Lab 5.1.1 Securing ESXi Hosts

Introduction

A network lab environment can be used to test upgrades/patches, evaluate new features, or as a training environment for hands-on experience.

Objectives

In this lab the student will:

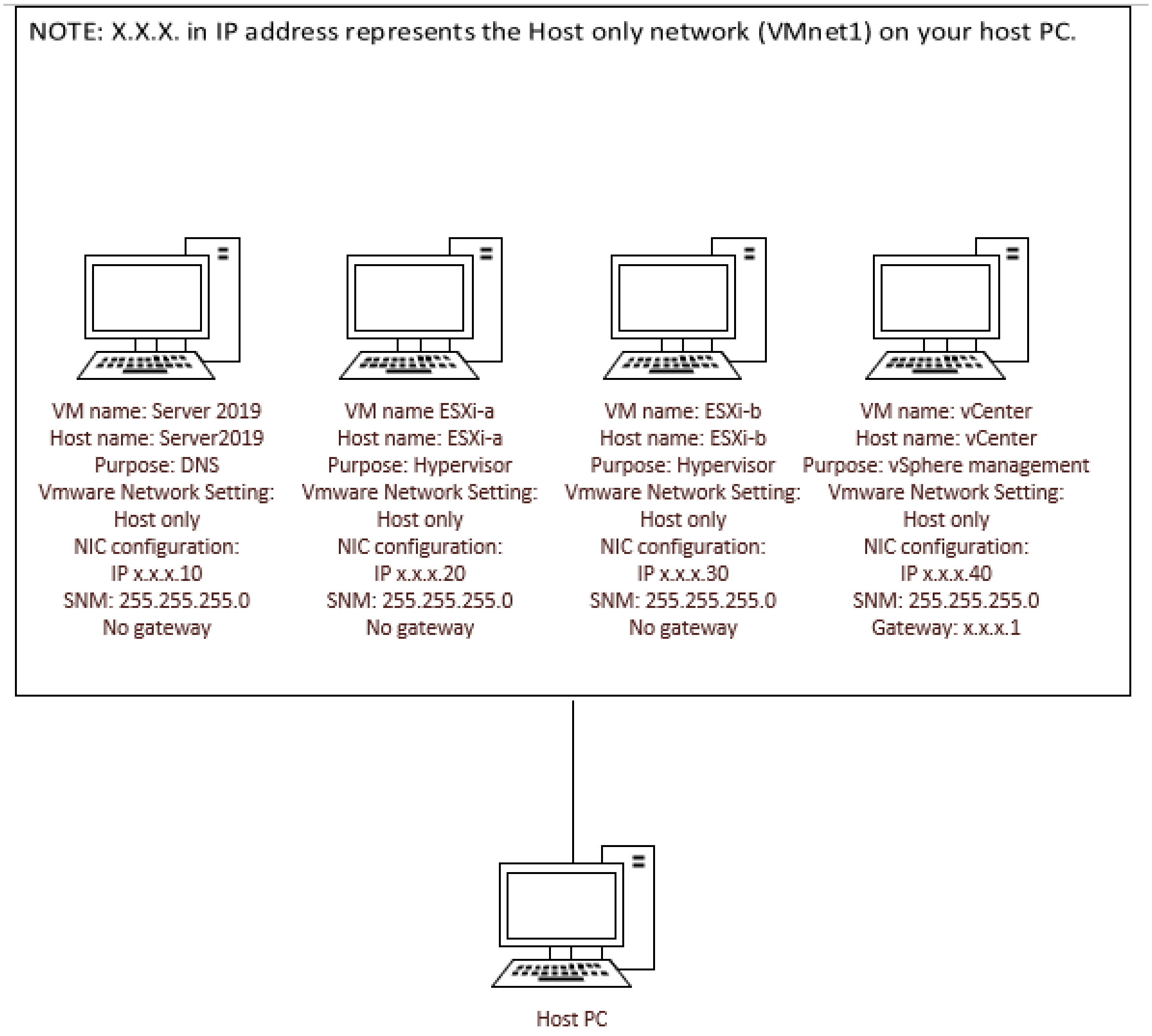
- Install, configure and manage virtual networking and storage [WECM]

Equipment/Supplies Needed

- Host Computer with VMware Workstation Pro
- 2 ESXi 6.7 VM’s
- 1 Windows Server VM for DNS and AD
- 1 vCenter VM for administration
- Reference: VMware ESXi Installation and Setup Guide [17 APR 2018]

Assignment

Student will harden ESXi hosts.
Key activities include the following:
(1) Working with ESXi firewall, making security changes on ESXi, and testing for results.



NOTE: X.X.X. in IP address represents the Host only network (VMnet1) on your host PC.

Procedure

1. You will harden ESXi-A from vCenter by changing various settings. Ensure both ESXi VMs, Windows Server VM, and vCenter VMs are running.
2. Sign into vCenter as the previously created Domain user with vSphere administrative rights.
   A. Select ESXi host A in vCenter and click on Configure in the right pane.
   B. Under System, select Firewall, then click the Edit button.
   C. Select the SSH Server service and edit the service to not Allow connections from any IP. Enter the IP of your Windows Server VM as the only IP allowed to connect to this ESXi host with SSH. Ensure the check is still in the box to the left of the service. Hint: when selecting a service, click in the Incoming or Outgoing Ports columns and the box will remain checked for that service. **SCREENSHOT THIS STEP.**
   D. Do the same for the DNS Client, DHCP Client, and Software iSCSI Client services, however be sure to enter only the IP of FreeNAS when editing the software iSCSI client service. The Windows Server VM IP should be used for the other services. **SCREENSHOT EACH SERVICE IN THIS STEP AFTER MAKING THE REQUIRED CHANGES.**
   E. Disable the Wake on Lan (WOL), and SNMP Server services by removing the check mark from their respective boxes.
   F. Apply all the changes made in steps C – E above. You'll notice that the services disabled no longer show as a running service under the Firewall heading. You'll also notice that some of the

services show the IP you entered in the steps above. **SCREENSHOT THIS STEP TO SHOW THE WOL AND SNMP SERVICES DO NOT SHOW IN THE LIST OF RUNING SERVICES IN ALPHBETICAL ORDER.**

3. Install Putty on your host PC and attempt to SSH to ESXi-A. It should time out because you configured the SSH service to only accept connections from the Windows Server IP.

   A. This is proper error handling. If the error had said something like SSH is disabled on this ESXi host then an attacker would know that the IP is an ESXi host and they would alter their attack accordingly. Even if the error message simply said something like access denied, an attacker would know they are dealing with a live IP address and they would find another way to attack.

4. Install Putty on your Windows Server VM and attempt to open a SSH session to ESXi-A. It should succeed because of your firewall configuration. Note: the username is Root and the password is whatever you used when you installed ESXi.

5. On your host PC open a browser window and enter the IP of ESXi-a. Enter the username, which is root, and enter a wrong password and attempt to login. Notice the error message is an incorrect username or password. This is proper error handling. If the error message said something like a wrong password then an attacker would know the username is correct but the password is not.

6. Submit the following items as evidence of lab completion for grading. Put all screenshots in a Word or PDF document and upload that document for grading.

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Screenshot of SSH Server service	1 correct answer; 16 pt each
	Screenshot of DNS Client service	1 correct answer; 16 pt each
	Screenshot of DHCP Client service	1 correct answer; 16 pt each
	Screenshot of Software iSCSI Client service	1 correct answer; 16 pt each
	Screenshot of WOL service	1 correct answer; 18 pt each
	Screenshot of SNMP Server service	1 correct answer; 18 pt each