

Information security – IV
Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 51
SNORT
Configuration and Demonstration

Hi, welcome to this session on snort configuration. In the previous session we were discussing how to install snort. I hope you were able to install snort if you are facing problems some of the problems will be able to solve in the forum, but then many of the problems if you face, the best place is to look into the web and then try to see how to fix the problem. So, we will not be able to solve all of your problems. So, please go ahead and look into the web and try to fix the installation of snort if you have any problems.

We will now proceed with how to configure snort and how to write the rules. We will also show a very small demo where we try to detect the icmp packets. Someone who tries to ping from another machine we will write rules to show how to detect icmp packets. Hope you are all familiar with the rules that we discussed in the theory section about 2 or three modules back. If not please recollect so, that we can frame the rules and do intrusion detection.

(Refer Slide Time: 01:26)

```
Ubuntu14 (Running) - Oracle VM VirtualBox
Terminal
mjsraman@mjsraman-Ubuntu14-32:~/daq-2.0.6/snort-2.9.11.15
mjsraman@mjsraman-Ubuntu14-32:~/daq-2.0.6/snort-2.9.11.15 sudo mkdir /etc/snort
mkdir: cannot create directory '/etc/snort': file exists
mjsraman@mjsraman-Ubuntu14-32:~/daq-2.0.6/snort-2.9.11.15 ls -l /etc/snort/prepr
C/rules/
total 0
mjsraman@mjsraman-Ubuntu14-32:~/daq-2.0.6/snort-2.9.11.15 ls -l /etc/snort/
total 268
-rw-r--r-- 1 mjsraman mjsraman 1281 Aug 20 2007 attribute_table.dtd
-rw-r--r-- 1 root root 3157 Jan 11 12:17 classification.config
-rw-r--r-- 1 mjsraman mjsraman 21050 Jun 10 2014 file_magic.conf
-rw-r--r-- 1 mjsraman mjsraman 31971 Nov 19 2015 gen-msg.map
drwxr-xr-t 2 root root 4096 Jan 11 11:53 preproc_rules
-rw-r--r-- 1 root root 687 Jan 11 12:17 reference.config
drwxr-xr-t 2 root root 4096 Jan 11 12:30 rules
-rw-r--r-- 1 mjsraman mjsraman 27110 Jan 11 12:15 snort.conf
-rw-r--r-- 1 mjsraman mjsraman 2335 Jul 7 2009 threshold.conf
-rw-r--r-- 1 mjsraman mjsraman 166006 Jul 14 2011 unicode.map
mjsraman@mjsraman-Ubuntu14-32:~/daq-2.0.6/snort-2.9.11.15

sudo mkdir /etc/snort
sudo mkdir /etc/snort/preproc_rules
sudo mkdir /etc/snort/rules
sudo mkdir /var/log/snort
sudo mkdir /usr/local/lib/snort_dynamicrules
sudo touch /etc/snort/rules/white_list.rules
sudo touch /etc/snort/rules/black_list.rules
sudo touch /etc/snort/rules/local.rules
sudo chmod -R 5775 /etc/snort
sudo chmod -R 5775 /var/log/snort
h -al /etc/snort
sudo chmod -R 5775 /usr/local/lib/snort
sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
cd /daq-2.0.6/
cd snort-2.9.11.1/
sudo cp -avr /etc/*.conf /etc/*map /etc/*dtd /etc/snort/
sudo cp -r /etc/*.conf /etc/snort/
sudo cp ./src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor*
/usr/local/lib/snort_dynamicpreprocessor/
sudo sed -i 's/include SRULE_PATH/include SRULE_PATH' /etc/snort/snort.conf
vim /etc/snort/snort.conf

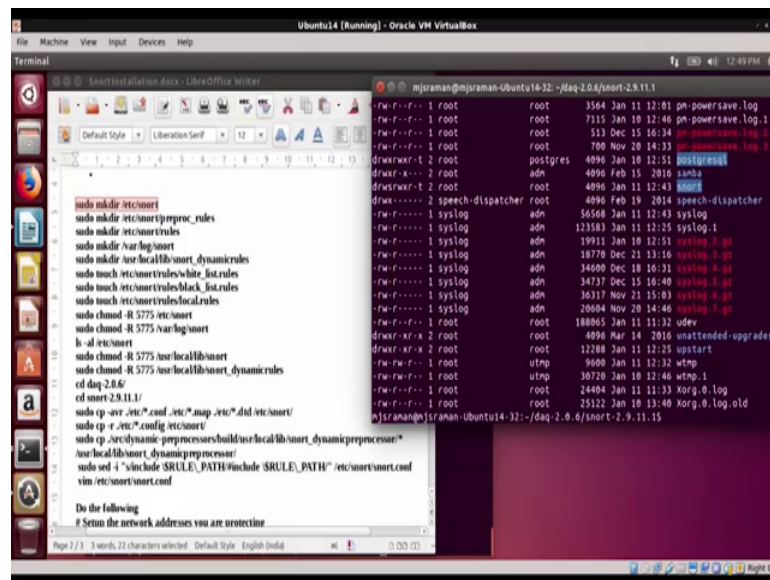
Do the following
# Set the network addresses you are protecting
```

So, let us now start with configuration of snort. So, if you look at this what we need to do is, we had actually installed snort in the directory called daq 2.0.6 and then snort 2 dot 9 dot 11 dot 1 and what we will do right now is, we will now try to create files and directories to store the configuration of snort. So, let us not use the default configuration of snort, we will copy the default configuration that comes along with snort into a separate directory and in that directory we will make the changes and we will use snort to run from that to use the configuration from a file from that directory which we had created new.

So, because of this what we are doing is, initially we are trying to create many of the directories. So, here it is we are creating a snort directory. So, since we have already created it for you. It will say the directory already exists, but then we will see that all these directories could be created and have been created before. See you need not use if you are already in the administrator mode you need not use sudo every time. So, let us now try to go ahead and see whether all these files have been created yes we have created pre-processing rules, directory has been created then see you see in this case that we have created both the rules and we have just blogged it saying that rules and pre proc rules. The reason why we are created already is as I told you it will take lot of time. So, you are your we are actually reducing the time spent on getting this configuration up and running.

So, in your case you have to execute all the step that is given on the left hand side of your screen in the word document. So, that is why we are given you all the commands. So, you can try those commands one by one and you have to create directories for white list, for black list and then something on local rules ok. So, let us go through this process quickly. So, let us see whether we have got our other directories created.

(Refer Slide Time: 03:40)



So, we look into the var directory and we see that there is a snort that is created, then we will go and see whether we have created snort dynamic rules and then we will also look at the white list rules and the black list rules.

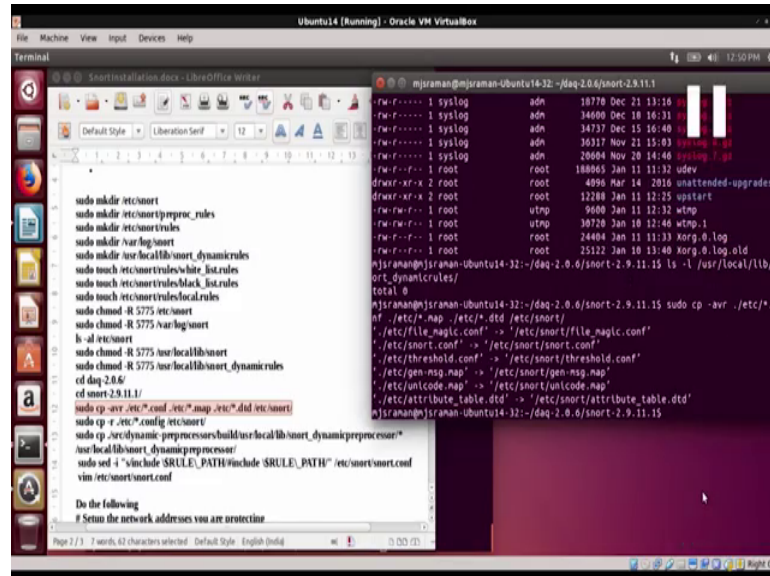
So here we see that this directory is also created, and then we look at white lists black list and so, if you have created almost all these things. So, this is no fun I mean those who are taken the previous sessions on unix will know how to do all these operations; and once you have done this ok. So, what we will have to do is we have to ensure that the file permissions are correct ok. So, that is what exactly you see from this sudo chmod minus Rc all these things should have the sticky bit ok. So, we have to chain the file mode 775. So, read write x read write x and then read only kind of files.

So, you have to create all these files and then what you do is then go to this the place where snort is installed. So, in our case we have installed snort within daq ok. So, if you had installed it separately it's you can go to this and then you take all the default configuration files that are there in snort, and then copy it into your directory from where you are going to work. So, that is exactly what we are doing. So, what we are doing is we are copying all the star dot corner files you star dot map files, star dot dtd files and copying it into etc slash snort.

So we will be doing the same thing for star dot conf files also. So, because this if I put the line will be too long. So, I just split it into 2 commands; so these 2 commands. So, let

us now copy those files. See I will also made a small error in the sense that previously, I had the something which I had configured.

(Refer Slide Time: 05:41)



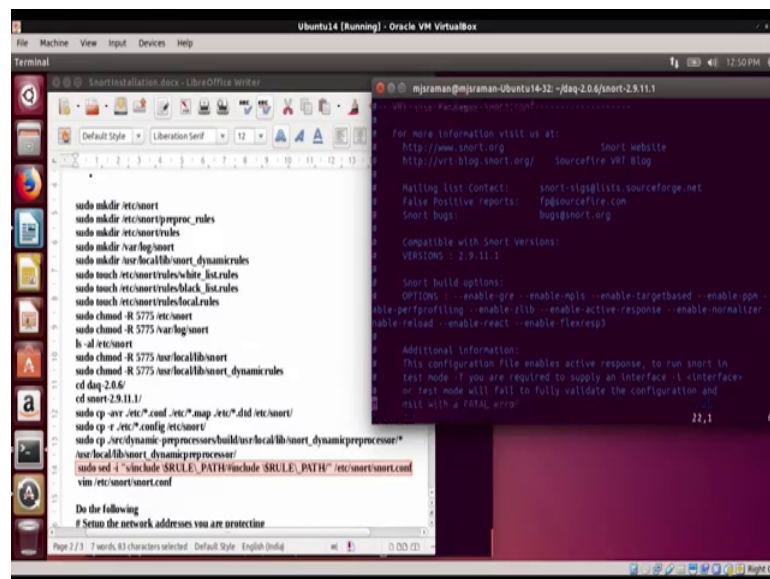
Now, what I have done is I have overwritten all the configuration, which essentially means my whatever I had tried to do a demo in the previous this thing which I tested now this whole configuration is lost, now these are some things that could happen to you also. So, then finally, if we found out that when he was executing one of these commands I mean I was seeing that the configuration file was not correct, and then I had to correct the configuration file and then get it working.

So, these type of bugs will also happen. So, here is what I have done, I would just over written whatever I was working for me and so, when I was testing it. So, before I started this course I had to test all this. So, now, it was working for me. So, what I do after this is. So, this is the part this part I mean what would this is a single command. So, if you look at this sudo cp is a single command. So, essentially I am trying to move the user local libs not dynamic pre-processor there.

Now this sudo is said what it tries to do is, I am trying to mask off all the rules because the more the rules the slower the snort is going to be. So, what I am trying to do is, I am trying initially I use this said script to mask off all the rules of snort and then only open up those rules which I want to do ok.

So, I will open up only the local dot rules, there are other rules for filtering the packets ok. So, all those files are there I do not want to include any of those files because this is just a demonstration in practice you would be opening up all those files also. So, what I do is in one shot in the configuration files dot conf I am just masking off all the rule file, and this since I thought I had already done it ok. Now I overwritten this snort dot conf I will show you that those files still have those rules ok. So, let us take a look at it sno[rt]-snort dot conf file.

(Refer Slide Time: 07:38)

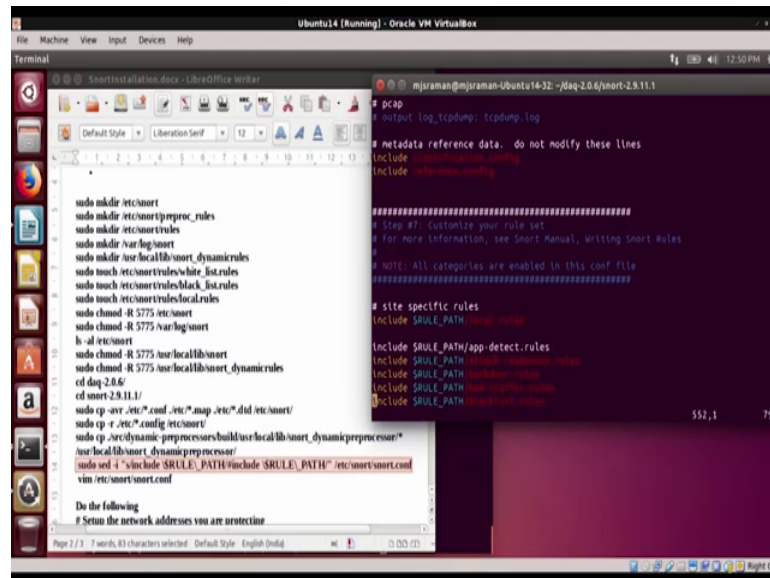


```
sudo mkdir /etc/snort
sudo mkdir /etc/snort/preproc_rules
sudo mkdir /etc/snort/rules
sudo mkdir /var/log/snort
sudo mkdir /usr/local/lib/snort_dynamicrules
sudo touch /etc/snort/rules/white_list.rules
sudo touch /etc/snort/rules/black_list.rules
sudo touch /etc/snort/rules/local.rules
sudo chmod -R 5775 /etc/snort
sudo chmod -R 5775 /var/log/snort
h -al /etc/snort
sudo chmod -R 5775 /usr/local/lib/snort
sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
cd /opt/daq-2.8.6/
cd snort-2.9.11.1/
sudo cp -avr ./etc/*.conf ./etc/*.map ./etc/*.dtd /etc/snort/
sudo cp -r ./etc/*.conf /etc/snort/
sudo cp ./etc/dynamic_preprocessors/build/usr/local/lib/snort_dynamicpreprocessor*
/usr/local/lib/snort_dynamicpreprocessor/
sudo sed -i 's/include SRULE_PATH/include SRULE_PATH' /etc/snort/snort.conf
vim /etc/snort/snort.conf

Do the following
# Setup the network addresses you are protecting
```

So, let us move down and if you look at include ok. So, this we have to include. So, here it is.

(Refer Slide Time: 07:47)



```
sudo mkdir /etc/snort
sudo mkdir /etc/snort/processor_rules
sudo mkdir /etc/snort/rules
sudo mkdir /var/log/snort
sudo mkdir /usr/local/lib/snort_dynamicrules
sudo touch /etc/snort/rules/white_list.rules
sudo touch /etc/snort/rules/black_list.rules
sudo touch /etc/snort/rules/local.rules
sudo chmod -R 5775 /etc/snort
sudo chmod -R 5775 /var/log/snort
h -al /etc/snort
sudo chmod -R 5775 /usr/local/lib/snort
sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
cd /usr/src/snort-2.9.11.1/
sudo cp -avr /etc/.conf /etc/.map /etc/.dtd /etc/snort/
sudo cp -r /etc/.conf /etc/snort/
sudo cp -r /usr/local/lib/snort_dynamicrules/build /usr/local/lib/snort_dynamicrules/processor/
sudo sed -i 's/include $RULE_PATH/include $RULE_PATH"/etc/snort/snort.conf
vim /etc/snort/snort.conf

# metadata reference data, do not modify these lines
include /etc/snort/snort.conf
include /etc/snort/snort.conf

#####
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
#####

# site specific rules
include $RULE_PATH/processor.rules
include $RULE_PATH/app/detect.rules
include $RULE_PATH/etohack/etohack.rules
include $RULE_PATH/trackback.rules
include $RULE_PATH/icmp/icmp.rules
include $RULE_PATH/snort/ast.rules
```

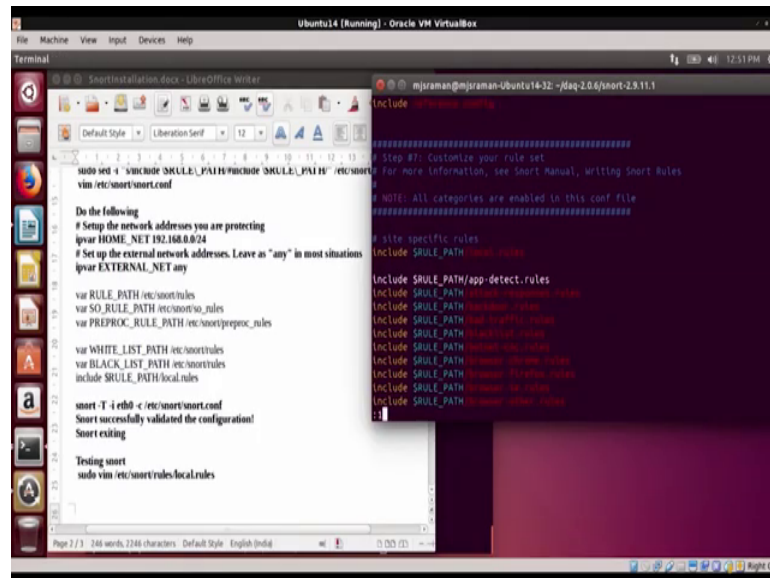
So, if you look at this my idea was to mask all these rules except the local rules ok.

So, because the local rule is one which I wanted to create, but unfortunately I had previously I had done it, now I had actually overwritten the file and because I overwritten the file I still have not executed this command, because I have not executed command all these files are still included in snort by default. So, later I will just run this script and then show that these files have been excluded by putting a hash in front of it. So, anyway let us.

So, this is how the site rules are there specified in snort. So, we will see all the rules. Now all these rules are enabled right now which we do not want because its going to slow down your system you have different kinds of policies. So, you can just see how many types of rules can be specified you can also you dynamic rules ok.

So, this is a part of the snorts configuration file now we will have to edit this file ok. So, we will have to edit the file to set up something like our network address and then what are all the stuff. So, what we will do is, this local dot rules is the one file we will add before we start snort ok. So, before we go to add this local dot rules file ok.

(Refer Slide Time: 09:06)



```
sudo sed -i 's/include $RULE_PATH/include $RULE_PATH/' /etc/snort/snort.conf
vim /etc/snort/snort.conf

Do the following
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.0/24
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
include $RULE_PATH/local.rules

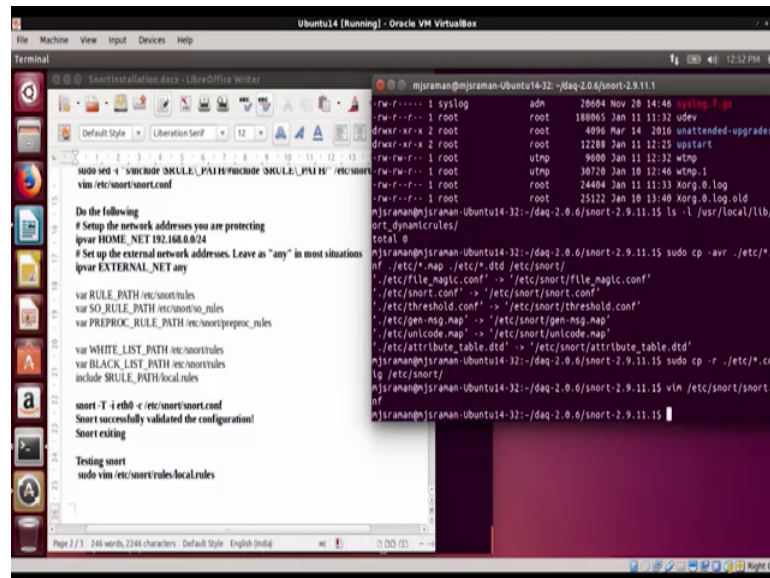
smart -t -i echo < /etc/snort/snort.conf
Smart successfully validated the configuration!
Smart exiting

Testing smart
sudo vim /etc/snort/rules/local.rules
```

What we will do is we will just and this is local dot rules that we are supposed to add ok. So, what we will do is, we will come out of this we will search for say for example, here. So, one of the configuration changes, we have to make in snort dot conf is this.

So, currently you see that ip were variable of a home net is it says any net. So, set up the network address you are protecting. So, for me in my local machine I have this network address 192.168.0.0 bar 24 that is to the mask is 255.255.255.0. So, that I have set it as 24. So, this is my local net which I want to protect. So, I will change this home net in this snort dot com file. So, I will change it to 192.168 dot actually my machines ip address is 192.168.0 dot I think its 5 or 6 one of this because the attacking machine I kept it as 5 and this is 6 I think.

(Refer Slide Time: 10:07)



```
Ubuntu14 [Running] - Oracle VM VirtualBox
Terminal
SmartInstallation.docx - LibreOffice Writer
mjsraman@mjsraman-Ubuntu14-32:~/daq-2.0.6/snort-2.9.11.1
~/fw-r----- 1 syslog      adm      26684 Nov 20 14:46 syslog.7.gz
~/fw-r----- 1 root         root     188865 Jan 11 11:32 udev
~/fw-r-xr-x  2 root         root     4096 Mar 14 2016 unattended-upgrades
~/fw-r-xr-x  2 root         root     12218 Jan 11 12:23 upstart
~/fw-rw-r--  1 root         utmp     9608 Jan 11 12:32 wtmp
~/fw-rw-r--  1 root         utmp     38720 Jan 10 12:46 wtmp.1
~/fw-rw-r--  1 root         root     24484 Jan 11 11:33 Xorg.0.log
~/fw-rw-r--  1 root         root     25122 Jan 10 13:40 Xorg.0.log.oid
mjsraman@mjsraman-Ubuntu14-32:~/daq-2.0.6/snort-2.9.11.15 ls -l /usr/local/lib/s
etc_dynamicrules/
total 0
mjsraman@mjsraman-Ubuntu14-32:~/daq-2.0.6/snort-2.9.11.15 sudo cp -avr ./etc/*
nf ./etc/*.map ./etc/*.dtd /etc/snort/
'./etc/file_magic.conf' -> '/etc/snort/file_magic.conf'
'./etc/snort.conf' -> '/etc/snort/snort.conf'
'./etc/threshold.conf' -> '/etc/snort/threshold.conf'
'./etc/gen-msg.map' -> '/etc/snort/gen-msg.map'
'./etc/unicode.map' -> '/etc/snort/unicode.map'
'./etc/attribute_table.dtd' -> '/etc/snort/attribute_table.dtd'
mjsraman@mjsraman-Ubuntu14-32:~/daq-2.0.6/snort-2.9.11.15 sudo cp -r ./etc/*
lg /etc/snort/
mjsraman@mjsraman-Ubuntu14-32:~/daq-2.0.6/snort-2.9.11.15 vim /etc/snort/snort.c
nf
mjsraman@mjsraman-Ubuntu14-32:~/daq-2.0.6/snort-2.9.11.15
```

```
sudo sed -i 's/INCLUDE SRULE_PATH/include SRULE_PATH/' /etc/snort
vim /etc/snort/snort.conf

Do the following
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.0.0/24
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
include SRULE_PATH local.rules

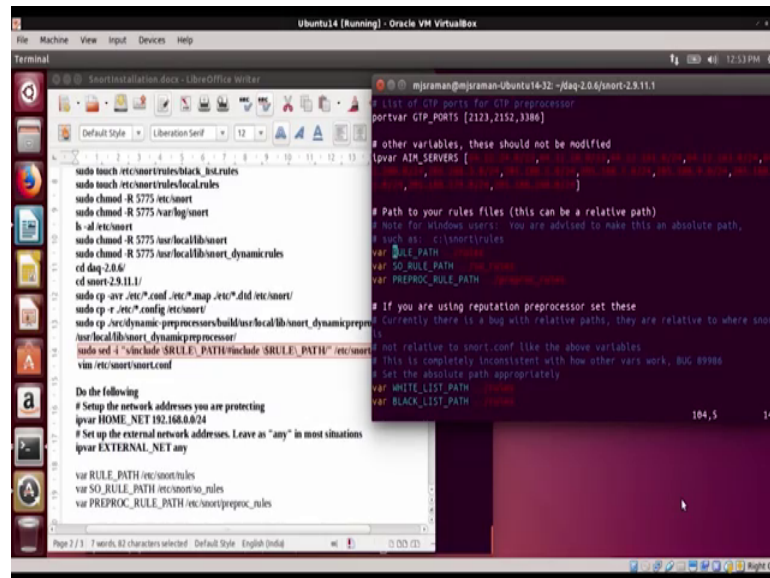
smart -T -i ethtool < /etc/snort/snort.conf
Smart successfully validated the configuration!
Smart exiting

Testing smart
sudo vim /etc/snort/rules/local.rules
```

ok. So, now, I have fixed the snort dot conf file. So, as I told you I had missed executing that set ok. So, what I will do is, I will now try to use this set ok. So, that I do not skip any step. So, this is exactly what we are telling sometimes you will skip any some steps. So, be careful. So, now, that I have vocalized-noise] executed this line you will see that all my include rules are now.

So, this is a configuration inclusion and here, they are here is a inclusion rules you see everything is mast. So, I am just removing local dot rules this means all the other rules are masked. So, I am just going to use the local drowsed rules alone for my demo then I will also set the other stuff. So, for example, external net is any that is then I will search for rule path.

(Refer Slide Time: 11:01)



```
Ubuntu14 [Running] - Oracle VM VirtualBox
Terminal
SmartInstallation.docx - LibreOffice Writer
mjrman@mjrman-Ubuntu14-32: ~/daq-2.0.6/snort-2.9.11.1
# List of GTP ports for GTP-preprocessor
portvar GTP_PORTS [2123,2152,3386]

# other variables, these should not be modified
ipvar ATM_SERVERS {
  192.168.0.100, 192.168.0.101, 192.168.0.102, 192.168.0.103, 192.168.0.104, 192.168.0.105, 192.168.0.106, 192.168.0.107, 192.168.0.108, 192.168.0.109, 192.168.0.110, 192.168.0.111, 192.168.0.112, 192.168.0.113, 192.168.0.114, 192.168.0.115, 192.168.0.116, 192.168.0.117, 192.168.0.118, 192.168.0.119, 192.168.0.120, 192.168.0.121, 192.168.0.122, 192.168.0.123, 192.168.0.124, 192.168.0.125, 192.168.0.126, 192.168.0.127, 192.168.0.128, 192.168.0.129, 192.168.0.130, 192.168.0.131, 192.168.0.132, 192.168.0.133, 192.168.0.134, 192.168.0.135, 192.168.0.136, 192.168.0.137, 192.168.0.138, 192.168.0.139, 192.168.0.140, 192.168.0.141, 192.168.0.142, 192.168.0.143, 192.168.0.144, 192.168.0.145, 192.168.0.146, 192.168.0.147, 192.168.0.148, 192.168.0.149, 192.168.0.150, 192.168.0.151, 192.168.0.152, 192.168.0.153, 192.168.0.154, 192.168.0.155, 192.168.0.156, 192.168.0.157, 192.168.0.158, 192.168.0.159, 192.168.0.160, 192.168.0.161, 192.168.0.162, 192.168.0.163, 192.168.0.164, 192.168.0.165, 192.168.0.166, 192.168.0.167, 192.168.0.168, 192.168.0.169, 192.168.0.170, 192.168.0.171, 192.168.0.172, 192.168.0.173, 192.168.0.174, 192.168.0.175, 192.168.0.176, 192.168.0.177, 192.168.0.178, 192.168.0.179, 192.168.0.180, 192.168.0.181, 192.168.0.182, 192.168.0.183, 192.168.0.184, 192.168.0.185, 192.168.0.186, 192.168.0.187, 192.168.0.188, 192.168.0.189, 192.168.0.190, 192.168.0.191, 192.168.0.192, 192.168.0.193, 192.168.0.194, 192.168.0.195, 192.168.0.196, 192.168.0.197, 192.168.0.198, 192.168.0.199, 192.168.0.200, 192.168.0.201, 192.168.0.202, 192.168.0.203, 192.168.0.204, 192.168.0.205, 192.168.0.206, 192.168.0.207, 192.168.0.208, 192.168.0.209, 192.168.0.210, 192.168.0.211, 192.168.0.212, 192.168.0.213, 192.168.0.214, 192.168.0.215, 192.168.0.216, 192.168.0.217, 192.168.0.218, 192.168.0.219, 192.168.0.220, 192.168.0.221, 192.168.0.222, 192.168.0.223, 192.168.0.224, 192.168.0.225, 192.168.0.226, 192.168.0.227, 192.168.0.228, 192.168.0.229, 192.168.0.230, 192.168.0.231, 192.168.0.232, 192.168.0.233, 192.168.0.234, 192.168.0.235, 192.168.0.236, 192.168.0.237, 192.168.0.238, 192.168.0.239, 192.168.0.240, 192.168.0.241, 192.168.0.242, 192.168.0.243, 192.168.0.244, 192.168.0.245, 192.168.0.246, 192.168.0.247, 192.168.0.248, 192.168.0.249, 192.168.0.250, 192.168.0.251, 192.168.0.252, 192.168.0.253, 192.168.0.254, 192.168.0.255}
}

# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snortrules
var RULE_PATH /etc/snortrules
var SO_RULE_PATH /etc/snort/rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort
# is installed. This is completely inconsistent with how other vars work. BUG #9986
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules

Do the following
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.0.0/24
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

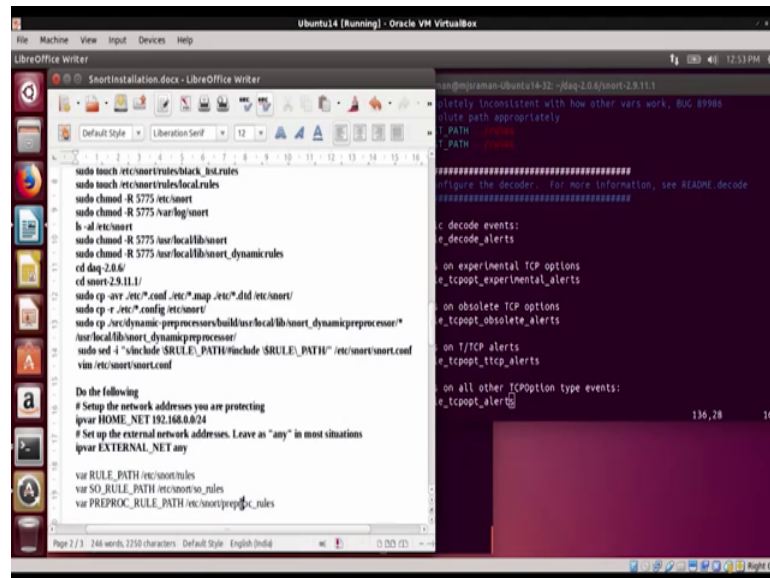
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
```

And then the rule path it says dot dot slash rules which I do not want because its a local snorts rules I want to move the rule part to etcs slash snort that rules.

So, the best way for this is please do not remove anything make a copy of the current rule path then mask the old rule path and then include the new rule path. Otherwise you will not know what an in fact, it will be a better option for you even to write a command saying that look I have changed these paths ok.

So, here we are. So, we have mask the previous three lines and then we are adding the new lines to configure the snort. So, etc snort rules and then etc snort s o rules and all those things dynamic rules, pre-processing rules, all these things we will change one by one here we are change the dynamic rules, then we are changing those pre-processing rules.

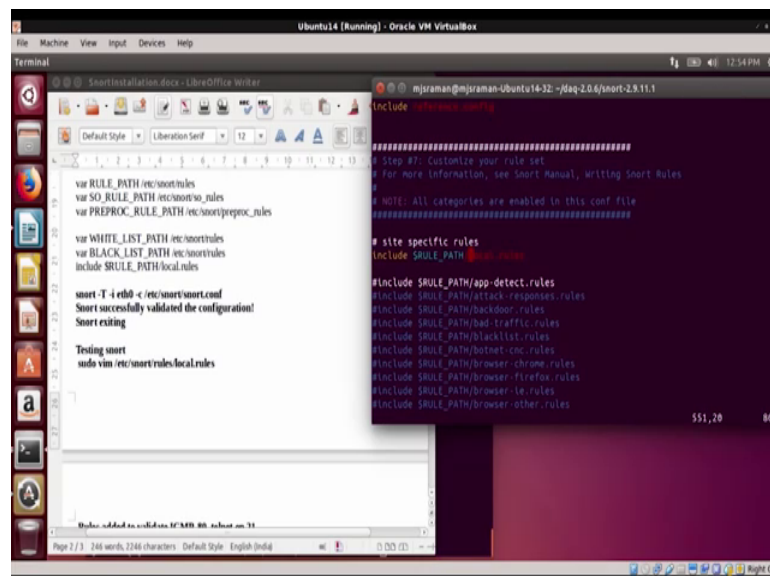
(Refer Slide Time: 11:54)



And we will go ahead and take a look at the other rules also for example, black list white list and all that. So, here we will go and change the black list because we have copied this black list to a new directory in etc snort rules. So, it's changed those black lists and white list path also, similarly make a copy then comment out the old stuff and then create the new path ok.

So, once you create the new path, then what we should do is after you create the new path I think what we should do now is to test whether you are able to ok. So, here it is.

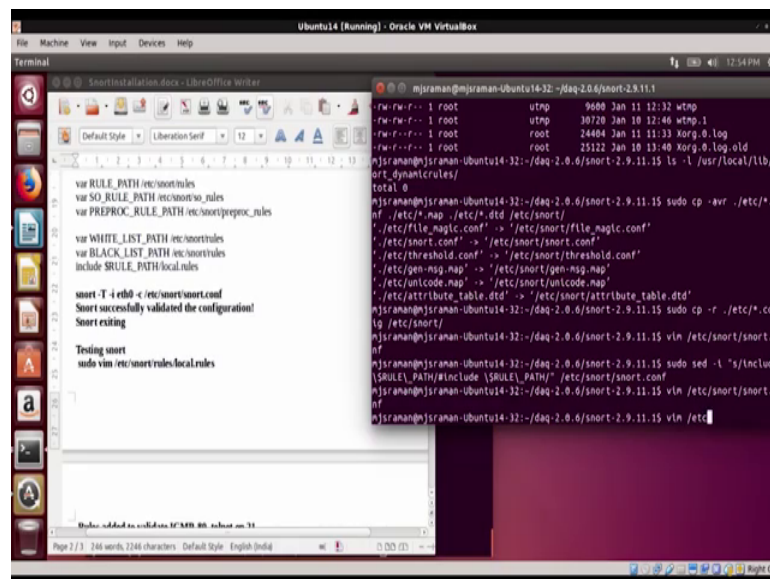
(Refer Slide Time: 12:36)



So, now we have now setup the configuration file there are 2 things that we should know. One you have to test whether the configuration file is correct. So, for that you can just before you go and edit this local dot rules file, you can now close this file and then execute this command. So, its snort, minus t minus i eth 0 or one depending on which interface you want to monitor minus c that is the configuration file, now if your configuration file is correct and it does not have any syntax error you will get a message like this, we will see that we will demo it and we will see that it will just snort successfully validate the configuration.

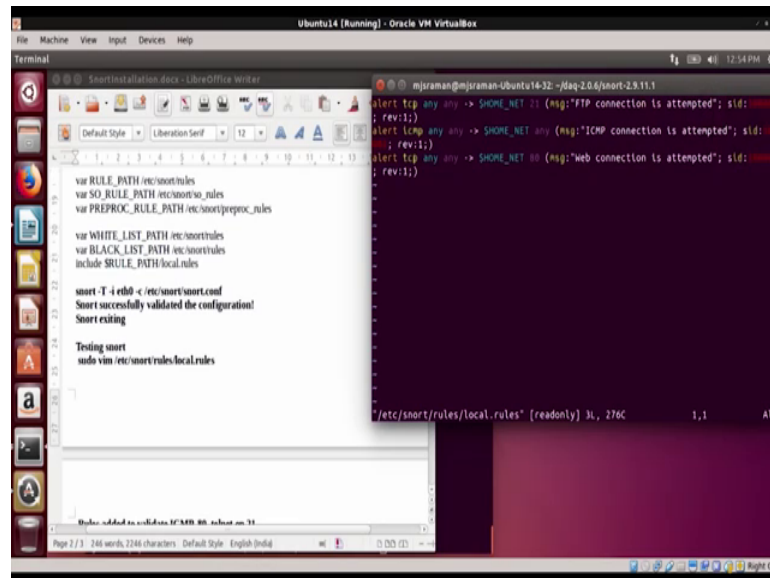
Now, only after you validate successfully the configuration you go and add the rules ok. In our case we mix it because we already done it. So, it works so, but in your case always validates this configuration file before you type the rules. So, let us go head and see whether we can. So, we will just close this ok.

(Refer Slide Time: 13:36)



And then we will edit the rules file. So, you will have to type the rules file ok. So, let us go to rules and then local dot rules and here is what we had done in our theory session.

(Refer Slide Time: 13:50)



```
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
include $RULE_PATH local.rules

snort -T -i eth0 -c /etc/snort/snort.conf
Snort successfully validated the configuration!
Snort exiting

Testing snort
sudo vim /etc/snort/rules/local.rules
```

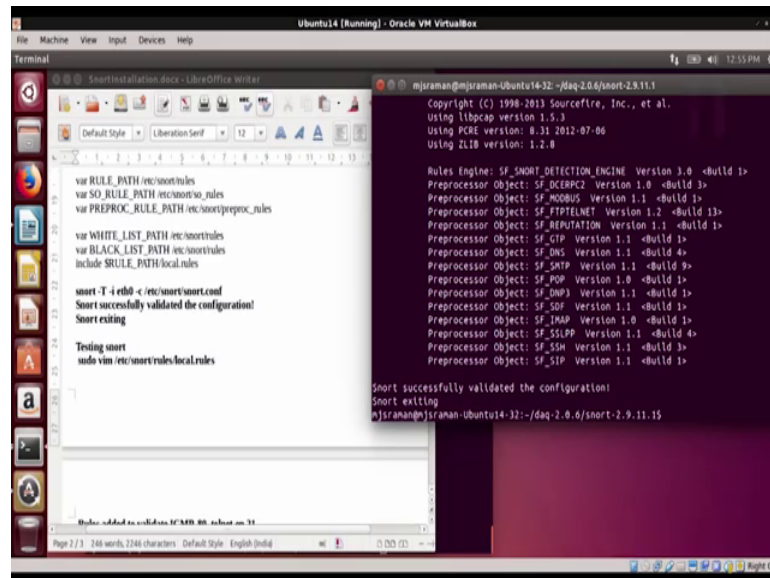
```
alert tcp any any -> $HOME_NET 21 (msg:"FTP connection is attempted"; sid:1000000; rev:1);
alert icmp any any -> $HOME_NET any (msg:"ICMP connection is attempted"; sid:1000001; rev:1);
alert tcp any any -> $HOME_NET 80 (msg:"Web connection is attempted"; sid:1000002; rev:1);
```

Page 2 / 3 246 words, 2246 characters Default Style English India

So, here we say we have got three rules ok. Now please again note that before you edit the rules files please check the configuration using the previous command snort minus t minus i e t a 0. Now this eth 0 should match the interface address that you had given in the in the first home net ok. So, please be careful about it and here you have the first line says that alert on any tcp connection, if its a if you if someone tries to access port number 21 say that fg ftp connection is attempted, then if someone tries to do a ping or icmp probe or just say that icmp connection is attempted and then the third one says that if there is someone looks into your 80 then check whether web connection is attempted.

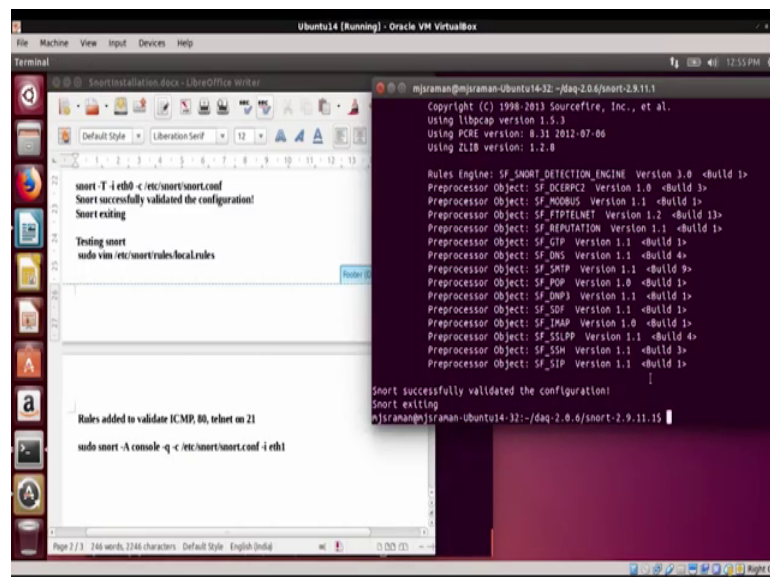
So, these three rules we just have you can write more rules. So, let us. So, this is just a read only file. So, I mean we mandatorily made it read only right now. So, then what we do is, we now go head and then verify the configuration. I told you that we will be verifying the configuration remember in our case it is Ethernet 1 even though that cut and paste says Ethernet 0 we are monitoring the Ethernet 1 interface and then I am trying to validate the configuration file you see that this says snort successfully validate the configuration and snort is exiting.

(Refer Slide Time: 15:14)



So, now that we have done it ok. So, now, that we also added the rules now remember all these things will take a lot of time do not make error its rules syntax and all that. So, once it is done ok. So, we will now run snort ok.

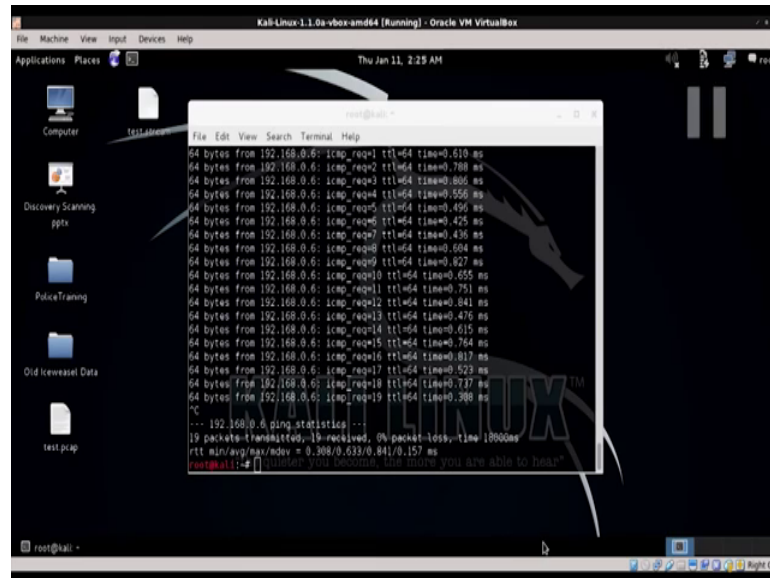
(Refer Slide Time: 15:33)



So, will now run snort. So, we will type the command snort. So, I run it in route mode minus a console, which means what it says is that please log the messages on the console and then it says minus q minus c, c is the configuration file and then it says minus i which is the interface you want to monitor and then leave it as it is that is it.

Now, you have snort is configured to follow those three rules that we had seen earlier ok. So, now, what I do is what I do is, I have a kali Linux in another virtual machine and I have connected this kali Linux along with this ubuntu. So, here is the kali Linux.

(Refer Slide Time: 16:21)

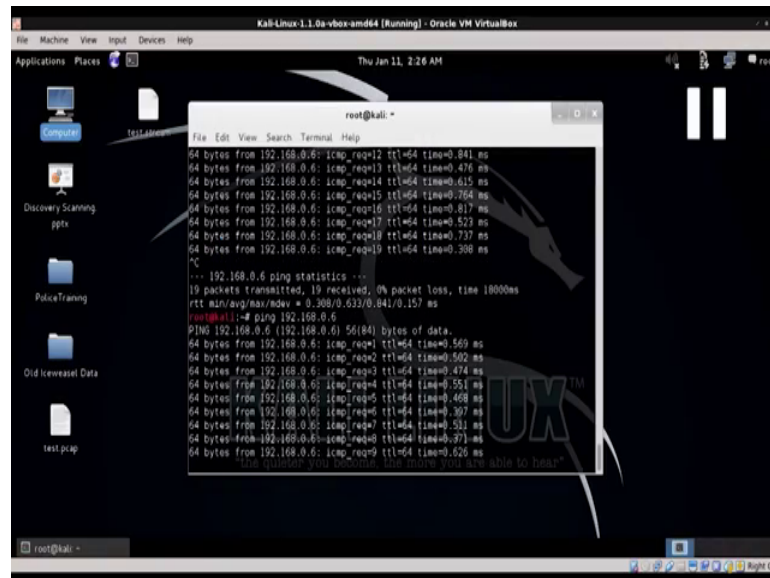


```
root@kali:~# ping -q 192.168.0.6
64 bytes from 192.168.0.6: icmp_req=1 ttl=64 time=0.610 ms
64 bytes from 192.168.0.6: icmp_req=2 ttl=64 time=0.788 ms
64 bytes from 192.168.0.6: icmp_req=3 ttl=64 time=0.806 ms
64 bytes from 192.168.0.6: icmp_req=4 ttl=64 time=0.556 ms
64 bytes from 192.168.0.6: icmp_req=5 ttl=64 time=0.496 ms
64 bytes from 192.168.0.6: icmp_req=6 ttl=64 time=0.425 ms
64 bytes from 192.168.0.6: icmp_req=7 ttl=64 time=0.436 ms
64 bytes from 192.168.0.6: icmp_req=8 ttl=64 time=0.664 ms
64 bytes from 192.168.0.6: icmp_req=9 ttl=64 time=0.927 ms
64 bytes from 192.168.0.6: icmp_req=10 ttl=64 time=0.655 ms
64 bytes from 192.168.0.6: icmp_req=11 ttl=64 time=0.751 ms
64 bytes from 192.168.0.6: icmp_req=12 ttl=64 time=0.641 ms
64 bytes from 192.168.0.6: icmp_req=13 ttl=64 time=0.476 ms
64 bytes from 192.168.0.6: icmp_req=14 ttl=64 time=0.415 ms
64 bytes from 192.168.0.6: icmp_req=15 ttl=64 time=0.764 ms
64 bytes from 192.168.0.6: icmp_req=16 ttl=64 time=0.817 ms
64 bytes from 192.168.0.6: icmp_req=17 ttl=64 time=0.523 ms
64 bytes from 192.168.0.6: icmp_req=18 ttl=64 time=0.717 ms
64 bytes from 192.168.0.6: icmp_req=19 ttl=64 time=0.398 ms
PC
--- 192.168.0.6 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 1900ms
rtt min/avg/max/mdev = 0.308/0.633/0.841/0.157 ms
root@kali:~#
```

So, here is what I have done. So, this kali Linux is we have this 192 168. So, what I do is now this kali Linux will try to ping the other machine that is the machine where we are configured snort ok. So, now, I try to ping it. So, it says the, it receives the ping. So, let us now go back to the snort configuration and you see that the snort starts printing the log message saying that icmp connection is attempted ok. So, that you remember giving the minus q option for capturing the log. So, this minus q is called the quiet option it does not print lot of headers and all that because I want only these logs along to be to be given to me.

So, if you see this, this guy goes ahead and then starts showing the atoms of the ping.

(Refer Slide Time: 17:16)



And in this way ok. So, we have been able to detect that someone has been trying to ping our network and alert has been sent. Now life is much more complicated, but this is just a demo session hope you are able to follow step by step, even though we had run it through it very fast I think from your point of view, this whole step we believe should take somewhere between 1 to 2 hours if there are no errors, and if there are errors its from 2 hours it could be any time ok.

So, try this out and probably you could also look at putting more complicated rules and then see whether this stuff works ok. Now your configuration all set up now you have to put the rules at the appropriate place, you have to enable certain rules which we have masked in the snort dot conf file you might have to modify certain rules. So, just go through each one of these files whenever you have a time, and then learn more about intrusion detection and how we can prevent it.

Thank you very much.