

CA SENT LE SAPIN !

VOYAGE DANS LE MONDE DE LA RECHERCHE EN SÉCURITÉ SAP

Yvan GENUER, Alexandre BOLLE REDDAT



devoteam



onapsis

SOMMAIRE

- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion



devoteam



onapsis

SOMMAIRE

- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion



devoteam



onapsis

SAP ?



SAP ?



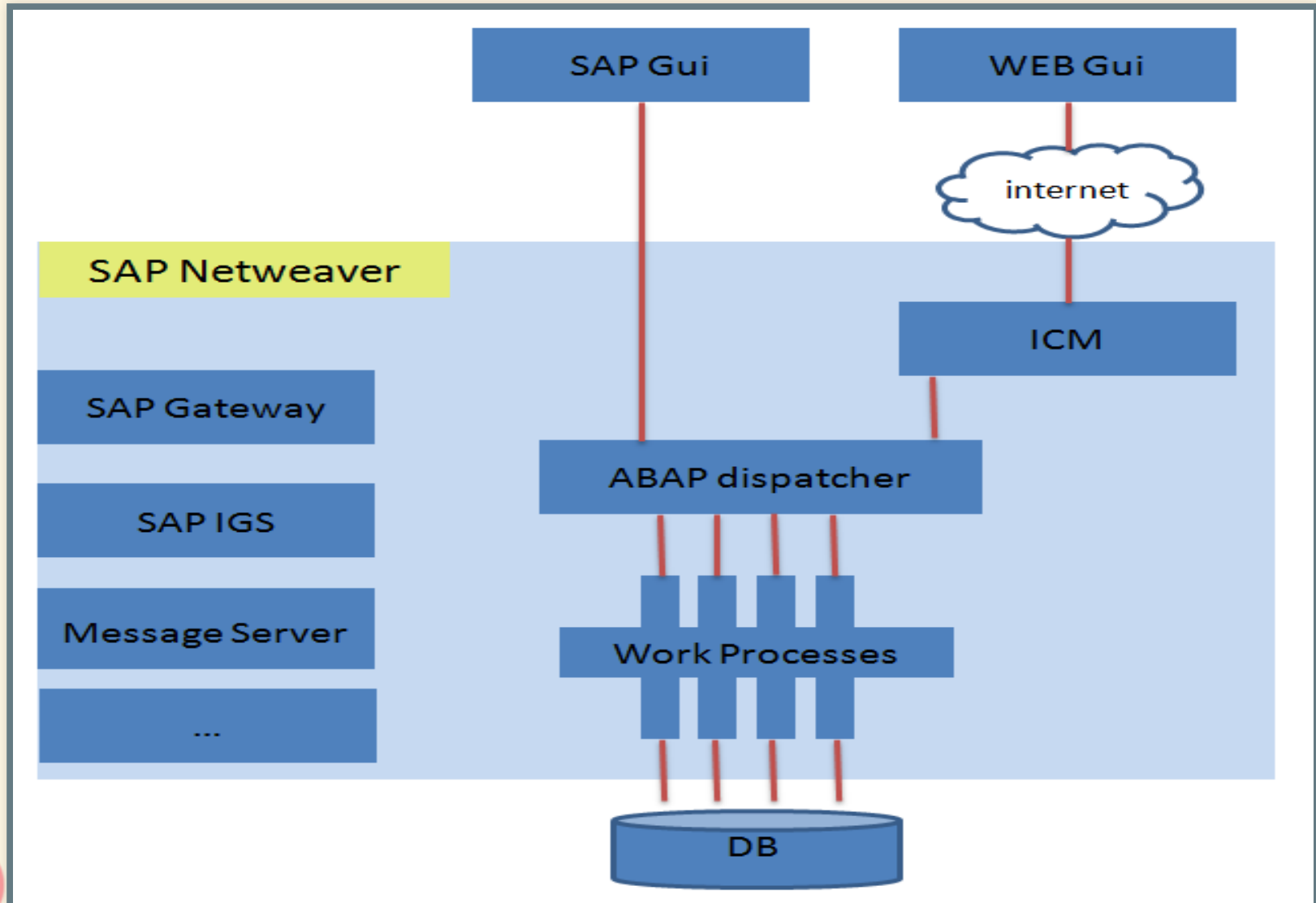
<https://www.sap.com/corporate/en/company.html>

SAP ?

Les clients SAP produisent
72% des bières
du monde



ARCHITECTURE D'UN SYSTÈME SAP



VOCABULAIRE SAP

SID	SAP système identifiant (3 char)
<sid>adm	Utilisateur administrateur (bobadm, prdadm, d01adm, etc)
Numéro de system SAP	Un identifiant sur deux chiffres. SN = 05, port = 3205, 3305, 3605, etc.

VOCABULAIRE SAP

ABAP	Advanced Business Application Programing
Report	Programme ABAP
Module fonction	Fonction ABAP
Transaction	Alias permettant de lancer une séquence de report (SU01, SM21, SIGS, etc)

LES CONCEPTS WTF...

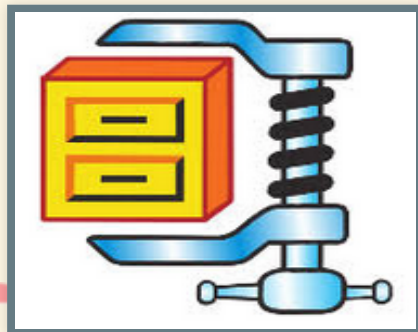
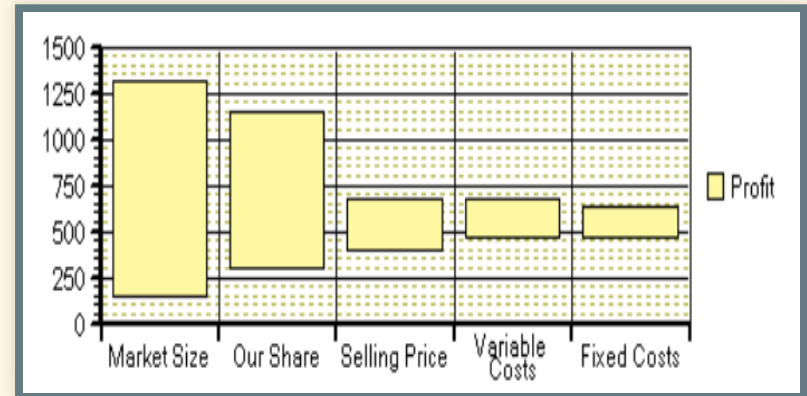
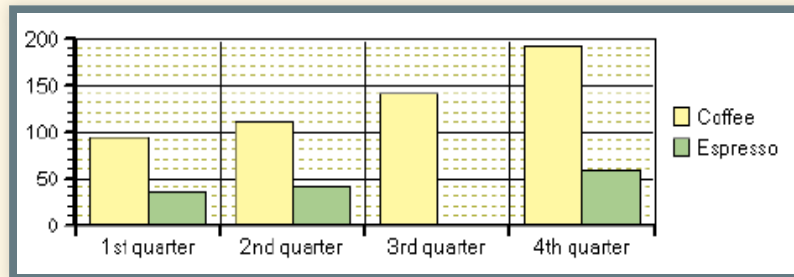
- Les services SAP tournent sur sidadm
- Le kernel SAP = ensemble de binaires sur l'OS
- Code source ABAP = dans la base de données
 - compatibilité...
 - ... du coup **accessible!**
- Tout système SAP possède un environnement de développement

SOMMAIRE

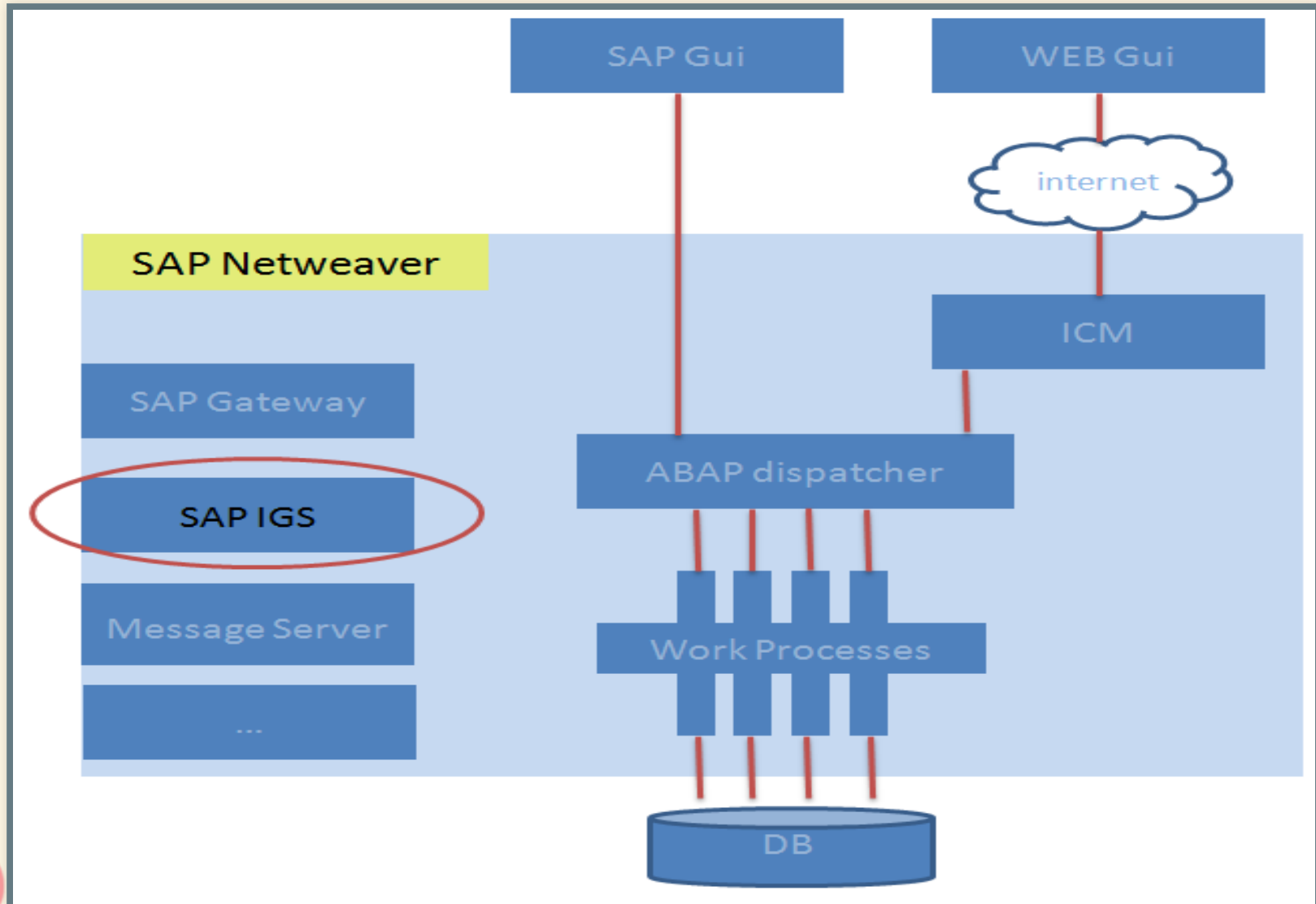
- SAP ?
- **SAP IGS ?**
- Protocole IGS
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion

A QUOI IL SERT ?

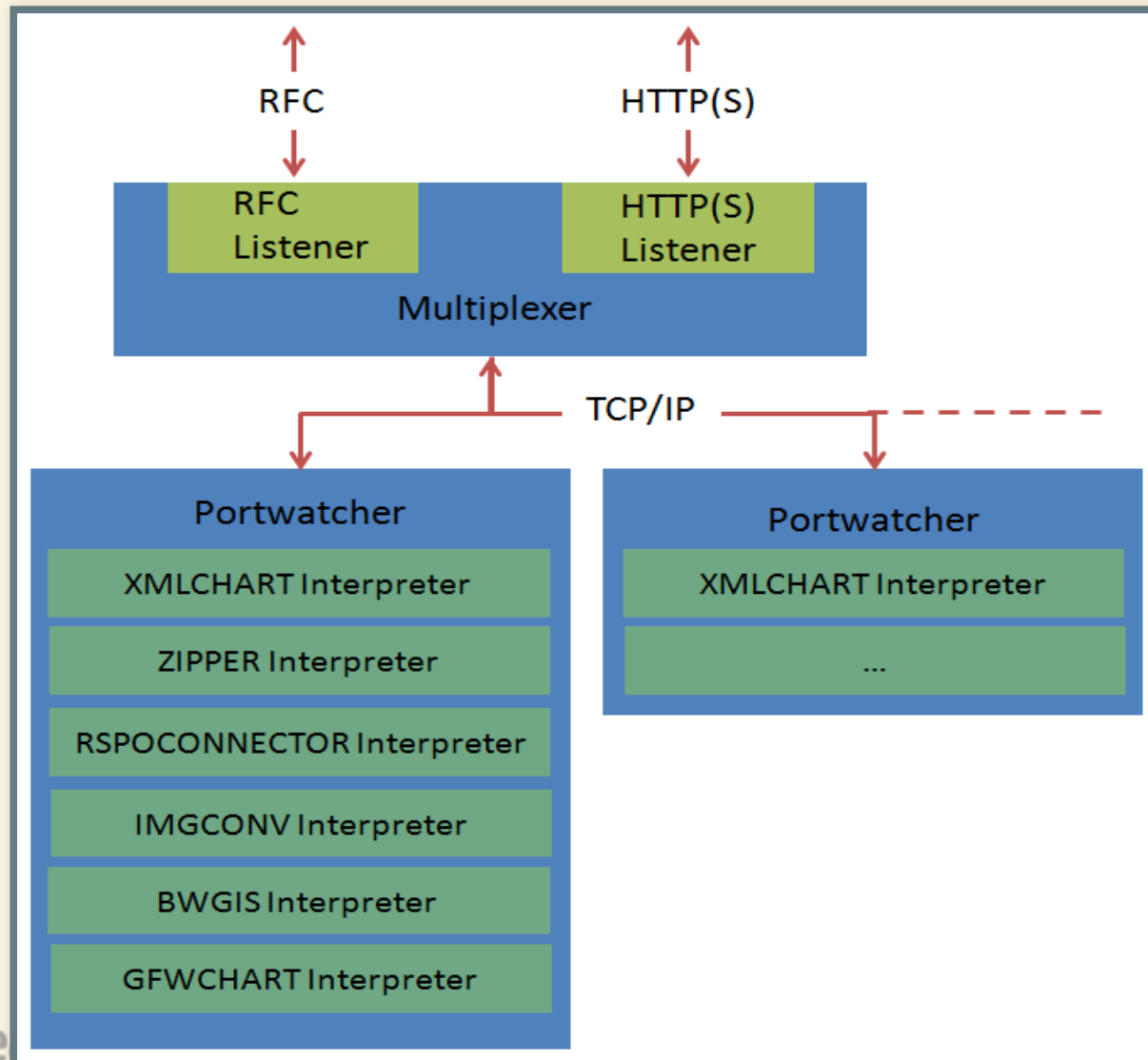
SAP Internet Graphics Services



ARCHITECTURE DU SERVICE SAP IGS



ARCHITECTURE DU SERVICE SAP IGS



ARCHITECTURE DU SERVICE SAP IGS

```
bobadm@sapbob:~# ss -lntp | grep igs
LISTEN  0      128      *:40000  *: *    users:(("igsmux_mt",pid=42225,fd=9)
LISTEN  0      20       *:40001  *: *    users:(("igspw_mt",pid=42226,fd=7)
LISTEN  0      20       *:40002  *: *    users:(("igspw_mt",pid=42227,fd=7)
LISTEN  0      128      *:40080  *: *    users:(("igsmux_mt",pid=42225,fd=6)
```

4<SN>00 RFC Listener

4<SN>80 HTTP Listener

4<SN>01 Portwatcher 1

4<SN>02 Portwatcher 2

ARCHITECTURE DU SERVICE SAP IGS

```
root@sapbob:~# pstree -a
```

```
...
├─sapstart pf=/usr/sap/B0B/SYS/profile/B0B_D00_sapbob
│   ├─B0B_00_DP pf=/usr/sap/B0B/SYS/profile/B0B_D00_sapbob
│   │   └─B0B_00_BTC_W5 pf=/usr/sap/B0B/SYS/profile/B0B_D00_sapb
│   │       ...
│   │       └─{B0B_00_DP}
│   └─ig.sapB0B_D00 -mode=profile pf=/usr/sap/B0B/SYS/profile/B0
│       ├─igsmux_mt -mode=profile -restartcount=0 -wdpid=40722 p
│       │   └─19*[{igsmux_mt}]
│       ├─igspw_mt -mode=profile -no=0 -restartcount=0 -wdpid=40
│       │   └─15*[{igspw_mt}]
│       └─igspw_mt -mode=profile -no=1 -restartcount=0 -wdpid=30
│           └─15*[{igspw_mt}]
```

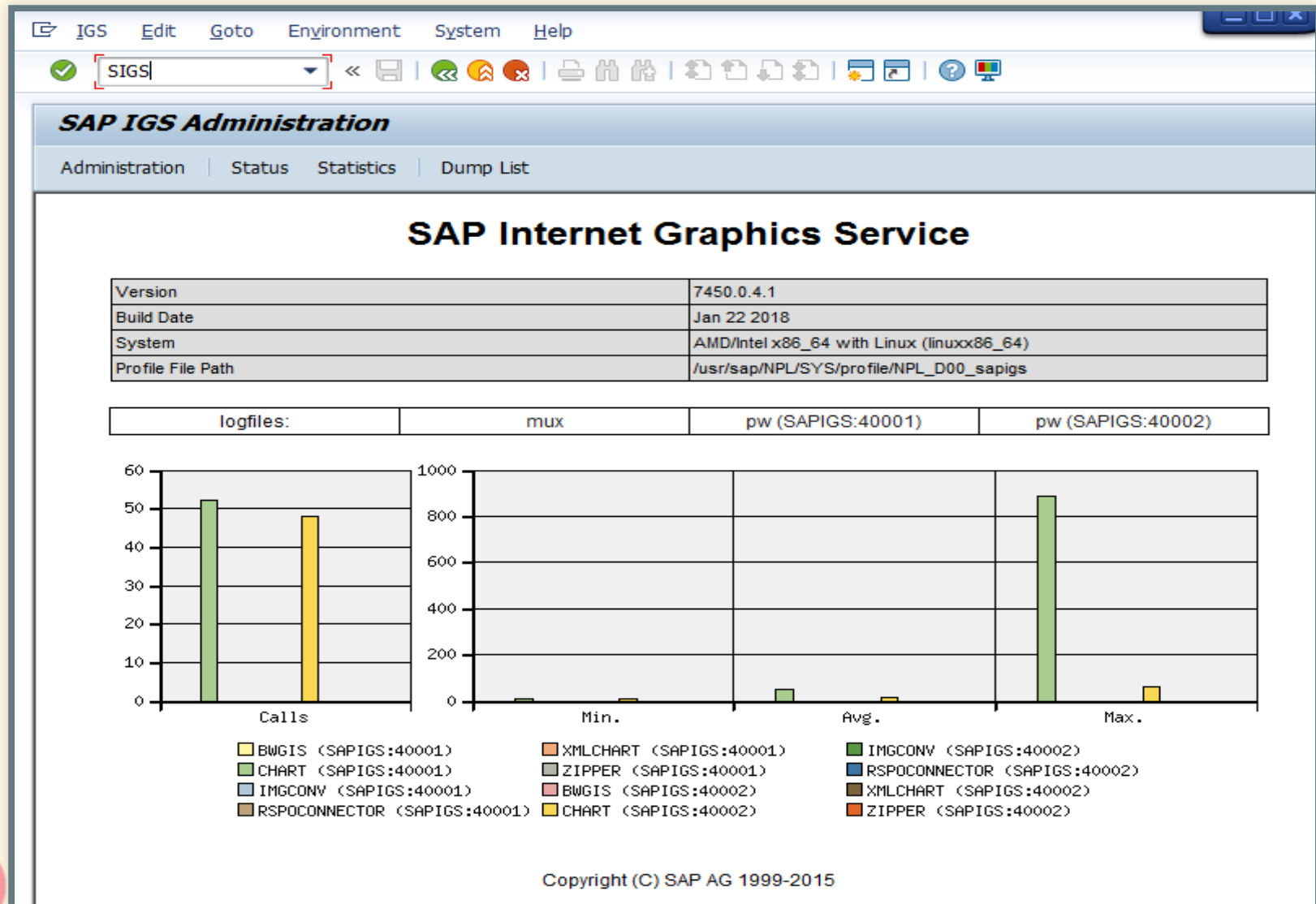


devoteam



onapsis

ARCHITECTURE DU SERVICE SAP IGS



SOMMAIRE

- SAP ?
- SAP IGS ?
- **Protocole IGS**
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion

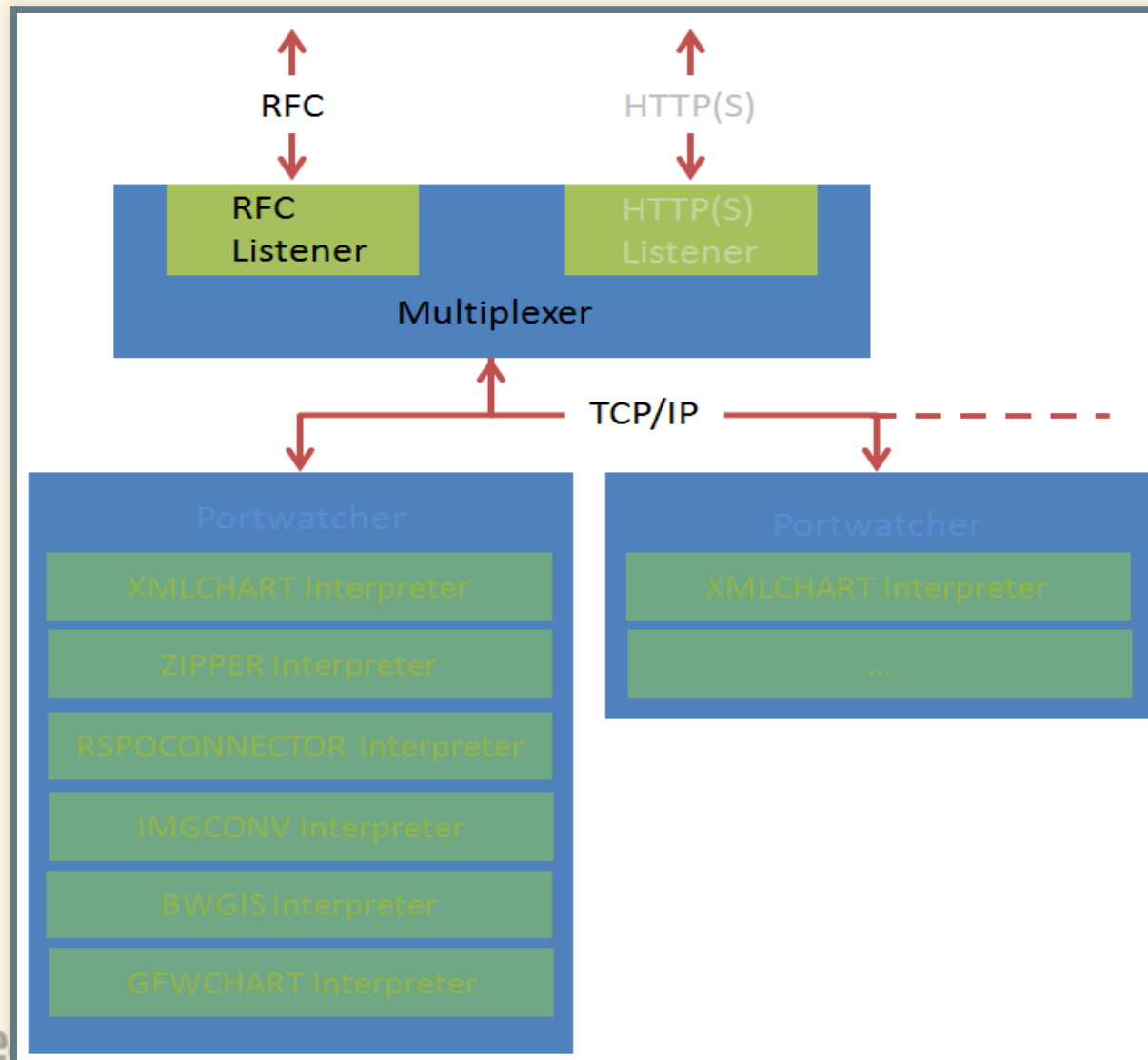


devoteam

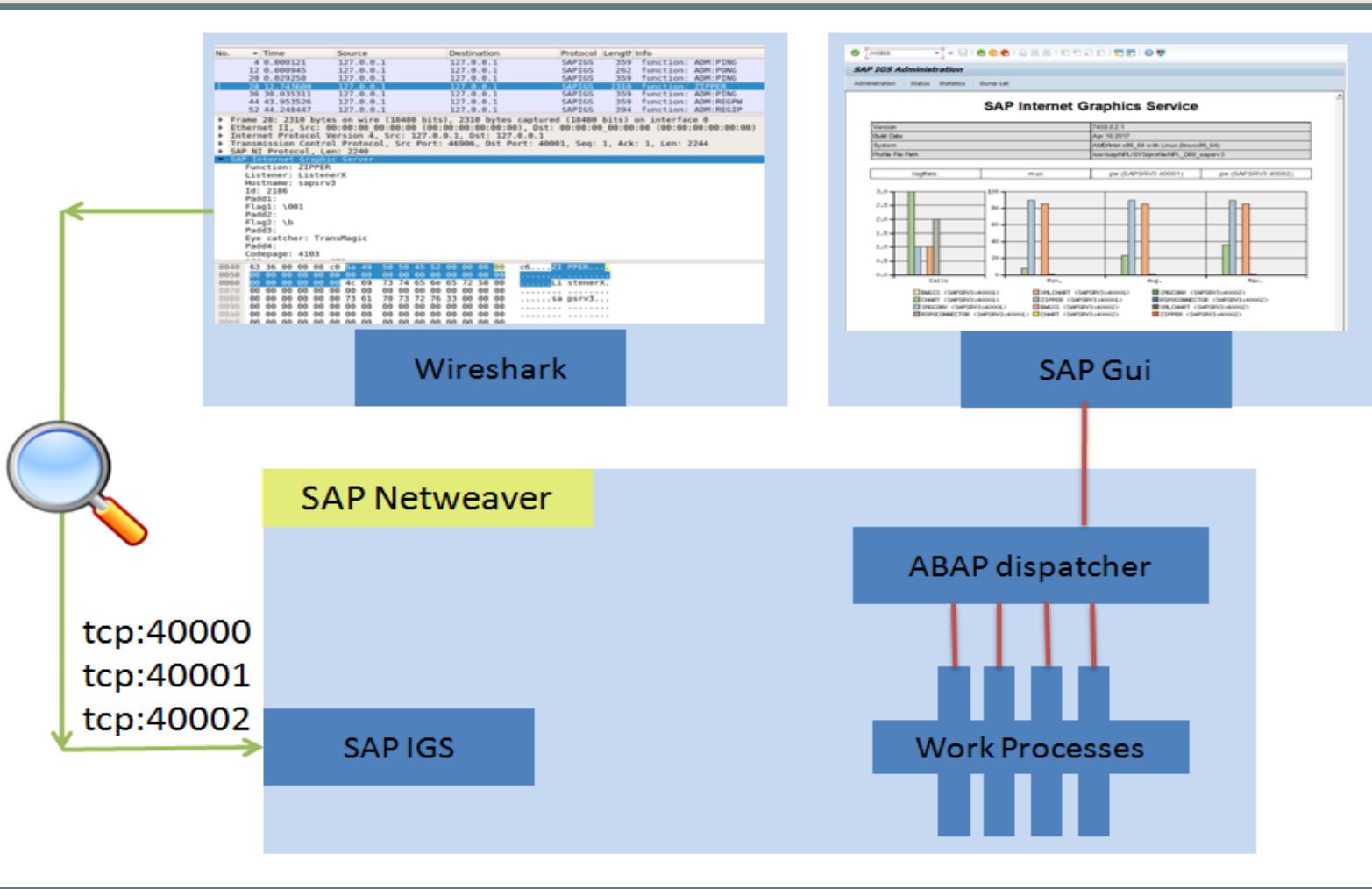


onapsis

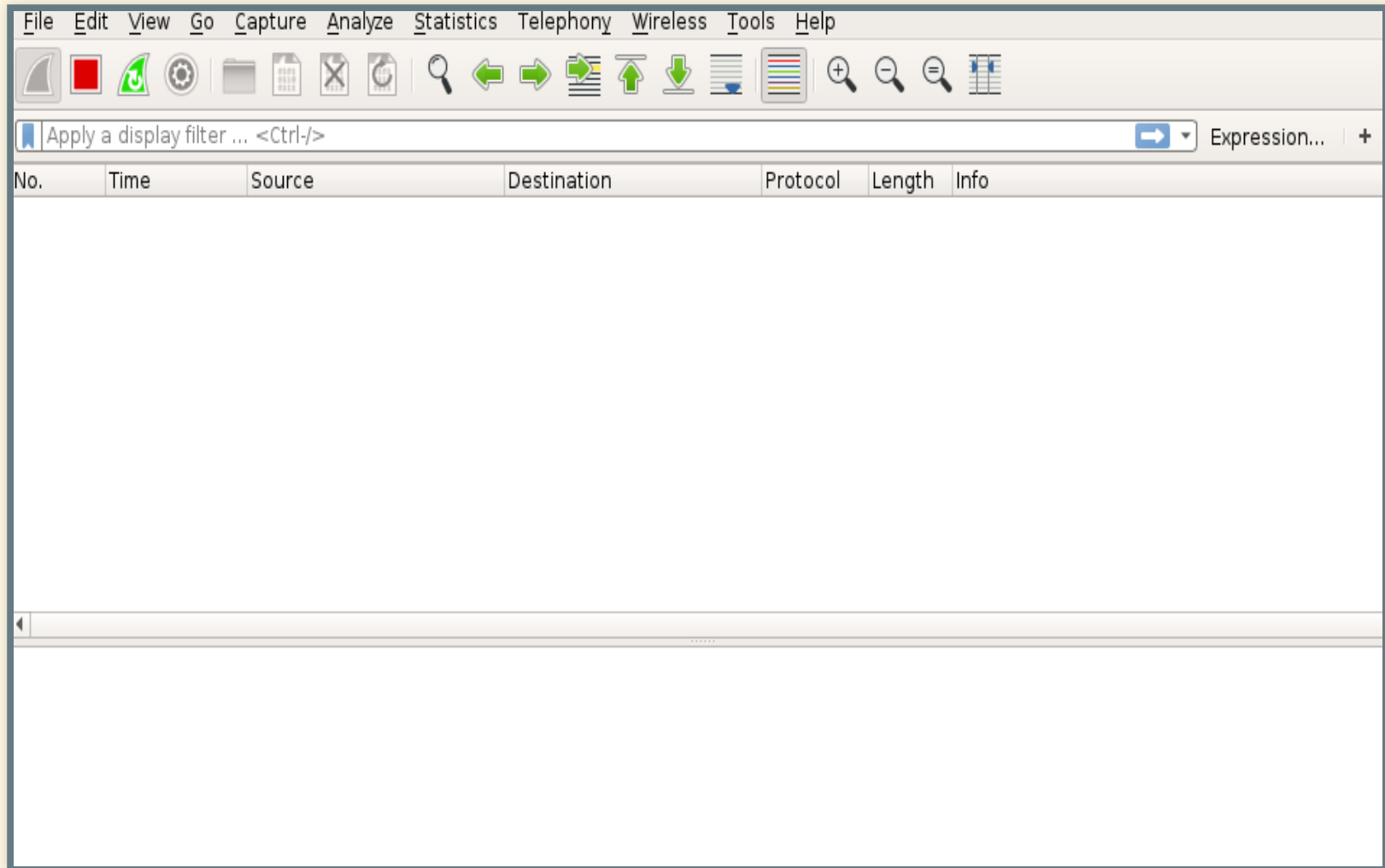
PROTOCOLE IGS : TEST



PROTOCOLE IGS : TEST



PROTOCOLE IGS : TEST



devoteam



onapsis

PROTOCOLE IGS : TEST

- Découverte des sockets internes

```
/tmp/.sapstream40000  
/tmp/.sapstream40001  
/tmp/.sapstream40002
```

PROTOCOLE IGS : TEST

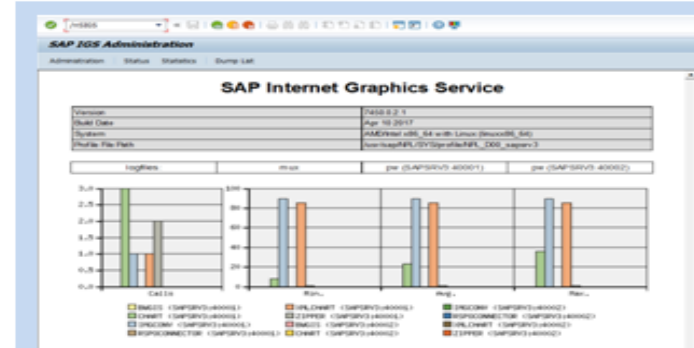
No.	Time	Source	Destination	Protocol	Length	Info
4	0.000121	127.0.0.1	127.0.0.1	SAPGS	359	Function: ADM:PING
12	0.000345	127.0.0.1	127.0.0.1	SAPGS	262	Function: ADM:PING
20	0.002250	127.0.0.1	127.0.0.1	SAPGS	359	Function: ADM:PING
30	0.002300	127.0.0.1	127.0.0.1	SAPGS	210	Function: ADM:PING
38	0.035311	127.0.0.1	127.0.0.1	SAPGS	359	Function: ADM:PING
44	0.053526	127.0.0.1	127.0.0.1	SAPGS	359	Function: ADM:RECEIVE
52	0.248447	127.0.0.1	127.0.0.1	SAPGS	394	Function: ADM:RECEIVE

Frame 20: 2310 bytes on wire (18480 bits), 2310 bytes captured (18480 bits) on interface 0
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 46906, Dst Port: 40001, Seq: 1, Ack: 1, Len: 2244
SAP IS Protocol, Len: 2244

SAP Internet Graphics Server
Function: ZIPPER
Listener: ListenerX
Hostname: saprv3
Id: 2180
Padd1: 1001
Flag1: 1001
Padd2: 10
Padd3: 10
Eye catcher: TransMagic
Padd4:
Codepage: 4103

0040: 63 36 00 00 00 c0 2a 49 50 50 45 52 00 00 00 00 c6...ZIPPER...
0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00ListenerX...
0060: 00 00 00 00 00 00 4c 69 73 74 65 66 65 72 58 00SAPRV3...
0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080: 00 00 00 00 00 00 73 61 70 73 72 76 33 00 00 00
0090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Wireshark



SAP Gui

SAP Netweaver

/tmp/.sapstream40000
/tmp/.sapstream40001
/tmp/.sapstream40002

SAP IGS

ABAP dispatcher

Work Processes

PROTOCOLE IGS : TEST

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
79	90.661601	127.0.0.1	127.0.0.1	TCP	66	40001 → 48952 [FIN, ACK] Seq=1 Ack=1605 Win=0 Len=0
80	90.661618	127.0.0.1	127.0.0.1	TCP	66	48952 → 40001 [ACK] Seq=198 Ack=2 Win=0 Len=0
81	98.376020	127.0.0.1	127.0.0.1	TCP	74	49634 → 40001 [SYN] Seq=0 Win=43690 Len=0
82	98.376029	127.0.0.1	127.0.0.1	TCP	74	40001 → 49634 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
83	98.376036	127.0.0.1	127.0.0.1	TCP	66	49634 → 40001 [ACK] Seq=1 Ack=1 Win=4 Len=0
84	98.376065	127.0.0.1	127.0.0.1	TCP	1670	49634 → 40001 [PSH, ACK] Seq=1 Ack=1 Len=1604
85	98.376068	127.0.0.1	127.0.0.1	TCP	66	40001 → 49634 [ACK] Seq=1 Ack=1605 Win=0 Len=0
86	98.376078	127.0.0.1	127.0.0.1	TCP	66	49634 → 40001 [FIN, ACK] Seq=1605 Ack=1605 Win=0 Len=0
87	98.376148	127.0.0.1	127.0.0.1	TCP	66	40001 → 49634 [FIN, ACK] Seq=1 Ack=1605 Win=0 Len=0
88	98.376155	127.0.0.1	127.0.0.1	TCP	66	49634 → 40001 [ACK] Seq=1606 Ack=2 Win=0 Len=0
89	98.376646	127.0.0.1	127.0.0.1	TCP	74	58842 → 40000 [SYN] Seq=0 Win=43690 Len=0

▶ Frame 84: 1670 bytes on wire (13360 bits), 1670 bytes captured (13360 bits) on interface 0

▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)

▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

▶ Transmission Control Protocol, Src Port: 49634, Dst Port: 40001, Seq: 1, Ack: 1, Len: 1604

▼ Data (1604 bytes)

Data: 0000064041444d3a47455444554d50000000000000000000...

[Length: 1604]

Offset	Hex	ASCII
0000	00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00E.
0010	06 78 c7 08 40 00 40 06 6f 75 7f 00 00 01 7f 00	.x..@.@.ou.....
0020	00 01 c1 e2 9c 41 c7 9d e7 50 f6 16 ec 20 80 18A...P.....
0030	01 56 04 6d 00 00 01 01 08 0a 00 00 20 49 00 00	.V.m.....I..
0040	20 49 00 00 06 40 41 44 4d 3a 47 45 54 44 55 4d	I...@AD M:GETDUM
0050	50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	P.....
0060	00 00 00 00 00 00 00 4c 69 73 74 65 6e 65 72 33 33L1 stener33
0070	35 36 39 34 30 30 30 00 00 00 00 00 00 00 00 00	5694000.
0080	00 00 00 00 00 00 00 73 61 70 69 67 73 00 00 00 00sa pigs....
0090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0	00 00 00 00 00 00 00 35 37 30 38 38 00 00 00 00 00S 7088....
00e0	00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00
00f0	00 00 80 05 00 00 50 80 04 24 aa 7f 00 00 80 05P. \$.
0100	00 00 00 00 00 00 54 72 61 6e 73 4d 61 67 69 63Tr ansMagic
0110	00 00 34 31 30 33 33 33 36 00 00 00 00 00 00 00	..410333 6.....
0120	00 00 00 00 00 00 31 30 32 34 00 00 00 00 00 0010 24.....



devoteam



onapsis

PROTOCOLE IGS : BINAIRES

Binaires du kernel SAP associés à l'IGS

igsmux_mt	Multiplexer
igspw_mt	Portwatcher
bwgis.so	Library for BWGIS interpreter
bwgis_c.so	Library for BWGIS interpreter
gfwchart.so	Library for CHART interpreter
gfwchart_c.so	Library for CHART interpreter
imgconv.so	Library for IMGCONV interpreter
rspoconnector.so	Library for RSPOCONNECTOR interpreter
sgxgis.so	Library for SAPIGSXML interpreter
xmlchart.so	Library for XMLCHART interpreter
xmlchart_c.so	Library for XMLCHART interpreter
zipper.so	Library for ZIPPER interpreter

PROTOCOLE IGS : BINAIRES

```
root@sapbob:/sapmnt/B0B/exe/uc/linuxx86_64# file igsmux_mt
igsmux_mt: ELF 64-bit LSB executable, x86-64, version 1 (SYSV),
dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2,
for GNU/Linux 2.6.4, BuildID[sha1]=d800fb09cf0729672a6993557126871
not stripped
```

PROTOCOLE IGS : RÉSULTATS

PROTOCOLE IGS : RÉSULTATS

- Tout est en clair

```
0030 01 56 11 93 00 00 01 01 08 0a 00 00 2c 04 00 00 .v..... ,...
0040 2c 04 00 00 01 67 41 44 4d 3a 49 4c 4c 42 45 42 ,....gAD M:ILLBEB
0050 41 43 4b 00 00 00 00 00 00 00 00 00 00 00 00 ACK.....
0060 00 00 00 00 00 00 4c 69 73 74 65 6e 65 72 33 33 .....Li stener33
0070 35 37 31 38 38 31 36 00 00 00 00 00 00 00 00 00 5718816. ....
0080 00 00 00 00 00 00 73 61 70 69 67 73 00 00 00 00 .....sa pigs....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00d0 00 00 00 00 00 00 00 35 37 30 39 35 00 20 20 20 .....5 7095.
00e0 20 20 20 20 20 20 20 20 20 20 01 00 00 00 00 00 .....
00f0 00 00 a7 00 00 00 c0 2e 00 78 2d 7f 00 00 a7 00 ..... .x-.....
0100 00 00 20 20 20 20 54 72 61 6e 73 4d 61 67 69 63 .. Tr ansMagic
0110 00 00 00 00 00 00 61 70 70 6c 69 63 61 74 69 6f .....ap plicatio
0120 6e 2f 6f 63 74 65 74 2d 73 74 72 65 61 6d 20 20 n/octet- stream
0130 20 20 20 20 20 20 44 55 4d 50 20 20 20 20 20 20 DU MP
0140 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0150 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0160 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0170 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0180 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0190 20 20 20 20 20 20 37 00 00 00 00 00 00 00 40 94 7. ....@.
01a0 06 88 2d 7f 00 00 62 6c 61 62 6c 61 0a ...-...bl abla.
```



PROTOCOLE IGS : RÉSULTATS

Récupération des noms des fonctions d'administration

```
1: "ADM:REGPW",      # Register a PortWatcher
2: "ADM:UNREGPW",    # Unregsiter a PortWatcher
3: "ADM:REGIP",      # Register an Interpreter
4: "ADM:UNREGIP",    # Unregsiter an Interpreter
5: "ADM:FREEIP",     # Inform than Interpreter is free
6: "ADM:ILLBEBACK",  # Call back function
7: "ADM:ABORT",      # Abort Interpreter work
8: "ADM:PING",       # Ping receive
9: "ADM:PONG",       # Ping send
10: "ADM:SHUTDOWNIGS", # Shutdown IGS
11: "ADM:SHUTDOWNPW", # Shutdown PortWatcher
12: "ADM:CHECKCONSUMER", # Check Portwatcher status
```

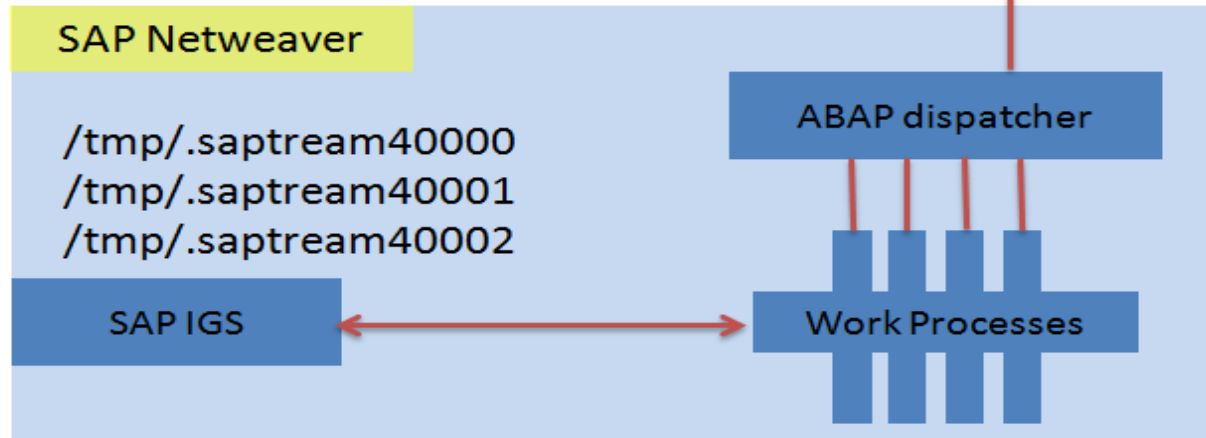
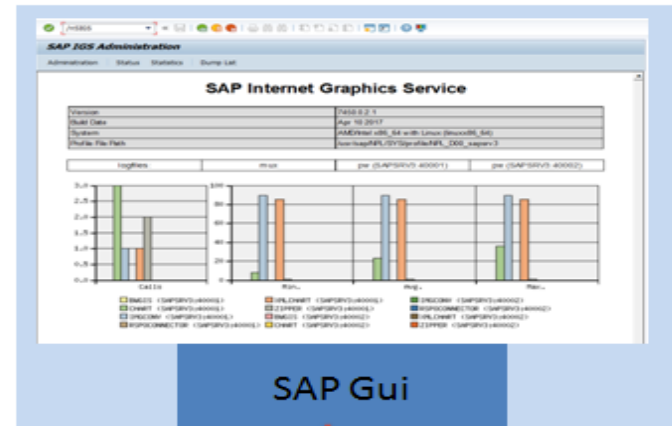
PROTOCOLE IGS : RÉSULTATS

Récupération des noms des fonctions d'administration

```
13: "ADM:FREECONSUMER", # Inform than portwather is free
14: "ADM:GETLOGFILE",   # Display log file
15: "ADM:GETCONFIGFILE", # Display configfile
16: "ADM:GETDUMP",      # Display dump file
17: "ADM:DELETEDUMP",   # Delete dump file
18: "ADM:INSTALL",      # ???
19: "ADM:SWITCH",        # Switch trace log level
20: "ADM:GETVERSION",   # Get IGS Version
21: "ADM:STATUS",       # Display IGS Status
22: "ADM:STATISTIC",    # old Display IGS Statistic
23: "ADM:STATISTICNEW", # Display IGS Statistic
24: "ADM:GETSTATCHART", # Get IGS Statistic chart
25: "ADM:SIM",          # Simulation function
```

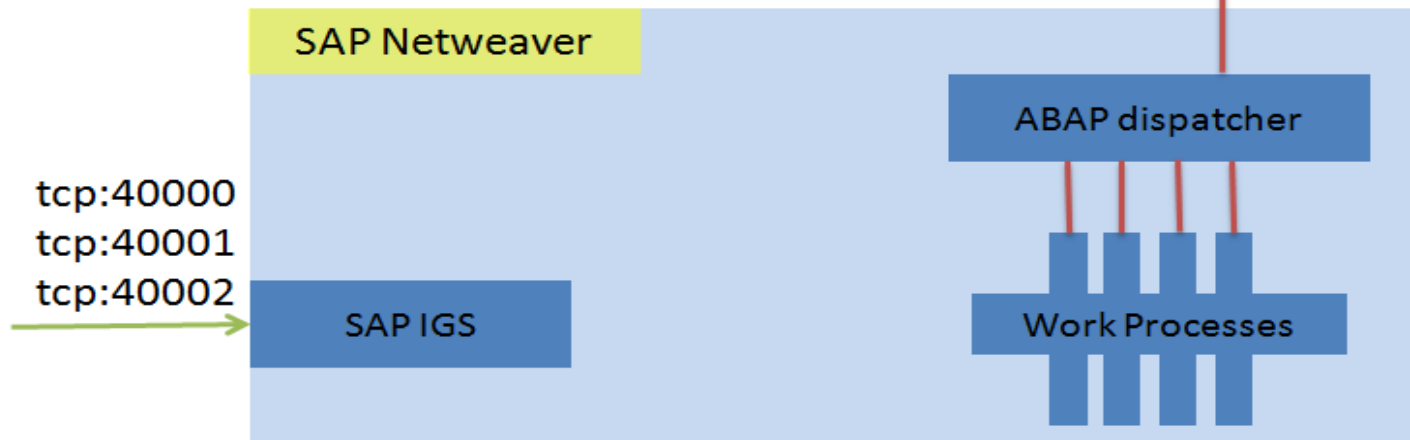
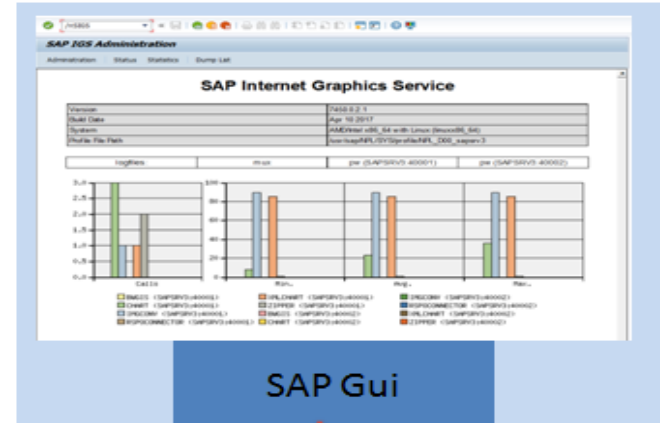
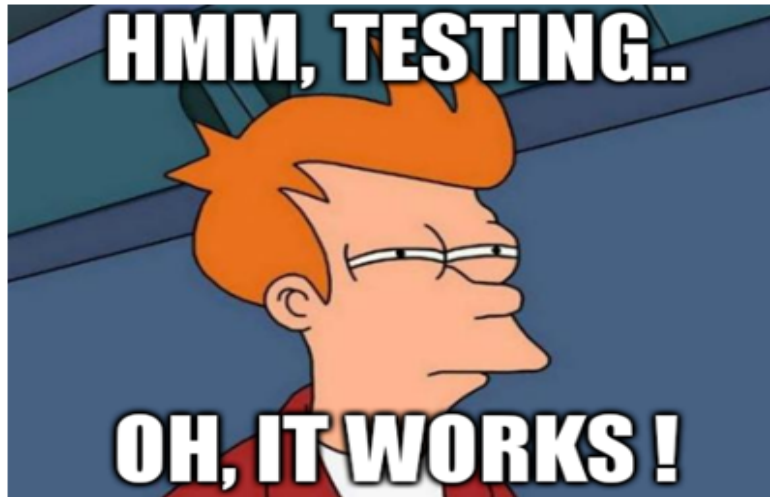
PROTOCOLE IGS : RÉSULTATS

- Pas de mécanisme d'authentification...



PROTOCOLE IGS : RÉSULTATS

- Pas de mécanisme d'authentification...



SOMMAIRE

- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion

OUTILS : PYSAP

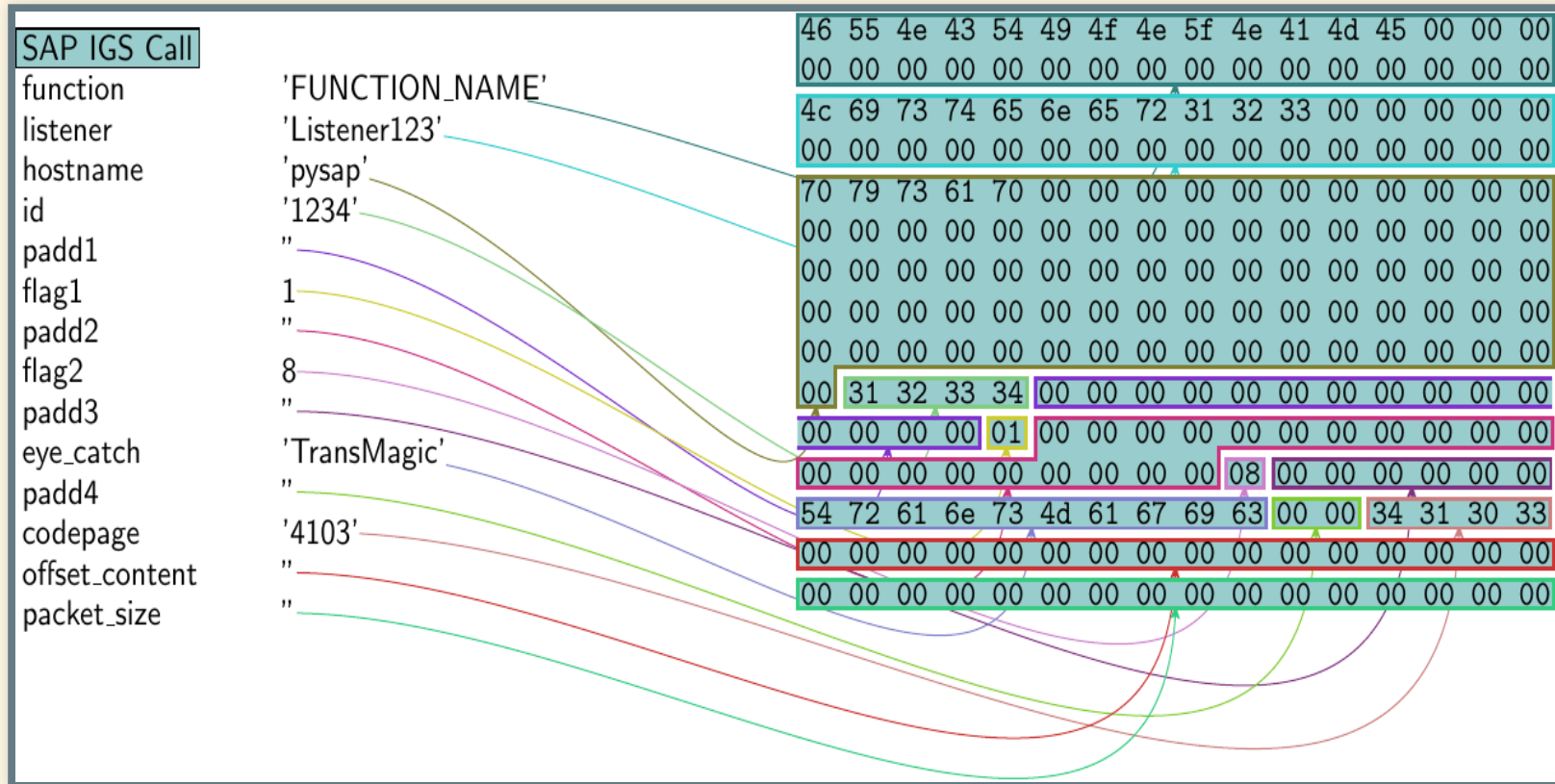
Librairie python

Utilisant scapy

SAP NI, SAP MS, SAP ENQ, ...

... **SAP IGS**

OUTILS : PYSAP



OUTILS : SAP-DISSECTION

Plugin wireshark

SAP NI, SAP MS, SAP ENQ, ...

... **SAP IGS**



devoteam



onapsis

OUTILS : SAP-DISSECTION

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, navigation, and analysis. A display filter bar shows "Apply a display filter ... <Ctrl-/>" and an "Expression..." field.

The main packet list pane displays a table of captured packets:

No.	Time	Sou	Des	Protocol	Length	Info
1	0.000000	1...	1...	TCP	74	39439 → 40001 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=374430...
2	0.000010	1...	1...	TCP	74	40001 → 39439 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK_PERM=1 T...
3	0.000022	1...	1...	TCP	66	39439 → 40001 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=3744300 TSecr=3744300
4	0.000094	1...	1...	SAPIGS	1670	function: ADM:GETDUMP
5	0.000098	1...	1...	TCP	66	40001 → 39439 [ACK] Seq=1 Ack=1605 Win=174720 Len=0 TSval=3744300 TSecr=3744...
6	0.000134	1...	1...	TCP	66	40001 → 39439 [FIN, ACK] Seq=1 Ack=1605 Win=174720 Len=0 TSval=3744300 TSecr...
7	0.000437	1...	1...	TCP	66	39439 → 40001 [FIN, ACK] Seq=1605 Ack=2 Win=43776 Len=0 TSval=3744300 TSecr=...
8	0.000442	1...	1...	TCP	66	40001 → 39439 [ACK] Seq=2 Ack=1606 Win=174720 Len=0 TSval=3744300 TSecr=3744...
9	0.000968	1...	1...	TCP	74	35685 → 40000 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=374430...

Below the packet list, the packet details pane shows the structure of the selected packet (Frame 1):

- Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- Transmission Control Protocol, Src Port: 39439, Dst Port: 40001, Seq: 0, Len: 0

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII:

```
0000 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E.
0010 00 3c e7 47 40 00 40 06 55 72 7f 00 00 01 7f 00 .<.G@.@. Ur.....
0020 00 01 9a 0f 9c 41 ac e8 c5 6b 00 00 00 00 a0 02 ....A.. .k.....
0030 aa aa fe 30 00 00 02 04 ff d7 04 02 08 0a 00 39 ...0....9
0040 22 2c 00 00 00 00 01 03 03 07 ".....
```

The status bar at the bottom indicates: Transmission Control Protocol (tcp), 40 bytes | Packets: 164 · Displayed: 164 (100.0%) · Load time: 0:0.2 | Profile: Default

SOMMAIRE

- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- **ADM:INSTALL**
- Vulnérabilités
- Conclusion



devoteam

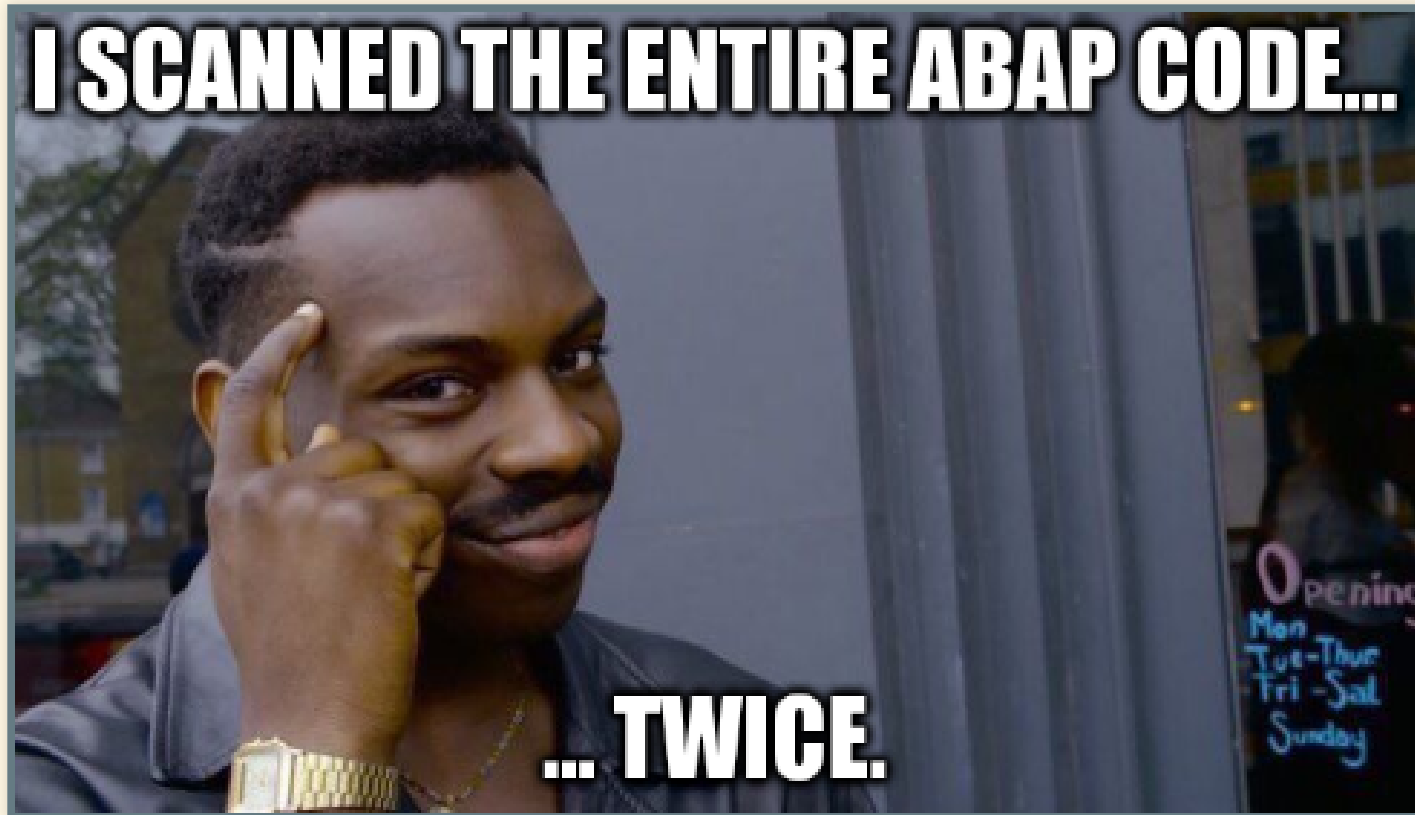


onapsis

ADM:INSTALL : POURQUOI ?

- A cause de son nom...
- Trouvé dans le binaire, mais n'apparaît jamais dans nos captures réseaux

ADM:INSTALL : RECHERCHE D'INFORMATION



ADM:INSTALL : RECHERCHE D'INFORMATION

- Recherche du pattern "ADM:INSTALL" dans tout le code ABAP
- 30.000 programmes... **1 occurrence !**

ADM:INSTALL : SAPMAP_INSTALL_SHAPEFILES

Class Builder Class CL_RSR_WWW_ITEM_WEBMAP Display

Repository Browser

Class / Interface

CL_RSR_WWW_ITEM_WEBMAP

Object Name Description

CL_RSR_WWW_ITEM_WEBMAP	Complete Map in Web
Superclasses	
Subclasses	
Attribute	
Methods	
Inherited Methods	
Redefinitions	
SAPMAP_INSTALL_SHAPEFILES	Installs Missing ShapeFiles on IGS
CREATE_GEO_COMMAND_URL	Create URL for Geographic Interact
SAPMAP_GET_LOGSYS	Fetching the Logical System Name
CHECK_DP_VALIDITY	Check if DP is Allowed for Map Laye
CREATE_GEO_NAV_TOOLBAR	Create HTML for Cartographic Inter

Method

SAPMAP_INSTALL_SHAPEFILES

```
185 ENDIF.  
186 CALL METHOD l_r_igsdata->send  
187 EXPORTING  
188     farm_type           = 'ADM:INSTALL'  
189     rfcdestination      = l_rfc_destination  
190 IMPORTING  
191     msg_text            = l_error_msg  
192 EXCEPTIONS  
193     rfc_communication_error = 1  
194     rfc_system_error      = 2  
195     internal_error       = 3.  
196 IF sy-subrc <> 0.  
197     CLEAR l_s_raise.  
198     l_s_raise-arbgb = 'RSWWW'.  
199     l_s_raise-typ = 'I'.  
200     l_s_raise-txtnr = '004'.  
201     CALL METHOD raise_message  
202     EXPORTING  
203         l_s_raise = l_s_raise
```

ADM:INSTALL : SAPMAP_INSTALL_SHAPEFILES

- Vérifie s'il y a des shapefiles manquants sur l'IGS
- Si oui il upload les shapefiles via la fonction nommée adm:install
- ADM:INSTALL = installation de nouveaux shapefiles

ADM:INSTALL : SAPMAP_INSTALL_SHAPEFILES

"On peut peut-être envoyer autre chose qu'un shapefile
?"

ADM:INSTALL : SAPMAP_INSTALL_SHAPEFILES

- Code un peu compliqué
- Beaucoup d'appels à d'autres fonctions
- Failed si on essaye de l'exécuter...



devoteam



onapsis

ADM:INSTALL : DEBUGGER ABAP

- Un système SAP fourni en standard un environnement de développement
- Donc avec un debugger...

User System Help

✓

SAP

New password

Client

User

Password

Logon Language

root@sapigs:/usr/sap/NPL/D00/igs/data# _

root@sapigs:~# _

I

ADM:INSTALL : PACKET IGS

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000078	127.0.0.1	127.0.0.1	TCP	8258	52927 → 40001 [PSH, ACK] Seq=...
5	0.000082	127.0.0.1	127.0.0.1	TCP	66	40001 → 52927 [ACK] Seq=1 Ack=...
6	0.000109	127.0.0.1	127.0.0.1	SAPIGS	1654	function: ADM:INSTALL
7	0.000111	127.0.0.1	127.0.0.1	TCP	66	40001 → 52927 [ACK] Seq=1 Ack=...
8	0.000143	127.0.0.1	127.0.0.1	TCP	66	40001 → 52927 [FIN, ACK] Seq=...

▶ Frame 6: 1654 bytes on wire (13232 bits), 1654 bytes captured (13232 bits)
 ▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
 ▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
 ▶ Transmission Control Protocol, Src Port: 52927, Dst Port: 40001, Seq: 8193, Ack: 1, Len: 1588
 ▶ [2 Reassembled TCP Segments (9780 bytes): #4(8192), #6(1588)]
 ▶ SAP NI Protocol, Len: 9776
 ▼ SAP Internet Graphic Server

Function: ADM:INSTALL

Listener: Listener-1140845296
 Hostname: sapsrv3
 Id: 2187
 Padd1:
 Flag1: \001
 Padd2:

0000	00 00 26 30 41 44 4d 3a 49 4e 53 54 41 4c 4c 00	..&0ADM: INSTALL.
0010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0020	00 00 00 00 4c 69 73 74 65 6e 65 72 2d 31 31 34List ener-114
0030	30 38 34 35 32 39 36 00 00 00 00 00 00 00 00 00	0845296.
0040	00 00 00 00 73 61 70 73 72 76 33 00 00 00 00 00saps rv3.....
0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090	00 00 00 00 00 32 31 38 37 00 76 76 76 76 76 76218 7.vvvvvvv
00a0	76 76 76 76 76 76 76 76 01 00 00 00 00 00 00 00	vvvvvvvvv
00b0	70 25 00 00 50 5a 01 cc 0e 7f 00 00 70 25 00 00	p%..PZ..p%..
00c0	76 76 76 76 54 72 61 6e 73 4d 61 67 69 63 00 00	vvvvTran sMagic..
00d0	34 31 30 33 31 33 34 34 00 00 00 00 00 00 00 00	41031344
00e0	00 00 00 00 38 31 30 32 00 00 00 00 00 00 00 00	8102

ADM:INSTALL : PACKET IGS

- Si nous renvoyons ce packet sur le port 40000
- Les fichiers shapefiles sont aussi créés...
- ... **a distance, sans être authentifié sur SAP**

SOMMAIRE

- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- ADM:INSTALL
- **Vulnérabilités**
- Conclusion



devoteam



onapsis

```
root@sapigs:/usr/sap/NPL/D00/igs/data# _
```

```
villain # python igs_admininstall_upload.py -h  
Usage: igs_admininstall_upload.py [options] -d <remote host>
```

This example script exploit CVE-2018-2420 to upload arbitrary file on /usr/sap/SID/Dxx/igs/data directory

Options:

-h, --help show this help message and exit

Target:

-d REMOTE_HOST, --remote-host=REMOTE_HOST
Remote host

-p REMOTE_PORT, --remote-port=REMOTE_PORT
Remote port [40000]

--route-string=ROUTE_STRING
Route string for connecting through a SAP Router

Misc options:

-i FILE Input file to upload [poc.txt]

-n FILE_NAME Target filename [input filename]

-a FILE_PATH Target file path [output/]

-v, --verbose Verbose output [False]

pysap 0.1.14 - <https://www.coresecurity.com/corelabs-research/open-source-tools/pysap>
- <https://github.com/CoreSecurity/pysap>

```
villain # _
```

I

VULNÉRABILITÉS : TÉLÉDÉCHARGEMENT DE FICHIERS

2615635 - [CVE-2018-2420] Unrestricted File Upload
in SAP Internet Graphics Server (IGS)

igs/pw/install = disable

```
root@sapigs:/sapmnt/NPL/exe/uc/linuxx86_64# _
```

```
villain # python igs_admininstall_dos.py -h  
Usage: igs_admininstall_dos.py [options] -d <remote host>
```

This is a PoC for CVE-2018-2421

Options:

-h, --help show this help message and exit

Target:

-d REMOTE_HOST, --remote-host=REMOTE_HOST
Remote host

-p REMOTE_PORT, --remote-port=REMOTE_PORT
Remote port [40000]

--route-string=ROUTE_STRING

Route string for connecting through a SAP Router

uter

Misc options:

-v, --verbose Verbose output [False]

pysap 0.1.14 - [https://www.coresecurity.com/corelabs-research/open-source-](https://www.coresecurity.com/corelabs-research/open-source-tools/pysap)

[tools/pysap - https://github.com/CoreSecurity/pysap](https://github.com/CoreSecurity/pysap)

```
villain # _
```

VULNÉRABILITÉS : DÉNI DE SERVICE

2616599 - [CVE-2018-2421] Denial of Service in SAP
Internet Graphics Server (IGS) Portwatcher

SOMMAIRE

- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion



devoteam



onapsis

CONCLUSION

- Propriétaire != sécurisé
- Pas si compliqué que ça
- Reverse, network, ABAP, python, web...

- SAP <https://www.sap.com/corporate/en/company.html>
- SAP IGS online help [IGS SAP Help](#)
- SAP Security notes [2525222](#), [2538829](#), [2615635](#), [2616599](#)
- gdb peda <https://github.com/longld/peda>
- PySAP <https://github.com/CoreSecurity/pysap>
- SAP-Dissection <https://github.com/CoreSecurity/SAP-Dissection-plugin-for-Wireshark>
- Devoteam <https://www.cert-devoteam.fr/>
- Onapsis <https://www.onapsis.com>

MERCI !

ygenuer [\x40] onapsis.com

alexandre.bolle.reddat [\x40] devoteam.com