Lab 1: Setting up and configuring Security Onion

Introduction

As the first exercise for this chapter, we will deploy and configure a Security Onion VM. We will extend the functionality of this Security Onion appliance throughout the remainder of this semester and use its analytics and search capabilities extensively later when threat hunting.

This lab covers the following topics:

1. Deploying the Security Onion VM & Configuring Security Onion
2. Installing VMware tools
3. Updating Suricata rulesets & Adding a web portal user
4. Deploying Wazuh agents

**Submission:** You need to submit a detailed lab report, with screenshots, to describe what you have done and observed. Questions will be defined as you progress through the lab. The lab report will be compiled as a Word document and submitted on Brightspace by **MONTH DAY at TIME AM/PM.**

Objective 1: Deploying the Security Onion VM

We will now deploy a Security Onion VM for our lab environment. Follow along with the next process to get the VM up and running.

1. Head on over to https://securityonionsolutions.com/software/ and download the latest version of the Security Onion appliance (2.3.21 as of the writing of this book), as illustrated in the following screenshot:

Figure 1.1 – Exercise 1: Downloading Security Onion

A screenshot of a computer

Description automatically generated

2. With the Security Onion appliance **International Organization for Standardization (ISO)** file downloaded, open VMware Workstation and select **File – New Virtual Machine**. Choose the **Typical** configuration option and click **Next**. The process is illustrated in the following screenshot:

Figure 1.2 – Exercise 1: Creating a new VM

A screenshot of a computer program

Description automatically generated

3. On the **Install operating system from** the screen, select the **Installer disc** option, hit **Browse**, and find the ISO file for Security Onion you just downloaded. Click **Open**, followed by **Next**. The process is illustrated in the following screenshot:

Figure 1.3 – Exercise 1: Creating a VM – attaching an ISO file

A screenshot of a computer

Description automatically generated

4. The next screen asks you to specify the operating system for the VM you are building. Choose **Linux**, version **CentOS 7 64-bit**. Click **Next** to continue the deployment process. The following screenshot illustrates this process:

Figure 1.4 – Exercise 1: Creating a VM – choosing an operating system

A screenshot of a computer program

Description automatically generated

5. Now, it is time to name our VM. I chose to call it **Security Onion**. Specify a name and click **Next**. The process is illustrated in the following screenshot:

Figure 1.5 – Exercise 1: Creating a VM – naming the VM

A screenshot of a virtual machine

Description automatically generated

6. The next screen asks you to specify the size of the virtual disk the operating system will use. My advice is the more, the better. Security Onion will be able to record and correlate over a longer period of time the more space it has to store data on. As a minimum, choose **500 GB** here. Click **Next** to proceed to the summary screen. The process is illustrated in the following screenshot:

Figure 1.6 – Exercise 1: Creating a VM – disk size

A screenshot of a computer

Description automatically generated

7. As a final configuration step for the VM, click on the **Customize Hardware** button on the **Summary** screen and enter the following details for the VM's resources:

Figure 1.7 – Exercise 1: Creating a VM – hardware settings

A screenshot of a computer

Description automatically generated

These numbers are aligned with the minimum specifications for a typical Security Onion deployment. They are chosen for optimal performance, but less will typically get you going as well. Keep in mind, though, that if you change resources later you will have to reinitiate the setup process, which will wipe all data that was collected by the Security Onion appliance.

As a final note, there are two network adapters configured. One will be used for management and the other for network packet monitoring (sniffing). In the book's lab setup, **LabBox\_Red** is connected to the industrial network segment, while **LabBox\_Orange** is connected to the SPAN port, as described in Chapter 19, Lab Setup. The SPAN port will feed the Security Onion appliance (cloned) network packets from the lab environment. The rule of thumb here is the better we are at feeding sniffing data, the more accurate and wholesome the Security Onion solution will be.

8. We are now ready to install the Security Onion operating system. In VMware Workstation, for the Security Onion VM, click the **Power On this Virtual Machine** button and wait until the VM boots into the following selection screen:

Figure 1.8 – Exercise 1: Installing Security Onion – selection screen

A screen shot of a computer

Description automatically generated

9. Highlight **Install Security Onion 2.3.21** and hit Enter to start the install process.

10. Type in **yes** to confirm you want to wipe the hard drive and install the Security Onion operating system. The following screenshot illustrates this:

Figure 1.9 – Exercise 1: Installing Security Onion – writing the operating system to disk

A screen shot of a computer error

Description automatically generated

11. At this point, the operating system is about to get installed, and the installer asks for an administrative username and password to use for the new install. Specify a username and password and hit Enter.

12. The installer will now format the hard drive and install the Security Onion operating system, as illustrated in the following screenshot:

Figure 1.10 – Exercise 1: Installing Security Onion – operating system installation in progress

A screenshot of a computer

Description automatically generated

At the end of the operating system installation process, the installer asks you to confirm a reboot. Hit to confirm.

13. After the installer reboots, log in to the newly installed operating system with the credentials you set up. The configuration process starts at this point.

14. For **Would you like to continue?** Hit **Yes**, as illustrated in the following screenshot: Figure 1.11 – Exercise 1: Installing Security Onion – starting the Security Onion setup

A computer screen shot of a computer screen

Description automatically generated

15. We are going to configure Security Onion as **EVAL**, as illustrated in the following screenshot. This installation mode allows us to try out (evaluate) all aspects of Security Onion:

Figure 1.12 – Exercise 1: Installing Security Onion – selecting the EVAL install

A screen shot of a computer

Description automatically generated

16. Next, we choose the **STANDARD** install, which allows the Security Onion appliance to retrieve updates over the internet. **AIRGAP** is an interesting option, especially on industrial networks that are completely isolated from the outside world. Both options are shown in the following screenshot:

Figure 1.13 – Exercise 1: Installing Security Onion – selecting STANDARD install conditions

A screen shot of a computer

Description automatically generated

17. Time to give a name to our new Security Onion appliance. I chose **IND-SecurityOnionv2**, as illustrated in the following screenshot:

Figure 1.14 – Exercise 1: Installing Security Onion – naming the appliance

A screenshot of a computer

Description automatically generated

18. At this point, we need to choose which physical interface will be used for the management NIC. Choose the first interface for now, but keep in mind that we might have to rewire things (in the VM settings) if we cannot get connected after the install process. The process is illustrated in the following screenshot:

Figure 1.15 – Exercise 1: Installing Security Onion – choosing the management interface

A screen shot of a computer

Description automatically generated

19. The next couple of screens have us specify IP address details such as **static** versus **DHCP**; the IP address if we choose **static, netmask, gateway**; the domain name; an finally, the DNS server for the network we are on. Configure this according to your setup (I am using a static IP address of **172.25.100.250**). The process is illustrated in the following screenshot:

Figure 1.16 – Exercise 1: Installing Security Onion – management interface DNS search domain

A screen shot of a computer

Description automatically generated

After entering the configuration details for the management interface, the installer will initialize the network.

20. Next, we need to specify the physical adapter that will be used as a monitoring (sniffing) interface. Select the remaining interface and hit **Ok**. The process is illustrated in the following screenshot:

Figure 1.17 – Exercise 1: Installing Security Onion – selecting the monitoring interface

A screenshot of a computer

Description automatically generated

21. On the next install screen, select **Automatic** as the operating system patch schedule to allow Security Onion to update certain parts of the appliance. Hit Enter to continue.

22. Now, we need to specify the **HOME\_NET** IP address range. This should be set to cover the range of the industrial network (**172.25.100.0/24** for the lab network) and allows Security Onion to differentiate between internal and external network addresses, used for several secrecy tools and checks. Set the IP address range and hit Enter to continue.

23. Now, we are asked to select the **Components** we want to install (the security services we want to have running). Leave the default selection (we want to play with all the tools) and hit **Ok** to continue. The process is illustrated in the following screenshot:

Figure 1.18 – Exercise 1: Installing Security Onion – selecting components to install

A screen shot of a computer

Description automatically generated

24. The next step asks us to confirm for Security Onion to use the **default Docker IP range**. Leave the selection as **Yes** and hit *Enter* to continue.

25. Next, we need to specify an email address and password for the administrator of the web interface. Specify the credentials to continue the install process.

26. Leave the access method set as **IP** on the next screen and hit Enter to continue.

Now, choose **Yes** to run, to allow and set up the IP addresses on the network that are allowed to log in to the Security Onion management interfaces and web portal. The process is illustrated in the following screenshot:

Figure 1.19 – Exercise 1: Installing Security Onion – allowing the industrial network range

A screen shot of a computer

Description automatically generated

27. And finally, the installer asks us to confirm whether to continue setting up the Security Onion appliance, as illustrated in the following screenshot:

Figure 1.20 – Exercise 1: Installing Security Onion – confirming install in EVAL mode

A screen shot of a computer

Description automatically generated

The installer will now configure the appliance and set things up according to the selections we made. At the end, we will be presented with a **Process completed** message and asked to confirm a reboot. After the reboot, we are ready to start using the Security Onion appliance. The process is illustrated in the following screenshot:

Figure 1.21 – Exercise 1: Installing Security Onion – install process completed

A screen shot of a computer

Description automatically generated

This concludes the install process of the Security Onion VM. Next, let's look at some configurations aimed at getting the most out of the new VM.

Objective 2.0: Configuring Security Onion

With the Security Onion VM up and running, let's look at three initial configuration procedures I tend to do on all new Security Onion deploys: **installing VMware tools, updating the Suricata ruleset, and adding a web interface user (non-admin)** for day-to-day use.

Objective 2.1: Installing VMware tools

VMware tools are the host-based additions to a VM that allow better integration of the guest VM with the host (VMware Workstation). The VMware tools provide a better user experience and overall improved operability of the VM, so let's install them.

Log in to the Security Onion appliance over SSH (**ssh adm-pac@172.25.100.250**) and enter the following commands:

|  |
| --- |
| sudo yum update  sudo yum install open-vm-tools-desktop fuse |

These commands update the package repository files and then install the required VMware tools' executables, as illustrated here:

Figure 1.22 – Configuring Security Onion: installing VMware tools

A screenshot of a computer

Description automatically generated

The install requires a reboot, so reboot the VM (**sudo reboot**).

Objective 2.2: Updating Suricata rulesets

Suricata rules are what allow the Suricata IDS engine to detect threats. Keeping your rules up to date allows Suricata to find new threats, so perform this process regularly.

Open your terminal and enter the following command to update the Suricata ruleset:

|  |
| --- |
| sudo so-rule-update |

That's all you have to do. Security Onion will now update your ruleset and restart the Suricata engine for you, as illustrated here:

Figure 6.31 – Configuring Security Onion: Suricata ruleset update

A screenshot of a computer program

Description automatically generated

We now have a fresh set of Suricata detection rules. To finalize the Security Onion setup, we will conclude this section by configuring a web portal user to allow us non-admin access to the Security Onion web-based services.

Objective 2.3: Adding a web portal user

SSH into the Security Onion appliance and run the following command to add a web portal user: **sudo so-user-add** [**web-pac@ot-domain.local**](mailto:web-pac@ot-domain.local)

Enter the **sudo** password, followed by the password for the new user, and we are all set. The process is illustrated here:

* [adm-pac@IND-SecurityOnionv2 SecurityOnion]$ sudo so-user-add [web-pac@ot-domain.local](mailto:web-pac@ot-domain.local)
* [sudo] password for adm-pac:
* Enter new password:
* Successfully added new user to SOC
* Successfully added user to TheHive
* Successfully added user to Fleet

We can now use the web portal interface for Security Onion by navigating to **https://172.25.100.250** and logging in with the account we just created (**web-pac@ot-domain.local**), to arrive at the following screen:

Figure 6.32 – Configuring Security Onion: the Security Onion web portal

A screenshot of a computer

Description automatically generated

That covers the installation and initial configuration process of our Security Onion appliance. Next, we will add some functionality by configuring Wazuh.

Objective 3.0: Deploying Wazuh agents

Wazuh is a host-based security monitoring agent with functionality that includes event log forwarding and HIDS capabilities. We also discussed how Wazuh operates with an agent/manager setup. The Wazuh manager comes built into Security Onion, but to allow agents to communicate with the manager service, we must first enable access (define the proper firewall exceptions). To do this, follow the next configuration steps:

1. SSH into the Security Onion appliance and run the **sudo so-allow** command.
2. **so-allow** runs and asks you what you want to do (**Please enter your selection**).
3. Choose the **w** option for **Wazuh** **agent – Port 1514/tcp/udp**.
4. Now, specify the IP address range of the lab network (**172.25.100.0/24**).
5. Confirm the requested change by hitting Enter.

The process is illustrated in the following screenshot:

Figure 6.33 – Configuring Security Onion: allowing Wazuh manager access

A screenshot of a computer program

Description automatically generated

That takes care of allowing Wazuh access to the management service. Next, we need to register our agents with the Wazuh manager. To do this, follow the next procedures:

1. In the SSH Terminal, run the **sudo so-wazuh-agent-manage** command.
2. This starts the Wazuh agent management terminal. Select action **A** for Add an agent.
3. Now, enter the new agent's name—this is typically the hostname of the system the agent will be installed on.
4. Specify the IP address of the agent.
5. Confirm the addition of the new agent by entering y, as illustrated in the following screenshot:

Figure 6.34 – Configuring Security Onion: adding the Wazuh agent

A screenshot of a computer

Description automatically generated

As part of the registration process, the Wazuh manager generates a key that the agent needs to send with the communications to prove who it is.

We need to extract this key before installing the agent on the endpoint.

To do so, proceed as follows:

1. In the Wazuh management terminal, select action E for the Extract key for an agent.
2. Specify which agent ID to extract the key for, as illustrated in the following screenshot:

Figure 6.35 – Configuring Security Onion: extracting the Wazuh agent key

A screen shot of a computer

Description automatically generated

1. Record the key somewhere you can retrieve it.

This process will have to be done for every agent before installing it on a system. Next, we are going to install the agent on the endpoint. Follow along with these instructions to get the Wazuh agent installed on HMI-1:

1. Head on over to https://documentation.wazuh.com/3.13/installation-guide/installing-wazuh-agent/windows/wazuh\_agent\_package\_windows.html and click on the Windows installer download link.
2. Copy the installer file onto the endpoint on which you want to install it (HMI-1, in this lab's case).
3. Install the agent by double-clicking on the installer file and following the instructions, leaving all options at their default settings.
4. At the end of the installation process, make sure to select Run Agent configuration interface before clicking Finish, as illustrated in the following screenshot:

Figure 6.36 – Configuring Security Onion: installing the Wazuh agent

A screenshot of a computer

Description automatically generated

1. In the Wazuh Agent Manager screen that pops up, fill in the IP address of the Security Onion server (172.25.100.250) and paste in the agent key that we just generated in the Wazuh manager, then click Save.
2. If all went well, the popup that results from the save should display the correct hostname and IP address for the endpoint we just installed the agent on, as illustrated in the following screenshot:

Figure 6.37 – Configuring Security Onion: configuring the Wazuh agent

A screenshot of a computer

Description automatically generated

1. Click **OK** on the Confirm screen and go to the **View** – **View Config** page in the **Agent Manager**.
2. This opens up the configuration file. We are going to replace all of the content of the configuration file with the contents of the prepared Wazuh configuration file that I posted here: <https://github.com/SackOfHacks/Industrial-Cybersecurity-2nd-Edition/blob/main/wazuh-config/ossec.conf>.
3. Once you have replaced the content, make sure you update the server address variable if your Security Onion is on a different IP address, as follows:

Figure 6.38 – Configuring Security Onion: configuring the Wazuh agent

A computer screen with text

Description automatically generated

1. The major difference between the stock configuration and the one I uploaded is in the addition of event forwarding of System Monitor (Sysmon) logs and PowerShell script logging events. We will be adding these two log collection methods to our future setup for visualization, correlation, and alerting. The section in question that is different is shown here:

**<localfile>**

**<location>Microsoft-Windows-Sysmon/Operational</location>**

**<log\_format>eventchannel</log\_format>**

**</localfile>**

**<localfile>**

**<location>Microsoft-Windows-PowerShell/Operational</location> <log\_format>eventchannel</log\_format>**

**</localfile>**

**<localfile>**

**<location>PowerShellCore/Operational</location> <log\_format>eventchannel</log\_format>**

**</localfile>**

You could add those lines to the stock configuration instead of updating the entire configuration file, which would be sufficient. It's up to you.

1. Save the config file and select **Manage – Restart** to restart the Wazuh agent with the new configuration.
2. All went well; if you open the log file (View – View Logs) after a few minutes, the log should not show connection errors or reconnection attempts.

*That's it***…**We now have a functioning Wazuh event forwarding and HIDS infrastructure running in our environment.