

# Information and Networking Security

## Term: Spring 2025

### Laboratory Exercise 5-2 – Hands-on with Intrusion Detection

#### 1. Overview

This individual laboratory exercise will provide some hands-on experience with firewall configuration and intrusion detection.

#### 2. Resources required

This exercise requires the Ubuntu with Snort and Other Tools exercise in the Virginia Cyber Range.

#### 3. Initial Setup

Log in to your Cyber Range account and select the Exercise Environment “Ubuntu with Snort and Other Tools”.

Click “start” to start your environment. When the systems are ready, click the “join” button and select the Primary Machine (desktop.example.com) from the dropdown menu to get to your Linux desktop login. If you are asked to log in, credentials for this Ubuntu Linux VM are below.

Username: **student**

Password: **student**

Note that you will need to use the Linux **sudo** utility to execute many of the commands in the following sections. The student account has **sudo** access using the password above. For more information on the Linux **sudo** command, type “**man sudo**” in a terminal window on your Linux VM.

---

This exercise makes use of resources provided in the Cyber Range. It is a single Ubuntu virtual machine with artifacts necessary for this lab.

#### Task : Intrusion Detection

Instead of observing live network traffic from a network interface, we will use snort to process a packet capture file (.pcap files) from previously captured network traffic.

Before we run Snort against captured packets, we’ll take a look at some snort rules (signatures) in the /etc/snort/rules directory. To do this, open a terminal window and switch to the appropriate directory.

```
$ cd /etc/snort/rules
$ ls ← this will list the rule files
```

Examine the file **shellcode.rules** using the text editor of your choice (your Linux VM includes *vi* and *nano*, as well as a GUI text editor called *mousepad*).



# Information and Networking Security

## Term: Spring 2025

```
$ mousepad shellcode.rules &
```

Each rule has a unique Snort ID number (sid), which is included in the signature. In *shellcode.rules*, find **sid:648** amongst the rules in that file and answer the following questions.

1. What is the specific byte signature ("content:") that sid:648 tries to match?

ANS: content:"|90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90|"

2. What *action* is Snort supposed to take if the signature contained in sid:648 is matched?

```
alert tcp $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any
```

3. Why might sid:648 often result in false positive alerts during large binary file transfers, such as image files?

SID:648 often results in false positive alerts during large binary file transfers such as image files/BINARY OR NON-TEXT DATA

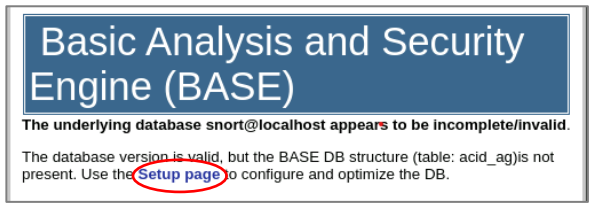
Change directories to **/home/student/lab2** and run **snort** against the packet capture file called **theft.pcap** in that directory as shown here.

```
$ sudo /usr/local/bin/snort -c /etc/snort/snort.conf -r /home/student/lab2/theft.pcap
```

[When using **sudo** you may be asked to enter your student password: **student**]

When Snort finishes processing, open a web browser on your Cyber Range virtual machine (Click on the Applications menu, then Web Browser) and browse to **http://localhost/base**. BASE is the Basic Analysis and Security Engine. BASE provides a web-based user interface for snort results and it is installed on your Ubuntu virtual machine along with Snort.

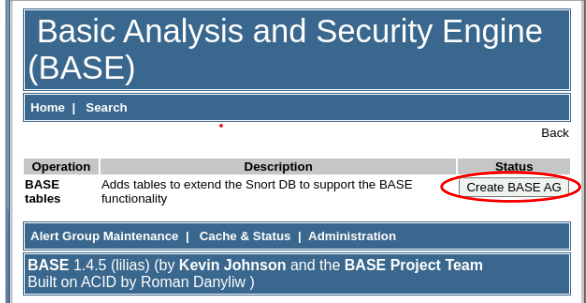
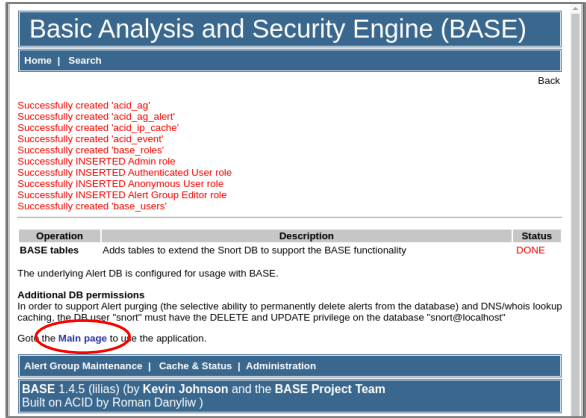
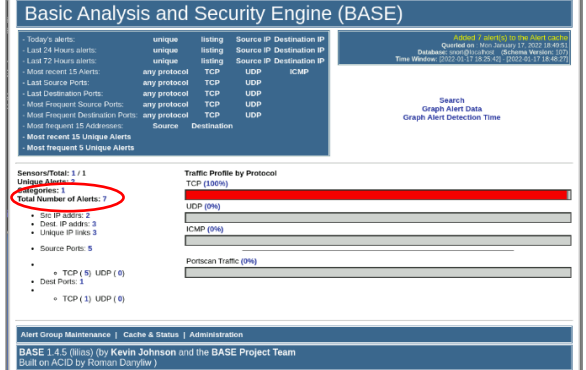
The first time you use BASE, you will have to click through the steps to properly configure the Snort database for use with BASE.

<b>Step 1.</b> Click on the link shown at right to get to the BASE DB setup page.	
<b>Step 2.</b> Click on the button shown at right to extend the Snort database to support BASE functionality.	



# Information and Networking Security

## Term: Spring 2025

	
<p><b>Step 3.</b> Click on the link shown at right to navigate to the BASE main page.</p>	
<p>The BASE main page shown at right will display the status of the backend analysis of the 'theft.pcap' packet capture. The homepage should show the results of the scan with a total of 27,000+ Total Number of Alerts (the example at right is only showing 7 Alerts so far). It will take several minutes for the back-end alert processing to complete, so you might have to refresh the page a few times.</p>	

Review the alerts (you might have to do some filtering and review the 'unique' alerts) and answer the following questions.

- In an attack classified by Snort as "attempted recon", an attacker was trying to steal a specific, and very sensitive, file from the target system. What file was she after?  
/etc/passwd
- What is the technique that the attacker was trying to use to steal the file (hint: there are packets that trigger multiple different alerts)?



## Information and Networking Security

Term: Spring 2025

The attacker used a Directory Traversal technique with an HTTP GET request to try to access the `/etc/passwd` file, triggering multiple Snort alerts for reconnaissance and unauthorized file access.

6. **There are several UDP alerts on traffic with source IP address 0.0.0.0 and source port 68. What is the destination IP address for the packets that triggered those alerts?**

255.255.255.255 port 67

7. **Why might you conclude that the alert from the previous question is a false positive (hint: look at the source and destination port numbers; you might also have to do some online research)?**

The traffic described (source IP: 0.0.0.0, source port: 68, destination IP: 255.255.255.255, destination port: 67) is typical of DHCP (Dynamic Host Configuration Protocol) communication.

