**]Lab Introduction:**

Security Onion is a free and open Linux distribution for threat hunting, enterprise security monitoring, and log management. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!

Security Onion includes a native web interface with built-in tools analysts use to respond to alerts, hunt for evil, catalog evidence into cases, monitor grid performance, and much more. Additionally, third-party tools, such as Elasticsearch, Logstash, Kibana, Suricata, Zeek (formerly known as Bro), Wazuh, Stenographer, CyberChef, NetworkMiner, and many more are included.

**Lab Requirements:**

This lab is divided into four parts:

1. Prepare Ubuntu Virtual Machine
2. Security Onion iso verification
3. Preparing VM for Security Onion Installation
4. Alert Triage and Case Creation

You are required to have screenshots of every step that’s followed in this lab. Please see submission requirements below in this document for the lab.

# A. Prepare Ubuntu Virtual Machine [10 Marks]

1. Download Ubuntu from : <https://ubuntu.com/download/desktop>and understand the requirements of the machine.
2. Make sure you give the name of VM as **firstname\_Ubuntu** and user name as firstname.
3. Paste **the screenshot** of final configuration of Ubuntu Machine**. [5 Marks]**

A screenshot of a computer

Description automatically generated

1. What is the ip- address of the machine? Paste **the screenshot** showing the command executed to get the ip-address of the machine. **[1+4 Marks]**

The ip address- 192.168.44.141

A screenshot of a computer

Description automatically generated

# B. Security Onion iso Verification [18 Marks]

1. Use the following website to follow the steps listed to download and verify the Security Onion

ISO image. - [https://github.com/Security-Onion-](https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md)

[Solutions/securityonion/blob/master/VERIFY\_ISO.md](https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md)

1. **Paste the screenshot** showing download and import the signing key. **[2 Marks]**

A screenshot of a computer

Description automatically generated

1. **Paste the screenshot** showing download the signature file for the ISO**.** **[2 Marks]**

A screenshot of a computer

Description automatically generated

## Paste the screenshot showing download the ISO image. [2 Marks]

A screenshot of a computer

Description automatically generated

1. **Paste the screenshot** showing verify the downloaded ISO image using the signature file. **[2 Marks]**

A computer screen shot of a computer program

Description automatically generated

1. Answer the following questions:
   1. What do you mean by wget command? . **[1 Mark]**

In Ubuntu, "wget" is a command-line tool used to download files from the web.

* 1. What is the value of signing key? **[1 Mark]**

The value of signing key: 7C1060B7FE507013

* 1. What do you mean by “200 OK” mean? **[1 Mark]**

The term "200 OK" in the context of Ubuntu refers to a status code often seen while communicating with web servers. It denotes a successful HTTP response, meaning the server has handled the request correctly and is providing the desired data or content.

* 1. What is the length of octet-stream received? **[1 Mark]**

543

* 1. What is the length of iso that’s downloaded? **[1 Mark]**

8.23G

* 1. What is the primary key fingerprint? **[2 Mark]**

C804 A93D 36BE 0C73 3EA1 9644 7C10 60B7 FE50 7013

* 1. What do you mean by Good signature? **[3 Mark]**

A "good signature" in Ubuntu refers to a verification procedure that verifies the legitimacy and integrity of a digital signature connected to a software package, making sure it hasn't been tampered with and is from a reliable source.

# C. Preparing VM for Security Onion Installation[32 Marks]

1. Prepare Security Onion machine : [https://securityonionsolutions.com/software.](https://securityonionsolutions.com/software) This page also contains a great number of helpful resources for installing and configuring various aspects of Security Onion. Understand the requirements of the machine from <https://docs.securityonion.net/en/2.3/installation.html>.
2. Create a new virtual machine for Security Onion. You are required to prefix your VM name with your firstname e.g **firstname\_SecurityOnion**. **Paste the screenshot**. **[2**

## Marks]

A screenshot of a computer

Description automatically generated

1. **Paste the screenshot** in Security Onion setup where you enter the hostname.**[2 Marks]**

A computer screen shot of a blue screen

Description automatically generated

1. What is the gateway IPV4 address? **Paste the screenshot**.**[2 Marks]**

A screen shot of a computer

Description automatically generated

1. What are the optional services that are enabled for this installation?**[2 Marks]**

A screenshot of a computer

Description automatically generated

1. Provide a two line write up of each of the services installed. **[5 marks]**
2. **Paste the screenshot** of the email address which is used to create an administrator account for the web interface. **[1 Mark]**

A screenshot of a computer

Description automatically generated

1. **Paste the screenshot** for the final configuration of Security Onion.**[2 Marks]**

A screenshot of a computer

Description automatically generated

1. **Paste the screenshot** after the machine is rebooted after finishing installation where you enter eval login details and see the access information of security onion web interface.**[2 Marks]**

A screenshot of a computer

Description automatically generated

1. Answer the following questions:
   1. How many Network Interface you require?

Ans: 2 network interfaces.

* 1. What is the role of each of the network interface cards?

Ans: The two network interface cards allow LAN management access & mirrored traffic to reach the security onion.

* 1. Which NIC should have static IP address and why? **Share the screenshot** showing the ipaddress of that NIC.

**Ans:**

**A screenshot of a computer

Description automatically generated**

* 1. What’s the role of **so-allow** command in security onion?**[1 mark]**
  2. What’s is the role of so-status command? **Paste the screenshot** showing all the services up and running**.**

**Ans:**

A screenshot of a computer program

Description automatically generated

* 1. What is the command used for replaying network traffic in Security Onion?

**Ans:**

* 1. What’s the number of successful packets you received?

Ans

A computer screen with text on it

Description automatically generated

# D. Alert Triage and Case Creation[40 Marks]

1. Paste the screenshot showing the access to webinterface (Login to Security Onion)

A screenshot of a computer

Description automatically generated

1. How many alerts are captured by Alerts Interface?

**Ans:**

A screenshot of a computer

Description automatically generated

1. If your student-id is even, you need to take up an alert of medium severity label else take high severity label alert.
2. Provide your **student-id here** and **highlight the alert** which has been chosen for discussion in your **screenshot**. **[1+3Marks]**

**Ans: My student ID- 100899259**

A screenshot of a computer

Description automatically generated

1. What’s the count of the alert? What does it mean?

**Ans: 9**

1. Provide the following information about the alert: **[6 Marks]**
   1. Timestamp field: 2023-08-01T03:44:25.049Z
   2. rule.name: ET MALWARE Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)
   3. event.severity\_label: high. iv. source.ip: 192.168.3.65

v. source.port:1036

vi. destination.ip: 188.72.243.72

vii. destination.port: 80

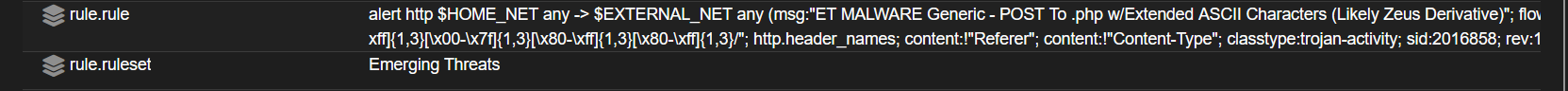
* 1. event.module: suricata
  2. ix. network.protocol: TCP

x. rule.category: A Network Trojan was detected

xi. rile.reference: https://doc.emergingthreats.net/2016858

xii. rule.uuid: 2016858

1. Provide the screen shot of rule.rule and discuss the rule in your own words.

Ans: 

1. **Provide the screenshot** for locating the stream and render a high level overview of the packets[3- Way TCP Handshake]- **[2 Marks]**

A screenshot of a computer

Description automatically generated

1. **Paste the screenshot** of ASCII transcript of the attacke [ Data containing GET,POSTetc.]- **[2 Marks]**

A screenshot of a computer

Description automatically generated

1. **Escalate this alert** as a new case. Provide a **video recording** explaining all the tabs of the case. Add all metadata for the case in terms but not limited to comments, attachments, events, observables and history. You should have atleast 3 IOCs in your observables. All these things should be provided in your video recording. Also show how the alert is now presented in escalated toggle event for Alerts Interface. **[11 Marks]**

**Things to Explore:**

You are welcome to explore beyond the mandatory requirements if you wish.

**General Submission Requirements**

* Include an opening comment with your full name and a short description of the lab.
* Please name your file as fistname\_Lab1.pdf.
* The assignment asks you to provide response on the questions being asked. At times you must also provide screenshot for the work you have done. Please make sure you use the exact numbering scheme as used in the assignment while responding to questions. The assignment needs to be submitted in pdf with much clarity on the screenshot.
* There is no way student is allowed to change the order of the assignment and the numbering. If a student doesn’t know the answer, please write N/A in the response of that question.
* Please make sure all your screenshots should have your name as name of virtual machine and time stamp of your. This is primarily needed to make sure that each student should perform the lab on their own.
* Academic Integrity violations would be treated severely.