

CRESTCon 2012



SAP Slapping

A Penetration Testers Guide

\$ /usr/bin/who

- Dave Hartley - Principal Security Consultant @MWR.
- CHECK and CREST Certified (Application & Network).
- CREST Assessor (help design and invigilate exams).
- @nmonkee

What it is...

- This talk aims to provide the audience with just enough information to help you go from zer0 to her0 in as short a time as is possible when encountering SAP systems during engagements.
- Hopefully without serious fail!

What it isn't...

- This talk will not provide a deep understanding of SAP, nor will it provide you with the abilities to perform in depth, effective and comprehensive security assessments of SAP landscapes.
- Original talk was **137** slides and even that didn't cover everything!
- This is the condensed version... I'm gonna move fast - keep up ;)

Disclaimer

- This talk shamelessly re-imagines the original works of the following players:
 - Alexander Polyakov (dsecrg.com)
 - Andreas Wiegenstein (virtualforge.com)
 - Ian de Villiers (sensepost.com)
 - Joshua 'Jabra' Abraham & Willis Vandevanter (rapid7.com)
 - Raul Siles (taddong.com)
 - Mariano Nuñez Di Croce (onapsis.com)



Agenda

- Background
- SAP Infrastructure/Landscape
- SAP Databases
- SAP Connectivity
- SAP Transactions, Reports and Programs
- SAP Web



Background

SAP Primer

Background

- SAP (Systems, Applications, and Products in Data Processing) is one of the world's largest software companies!
- SAP's products focus on Enterprise Resource Planning (ERP).
- There are five major enterprise applications in SAP's Business Suite.

Background

- SAP ERP Central Component (SAP ECC) previously named R/3.
- Customer Relationship Management (CRM).
- Product Lifecycle Management (PLM).
- Supply Chain Management (SCM).
- Supplier Relationship Management (SRM).

Very Basic Overview of SAP

- The language of SAP is ABAP.
- Classic ABAP applications (called “transactions”) are executed through a proprietary (fat) client called SAP GUI.
- The communication between SAP GUI and the server is based on a proprietary protocol called DIAG.
- “Modern” ABAP applications (Business Server Pages and Web Dynpro ABAP) can be executed with a standard Web browser via NetWeaver Web Application Servers.
- ABAP programs can be called remotely via Remote Function Calls (RFC).

How Hard is it to Hack?

SAP Community Network Forums: Whether SAP Business One has been ...

sdn.sap.com/thread.jspx?threadID=1585933

RSS

Google

Re: Whether SAP Business One has been hacked before

Posted: Jan 21, 2010 11:07 AM in response to: [Gokul K.](#)

   Reply

Hi Gokul,

If you are talking about the UID and password hacking and tampering of data, I cannot say that its impossible. But only a real computer genius can pull out a thing like that. As the Password information is stored in an encrypted format and no one knows the algorithm for that encryption.

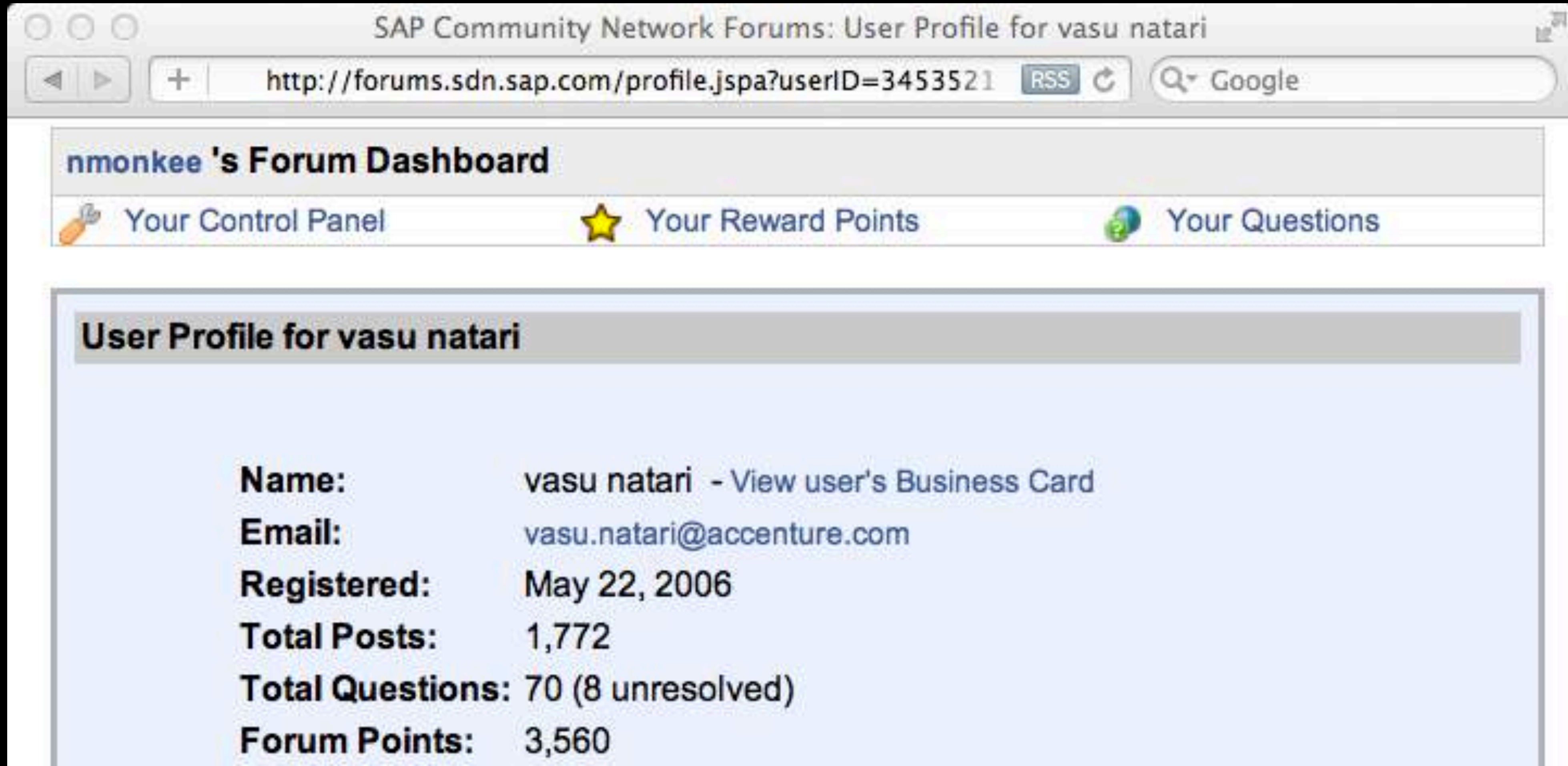
Rest assured that the Data is safe.

Assure the customer that SAP is a very Old company founded in 1972, and it has fool proof ways of doing things. SAP has 89,000 SAP B1 customers in 120 countries and 10,000 customers in India alone, and until now we dont have a case of password tampering.

Hope it helps,

Vasu Natari.



Apparently it takes a Genius!



SAP Community Network Forums: User Profile for vasu natari

http://forums.sdn.sap.com/profile.jspa?userID=3453521 RSS Google

nmonkee 's Forum Dashboard

 Your Control Panel  Your Reward Points  Your Questions

User Profile for vasu natari

Name:	vasu natari - View user's Business Card
Email:	vasu.natari@accenture.com
Registered:	May 22, 2006
Total Posts:	1,772
Total Questions:	70 (8 unresolved)
Forum Points:	3,560

Does it Really?

- I'm no Genius :'(
- But I can hack SAP and by the end of this presentation, you can too ;)
- If your a practiced network and application pen tester, then this is not scary or hard.

What Makes a Win?

- SAP Administration privileges at the Operating system level (<sid>adm user) or higher.
- DBA privileges over SAP database schemas or higher.
- SAP_ALL privileges over the production client or equivalent.
- Any one of the above can be used to gain the others ;)



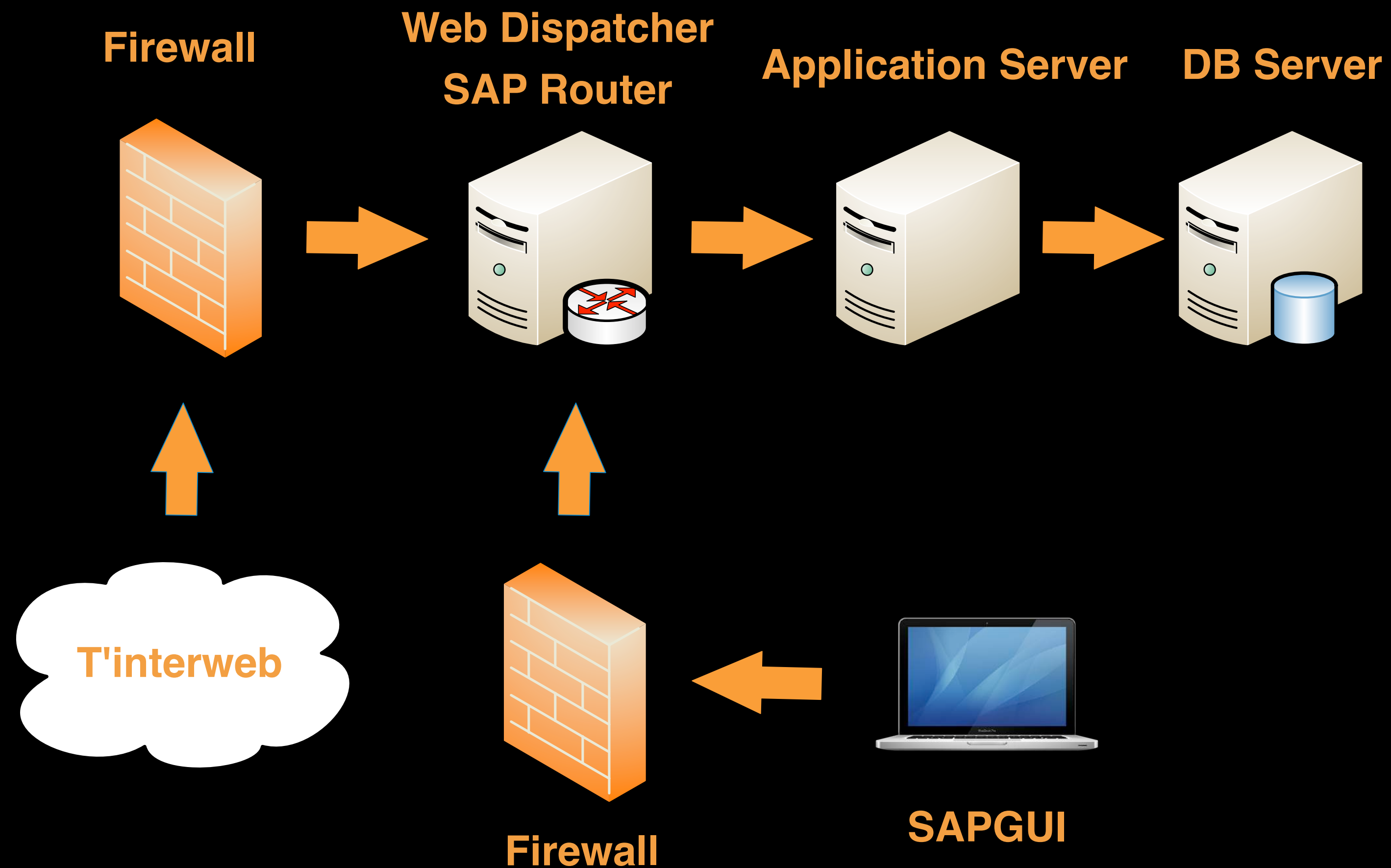
SAP Infra & Landscape

DEV, QAS and PROD

SAP Infrastructure

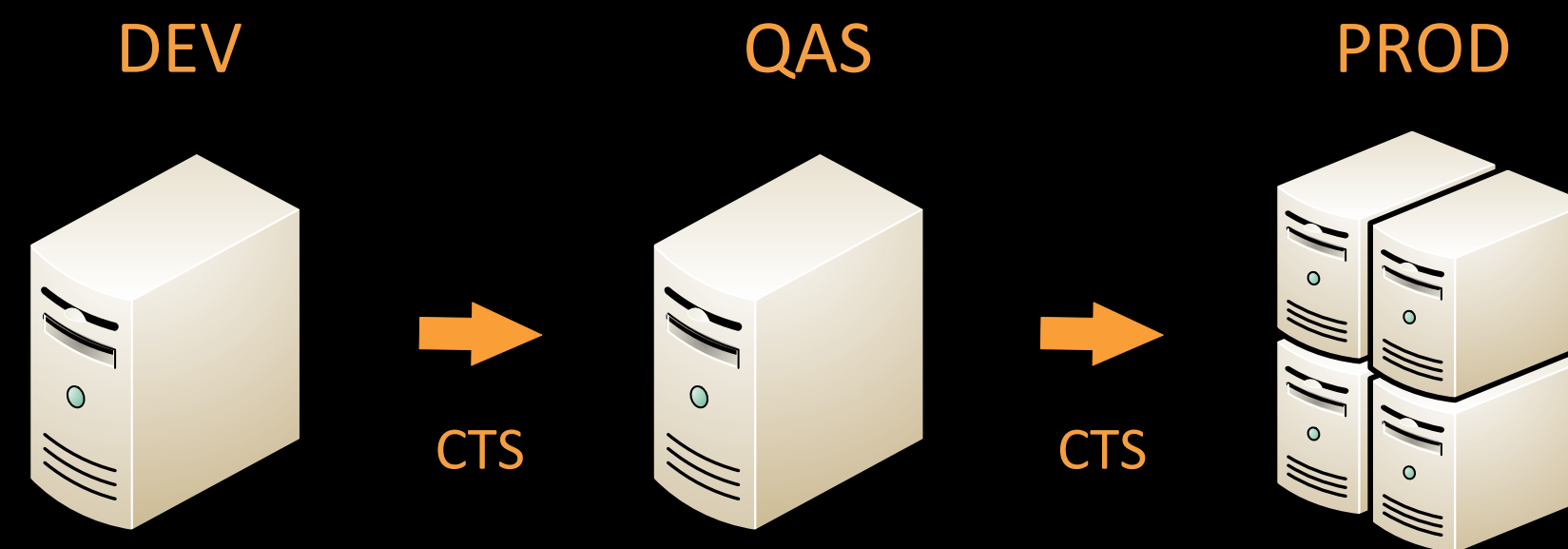
- SAP uses an N-Tier structure. Each SAP deployment will consist of at least one module (usually running on a dedicated server), one database server and the appropriate SAP GUI client (exception: ITS, WAS, AS, Portal etc. provide web-based browser clients).
- Multiple instances of SAP and databases may occupy the same physical infrastructure.
- You may also come across virtualised systems all running under one hypervisor.

SAP Infrastructure



SAP Landscape

- Typically a three-system landscape is implemented.
- Development Server (DEV)
- Quality Assurance Server (QAS)
- Production Server (PROD)
- The landscape design is not to facilitate redundancy, but to enhance "configuration pipeline management".
- Changes are migrated from DEV through to PROD via a process called "Change and Transport Management" (CTS, or Transports).



Change & Transport System

- The Change and Transport System (CTS) is used to transport changes between SAP systems.
- The Common Transport Directory (CTD) is the directory where changes (transports) are exported to and imported from in a SAP landscape (NFS & SMB/CIFS).
- The directory must be shared for all systems in the landscape.

NFS nosuid

- Often the NFS shares are exported and mounted without the nosuid option.

```
//set uid and gid to root (and spawn a shell)
#include <stdlib.h>
int main(int argc, char **argv, char **envp){
    setuid(0);
    setgid(0);
    execve("/bin/sh",argv,envp);
    return(0);
}
```

- <http://www.bindshell.net/tools/become.html> & <ftp://ftp.cs.vu.nl/pub/leendert/nfsshell.tar.gz>



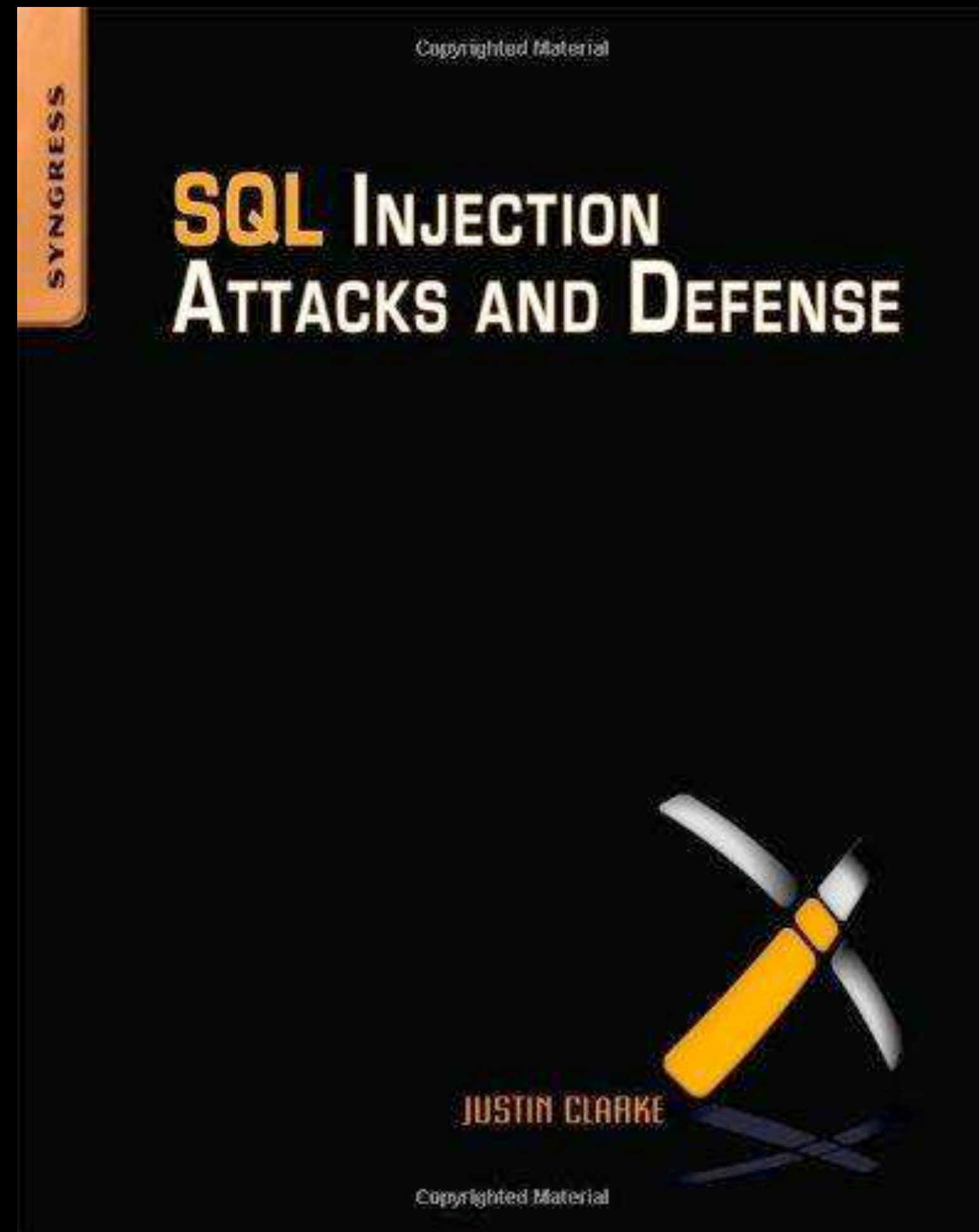
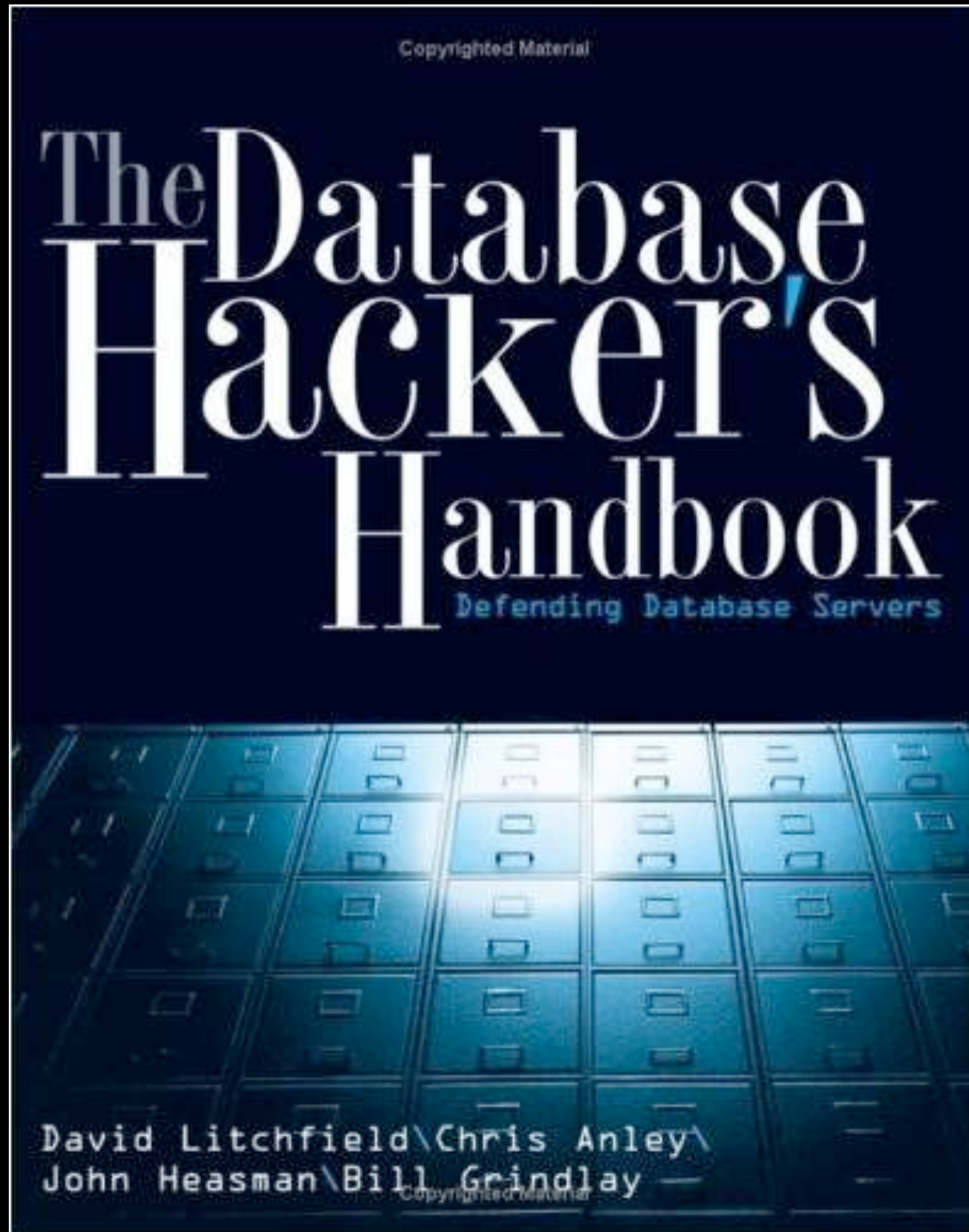
SAP Databases

MSSQL, Oracle, SAP MaxDB, etc.

SAP Databases

- DB2
- Sybase ASE
- Oracle
- MS SQL
- MaxDB
- Informix

Database Hacking 101



Oracle

- SAP mandates that Oracle be configured with the `remote_os_authent` parameter set to `TRUE`, which means that Oracle will authenticate remote connections using the `os_authent_prefix` - without supplying a password!
- The following is a quote from SAP:

“Do not change the value of the Oracle parameter `REMOTE_OS_AUTHENT` to `FALSE`. The `OPS$` mechanism needs to be able to work from remote clients – for example, SAP System work processes need to be able to log on to the application servers as the user `OPS$<sapsid>adm`. Therefore, keep this parameter set to `TRUE`.”

Oracle

- Create a "tnsnames.ora" file, specifying connection parameters.

```
sap01=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST = 192.168.1.10)(PORT = 1527)))  
(CONNECT_DATA=(SID=TO1)))
```

- Create a local user, with username <sid>adm (sap01adm) and login as this user before running sqlplus.

```
# adduser sap01adm  
# mv tnsnames.ora to /home/sap01adm/.tnsnames.ora  
# su - sap01adm  
# sqlplus /@sap01  
SQL> select mandt, bname, bcode from usr02;
```

SAP Max-DB

- MAX DB has a similar mechanism to Oracle REMOTE_OS_AUTHENT - XUSER.
- If the OS user you have compromised has a file named .XUSER.62 in their home directory, they can connect to the database by specifying the defined user key alone.
- No need to enter a username and/or password!.

```
$ ls -al /home/sqdbwq/.XUSER.62  
-rw----- 1 sqdbwq sapsys 1724 Nov 22 2011 .XUSER.62
```

```
$ dbmcli -d BWQ -U c -USQL DEFAULT sql_execute select mandt, bname, bcode from usr02
```



SAP Connectivity

SAPRouter, SAP GUI and SAP Web GUI

Connecting to SAP

- SAP users can connect using:
 - SAPGUI (Windows)
 - SAPGUI (JAVA)
 - WEBGUI (Browser)
 - Remote Function Call (RFC)
 - Applications such as VisualAdmin, Mobile client and many-many more...

Communications

Software	Password encryption	Data encryption	Mitigation
SAPGUI	DIAG (can be decompressed)	DIAG (can be decompressed)	SNC
JAVAGUI	DIAG (can be decompressed)	DIAG (can be decompressed)	SNC
WEBGUI	Base64	NO	SSL
RFC	XOR with known value	DIAG (can be decompressed)	SNC
Visual Admin	Proprietary encoding	NO	SSL
Mobile Admin	NO	NO	SSL

SAPRouter

- SAPRouter is a SAP program working as a reverse proxy, which analyses connections between SAP systems and between SAP systems and external networks.
- It is designed to analyse and restrict SAP network traffic which was allowed to pass through the firewall.

SAPRouter

- The SAPRouter can be used for:
 - Filtering requests based on IP addresses and/or protocol.
 - Logging connections to SAP systems.
 - Enforcing the use of a *secret* password for communications.
 - Enforcing transport level security using Secure Network Communications (SNC).



SAPRouter

P	FQDN.client	DNS-SAPSystemName	SAPServiceName	s3cr3tPassw0rd
P	192.168.0.*	10.0.0.*	*	
S	192.168.1.*	10.1.0.*	*	
P	192.168.2.10	10.2.0.54	3203	
D	*	*	*	

SAPRouter

- If it responds to “info-requests” (\$ saprouter -l) - then it is possible to discover internal SAP servers and IP address schemes in use.
- If the rules are misconfigured (P instead of S) or lax (*) - then it may be possible to port scan internal systems, proxy communications to and attack internal SAP systems ;)
- The attack tool kit ‘Bizploit’ contains a plugin called ‘saprouterSpy’ that can:
 - Port scan through the SAPRouter to map internal systems and;
 - Proxy connections automagically to internal SAP systems.

Bizploit - SAPRouter Demo

```
monkee@muaddib ~/tool-box/sap/HitB/tools/bizexploit $ ./bizexploit -s SAPRouter-saprouterSpy-Demo.scr █
```

SAP GUI

- Proprietary fat client, available as Windows executable and Java application.
- Client-Server Communication via DIAG protocol.
- DIAG can be encrypted with SNC, but is only compressed by default.
- Provides methods to interchange files with the SAP application server.
- Execution of screen-events can be scripted.

SAPGUI (JAVA)

- `$./sapgui /H/10.1.1.6/S/3201`
- In its simplest form, a connection string contains an IP address and a port number.
- IP address and port number are marked with the prefixes '/H/' (for host) and '/S/' (for service).
- Note that the port number for a SAP application server is by convention 3200 plus the two-digit SAP system number.

SAPGUI (Windows)

- There are approx. 1,000 ActiveX controls installed with SAPGUI (Windows). Most if not all have the kill bit set :(-
- There are ActiveX controls that can:
 - Connect to SAP servers (automated brute force attack ftw!).
 - Download files.
 - Read/Write/Delete files.
 - Execute commands (locally and on SAP servers).

SAPGUI (Windows)

- Users can launch the SAP GUI from SAP shortcuts on their desktop.
- If HKCU\Software\SAP\SAPShortcut\Security EnablePassword=1, then the password will be stored in the shortcut!
- Password is encoded (Kernel <= 6.40).
- Password is encrypted (Kernel 7.10 & 7.20).

SAP Clients

- In SAP land, clients are things you connect to using a GUI ;)
- The range is 000 - 999, with the default clients being 000, 001, 066.
- If the client you try and connect to via RFC does not exist, SAP will error:
“Client <client> is not available”
- Brute force the whole range to discover available ones ;)

Bizploit - RFC Brute Force Demo

SAP Default Credentials

User	Description	Clients	Password
SAP*	Super user	000, 001, 066 & new clients	06071992 & PASS
DDIC	ABAP Dictionary super user	000, 001	19920706
TMSADM	Transport Management System user	000	PASSWORD
EARLYWATCH	EarlyWatch service user	066	SUPPORT
SAPCPIC	Communications user	000, 001	ADMIN

SAP GUI Client Attacks

- WS_EXECUTE - Executes an operating system command on the client.
- GUI_UPLOAD - Uploads a file from the Client to the Server.
- GUI_DOWNLOAD - Downloads a file from the Server to the Client.
- Class CL_GUI_FRONTEND_SERVICES - Provides various other functions including directory listing, access to clipboard etc.
- Underlying ABAP Commands CALL METHOD OF and CALL cfunc.
- See SAPProx (<http://www.sensepost.com/labs/tools/poc/sapprox>) PoC tool from Sensepost for MiTM win - I've not yet seen automated/weaponised attack tool kit.

Transactions, Reports & Programs

ABAP & RFC's

Transactions

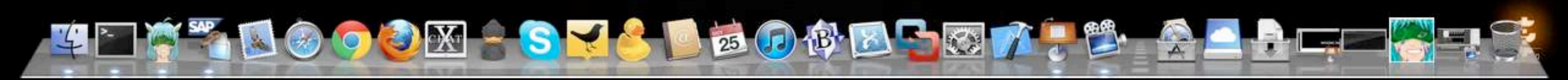
- SAP-ABAP supports two types of programs - Report Programs & Dialog Programs. Report Programs are used when large amounts of data needs to be displayed.
- Transactions can be called via system-defined or user-specific, role-based menus. They can also be started by entering the transaction code directly into a command field.
- Transactions can also be invoked programmatically by means of the ABAP statements `CALL TRANSACTION` and `LEAVE TO TRANSACTION`.

(Phun)Transactions

Transaction Code / Report	Purpose
SM69	Configure OS commands
SM49	Execute OS commands
RSBDCOS0	Execute OS commands
RPCIFU01	Display file
RPCIFU03	Download Unix file

SM69 Demo

Macintosh HD
SAP



USR02 & USH02

- SAP has implemented a number of different password hashing mechanisms.
- Hashes are stored in table USR02 (BCODE & PASSCODE) and USH02.
- john-the-ripper can be used to crack SAP hashes (codevn B and G).

SAP Hashing Mechanisms

Code Vers	Description
A	Obsolete
B	Based on MD5, 8 characters, uppercase, ASCII
C	Not implemented
D	Based on MD5, 8 characters, uppercase, UTF-8
E	Reserved
F	Based on SHA1, 40 characters, case insensitive, UTF-8
G	Code version F + code version B (2 hashes)
H/I	Passwords with random salts

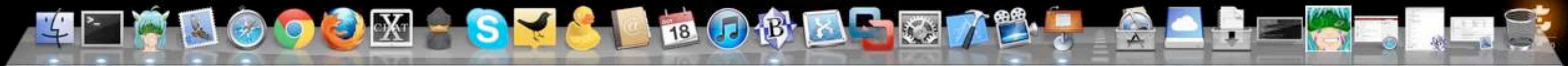
Cracking Hashes

- A small perl script is provided with john (sap_prepare.pl) that parses the content of a tab separated file (SAP calls those 'XLS files').
- Export SAP table USR02 or USH02 to XLS and pass to the script - then crack with john.
- If you have access to both password types (B and G) you should start cracking B first 'cause it's a lot faster.

SE11 & USR02 Hash Cracking Demo


```
SAPGUI — bash
bash
atreydes:SAPGUI nmonkee$ ./SAPGUI -o /H/172.26.0.100/S/3200
```

Macintosh HD
SAP



Bypassing MANDT

- SAP enforces data segregation via the MANDT field.
- MANDT is the unique identifier that is assigned to each client.
- SE11 will provide access to data for the current client only (as will RFC_READ_TABLE and SQVI etc.)
- To access the data of other clients use transaction SE80 (ABAP Workbench) create a custom ABAP program and call EXEC SQL (native SQL) from within.

ABAP

- ABAP is the SAP high-level programming language used to develop business applications and programs. ABAP programs reside in the SAP database in two forms:
 - source code (table REPOSRC) - which can be viewed and edited with the ABAP Workbench tools (transaction SE80).
 - generated code (table REPOLOAD) - a binary representation somewhat comparable with Java bytecode.
- In PROD, modification of ABAP code is prohibited; however...
- There is no CRC check - so what if you pwned the DB?

Remote Function Call (RFC)

- Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems.
- SAP systems can communicate with other SAP systems, or non-SAP system using RFC and/or by calling functions directly in a system (using an ABAP interface or RFC API).
- RFC's are basically independent ABAP modules that can be called locally or remotely.

Remote Function Call (RFC)

- RFC can require authentication - `RfcInstallExternalLogonHandler` and/or `AUTHORITY_CHECK_RFC`.
- It's a PITA to secure many RFC's granularly - so `S_RFC` "*" authorization is VERY common!
- All SAP communications are in the clear, by default (including RFC's) and are easily decompressed (http://conus.info/utis/SAP_pkt_decompr.txt).

Remote Function Call (RFC)

- Passwords are obfuscated with a simple XOR operation (using a fixed key!)
- 0x96, 0xde, 0x51, 0x1e, 0x74, 0xe, 0x9, 0x9, 0x4, 0x1b, 0xd9, 0x46, 0x3c, 0x35, 0x4d, 0x8e, 0x55, 0xc5, 0xe5, 0xd4, 0xb, 0xa0, 0xdd, 0xd6, 0xf5, 0x21, 0x32, 0xf, 0xe2, 0xcd, 0x68, 0x4f, 0x1a, 0x50, 0x8f, 0x75, 0x54, 0x86, 0x3a, 0xbb
- `$./getPassword.py -o password`
0xe6 0xbf 0x22 0x6d 0x3 0x61 0x7b 0x6d
- `$./getPassword.py -d "e6 bf 22 6d 03 61 7b 6d"`
password

Remote Function Call (RFC)

- ABAP Programs call a remote Function Module using the command `CALL FUNCTION <name> DESTINATION <index key>`.
- The DESTINATION argument is a index key to an RFC Destinations table (RFCDES), maintained through transaction SM59.
- RFC communication is done through the Gateway Service.
- Each instance of a SAP system has a Gateway.
- The Gateway enables communication between work processes and external programs, as well as communication between work processes from different instances or SAP Systems.

Remote Function Call (RFC)

- There are a number of RFC's installed by default.
- RFC_DOCU - Can be used to discover installed functions.
- RFC_SYSTEM_INFO - Returns verbose system information.
- RFC_PING - Can be used to check for availability of remote RFC Server(s).
- All without authentication!



RFC_SYSTEM_INFO

Running 'sapinfo' against [172.16.252.135(0)-SAPRFC(0)]

[VULN] Remote system information disclosure

Remote system information:

RFC Log Version: 011

Release Status of SAP System: 702

Kernel Release: **720**

Operating System: Linux

Database Host: **NPLHOST**

Central Database System: **ADABAS D**

Integer Format: Little Endian

Hostname: nplhost

Float Type Format: IEEE

IP Address: 192.168.234.42

System ID: **NPL**

RFC Destination: **nplhost_NPL_42**

Timezone: 0 (diff from UTC in seconds)

Character Set: 4103

Daylight Saving Time:

Machine ID: 390

Remote Function Call (RFC)

- RFCEXEC - Bundled with the RFCSDK and provides the following functions:
 - RFC_RAISE_ERROR
 - RFC_MAIL
 - RFC_REMOTE_PIPE
 - RFC_REMOTE_FILE
 - RFC_REMOTE_EXEC

Remote Function Call (RFC)

- RFCEXEC is protected through rfcexec.sec file directives.
- Default is to allow everything!
- It's also a blacklist usual bypasses e.g.
 - foo.exe, foo.eXe, foo.EXE etc.

Remote Function Call (RFC)

- SAPXPG - Shipped with SAP AS and used for execution of external commands and programs.
- Installs the following functions:
 - SAPXPG_END_XPG
 - SAPXPG_START_XPG_LONG
 - SAPXPG_START_XPG
- Started programs restricted through the secinfo file.

Remote Function Call (RFC)

- External RFC servers can work in two different modes: started and registered.
- A started external server is a program that is initiated by a Gateway Server when a RFC call matching its destination is received (statically set).
- If the server resides in a remote host, the Gateway connects with the remote host and starts the program.

Remote Function Call (RFC)

- An external server registers itself at a specific SAP Gateway by sending an ID string (Program ID aka Tpname) to the Gateway.
- When the Gateway receives an RFC call for that destination, the call is forwarded to the external system.
- When in registered mode anyone can dynamically register with the Gateway as an external RFC server using an existing Program ID.
- This can be captured off of the wire or from the Gateway monitor (by default in newer kernels remote access is denied).

Evil Twin and Callback

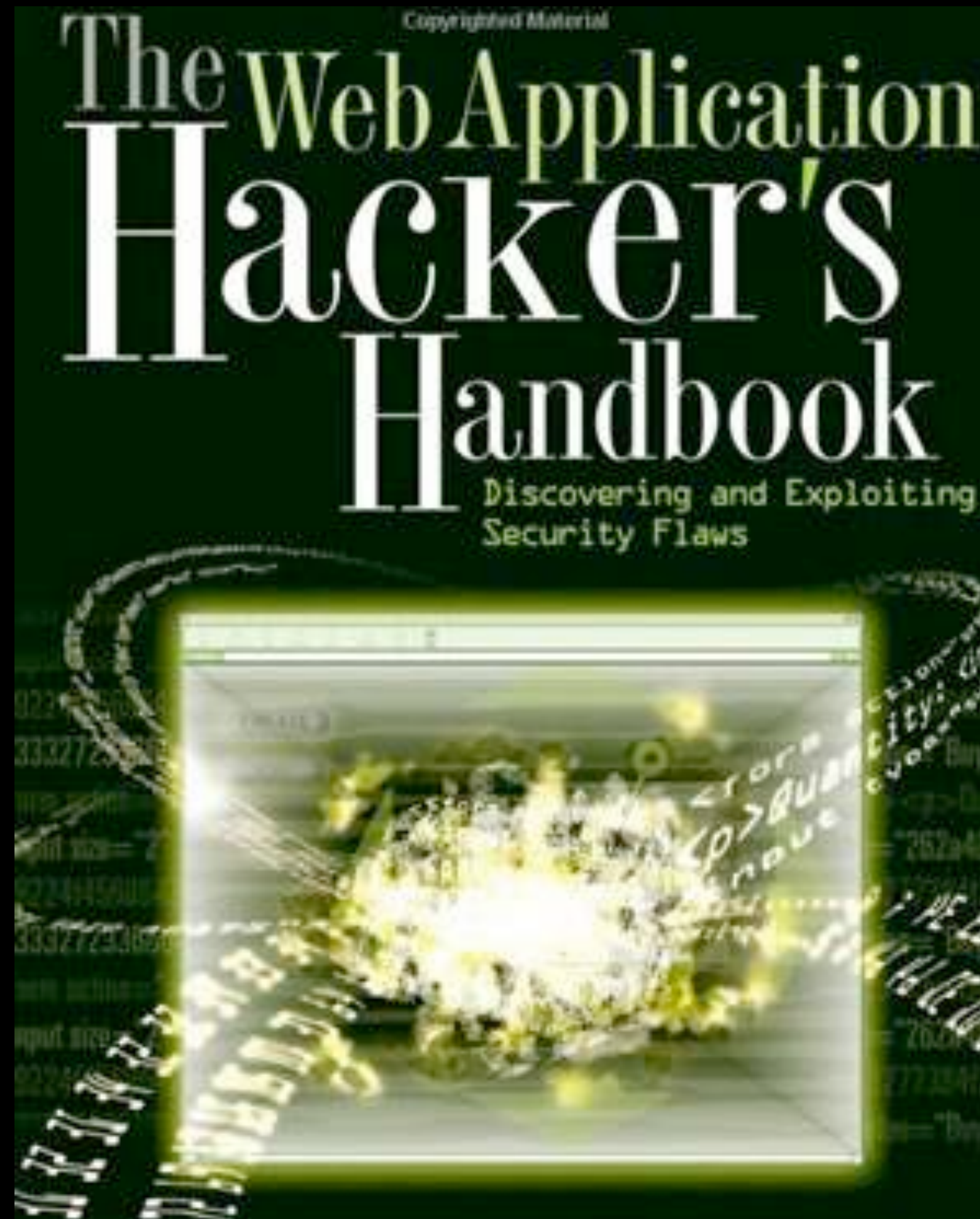
- The Evil twin attack is basically a man-in-the-middle attack whereby a malicious External RFC server is registered with the Gateway so that an attacker can capture, manipulate and replay RFC calls.
- Requires that legit RFC servers are blocked (DoS).
- The Callback attack leverages a feature of the RFC protocol. Namely by exploiting the callback routine, which allows a server to execute code on the calling client.
- The client is often a SAP Application Server (running with SAP_ALL).



SAP Web

NetWeaver, AS ABAP/J2EE, ITS, ICM, Web Dispatcher, EP and BO XI

Web Hacking 101



SAP Application Server (Netweaver)

- 2002 - SAP Web Application Server 6.20
- 2003 - SAP Web Application Server 6.30
- 2004 - SAP Netweaver 04
- 2006 - SAP Netweaver 7.0 (2004s)
- 2009 - SAP Netweaver 7.1 ABAP/AS
- 2010 - SAP Netweaver 7.2 ABAP/Java AS
- 2011 - SAP Netweaver 7.3 ABAP/Java AS

Fingerprinting

- Versions (and sometimes SAP SID and System Number) are disclosed in:
 - HTTP and SOAP responses.
 - Server headers.
 - Error messages.
 - HTML comments/source.
 - 403 and 404 pages.

SAP Application Server

- SAP has many web servers, such as: WEB AS, ITS, IGS etc.
- SAP AS can execute ABAP and/or Java programs. Allowing the use of ABAP-based Business Server Pages (BSP) and/or Java (JSP), as well as other technologies:
 - Web services.
 - Webdynpro.
 - Enterprise JavaBeans (EJB).
 - Portal iViews.

SAP Application Server

- The SAP Internet Transaction Server (ITS) translates dialog screens into HTML pages so that users can interact with SAP applications via a web browser.
- The Internet Communication Manager (ICM) is the evolution of the ITS component.
- The ICM web requests are handled by the Internet Communication Framework (ICF), which provides ICF services.

SAP Application Server

- ICF services are akin to .php/.asp/.jsp etc.
- There are over 1,500 ICF standard services.
- Some are public and require no authentication.
- The ICM also provides a SOAP interface to RFC!
- Metasploit - `auxiliary/scanner/sap/sap_icm_urlscan.rb`

Web Dispatcher

- The SAP Web Dispatcher is a program that works as a reverse proxy and load balancer for incoming HTTP(S) requests. Specifically it can be used for:
 - Load balancing - selecting the appropriate Application Server (AS).
 - Filtering URLs - rejecting well-known attack patterns and/or restricting access to private sections.

Web Dispatcher

- URL filtering is enabled by configuring the parameter wisp/permission_table.
- Example URL ACL below (P - Permit / D - Deny)

P	/sap/public/*
P	/sap/bc/harmless.cgi
D	*.cgi
P	/sap/bc/ping
D	*

SAP Management Console

- SAP MC found on port 5<instance>13 (HTTP)/5<instance>14 (HTTPS).
- Used for remote management of SAP servers - installed by default!
- HTTP only by default and uses basic auth (base64).
- Possible to enumerate users, determine lockout thresholds and audit settings.
- As well as quite a few information disclosure issues we have command exec ;)

SAP Management Console

The screenshot displays the SAP Management Console interface. The left sidebar shows a tree view of SAP Systems, including NPL, Database, DVEBMGS42 on nplhost, and SCS00 on nplhost. The main area shows the status of System NPL as Running, with 2 instances. Below this, a table lists the instances of NPL(3).

SAP Management Console

File Tools ?

SAP Systems

- NPL
 - Database
 - NPL(ABAP) on nplhost
 - DVEBMGS42 on nplhost
 - Process List
 - Open Alerts
 - Current Status
 - Queue Statistics
 - Access Points
 - AS ABAP WP Table
 - ICM
 - Log Files
 - Computer System
 - SCS00 on nplhost
 - Process List
 - Access Points
 - Enqueue Locks
 - Enqueue Statistic
 - AS Java Cluster Message
 - Log Files
 - Computer System

SAP NetWeaver™
SAP Management Console

System NPL
Status: **Running**
Instances: 2, 1 ABAP

Database
ABAP SAPDB on nplhost(Run...


NPL(3)

Hostname	Status	Features	Instance Number
nplhost	Running	Database types ABAP	
DVEBMGS42 o...	Running	ABAP, Enqueue Se...	42
SCS00 on nplhost	Running	Enqueue Server, M...	0

Metasploit - SAP Management Console Demo

Armitage View Hosts Attacks Workspaces Help

- auxiliary
- exploit
- payload
- post



IP Address	OS
172.26.0.200	Linux (Ubuntu)
172.26.0.201	Linux (Ubuntu)
172.26.0.100	Windows
172.26.0.101	Windows
172.26.0.98	Windows
172.26.0.99	Windows

Console X

```
User Name: [ security ]
Password: [          ]

[ OK ]
```

```
= [ metasploit v4.1.0-release [core:4.1 api:1.0]
+ -- == [ 751 exploits - 389 auxiliary - 103 post
+ -- == [ 228 payloads - 27 encoders - 8 nops

msf >
```

SAP Application Server J2EE

- Portal, Mobile, BO XI, PI, SAP Solution Manager and many more products and/or custom apps rely on the SAP J2EE engine.
- It is similar to any other Application Server like Apache Tomcat , BEA Weblogic, IBM Websphere or Oracle Appserver.
- Version 7.2 contains more than 1,200 applications and all of them are enabled by default!

Invoker Servlet

- Possible to bypass filter settings by using default servlet URLs (if EnableInvokerServletGlobally true).
- Servlet in web.xml below can be called two ways:
- /admin/critical/CriticalAction - get prompted for auth :(
- /servlet/com.sap.admin.CriticalAction - bypass auth.

```
<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>
```

Verb Tampering

- web.xml below specifies that the servlet requires authentication when called with GET request.

- A HEAD request will execute as a GET - but won't require auth!

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

- See http://mirror.transact.net.au/sourceforge/w/project/wa/waspap/waspap/Core/Bypassing_VBAAC_with_HTTP_Verb_Tampering.pdf

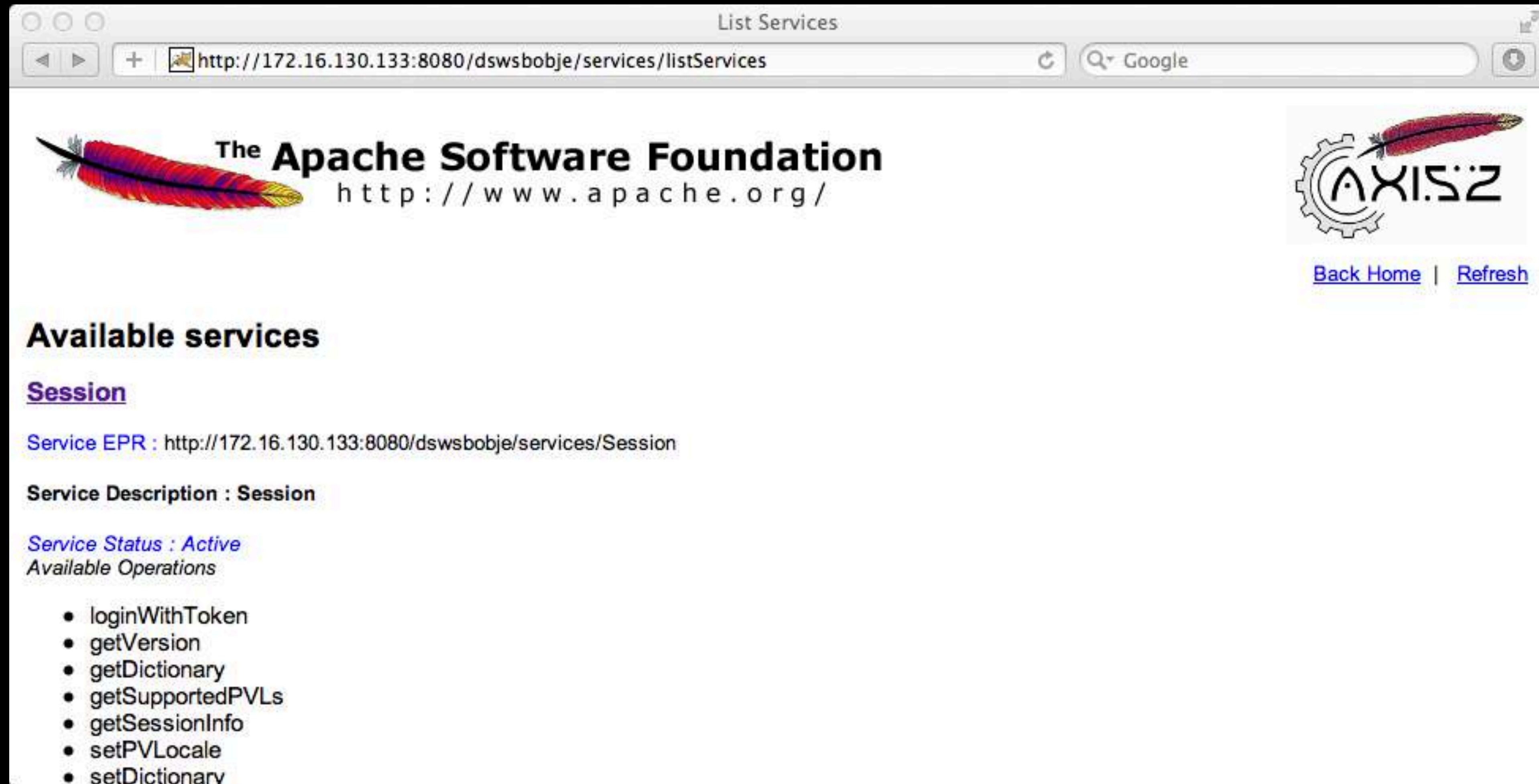
SAP Business Objects (BO)

- SAP Business Objects (a.k.a. BO, BO XI, BOBJ) provides Business Intelligence via a Service Orientated Architecture (SOA) - SOAP/WebServices.
- Very complicated architecture.
- Administrative interface - <http://server:6405/CmcApp> & <http://server:8080/CmcApp>
- Web Services - <http://server:8080/dswsbobje>
- Query interface - <http://server:6405/InfoViewApp>
- Reporting interface - <http://server:6045/AnalyticalReporting>

SAP Business Objects (BO)

- Fingerprinting (response contains version).
 - GET - `http://server:6405/AnalyticalReporting/AnalyticalReporting_merge_web.xml`
 - SOAP - `http://server:8080/dswsbobje/services/Session`
- User enumeration (error: invalid password for valid users)
 - SOAP - `http://server:8080/dswsbobje/services/session`
- Reflective and Stored XSS all over the place.

listServices



List Services

http://172.16.130.133:8080/dswsbobje/services/listServices

Google

The Apache Software Foundation
http://www.apache.org/

AXIS2

[Back Home](#) | [Refresh](#)

Available services

Session

Service EPR : http://172.16.130.133:8080/dswsbobje/services/Session

Service Description : Session

Service Status : Active

Available Operations

- loginWithToken
- getVersion
- getDictionary
- getSupportedPVLs
- getSessionInfo
- setPVLocale
- setDictionary

Metasploit - Business Objects

Demo

Armitage

Armitage View Hosts Attacks Workspaces Help

auxiliary

admin

sap

sap_mgmt_con_osexec

scanner

http

sap_businessobjects_user_brute

sap_businessobjects_user_brute_web

sap_businessobjects_user_enum

sap_businessobjects_version_enum

sap_icm_urlscan

sap

sap_mgmt_con_abaplog

sap_mgmt_con_brute_login

sap_mgmt_con_extractusers

172.26.0.200

172.26.0.201

172.26.0.100

172.26.0.101

172.26.0.98

172.26.0.99

Console X

```

MMMMI  MMMM  MMMMMM  MMMM  jMMMM
MMMMI  MMMM  MMMMMM  MMMM  jMMMM
MMMMI  MMMM  MMMMMM  MMMM#  JMMMM
MMMMR  ?MMMM  MMMM  .dMMMM
MMMMMm `?MM  MMMM` dMMMM
MMMMMMN ?MM  MM?  NMMMMN
MMMMMMMMNe      JMMMMMMMM
MMMMMMMMMMMMNm,  eMMMMMMMMMM
MMMMMMMMMMMMMMNx  MMMMMMMMMMMM
MMMMMMMMMMMMMMMMm+. .+MMMMMMMMMMMMM

      =[ metasploit v4.1.0-testing [core:4.1 api:1.0]
+ -- --[ 747 exploits - 389 auxiliary - 92 post
+ -- --[ 228 payloads - 27 encoders - 8 nops
      =[ svn r13973 updated today (2011.10.17)

msf >

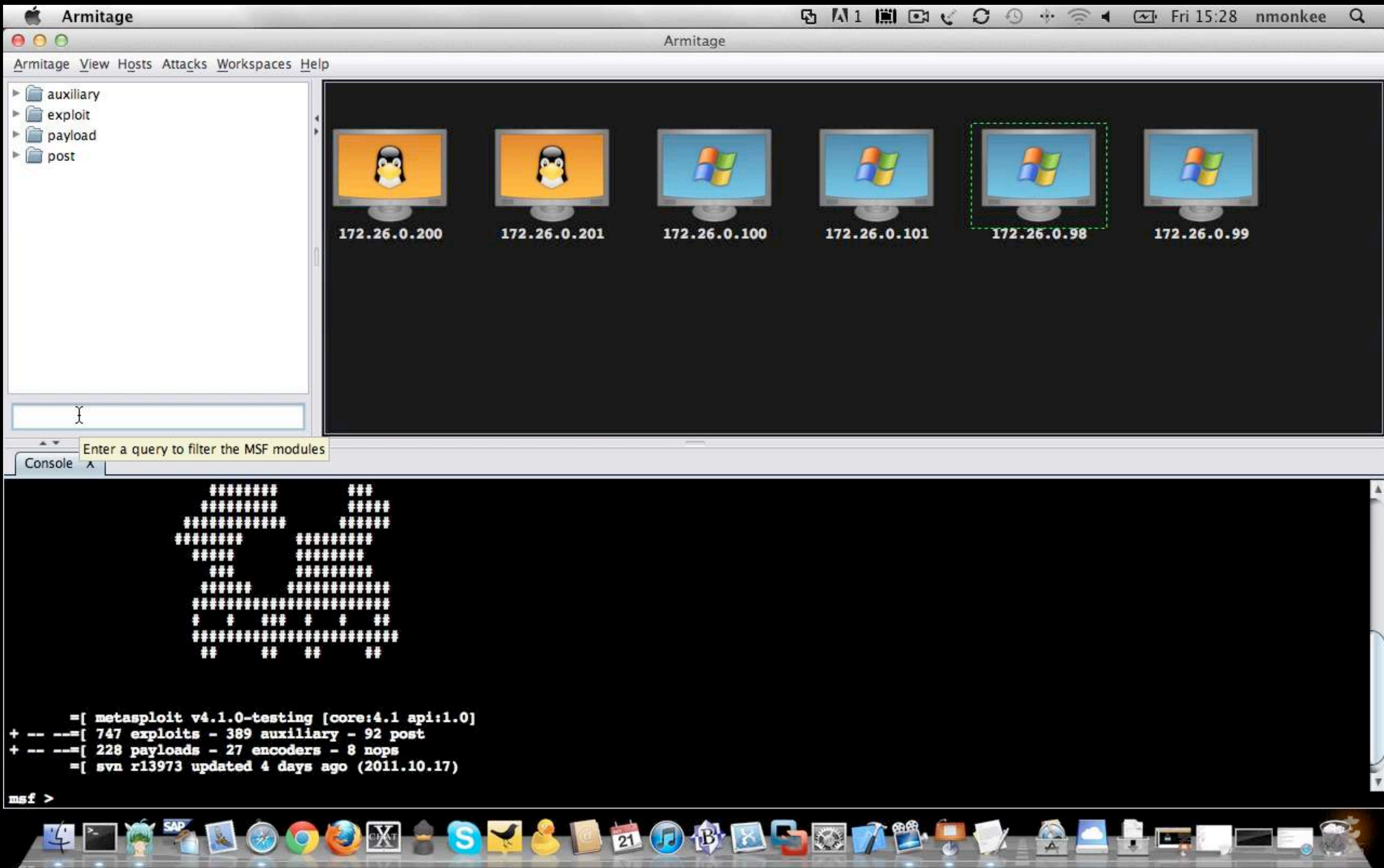
```


Axis2

- Business Objects uses Apache Axis2 for Web Services.
- Default credentials for Axis2 are stored in the axis2.xml file:
 - C:\Program Files\Business Objects\Tomcat55\webapps\zdswsbobje\WEB-INF\conf\axis2.xml
- `<parameter name="userName">admin</parameter>`
`<parameter name="password">axis2</parameter>`

Metasploit - Business Objects

Axis2 Demo



fin.

Ta Muchly for Listening

- Special thanks for peer review, excellent feedback and generally being cool dudes...
- Chris John Riley
- Mariano Nuñez Di Croce
- Steve Lord





Questions?
Dave Hartley

