L’agent qui parlait trop

Yvan Genuer

SSTIC 2020 // 3-5 juin 2020 // Rennes, France

Clause de non responsabilité (english)

- This presentation contains references to the products of SAP SE. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.

- Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.

- SAP SE 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.

Objectifs

SAP Security Notes July ‘19: Critical Vulnerability Affecting Solution Manager

... Security Notes July ‘19: Critical Vulnerability Affecting **Solution Manager** ... analysis include: Hot News SAP Note in **Solution Manager** Diagnostic Agent —the only Hot News ...

SAP Security Notes September ‘19: Critical Solution Manager Patch Now Available for Windows

SAP Security Notes September ‘19: Critical **Solution Manager** Patch Now Available for Windows ... analysis include: Critical vulnerability in **Solution Manager** Diagnostics Agent now also fixed for ...

SAP Security Notes June ‘19: SAP Increased Priority for SAP Solution Manager Patch

... Security Notes June ‘19: SAP Increased Priority for SAP **Solution Manager** Patch ... include: High Priority SAP Note related to **Solution Manager** -- SAP increased criticality for this ...

SAP Security Notes March 2020: Two Critical Patches Released to Protect Solution Manager from Cyberattacks

... Notes March 2020: Two Critical Patches Released to Protect **Solution Manager** from Cyberattacks ... HotNews Note —Missing authentication in **Solution Manager** Onapsis Research Labs is Top ...

onapsis

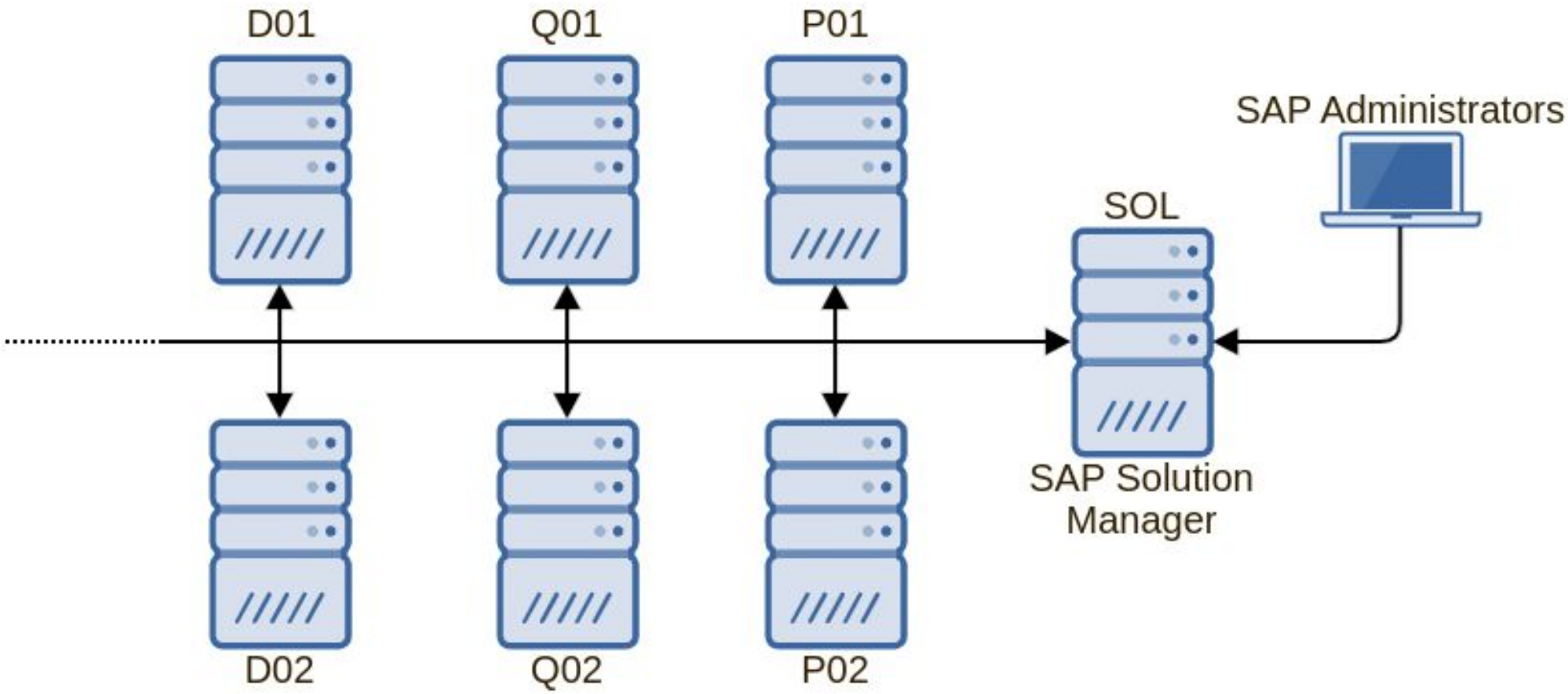
1. Introduction
2. Premier contact
3. Echec du “SAP Secure Storage”
4. Le service P4
5. Contournement d’authentification
6. Exécution de commande
7. Contre-mesures
8. Conclusion

onapsis

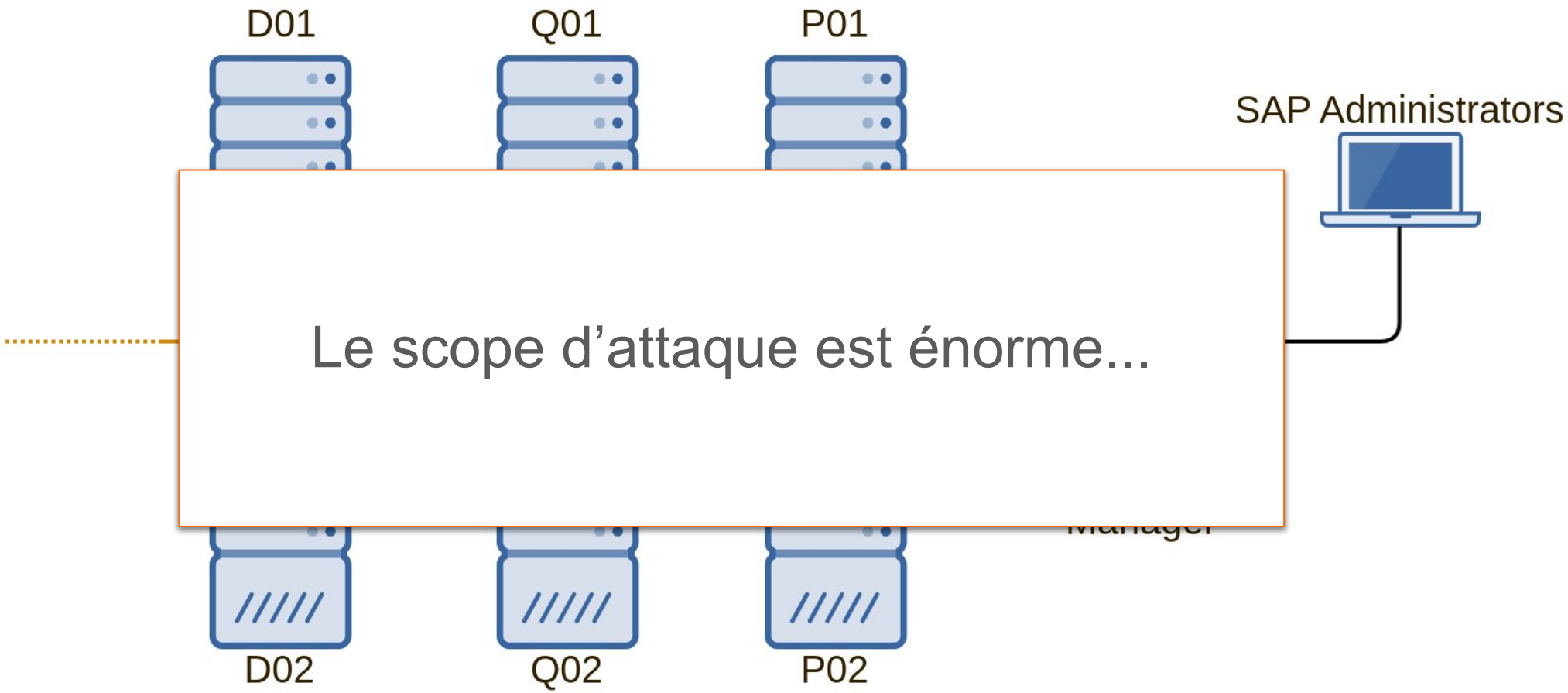
1. **Introduction**
2. Premier contact
3. Echec du “SAP Secure Storage”
4. Le service P4
5. Contournement d’authentification
6. Exécution de commande
7. Contre-mesures
8. Conclusion

Introduction - SolMan

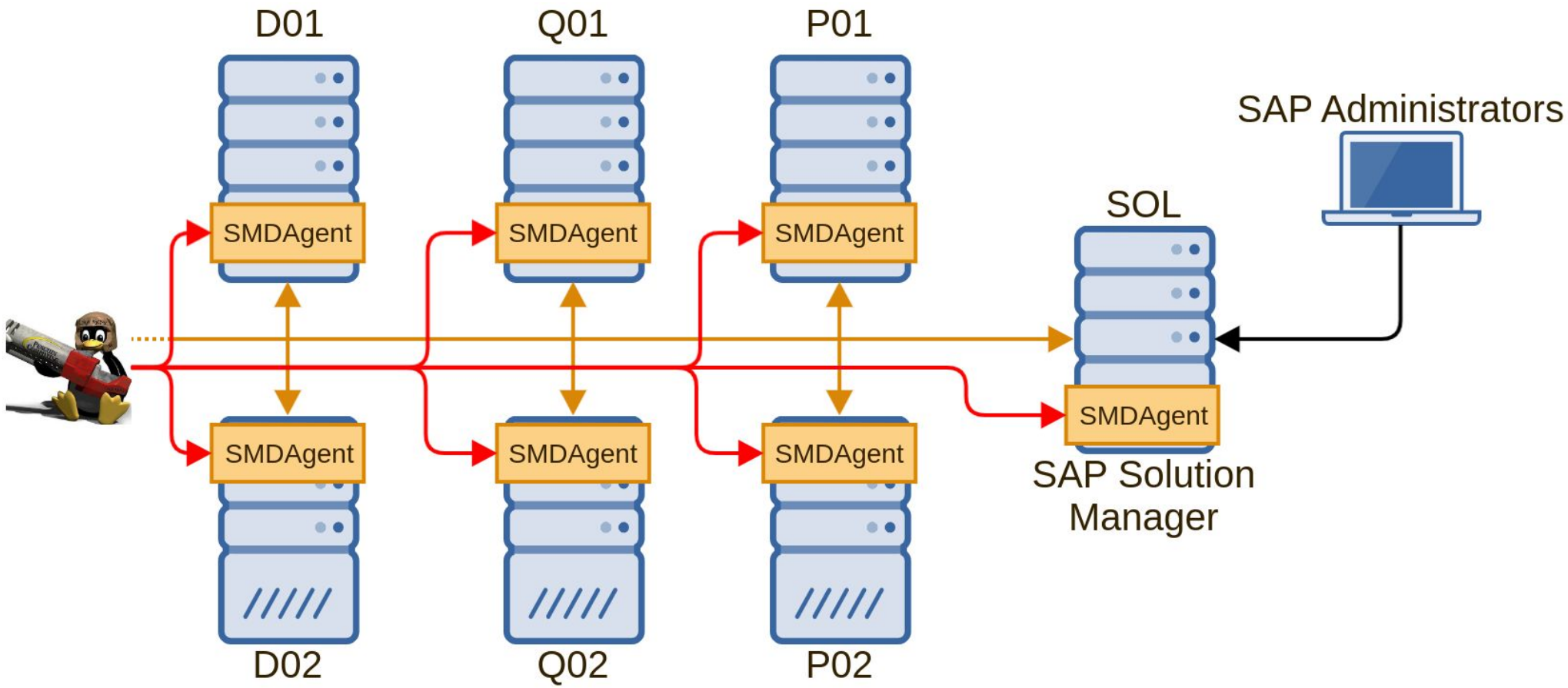
Un SAP pour les gouverner tous



Introduction - SMDAgent



Introduction - SMDAgent

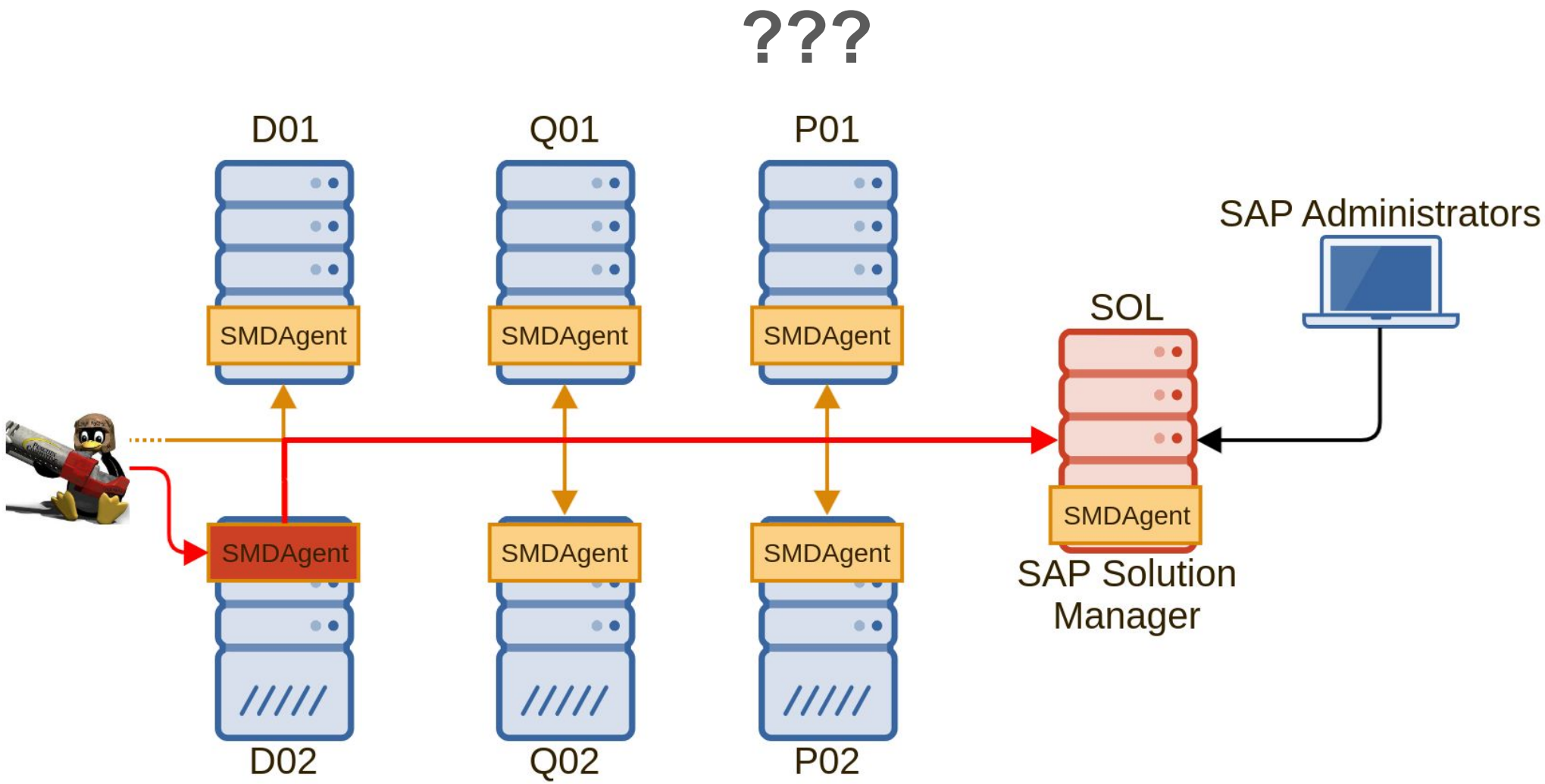


Introduction - SMDAgent

- Si cet agent est compromis, que puis-je faire ?

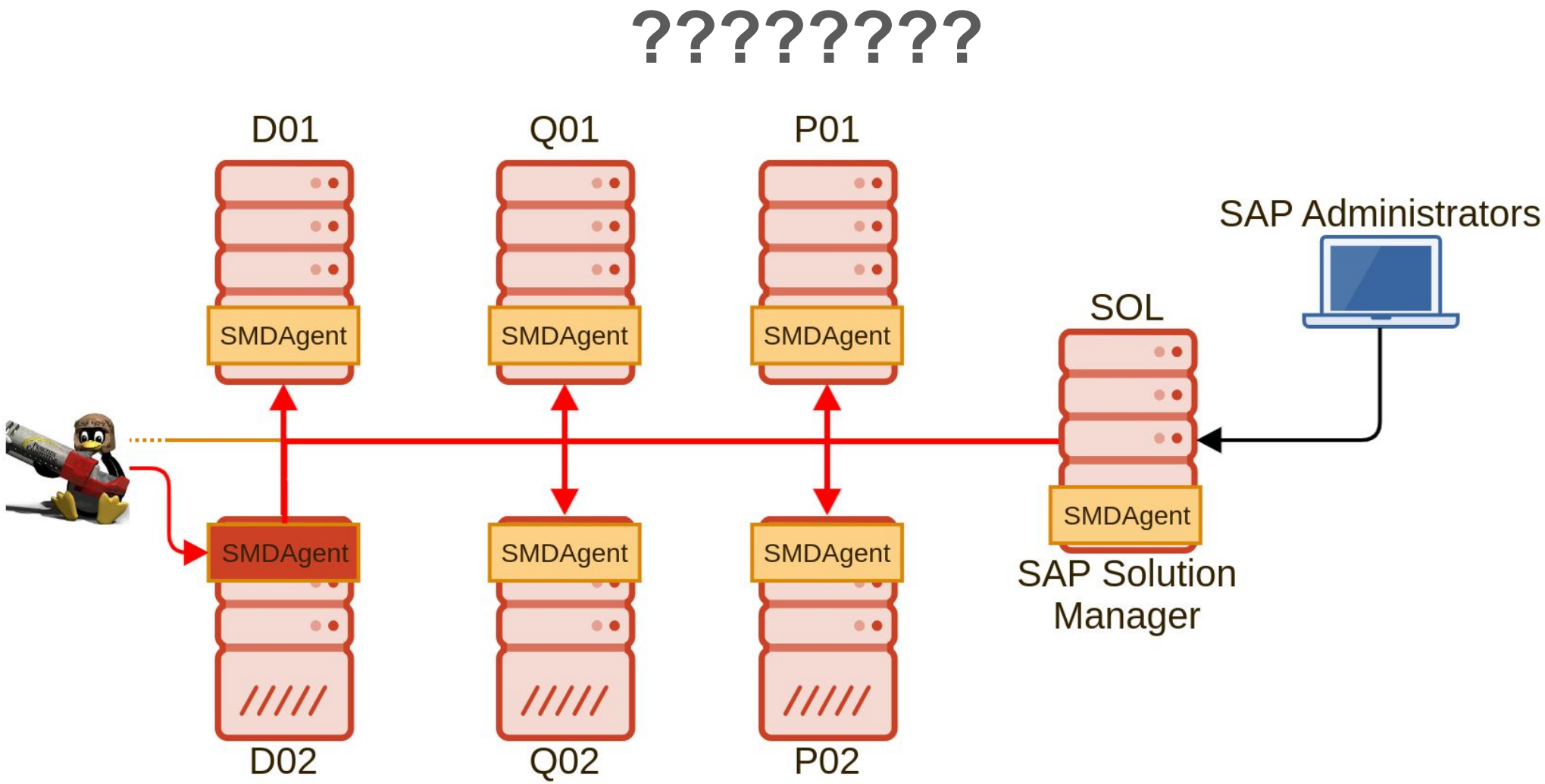
- Cet agent pourrait-il être un point d'entrée pour attaquer le Solman ?

Introduction - SMDAgent



onapsis

Introduction - SMDAgent



onapsis

1. Introduction
2. **Premier contact**
3. Echec du “SAP Secure Storage”
4. Le service P4
5. Contournement d’authentification
6. Exécution de commande
7. Contre-mesures
8. Conclusion

Premier contact

- Petit système SAP, sans base de données
- SID = DAA
- SN = 98

```
/usr/sap/DAA/SYS
/usr/sap/DAA/SYS/global                    # Répertoire global
/usr/sap/DAA/SYS/profile                   # Fichiers de configuration de l'instance
/usr/sap/DAA/SMD98                         # Répertoire de l’instance
/usr/sap/DAA/SMD98/work                    # Traces et logs
/usr/sap/DAA/SMD98/exe                     # Noyau
```

Premier contact

- Mais avec un répertoire spécifique : SMDAgent

```
/usr/sap/DAA/SMDAgent                          # Répertoire de l'agent
/usr/sap/DAA/SMDAgent/configuration            # Fichiers de configuration de l'agent
/usr/sap/DAA/SMDAgent/applications             # Applications de l'agent
/usr/sap/DAA/SMDAgent/applications.config      # Configuration des applications
```

Premier contact

- Répertoire des applications
- 36 applications par défaut

```
/usr/sap/DAA/SMDAgent/applications
[...]
./com.sap.smd.agent.application.sapstartsrv.remote_7.20.8.0.20181204114919
./com.sap.smd.agent.application.remoteos_7.20.8.0.20181204114919
./com.sap.smd.agent.application.global.configuration_7.20.8.0.20181204114919
./com.sap.smd.agent.application.remotesetup_7.20.8.0.20181204114919
./com.sap.smd.agent.application.wily_7.20.8.0.20181204114919
[...]
```

Premier contact

- Répertoire de configuration des applications

```
/usr/sap/DAA/SMDAgent/applications.config
[...]
./com.sap.smd.agent.application.sapstartsrv.remote
./com.sap.smd.agent.application.remoteos
./com.sap.smd.agent.application.global.configuration
./com.sap.smd.agent.application.remotesetup
./com.sap.smd.agent.application.wily4java
[...]
```

Premier contact

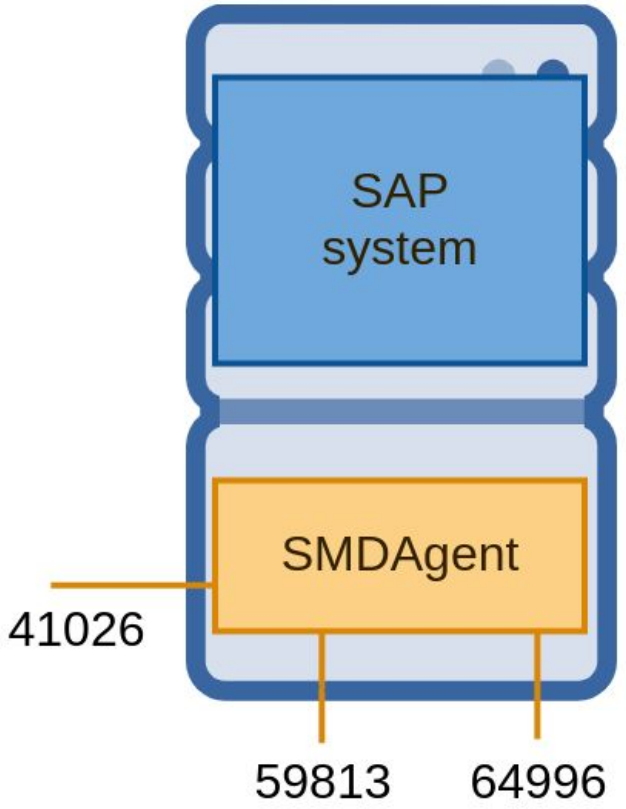
- Répertoire de configuration des applications
- Tous les fichiers sont chiffrés

```
# xxd _Default_Configuration.properties
0000000: 85f3 35e1 fcf7 0e18 36a8 cf69 e5eb a403  ..5.....6..i....
0000010: 2d0a 893a 1ade 0730 a64a 6b4a d0af fe05  -..:...0.JkJ....
0000020: ed29 4ffe 8165 fab5 9172 bfad dfd7 5a3a  .)O..e...r....Z:
0000030: 29ef 06f0 8108 4076 d2e5 7b40 2093 b1ba  ).....@v..{@ ...
0000040: e2d1 17ce d52c c1fa ac0f 9314 334a 4494  .....,......3JD.
0000050: 1ac4 d468 a9a2 9e49 4b9c 8b5d e9b8 9651  ...h...IK..]...Q
0000060: 83ba e3c0 1557 1922 7da5 e302 f236 5182  .....W.}....6Q.
0000070: 0122 4b8d 2b5e bc20 bd55 5227 c381 5441  .K.+^. .UR'..TA
0000080: cc70 a33a 5ff1 0c82 3efa b73b 2d6e e4ef  .p.:_...>..;-n..
0000090: 0dc6 1679 b607 eb88 96f8 c738 47c3 3ff7  ...y.......8G.?.
```


onapsis

Premier contact

- Un seul utilisateur : **daaadm**
- Propriétaire des services exposés :



onapsis

Premier contact

Port	Pattern	Binaire	Description
59813	5<SN>13	sapstartsrv	SAP Management Console
64996	6499<x>	jc.sapDAA_SMDA98	Communication interne
41026	<random>	jstart	Non documenté

Premier contact

Port	Pattern	Binaire	Description
59813	5<SN>13	sapstartsrv	SAP Management Console
64996	6499<x>	jc.sapDAA_SMDA98	Communication interne
41026	**<random>**	**jstart**	**Non documenté**

1. Introduction
2. Premier contact
3. **Echec du “SAP Secure Storage”**
4. Le service P4
5. Contournement d’authentification
6. Exécution de commande
7. Contre-mesures
8. Conclusion

Echec du “SAP Secure Storage”

- “SAP Secure Storage” est un composant présent sur chaque système SAP
- Stocke des clés, des mots de passe ou toute information importante
- Chiffré (normalement...)

Echec du “SAP Secure Storage”

- /usr/sap/DAA/SMDA98/SMDAgent/configuration/secstore.properties
- Seul l'utilisateur administrateur <sidadm> [daaadm] peut y accéder...

```
#SAP Secure Store file - Don't edit this file manually!
#Tue Oct 29 21:40:22 ART 2019
$internal/mode=Not encrypted
$internal/version=Ny4wMC4wMDAuMDAx
sld/usr=amF2YS5sYW5nLlN0cmluZ3w4fHNhcGFkbWluJCQkJCQkJCQkJCQkCg\=\=
sld/pwd=amF2YS5sYW5nLlN0cmluZ3wxNHx3UThjW2VYN3BkNGp+RiQkJCQkJAo\=
smd/agent/crypto/algo=amF2YS5sYW5nLlN0cmluZ3wxMXxERVNlZGUoMTY4KSQkJCQkJCQkJA\=\=
smd/agent/secretkey=amF2YS5sYW5nLlN0cmluZ3w0OHwxOTdmODYxZmQzZjE5ODdmODVlYTA3YWI0YWQ2\r\O
TJhMTNiYTE2NDQzYzQ5YmJhODYkJCQkJCQkJCQkJCQ\=
smd/agent/certificate/pass=amF2YS5sYW5nLlN0cmluZ3wzOHx7NUI0RTQ3RjEtNDdGMC1FQzY3LUUxMDAtM
DAw\r\nMEMwQThFMTFDfSQk
```


onapsis

Echec du “SAP Secure Storage”

- /usr/sap/DAA/SMDA98/SMDAgent/configuration/secstore.properties
- Seul l'utilisateur administrateur <sid>adm> [daaadm] peut y accéder...

```
#SAP Secure Store file - Don't edit this file manually!
#Tue Oct 29 21:40:22 ART 2019
$internal/mode=Not encrypted
$internal/version=7.00.000.001
sld/usr=java.lang.String|8|sapadmin$$$$$$$$$$$
sld/pwd=java.lang.String|14|wQ8c[eX7pd4j~F$$$$$$
smd/agent/crypto/algo=java.lang.String|11|DESede(168)$$$$$$$$$
smd/agent/secretkey=java.lang.String|48|197f861fd3f1987f85ea07ab4ad692a13ba16443c49bba86
$$$$$$$$$$$$
smd/agent/certificate/pass=java.lang.String|38|{5B4E47F1-47F0-ED67-A200-124CC4A8E66F}$$
```


onapsis

Echec du “SAP Secure Storage”

- /usr/sap/DAA/SMDA98/SMDAgent/configuration/secstore.properties
- Mais seulement encodé en base64...

```
#SAP Secure S
#Tue Oct 29 2
$internal/mod
$internal/ver
sld/usr=java.
sld/pwd=java.
smd/agent/cry
smd/agent/secretkey=java.lang.String|48|197f861fd3f1987f85ea07ab4ad692a13ba16443c49bba86
$$$$$$$$$$$$
smd/agent/certificate/pass=java.lang.String|38|{5B4E47F1-47F0-ED67-A200-124CC4A8E66F}$$
```

SSN 2772266 CVE-2019-0307

SSN 2745689 CVE-2019-0291

onapsis

Echec du “SAP Secure Storage”

- `/usr/sap/DAA/SMDA98/SMDAgent/configuration/secstore.properties`
- Qu'est-ce que c'est ?

```
#SAP Secure Store file - Don't edit this file manually!
#Tue Oct 29 21:40:22 ART 2019
$internal/mode=Not encrypted
$internal/version=7.00.000.001
sld/usr=java.lang.String|8|sapadmin$$$$$$$$$$$
sld/pwd=java.lang.String|14|wQ8c[eX7pd4j~F$$$$$$
smd/agent/crypto/algo=java.lang.String|11|DESede(168)$$$$$$$$$
smd/agent/secretkey=java.lang.String|48|197f861fd3f1987f85ea07ab4ad692a13ba16443c49bba86
$$$$$$$$$$$$
smd/agent/certificate/pass=java.lang.String|38|{5B4E47F1-47F0-ED67-A200-124CC4A8E66F}$$
```


onapsis

Echec du “SAP Secure Storage”

- Répertoire de configuration des applications
- Tous les fichiers sont chiffrés

```
# xxd _Default_Co
0000000: 85f3 35e                                        i....
0000010: 2d0a 893                                        J....
0000020: ed29 4ff                                        ...Z:
0000030: 29ef 06f                                        @ ...
0000040: e2d1 17c                                        .3JD.
0000050: 1ac4 d46                                        ]...Q
0000060: 83ba e3c                                        .6Q.
0000070: 0122 4b8                                        ..TA
0000080: cc70 a33a 5ff1 0c82 3efa b73b 2d6e e4ef  .p.:_...>..;-n..
0000090: 0dc6 1679 b607 eb88 96f8 c738 47c3 3ff7  ...y.......8G.?.
```

smd/agent/crypto/algo
smd/agent/secretkey

onapsis

Echec du “SAP Secure Storage”

.../com.sap.smd.agent.application.global.configuration/_Default_Configuration.properties

```
#eacd6b5629b21f48361dA8a9201d048ec9bc5d0f3674712d58254da998f7eb00e0966cef4991a
3d7c31261f0d0638eb520645be17e0270cb3b007b99189e599c1b82f322eefb484ce58a3f99f4a
e79d7sf2e39326c81be6a7f3cf70ef2cb6271c938dd7d521f8c1a720331da5183a029a30490dd
eb93d8fe5200a6aad0adabf319e30b22193be09f6ca6614e9167eca7126934e13310d067c0146a
92f124d4SMf4E2H1A3M089e7000e1b590fb8640f6f9e8ae9ba2d8baad432ba72d23724eea6dec5
0edpassword=j1Aw5y5Km5*ahwd42K)a54dz(ybo/esf>eN0=53bb6c9c130ef97b20e38ce36be
a7e4bdpassword=dcq2mUR7eyBea>N1=NrM9cak34/d8d6(2be26#ec1a6f0c7ee24a5fdf1db
e73r4fc7ddef6SMD9RF6873be3225082f6f62b524b7990aa9b97289de8dd70ffd5c778ac0f45be3
ad96wu3ac965d3b3469b58170aca63f51e6635d33f227dc2ee9806ee2eb11729f05f2b5f49e81
490c3bap2admin/pwd=Q6c4eX7pdg6P49fc46a6669f396d5087fc4dc6b6b8835dc30f12aa2b0
c74/37db2admin2ue3d=SAP9M5Nc35c8331ceb16c444599910853d3e76c5381b2e80d5f83eb0f
4b4fabapf31ee13=93d025f5d06fd3053a3345bf8fa41d742f6ba07aeab162810f62d7e82ebd33
0741/86bc72bdpwd=C4a2&Vga944c5a3866efe67fccbf23dae910c4a849933efe0c868b05f669
cc0c7bep6d854e117SMDA2NT1Sf275032e353eecb51f769d1b88ffd991bf0444d57c51a6cd27
b08dadc62a5bc890e80f975509150000b4dd950c0e67c89a3e91220d4c9bb6cf9067612063bf001
e2e.mai.password=0(X(5$76k9&7Fcfd5&de3ed0w2f6'3qd487bBG3F953e0e52b6b7653ec47
e2e.mai.user=SMfEXTERN9Wd45b200dde57aad90e11f0f4447d8cd59de0f3acf1500e9f0504fc
e2e.maiIntern.password=5(d9abJs<&*5!d-w(~49cXK2X-pUJ4bHZF_.Th8
e2e.maiIntern.user=SM_INTERN_WS
```

Echec du “SAP Secure Storage”

.../com.sap.smd.agent.application.global.configuration/_Default_Configuration.properties

```
#Tue Oct 29 21:40:21 ART 2019
BW/client=001
BW/host=solman.orl.onapsis.com
BW/sysnum=00
BW/user=SM_TECH_ADM
BW/password=j^Aw<y^EmT*?_hwoc}8K)R>u`z{ybo/~so>&N'=Z
BW/rfc/password=-Fcq2&mUR7yyBS2=>N5=NrMSzuk^/U6HJ((tb2%\#
BW/rfc/user=SMD_RFC
BW/ownSystem=false
I74/abap/admin/pwd=wQ8c[eX7pd4j~F
I74/abap/admin/user=SAPADMIN
I74/abap/client=000
I74/abap/com/pwd=C'un4%Vy4`
I74/abap/com/user=SMDAGENT_S72
dcc.url=http\://solman.com\:50000/sap/bc/srt/scs/sap/e2e_dcc_push?sap-client\=001
e2e.mai.password=\=X\#\=&k%&JFC]d\\;^}CeJUwst8'_qd4-d_bBG3F95
e2e.mai.user=SM_EXTERN_WS
e2e.maiIntern.password=56{Y90DJs<&*5!d-w(~49cXK2X-pUJ4bHZF_.Th8
e2e.maiIntern.user=SM_INTERN_WS
```

Echec du “SAP Secure Storage”

.../com.sap.smd.agent.application.global.configuration/_Default_Configuration.properties

```
#Tue Oct 29 21:40:21 ART 2019
BW/client=001
BW/host=solman.orl.onapsis.com
BW/sysnum=00
BW/user=SM_TECH_ADM
BW/password=j^Aw<y^EmT*?_hwoc}8K)R>u`z{ybo/~so>&N'=Z
BW/rfc/password=-Fcq2&mUR7yyBS2=>N5=NrMSzuk^/U6HJ((tb2%\#
BW/rfc/user=SMD_RFC
BW/ownSystem=false
I74/abap/admin/pwd=wQ8c[eX7pd4j~F
I74/abap/admin/user=SAPADMIN
I74/abap/client=000
I74/abap/com/pwd=C'un4%Vy4`
I74/abap/com/user=SMDAGENT_S72
dcc.url=http\://solman.com\:50000/sap/bc/srt/scs/sap/e2e_dcc_push?sap-client\=001
e2e.mai.password=\=X\#\=&k%&JFC]d\\;^}CeJUwst8'_qd4-d_bBG3F95
e2e.mai.user=SM_EXTERN_WS
e2e.maiIntern.password=56{Y90DJs<&*5!d-w(~49cXK2X-pUJ4bHZF_.Th8
e2e.maiIntern.user=SM_INTERN_WS
```

Echec du “SAP Secure Storage”

.../com.sap.smd.agent.application.global.configuration/_Default_Configuration.properties

```
#Tue Oct 29 21:40:21 ART 2019
BW/client=001
BW/host=solman.orl.onapsis.c
BW/sysnum=00
BW/user=SM_TECH_ADM
BW/password=j^Aw<y^EmT*?_hwo
BW/rfc/password=-Fcq2&mUR7yy
BW/rfc/user=SMD_RFC
BW/ownSystem=false
I74/abap/admin/pwd=wQ8c[eX7pd4j~F
I74/abap/admin/user=SAPADMIN
I74/abap/client=000
I74/abap/com/pwd=C'un4%Vy4`
I74/abap/com/user=SMDAGENT_S72
dcc.url=http\://solman.com\:50000/sap/bc/srt/scs/sap/e2e_dcc_push?sap-client\=001
e2e.mai.password=\=X\#\=&k%&JFC]d\\;^}CeJUwst8'_qd4-d_bBG3F95
e2e.mai.user=SM_EXTERN_WS
e2e.maiIntern.password=56{Y90DJs<&*5!d-w(~49cXK2X-pUJ4bHZF_.Th8
e2e.maiIntern.user=SM_INTERN_WS
```

Role Assignments

Stat...	Role	Short Role Description	Ind...
	SAP_J2EE_ADMIN	Administration User for the SAP J2EE Engine	
	ZSAP_SM_TECH_ADM	Role for Technical Administrator SM_TECH_ADM (s...	
	ZSAP_SM_USER_ADMIN	Admin Authorization for User Management	

onapsis

Echec du “SAP Secure Storage”

- Si cet agent est compromis, que puis-je faire ?

- Cet agent pourrait-il être un point d'entrée pour attaquer le Solman ?

Echec du “SAP Secure Storage”

- Si cet agent est compromis, que puis-je faire ?
  → **Obtenir l’accès au système SAP**
  → **Récupérer les informations de connexion au Solman**
  → **Obtenir l’accès au Solman**

- Cet agent pourrait-il être un point d'entrée pour attaquer le Solman ?
  → **YES !**

Echec du “SAP Secure Storage”

- **Si** cet agent est compromis, que puis-je faire ?
  → **Obtenir l’accès au système SAP**
  → **Récupérer les informations de connexion au Solman**
  → **Obtenir l’accès au Solman**

- Cet agent pourrait-il être un point d'entrée pour attaquer le Solman ?
  → **YES !**

Le service P4

- "Inception of the SAP Platform's Brain" @ HITB 2012
  - Juan Perez Etchegoyen
- L’agent exposait un service P4 sur 59804

Le service P4

- "Inception of the SAP Platform's Brain" @ HITB 2012
  - Juan Perez Etchegoyen
- L'agent exposait un service P4 sur 59804

- Maintenant le service P4 écoute sur :
  → **un port aléatoire entre [9000 - 65535]**
  → **change à chaque redémarrage de l'agent**

Le service P4

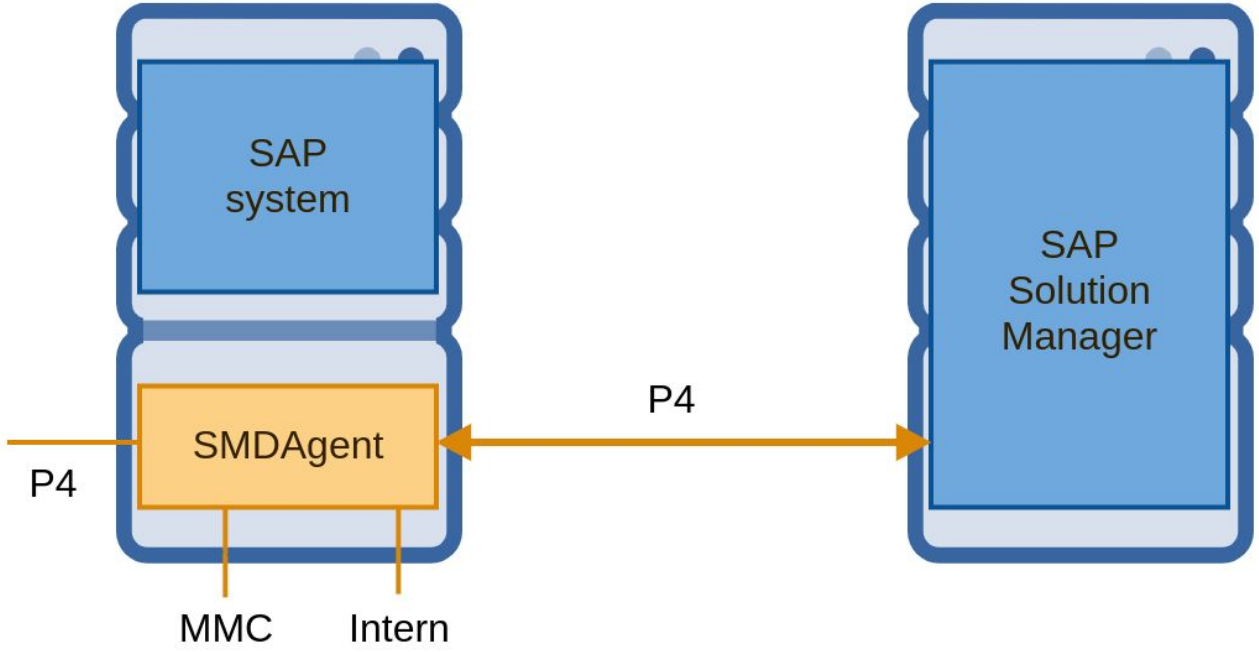
Port	Pattern	Binaire	Description
59813	5<SN>13	sapstartsrv	SAP Management Console
64996	6499<x>	jc.sapDAA_SMDA98	Communication interne
41026	**<random>**	**jstart**	**Non documenté**

Le service P4

Port	Pattern	Binaire	Description
59813	5<SN>13	sapstartsrv	SAP Management Console
64996	6499<x>	jc.sapDAA_SMDA98	Communication interne
41026	**9000-65535**	**jstart**	**Service P4**

Le service P4

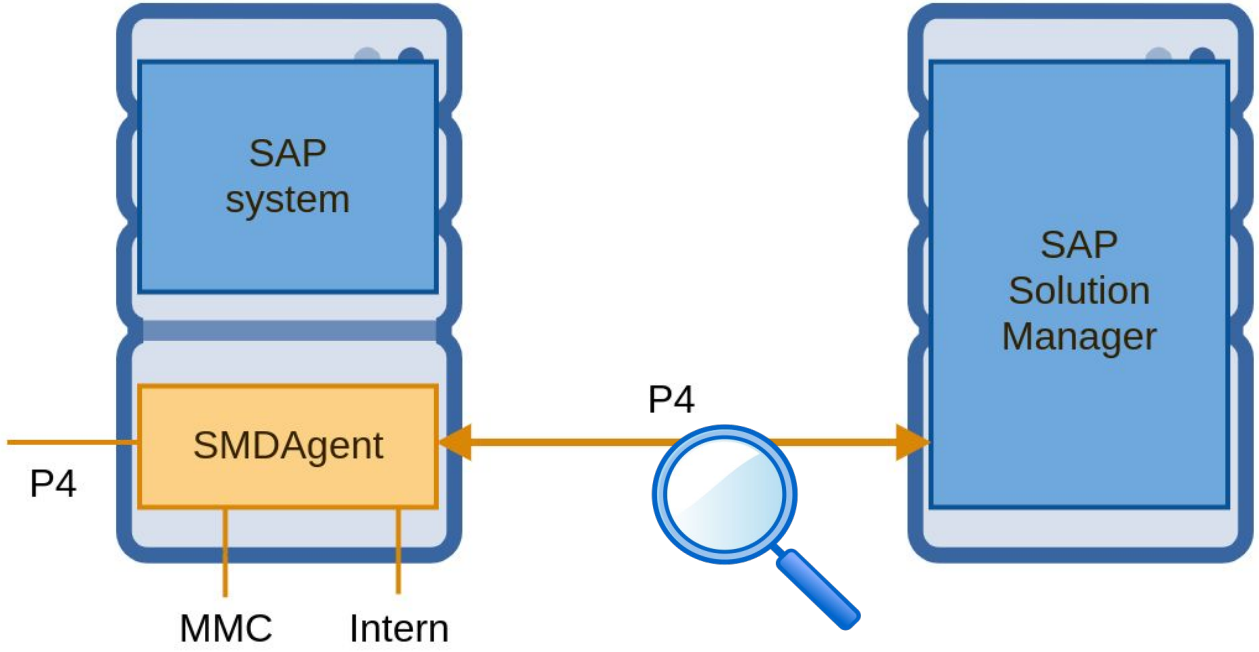
- Juste après le démarrage, l'agent initie une connexion avec son Solman



Le service P4

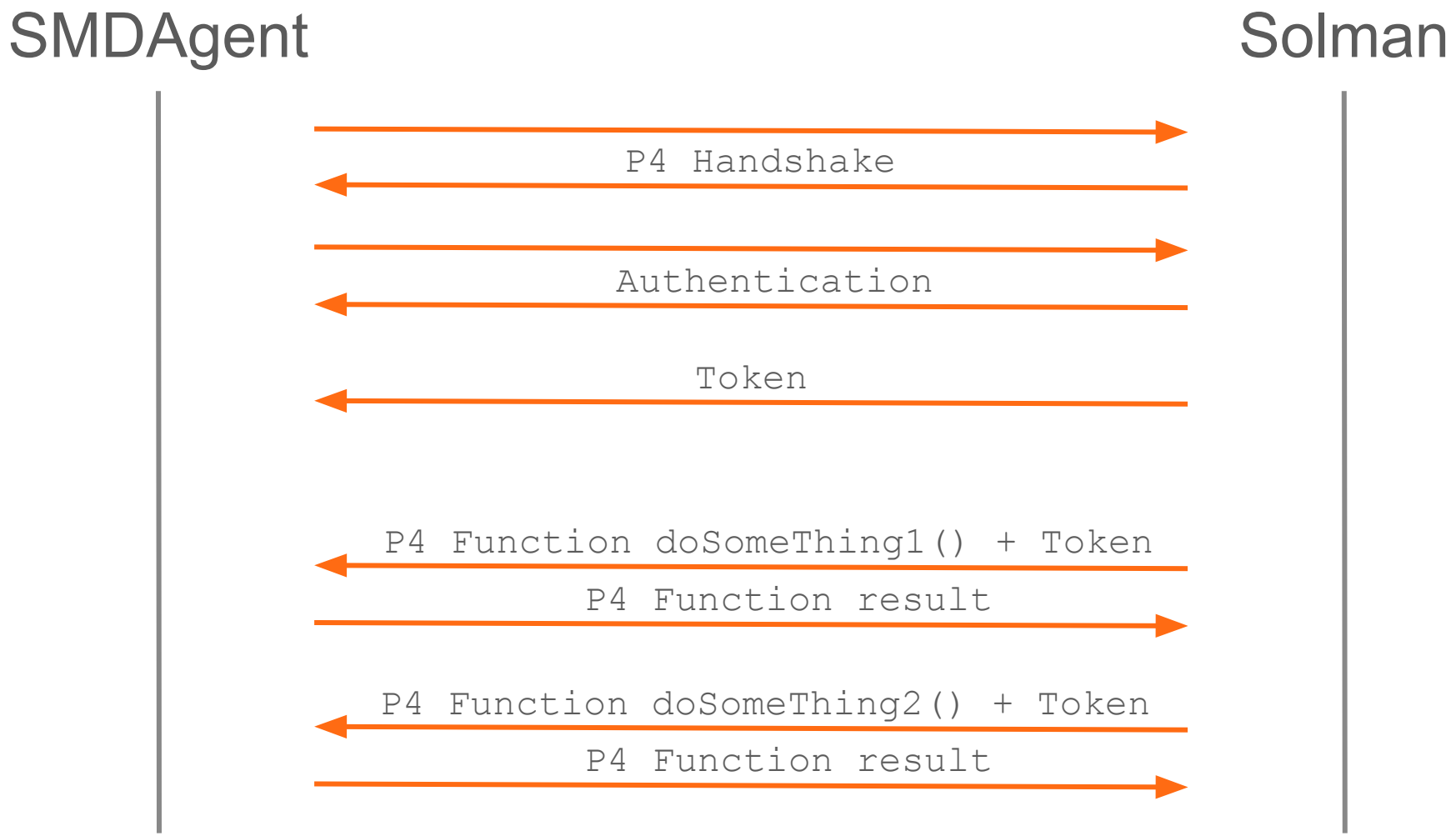
- Cette connexion restera tant que le l'agent sera en service

```
ESTAB     sapsystem:43756     solman:50204     users:((jstart,pid=75393,fd=66))
```



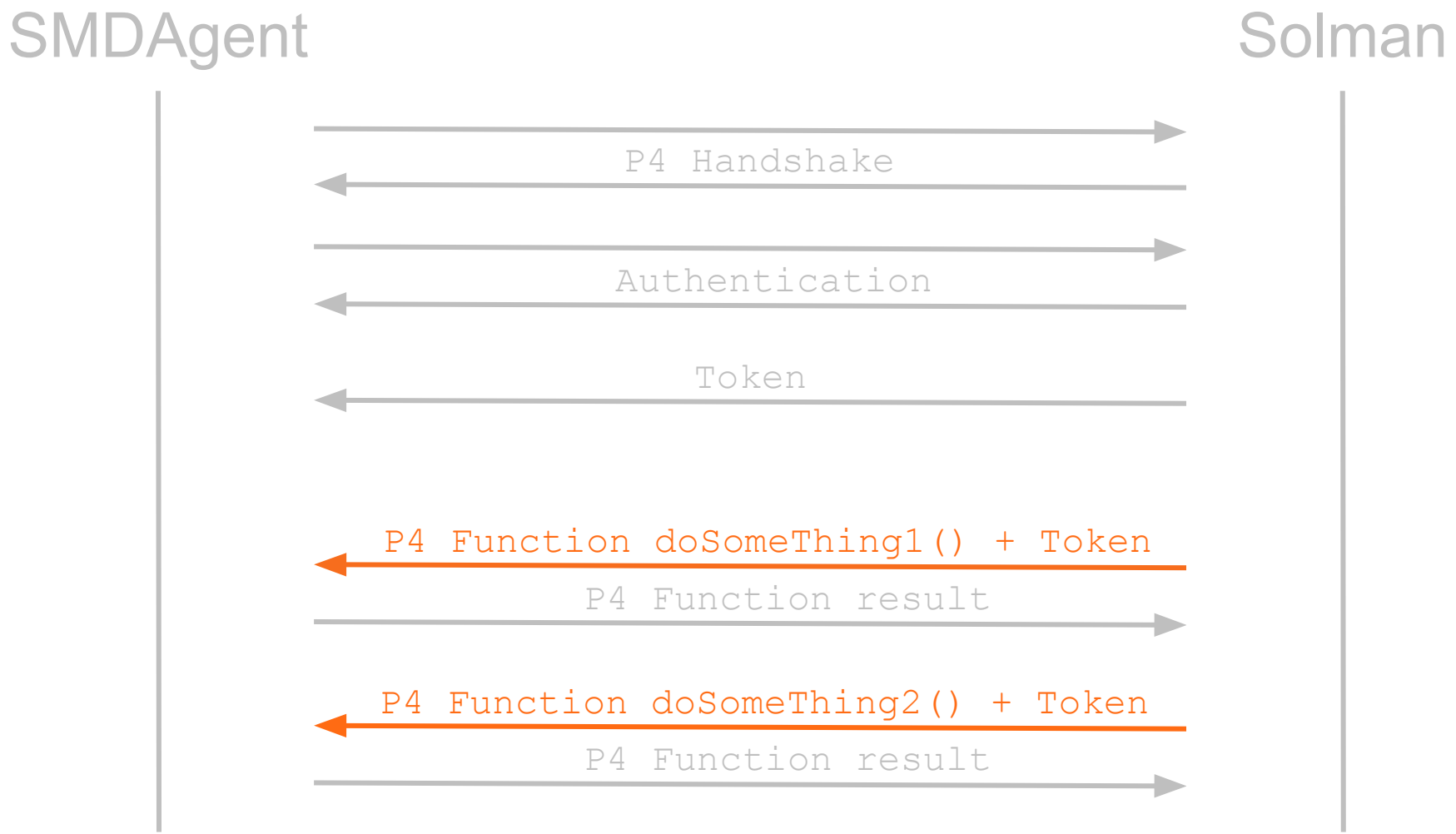
onapsis

Le service P4 - Sniffing



onapsis

Le service P4 - Sniffing



Le service P4 - Reversing

- Exemple : fonction P4 1_p4_getRuntimeStatus() + Token

```
00000000: 0000 4a00 0000 ffff ffff 5a15 8a01 bbbb  ..J.......Z.....
00000010: 0600 0000 005a 0000 0000 0000 1700 0031  .....Z.........1
00000020: 005f 0070 0034 005f 0067 0065 0074 0052  ._.p.4._.g.e.t.R
00000030: 0075 006e 0074 0069 006d 0065 0053 0074  .u.n.t.i.m.e.S.t
00000040: 0061 0074 0075 0073 0028 0029 0000 0050  .a.t.u.s.(.)...P
00000050: 0000 0000 5001 f02d                      ....P..-
```

Le service P4 - Reversing

- Exemple : fonction P4 1_p4_getRuntimeStatus() + Token

```
00000000: 0000 4a00 0000 ffff ffff 5a15 8a01 bbbb  ..J.......Z.....
00000010: 0600 0000 005a 0000 0000 0000 1700 0031  .....Z.........1
00000020: 005f 0070 0034 005f 0067 0065 0074 0052  ._.p.4._.g.e.t.R
00000030: 0075 006e 0074 0069 006d 0065 0053 0074  .u.n.t.i.m.e.S.t
00000040: 0061 0074 0075 0073 0028 0029 0000 0050  .a.t.u.s.(.)...P
00000050: 0000 0000 5001 f02d                      ....P..-
```

- Packet size
- Solman Header
- Function Name size
- Function Name
- Object ID
- Stub version
- Key

onapsis

Le service P4 - Reversing

- Exemple : fonction P4 1_p4_getRuntimeStatus() + Token

```
00000000: 0000 4a00 0000 ffff ffff 5a15 8a01 bbbb  ..J.......Z.....
00000010: 0600 0000 005a 0000 0000 0000 1700 0031  .....Z.........1
00000020: 005f 0070 0034 005f 0067 0065 0074 0052  ._.p.4._.g.e.t.R
00000030: 0075 006e 0074 0069 006d 0065 0053 0074  .u.n.t.i.m.e.S.t
00000040: 0061 0074 0075 0073 0028 0029 0000 0050  .a.t.u.s.(.)...P
00000050: 0000 0000 5001 f02d                      ....P..-
```

```
00000000: 0000 9300 0000 5a15 8a01 ffff ffff bbbb  ......Z.........
00000010: 0600 0000 005a 012e 0000 0001 0008 0073  .....Z.........s
00000020: 6563 7572 6974 7920 0020 0000 0000 0000  ecurity . ......
00000030: 0000 4a00 3200 4500 4500 5f00 4700 5300  ..J.2.E.E._.G.S.
00000040: 5400 5f00 5300 4f00 4cac ed00 0573 7200  T._.S.O.L....sr.
00000050: 1b63 6f6d 2e73 6170 2e73 6d64 2e61 7069  .com.sap.smd.api
00000060: 2e41 6765 6e74 5374 6174 7573 a91f 68b6  .AgentStatus..h.
00000070: ba21 ac06 0200 014c 0006 6d5f 6e61 6d65  .!.....L..m_name
00000080: 7400 124c 6a61 7661 2f6c 616e 672f 5374  t..Ljava/lang/St
00000090: 7269 6e67 3b78 7074 0007 5354 4152 5445  ring;xpt..STARTE
000000a0: 44                                       D
```


onapsis

Le service P4 - SMDAgent

- Renvoi de ce paquet sur le service P4 de l'agent

1. Introduction
2. Premier contact
3. Echec du “SAP Secure Storage”
4. Le service P4
5. **Contournement d’authentification**
6. Exécution de commande
7. Contre-mesures
8. Conclusion

Contournement d'authentification

- Changements observés après 100+ redémarrages

```
00000000: 0000 4a00 0000 ffff ffff 5a15 8a01 bbbb  ..J.......Z.....
00000010: 0600 0000 005a 0000 0000 0000 1700 0031  .....Z.........1
00000020: 005f 0070 0034 005f 0067 0065 0074 0052  ._.p.4._.g.e.t.R
00000030: 0075 006e 0074 0069 006d 0065 0053 0074  .u.n.t.i.m.e.S.t
00000040: 0061 0074 0075 0073 0028 0029 0000 0050  .a.t.u.s.(.)...P
00000050: 0000 0000 5001 f02d                      ....P..-
```

- Packet size
- Solman Header
- Function Name size
- Function Name

- **Object ID (change)**
- **Stub version (change)**
- **Key (change)**

onapsis

Contournement d'authentification - Object & Version

```
00000000: 0000 4a00 0000 ffff ffff 5a15 8a01 bbbb  ..J.......Z.....
00000010: 0600 0000 005a 0000 0000 0000 1700 0031  .....Z.........1
00000020: 005f 0070 0034 005f 0067 0065 0074 0052  ._.p.4._.g.e.t.R
00000030: 0075 006e 0074 0069 006d 0065 0053 0074  .u.n.t.i.m.e.S.t
00000040: 0061 0074 0075 0073 0028 0029 0000 0050  .a.t.u.s.(.)...P
00000050: 0000 0000 5001 f02d                      ....P..-
```

- Packet size
- Solman Header
- Function Name size
- Function Name

- **Object ID (change)**
- **Stub version (change)**
- Key (change)

onapsis

Contournement d'authentification - Object & Version

- Valeurs observées :

  00 00 00 00 < Object ID < 00 00 00 ff

  00 00 00 00 < Stub version < 00 00 00 05

- Plusieurs messages d'erreur différents :

  "object was not found"

  "incompatible version"

- **255 * 5 = 1275 requètes → Bruteforce à distance possible**

Contournement d'authentification - Key

```
00000000: 0000 4a00 0000 ffff ffff 5a15 8a01 bbbb  ..J.......Z.....
00000010: 0600 0000 005a 0000 0000 0000 1700 0031  .....Z.........1
00000020: 005f 0070 0034 005f 0067 0065 0074 0052  ._.p.4._.g.e.t.R
00000030: 0075 006e 0074 0069 006d 0065 0053 0074  .u.n.t.i.m.e.S.t
00000040: 0061 0074 0075 0073 0028 0029 0000 0050  .a.t.u.s.(.)...P
00000050: 0000 0000 5001 f02d                      ....P..-
```

- Packet size
- Solman Header
- Function Name size
- Function Name
- Object ID (change)
- Stub version (change)
- **Key (change)**

onapsis

Contournement d'authentification - Key

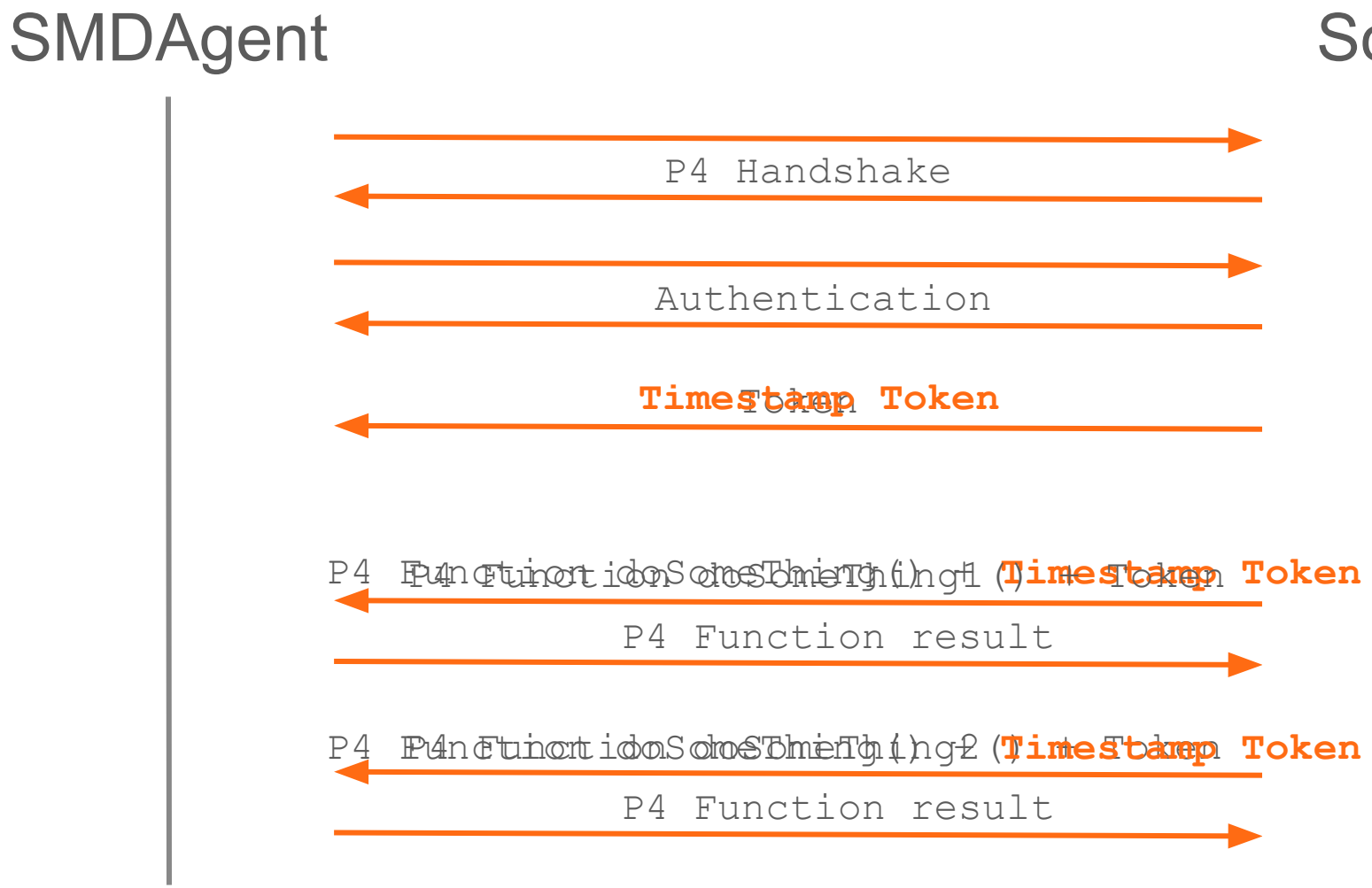
Valeurs	Little endian	Décimal
0xcc1ff02d	0x2df01fcc	770711500
0xad2bf02d	0x2df02bad	770714541
0xfe2bf02d	0x2df02bfe	770714622
0x7a2cf02d	0x2df02c7a	770714746
0x1a2df02d	0x2df02d1a	770714906
0xde3bf02d	0x2df03bde	770718686
0xe83bf02d	0x2df03be8	770718696

TEMPS

En fait c'est un Timestamp

onapsis

Contournement d'authentification - Timestamp key



onapsis

Contournement d'authentification - tl;dr

Si on connaît l'heure de démarrage de l'agent

=> Contournement d'authentification possible !

Contournement d'authentification - Heure de démarrage

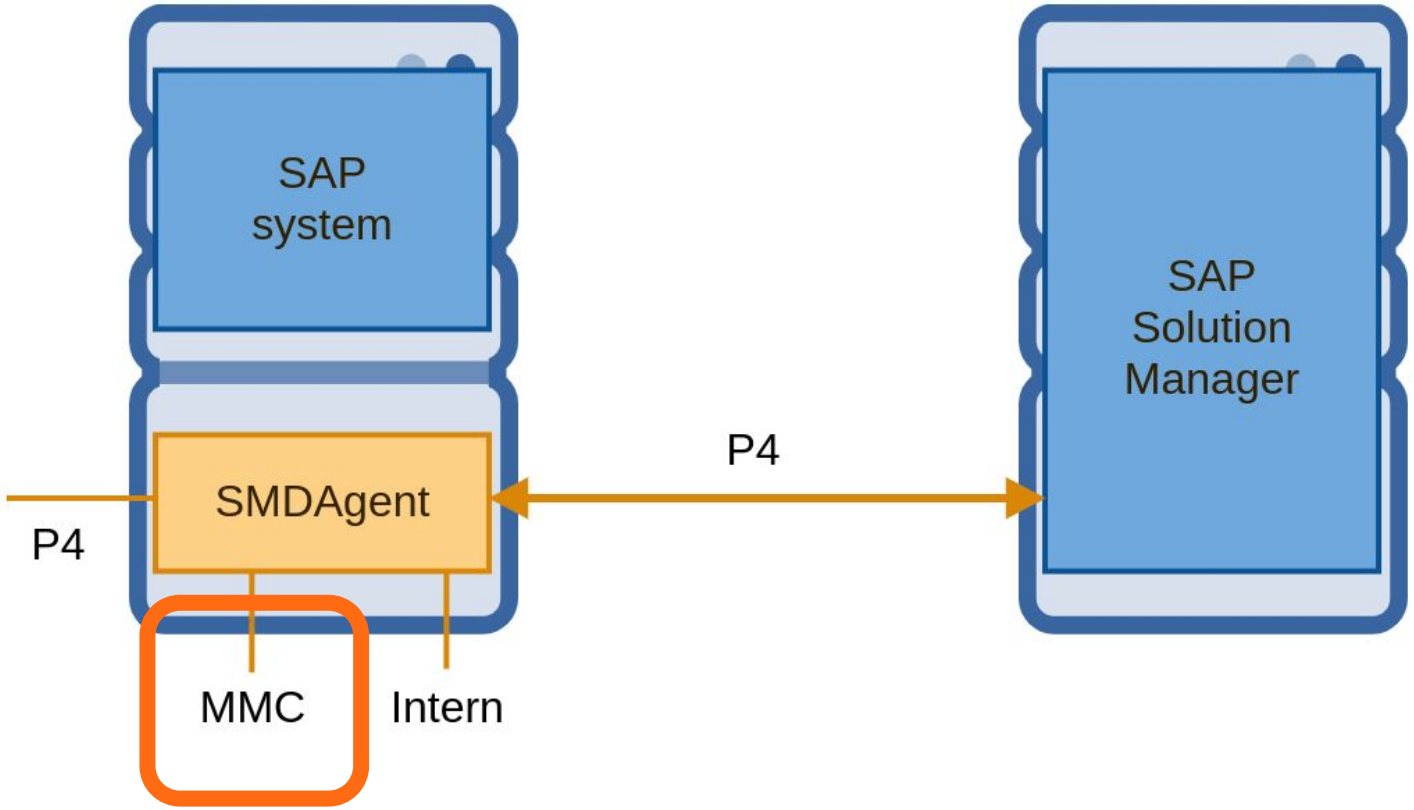
Comment connaître, **à distance**, l'heure du démarrage de l'agent ?

- ~~Guess ?~~
- ~~Déni de service à distance ?~~
  ~~…fail~~
- **Il suffit de demander... au SAP MC sur le 59813 !**

Contournement d’authentification - Heure de démarrage

- 86 web services
- 6 ‘unprotected’

```
AccessCheck
GetInstanceProperties
GetNetworkId
GetProcessList
GetSecNetworkId
GetSystemInstanceList
```

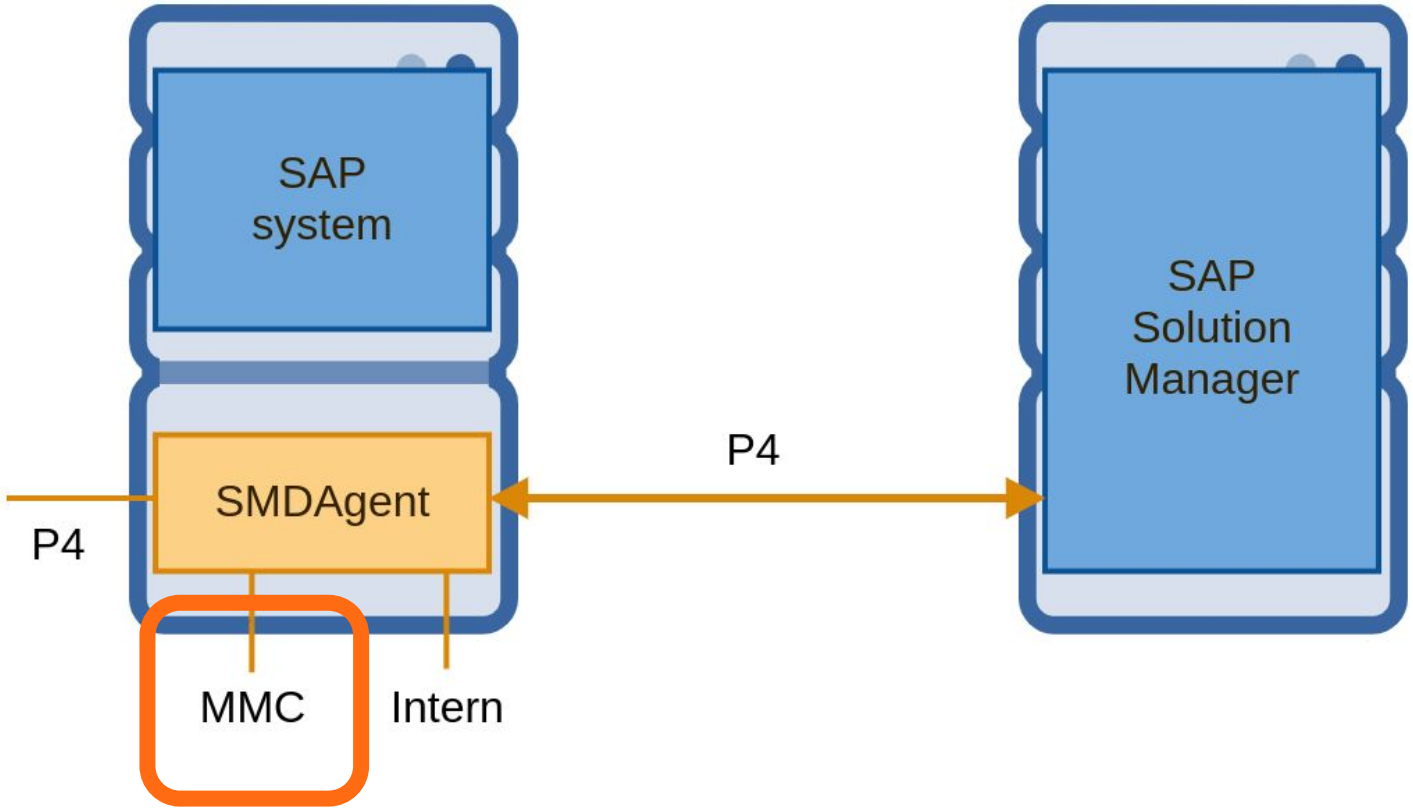


onapsis

Contournement d'authentification - Heure de démarrage

- 86 web services
- 6 'unprotected'

```
AccessCheck
GetInstanceProperties
GetNetworkId
GetProcessList
GetSecNetworkId
GetSystemInstanceList
```



onapsis

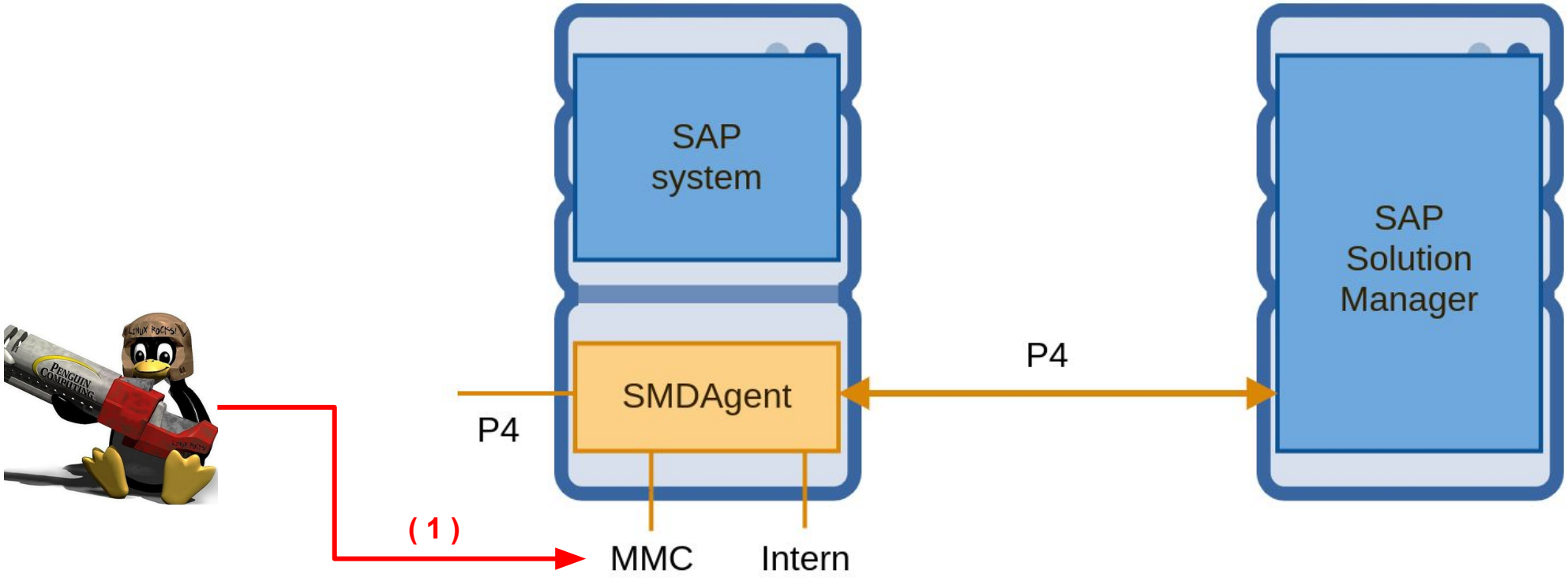
Contournement d'authentification - Heure de démarrage

```
<SOAP-ENV:Body>
  <SAPControl:GetProcessListResponse>
    <process>
      <item>
        <name>jstart</name>
        <description>J2EE Server</description>
        <dispstatus>SAPControl-GREEN</dispstatus>
        <textstatus>All processes running</textstatus>
        <starttime>2019 10 29 07:04:12</starttime>
        <elapsedtime>48:37:22</elapsedtime>
        <pid>38924</pid>
      </item>
    </process>
  </SAPControl:GetProcessListResponse>
</SOAP-ENV:Body>
```


onapsis

Contournement d'authentification - Attaque

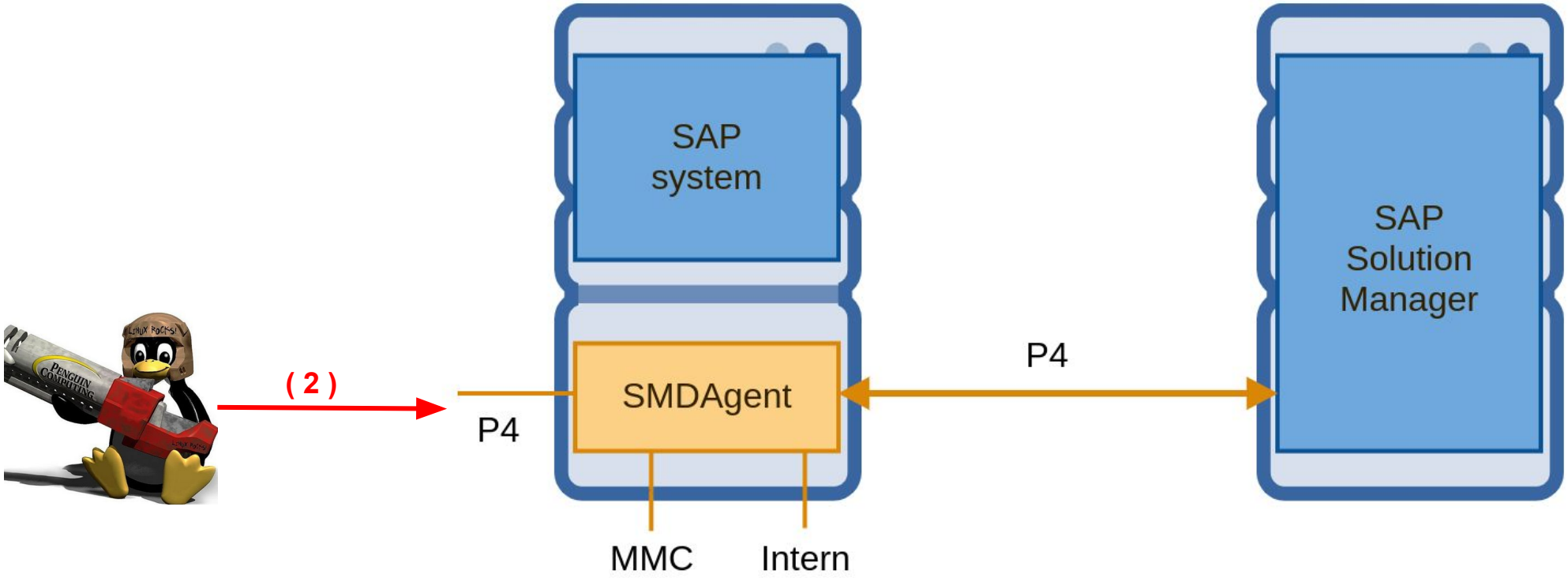
(1) Récupération de la date et l'heure de démarrage via la SAP MC



onapsis

Contournement d'authentification - Attaque

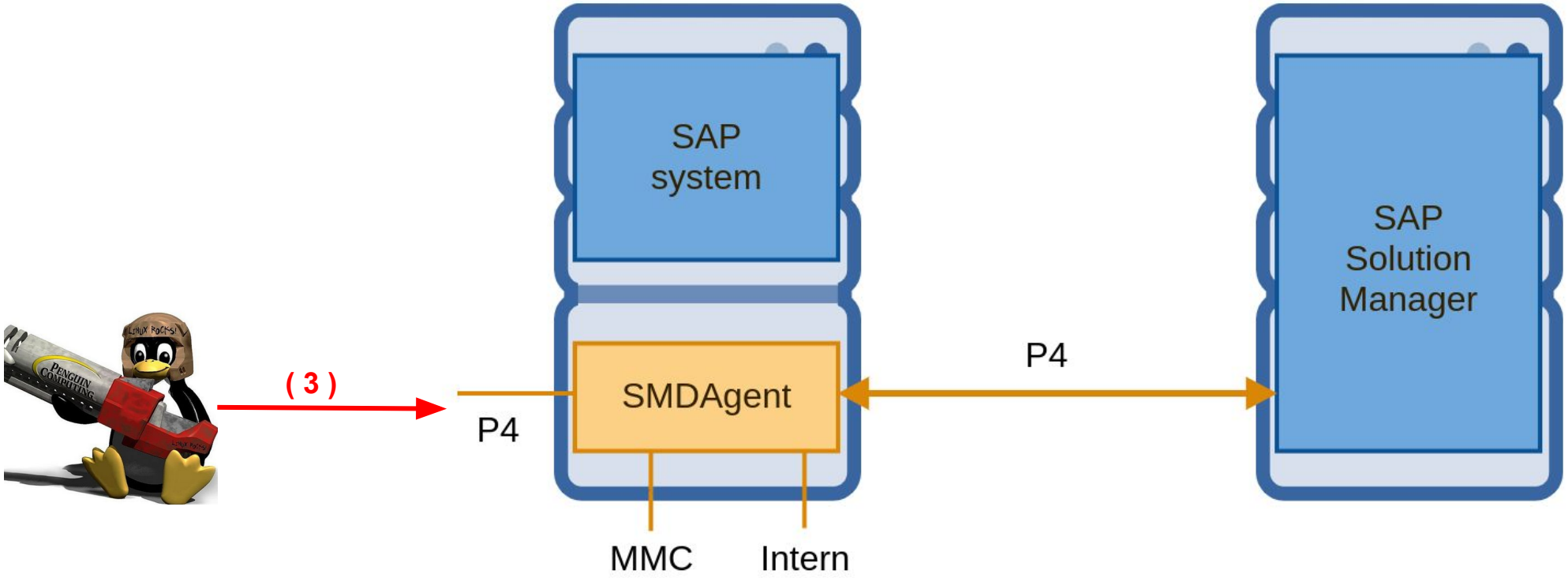
(2) Bruteforce de la token : 'Timestamp Key'



onapsis

Contournement d'authentification - Attaque

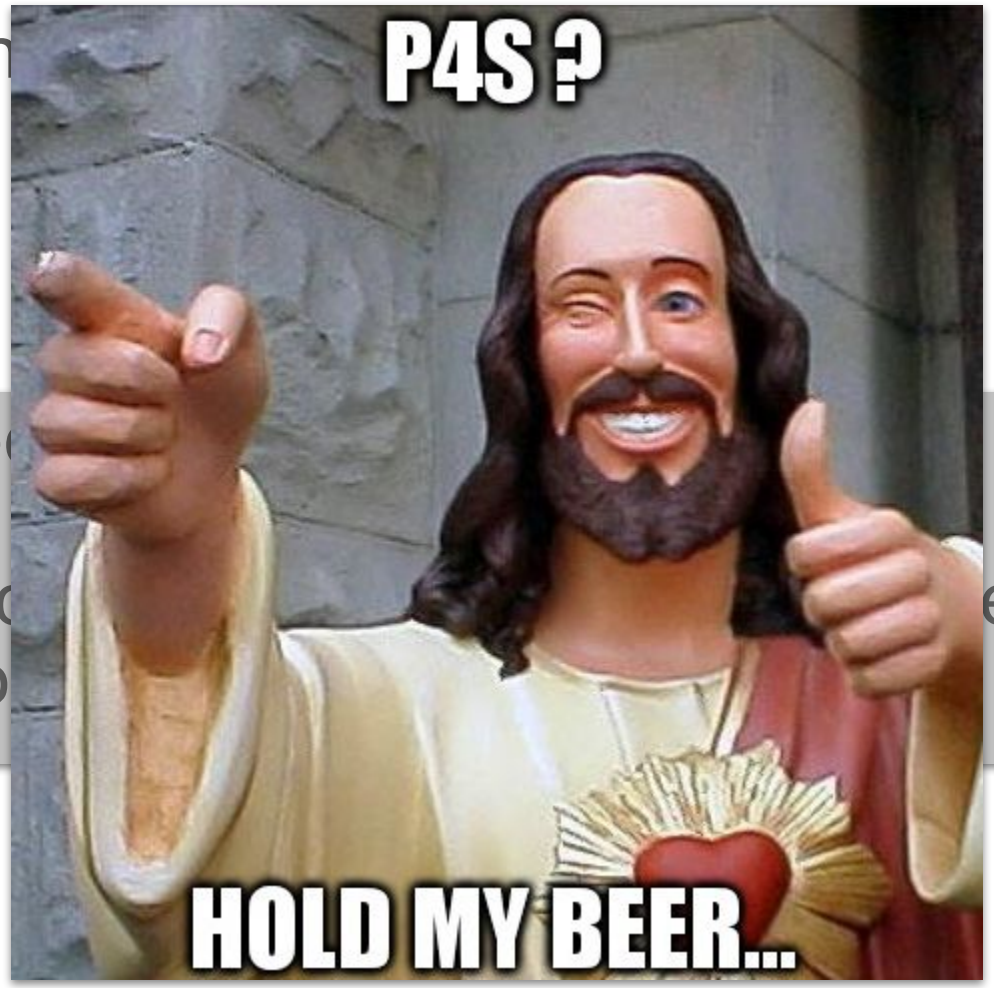
(3) Bruteforce de la token : 'Object ID' et 'Stub version'



onapsis

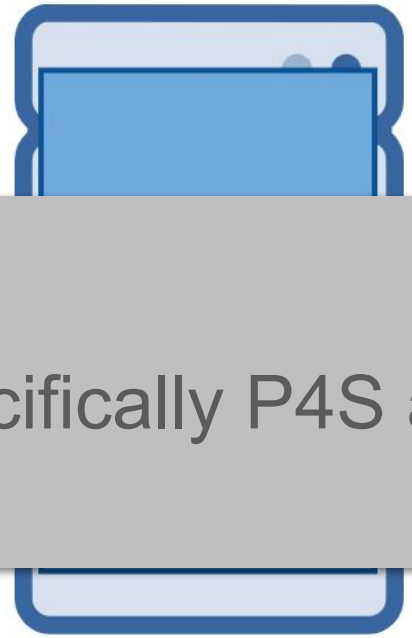
Contournement d’authentification - Attaque

(4) Exécution de fon



“Vulnerability reje

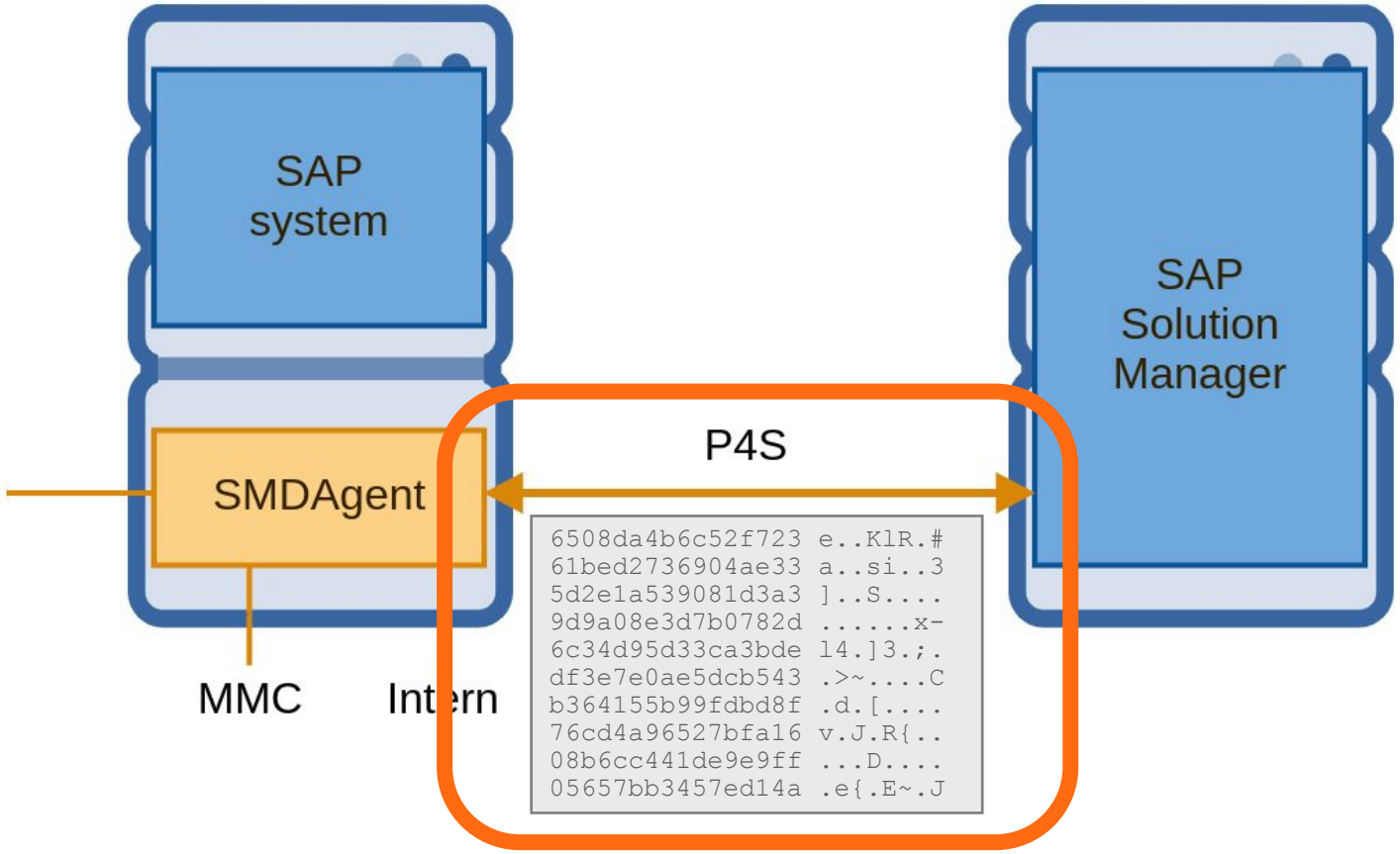
The vulnerability c ecifically P4S and not P4) is used fo



onapsis

Contournement d'authentification - Attaque P4S

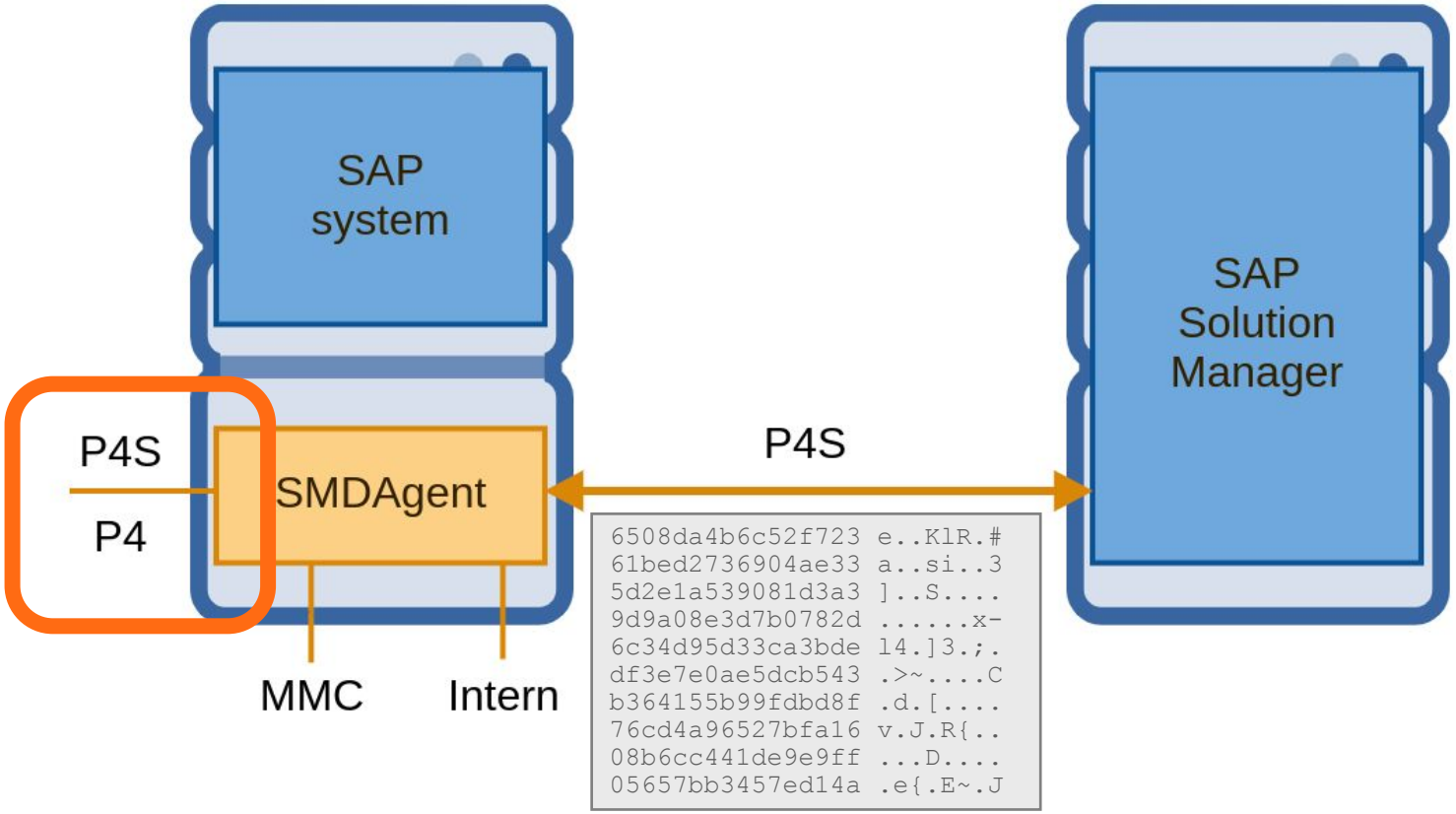
- Même si P4S est utilisé pour la communication entre l'agent et le solman



onapsis

Contournement d'authentification - Attaque P4S

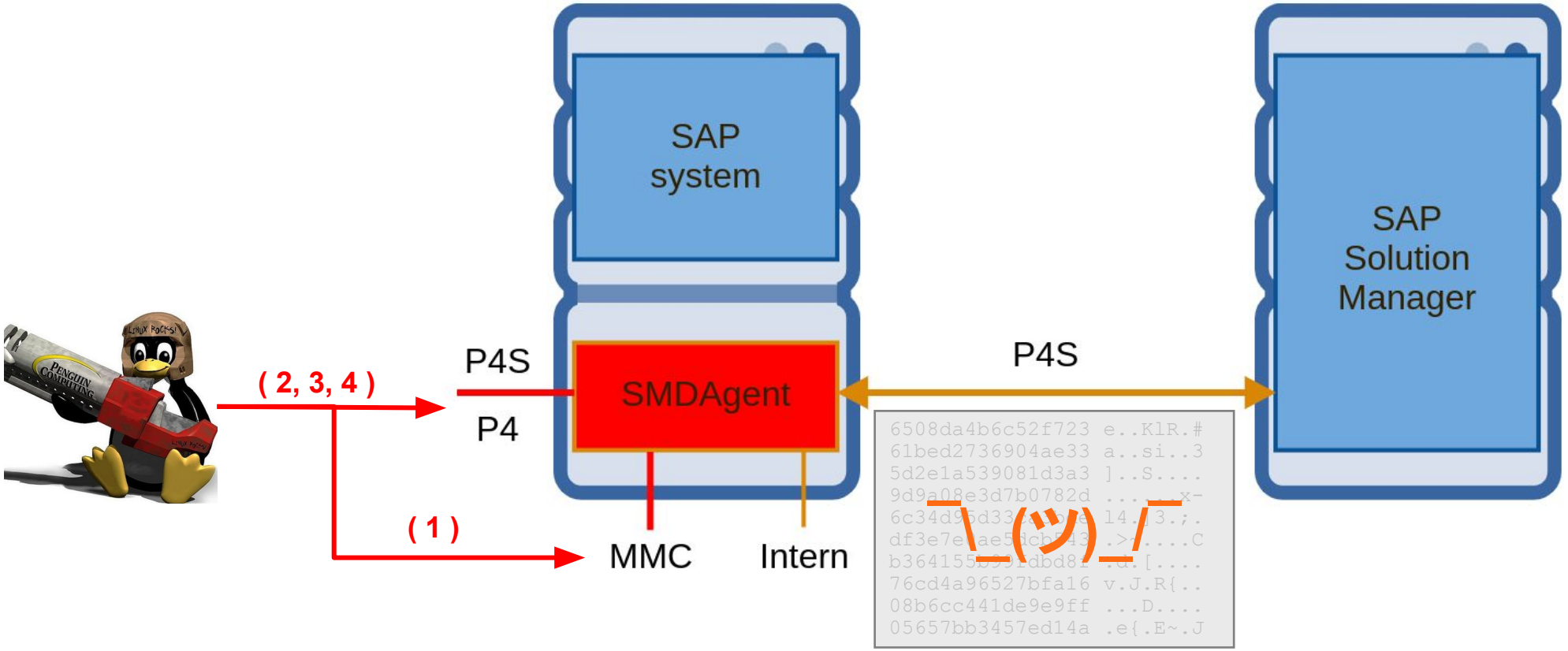
- Le service sur l'agent accepte **à la fois** les communication P4S et P4



onapsis

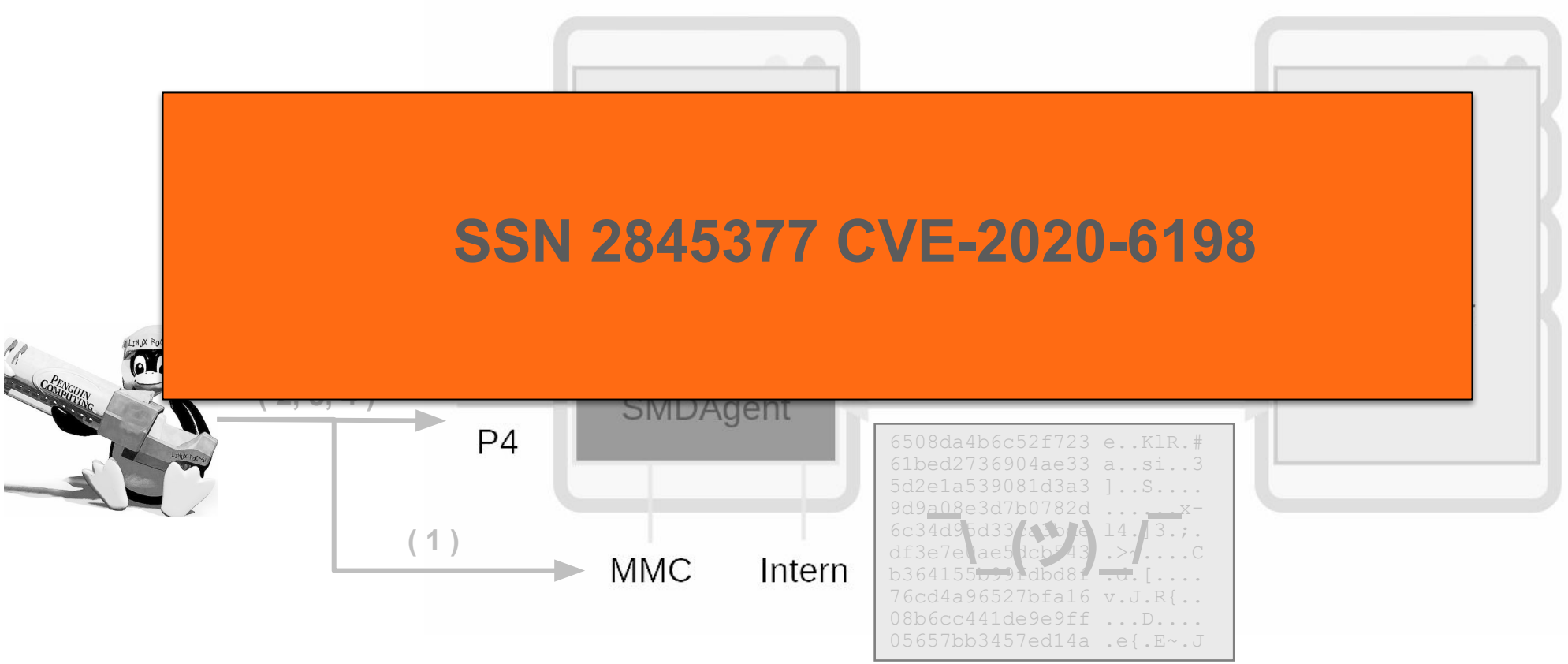
Contournement d'authentification - Attaque P4S

- L'attaque reste exactement la même



Contournement d’authentification - Attaque P4S

- L'attaque reste exactement la même



1. Introduction
2. Premier contact
3. Echec du “SAP Secure Storage”
4. Le service P4
5. Contournement d’authentification
6. **Exécution de commande**
7. Contre-mesures
8. Conclusion

Exécution de commande

- Parmis toute les applications de l'agent :
  com.sap.smd.agent.application.remoteos

- `ps find echo ping traceroute vmstat iostat df…`

- Cette 'liste blanche' de commandes est contrôlée par le fichier de configuration suivant :

`SMDAgent/applications/com.sap.smd.agent.application.remoteos/smd.config/commands.xml`

onapsis

Exécution de commande

- Exemple avec ping

```
...
<Cmd key="os.ping" name="Ping" desc="Verifies IP-level connectivity to
another TCP/IP computer.">
  <OsCmd ostype="WINDOWS" exec="ping" path="" param="true" runtime="60">
    <Exclude param="^-t$"/>
    <Help ref="help.os.ping"/>
  </OsCmd>
  <OsCmd ostype="UNIX" exec="ping -c 4" path="" param="true"
runtime="60">
    <Exclude param="^-(f|l)$"/>
    <Help ref="help.os.ping"/>
  </OsCmd>
</Cmd>
...
```

Exécution de commande

- Exemple avec ping

```
...
<Cmd key="os.ping" name="Ping" desc="Verifies IP-level connectivity to
another TCP/IP computer.">
  <OsCmd ostype="WINDOWS" exec="ping" path="" param="true" runtime="60">
    <Exclude param="^-t$"/>
    <Help ref="help.os.ping"/>
  </OsCmd>
  <OsCmd ostype="UNIX" exec="ping -c 4" path="" param="true"
runtime="60">
    <Exclude param="^-(f|l)$"/>
    <Help ref="help.os.ping"/>
  </OsCmd>
</Cmd>
...
```


onapsis

Exécution de commande

- Exemple avec ping

```
...
<Cmd key="os.ping" name="Ping" desc="Verifies IP-level connectivity to
another TCP/IP computer.">
  <OsCmd ostype="WINDOWS" exec="ping" path="" param="true" runtime="60">
    <Exclude param="^-t$"/>
    <Help ref="help.os.ping"/>
  </OsCmd>
  <OsCmd ostype="UNIX" exec="ping -c 4" path="" param="true"
runtime="60">
    <Exclude param="^-(f|l)$"/>
    <Help ref="help.os.ping"/>
  </OsCmd>
</Cmd>
...
```


onapsis

Exécution de commande

- Exemple avec ping

```
...
<Cmd key="os.ping" name="Ping" desc="Verifies IP-level connectivity to
another TCP/IP computer.">
  <OsCmd ostype="WINDOWS" exec="ping" path="" param="true" runtime="60">
    <Exclude param="^-t$"/>
    <Help ref="help.os.ping"/>
  </OsCmd>
  <OsCmd ostype="UNIX" exec="ping -c 4" path="" param="true"
runtime="60">
    <Exclude param="^-(f|l)$"/>
    <Help ref="help.os.ping"/>
  </OsCmd>
</Cmd>
...
```

Exécution de commande

- Exemple avec ping

```
...
<Cmd key="os.ping" name="Ping" desc="Verifies IP-level connectivity to
another TCP/IP computer.">
  <OsCmd ostype="WINDOWS" exec="ping" path="" param="true" runtime="60">
    <Exclude param="^-t$"/>
    <Help ref="help.os.ping"/>
  </OsCmd>
  <OsCmd ostype="UNIX" exec="ping -c 4" path="" param="true"
runtime="60">
    <Exclude param="^-(f|l)$"/>
    <Help ref="help.os.ping"/>
  </OsCmd>
</Cmd>
...
```


onapsis

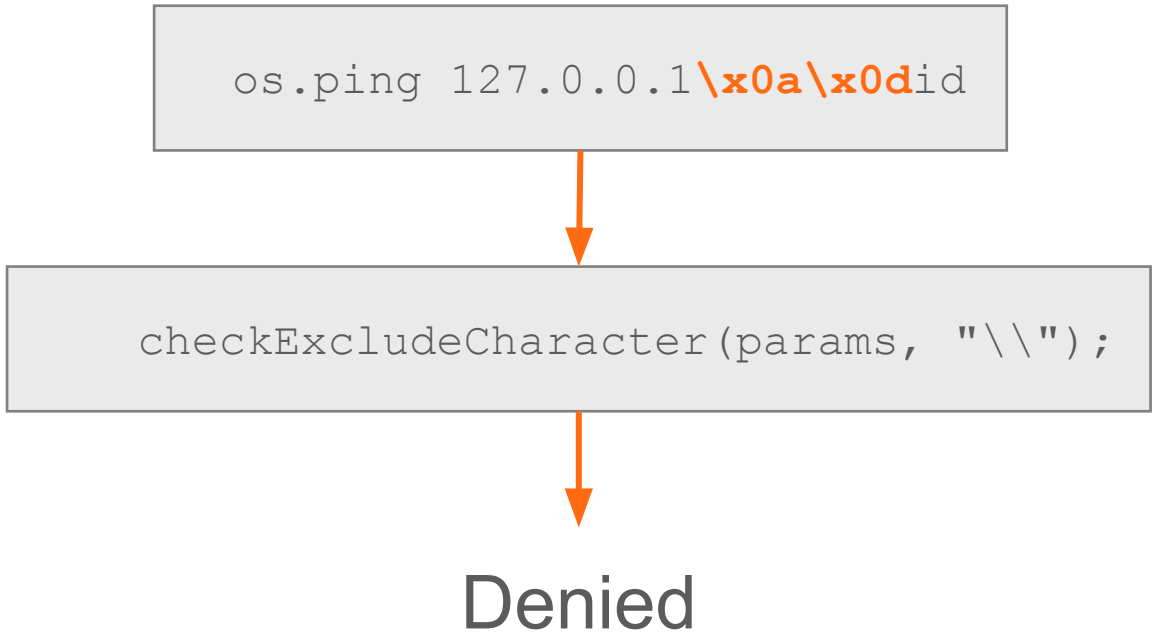
Exécution de commande

- Liste noire

```
// Unix Blacklist
protected void filterParameters(String params) throws RemoteOsException {
            checkExcludeCharacter(params, "|");
            checkExcludeCharacter(params, "&");
            checkExcludeCharacter(params, ">");
            checkExcludeCharacter(params, "<");
            checkExcludeCharacter(params, ";");
            checkExcludeCharacter(params, "\\");
            checkExcludeCharacter(params, "`");
            checkExcludeCharacter(params, "'");
            checkExcludeCharacter(params, "\n");
            checkExcludeCharacter(params, "\r");
            checkExcludeCharacter(params, "$(");
            checkExcludeCharacter(params, "!");
            checkExcludeCharacter(params, "^");
            checkExcludedParameters(params);
}
```

Exécution de commande

- Problème lié à l'échappement de caractères :



Exécution de commande

- Problème lié à l'échappement de caractères :

```
...
00000a10: 702e aced 0005 7400 076f 732e 7069 6e67  p.....t..os.ping
00000a20: 7400 0931 3237 2e30 2e30 2e31 0a0d 6964  t..127.0.0.1..id
00000a30: 7073 7200 136a 6176 612e 7574 696c 2e48  psr..java.util.H
...
```

```
checkExcludeCharacter(params, "\\");
```

OK

onapsis

Exécution de commande

- Problème lié à l'échappement de caractères :

```
...
00000a10: 702e aced 0005 7400 076f 732e 7069 6e67  p.....t..os.ping
00000a20: 7400 0931 3237 2e30 2e30 2e31 0a0d 6964  t..127.0.0.1..id
00000
...                                                                H
```

SSN 2808158 2823733 2839864

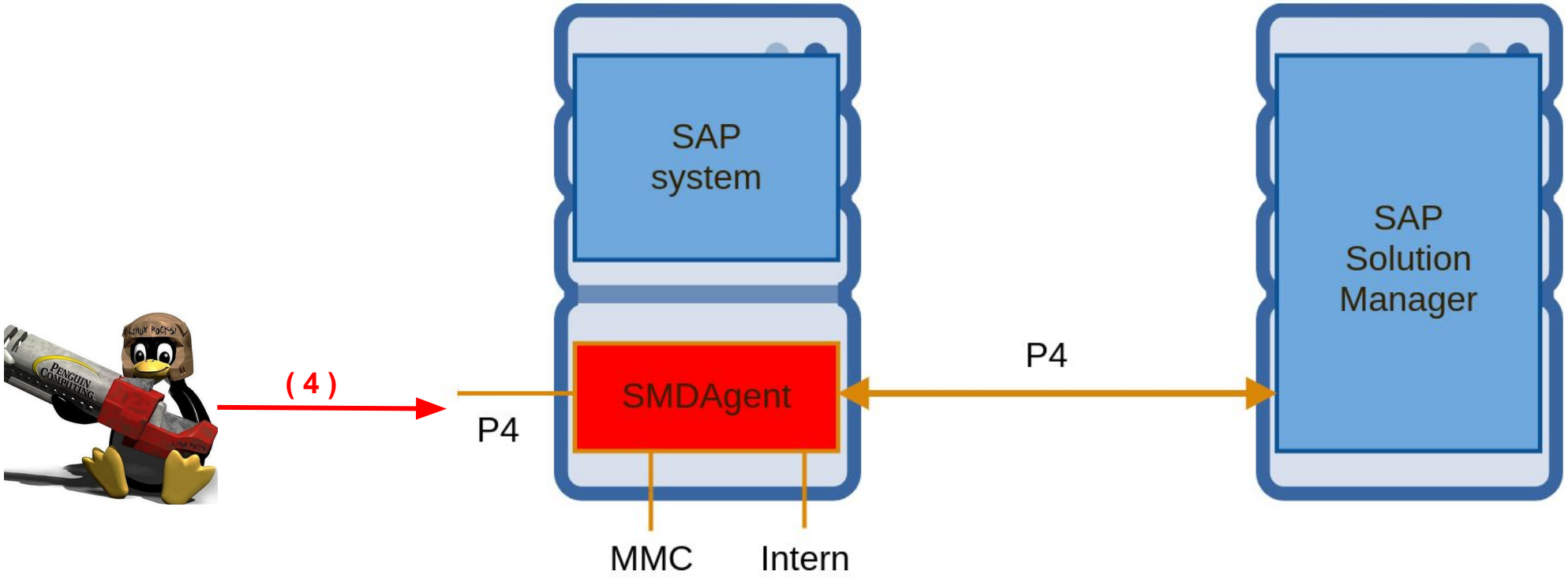
CVE-2019-330

OK

onapsis

Exécution de commande

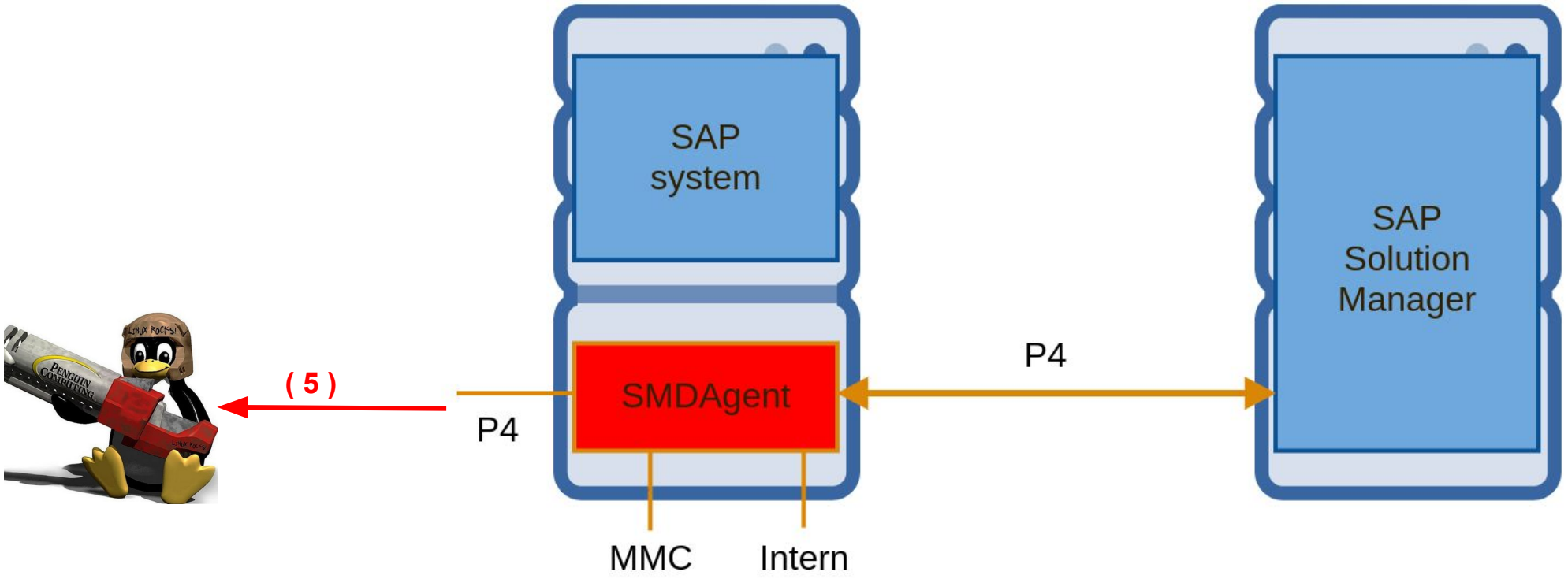
(4) Exécution de commande OS sans restriction



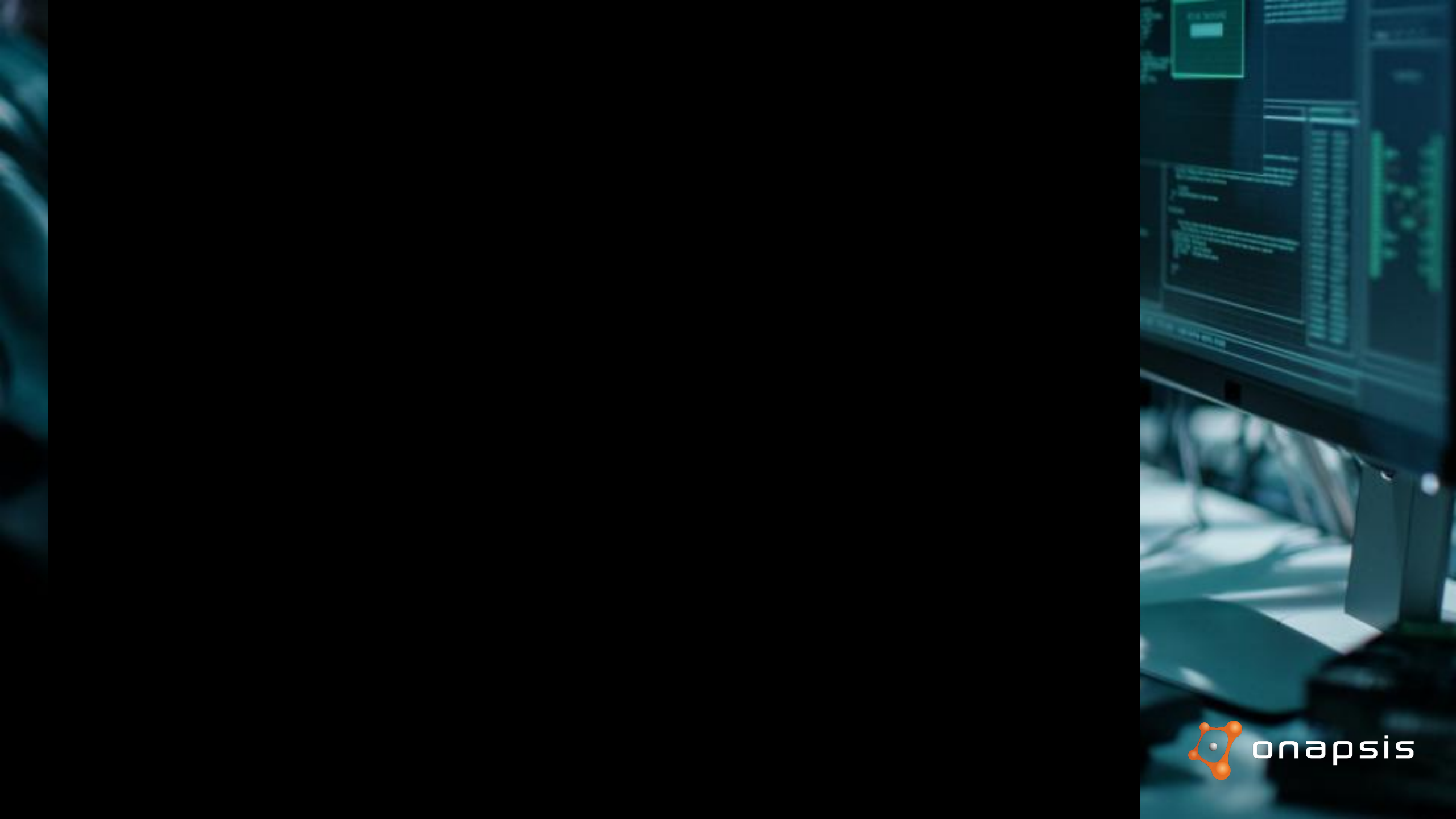
onapsis

Exécution de commande

(5) Exfiltration des données d'identification du SolMan



onapsis


onapsis

Contre-mesures

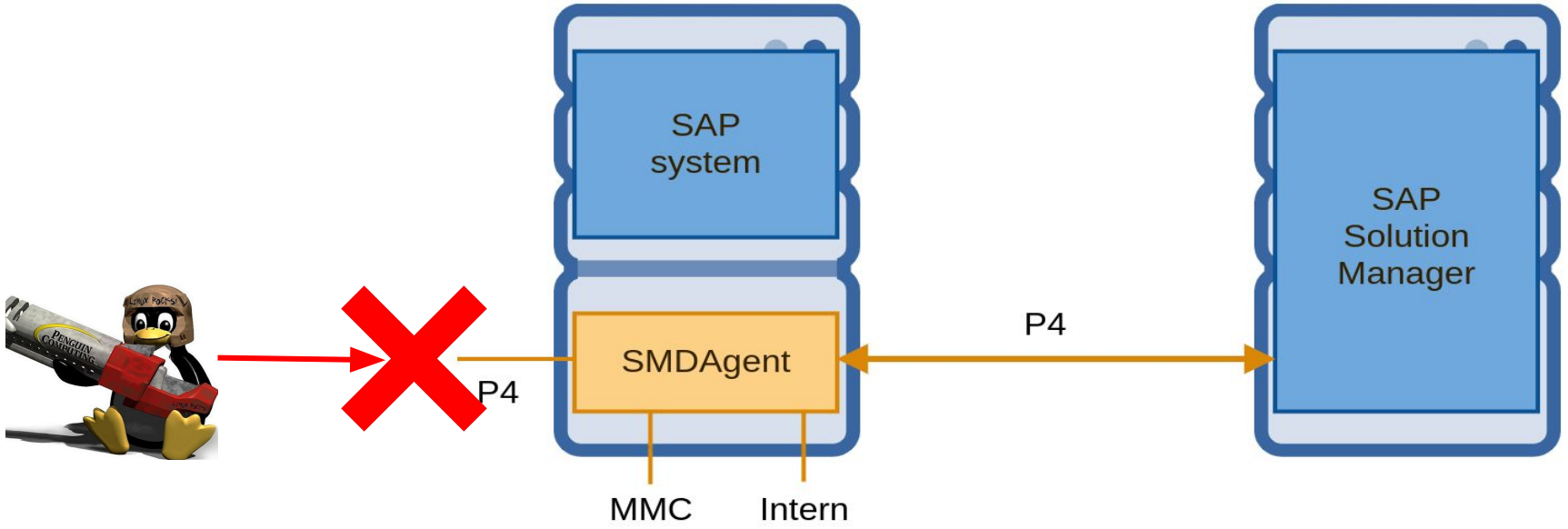
- Activer le chiffrement du SAP Secure Storage pour l'agent
  - Instruction : SAP Note **2772266** & **2748699**

```
#SAP Secure Store file - Don't edit this file manually!
#Tue Oct 29 21:40:22 ART 2019
$internal/mode=encrypted
$internal/version=Ny4wMC4wMDAuMDAx
sld/usr=BnJftsjYlR1GdU4qdic2qfHVPj3mnqyx1Nfg\r\njKBf3EoTlCMx8w4CbAi\=\=
sld/pwd=Cyg37gOTK0neTaAIkT0BYl+6XgSjO1cMzP1RdcS+e8yNz+0ukjezafCeYkMLLDoc
smd/agent/crypto/algo=jKBf3EoTlCMx8w4CbAiX3T+XMFB98lVWXNmMHnAA92+t9q5juLjkyA\=\=
smd/agent/secretkey=XiteJHXHmEoUrwqpIEB5wDv7NAo5bOWxNMJ93VwLZj9Fec7Qf+/y2QyJX2e5Nl/8\r\n
Zw5qwRpPjzPWk7Zc7qxREWFZCHLRQsYDvmvTRdgThoI\=
smd/agent/certificate/pass=BFujkvdSXtDmw0hOGKJp7utovPz9cHhAPIUjWVtRFR8BhL6jNOakcJKAh/l73
5ZeonGAehpKkHOSQoF41VLDX
```


onapsis

Contre-mesures

- Interdire l'accès au service P4 de **tous** les agents
  - Manuellement ou patcher les agents : SAP Note **2845377**
  - Attention quelques effets de bords : SAP Note **2904933**



onapsis

Contre-mesures

- Restreindre l'application 'remoteos'
  - Modifier le **`commands.xml`**, puis le déployer sur tous les agents
  - Manuellement ou via le correctif : SAP Note **2823733**
  - Appliquer les correctifs liés à 'remoteos' : SAP Note **2808158 2839864**
  - Attention quelques effets de bords : SAP Note **2849096**

```
...
  <OsCmd ostype="UNIX" exec="custom_command" path="" param="false"
runtime="60">
  </OsCmd>
...
```


onapsis

Contre mesures

- Tout est corrigé depuis les versions SAP Solution Manager 7.20 suivantes :
  - SOLMANDIAG 720 SP004 000011
  - SOLMANDIAG 720 SP005 000012
  - SOLMANDIAG 720 SP006 000013
  - SOLMANDIAG 720 SP007 000019
  - SOLMANDIAG 720 SP008 000015
  - SOLMANDIAG 720 SP009 000007
  - SOLMANDIAG 720 SP010 000001

1. Introduction
2. Premier contact
3. Echec du “SAP Secure Storage”
4. Le service P4
5. Contournement d’authentification
6. Exécution de commande
7. Contre-mesure
8. **Conclusion**

Conclusion

- En utilisant cette chaîne de vulnérabilités, un attaquant peut :
  - → Contourner le processus d'authentification sur le SMDAgent
  - → Exécuter des commandes OS en tant qu'administrateur du SMDAgent
  - → Déchiffrer et extraire les données d’identification critiques du SolMan

- Post exploitation :
  - → Falsification de données critiques
  - → Déni de service
  - → Qui sait ?

Conclusion - Chronologie

• 2018 Décembre	Début	Rapport à SAP
• 2019 Janvier → Mars	¼ temps	
• 2019 Avril	Plein temps	
• 2019 Mai	½ temps	Rapport à SAP
• 2019 Juin	Stop	
• 2019 Juillet → 2020 Mars		Publication des correctifs

Conclusion - Références

- “Inception of the SAP Platform's Brain” https://www.youtube.com/watch?v=2SfhdHC4Dtk
- 2808158 CVE-2019-0330 https://launchpad.support.sap.com/#/notes/2808158
- 2823733 CVE-2019-0330 https://launchpad.support.sap.com/#/notes/2823733
- 2839864 CVE-2019-0330 https://launchpad.support.sap.com/#/notes/2839864
- 2849096 - https://launchpad.support.sap.com/#/notes/2849096
- 2772266 CVE-2019-0307 https://launchpad.support.sap.com/#/notes/2772266
- 2738791 CVE-2019-0318 https://launchpad.support.sap.com/#/notes/2738791
- 2748699 CVE-2019-0291 https://launchpad.support.sap.com/#/notes/2748699
- 2845377 CVE-2020-6198 https://launchpad.support.sap.com/#/notes/2845377
- 2904933 - https://launchpad.support.sap.com/#/notes/2904933
- SAP Product Respond Team secure@sap.com

onapsis

Merci !

Questions ?

Yvan ‘iggy’ Genuer

@_1ggy

ygenuer[\x40]onapsis.com