# Lab 5.1.4 Network Security Monitoring

**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:

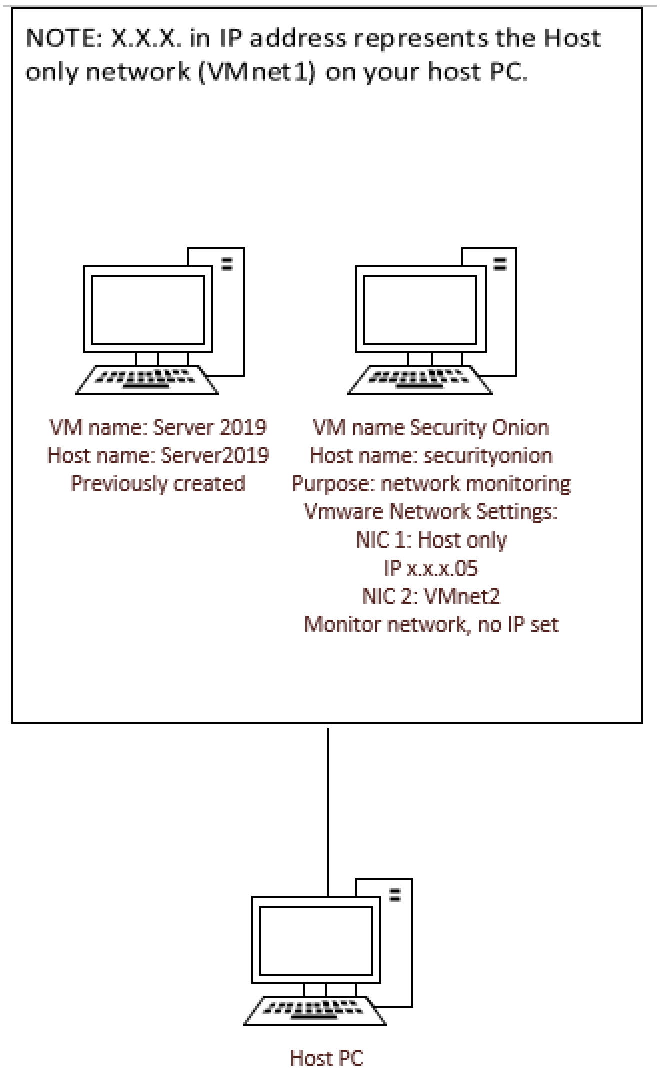
- Install, configure and manage virtual networking and storage [WECM]

**Equipment/Supplies Needed**

- Host Computer with VMware Workstation Pro
- Active Directory Windows Server VM previously installed
- Security Onion ISO

**Assignment**

Students will install and perform a basic configuration of Security Onion.
Key activities include the following:
(1) Install a Security Onion VM on your host PC.



**Procedure**

1. You will install and configure a new Security Onion (SO) VM for network monitoring. Download the SO ISO from the ITNW 2355 lab repository found in the lab.
2. Create a new VM in VMware Workstation with the Operating System as Linux and select Ubuntu 64 bit.
    A. Name the VM **SecurityOnion**.
    B. Select disk size of 100GB and save as a single file.
    C. Set Memory at 16GB.
    D. Set Processors as 2 CPU's and 2 Cores.
    E. Set the NIC to Host-only.
    F. Add another NIC and set it to VMnet2.
    G. Power on the VM and select Basic Graphics Mode as the boot option if you are given the choice.
    H. Answer yes to install SO.
    I. Enter a new username of **admin** with the same password you use on your other VMs. The installation could take some time to complete. It may look like it's stuck on several steps but it really is doing something. Be patient. If your VM screen goes blank press the enter key to see the progress again.
    J. When SO is installed you may be prompted to reboot, or it may reboot automatically. Sign in with the admin user and password you created earlier after the reboot.

K. After beginning the startup configuration select Evaluation Mode. Use the tab key to move from field to field and use the spacebar to select an option.
L. Use airgap install conditions because you do not have a NIC set to NAT.
M. Set the OS patch schedule to Manual.
N. The host name should be the default **securityonion**.
O. The management NIC will be the Host-only NIC, which should be ens33. That's the NIC you'll use to manage SO. Set a static IP of x.x.x.5 in your Host-only network. You should know what x.x.x represents by now. If you need to, use the Virtual Network Editor in VMware Workstation to see what the Ipv4 Host-only network is. You'll also need to know the subnet mask and gateway of the network. The DNS setting should be your Domain Controller IP. The DNS search domain is your AD name.
P. Set the monitor network to the VMnet2 NIC, which should be ens34.
Q. Set your HOME-NET address with the CIDR notation used in your VMnet2 network. Edit the network so it shows the correct network address and CIDR notation for your VMnet2 network.
R. You'll next see a window that mentions services. Click ok to see the next screen where you will leave all the components selected for installation. There are some pretty strange looking names that you may not have heard of, that's ok. Leave them all selected.
S. Enter an email account as instructed. You can use your mymail account if you want or you can use a fake account, it really does not matter because you're Host-only. **You do need to remember the email account and password**.
T. Choose IP as the access method for the Web interface.
U. Answer Yes to running so-allow.
V. Enter the IP of your Windows Server Domain Controller as the IP to manage SO. The dialogue box simply says "Enter a single IP address or an IP range, in CIDR notation" which is pretty cryptic. What it's asking for is the single IP or entire subnet in CIDR format that can access SO from a browser. Start your Domain Controller if it is not running yet.
W. Answer Yes to set this machine up as an EVAL. This is the final stage of installation and will take the longest to complete. Be patient. Reboot the VM when installation is complete.
X. When SO reboots log in to the console with username admin and the password you set. Run the command sudo so-allow to add a new firewall rule.
Y. **Screenshot the SO console.**
Z. Go to your Domain Controller, install Chrome, if not already installed using the offline installer found **here**. In Chrome, enter the IP of SO as a https Web site. Sign in using the email address/password you created in step 2S above.

**Answer the following questions and submit them in a Word document along with the screenshot. Use Google and/or the PDF in the lab to find the answer to the questions below.**

**Looking at the SO console what is Analyst and what is it used for?**
**Looking at the Chrome screen what is CyberChef and what is it used for?**
**Looking at the Chrome screen what is Playbook and what is it used for?**
**Looking at the Chrome screen what is TheHive and what is it used for?**

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

| Concerns<br>Working Towards Proficiency | Criteria<br>Standards for This Competency | Accomplished<br>Evidence of Mastering Competency |
|---|---|---|
| | Screenshot of SO console | 1 correct answer; 20 pt each |
| | Answer to Analyst question | 1 correct answer; 20 pt each |
| | Answer to CyberChef question | 1 correct answer; 20 pt each |
| | Answer to Playbook question | 1 correct answer; 20 pt each |
| | Answer to TheHive question | 1 correct answer; 20 pt each |