

STEALING GUESTS... THE VMWARE WAY

Justin Morehouse & Tony Flick
ShmooCon 2010

DISCLAIMER

Standard disclaimer verbiage...

- Everything said, showed, implied, etc. is not the opinion of our employers, friends, dogs, VMware, ShmooCon, etc.
- This disclaimer is not endorsed by our lawyers.

ABOUT US

Justin Morehouse

- Assessment Lead @ Large Retailer in Southeast USA
- Controls 58.2% of the MacBook Pro flipping market on Craigslist

Tony Flick

- Principal @ FYRM Associates
- Has never mistaken Hunts ketchup for Heinz ketchup...EVER!

WARNING

What this presentation IS NOT:

- 0 day release - worked w/VMware
- A demonstration of rocket science

What this presentation IS:

- A reminder of the security implications of virtualization
- The culmination of 'sanity' projects

TIMELINE

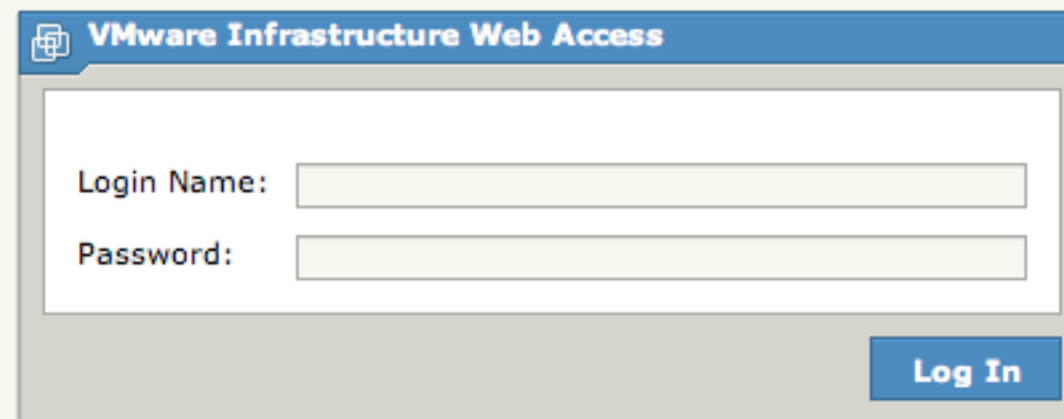
- Vulnerability identified on 5/14/09
- Reported to VMware on 5/15/09
- VMware responded on 5/21/09
- CVE-2009-3733 reserved on 10/20/09
- VMSA-2009-0015 released on 10/27/09
 - 'b. Directory Traversal vulnerability'

IDENTIFICATION

- Originally identified on VMware Server 2.0.1 build 156745 (on Ubuntu 8.04)
- Thought to be localized to inside of NAT interface of Host (8307/tcp)
- Can steal VMs from within other VMs... if NAT'd
 - Kinda cool, not really practical
- What we originally reported to VMware & submitted to ShmooCon

but.....

DOES THIS LOOK FAMILIAR?



The image shows a web browser window with a blue title bar that reads "VMware Infrastructure Web Access". Inside the window, there is a login form with two text input fields. The first field is labeled "Login Name:" and the second field is labeled "Password:". Below the password field, there is a blue button with the text "Log In".

HOW ABOUT THIS?

VMware ESX Server 3 Welcome



Getting Started

If you need to access this host remotely, use the following program to install VMware Infrastructure client software. After running the installer, start the client and log in to this host.

- [Download VMware Infrastructure Client](#)

To streamline your IT operations with VMware Infrastructure, use the following program to install VirtualCenter Server. VirtualCenter Server will help you consolidate and optimize workload distribution across ESX Server hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.

- [Download VMware VirtualCenter Server](#)

If you need more help, please refer to our documentation library:

- [VMware Infrastructure 3 Documentation](#)

For Administrators

VMware Infrastructure Web Access

VMware Infrastructure Web Access streamlines remote desktop deployment by allowing you to organize and share virtual machines using ordinary web browser URLs.

- [Log in to Web Access](#)

Web-Based Datastore Browser

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

- [Browse datastores in this host's inventory](#)

ESX Server Scripted Installer

This browser-based utility allows you to automate host provisioning.

- [Log in to the Scripted Installer](#)

For Developers

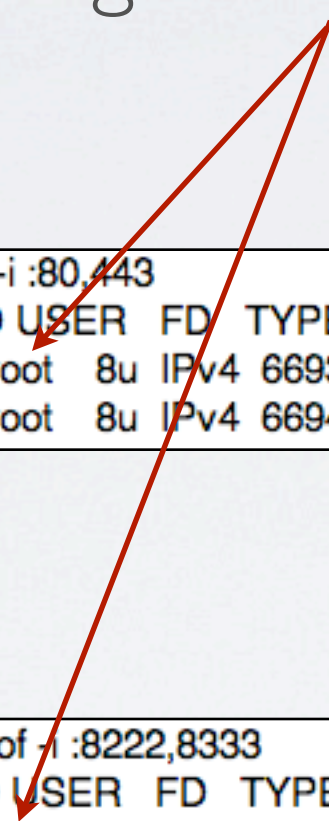
VULNERABILITY

- Web Access web servers also vulnerable
 - Server (default ports 8222/8333) - ../ x 6
 - ESX/ESXi (default ports 80/443) - %2E%2E/ x 6
- No longer requires NAT mode / Remotely exploitable
- Not as straightforward as originally thought
 - Still trivial to exploit because...

IT'S GOOD TO BE ROOT

- Web servers are running as root = complete access

- ESX/ESXi



```
root@esx:~# lsof -i :80,443
COMMAND  PID USER  FD  TYPE DEVICE SIZE NODE NAME
vmware-ho 1651 root   8u  IPv4  6693    TCP *:https (LISTEN)
vmware-ho 1651 root   8u  IPv4  6694    TCP *:http (LISTEN)
```

- Server

```
root@server:~# lsof -i :8222,8333
COMMAND  PID USER  FD  TYPE DEVICE SIZE NODE NAME
vmware-ho 6863 root   6u  IPv4  17272   TCP *:8333 (LISTEN)
vmware-ho 6863 root   7u  IPv4  17273   TCP *:8222 (LISTEN)
```


HOW IT WORKS ON SERVER

- Proxy used to redirect requests based on URL
- /etc/vmware/hostd/proxy.xml (includes mappings)
 - /sdk = 8307/tcp
 - /ui = 8308/tcp

```
<e id="1">
  <_type>vim.ProxyService.LocalServiceSpec</_type>
  <accessMode>httpsWithRedirect</accessMode>
  <port>8307</port>
  <serverNamespace>/sdk</serverNamespace>
</e>
<e id="2">
  <_type>vim.ProxyService.LocalServiceSpec</_type>
  <accessMode>httpsWithRedirect</accessMode>
  <port>8308</port>
  <serverNamespace>/ui</serverNamespace>
</e>
```


HOW IT WORKS ON SERVER

- Web server on 8308/tcp is vulnerable, but will only serve certain filetypes (xml, html, images, etc.)
- Web server on 8307/tcp is also vulnerable, but serves ALL filetypes
- Simply append /sdk to our URL request and we've got complete access to Host filesystem (including other Virtual Machines)
- ESX/ESXi - ALL web servers return ALL filetypes (no /sdk)

VULNERABLE VERSIONS

Server

- VMware Server 2.x < 2.0.2 build 203138 (Linux)
- VMware Server 1.x < 1.0.10 build 203137 (Linux)

ESX/ESXi

- ESX 3.5 w/o ESX350-200901401-SG
- ESX 3.0.3 w/o ESX303-200812406-BG
- ESXi 3.5 w/o ESXe350-200901401-I-SG

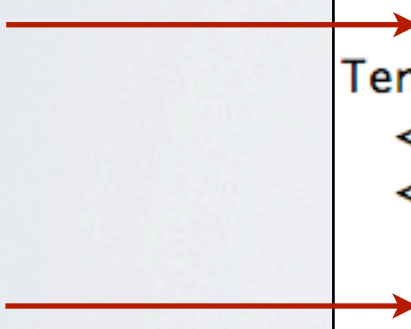
GUESTSTEALER

- Perl script remotely 'steals' virtual machines from vulnerable hosts
- Supports Server, ESX, ESXi
- Allows attacker to select which Guest to 'steal'
- Utilizes VMware configuration files to identify available Guests and determine associated files

VMINVENTORY.XML

- /etc/vmware/hostd/vmInventory.xml (default location)
- Gives us Guest inventory & location information


```
<ConfigRoot>
  <ConfigEntry id="0000">
    <objID>48</objID>
    <vmxCfgPath>/var/lib/vmware/Virtual Machines/
TenableAppliance-1.0.3/TenableAppliance.vmx</vmxCfgPath>
  </ConfigEntry>
  <ConfigEntry id="0001">
    <objID>80</objID>
    <vmxCfgPath>/var/lib/vmware/Virtual Machines/Snort
(Ubuntu 8.0.3)/Snort (Ubuntu 8.0.3).vmx</vmxCfgPath>
  </ConfigEntry>
</ConfigRoot>
```



GUEST .VMX & .VMDK

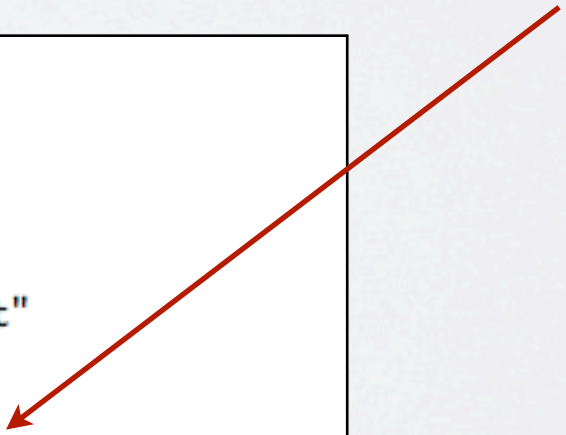
- .vmx gives us Guest config and file locations

```
scsi0.present = "FALSE"  
scsi0.sharedBus = "none"  
memsize = "512"  
scsi0:0.present = "FALSE"  
scsi0:0.fileName = "Windows XP.vmdk"  
scsi0:0.writeThrough = "TRUE"  
ethernet0.present = "TRUE"
```



- .vmdk (disk image) can point to other .vmdk images

```
# Disk DescriptorFile  
version=1  
encoding="UTF-8"  
CID=b74fb48a  
parentCID=ffffffff  
createType="monolithicFlat"  
  
# Extent description  
RW 20971520 FLAT "Windows XP-flat.vmdk" 0
```



LIVE DEMO

MITIGATION STRATEGIES

- Patch, patch, patch
 - Hosts are an attractive target (compromise one = access many)
- Better yet...Segment, segment, segment
 - Segment management interfaces
 - Segment systems of different security levels
 - Don't share physical NICs between different security levels
- Virtualization is not always the 'best answer'

QUESTIONS?

GuestStealer available for download @

www.fyrmassociates.com