**Intrusion, Detection, and Response**

## Cloud Environment

Graphical user interface, application

Description automatically generated

Diagram

Description automatically generated

## Installation Process

Access root

sudo su –

## Allow traffic rules in your system

ufw allow 22

ufw allow 443

ufw allow 7736

## Initiate Setup

sosetup

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

After Reboot:

sudo su –

nano /etc/hosts

Text

Description automatically generated

sosetup

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Now go to [www.ifconfig.me](http://www.ifconfig.me)

In your terminal provide access to your ip address

so-allow

Select option [a]

Type your ip address.

How would you add UIW’s address space?

<https://host.io/uiw.edu>

<https://whois.ipip.net/AS33683>

<https://ipinfo.io/AS33683/198.49.125.0/24>

Allow UIW’s address space:

208.91.16.0/22

198.49.125.0/24

Text

Description automatically generated

Text

Description automatically generated

You can later check the same information with:

*ufw status*

Before starting activity in your browser allow port 80 in UFW:

*ufw allow from 75.1.50.210 proto tcp to any port 80*

Allow UIW’s address space:

208.91.16.0/22

198.49.125.0/24

*Text

Description automatically generated with low confidence*

*Graphical user interface, text, application, email

Description automatically generated*

Graphical user interface, text, application, email

Description automatically generated

Text

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

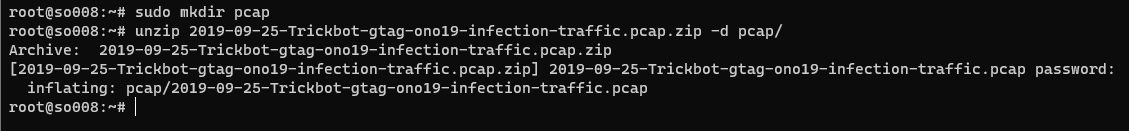
You will need to install zip and unzip to decompress this file.

Text

Description automatically generated

Make a directory named pcap and unzip the file in the newsly generated directory.

The industry standard password is : infected



Validate that your pcap is in this file:

Text

Description automatically generated

Now it is time to load the new PCAP into security onion.

What commands do you have available?

Type *so*, hit the tab key twice, and select *y*

A picture containing text

Description automatically generated

Import the pcap into security onion. You have two options:

1. so-replay-pcap
2. so-import-pcap

There is a big difference between the two. The so-replay-pcap command will have the timestamps of the original files, and the so-import-pcap command will have the timestamp of the day/time you imported the file.

so-import-pcap pcap/2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap

Time to analyze our data!