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 192.168.1.53:
Not shown: 1707 closed ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>rpcbind</td>
</tr>
<tr>
<td>113/tcp</td>
<td>open</td>
<td>auth</td>
</tr>
<tr>
<td>389/tcp</td>
<td>open</td>
<td>ldap</td>
</tr>
<tr>
<td>902/tcp</td>
<td>open</td>
<td>iss-realsecure-sensor</td>
</tr>
</tbody>
</table>

vmware-authd
VMware: Server

```
220 VMware Authentication Daemon Version 1.0, MKSDisplayProtocol: VNC
USER defcon16
331 Password required for defcon16.
XPAS mY+g/lrSaoIH4
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 0 0 0 1 01
1 01 04 cmd/1 11 00 0 0 0 0 0 0 0 1 01
1 01 43 ##/1 71 00 0 0 0 0 0 0 1 01
1 01 73 op/1 71 60 0 0 0 0 0 0 1 01
1 02 106 query/1 71 00 0 0 0 0 0 0 1 01
1 02 163 in/1 71 00 0 0 0 0 0 0 1 01
1 02 197 filter/1 71 10 0 0 0 0 0 0 1 01
1 02 19b searchPath/1 71 10 0 0 0 0 0 0 1 01
1 02 19a tuplePath/1 71 00 0 0 0 0 0 0 1 01
1 02 292 #/1 71 10 0 0 0 0 0 0 1 01
1 02 161 out/1 71 00 0 0 0 0 0 0 1 01
```
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

```ruby
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

Interesting ports on 192.168.1.58:
Not shown: 65528 filtered ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>427/tcp</td>
<td>closed</td>
<td>svrloc</td>
</tr>
<tr>
<td>443/tcp</td>
<td>open</td>
<td>https</td>
</tr>
<tr>
<td>902/tcp</td>
<td>open</td>
<td>iss-realsecure</td>
</tr>
<tr>
<td>903/tcp</td>
<td>open</td>
<td>iss-console-mgr</td>
</tr>
<tr>
<td>5988/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
<tr>
<td>5989/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
</tbody>
</table>
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

**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]
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
• 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
• Questions?