**Securing VMware vSphere**

As with most other areas of security within information technology, securing a vSphere environment means securing all the various components of vSphere. Specifically, securing vSphere involves securing the following

components:

* The ESXi hosts
* vCenter Server The VMs, specifically the guest operating systems (guest OSs) runninginside the VMs
* The applications running in the VMs

1. Log on to the ESXi shell via SSH.

2. To display the current firewall rules, run the following command:

esxcli network firewall ruleset list

3. Make a backup of the firewall configuration file:

cp /etc/vmware/firewall/service.xml

/etc/vmware/firewall/service.xml.bak

4. Allow the firewall configuration file to be changed with the following:

chmod 644 /etc/vmware/firewall/service.xml

5. Toggle the sticky bit flag using the following command:

chmod +t /etc/vmware/firewall/service.xml

6. Open the firewall configuration file with a text editor; in this example Vi is

used:

vi /etc/vmware/firewall/service.xml

7. add a service following the same syntax as those

that already exist in the file:

<service id='0101'>

<id>lab.local</id>

<rule id='0000'>

<direction>inbound</direction>

<protocol>udp</protocol>

<porttype>dst</porttype>

<port>1337</port>

</rule>

<rule id='0001'>

<direction>outbound</direction>

<protocol>udp</protocol>

<porttype>src</porttype>

<port>1337</port>

</rule>

<enabled>true</enabled>

<required>false</required>

</service>

8. Change the firewall configuration permissions back to their original value:

chmod 444 /etc/vmware/firewall/service.xml

9. Update the firewall configuration by running the following command:

esxcli network firewall refresh

