DEFCON16

Virtually Hacking

08 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?

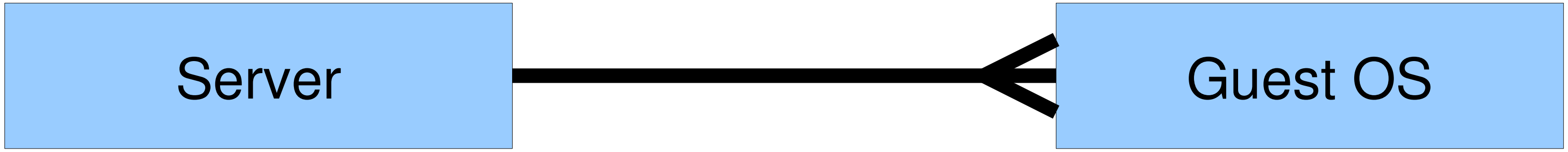
Different Flavours

- Player
- Workstation
- Server (GSX)
- ESX

Different Flavours

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

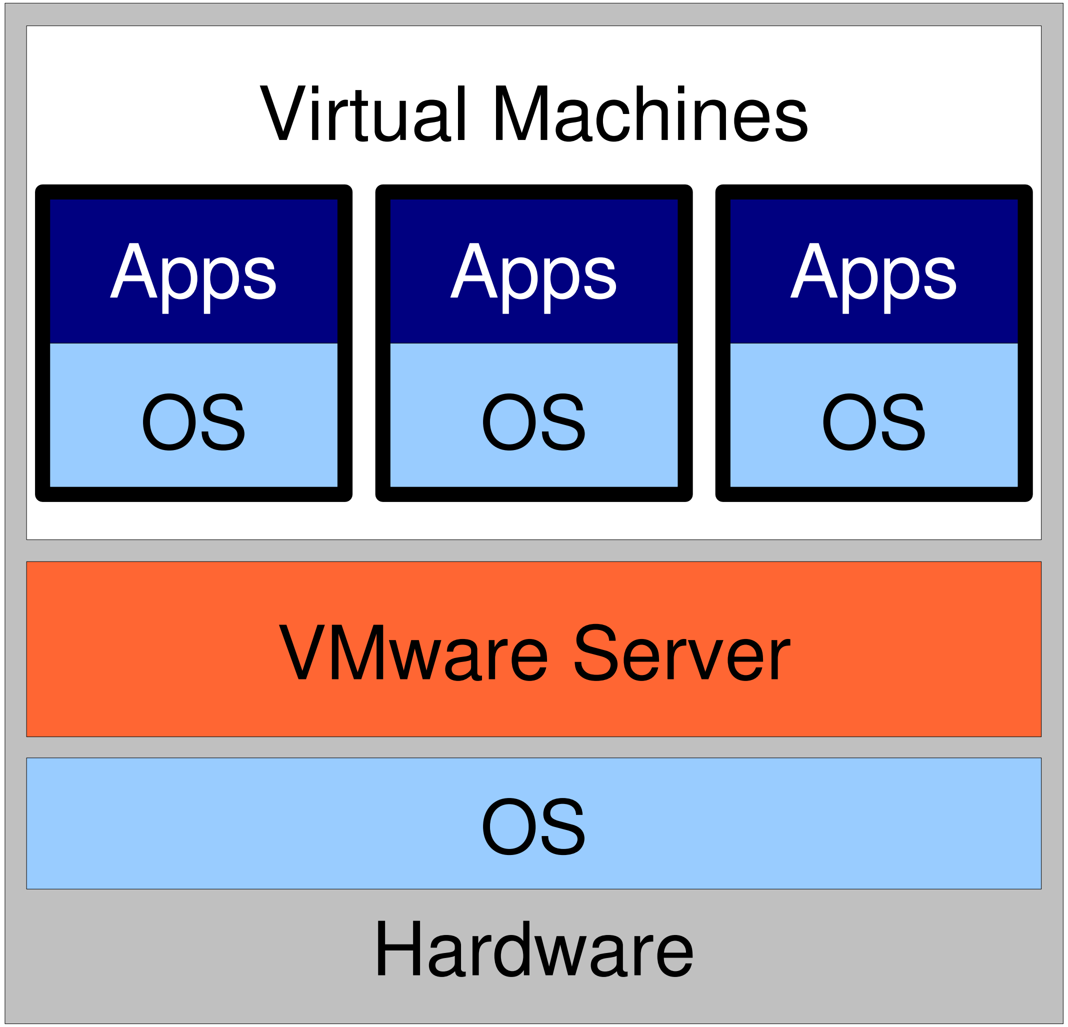
Key concepts



- One server can run multiple operating systems

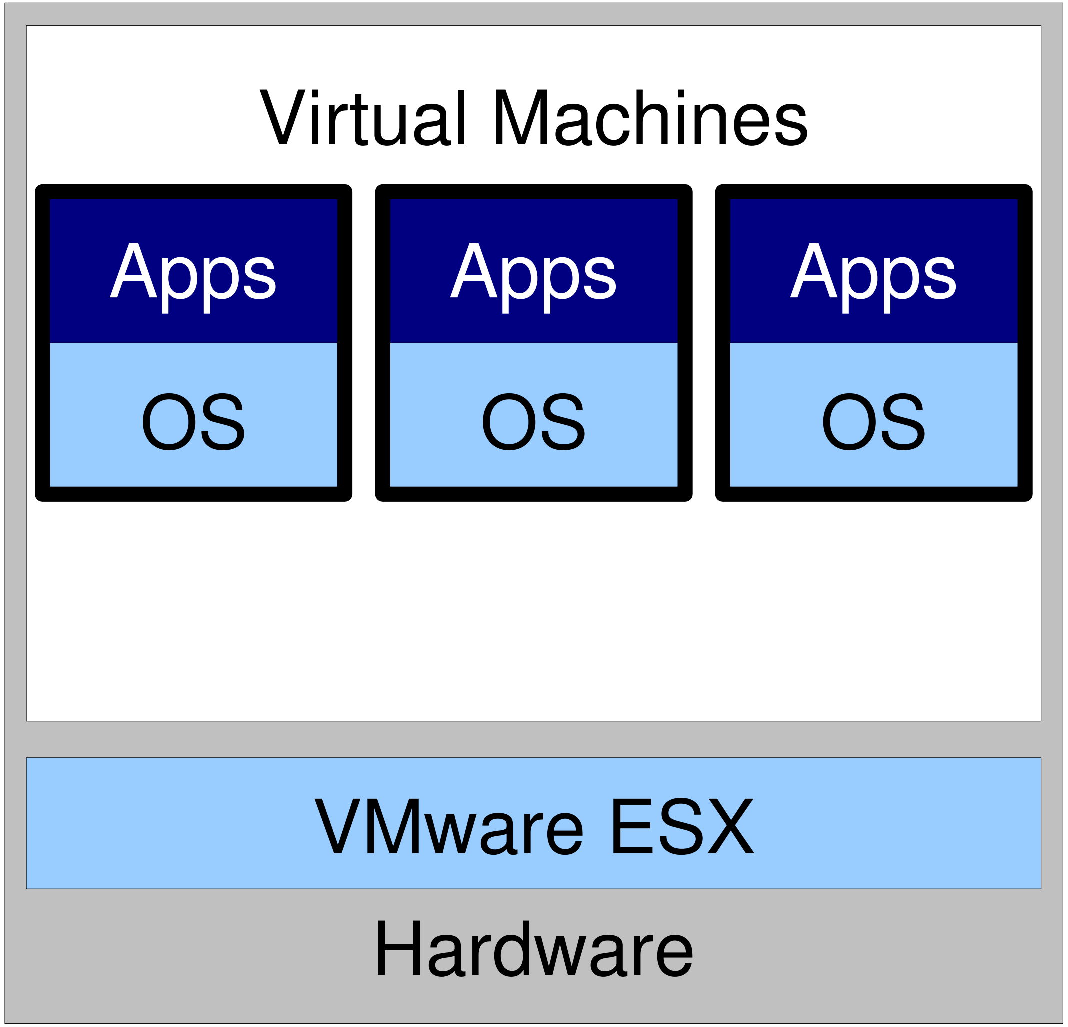
Key concepts

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)

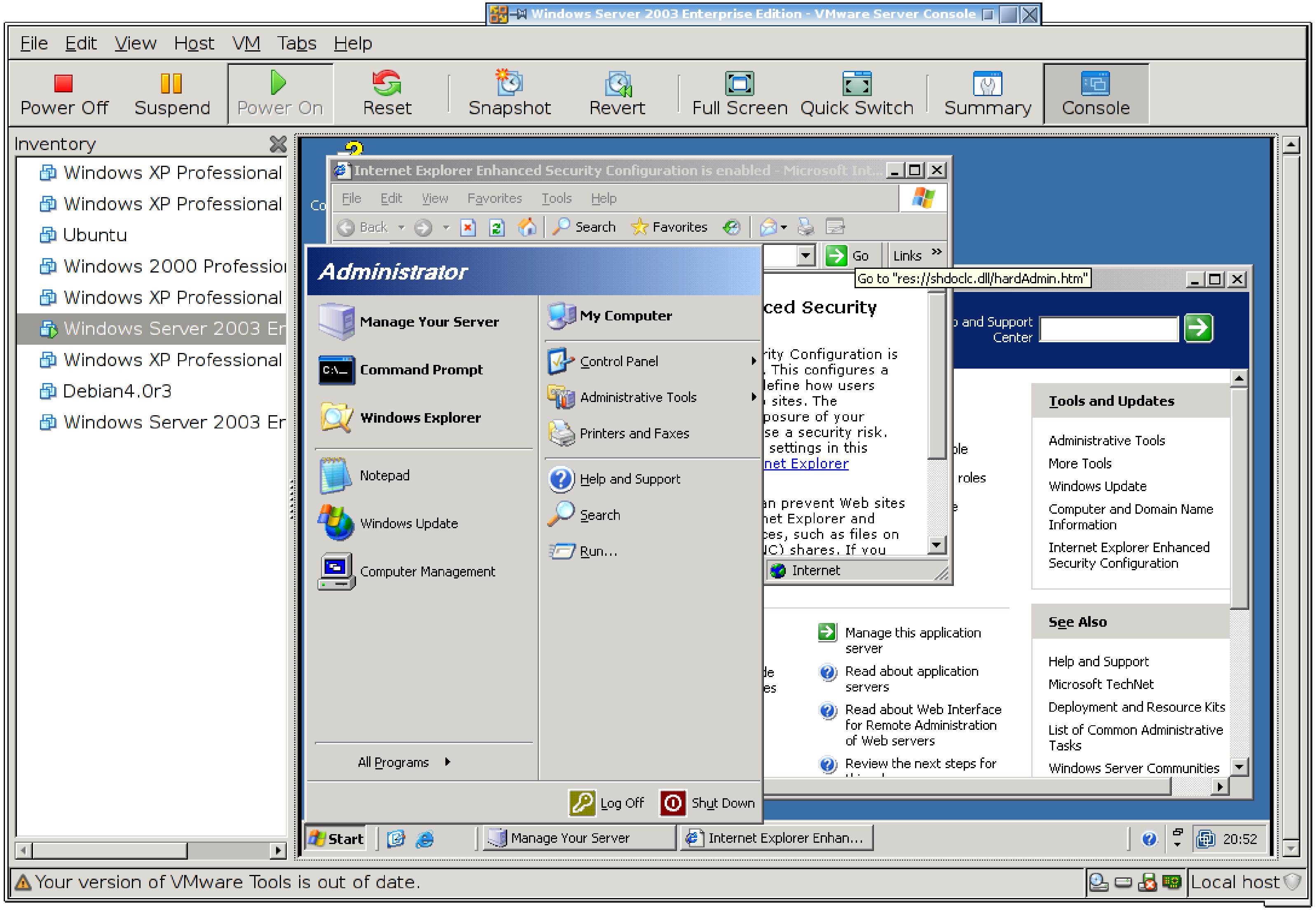
Key concepts

- 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



ced Security

rity Configuration is . This configures a lefine how users sites. The posure of your se a security risk. settings in this net Explorer

n prevent Web sites net Explorer and ces, such as files on IC) shares. If you

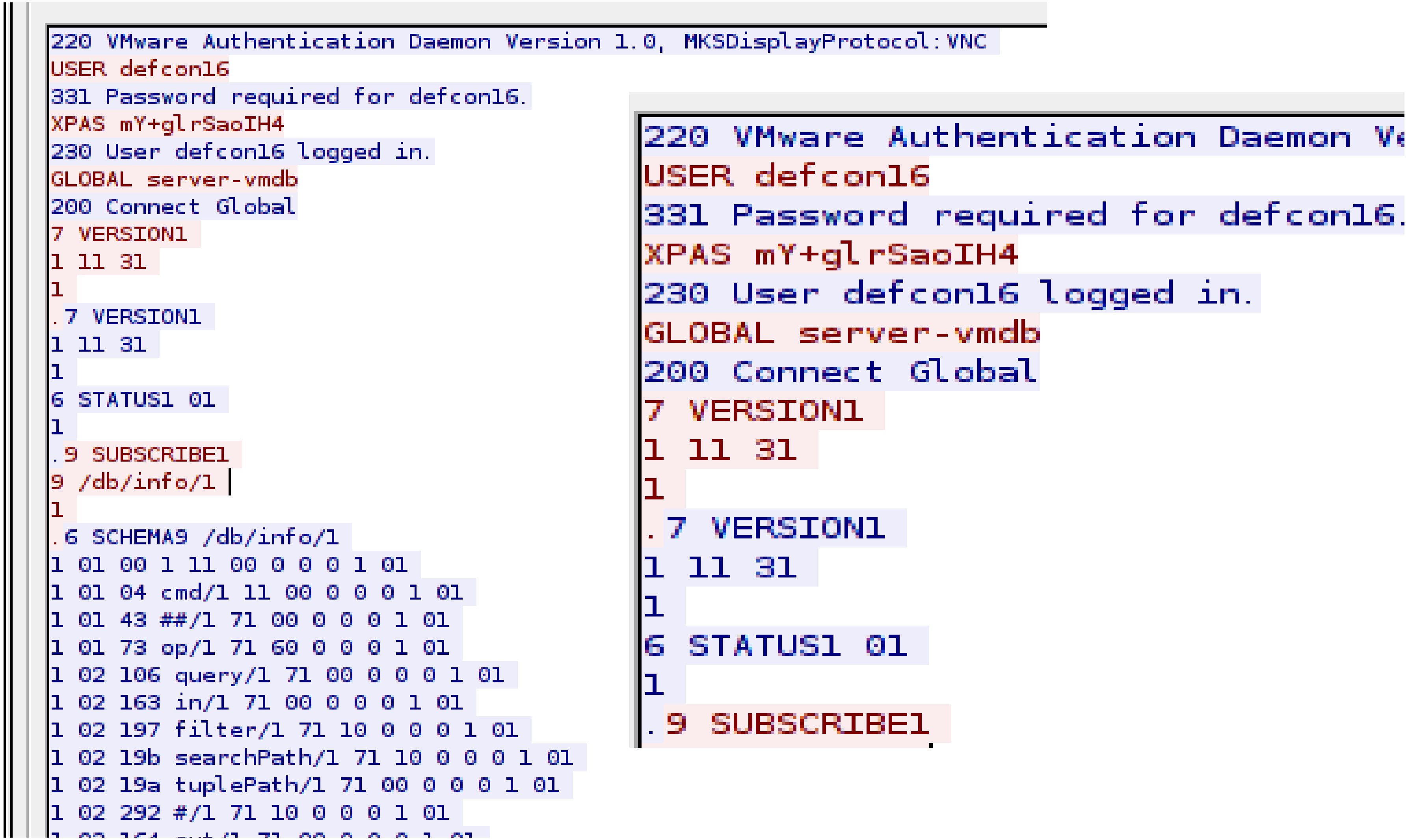
Your version of VMware Tools is out of date.

VMware:Server

```
Interesting ports on 192.168.1.53:
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 out/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.pl

- List VM's
- Get state
- Start/Stop
- Get config
- Get remote connections
- Set guest info

VMware:Server - Tools

VMware VIX API

- List VM's
- 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

```
require 'ruby_vix'
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

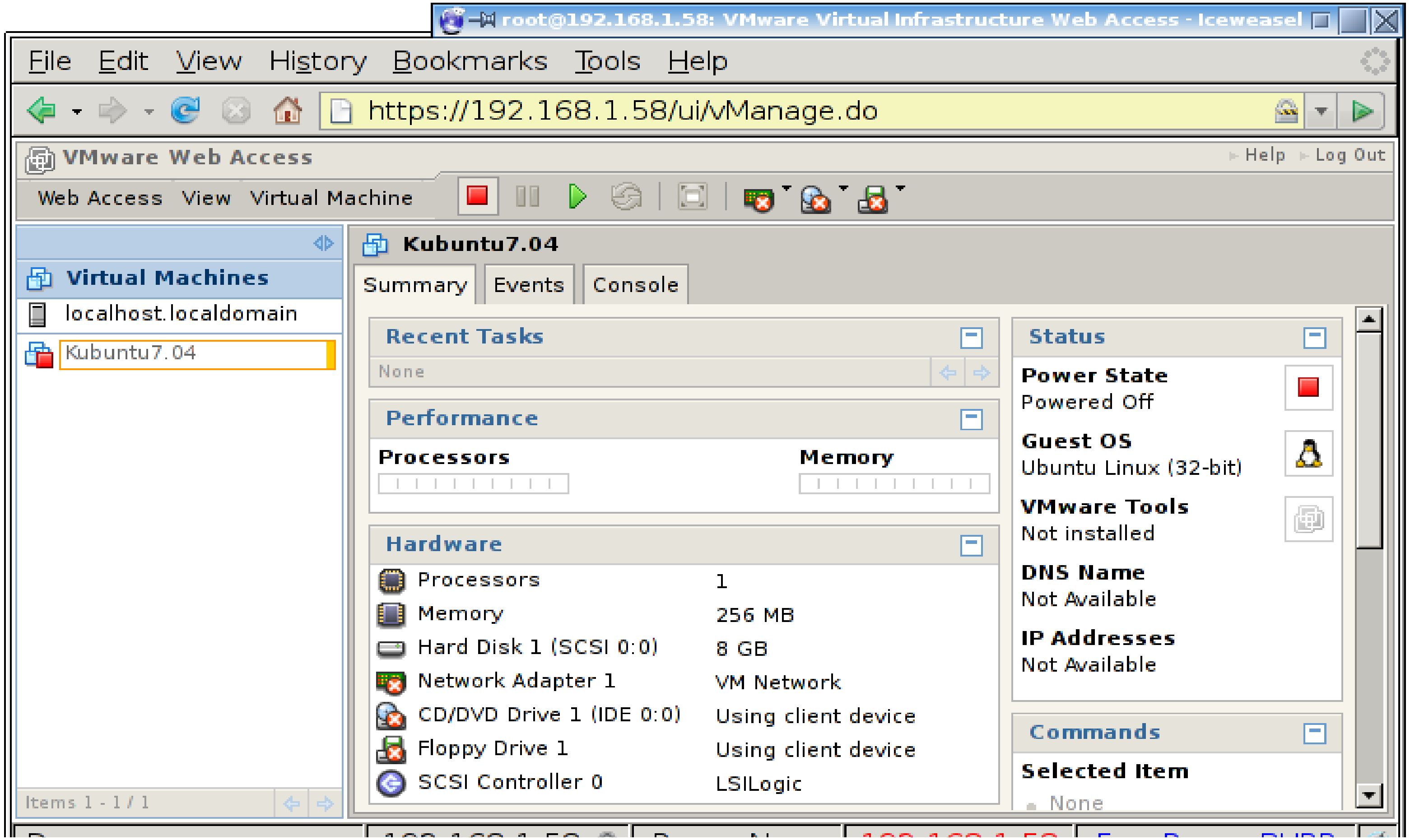
VMware:Server - Demo

- 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



Processors	1
Memory	256 MB
Hard Disk 1 (SCSI 0:0)	8 GB
Network Adapter 1	VM Network
CD/DVD Drive 1 (IDE 0:0)	Using client device
Floppy Drive 1	Using client device
SCSI Controller 0	LSILogic

Power State
Powered Off

Guest OS
Ubuntu Linux (32-bit)

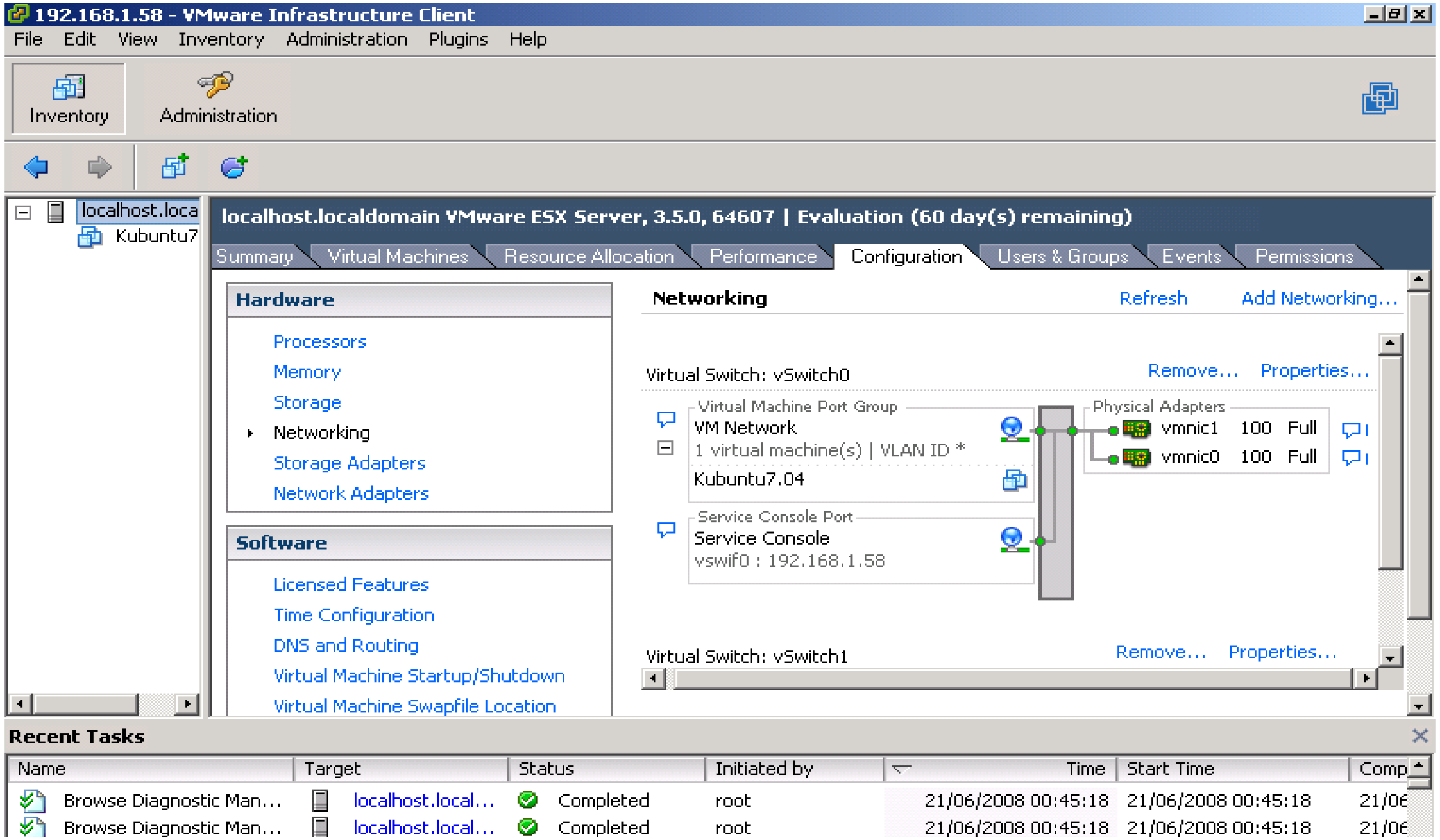
VMware Tools
Not installed

DNS Name
Not Available

IP Addresses
Not Available

MWR InfoSecurity

VMware:ESX



localhost.localdomain VMware ESX Server, 3.5.0, 64607 | Evaluation (60 day(s) remaining)

Hardware

- Processors
- Memory
- Storage
- Networking
- Storage Adapters
- Network Adapters

Software

- Licensed Features
- Time Configuration
- DNS and Routing
- Virtual Machine Startup/Shutdown
- Virtual Machine Swapfile Location

Networking

Virtual Switch: vSwitch0

Virtual Machine Port Group
VM Network
1 virtual machine(s) | VLAN ID *
Kubuntu7.04

Service Console Port
Service Console
vswif0 : 192.168.1.58

Physical Adapters		
vmnic1	100	Full
vmnic0	100	Full

Virtual Switch: vSwitch1

Recent Tasks

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	21/06
Browse Diagnostic Man...	localhost.local...	Completed	root	21/06/2008 00:45:18	21/06/2008 00:45:18	21/06

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 API

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

Vmware:ESX - Demo

- Perform checks unauthenticated
- Exploit weaknesses

Structure

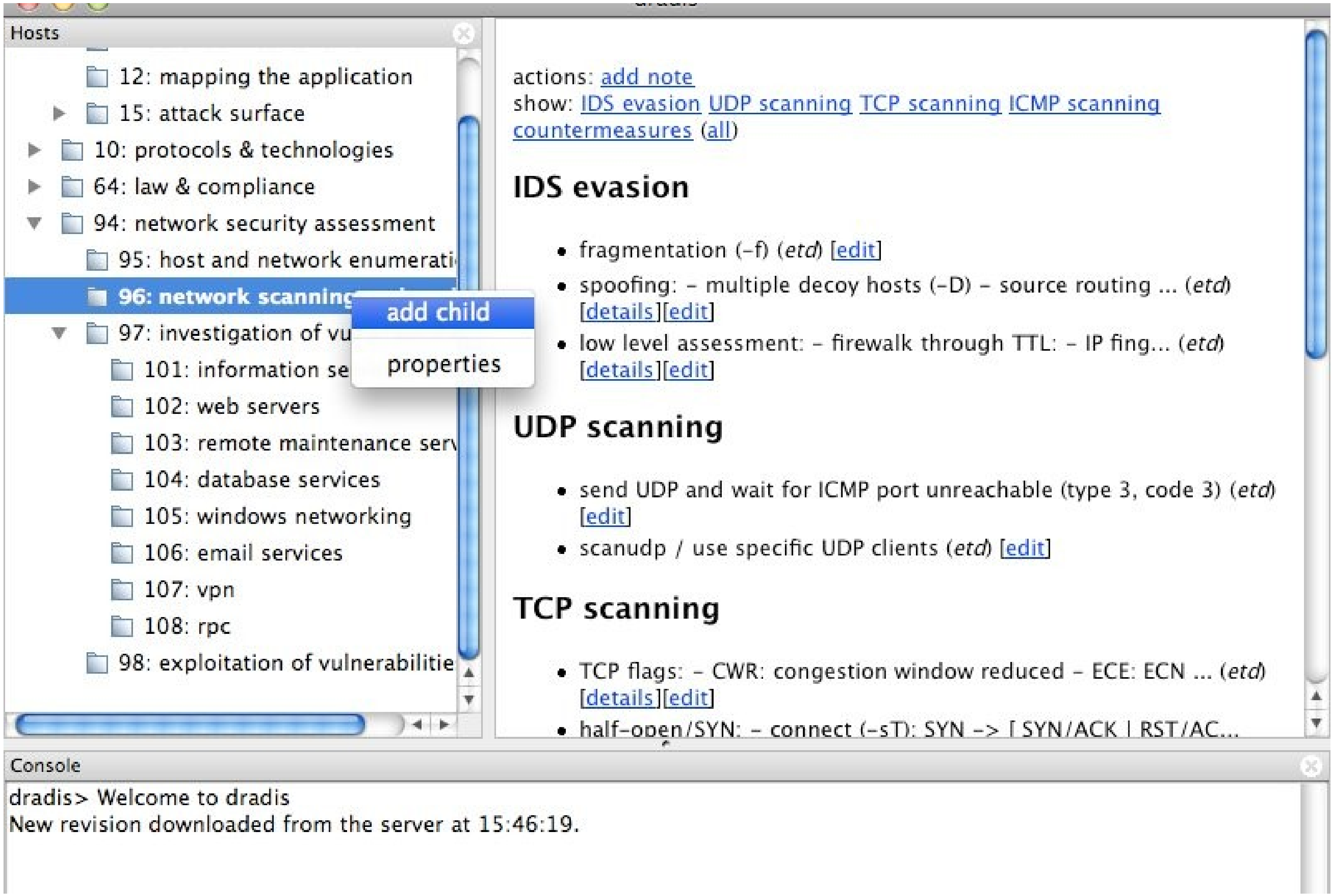
- VMware
  - Different flavours
  - Key concepts
- Hacking VMware Server + Demo
- Hacking VMware ESX + Demo
- **dradis – putting it all together**
- Recommendations
  - Am I going to get owned?

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



- 12: mapping the application
- 15: attack surface
- 10: protocols & technologies
- 64: law & compliance
- 94: network security assessment
  - 95: host and network enumerati
  - 96: network scanning
  - 97: investigation of vu
    - 101: information se
    - 102: web servers
    - 103: remote maintenance serv
    - 104: database services
    - 105: windows networking
    - 106: email services
    - 107: vpn
    - 108: rpc
  - 98: exploitation of vulnerabilitie

actions: [add note]

show: [IDS evasion] [UDP scanning] [TCP scanning] [ICMP scanning] [countermeasures] ([all])

IDS evasion

- fragmentation (-f) (*etd*) [edit]
- spoofing: - multiple decoy hosts (-D) - source routing ... (*etd*) [details][edit]
- low level assessment: - firewalk through TTL: - IP fing... (*etd*) [details][edit]

UDP scanning

- send UDP and wait for ICMP port unreachable (type 3, code 3) (*etd*) [edit]
- scanudp / use specific UDP clients (*etd*) [edit]

TCP scanning

- TCP flags: - CWR: congestion window reduced - ECE: ECN ... (*etd*) [details][edit]
- half-open/SYN: - connect (-sT): SYN -> [SYN/ACK | RST/AC...

```
dradis> Welcome to dradis
New revision downloaded from the server at 15:46:19.
```

dradis

- Provide it with a description of the environment
- It can then provide checks or operations based on this
- e.g.

Host is ESX	->	Determine version
Version is 3.5	->	Determine services
SSH is enabled	->	Check for weak accounts

etc...

dradis

- Lets 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 always be a single point of failure
- Recommendation is to keep management networks separate from your core networks and guest networks
- There is nothing stopping you from hardening the installation beyond the default
  - Don't forget things like CIScan for example
  - Do you use all of the services running?

Am I Going to Get Owned?

- Harden the virtual network
  - Disable promiscuous mode
  - Reject MAC address changes
  - Reject traffic with a forged IP address

- 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?

Future work

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

END

- 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

END

- Questions?