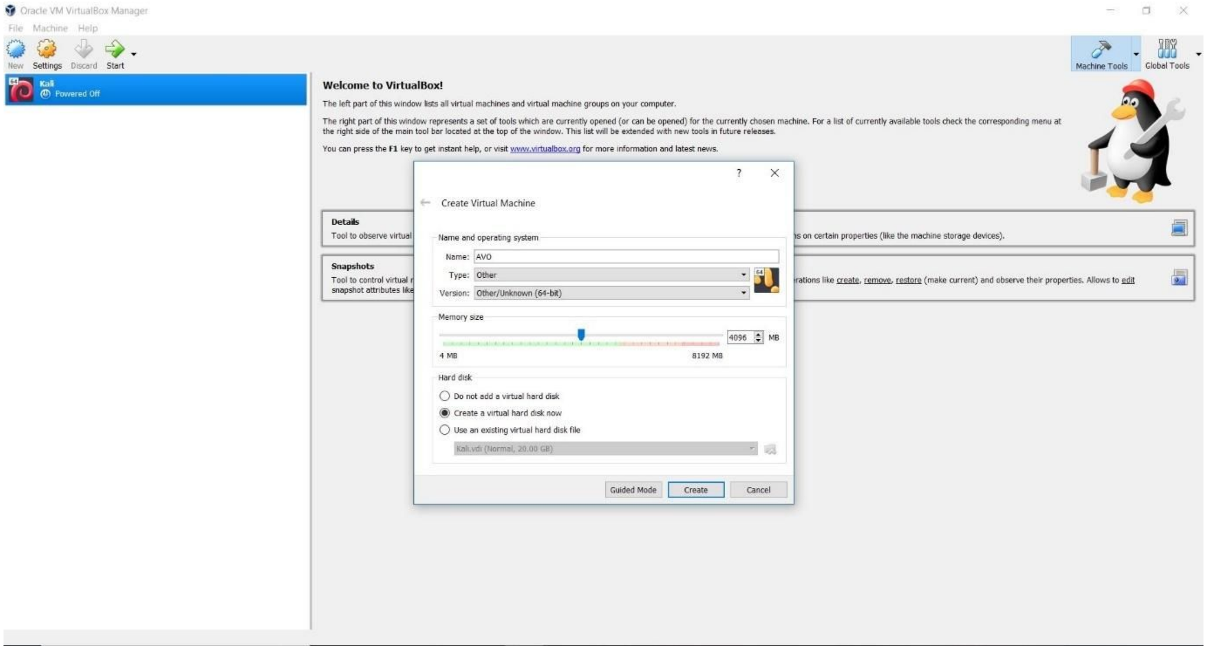
Gujarat Forensic Sciences University

Institute of Forensic Science

By: Nitin Mathew

Installation of Alien Vault Ossim

- **Step 1:** Open a VirtualBox and click on New Button given in top left corner. Give OS Name, Type and Version, Memory and Add Virtual Hard Disk to new Machine.



Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. For a list of currently available tools check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be extended with new tools in future releases.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

Tool to observe virtual ... s on certain properties (like the machine storage devices).

Tool to control virtual ... rations like create, remove, restore (make current) and observe their properties. Allows to edit snapshot attributes like

Create Virtual Machine

Name and operating system

Name: AVO

Type: Other

Version: Other/Unknown (64-bit)

Memory size: 4096 MB (4 MB – 8192 MB)

Hard disk

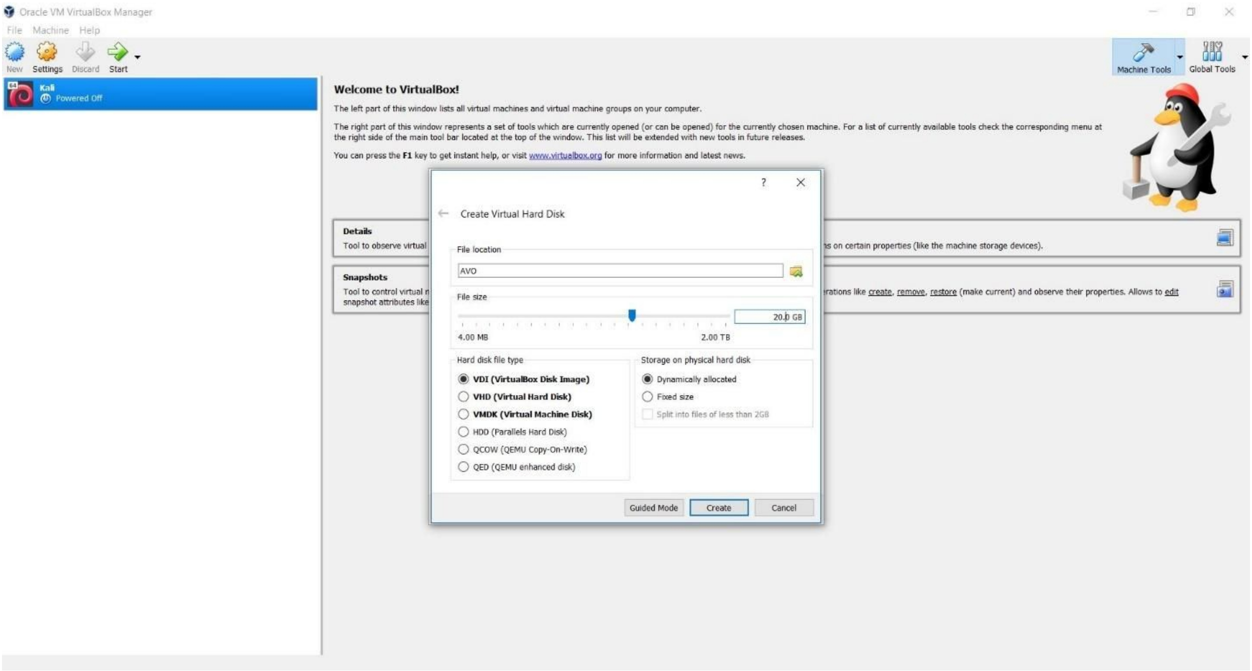
○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

Kali.vdi (Normal, 20.00 GB)

- **Step 2:** Select File Type and also choose the manner in which hard disk should grow that can be dynamic or static and also allocate the disk size.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Machine Tools Global Tools
Kali
Powered Off

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. For a list of currently available tools check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be extended with new tools in future releases.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

Details

Tool to observe virtual … ns on certain properties (like the machine storage devices).

Snapshots

Tool to control virtual m … rations like create, remove, restore (make current) and observe their properties. Allows to edit snapshot attributes like …

Create Virtual Hard Disk

File location: AVO

File size: 20.0 GB (4.00 MB – 2.00 TB)

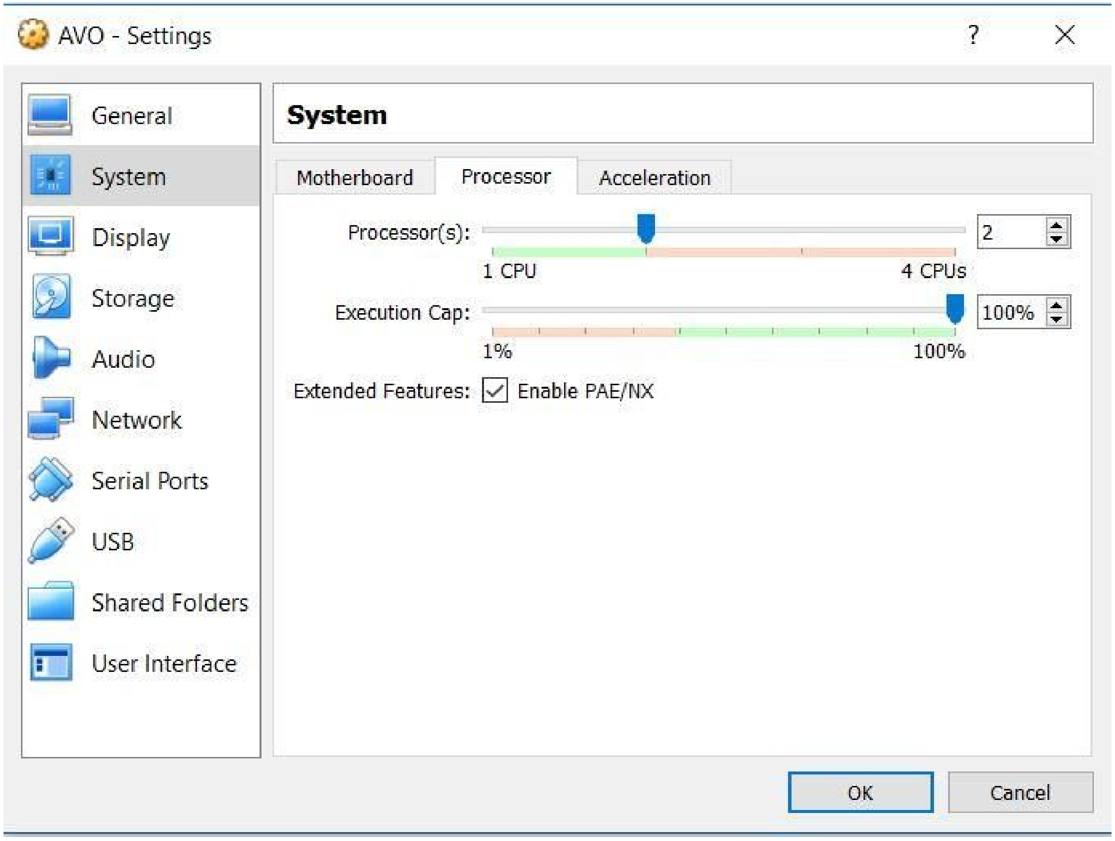
Hard disk file type

- ● **VDI (VirtualBox Disk Image)**
- ○ **VHD (Virtual Hard Disk)**
- ○ **VMDK (Virtual Machine Disk)**
- ○ HDD (Parallels Hard Disk)
- ○ QCOW (QEMU Copy-On-Write)
- ○ QED (QEMU enhanced disk)

Storage on physical hard disk

- ● Dynamically allocated
- ○ Fixed size
- □ Split into files of less than 2GB

- **Step 3:** Now the Virtual Machine is created, and it is shown in the left bar of Virtual Box. Right Click on the Alien Vault and select Settings, then this popup box will load in that go to systems Tab and in that processor and make sure atleast 2 CPUs are allocated.



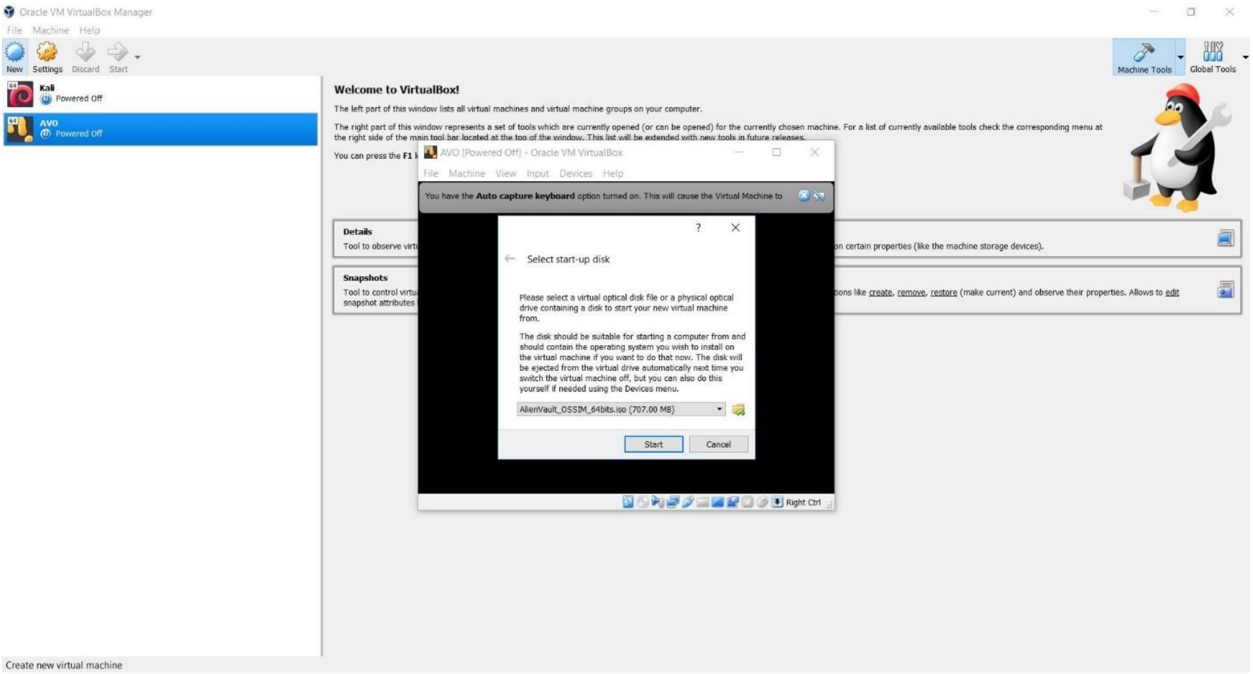
System

Processor(s): 2

Execution Cap: 100%

Extended Features: ☑ Enable PAE/NX

- **Step 4:**Now Click on the created virtual machine and click on start then choose the folder where iso copy of machine is located this only happens on first time execution.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Machine Tools Global Tools
Kali
Powered Off
AVO
Powered Off
AVO [Powered Off] - Oracle VM VirtualBox
File Machine View Input Devices Help
Details
Snapshots
Start
Cancel
Right Ctrl
Create new virtual machine

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. For a list of currently available tools check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be extended with new tools in future releases.

You can press the **F1** k

Tool to observe virt … on certain properties (like the machine storage devices).

Tool to control virtu … tions like create, remove, restore (make current) and observe their properties. Allows to edit snapshot attributes

You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to

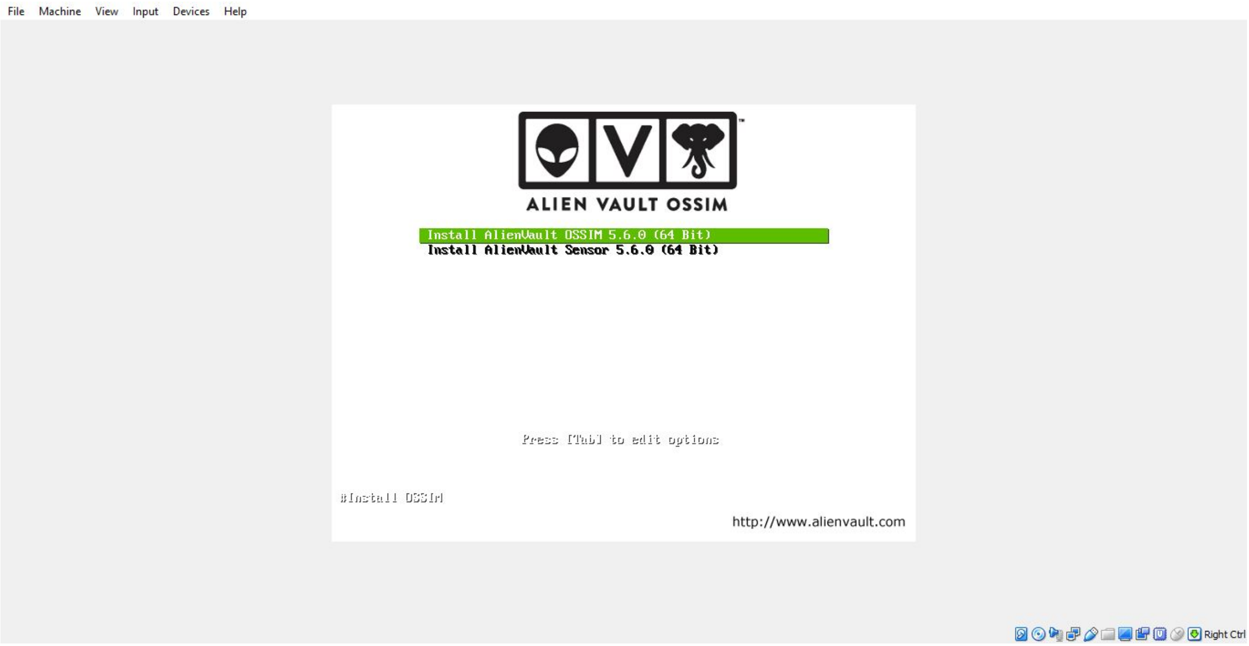
Select start-up disk

Please select a virtual optical disk file or a physical optical drive containing a disk to start your new virtual machine from.

The disk should be suitable for starting a computer from and should contain the operating system you wish to install on the virtual machine if you want to do that now. The disk will be ejected from the virtual drive automatically next time you switch the virtual machine off, but you can also do this yourself if needed using the Devices menu.

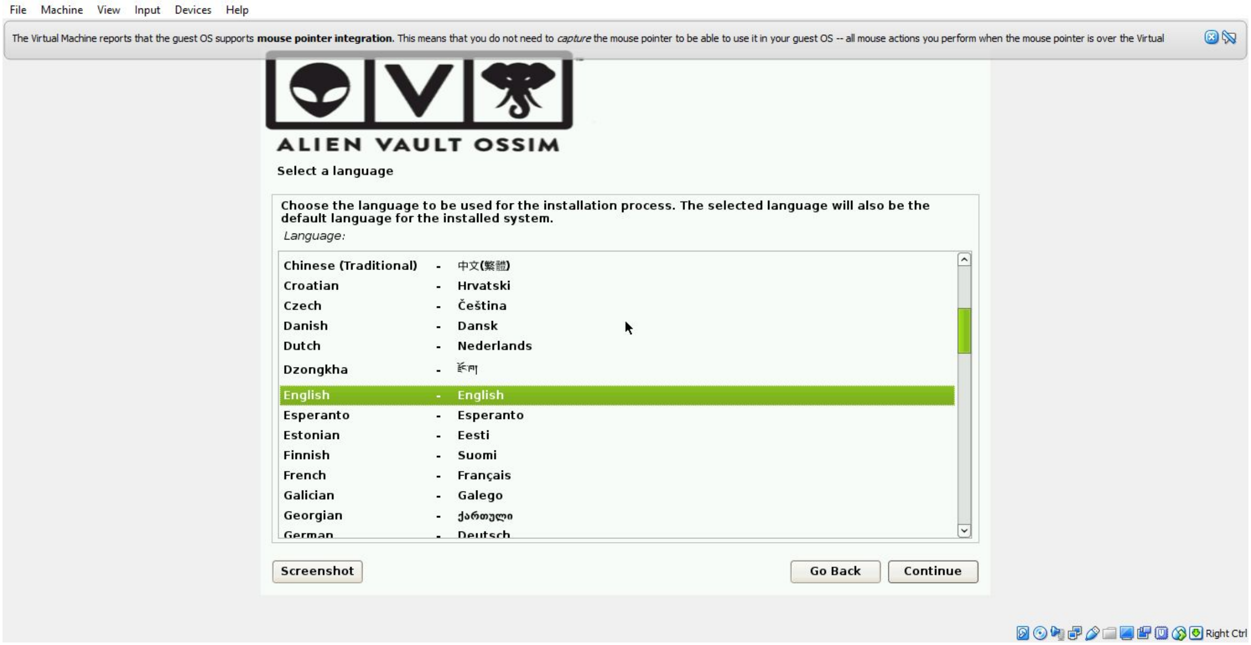
AlienVault_OSSIM_64bits.iso (707.00 MB)

- **Step 5:** After completing all settings, start the Alien Vault, and click Install Alien Vault Ossim


File Machine View Input Devices Help
ALIEN VAULT OSSIM
http://www.alienvault.com
Right Ctrl

```
Install AlienVault OSSIM 5.6.0 (64 Bit)
Install AlienVault Sensor 5.6.0 (64 Bit)

Press [Tab] to edit options

#Install OSSIm
```

- **Step 6:** Select a Language, and click Continue



The Virtual Machine reports that the guest OS supports **mouse pointer integration.** This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual

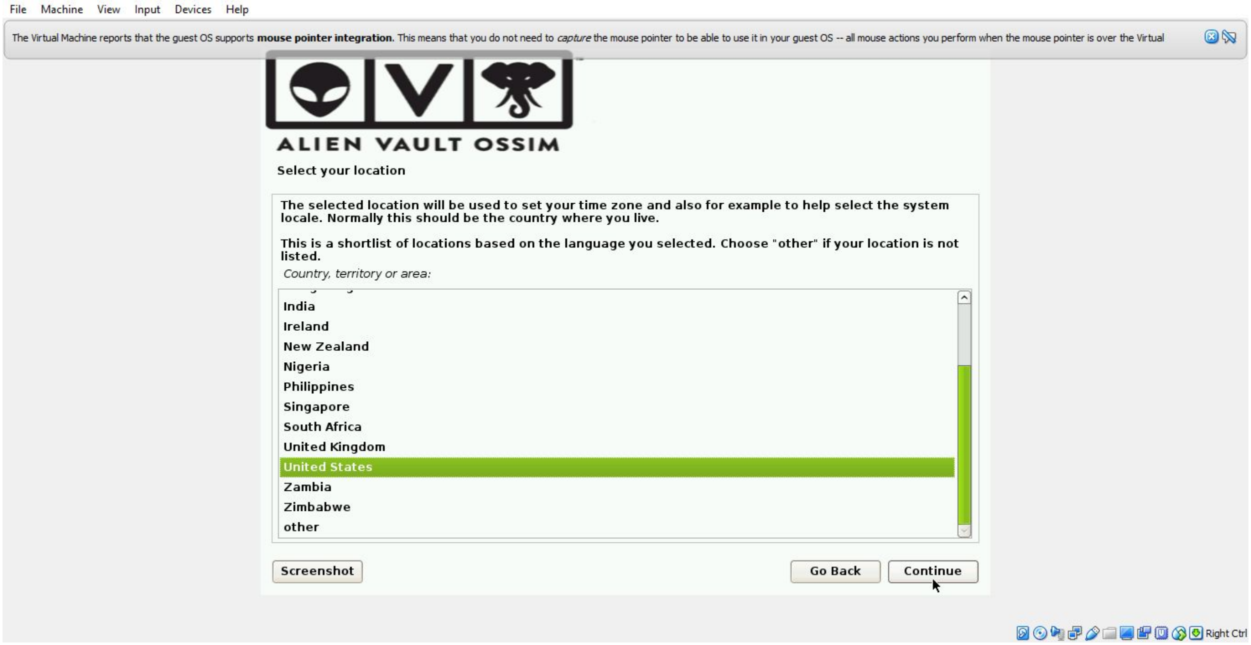
Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	རྫོང་ཁ
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch

- **Step 7:** Select Location, and Click Continue



The Virtual Machine reports that the guest OS supports **mouse pointer integration.** This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual

Select your location

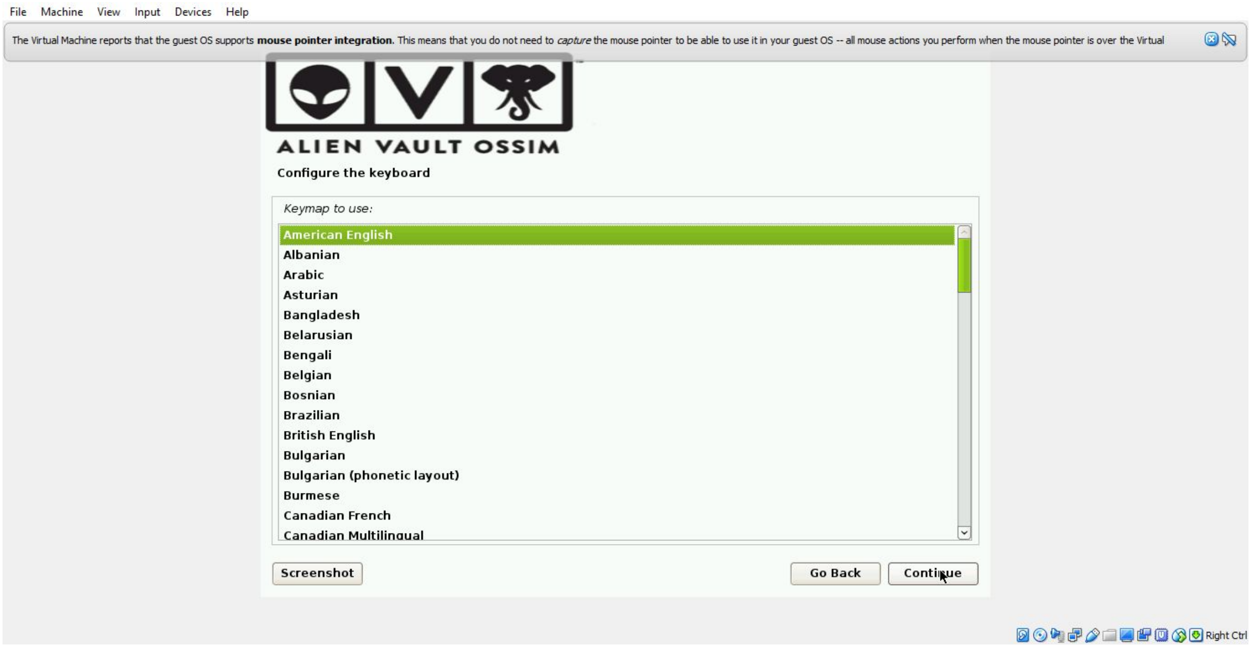
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.

Country, territory or area:

India
Ireland
New Zealand
Nigeria
Philippines
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other

- **Step 8:** Configure the Keyboard, and Click Continue



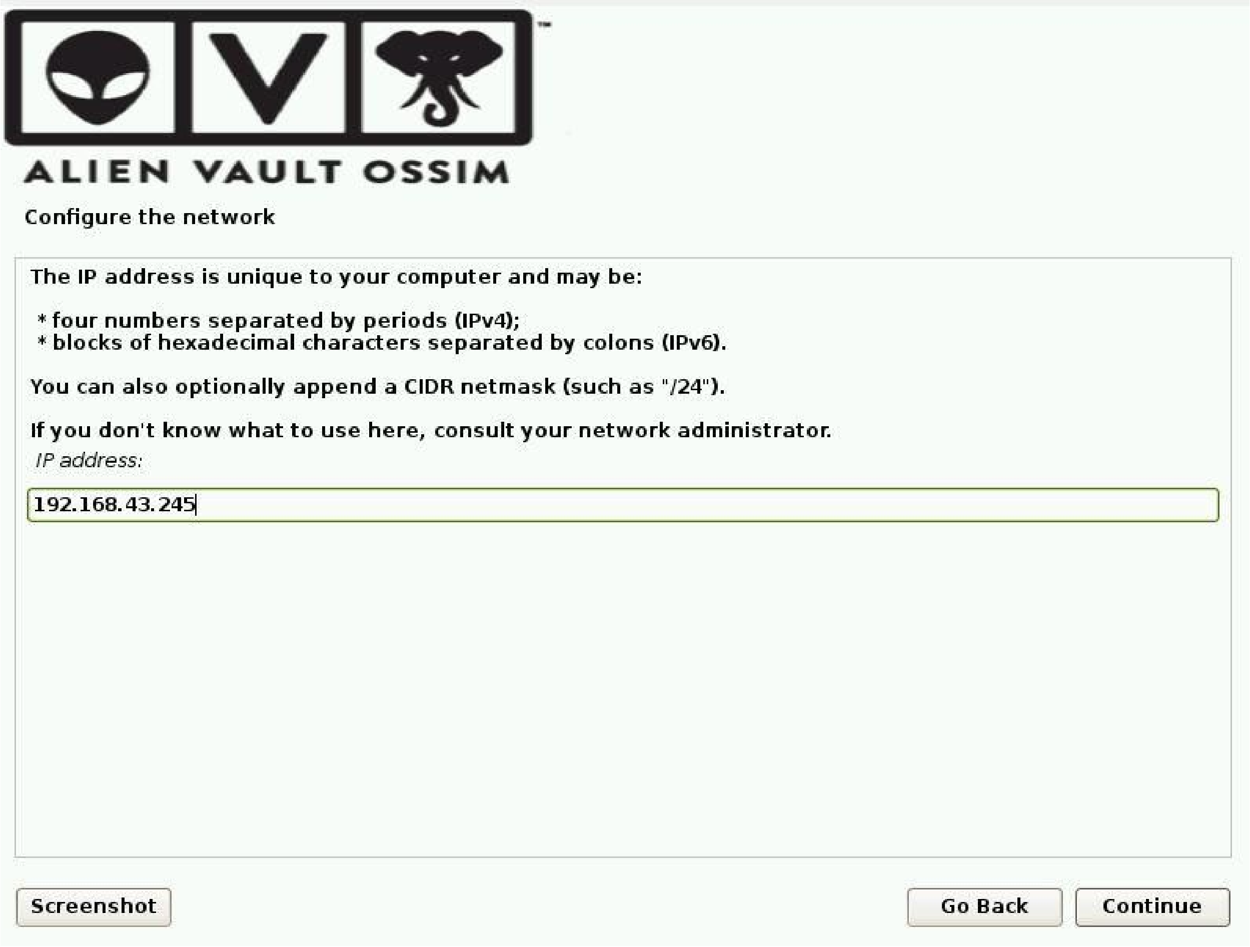
The Virtual Machine reports that the guest OS supports **mouse pointer integration.** This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual

Configure the keyboard

Keymap to use:

American English
Albanian
Arabic
Asturian
Bangladesh
Belarusian
Bengali
Belgian
Bosnian
Brazilian
British English
Bulgarian
Bulgarian (phonetic layout)
Burmese
Canadian French
Canadian Multilingual

- **Step 9:** Configure the Network, Give the Host IP address, and click continue



Configure the network

The IP address is unique to your computer and may be:

* four numbers separated by periods (IPv4);
* blocks of hexadecimal characters separated by colons (IPv6).

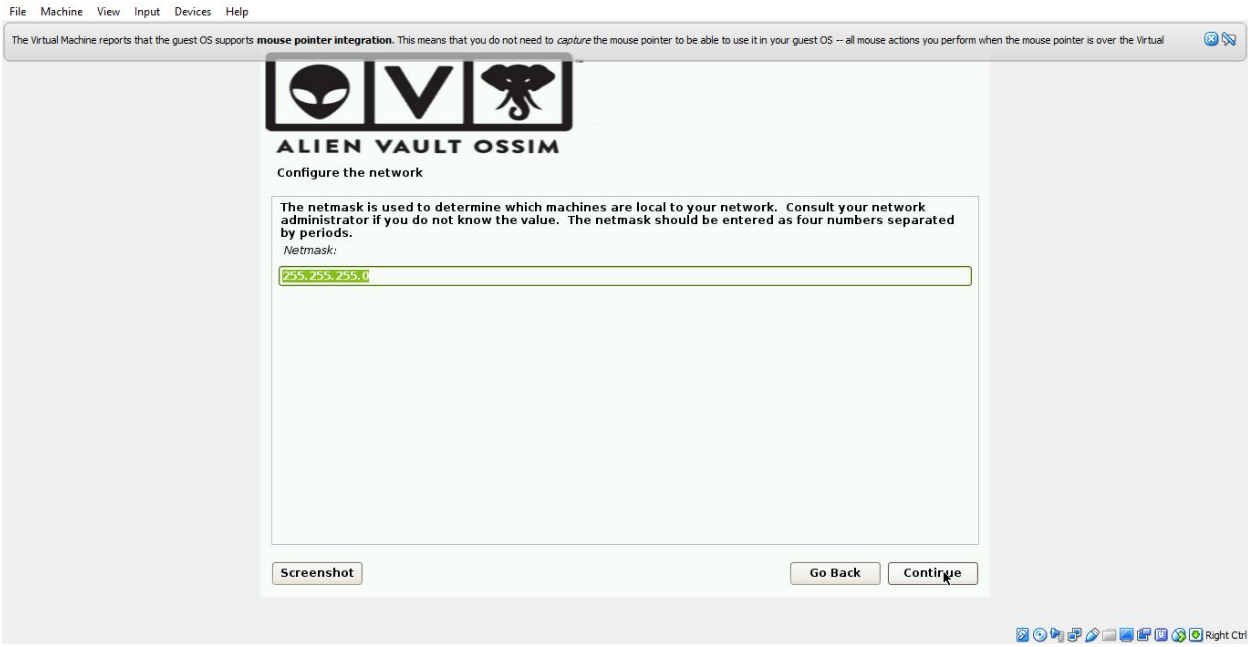
You can also optionally append a CIDR netmask (such as "/24").

If you don't know what to use here, consult your network administrator.

IP address:

192.168.43.245

- **Step 10:** Configure the Network, give the net mask, and click continue



The Virtual Machine reports that the guest OS supports **mouse pointer integration.** This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual

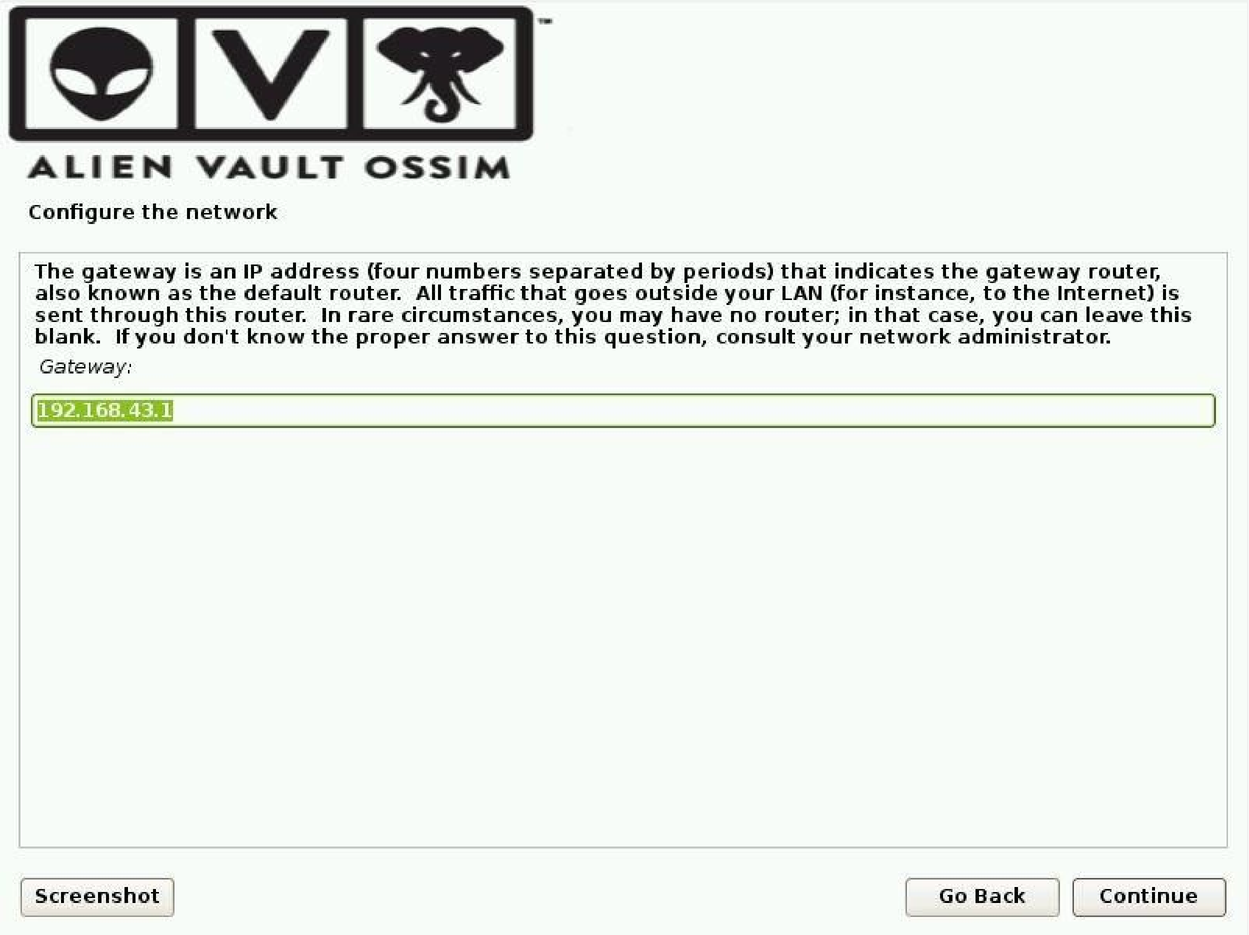
Configure the network

The netmask is used to determine which machines are local to your network. Consult your network administrator if you do not know the value. The netmask should be entered as four numbers separated by periods.

Netmask:

255.255.255.0

- **Step 11:** Configure the network, Give the gateway, and click continue



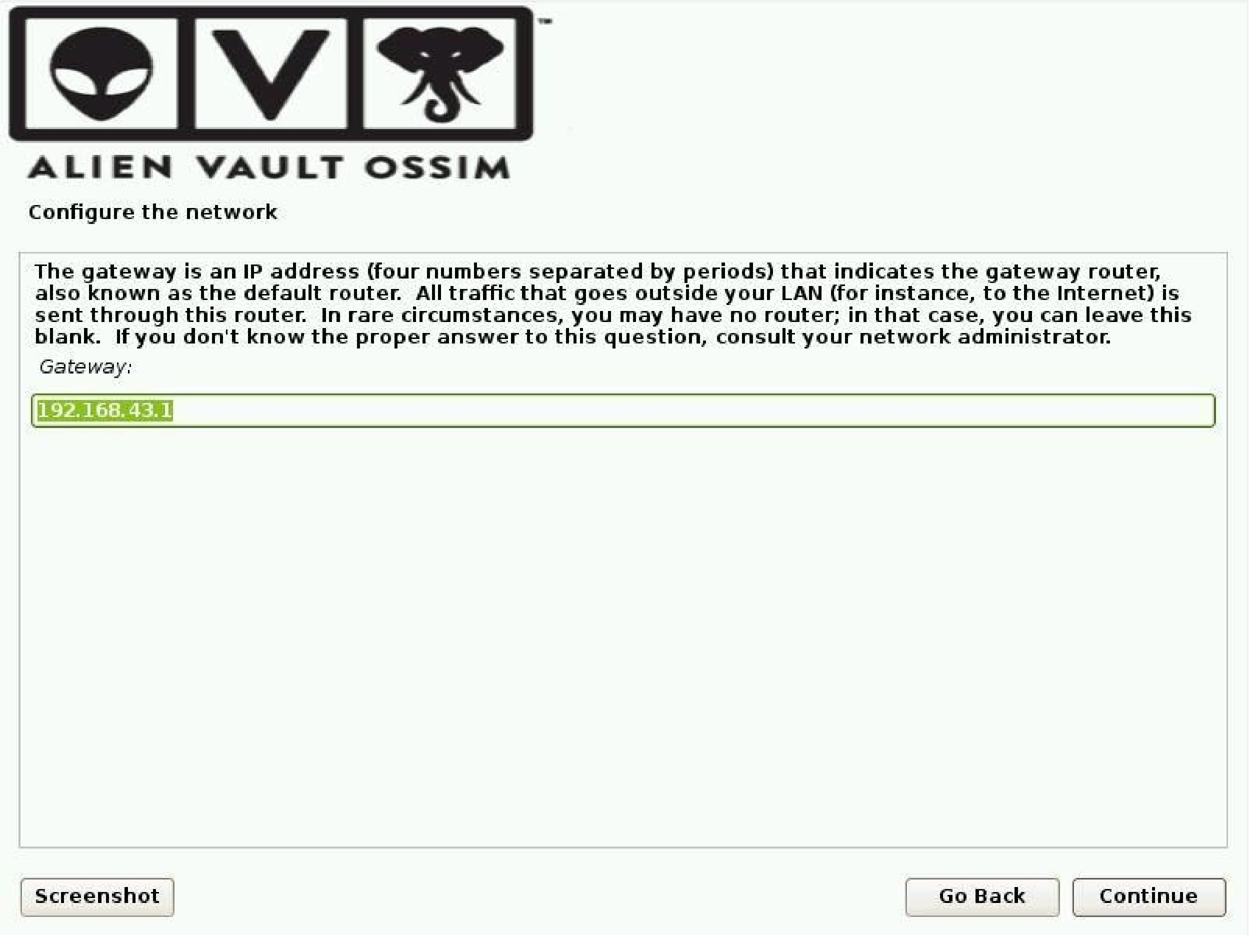
Configure the network

The gateway is an IP address (four numbers separated by periods) that indicates the gateway router, also known as the default router. All traffic that goes outside your LAN (for instance, to the Internet) is sent through this router. In rare circumstances, you may have no router; in that case, you can leave this blank. If you don't know the proper answer to this question, consult your network administrator.

Gateway:

192.168.43.1

- **Step 12:** Configure the network, Give the Name Server Addresses, and click continue



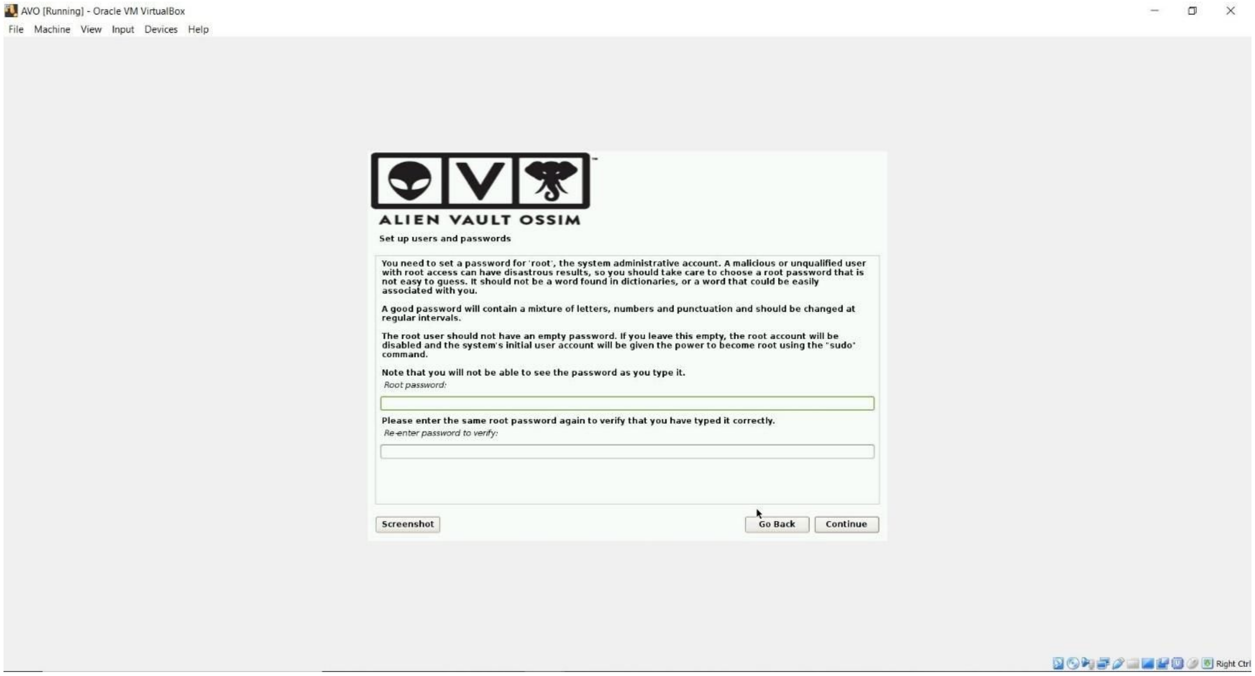
Configure the network

The gateway is an IP address (four numbers separated by periods) that indicates the gateway router, also known as the default router. All traffic that goes outside your LAN (for instance, to the Internet) is sent through this router. In rare circumstances, you may have no router; in that case, you can leave this blank. If you don't know the proper answer to this question, consult your network administrator.

Gateway:

192.168.43.1

- **Step 13:** Setup User and Password



Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

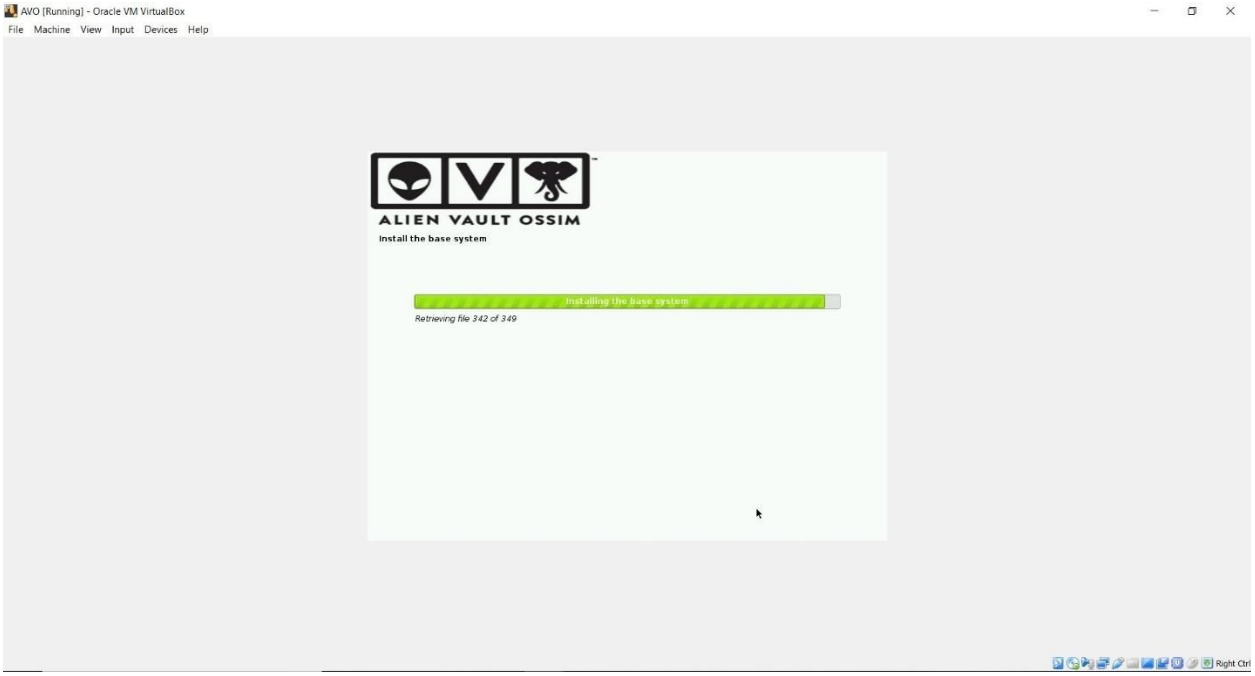
Note that you will not be able to see the password as you type it.

Root password:

Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

- **Step 14:** Alien Vault is Installing

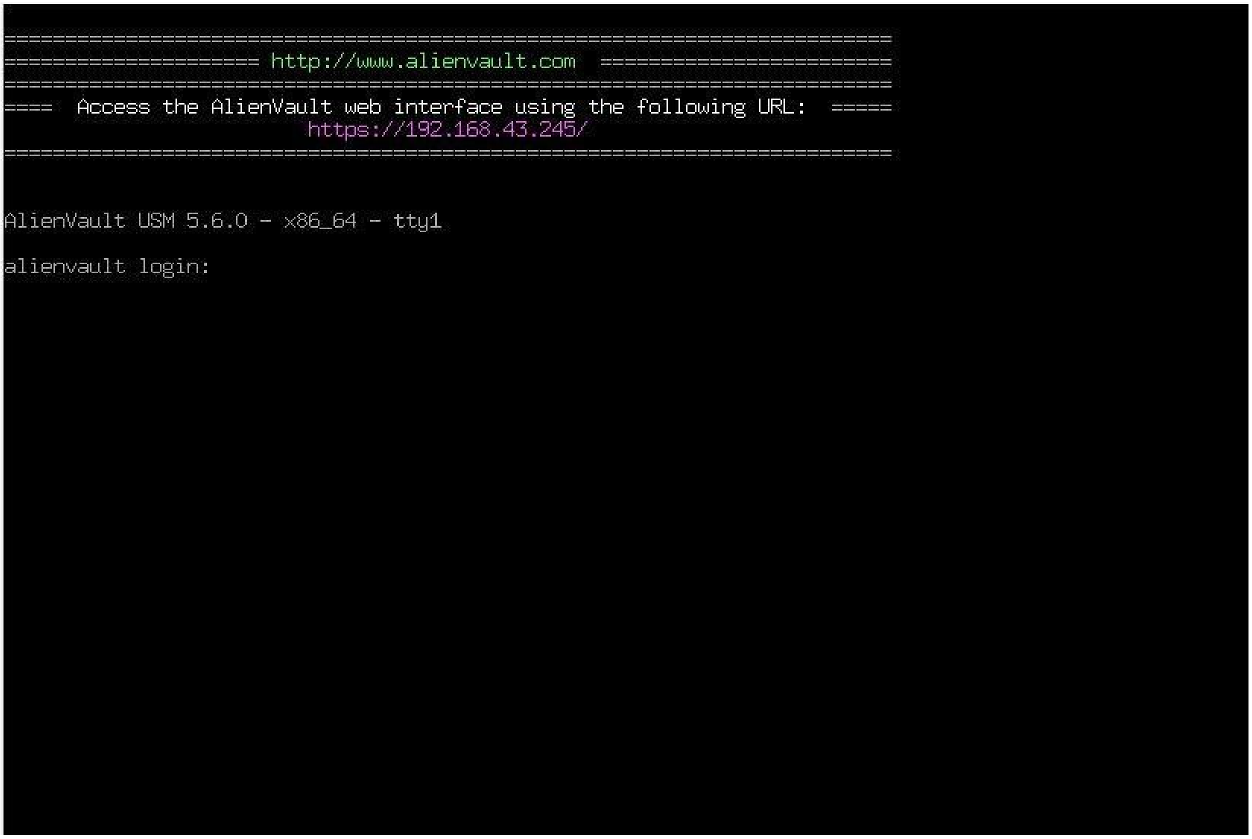

AVO [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ALIEN VAULT OSSIM
Right Ctrl

Install the base system

Installing the base system

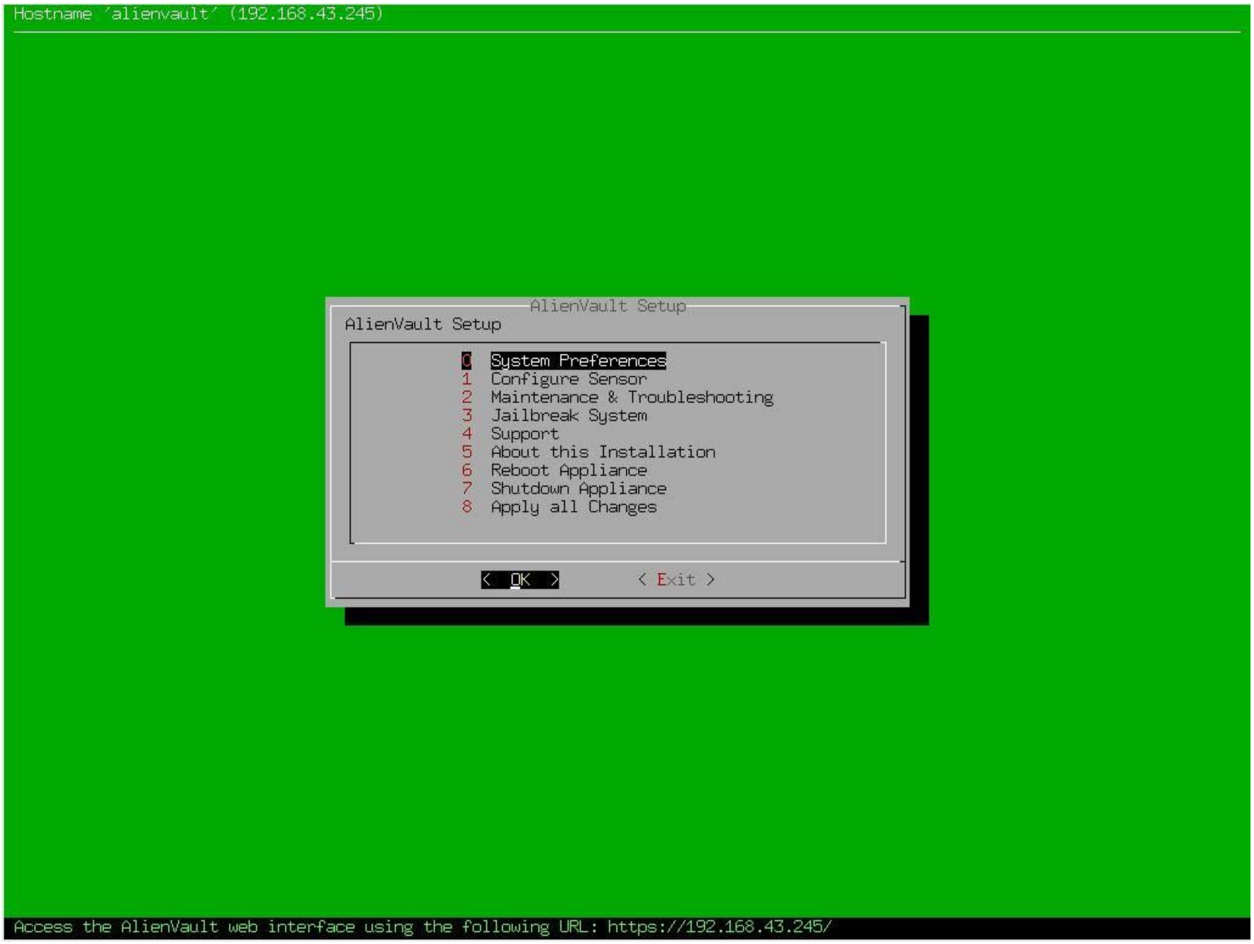
Retrieving file 342 of 349

- **Step 15:** Login using alien vault credentials



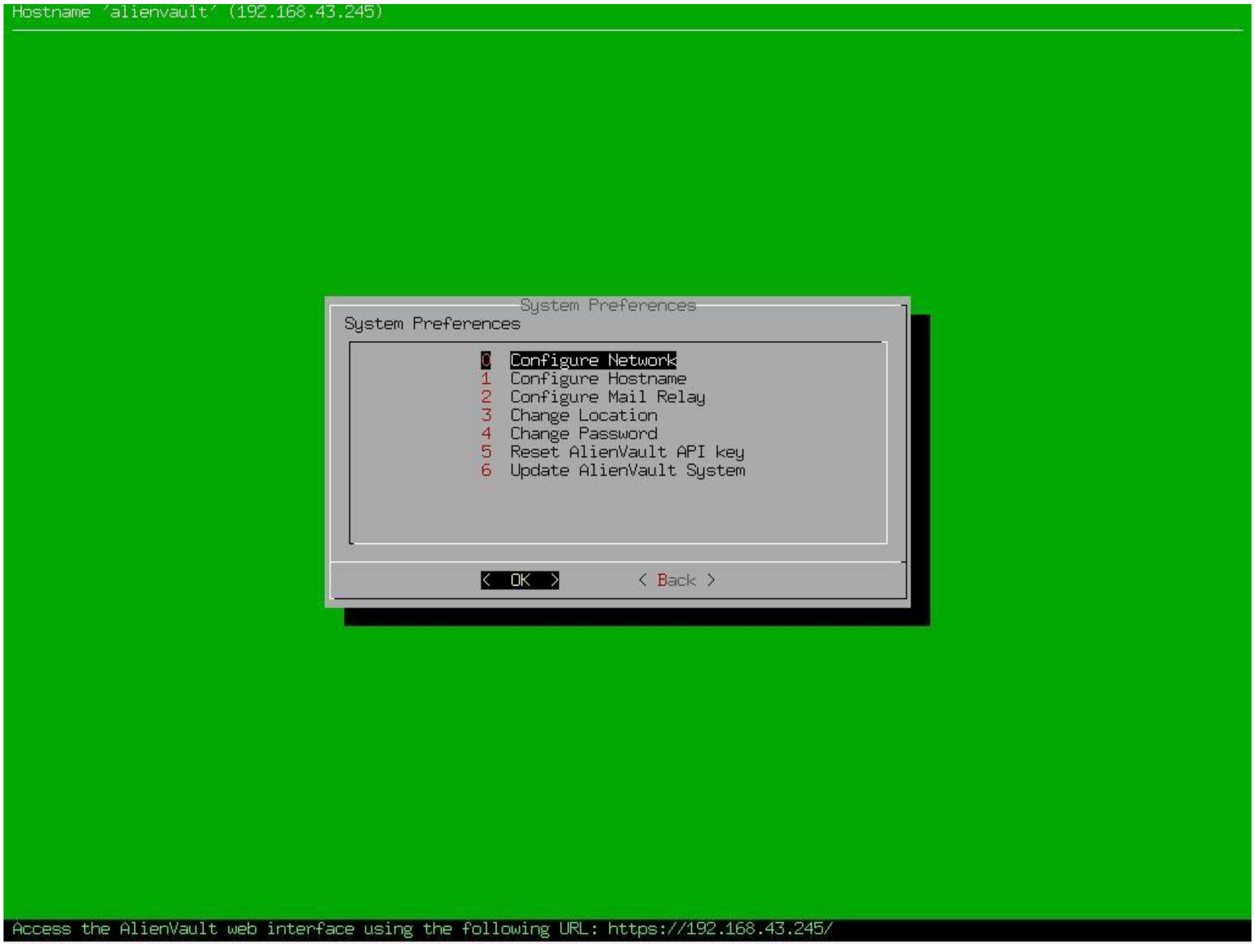
```
==========================================================================
===================== http://www.alienvault.com  ========================
==========================================================================
====  Access the AlienVault web interface using the following URL:  =====
                         https://192.168.43.245/
==========================================================================


AlienVault USM 5.6.0 - x86_64 - tty1

alienvault login:
```

Step 16: You will come up with the following screen



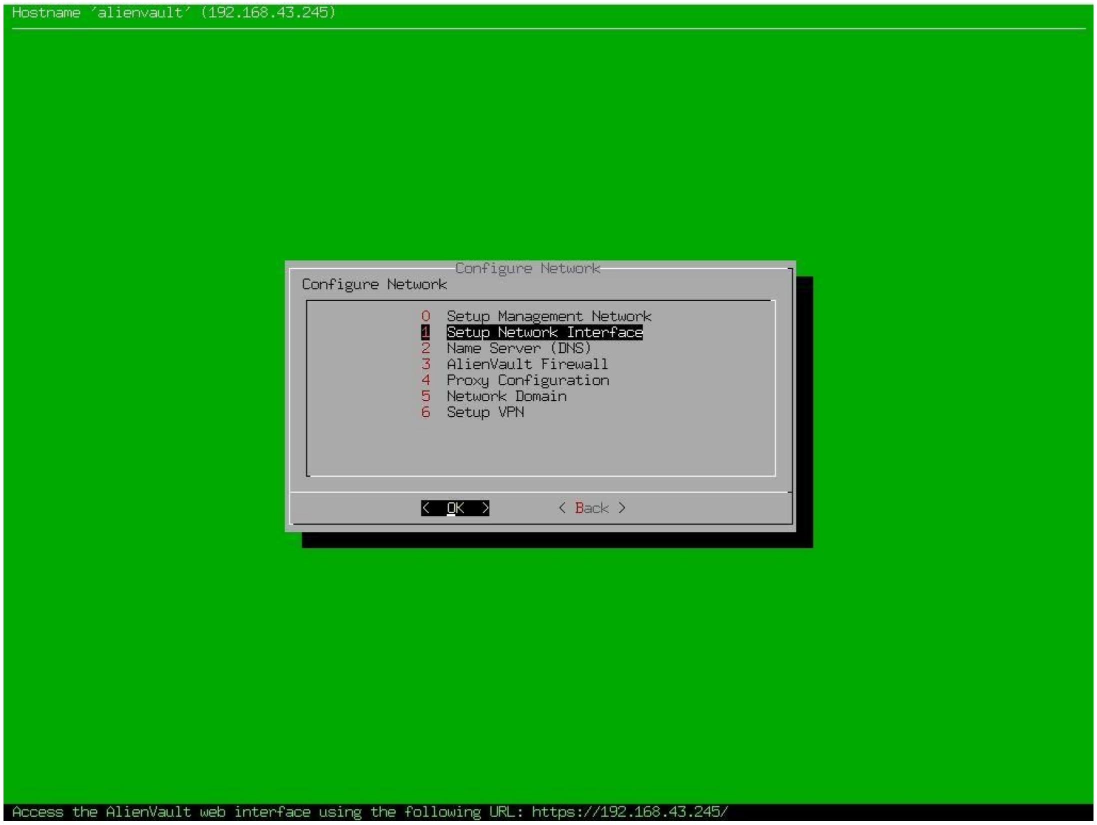
```
Hostname 'alienvault' (192.168.43.245)

AlienVault Setup
AlienVault Setup

0  System Preferences
1  Configure Sensor
2  Maintenance & Troubleshooting
3  Jailbreak System
4  Support
5  About this Installation
6  Reboot Appliance
7  Shutdown Appliance
8  Apply all Changes

< OK >    < Exit >

Access the AlienVault web interface using the following URL: https://192.168.43.245/
```

Step 17: Now Change the subnet to 255.0.0.0 which can be reached by going in system preferences in that go to Configure Network Option.



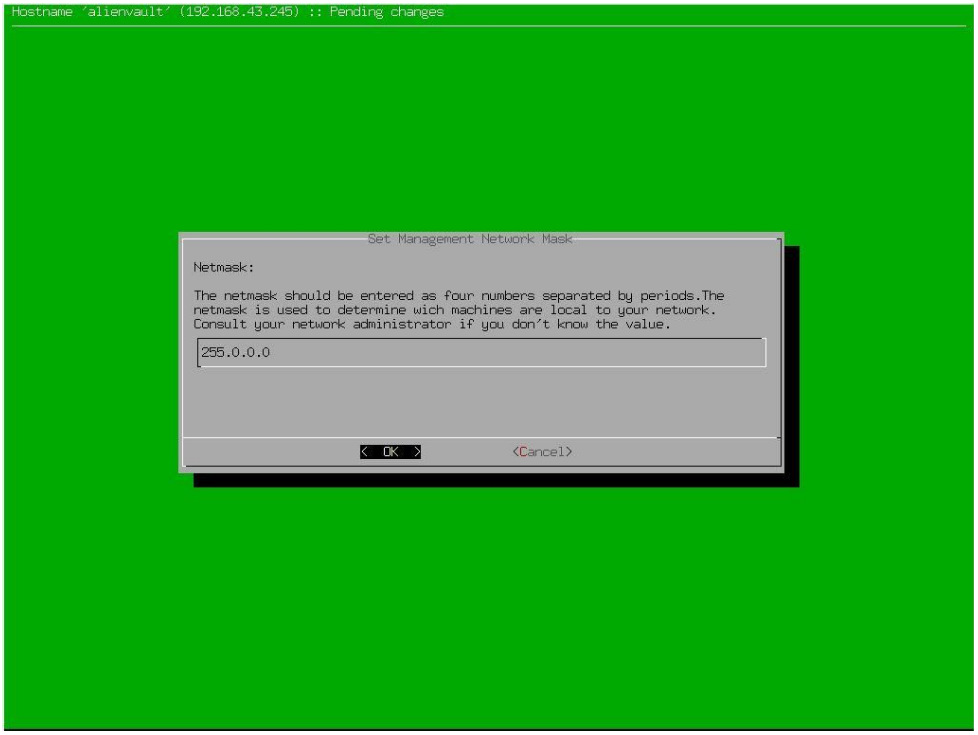
```
Hostname 'alienvault' (192.168.43.245)

System Preferences
System Preferences

0  Configure Network
1  Configure Hostname
2  Configure Mail Relay
3  Change Location
4  Change Password
5  Reset AlienVault API key
6  Update AlienVault System

< OK >        < Back >

Access the AlienVault web interface using the following URL: https://192.168.43.245/
```

- **Step 18:**In configure network option choose setup network interface.



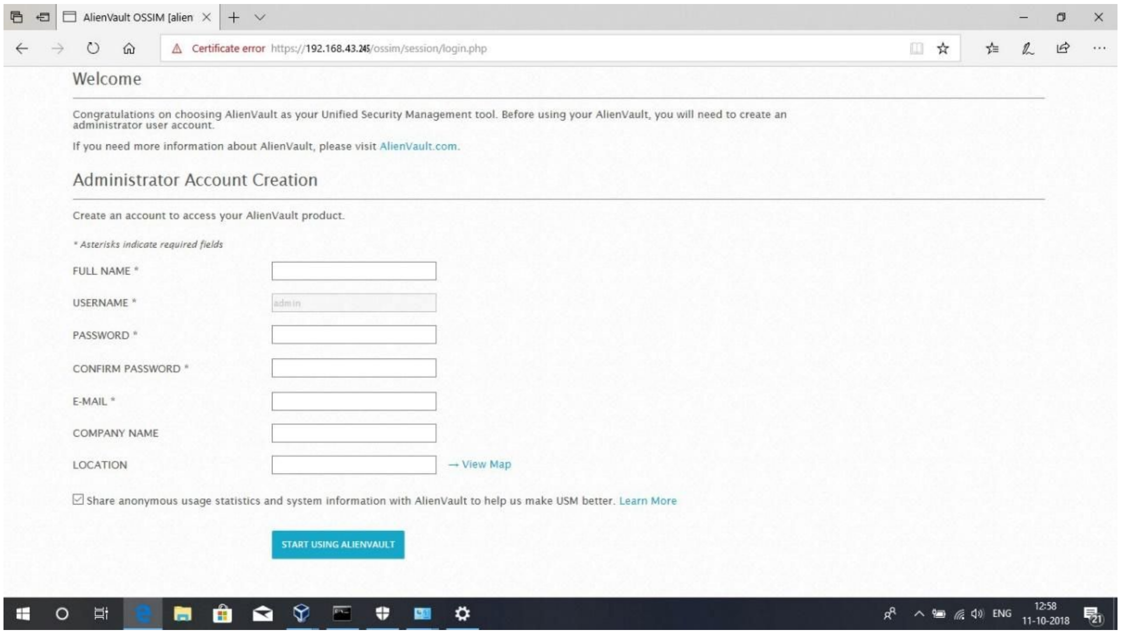
```
Hostname 'alienvault' (192.168.43.245)

Configure Network
Configure Network
 0  Setup Management Network
 1  Setup Network Interface
 2  Name Server (DNS)
 3  AlienVault Firewall
 4  Proxy Configuration
 5  Network Domain
 6  Setup VPN

< OK >        < Back >

Access the AlienVault web interface using the following URL: https://192.168.43.245/
```

- **Step 19:** In network interface change the subnet address to 255.0.0.0 r.



```
Hostname 'alienvault' (192.168.43.245) :: Pending changes

Set Management Network Mask
Netmask:

The netmask should be entered as four numbers separated by periods.The
netmask is used to determine wich machines are local to your network.
Consult your network administrator if you don't know the value.

255.0.0.0

< OK >                <Cancel>
```

- **Step 20:** Once this done apply the changes and then open the URL in browser.
  For Example, in this the ip is taken as 192.168.43.245
  So, in browser enter https://192.168.43.245/



Certificate error https://192.168.43.245/ossim/session/login.php

Welcome

Congratulations on choosing AlienVault as your Unified Security Management tool. Before using your AlienVault, you will need to create an administrator user account.

If you need more information about AlienVault, please visit AlienVault.com.

Administrator Account Creation

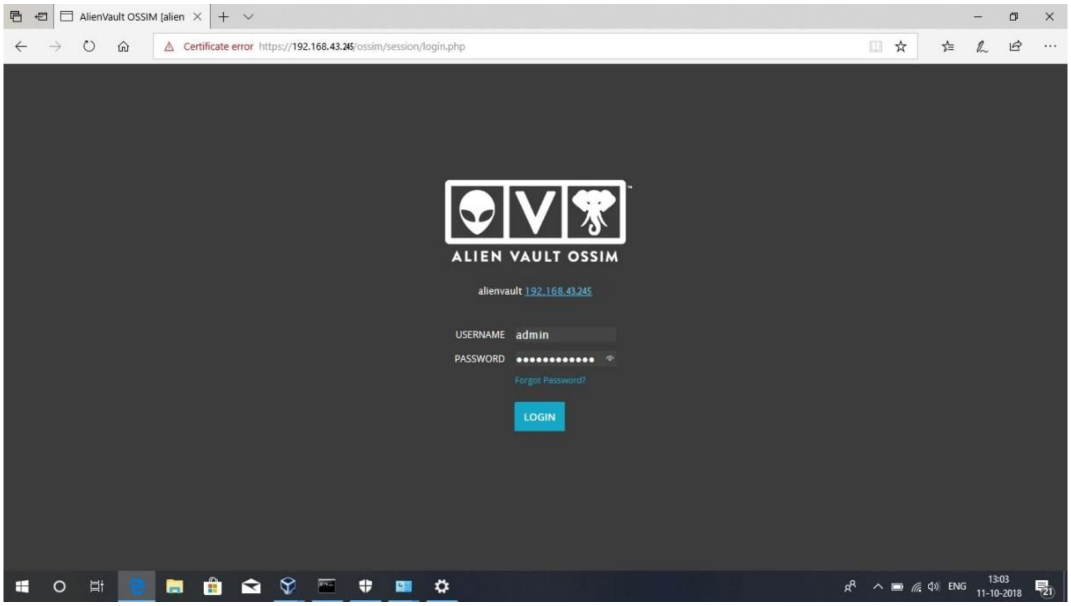
Create an account to access your AlienVault product.

* Asterisks indicate required fields

FULL NAME *	
USERNAME *	admin
PASSWORD *	
CONFIRM PASSWORD *	
E-MAIL *	
COMPANY NAME	
LOCATION	→ View Map

☑ Share anonymous usage statistics and system information with AlienVault to help us make USM better. Learn More

- **Step 21:** Enter the login credentials you provided in alien vault.



AlienVault OSSIM [alien

Certificate error https://192.168.43.245/ossim/session/login.php

ALIEN VAULT OSSIM

alienvault 192.168.43.245

USERNAME admin

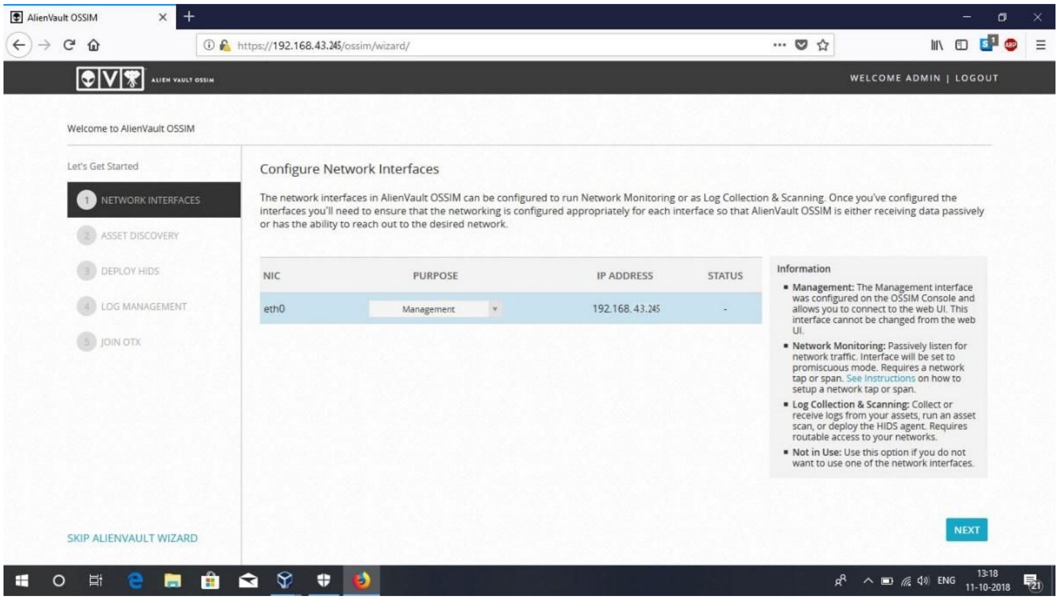
PASSWORD ●●●●●●●●●●●●●

Forgot Password?

LOGIN

13:03 11-10-2018

- **Step 22:** Once valid user credentials are entered users are greeted with following dashboard page.



AlienVault OSSIM

https://192.168.43.245/ossim/wizard/

ALIEN VAULT OSSIM

WELCOME ADMIN | LOGOUT

Welcome to AlienVault OSSIM

Let's Get Started

1 NETWORK INTERFACES

2 ASSET DISCOVERY

3 DEPLOY HIDS

4 LOG MANAGEMENT

5 JOIN OTX

Configure Network Interfaces

The network interfaces in AlienVault OSSIM can be configured to run Network Monitoring or as Log Collection & Scanning. Once you've configured the interfaces you'll need to ensure that the networking is configured appropriately for each interface so that AlienVault OSSIM is either receiving data passively or has the ability to reach out to the desired network.

NIC	PURPOSE	IP ADDRESS	STATUS
eth0	Management	192.168.43.245	-

Information

- **Management:** The Management interface was configured on the OSSIM Console and allows you to connect to the web UI. This interface cannot be changed from the web UI.
- **Network Monitoring:** Passively listen for network traffic. Interface will be set to promiscuous mode. Requires a network tap or span. See Instructions on how to setup a network tap or span.
- **Log Collection & Scanning:** Collect or receive logs from your assets, run an asset scan, or deploy the HIDS agent. Requires routable access to your networks.
- **Not in Use:** Use this option if you do not want to use one of the network interfaces.

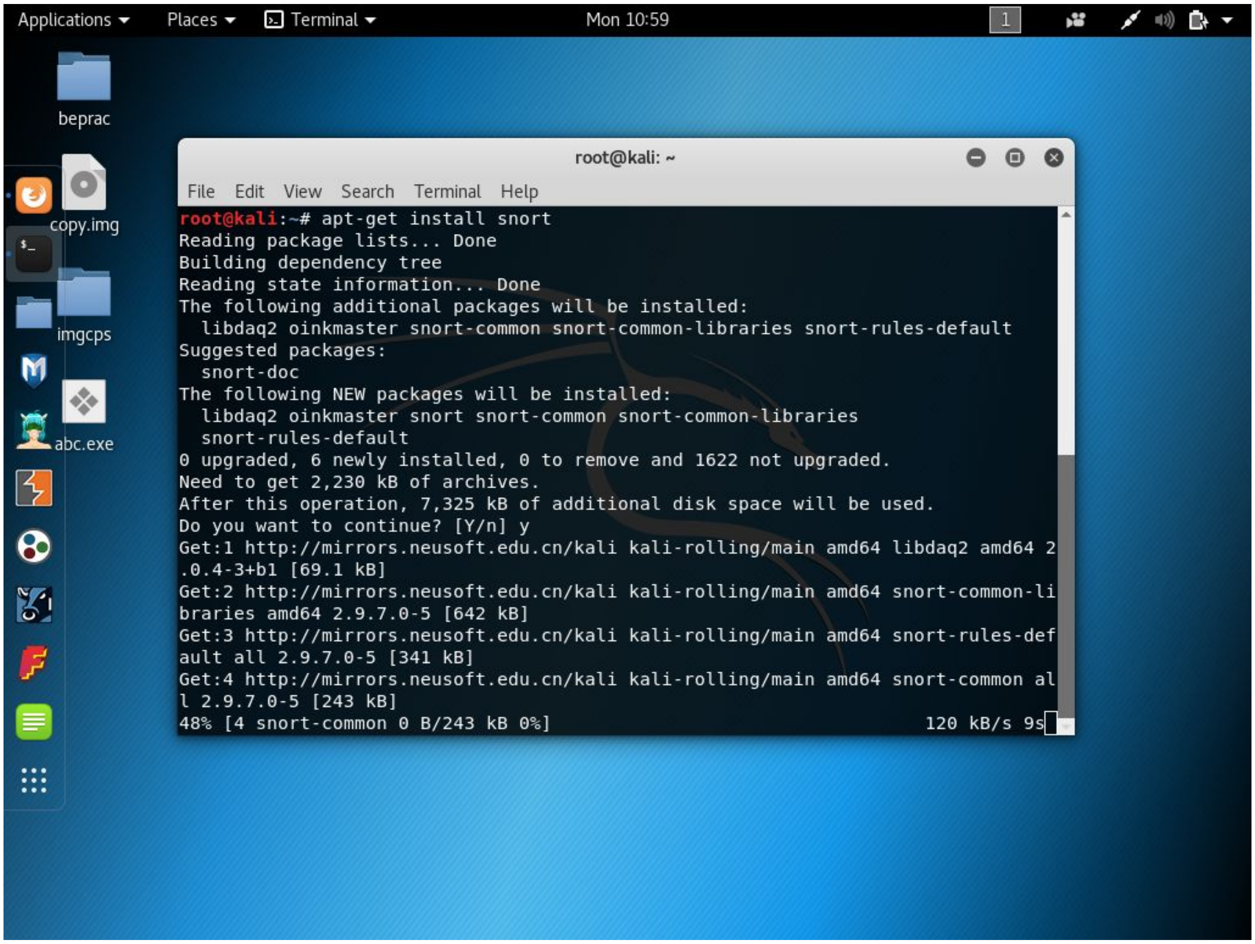
SKIP ALIENVAULT WIZARD

NEXT

13:18 11-10-2018

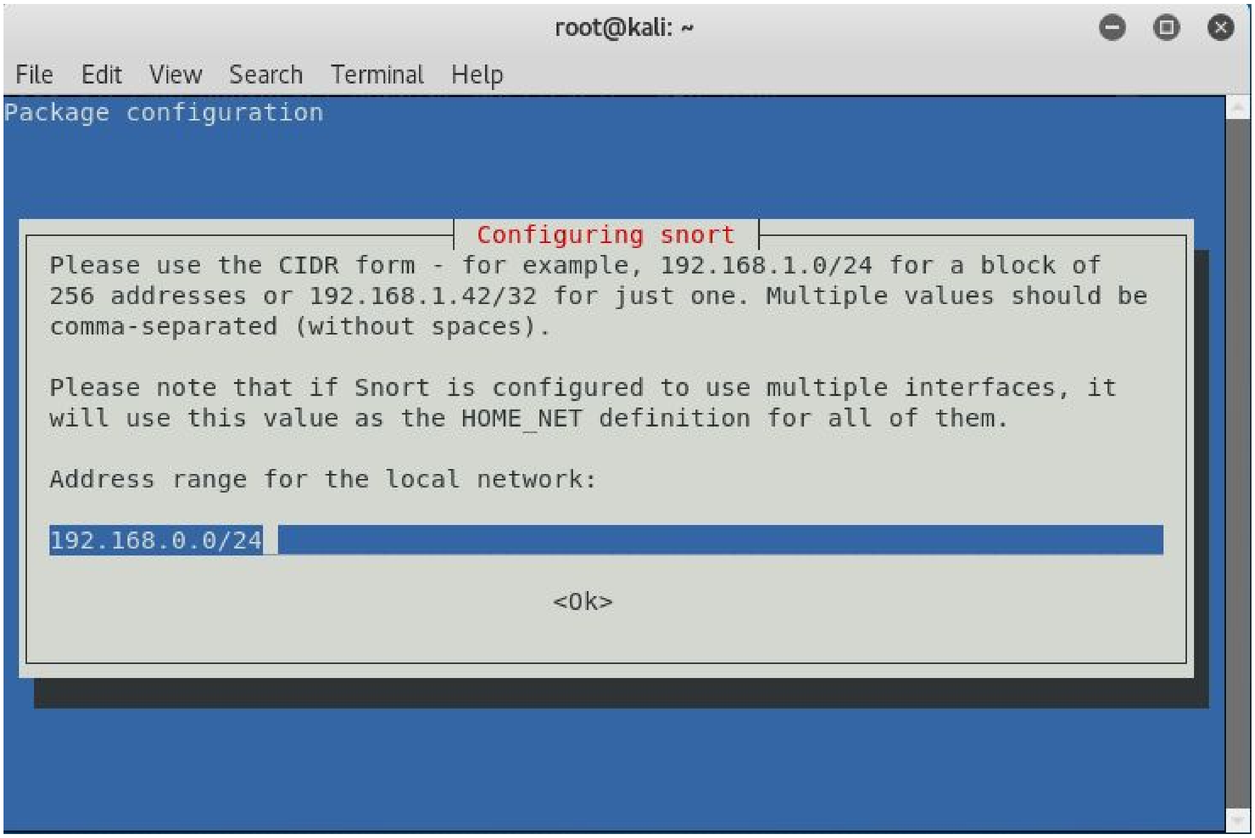
Installation of Snort in any Linux distribution

- **Step 1:** Open Terminal and type apt-get install snort (this command installs Snort. If you are not root, “type sudo apt-get install snort”)



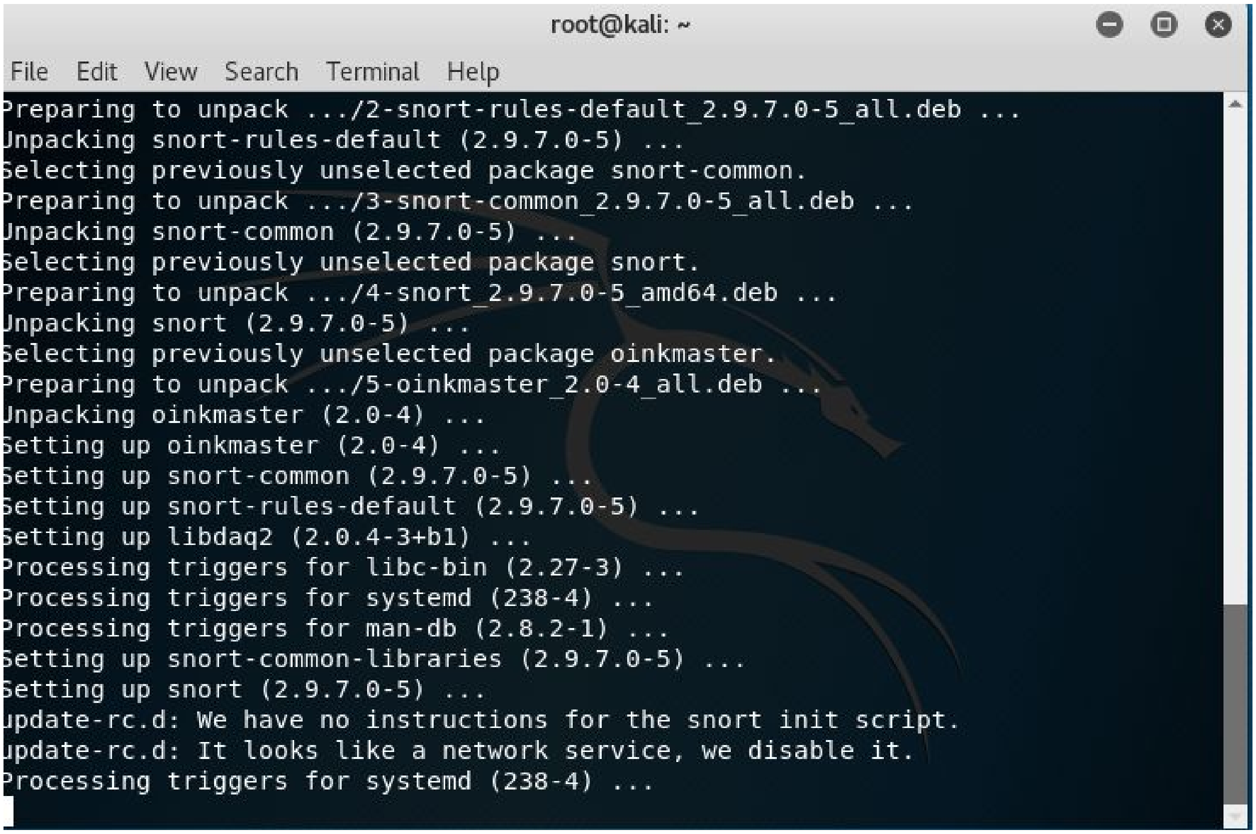
```
root@kali:~# apt-get install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdaq2 oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 oinkmaster snort snort-common snort-common-libraries
  snort-rules-default
0 upgraded, 6 newly installed, 0 to remove and 1622 not upgraded.
Need to get 2,230 kB of archives.
After this operation, 7,325 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirrors.neusoft.edu.cn/kali kali-rolling/main amd64 libdaq2 amd64 2
.0.4-3+b1 [69.1 kB]
Get:2 http://mirrors.neusoft.edu.cn/kali kali-rolling/main amd64 snort-common-li
braries amd64 2.9.7.0-5 [642 kB]
Get:3 http://mirrors.neusoft.edu.cn/kali kali-rolling/main amd64 snort-rules-def
ault all 2.9.7.0-5 [341 kB]
Get:4 http://mirrors.neusoft.edu.cn/kali kali-rolling/main amd64 snort-common al
l 2.9.7.0-5 [243 kB]
48% [4 snort-common 0 B/243 kB 0%]                                120 kB/s 9s
```

- **Step 2:** Configure Snort by providing the range of ip address.



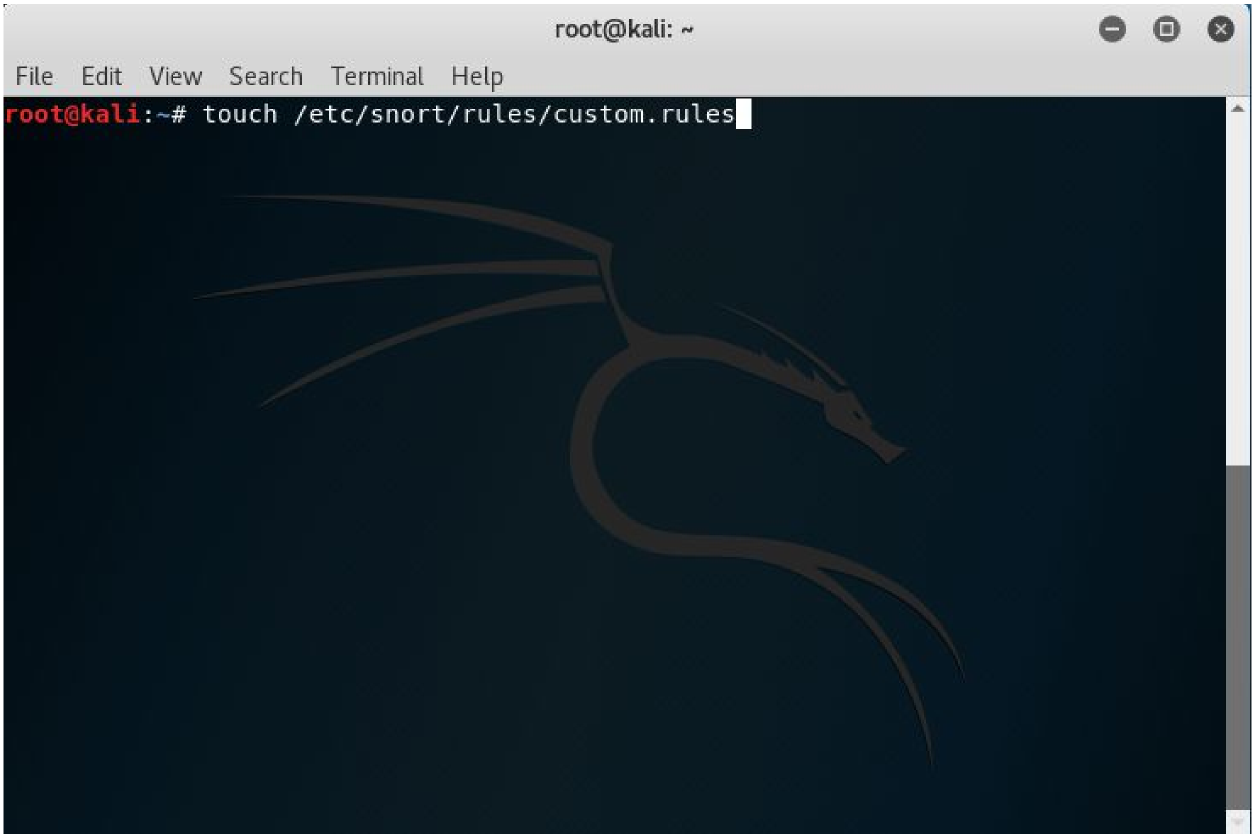
```
Package configuration

                         Configuring snort
  Please use the CIDR form - for example, 192.168.1.0/24 for a block of
  256 addresses or 192.168.1.42/32 for just one. Multiple values should be
  comma-separated (without spaces).

  Please note that if Snort is configured to use multiple interfaces, it
  will use this value as the HOME_NET definition for all of them.

  Address range for the local network:

  192.168.0.0/24

                                <Ok>
```

- **Step 3:** Once you click Ok further installation of dependencies installation begins.



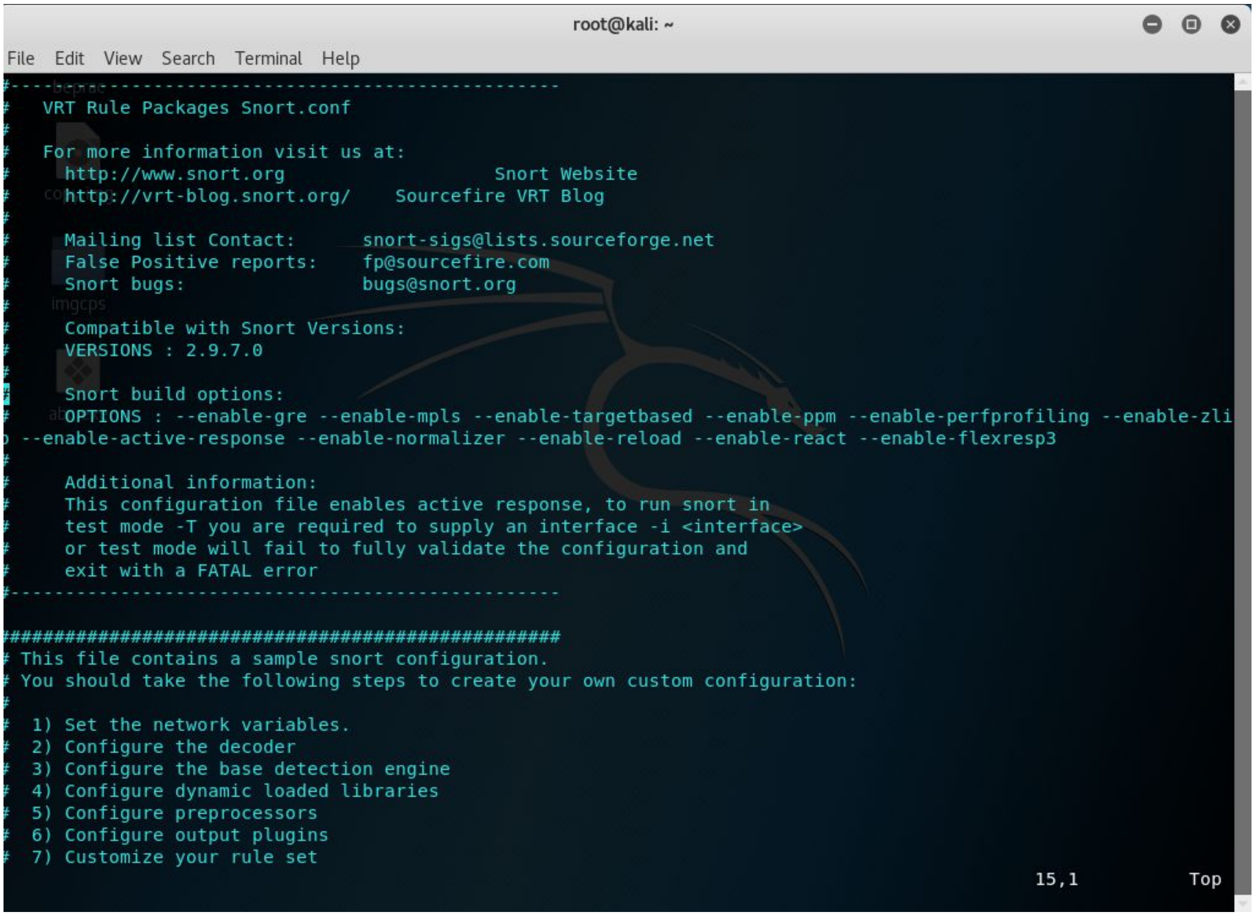
```
Preparing to unpack .../2-snort-rules-default_2.9.7.0-5_all.deb ...
Unpacking snort-rules-default (2.9.7.0-5) ...
Selecting previously unselected package snort-common.
Preparing to unpack .../3-snort-common_2.9.7.0-5_all.deb ...
Unpacking snort-common (2.9.7.0-5) ...
Selecting previously unselected package snort.
Preparing to unpack .../4-snort_2.9.7.0-5_amd64.deb ...
Unpacking snort (2.9.7.0-5) ...
Selecting previously unselected package oinkmaster.
Preparing to unpack .../5-oinkmaster_2.0-4_all.deb ...
Unpacking oinkmaster (2.0-4) ...
Setting up oinkmaster (2.0-4) ...
Setting up snort-common (2.9.7.0-5) ...
Setting up snort-rules-default (2.9.7.0-5) ...
Setting up libdaq2 (2.0.4-3+b1) ...
Processing triggers for libc-bin (2.27-3) ...
Processing triggers for systemd (238-4) ...
Processing triggers for man-db (2.8.2-1) ...
Setting up snort-common-libraries (2.9.7.0-5) ...
Setting up snort (2.9.7.0-5) ...
update-rc.d: We have no instructions for the snort init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for systemd (238-4) ...
```

- **Step 4:** Once the installation is done we can create our own custom rules by using the following command touch /etc/snort/rules/custom.rules (this creates a rule file).



```
root@kali:~# touch /etc/snort/rules/custom.rules
```

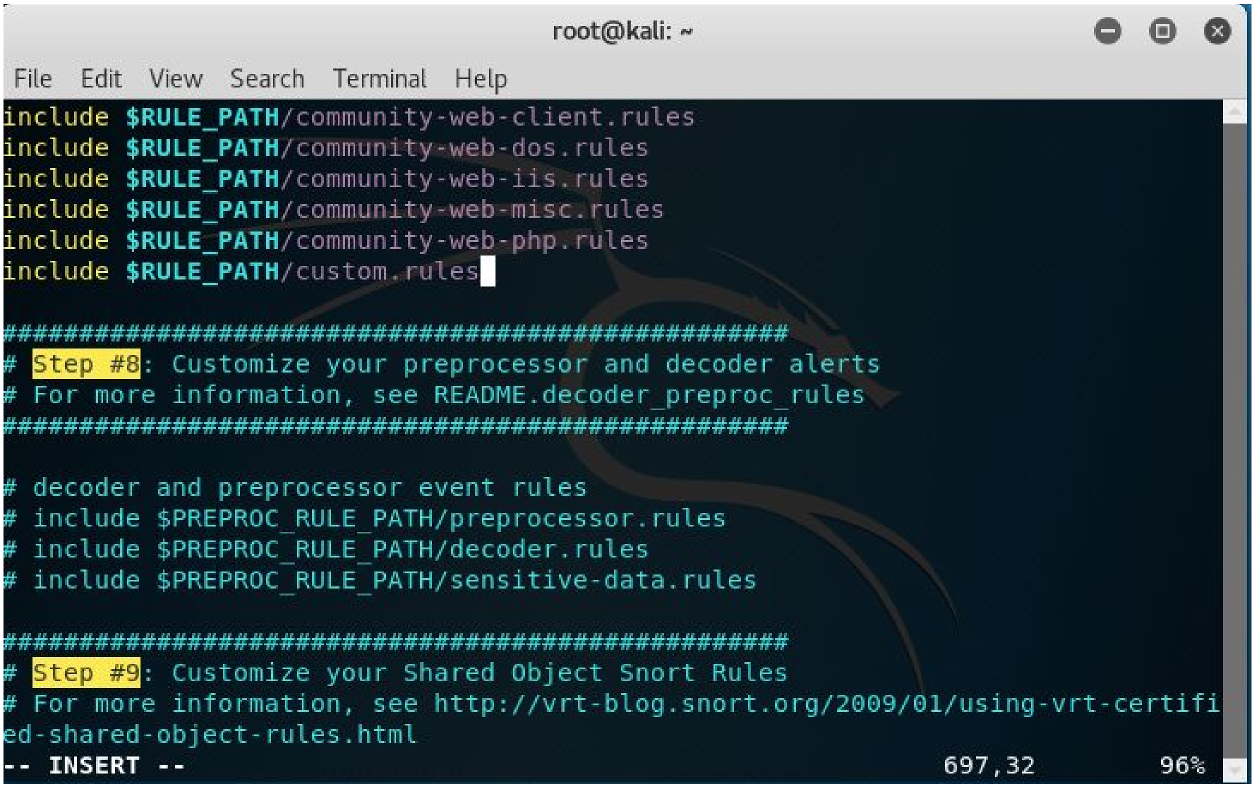
- **Step 5:** To change the Configuration of snort type command vi /etc/snort/snort.conf and make sure to press i for insert mode.



```
#--------------------------------------------------
#   VRT Rule Packages Snort.conf
#
#   For more information visit us at:
#     http://www.snort.org                   Snort Website
#     http://vrt-blog.snort.org/    Sourcefire VRT Blog
#
#     Mailing list Contact:      snort-sigs@lists.sourceforge.net
#     False Positive reports:    fp@sourcefire.com
#     Snort bugs:                bugs@snort.org
#
#     Compatible with Snort Versions:
#     VERSIONS : 2.9.7.0
#
#     Snort build options:
#     OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --enable-zli
b --enable-active-response --enable-normalizer --enable-reload --enable-react --enable-flexresp3
#
#     Additional information:
#     This configuration file enables active response, to run snort in
#     test mode -T you are required to supply an interface -i <interface>
#     or test mode will fail to fully validate the configuration and
#     exit with a FATAL error
#--------------------------------------------------

###################################################
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
#  1) Set the network variables.
#  2) Configure the decoder
#  3) Configure the base detection engine
#  4) Configure dynamic loaded libraries
#  5) Configure preprocessors
#  6) Configure output plugins
#  7) Customize your rule set
                                                                                           15,1          Top
```

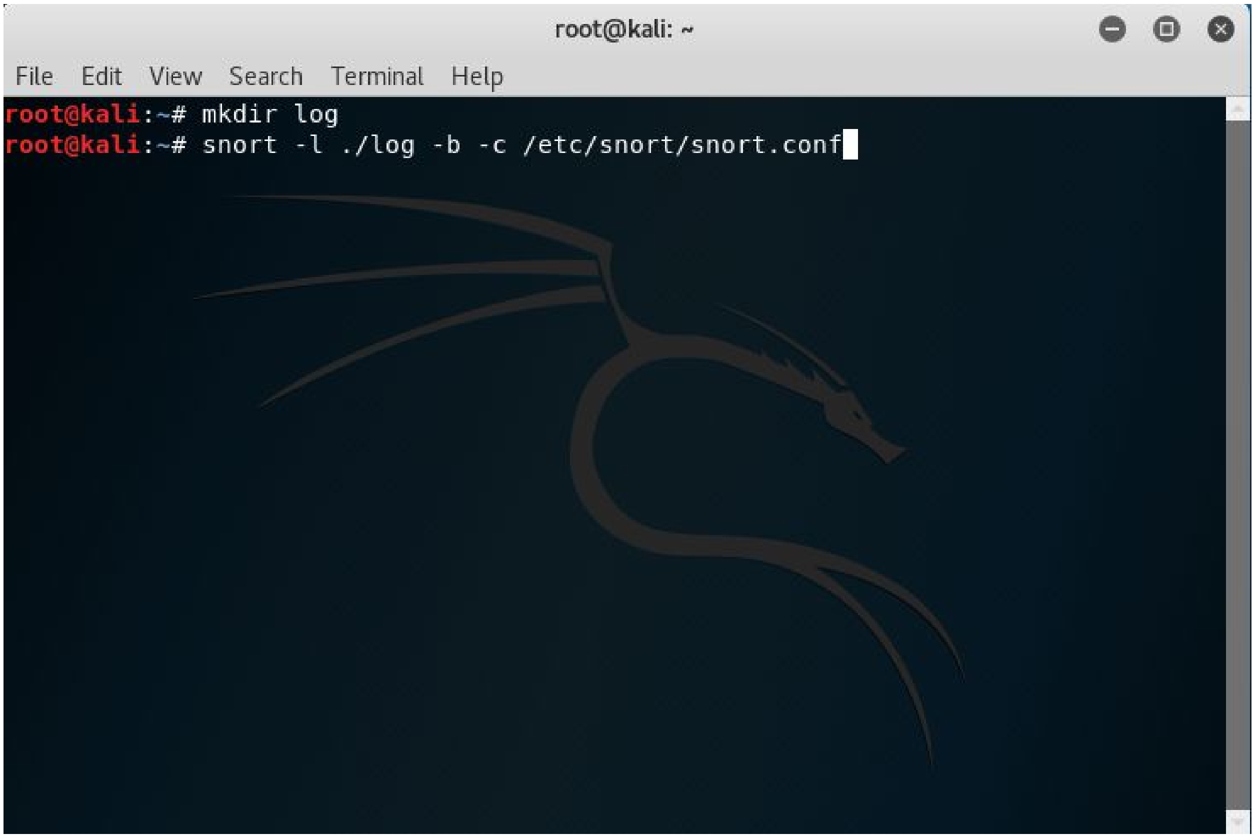
- **Step 6:** Once in configuration file press i to get in insert mode and enter path for our custom made rule file and then

:wq so as to save changes and exit.



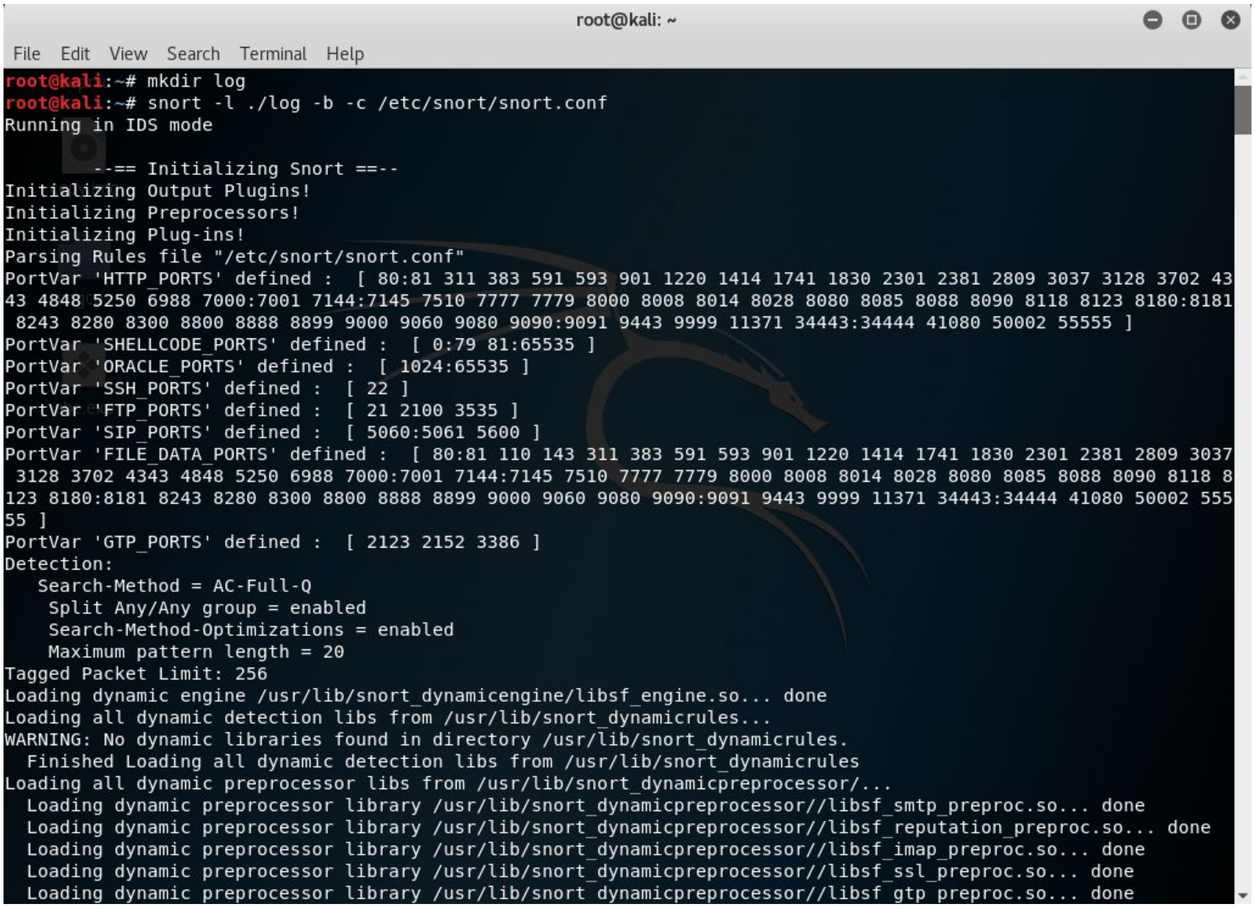
```
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/custom.rules

###################################################
# Step #8: Customize your preprocessor and decoder alerts
# For more information, see README.decoder_preproc_rules
###################################################

# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH/preprocessor.rules
# include $PREPROC_RULE_PATH/decoder.rules
# include $PREPROC_RULE_PATH/sensitive-data.rules

###################################################
# Step #9: Customize your Shared Object Snort Rules
# For more information, see http://vrt-blog.snort.org/2009/01/using-vrt-certifi
ed-shared-object-rules.html
-- INSERT --                                                 697,32        96%
```

- **Step 7:** To run basic snort with basic logging function type command snort -l ./log -b -c /etc/snort/snort.conf (this runs Snort in NIDS mode)



```
root@kali:~# mkdir log
root@kali:~# snort -l ./log -b -c /etc/snort/snort.conf
```

- **Step 8:** Once you run this command following output can be seen which will be later stored in log file.



```
root@kali:~# mkdir log
root@kali:~# snort -l ./log -b -c /etc/snort/snort.conf
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 43
43 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181
 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037
 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8
123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 555
55 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_smtp_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_reputation_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_imap_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_ssl_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_gtp_preproc.so... done
```