Alienvault OSSIM Project

IP Address Reference:

OSSIM: 192.168.0.13
Ubuntu Attacker: 192.168.0.15
Ubuntu Victim: 192.168.0.16
Kali: 192.168.0.17
Subnet: 255.255.255.0

Virtual Machine Hardware Specifications:

	NIC	CPU	HDD	RAM
OSSIM	1 NIC, 'intnet', Promiscuous Mode = Allow All	2	20GB	8192MB
Ubuntu Attacker	1 NIC, 'intnet'	1	10GB	1024MB
Ubuntu Victim	1 NIC, 'intnet'	1	10GB	1024MB

These are the three virtual machines that you will need to perform the project. The *Ubuntu Victim* VM will be used to access the OSSIM web interface. The *Ubuntu Attacker* VM will be used to attempt attacks on both the OSSIM VM and the *Ubuntu Victim* VM. Using a Virtualbox Internal Network ensures constrained communication between the virtual machines but will prevent any communication with the host or with other machines.

Setting Up Your Environment

- Create the three virtual machines and then immediately make an 'Initial Creation' snapshot
- Now, configure the hardware options for each virtual machine and create a 'Hardware Configured' snapshot.
- Start OSSIM and connect the installation ISO when prompted. Ensure that the proper IP address is configured, that the correct timezone is chosen, and that the subnet is correct.
    - If the installation hangs on installing the base system, give it some time. If this persists, check that the VM had 2 (two) CPUs.
    - Do not attempt to perform two VM operating system installations at once. Do not have any other VMs or unnecessary programs running during the OSSIM installation.
- Install the two Ubuntu VMs with all default settings, no special partitioning. Make sure to choose the correct timezone. Restart when prompted, then shut the VMs off and take 'OS Installed' snapshots.
- Boot the Ubuntu VMs and configure static IP addresses, then test connectivity using ping.

Configuring OSSIM

- Once installation has been completed (or if you were provided with a preinstalled OSSIM VM), ensure that the OSSIM VM is turned off, and then take a 'OS Installed' snapshot, if one does not already exist.
- Start the OSSIM VM in Headless mode, preferably when no other VMs are running (disk usage can be high at bootup for OSSIM). Allow a few minutes to pass.
    - https://www.thomas-krenn.com/en/wiki/Headless_Mode_for_Virtual_Machines_of_VirtualBox

- When the preview pane for OSSIM shows a black screen with a terminal, the web UI can be successfully accessed at the IP address assigned to the OSSIM box using the *Ubuntu Victim* VM.
- Access the OSSIM Web UI (Bypass the insecure connection warning if present :) and configure login credentials immediately; make sure to take note of these.
- Login to the OSSIM Web UI and start the Getting Started Wizard.
- On Network Interfaces, click Next, as we only have one.
- On Asset Discovery, ensure that all VMs are showing up. Otherwise, check their configurations.
- Skip the Deploy HIDS step if you do not have Windows guests.
- Skip the Log Management and Join OTX pages.

Deploying HIDS Agents to the Ubuntu VMs

- Go to Environment/Detection/HIDS/Agents/Agent Control and use the Add Agents button to add any nonpresent hosts.
- Connect the USB drive containing the OSSEC HIDS Agent to a host and copy the file over, then disconnect the device.
- Unzip the HIDS agent files using the tar command, then run the install.sh file
- Install as an 'agent'
- Use default installation environment
- Input the correct IP address for the OSSEC HIDS server (OSSIM appliance)
- Run the integrity check daemon, rootkit detection engine, active response, and press Enter to begin installation. Press Enter again when the installation completes to return to Terminal.
- Go to the OSSIM web UI and, in the Agent Control menu, extract the key for the host for which you wish to deploy HIDS. Copy this.
- Virtualbox may not allow you to copy to and from VMs without installing Guest Additions. Another option is to access the web UI from the host where you wish to deploy HIDs.
- Run /var/ossec/bin/manage_agents and choose I to import a key. Paste your key and confirm.
- Restart the ossec service to apply the changes.
- In the OSSIM Web UI, go to Environment/Detection/HIDS/HIDS Control and restart the HIDS Service to pick up the new agent.
- Following this, you should be able to go the Environment/Detection/Agents/Agent Control and see that the specific host is now marked as Active.
- Repeat this until all hosts have HIDS installed.

- Download and installation
  - https://youtu.be/Xfa-zIYhX3c
- Configuration of OSSIM
  - https://youtu.be/y2F3VqOXzus
- Attack event scenarios
  - https://youtu.be/WGNmIR8Lqgo