



DEFCON16

Virtually Hacking

08th August 2008

john.fitzpatrick@mwrinfosecurity.com

Why VMware?

- Virtualisation has taken off and is here to stay
- Many of our clients are using virtualisation technologies
- Virtualisation services are being sold
- VMware is the dominant product*
- Need to be familiar with a product in order to hack it

*source - silicon.com

Structure

- VMware
 - Different flavours
 - Key concepts
- Hacking VMware Server + Demo
- Hacking VMware ESX + Demo
- dradis – putting it all together
- Recommendations
 - Am I going to get owned?

Structure

- **VMware**
 - **Different flavours**
 - **Key concepts**
- Hacking VMware Server + Demo
- Hacking VMware ESX + Demo
- dradis – putting it all together
- Recommendations
 - Am I going to get owned?

Different Flavours

- Player
- Workstation
- Server (GSX)
- ESX

Different Flavours

- Player
- ~~Workstation~~
- **Server (GSX)**
- **ESX**

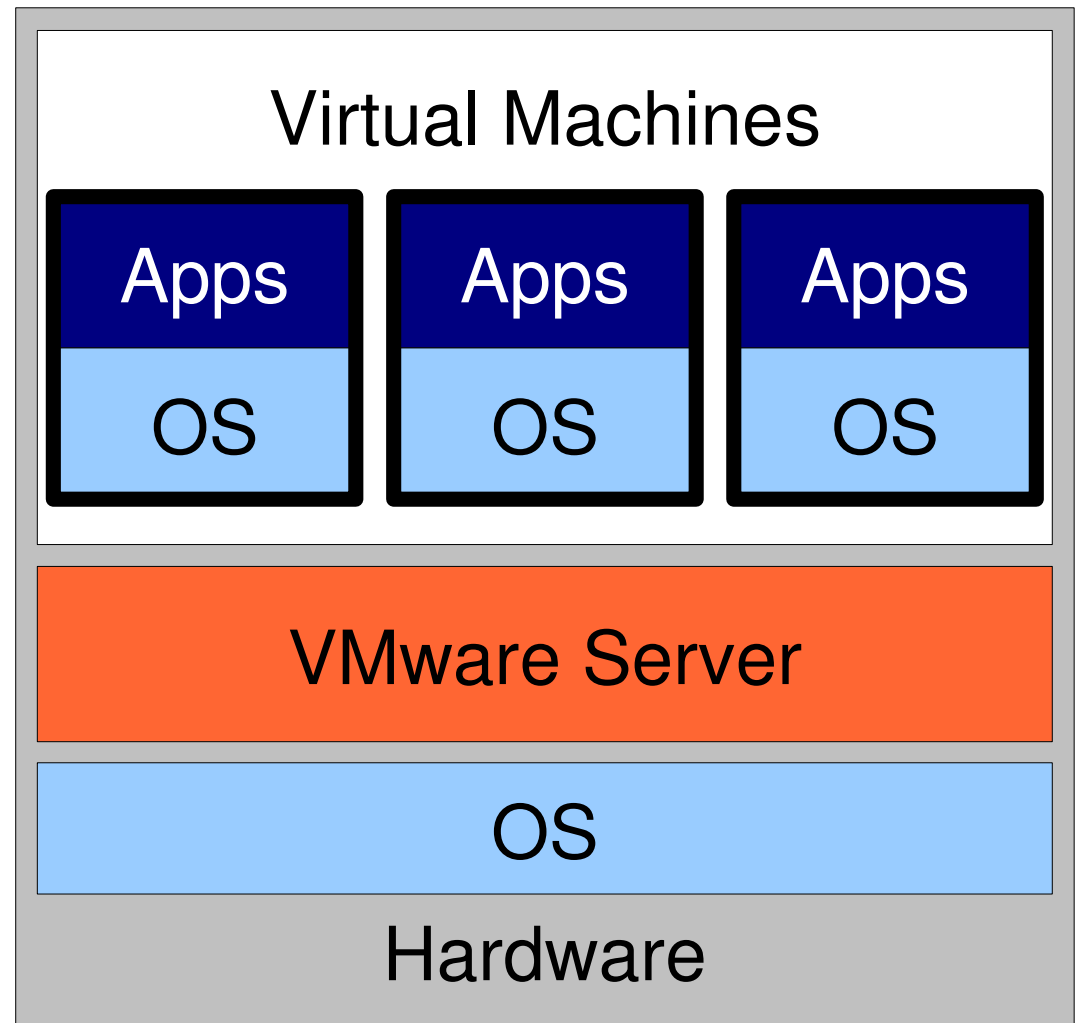
Key concepts



- One server can run multiple operating systems

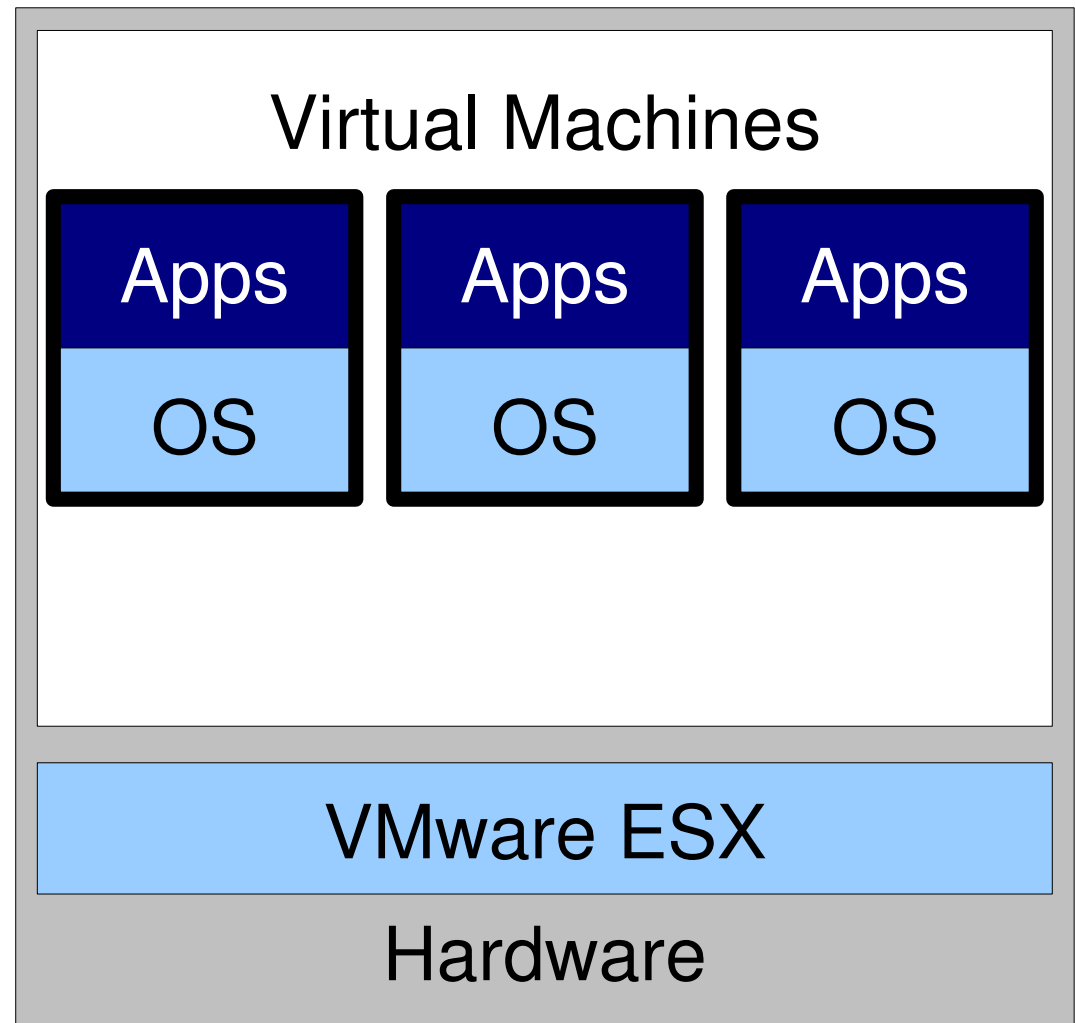
Key concepts

VMware Server



Key concepts

VMware ESX



Key concepts

Overview of the main files which make up a virtual machine

- Primary configuration file (.vmx)
- Virtual disk file – the virtual machines hard drive (.vmdk)
- Virtual machines snapshot (.vmsn)
- Virtual machines page file (.vmem)

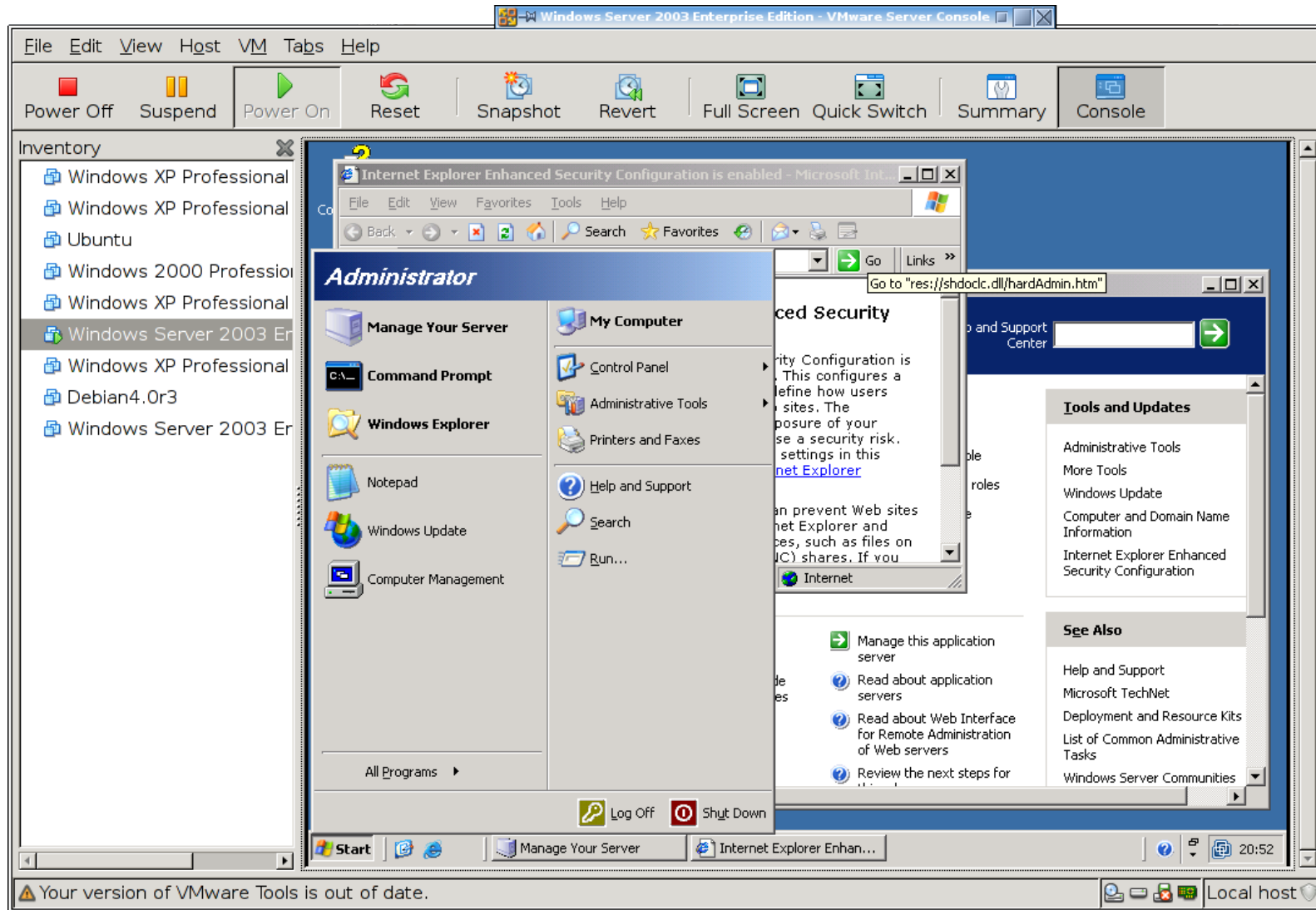
Key concepts

- Virtual machine disk file can be mounted
- Files can therefore easily be read from the disk
- Demo...

Structure

- VMware
 - Different flavours
 - Key concepts
- **Hacking VMware Server + Demo**
- Hacking VMware ESX + Demo
- dradis – putting it all together
- Recommendations
 - Am I going to get owned?

VMware:Server



VMware:Server

Interesting ports on 192.168.1.63:

Not shown: 1707 closed ports

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
80/tcp	open	http
111/tcp	open	rpcbind
113/tcp	open	auth
389/tcp	open	ldap
902/tcp	open	iss-realsecure-sensor

vmware-authd



VMware:Server

```

220 VMware Authentication Daemon Version 1.0, MKSDisplayProtocol:VNC
USER defcon16
331 Password required for defcon16.
XPAS mY+glrSaoIH4
230 User defcon16 logged in.
GLOBAL server-vmdb
200 Connect Global
7 VERSION1
1 11 31
1
.7 VERSION1
1 11 31
1
6 STATUS1 01
1
.9 SUBSCRIBE1
9 /db/info/1 |
1
.6 SCHEMA9 /db/info/1
1 01 00 1 11 00 0 0 0 1 01
1 01 04 cmd/1 11 00 0 0 0 1 01
1 01 43 ##/1 71 00 0 0 0 1 01
1 01 73 op/1 71 60 0 0 0 1 01
1 02 106 query/1 71 00 0 0 0 1 01
1 02 163 in/1 71 00 0 0 0 1 01
1 02 197 filter/1 71 10 0 0 0 1 01
1 02 19b searchPath/1 71 10 0 0 0 1 01
1 02 19a tuplePath/1 71 00 0 0 0 1 01
1 02 292 #/1 71 10 0 0 0 1 01
1 02 164 .../1 71 00 0 0 0 1 01

```

```

220 VMware Authentication Daemon Ve
USER defcon16
331 Password required for defcon16.
XPAS mY+glrSaoIH4
230 User defcon16 logged in.
GLOBAL server-vmdb
200 Connect Global
7 VERSION1
1 11 31
1
.7 VERSION1
1 11 31
1
6 STATUS1 01
1
.9 SUBSCRIBE1

```

VMware:Server - Tools

vmware-cmd

- List VMs
- Get state
- Start/Stop
- Get config
- Get remote connections
- Set guest info

VMware:Server - Tools

VMware VIX API

- List VMs
- Power On/Off
- Login Guest
- Copy file from host to guest / guest to host
- Run program in guest
- Run script in guest

VMware:Server - Tools

VMware VIX API

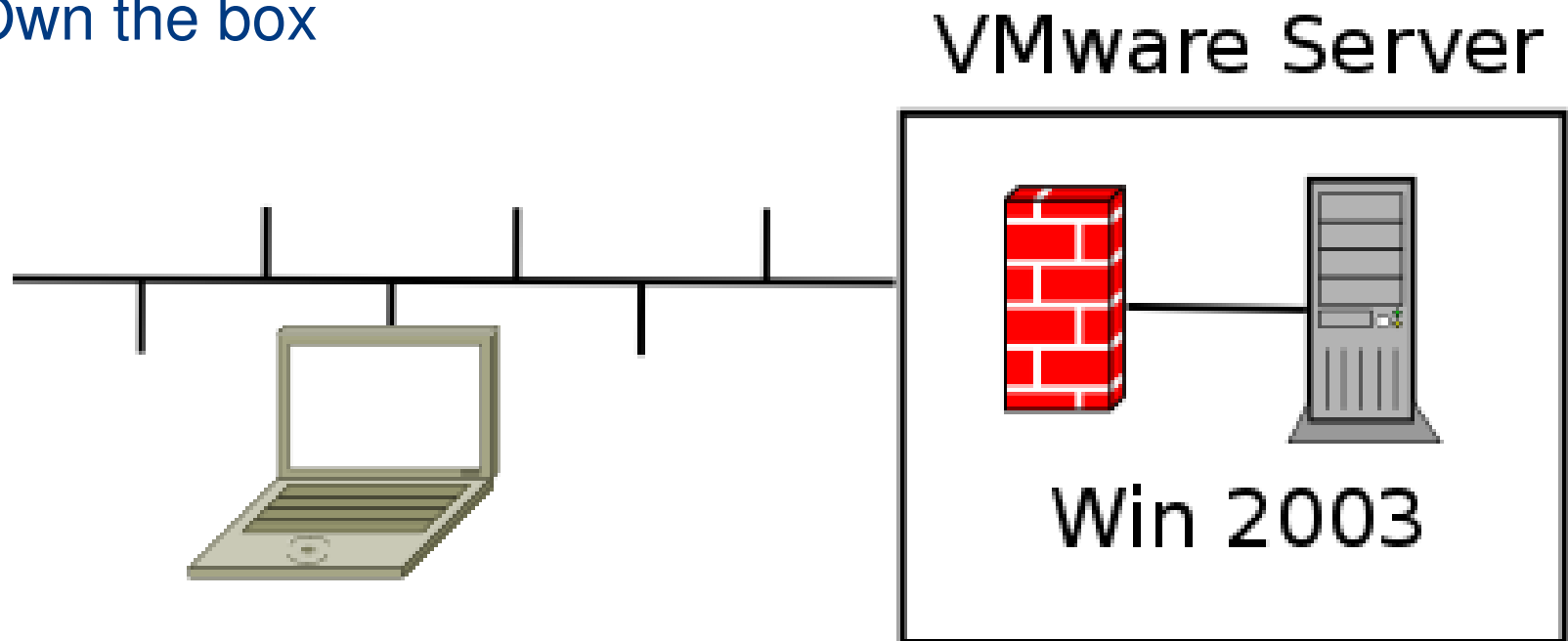
- Ruby bindings

```
1: require 'ruby_vix'  
2: Vix.RunProgramInGuest('10.0.0.9', 902, s_username, s_password, vmusername,  
    vmpassword, '/var/vms/windows.vmx', 'net user vmuser vmuser /ADD', "")
```

- Easily scriptable
- Equivalent to 130 lines of C

VMware:Server - Demo

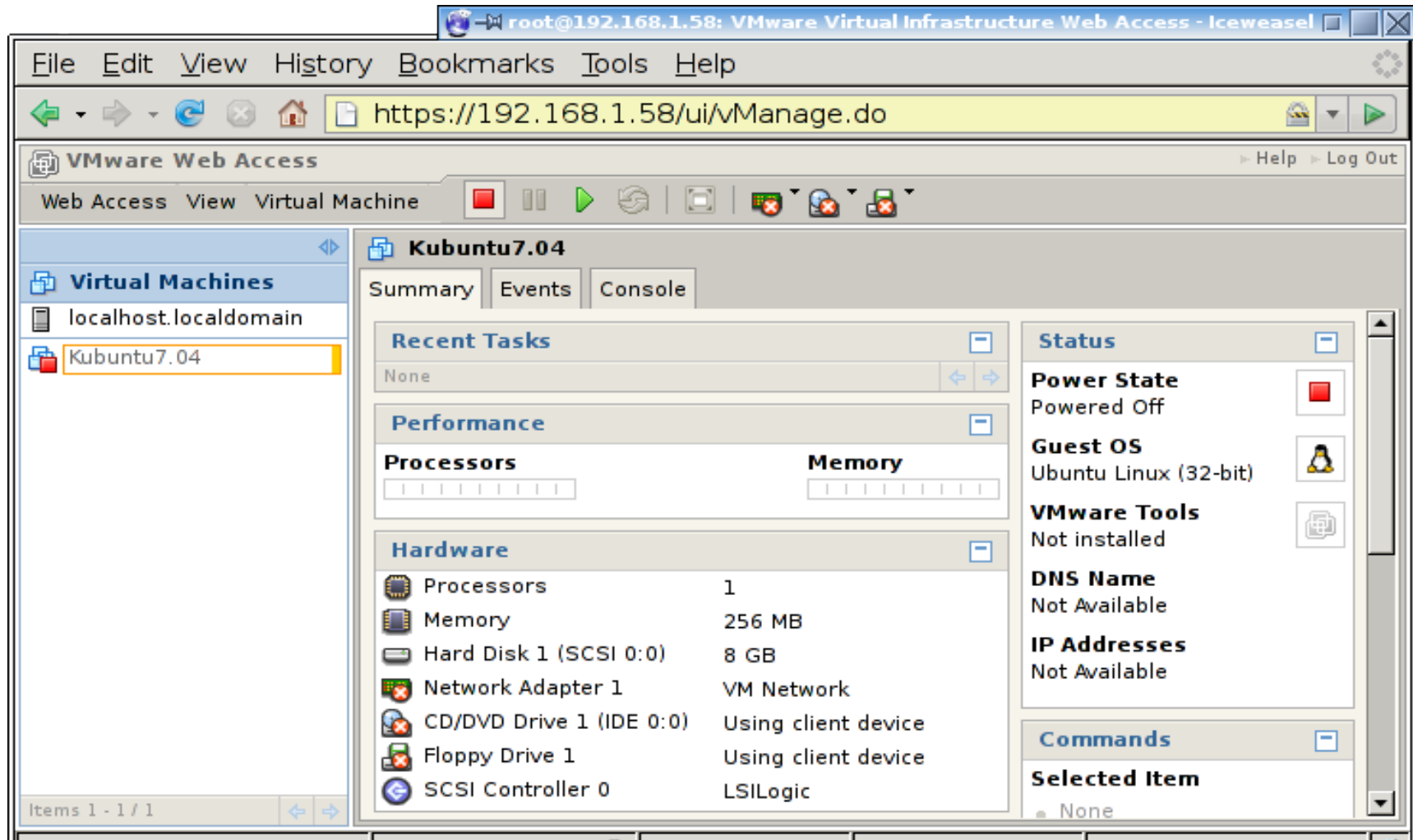
- Obtain credentials
- Extract information
- Own the box



Structure

- VMware
 - Different flavours
 - Key concepts
- Hacking VMware Server + Demo
- **Hacking VMware ESX + Demo**
- dradis – putting it all together
- Recommendations
 - Am I going to get owned?

VMware:ESX



VMware:ESX

The screenshot displays the VMware Infrastructure Client interface. The main window title is "192.168.1.58 - VMware Infrastructure Client". The interface is divided into several sections:

- Navigation:** Includes "Inventory" and "Administration" buttons at the top.
- Tree View:** Shows the hierarchy: localhost.localdomain > VMware ESX Server, 3.5.0, 64607 | Evaluation (60 day(s) remaining) > Kubuntu7.
- Configuration Tabs:** Summary, Virtual Machines, Resource Allocation, Performance, Configuration (selected), Users & Groups, Events, Permissions.
- Hardware Section:** Lists Processors, Memory, Storage, Networking (selected), Storage Adapters, and Network Adapters.
- Software Section:** Lists Licensed Features, Time Configuration, DNS and Routing, Virtual Machine Startup/Shutdown, and Virtual Machine Swapfile Location.
- Networking Diagram:** Shows two virtual switches:
 - vSwitch0:** Connected to a "VM Network" (1 virtual machine(s) | VLAN ID *) which is connected to the "Kubuntu7.04" VM. It is also connected to physical adapters "vmnic1" and "vmnic0", both with speed 100 and full duplex.
 - vSwitch1:** Connected to a "Service Console" (vswif0 : 192.168.1.58).
- Recent Tasks Table:**

Name	Target	Status	Initiated by	Time	Start Time	Comp
Browse Diagnostic Man...	localhost.local...	Completed	root	21/06/2008 00:45:18	21/06/2008 00:45:18	21/0€
Browse Diagnostic Man...	localhost.local...	Completed	root	21/06/2008 00:45:18	21/06/2008 00:45:18	21/0€

VMware:ESX

Interesting ports on 192.168.1.58:

Not shown: 65528 filtered ports

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
427/tcp	closed	svrloc
443/tcp	open	https
902/tcp	open	iss-realsecure
903/tcp	open	iss-console-mgr
5988/tcp	open	unknown
5989/tcp	open	unknown

VMware:ESX

- Provides a web service (SOAP) interface
 - <https://vmware-esx/sdk>
- Web server
 - <https://vmware-esx/ui>
 - <https://vmware-esx/mob>
- VMware authd still available on port 902
 - VMware-serverd not present
- COS (Console Operating System) via SSH
 - Red Hat derived

Vmware:ESX - Tools

VI SDK

- Example operations include:
 - RebootGuest
 - RebootHost_Task
 - ScanHostPatch_Task
 - CreateUser
 - RemoveVirtualSwitch

Vmware:ESX - Demo

- Run Tools

Structure

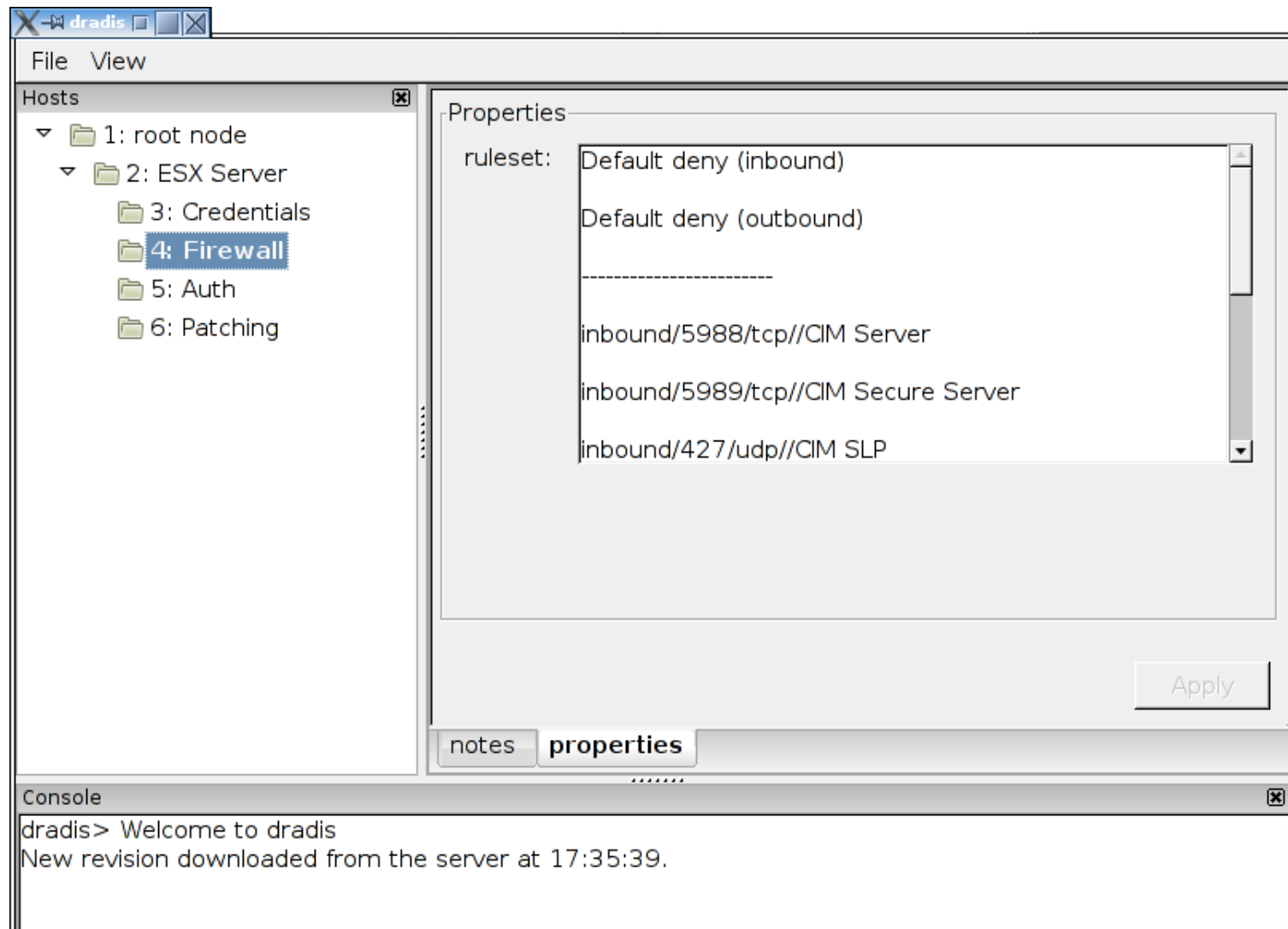
- VMware
 - Different flavours
 - Key concepts
- Hacking VMware Server + Demo
- Hacking VMware ESX + Demo
- **dradis – putting it all together**
- Recommendations
 - Am I going to get owned?

dradis – A Quick Intro

- Tool for structuring information
- Client/Server architecture
- Ruby based
- Extensible
 - Add modules
 - Put together a methodology
- Intercept actions/results to perform conditional operations

<http://dradis.sourceforge.net>

dradis – A Quick Intro



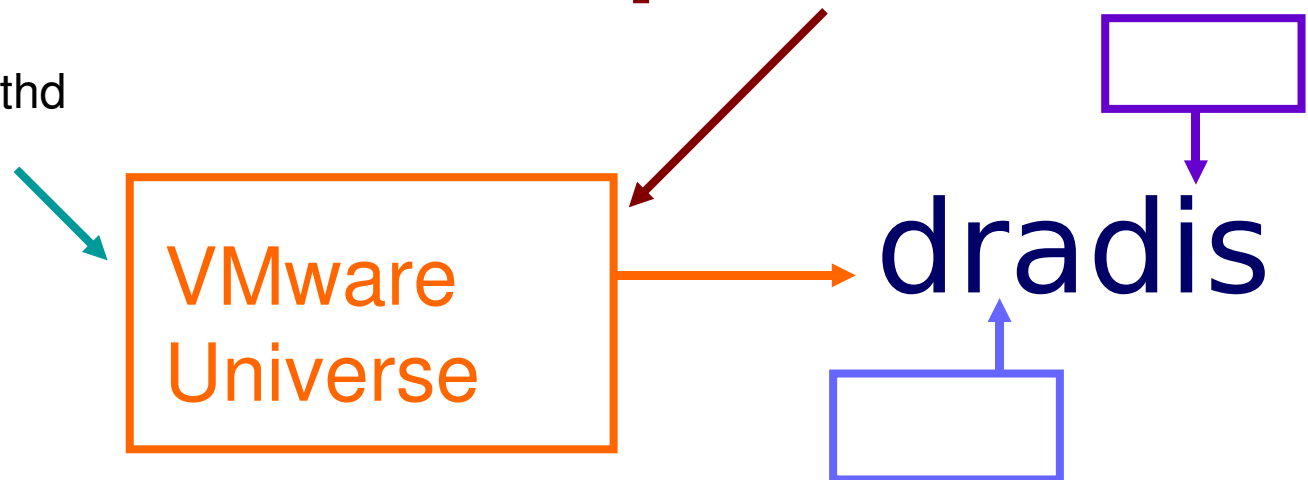
dradis

concepts

- VMware Server
- VMware ESX
- virtual switch
- VIX API
- authentication
- vnic0
- vmware-authd
- ...

actions

- create_user
- reboot guest
- patching_level
- find_version
- user_list
- reboot



dradis

- Let's see it in action
- Demo

Structure

- VMware
 - Different flavours
 - Key concepts
- Hacking VMware Server + Demo
- Hacking VMware ESX + Demo
- dradis – putting it all together
- **Recommendations**
 - **Am I going to get owned?**

Am I Going to Get Owned?

- Have you followed VMware's security guidance?
- Have you applied updates?

Am I Going to Get Owned?

- VMware will normally be a juicy target for an attacker
- Keep management networks separate from your core networks and guest networks
- Harden the virtual network
 - Disable promiscuous mode
 - Reject MAC address changes
 - Reject traffic with a forged IP address

Am I Going to Get Owned?

- Disable copy and paste between guest and host
- Can guest OS read the CD drive on the host OS?
- Am I logging enough / too much?
- There is nothing stopping you from hardening the installation beyond the default
 - Don't forget tools like Bastille or CISscan
 - Do you use all of the services running?

Future work

- Still plenty to play with
- Still lots of VMware technologies to cover

To Conclude

- Have a play with the tools
- Let me know what you think
- Let me know any new features you would like to see
- Tools available from:
 - <http://www.tinternet.org.uk>
 - <http://www.mwrinfosecurity.com>
- dradis is available from:
 - <http://dradis.sourceforge.net>

To Conclude

- Questions?