**Assignment 4:** Configure a Security Onion server and research the available tools and options.

*(This will be marked with a* ***75/20/5*** *split. 75% will be your assignment mark from Individual section, 20% will be your assignment mark for install and hardening, and 5% will be your team rubric.)*

**Required Resources**

* Security Onion Downloaded from NetShare (as per instructions below)
* Ubuntu Apache Server from previous assignment

**Professional Documentation**

All documentation must be done in a **professional style**. It must include:

* Title page
* **Updateable** Table of Contents
* Document introduction
* Section introductions or description, each section must be clearly identified
* Graphics or screenshots MUST include a title with a short description
* Any direct or copied quotes or graphics MUST be properly credited in a footnote
* ALL sources MUST be properly cited (APA format) and placed at the end of your document in a bibliography.
* **NO** embedded, zipped or compressed files. \*\* All scripts must be converted to text before including them in your documentation. \*\*
* **1 Professional Word Document ONLY.**

**Research and documentation sections** -Please complete all research and question responses in your own words. Research sections not completed in your own words may result in a mark of 0 for the section.

**NOTE:** Please do NOT copy and paste responses from internet, **even with a citation**. I expect each section or response to be in your own words. Be prepared to explain your responses and demonstrate your comprehension.

**No marks** will be given for cited or credited information included in document.

***\*\* I recommend completing any research section before completing any required task listed below as you will have a much better understanding of the material and data.***

**Evaluation:** This assignment is markedas per the attached Rubric (marks will be deducted for deviating from Requirements). \*\*You may be asked to demonstrate some of your assignment to show your comprehension of the material.

**Marking and Assignment Notes:**

* ScreenshotsMUST include user or device identifying information.
* Screenshots MUST be added to your document in the order of creation.
* Documentation must meet Professionalism requirements.
* **Automatic mark of 0 - Assignment not submitted or work not original.**

<http://www.nscc.ca/docs/about-nscc/policies-procedures/policy-studentcodeofconduct.pdf>

<https://www.nscc.ca/docs/about-nscc/policies-procedures/policy-academicintegrity.pdf>

**NOTE: This assignment will require some adaption to the current Apache server and research and troubleshooting.**

**Team Portion of Assignment**

**Team Assignment.** As this is a Team Task please make sure to identify which part(section) of the preparation, configuration/ setup steps or documentation you completed for this assignment. You must identify the authors of each section **and** it must be mirrored in your work journal.

*Ex. Technology Equipment and Disposal Policy by Marie Dutka, edited by Bruce Orca.*

**Task 1 – Review the install and configuration of a Security Onion Server**

* Retrieve a “copy” of the Security Onion Server from the ISEC2700 Teams Channel Documents and open it in your VMWare. Make sure to select I copied when starting your server.

\*\* NO CHANGE LOG IS REQUIRED FOR THIS SERVER as it will be used for testing purposes only.

Use the following site and information to help you understand your Security Server and complete the teams portion of this assignment.

<https://docs.securityonion.net/en/2.4/>

* **Security Onion-2.4.20 setup configuration details (for review):** 
  + Standard Security Onion installation
  + Installed in Evaluation mode
  + Included Elastic License
  + Has internet access
  + Hostname = follows naming convention (this is a **S**ecurity **O**nion located in **r**ack **A1** **u32**)
  + Management Interface = NIC 1
    - IP = 192.168.208.50
    - Netmask = as per VMWare settings
    - Gateway = VMWare setting for NAT
    - DNS = default (no change required)
    - DNS Domain= default (no change required)
  + Connects **directly** to the internet
  + Kept all optional services and docker IP range
  + Use the setting identified in your VMWare Description to access the server.

NOTE: For security we will use the **HOSTNAME** for the web interface

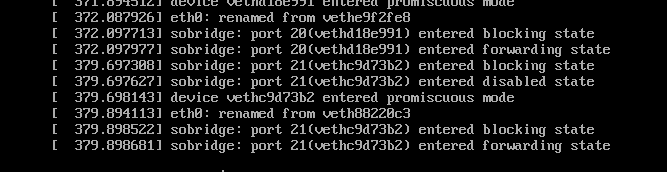
***ATTENTION: You may want a person copy as well as your Pod Team copy as it will make the Individual portion easier. I would recommend you save a copy of your Security Onion VM for personal use.***

Now that we have reviewed our Security Onion setup, load the VM into VMWare and confirm you are able to login. We will spend some time investigating our Security Onion server.

* Open your Security Onion server in your VMWare.

**ATTENTION:** It will take some time for your Security Onion to load as it has created multiple packet sniffing and capturing environments. You may see many pauses but do not log in until your server has completed loading.

**NOTE:** Once it has completed loading it may not show the required log in command, you will have to hit the enter key. Here is an example of what a completed startup may look like before you log in. Notice the number of sobridge ports loaded (yours may vary by a few).



*Image 1 – Security Onion server start up.*

***“And sure enough, even waiting will end…if you can just wait long enough.” William Faulkner***

*\*Notice the portal instructions that show up after login. You may want to remember these.*

* We will check our status to see if our server is having any issues by using the following command:

sudo so-status

* + Some services that have not yet started up (in **yellow**). Wait at least 5 minutes and check the status again.
  + Once the status is all green you are ready to move forward.
  + If any of your status show red please troubleshoot the issue before moving forward.

**Task 2 - Security Onion Dashboard, Tools and Utilities**

Let’s investigate what we can do with Security Onion.

Now that we have a little more understanding of what tools are available in Security Onion let’s grab some sample data and do some testing.

* If required, log in to your SO server
* To start we will need some packet captures to work with, we will gather some by using the following command:

sudo so-test

* + Note: you may see some warnings but this is normal due to the number and type of packets just ensure you have **some** “Successful Packets”.
* We will need to access our SO Web Console from our Apache server. In order to conserve memory please lower your Apache server to 2-4GB of memory as allowed by your device.
* Since we have selected to use our hostname we will need to resolve our OS server IP to our hostname by modifying the etc/hosts file on our Apache Server to add the following for IPv4:

SOServerIP SOServerHostname

* Log into your SO Web Console from your Apache Server. Remember it’s a secure site. \*\* This is a secure server so we **never** want to remember the password.
* Take some time to look at some of the information available in our Web console dashboard.

Now, let’s take a closer look at the **Alerts dashboard** and **Case Creation Tool**.

* First let’s look at our Alerts Dashboard options, notice we have two special options:
  + Acknowledged (colour coded based on severity)
  + Escalated
* Acknowledge your first 3 **Medium Severity** alerts
  + Now modify your options to show Acknowledged Alerts only
  + Confirm you can see your three options you selected earlier.
  + Return to your original view (all alerts visible).
* Escalate to a new case the first 3 **High Severity** Alerts
  + Now modify your options to show Escalated Alerts, notice it automatically selects Acknowledged as an Alert must be acknowledge in order to get escalated.
* **Stop**. Be prepared to demo your Alert Options.
* **Set your option back to default (no special options selected)**.
* Notice that you have the ability to group the Alert information in a variety of queries, currently our alerts are grouped by Name and Module.
* Change the grouping to Group By Sensor, Source IP/Port, Destination IP/Port, Name.
* Notice the additional information displayed.
* We will not require the observer.name as we understand the information all comes through out SO Server, so remove that filter.
* We also don’t need to network.community\_id so remove that filter as well.

Notice each alert has been given a severity label, let’s take some time to review our options for working with severity.

* Select any Alert that is identified as High severity and **Left** Click on the severity label (you may need to scroll over to see the column)
* Select **Include**
* Notice our new listing
* Let’s move back to our original filter and group our list in a way that shows our event.module
* Filter the Alerts and find all alerts the have the rule name ET MALWARE
* Now let’s select a suspicious alert that has a high severity and contains 2+ entries (count) and identifies a Trojan (Downloader) or Virus
  + Once you have selected, left clicking on the Alert rule.name and select Drilldown.
* Drilldown even further by selecting the > icon next to one of the alerts.
  + Scroll down and **review** all the information you have captured with your packet.
  + Hint: Make sure to determine what information is unique to your packet and what is part of your ruleset.
  + Once you have analyzed your packet capture, left click on the rule.name and add it to a Case.
  + Case Name = PodTeamName Case 1
  + Assign the case to one of your Team Members
    - You will need to add each team member to **Administration/Users**
    - Make sure to use firstinitiallastname@isec3700.ca (all lower case)as the email address
    - Role = Analyst
  + Set the case Status to In Progress
  + Set your case priority to 2
  + Use the review information your captured from above to create a short description about the threat packet and add it as a Comment to your Case.
* Repeat the steps above to capture additional packets (NOT ET MALWARE Trojans or Virus)
* Create a Case and complete the steps for each team member
* **NOTE:** You may all participate in the packet investigation, but you must have a user and case assignment for each team member.
* Be prepared to **demo** your Cases for each team member and your packet analysis.
* Return to your Alerts
* Select an Alert with more then one entry
* Left click on the rule.name again and select Drilldown then select Actions then PCAP
* Turn off your HEX view and review your PCAP again.
* Now select ONLY your option to “unwrap” your packet.
* **Analyze** the PCAP you have captured, be sure to each view and column.
* Be prepared to **demo** your PCAP analysis.

Now that we have reviewed how to find details around our alerts and packets let’s take another approach. Let’s assume that we are trying to capture details and data around a suspect attack or virus.

* Go back to your Alerts dashboard
* Select one of your alerts that has:
  + event.severity\_label = High
  + Select the one on your list with the high count (5+)
  + Drilldown
* Once you have drilled down into your alert, left click on the source IP and select Actions/Hunt
* Review the information shown in our Hunt dashboard.
* Change your query to review your selection options.
  + Identify the IP of your Web Server
  + Use at least 2 Queries to capture your Web Server IP in an event or metric.
* **Stop**. Be prepared to demo your HUNT and queries.

It is important to keep an up-to-date record of all changes and modifications made to your servers and have a reliable copy available as backup.

* Take a final snapshot of your Security Onion server in the **OFF** state.
* Make sure to create a Gold copy of your SO server.
* **\*\* NO CHANGE LOG REQUIRED FOR THIS SERVER.**

**Individual Portion of the Assignment.**

**Task 3 - Security Onion Tools**

\*\* You will find this section easier to complete if you download a personal copy of Security Onion from MS Teams.

Now that we have had some time to look around Security Onion let’s learn a little more about the tools available.

Each Team member will review each of the Tools listed in your Security Onion dashboard and use Security Onion and the Security Onion site along with any other resource required to help develop a better understanding of the tools and their abilities.

* **Stop**. Each Team Member must select one of the following tools listed and:
  + Write a **detailed** description of the tool, how it works and what would you use it for.
  + Be prepared to **demo** that tool including:
    - Explain how it works
    - What you would use it for
    - Live Tool Demo
      * Live Demo **MUST** demonstrate usage and example must show usefulness of Tool.
  + **No two team member may select the same tools.**
  + Tool Options are:
    - Kibana
    - Elastic Fleet
    - OSQuery Manager
    - InfluxDB
    - CyberChef
    - Playbook
    - Navigator

It is important to keep an up-to-date record of all changes and modifications made to your servers and have a reliable copy available as backup.

* Take a final snapshot of your Security Onion server in the **OFF** state.
* Make sure to create a Gold copy of your SO server.
* Upload your individual professional documentation to BrightSpace to the **individual** drop box.
* **\*\* NO CHANGE LOG REQUIRED FOR THIS SERVER.**

**Marking Rubric**

|  |  |
| --- | --- |
| **Value** | **Task** |
|  | **Team Section (Task 1-2)** |
| 4 | Alert Demo, including assigned alert, acknowledge and escalate |
| 10 | Demo a case study for each team member, must include:   * Case Name * Case assignment (including team member role and email) * Case Status * Case Priority * Case Description |
| 5 | PCAP Demo, select alert and select PCAP   * Show the List option in PCAP * Analyze at least one PCAP capture. |
| 4 | Hunt Demo that uses at least 2 queries capture the event or metric that includes:  a High severity alert with 5+ counts and identifies your web server. |
| 2 | Snapshot of Server of Security Onion Server |
| **25** | **Total Marks for Team Section** |
|  | **Individual Section (Task 3)** |
| 20 | Demo Security Onion tool including:   * + - Explain how it works     - What you would use it for     - Live Tool Demo       * Live Demo **MUST** demonstrate usage and example must show usefulness of Tool. |
| 2 | Final Snapshot of Security Onion |
| 6 | Write a detailed description of the tool, how it works and what would you use it for. |
| 2 | Professional Documentation |
| **30** | **Total Marks for documentation** |
|  |  |
| **55** | **Total Marks** |