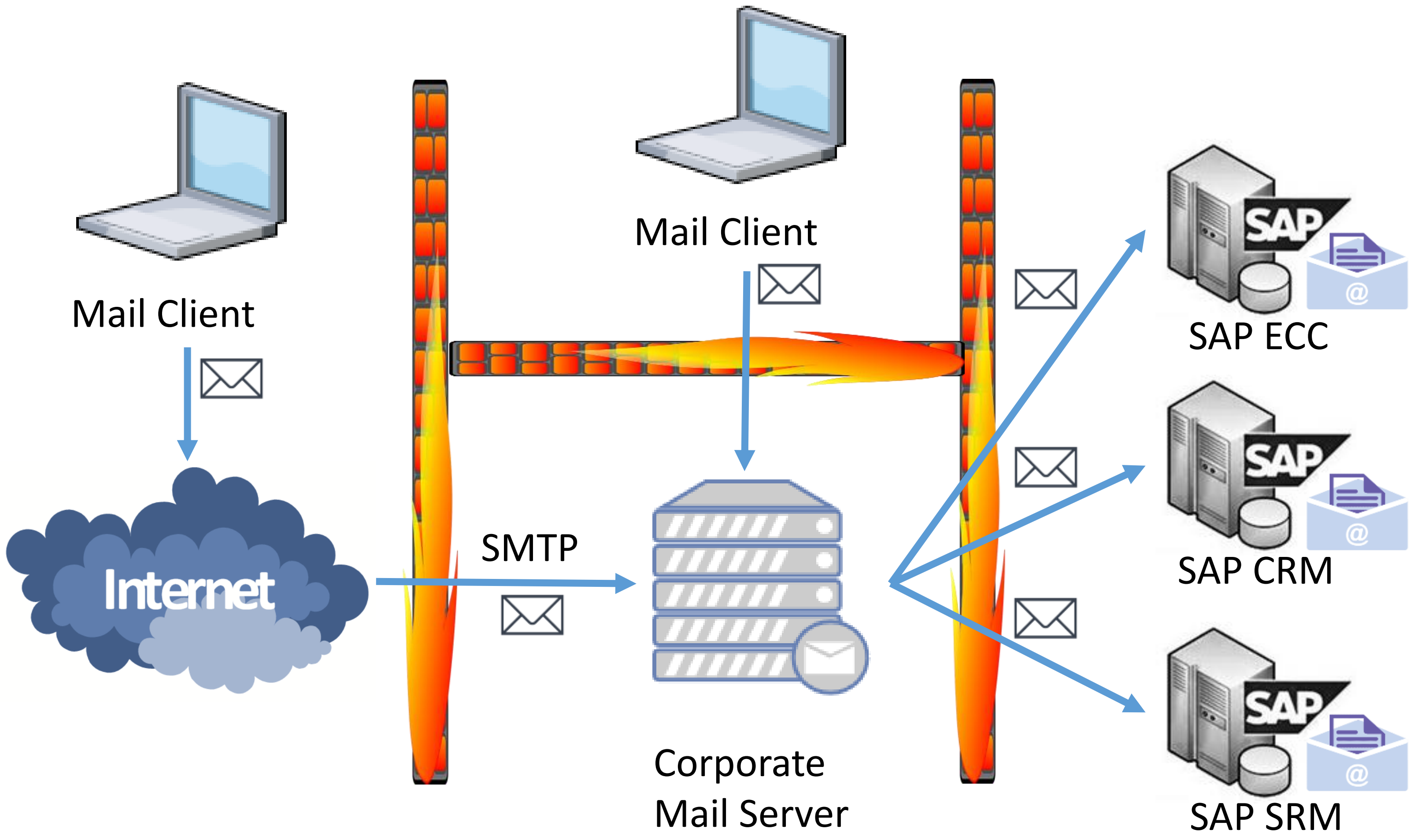
Almost all SAP products and types of systems allow the sending of emails.
This poses a security risk as well, but we focus here on receiving of emails into SAP.

Not every SAP customer has activated inbound email scenario's, but many do.
No exact numbers here, but a rough guess would be at least 50% of large SAP running companies do. Especially for workflow scenario's.

Type of system*	Supports outbound email	Supports inbound email
SAP ABAP	Yes	Yes
SAP JAVA	Yes	No
SAP HANA	Yes	No

* Some other products like SAP PI/PO might also allow inbound email via external adapters

SAP inbound mail architecture

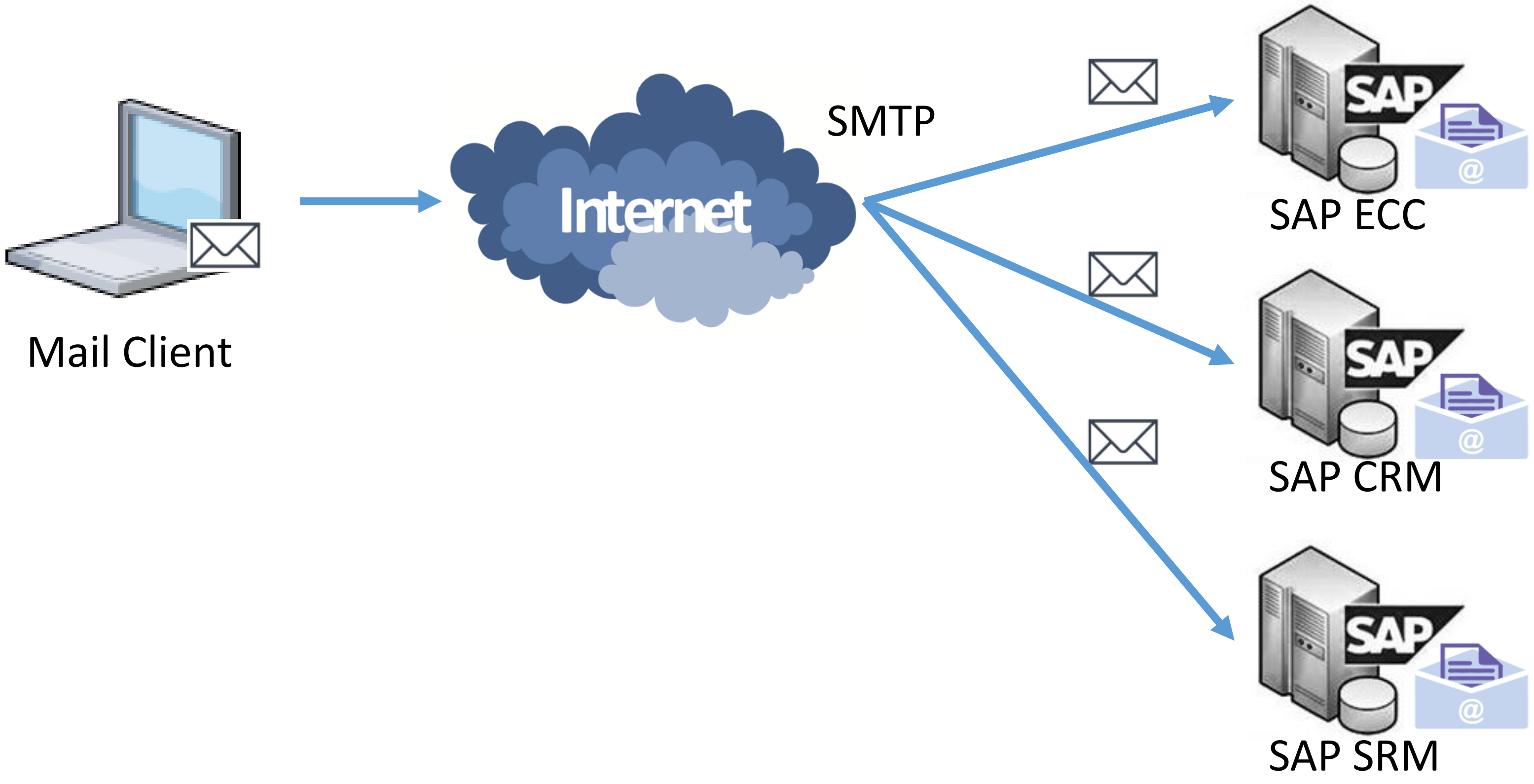


ERP-SEC
HARMONIZING BUSINESS AND SECURITY

SAP inbound mail architecture

But we have also seen this:

SAP SMTP node directly exposed to internet



SAP's ESMTP server

- Implemented in Internet Configuration Manager executable in the ABAP kernel
- Is an Extended SMTP server (hence the E).
- Has additional support features:
  - RFC 3461: SMTP Service Extension for Delivery Status Notifications (DSNs)
  - RFC 2920: SMTP Service Extension for Command Pipelining
- All other enhancements are not supported by SAP:
  - RFC 1652: SMTP Service Extension for 8bit-MIMEtransport
  - RFC 1845: SMTP Service Extension for Checkpoint/Restart
  - RFC 1870: SMTP Service Extension for Message Size Declaration
  - RFC 1985: SMTP Service Extension for Remote Message Queue Starting: - ETRN
  - RFC 2034: SMTP Service Extension for Returning Enhanced Error Codes
  - RFC 2487: SMTP Service Extension for Secure SMTP over TLS
  - RFC 2554: SMTP Service Extension for Authentication
  - RFC 3030: SMTP Service Extensions for Transmission of Large and Binary MIME Messages
  - RFC 3207: SMTP Service Extension for Secure SMTP over Transport Layer Security
- See SAP note 1098108 - SMTP plug-in: ESMTP enhancements

SAP inbound email processing

Requires some setup by your SAP basis team in the SAP Web Application Server.

Also your mail-team is needed to setup mail relaying to SAP.

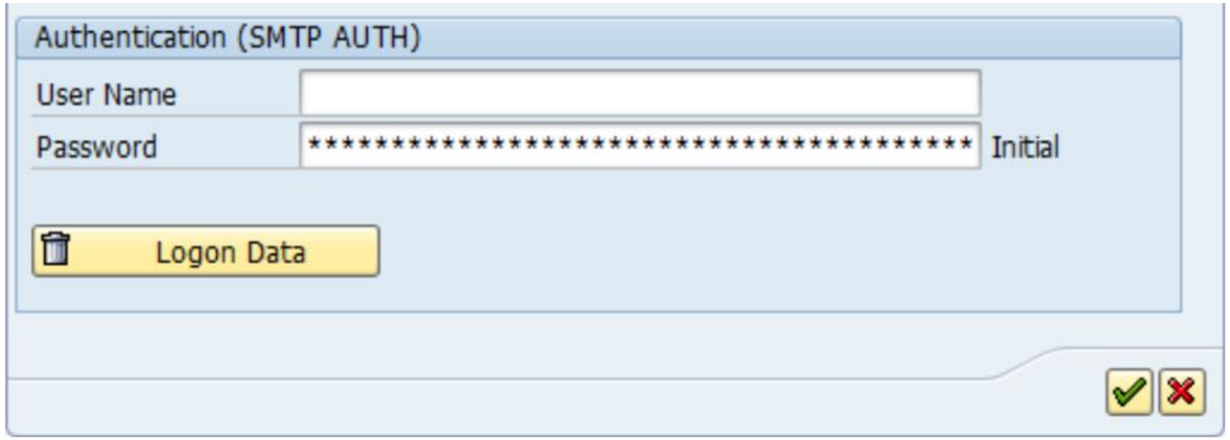
Some transactions in an SAP WAS involved in processing inbound mail:

SMICM	Activates the SMTP service on given port
SICF	Activates SAPConnect service. Contains SAP user for processing
SCOT	Domain name settings and detailed inbound and outbound rules. For example which users are allowed to send mail
SO50	The ABAP class that processes the incoming mails

To setup inbound email processing; Make sure to have followed
SAP note **455140 - Configuration of e-mail, fax, paging/SMS via SMTP**

SMTP authentication

- Only possible from **SAP Basis Release 7.31**
- See SAP note **1702632** - Authentication with user and password while sending mail through SAPconnect using SMTP
- Since recently SAP Support passwords longer than 20 characters (as of kernel 7.49 SP 111 – December 2016)
- See SAP note **2372893** - Longer passwords for SMTP authentication
- Configuration via transaction SCOT

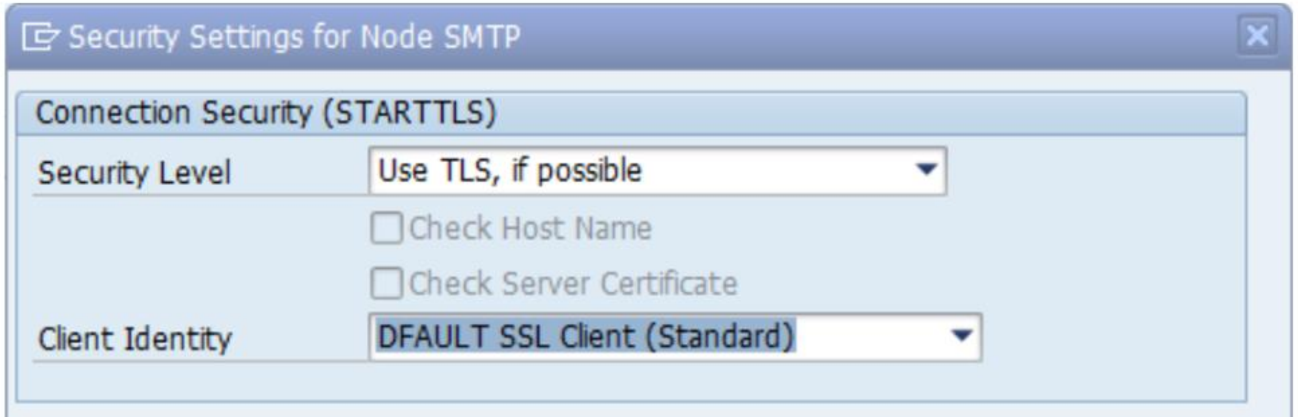


Authentication (SMTP AUTH)

User Name		
Password	**	Initial

SMTP encryption

- TLS is supported on communication layer
- S/MIME is supported for sending and receiving encrypted emails
- PGP is not supported
- Only possible from **SAP Basis Release 7.31**
- See SAP note **1747180** - SMTP via TLS and SMTP authentication
- See SAP note **1637415** – S/MIME integration in SAPconnect
- Configuration via transaction SCOT



Security Settings for Node SMTP

Connection Security (STARTTLS)

Security Level: Use TLS, if possible

□ Check Host Name

□ Check Server Certificate

Client Identity: DFAULT SSL Client (Standard)

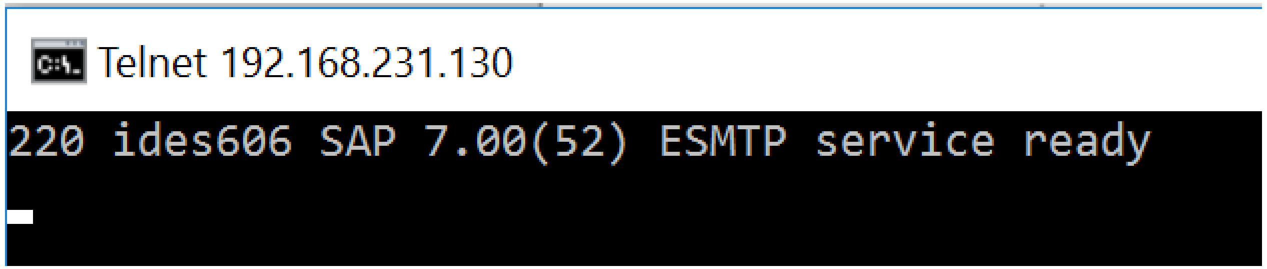
Vulnerabilities / Risks

- SAP SMTP Server information disclosure
- Denial Of Service
- Impersonating
- Open mail relaying
- SMB credential theft
- Influencing functional business processes

ALL UNAUTHENTICATED ;-)

SMTP server information disclosure

- SAP SMTP server by default greets you with vendor name and version number



Telnet 192.168.231.130

```
220 ides606 SAP 7.00(52) ESMTP service ready
```

DEMO

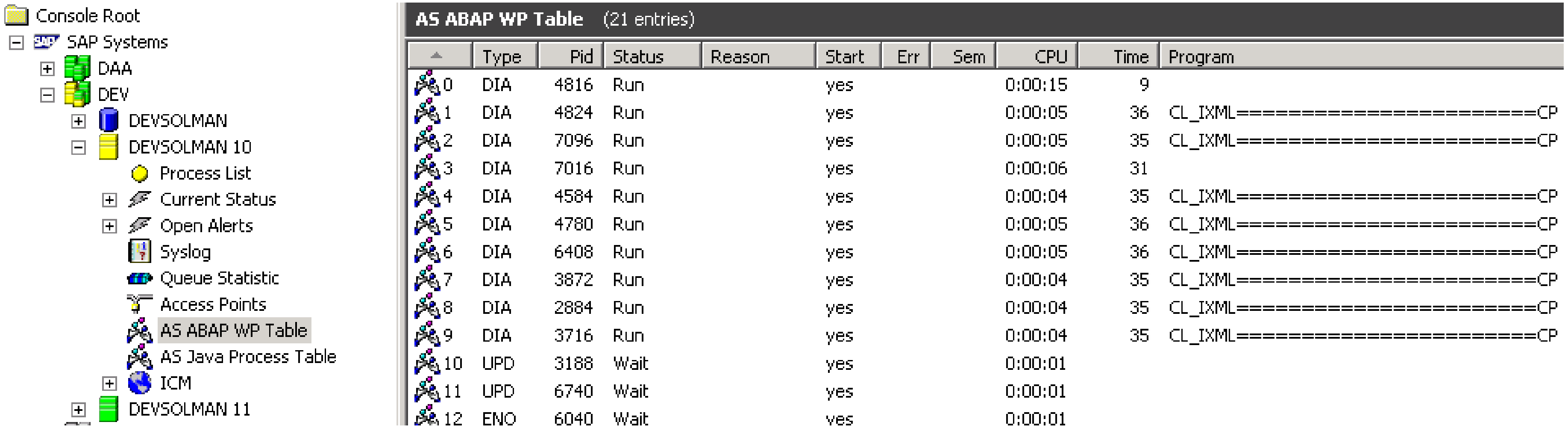
- Can be prevented with parameter ***icm/SMTP/show_server_header = FALSE***
- See note **2045861** - Hiding release information from the SMTP server banner
- 3 versions found in the wild

✓ SAP 6.20(50) ESMTP service ready
✓ SAP 7.00(52) ESMTP service ready
✓ SAP 8.04(53) ESMTP service ready

Denial of Service

- Possible in many ways, when fuzzing SMTP we easily found 5 ways
- Possible via internet
- Restrict direct access to SMTP port of ICM with firewall
- Use mail filtering for mass mails
- See SAP note 2308217 – Missing XML Validation vulnerability in Web-Survey

DEMO

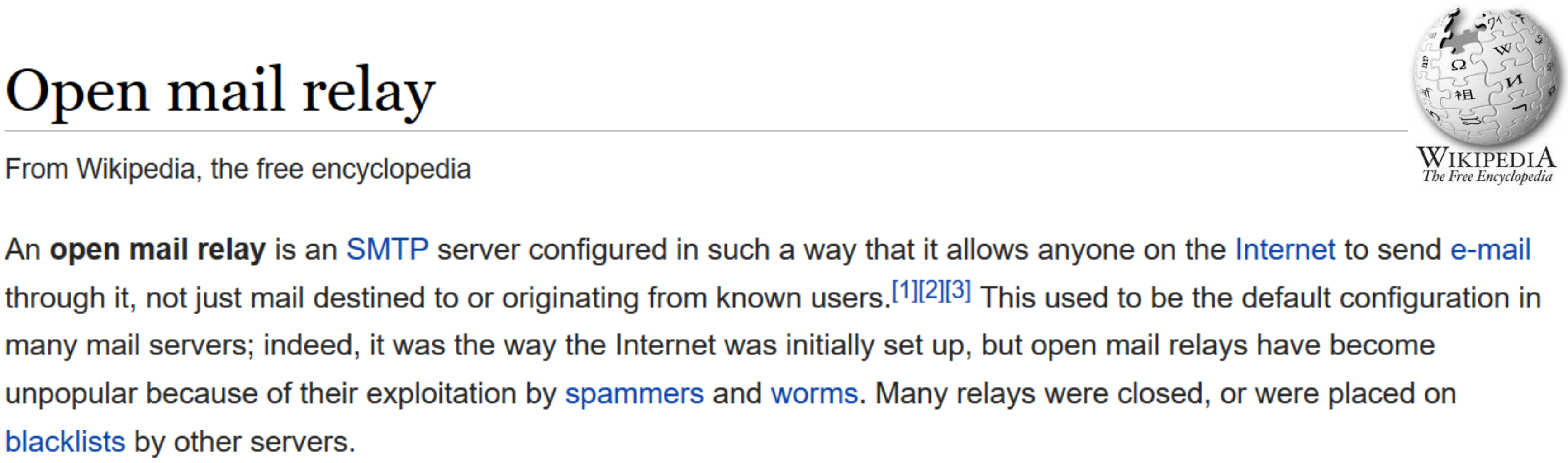


- Console Root
  - SAP Systems
    - DAA
    - DEV
      - DEVSOLMAN
      - DEVSOLMAN 10
        - Process List
        - Current Status
        - Open Alerts
        - Syslog
        - Queue Statistic
        - Access Points
        - AS ABAP WP Table
        - AS Java Process Table
        - ICM
      - DEVSOLMAN 11

AS ABAP WP Table (21 entries)

	Type	Pid	Status	Reason	Start	Err	Sem	CPU	Time	Program
0	DIA	4816	Run		yes			0:00:15	9	
1	DIA	4824	Run		yes			0:00:05	36	CL_IXML=======================CP
2	DIA	7096	Run		yes			0:00:05	35	CL_IXML=======================CP
3	DIA	7016	Run		yes			0:00:06	31	
4	DIA	4584	Run		yes			0:00:04	35	CL_IXML=======================CP
5	DIA	4780	Run		yes			0:00:05	36	CL_IXML=======================CP
6	DIA	6408	Run		yes			0:00:05	36	CL_IXML=======================CP
7	DIA	3872	Run		yes			0:00:04	35	CL_IXML=======================CP
8	DIA	2884	Run		yes			0:00:04	35	CL_IXML=======================CP
9	DIA	3716	Run		yes			0:00:04	35	CL_IXML=======================CP
10	UPD	3188	Wait		yes			0:00:01		
11	UPD	6740	Wait		yes			0:00:01		
12	ENQ	6040	Wait		yes			0:00:01		

Open mail relaying



Open mail relay

From Wikipedia, the free encyclopedia

An **open mail relay** is an SMTP server configured in such a way that it allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users.[1][2][3] This used to be the default configuration in many mail servers; indeed, it was the way the Internet was initially set up, but open mail relays have become unpopular because of their exploitation by spammers and worms. Many relays were closed, or were placed on blacklists by other servers.

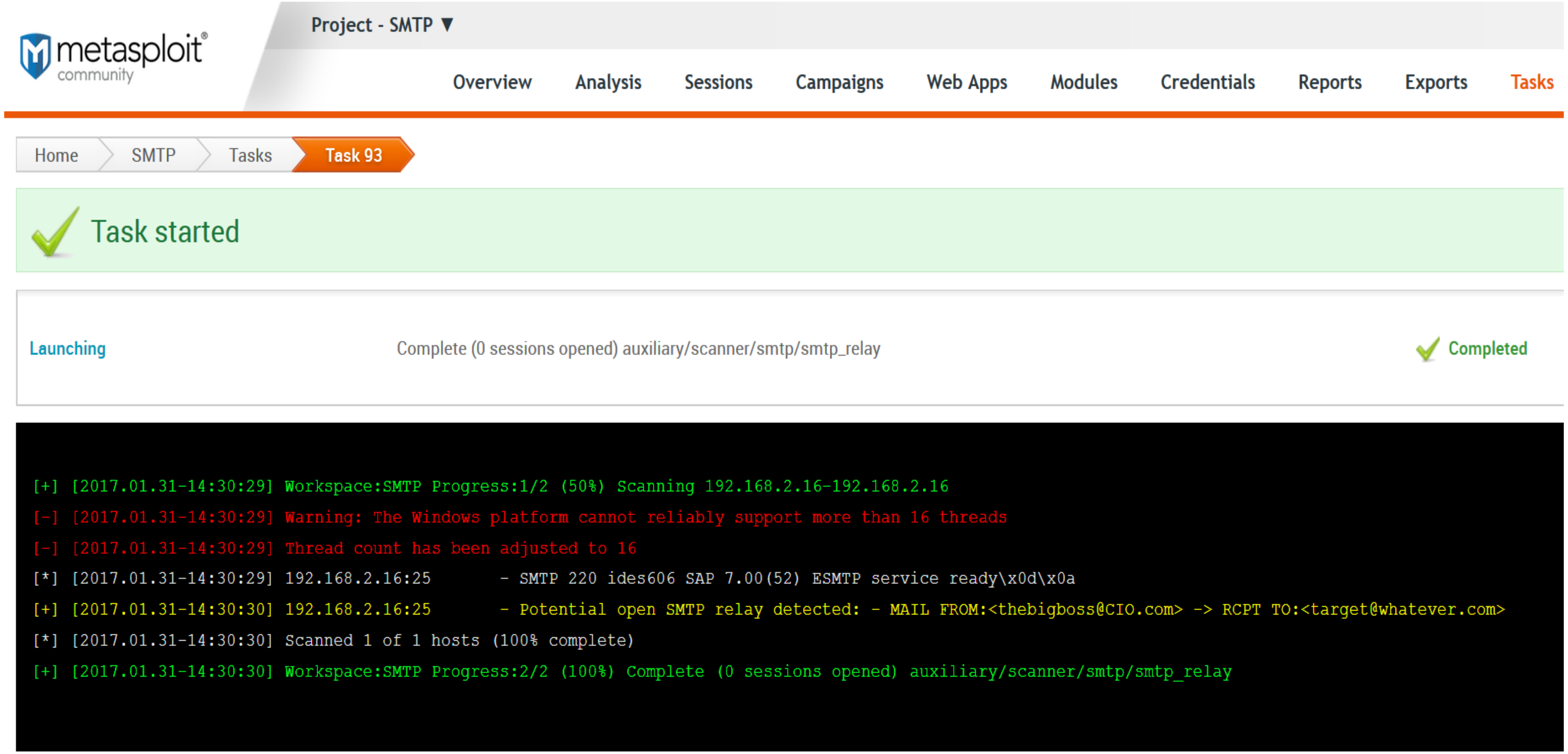
- Mail relaying is a security risk as it can be used to exhaust system resources by mass sending spam over your SMTP server or it can be used by spammers to hide themselves behind your IP-address
- Could get your corporate mail server blacklisted
- Is not really an SAP issue, but needs to be configured on your mail server
- See SAP note **1496168** - Relay problem while sending mails through SAPconnect
- Use SMTP authentication

Open mail relaying

Metasploit has a module to test your SAP SMTP node

But good old telnet will do as well, so simple; anyone can do it…

DEMO



✓ Task started

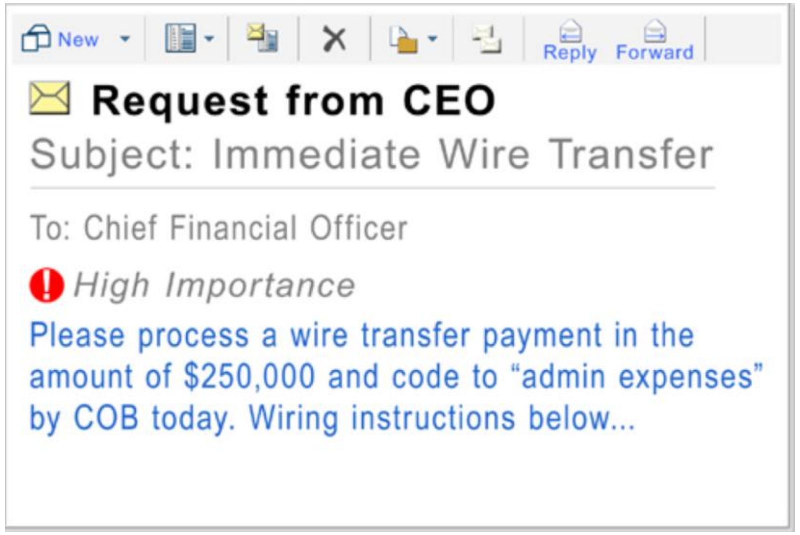
Launching | Complete (0 sessions opened) auxiliary/scanner/smtp/smtp_relay | ✓ Completed

```
[+] [2017.01.31-14:30:29] Workspace:SMTP Progress:1/2 (50%) Scanning 192.168.2.16-192.168.2.16
[-] [2017.01.31-14:30:29] Warning: The Windows platform cannot reliably support more than 16 threads
[-] [2017.01.31-14:30:29] Thread count has been adjusted to 16
[*] [2017.01.31-14:30:29] 192.168.2.16:25       - SMTP 220 ides606 SAP 7.00(52) ESMTP service ready\x0d\x0a
[+] [2017.01.31-14:30:30] 192.168.2.16:25       - Potential open SMTP relay detected: - MAIL FROM:<thebigboss@CIO.com> -> RCPT TO:<target@whatever.com>
[*] [2017.01.31-14:30:30] Scanned 1 of 1 hosts (100% complete)
[+] [2017.01.31-14:30:30] Workspace:SMTP Progress:2/2 (100%) Complete (0 sessions opened) auxiliary/scanner/smtp/smtp_relay
```

Impersonating

- No SAP specific issue, more a mail server configuration issue
- Impersonating is not a bug, but a SMTP ‘feature’
- Nevertheless prone to misuse and for example used for phishing attacks
- Facilitates crime like CEO fraud / the classic Nigerian scam, etc
- Prevention: Change your mail server setup to use for example SPF, DMARC, etc

  (no SAP setting involved here, mostly a ‘mail team’ activity)



Request from CEO

Subject: Immediate Wire Transfer

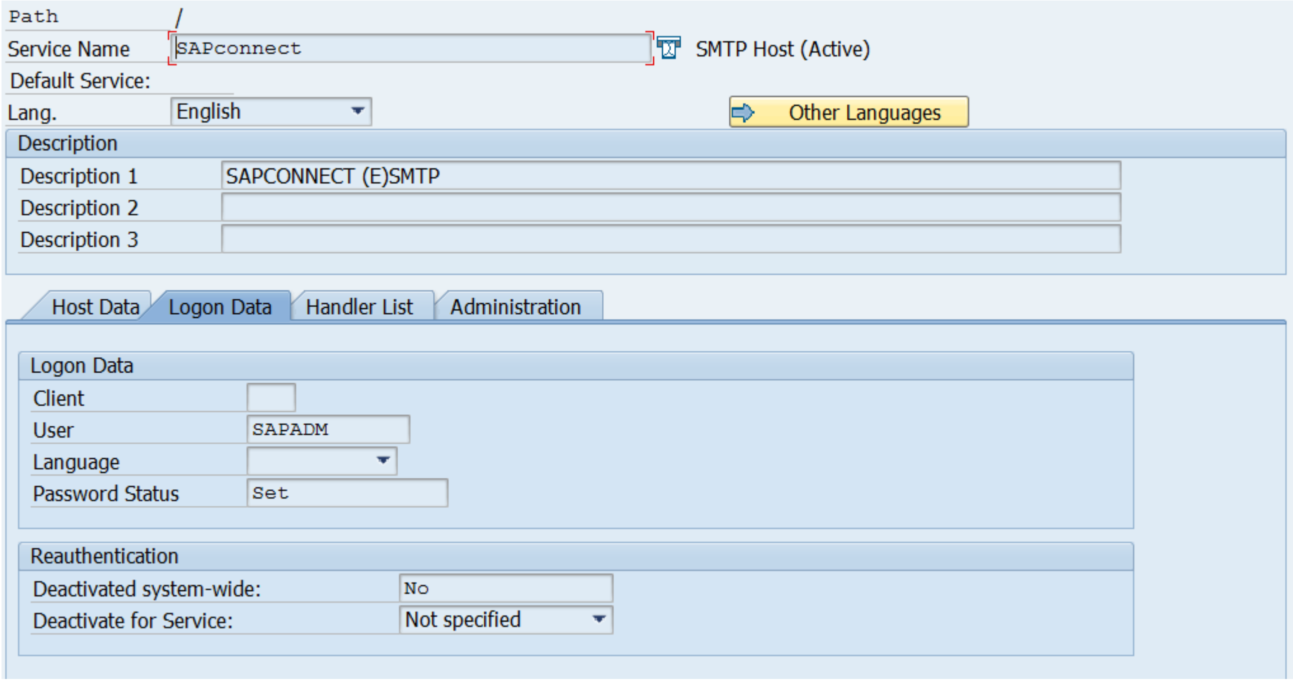
To: Chief Financial Officer

High Importance

Please process a wire transfer payment in the amount of $250,000 and code to “admin expenses” by COB today. Wiring instructions below...

Authorisations mail processing user

- The user in SAP that processes incoming mail often has SAP_ALL rights!
- Leaving no barrier between incoming mails and further business functions



Path /

Service Name SAPconnect SMTP Host (Active)

Default Service:

Lang. English

Description

Description 1 SAPCONNECT (E)SMTP

Description 2

Description 3

Logon Data

Client	
User	SAPADM
Language	
Password Status	Set

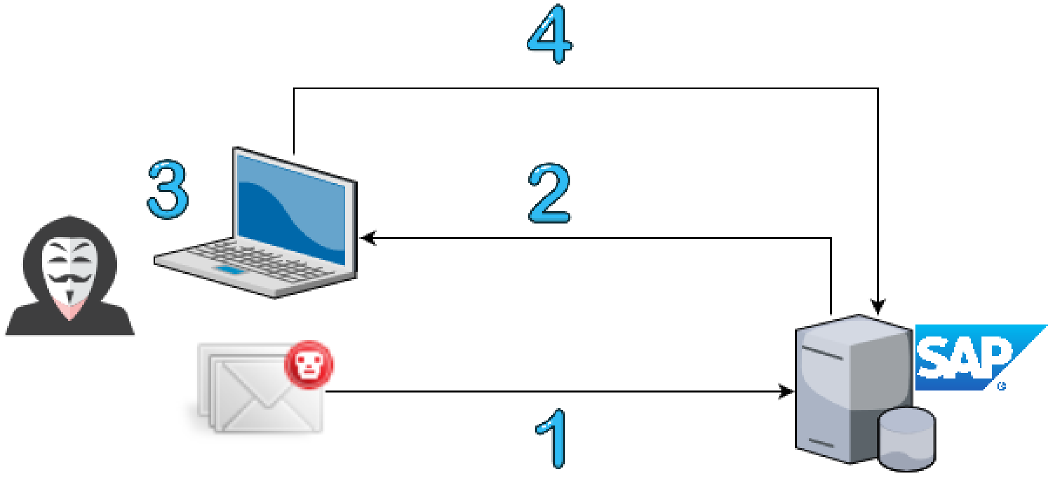
Reauthentication

Deactivated system-wide:	No
Deactivate for Service:	Not specified

- SAP recommends to use profile S_A.SCON profile, see SAP note 455140 - Configuration of e-mail, fax, paging/SMS via SMTP

SMB credential stealing

Send an email with specific XML attachment to SAP to retrieve the Password hash of the SAPService<SID> Windows Operating System user



1 Send email to SAP system (unauthenticated) with XML attachment pointing to own machine

2 SAP system running on Windows will process the mailattachment and try and connect over SMB

3 Use responder.py to capture NTLM hash and bruteforce offline via eg Hashcat (Or use SMB Relay to other machine)

4 Use credentials to connect to SAP system

Or just Relay the SMB credentials

SMB credential stealing

DEMO

- Prerequisites:
  - SO50 Inbound processing class: CL_UWS_FORM_RUNTIME_MAIL
  - Operating System must be Windows
- Works on all versions up to and inclusing SAP Netweaver 7.40 (7.50 protected by default by parameter ixml/dtd_restriction)
- To make things worse: SAPService<SID> in the wild is often added to Administrators group which makes exploitation way easier
- Retrieving SAPService<SID> password often means having the MASTER password
- This means breaking one password means breaking all of them
- Attack possible via internet, although SMB over internet often blocked in corporate firewall

SMB credential stealing

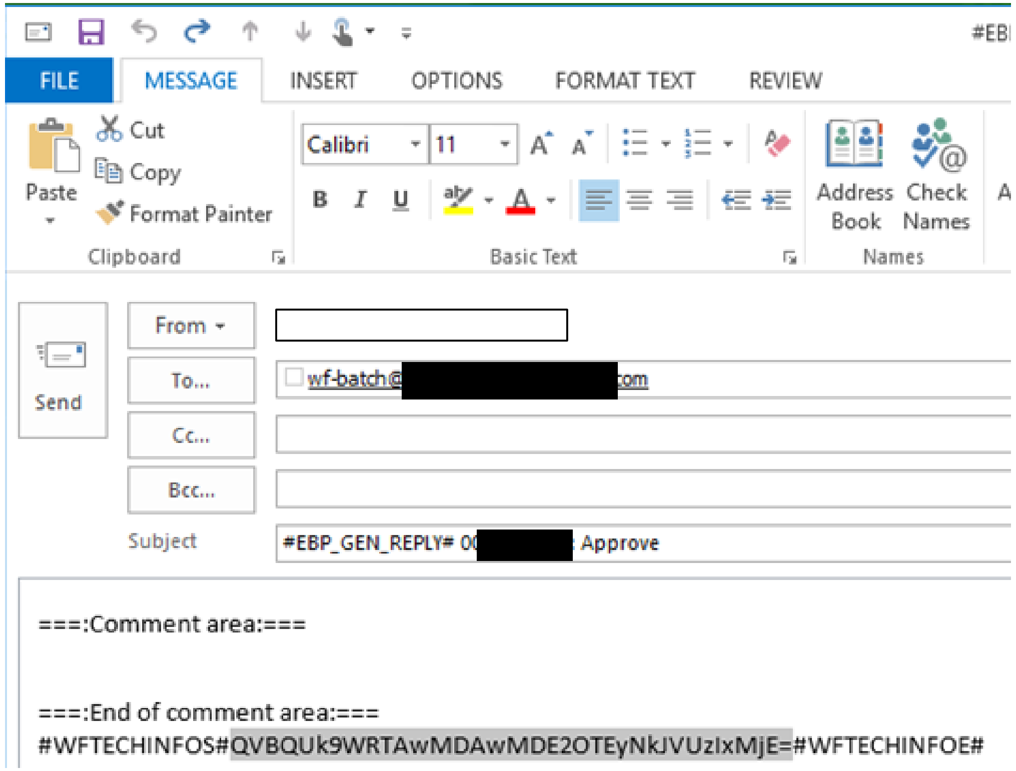
- Solution via SAP note **2308217** – Missing XML Validation vulnerability in Web-Survey (HIGH priority / CVSS 7.5 / 10)
- Block SMB ports 137,138,139,445 for outgoing traffic towards internet
- Set parameter ixml/dtd_restriction = expansion.
- See SAP note **1712860** – iXML: Protection against attacks via a DTD
- Do NOT add SAPService<SID> user to administrators group

Influencing business processes

- Creation of Masterdata
- Interfering with approval workflows, for example
  - order approvals
  - leave requests
  - expense approvals
  - SRM shopping Cart approvals
- Audit / compliancy workflows
- Attachments from external mails, like digital invoices, can be stored in SAP Content server. Often no virus scanning done
- Used email addresses can be easy to guess: For example
  - invoice@corp.com
  - purchase@corp.com
  - workflow@corp.com
  - approval@corp.com
  - orders@corp.com
  - Etc…

Influencing business processes

SRM shopping Cart approvals example:



To: wf-batch@[redacted]om

Subject: #EBP_GEN_REPLY# 00[redacted] Approve

===:Comment area:===

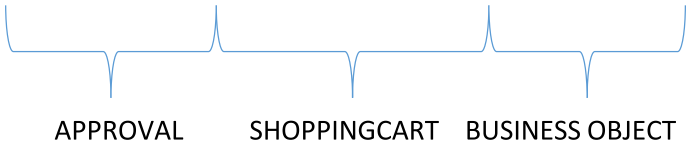
===:End of comment area:===
#WFTECHINFOS#QVBQUk9WRTAwMDAwMDE2OTEyNkJVUzIxMjE=#WFTECHINFOE#

BASE64:

QVBQUk9WRTAwMDAwMDE2OTEyNkJVUzIxMjE=

Plain text:

APPROVE000000169126BUS2121

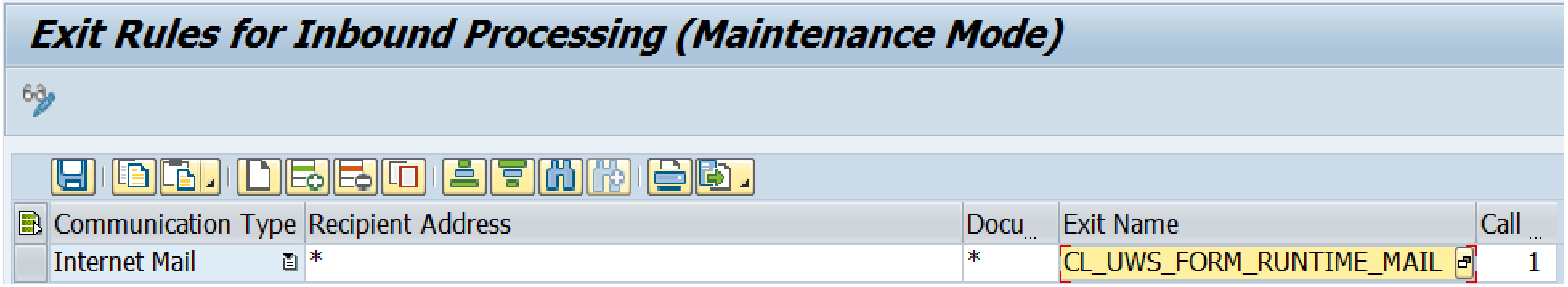

APPROVAL
SHOPPINGCART
BUSINESS OBJECT

Breaks Segregation of Duties / 4-eyes principle as the approval can be faked.

Influencing business processes

Prevention:

- Do not use easy guessable email addresses
- Implement additional checks in process to validate approval user is real
- Restrict the authorization of the processing SAP user in SICF
- Use the anti-virus scanning interface to scan email attachments
- Do not allow emails from ‘the world’ in SO50



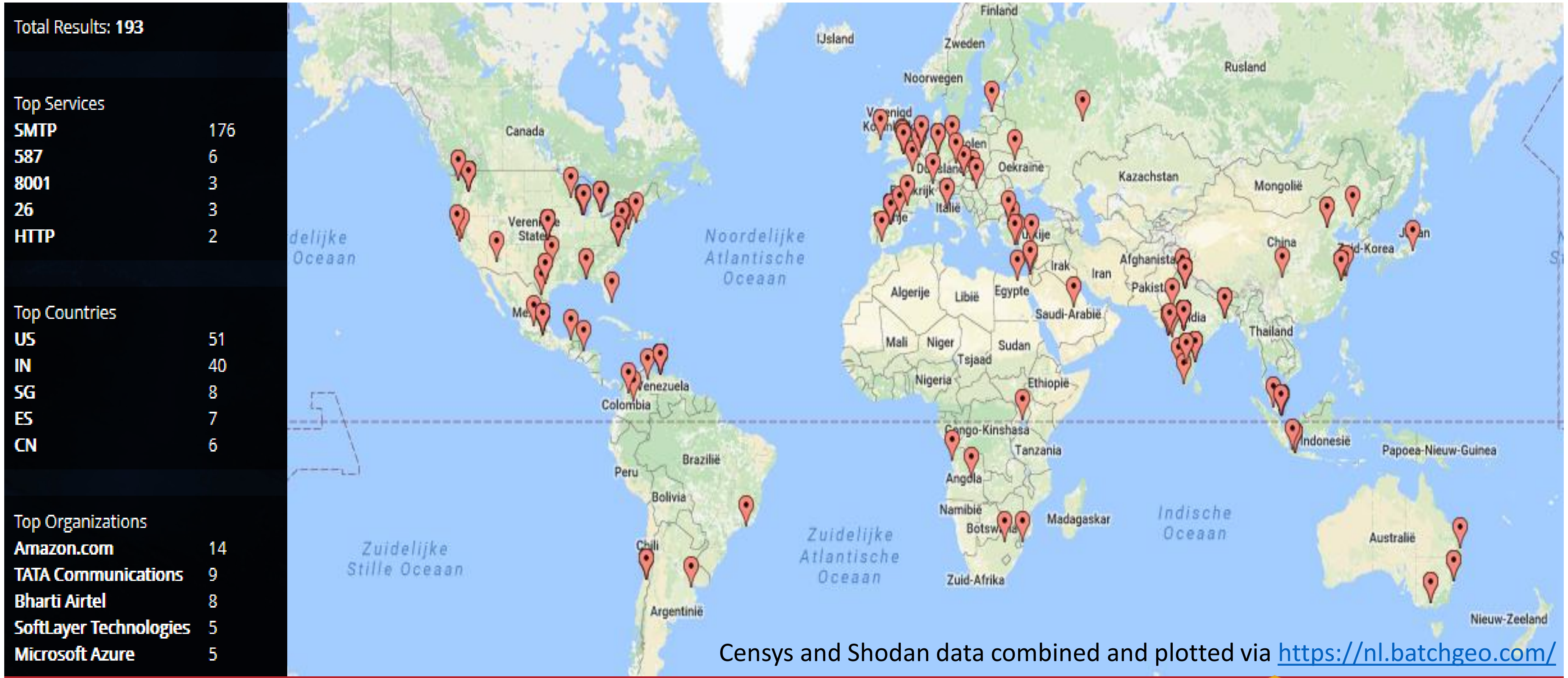
Exit Rules for Inbound Processing (Maintenance Mode)

Communication Type	Recipient Address	Docu...	Exit Name	Call ...
Internet Mail	*	*	CL_UWS_FORM_RUNTIME_MAIL	1

SAP SMTP internet presence

DEMO

~ 200 SAP ESMTP nodes found directly connected to the internet
Combined data from Censys.io / Shodan.io



Total Results: **193**

Top Services	
SMTP	176
587	6
8001	3
26	3
HTTP	2

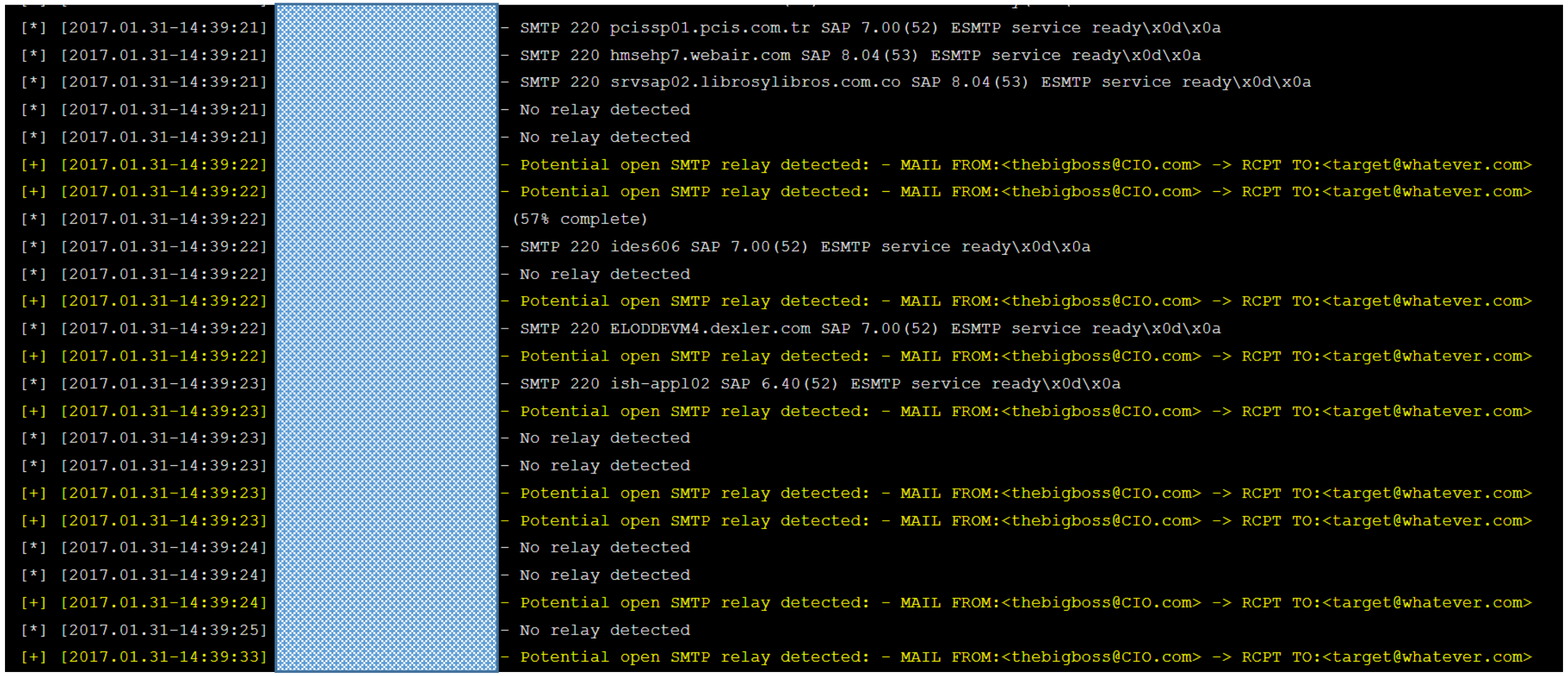
Top Countries	
US	51
IN	40
SG	8
ES	7
CN	6

Top Organizations	
Amazon.com	14
TATA Communications	9
Bharti Airtel	8
SoftLayer Technologies	5
Microsoft Azure	5

Censys and Shodan data combined and plotted via https://nl.batchgeo.com/

SAP SMTP internet presence

- SMTP relaying possible for 45% of SMTP nodes present on internet



```
[*] [2017.01.31-14:39:21] [redacted] - SMTP 220 pcissp01.pcis.com.tr SAP 7.00(52) ESMTP service ready\x0d\x0a
[*] [2017.01.31-14:39:21]            - SMTP 220 hmsehp7.webair.com SAP 8.04(53) ESMTP service ready\x0d\x0a
[*] [2017.01.31-14:39:21]            - SMTP 220 srvsap02.librosylibros.com.co SAP 8.04(53) ESMTP service ready\x0d\x0a
[*] [2017.01.31-14:39:21]            - No relay detected
[*] [2017.01.31-14:39:21]            - No relay detected
[+] [2017.01.31-14:39:22]            - Potential open SMTP relay detected: - MAIL FROM:<thebigboss@CIO.com> -> RCPT TO:<target@whatever.com>
[+] [2017.01.31-14:39:22]            - Potential open SMTP relay detected: - MAIL FROM:<thebigboss@CIO.com> -> RCPT TO:<target@whatever.com>
[*] [2017.01.31-14:39:22]             (57% complete)
[*] [2017.01.31-14:39:22]            - SMTP 220 ides606 SAP 7.00(52) ESMTP service ready\x0d\x0a
[*] [2017.01.31-14:39:22]            - No relay detected
[+] [2017.01.31-14:39:22]            - Potential open SMTP relay detected: - MAIL FROM:<thebigboss@CIO.com> -> RCPT TO:<target@whatever.com>
[*] [2017.01.31-14:39:22]            - SMTP 220 ELODDEVM4.dexler.com SAP 7.00(52) ESMTP service ready\x0d\x0a
[+] [2017.01.31-14:39:22]            - Potential open SMTP relay detected: - MAIL FROM:<thebigboss@CIO.com> -> RCPT TO:<target@whatever.com>
[*] [2017.01.31-14:39:23]            - SMTP 220 ish-appl02 SAP 6.40(52) ESMTP service ready\x0d\x0a
[+] [2017.01.31-14:39:23]            - Potential open SMTP relay detected: - MAIL FROM:<thebigboss@CIO.com> -> RCPT TO:<target@whatever.com>
[*] [2017.01.31-14:39:23]            - No relay detected
[*] [2017.01.31-14:39:23]            - No relay detected
[+] [2017.01.31-14:39:23]            - Potential open SMTP relay detected: - MAIL FROM:<thebigboss@CIO.com> -> RCPT TO:<target@whatever.com>
[+] [2017.01.31-14:39:23]            - Potential open SMTP relay detected: - MAIL FROM:<thebigboss@CIO.com> -> RCPT TO:<target@whatever.com>
[*] [2017.01.31-14:39:24]            - No relay detected
[*] [2017.01.31-14:39:24]            - No relay detected
[+] [2017.01.31-14:39:24]            - Potential open SMTP relay detected: - MAIL FROM:<thebigboss@CIO.com> -> RCPT TO:<target@whatever.com>
[*] [2017.01.31-14:39:25]            - No relay detected
[+] [2017.01.31-14:39:33]            - Potential open SMTP relay detected: - MAIL FROM:<thebigboss@CIO.com> -> RCPT TO:<target@whatever.com>
```

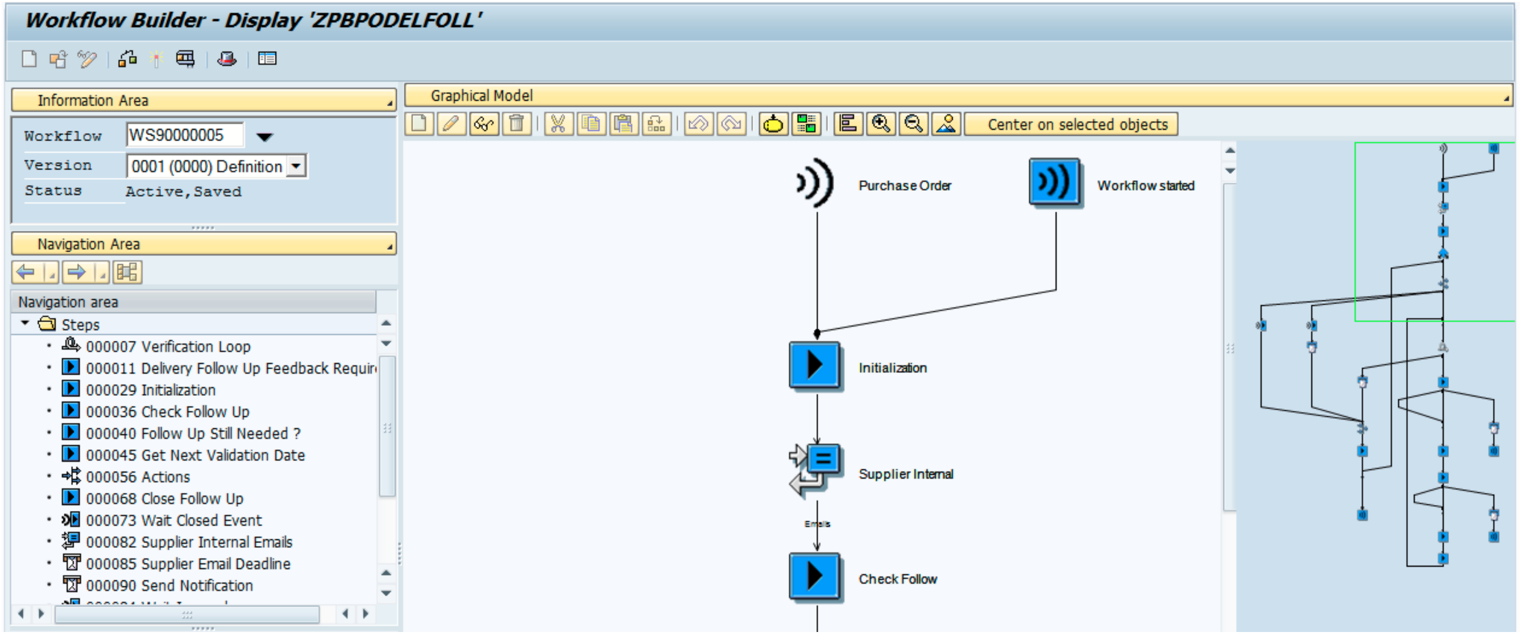
- And these are only the directly internet facing SAP SMTP nodes.
- Many companies relay email through their corporate mail servers to SAP
- Remember the before-mentioned easy guessable email addresses?

Concluding

- Inbound email is often used and can damage your business when abused
- Use SMTP authentication. When not possible due to old version of SAP consider using an intermediate SMTP server for auth/antivirus/spam filtering
- Implement mentioned SAP security notes (and have a process for that)
- Do not directly expose your SAP system’s SMTP port on the internet
- Block SMB ports to leave intranet (137,138,139,445)
- Set parameter *ixml/dtd_restriction = expansion*
- Do not use easy guessable email addresses
- Have your mail team secure the mail server setup
- Don’t give SAP_ALL to the email processing user in SICF
- Block direct access SMTP port ICM with firewall, allow only mail from mail server

Concluding

- Do NOT add SAPService<SID> user to administrators group.
- More research is needed in this area as SAP mail processing can become very complex.
- Especially workflow scenario's can become very complex with lots of variations and “Complexity kills security”.



Workflow Builder - Display 'ZPBPODELFOLL'

Workflow WS90000005
Version 0001 (0000) Definition
Status Active,Saved

Navigation area
Steps
- 000007 Verification Loop
- 000011 Delivery Follow Up Feedback Requir
- 000029 Initialization
- 000036 Check Follow Up
- 000040 Follow Up Still Needed ?
- 000045 Get Next Validation Date
- 000056 Actions
- 000068 Close Follow Up
- 000073 Wait Closed Event
- 000082 Supplier Internal Emails
- 000085 Supplier Email Deadline
- 000090 Send Notification

References

- SAP note 1098108 SMTP plug-in: ESMTP enhancements
- SAP note 455140 Configuration of e-mail, fax, paging/SMS via SMTP
- SAP note 1702632 Authentication with user and password while sending…
- SAP note 2372893 Longer passwords for SMTP authentication
- SAP note 1747180 SMTP via TLS and SMTP authentication
- SAP note 1637415 S/MIME integration in SAPconnect
- SAP note 2045861 Hiding release information from the SMTP server banner
- SAP note 2308217 Missing XML Validation vulnerability in Web-Survey
- SAP note 1496168 Relay problem while sending mails through SAPconnect using SMTP plug-in
- https://www.blackhat.com/docs/us-15/materials/us-15-Brossard-SMBv2-Sharing-More-Than-Just-Your-Files-wp.pdf

Discussion

Thank you

You’ve got mail

Owning a business with one email

Disclaimer

SAP, R/3, ABAP, SAP GUI, SAP NetWeaver and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only.

The authors assume no responsibility for errors or omissions in this document. The authors do not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

The authors shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of this document.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

No part of this document may be reproduced without the prior written permission of ERP Security BV.

ERP-SEC

HARMONIZING BUSINESS AND SECURITY

WWW.ERP-SEC.COM