

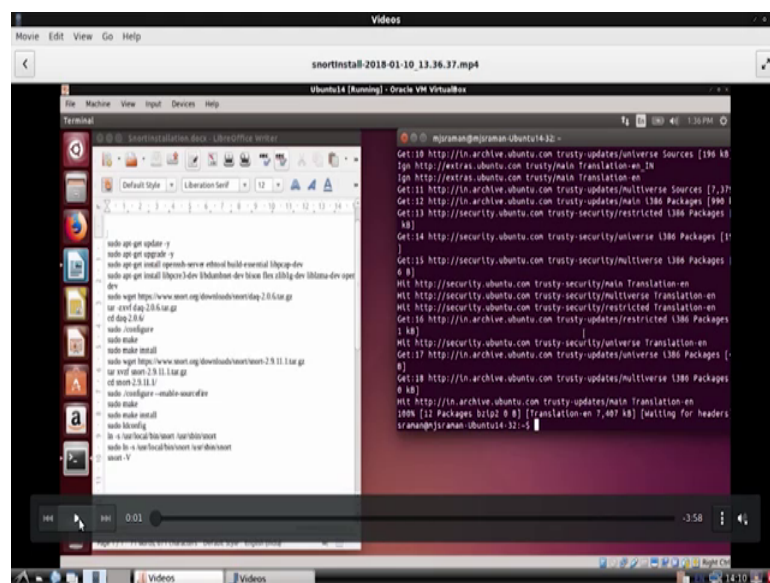
Information security - IV
Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 50
SNORT Rules

[FL] welcome to this session on network security and forensics. Until now we have been doing a lot of talking about intrusion detection system, intrusion prevention system etcetera. What we will do in this session is we will install the well known intrusion detection system the snort. Since the live installation process is going to take quite an amount of time depending on the connection speed and other things, what we will do is that, we will go ahead and install and we will go head and install it offline and we will actually record that session and play to you.

So, in that way even though the recording will be for about 5 to 10 minutes, what will happen is that in your case for example, if you get everything correct and your internet speed is quite good, you should be able to complete it within maximum of about half an hour what we have done in our case is, we have installed a virtual machine on top of our Linux box and then inside that virtual machine we are going to install snort ok.

(Refer Slide Time: 01:31)



If you just look at the screen right now, you can see that on the left hand side of this we have given a bunch of commands and these are all the commands, you can execute to

install snort in your machine. Now will go through these commands one by one and on the right hand side this is where our command execution will take place. Since we had already installed it before actually this will I mean complete very quickly, but then in a real time you will take about 5 minutes around for each of the step approximately, I mean not all the step will take 5 minutes you should be taking about half an hour for installing snort. Now we will go through why we want to do this why do we want to do this? We want to do this to show you that as a forensic expert you should be able to install tools and work with those tools.

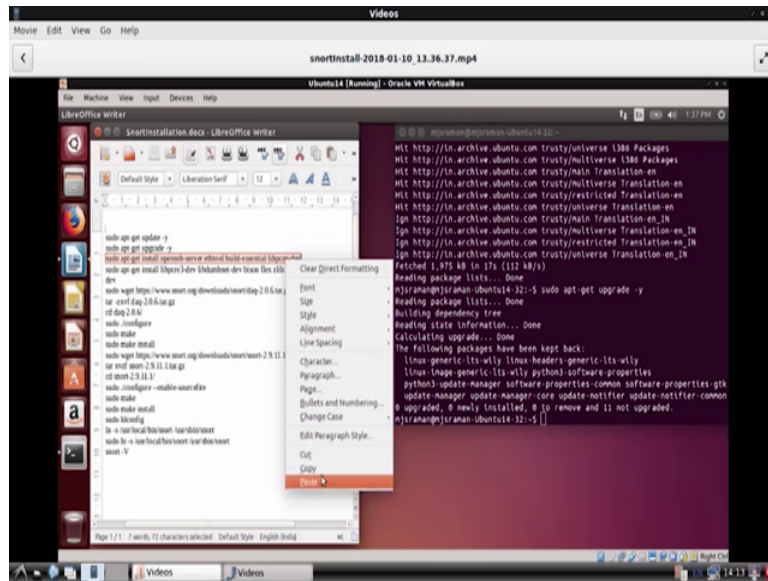
So, So, what will do is will just start off with the installation process, the first two lines of the installation process are the first two commands that we are going to execute is general before you install or update any of your Ubuntu machine. Now please remember the commands could be slightly different for other flavors of Linux therefore, we would request that you have a Ubuntu flavor running on a virtual box if you have kali Linux probably the commands would be slightly different, if it is not already installed ok.

So, let us start with the installation process. So, first will have to update our os and this will go something like this, once you in give a sudo update it will go and update the repositories and in the next step it will upgrade to the latest version of the files. So, let us cut and paste it. So, since it is a video recording I mean will cut and paste it, and then let this be over.

So, once this is done will cut and paste this upgrade process. So, in the upgrade. So, then see in your case for example, we in our case for example, it is already upgraded. So, we are actually executed this before to ensure that we do not spend lot of time showing you that live installation, but in your case probably I mean you should get something like this whatever is shown the following packages are kept back or something like this and zero upgrades, zero newly. So, in our case zero upgraded and zero newly installed because I already done the upgrade and attempting it again

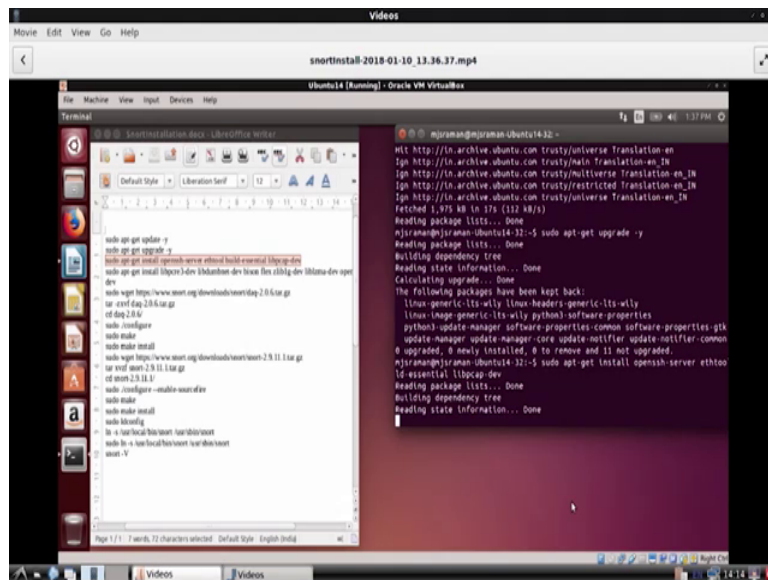
But in your case probably I mean it will say this many packages are have been upgraded and this many packages have being installed. Now before since we are going to get the source code and compile what we are going to do is, we are going to install the appropriate libraries that are needed for compiling the source code of snort ok.

(Refer Slide Time: 04:40)



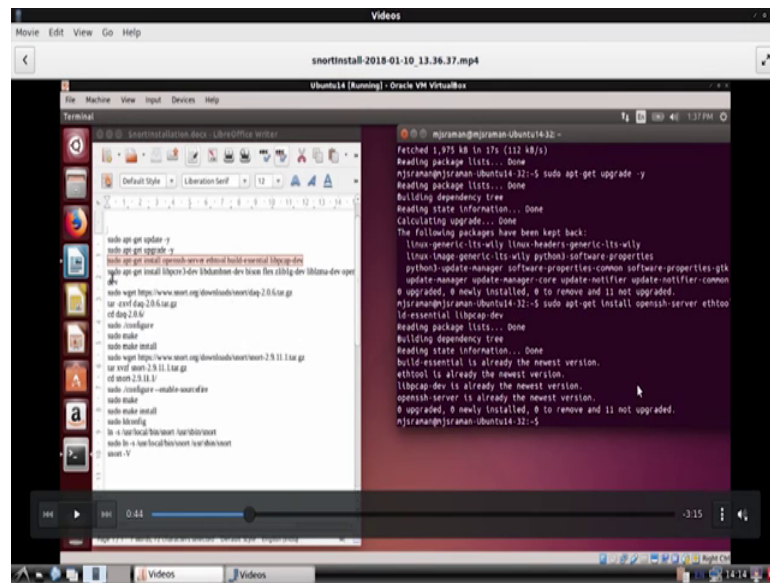
So, So, we are going to have bunch of libraries, this is the first set of libraries we are going to compile ok.

(Refer Slide Time: 04:47)



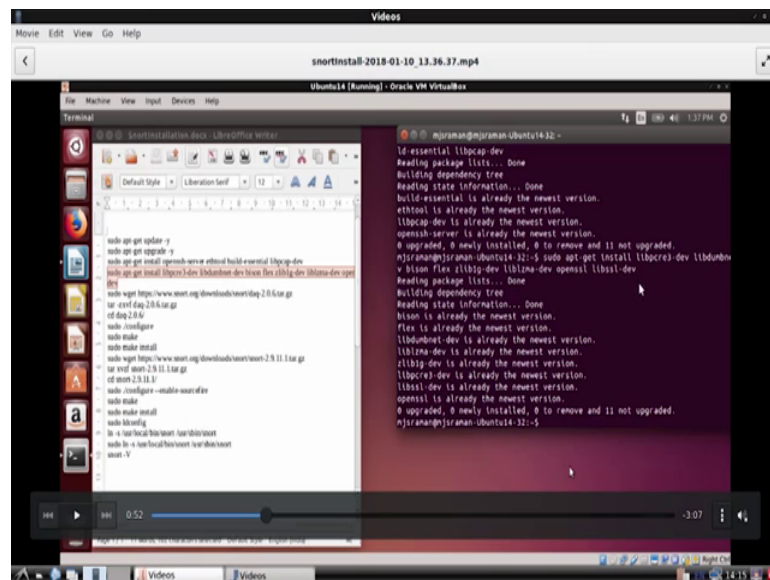
So, one of the things you should note is that you could actually I mean I have just spilt it into two parts this is the first part first set of libraries that I am installing, I am installing openssh server, ethtool and then libpcap etcetera and then we also have the next set of libraries. So, here is a next set of libraries you have to install bison flex these are parsers and things like that ok.

(Refer Slide Time: 05:16)



So, in our case as I told you I mean the installation is complete, because we have already installed all these packages. So, we get out very quickly, but probably in your case you might take a quite an amount of time to install these libraries, because these libraries have to be downloaded from the repository and then installed in your machine. So, here is an next set of libraries that we are installing. So, in order to quicken the process I am cutting and pasting the command.

(Refer Slide Time: 05:45)



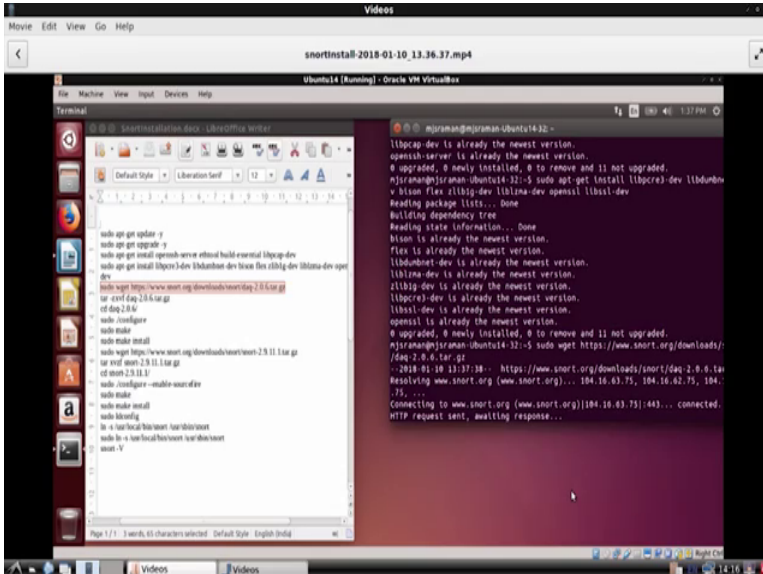
And so, here is the next set of libraries now please note down the names of these libraries I mean if you make a mistake in one of the library it may not get installed and you know all these all these logs might move off very quickly and you might miss installing one of these libraries. And there could be lot of problem once you miss some libraries. I mean when you compile the program, there would be compilation error then you will go into bunch of loops.

So, please ensure that there is no mistake in any of the steps the other thing that I have seen with many of the engineers is that, if some steps shows an error then people will leave that step and go to the next step. Please understand that in computer science every step has to be followed during installation process meticulously.

You its not a probability the machine does not work on probability and it cannot make a guess that such libraries may be made available or would be available etc, you have to make these libraries available therefore, do not skip any step ok. Please install I hope you know the shell command to show whether the previous command has being successful. So, use those kinds of commands and get the installation correct so.

The next item that we are going to do is we are going to actually get the daq libraries just part of snort and see one of the things that you should know about this step is currently it is using the version 2.0.6. Now you can see this 2.0.6 in your snort website ok.

(Refer Slide Time: 07:13)



```
mijsraman@mijsraman-ubuntu14:32~$ sudo apt-get update
mijsraman@mijsraman-ubuntu14:32~$ sudo apt-get install libpcap-dev
mijsraman@mijsraman-ubuntu14:32~$ sudo apt-get install libltdl-dev
mijsraman@mijsraman-ubuntu14:32~$ sudo wget https://www.snort.org/downloads/snort-2.9.8.tar.gz
mijsraman@mijsraman-ubuntu14:32~$ tar -zxvf snort-2.9.8.tar.gz
mijsraman@mijsraman-ubuntu14:32~$ cd snort-2.9.8
mijsraman@mijsraman-ubuntu14:32~/snort-2.9.8$ ls
mijsraman@mijsraman-ubuntu14:32~/snort-2.9.8$ ./configure
mijsraman@mijsraman-ubuntu14:32~/snort-2.9.8$ make
```

Now, see if for example, if this course is two or three months later if you go through the same course and you watch this video now this version would have changed. So, be careful about the version number.

(Refer Slide Time: 07:26)

The screenshot shows a terminal window within a virtual machine. The terminal displays the following commands and output:

```

sudo apt-get update &
sudo apt-get upgrade &
sudo apt-get install openssl-securelib build-essential libcap-dev
sudo apt-get install libopen3dev libklibdev libvnc-dev liblxde-dev open
dev
sudo wget https://www.sns.org/dm/ubuntus/instapq.2.0.6.tar.gz
tar -zxvf 2.0.6.tar.gz
sudo mkdir
sudo mkdir install
sudo wget https://www.sns.org/dm/ubuntus/inst/inst-2.0.11.tar.gz
tar -zxvf inst-2.0.11.tar.gz
cd inst-2.0.11.0
sudo ./install --make --source-dir
sudo make
sudo make install
sudo ./bin/qsig
in a /usr/local/bin/inst-usr/bin/inst
sudo ln -s /usr/local/bin/inst-usr/bin/inst
inst -Y
  
```

The terminal output on the right shows:

```

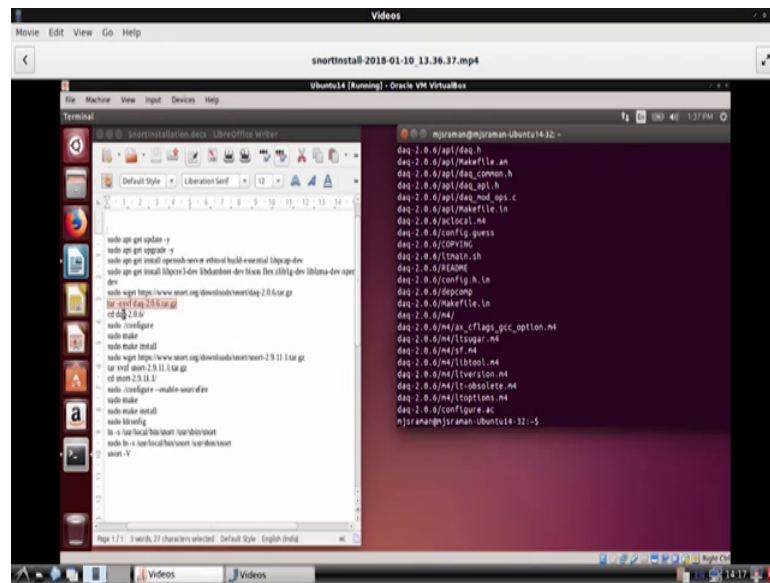
HTTP request sent, awaiting response... 302 Found
Location: https://snot-org-site.s3.amazonaws.com/production/release_files/
/000/000/073/original/daq.2.0.6.tar.gz?AWS-Algorithm=SHA256&AW
s-Credential=AKIAIACED2SPM5CTGANZ72018010R2FUS-EAST-132F332F&aws-reque
st&X-At:201801101807412&X-Amz-Expires=3600&X-Amz-SignedHeader=sns&X-Amz-Sign
ature=f5c49e7c52f94c9e3780b5ac3e383ade67c721a18006fc436e958
Name: Signature=f5c49e7c52f94c9e3780b5ac3e383ade67c721a18006fc436e958
Resolving snot-org-site.s3.amazonaws.com (snot-org-site.s3.amazonaws.com)
4.221.49.138
Connecting to snot-org-site.s3.amazonaws.com (snot-org-site.s3.amazonaws.c
om) [4.221.49.138]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 51803 (508K) [binary/octet-stream]
Saving to: 'daq.2.0.6.tar.gz.'

[09K]*****] 5,18,013  89.248/s  in 0.1
2018-01-10 13:37:47 (83.4 kB/s) - 'daq.2.0.6.tar.gz.' saved [51803]/51803
^Jsrangan@srangan-ubuntu14-32-5 [
  
```

So, if you look at this is 2.0.6 this is the current version number that we have got, I mean this dot one is coming because I already saved it I am trying to do it again. So, that is why this dot one is coming do not worry about. For you it will show it as daq dash some version number and dot tar dot gz has being downloaded.

So, these have to download this file and then we have to go inside this directory. So, we have to untar it. So, we will untar it.

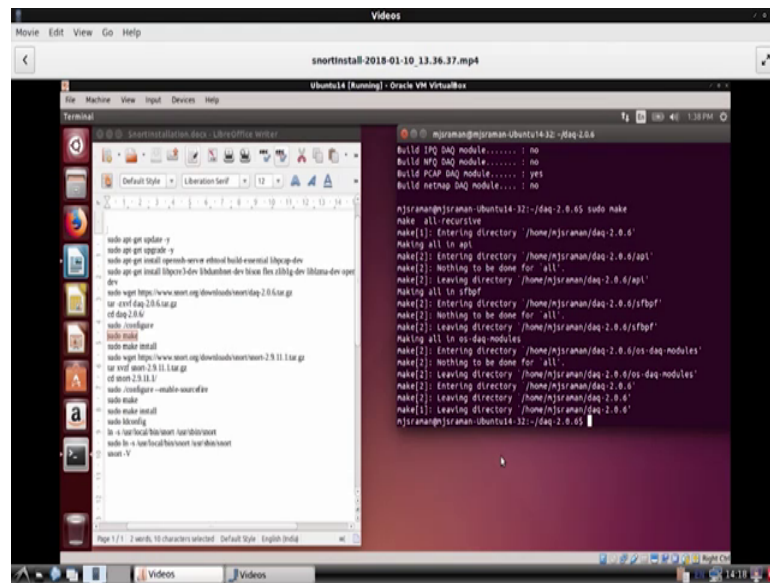
(Refer Slide Time: 08:03)



And then untaring will create this directory called daq 2.0.6, then we go inside that directory. So, once we go inside the directory then and this contains the whole source code you can take a look at source code for daq, but then what you do is you just have to configure and start do a make.

So, once you do a configure it will show you bunch of compiler option and what is the kind of compiler more or less has compiler get the environment ready for compilation of the source code. So, once it is done then we will go ahead and do a make of this. So, we will go ahead and do a make of this.

(Refer Slide Time: 08:43)



So, once see this make will take quite sometimes. So, in our case we have already done it and. So, therefore, it is over immediately. Now once you do a make and then you have to do something known as a make install; that means, you actually after you do the make the source code gets compiled, it will create bunch of libraries

Now, these libraries have to be put in some location. So, that is exactly now we are using all default location probably I mean, but I told you that putting anything in default location is bad by that is because we are just for training purposes, but in real life I would suggest that you make you use some of the configuration parameter, that are given along with this make and then install it in a different directory not in the directory which is given by default.

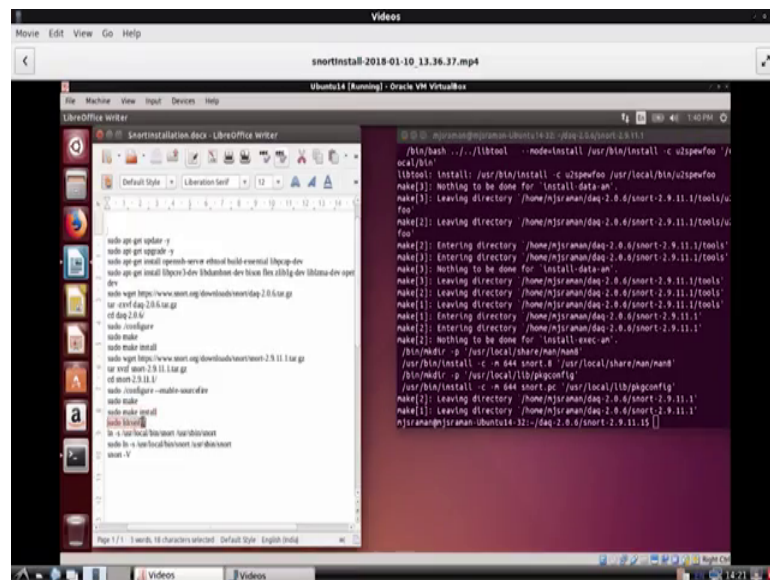
I mean sometimes what could happen is if you skip the default directory the software may not work properly and all that, but you have to fix all those problems for security purpose do not install in default directory, but since its training purposes we will go head and install it in the default directory

Now, this step actually would have taken lot of time for you, and other thing that you should know is you should have see the next step is you have to install this directories ok.

you have to get all the libraries in place configure the libraries in place, the dynamic libraries and things like that ok.

So, it will take some time I mean and. So, let us do a make and make should be over very quickly because you already made it and then we will do a make install ok. So, we will go ahead and do a make install and hopefully this should also complete and then will configure the libraries and then finally, we provide a link from user sbins snort so, that you need not add the path.

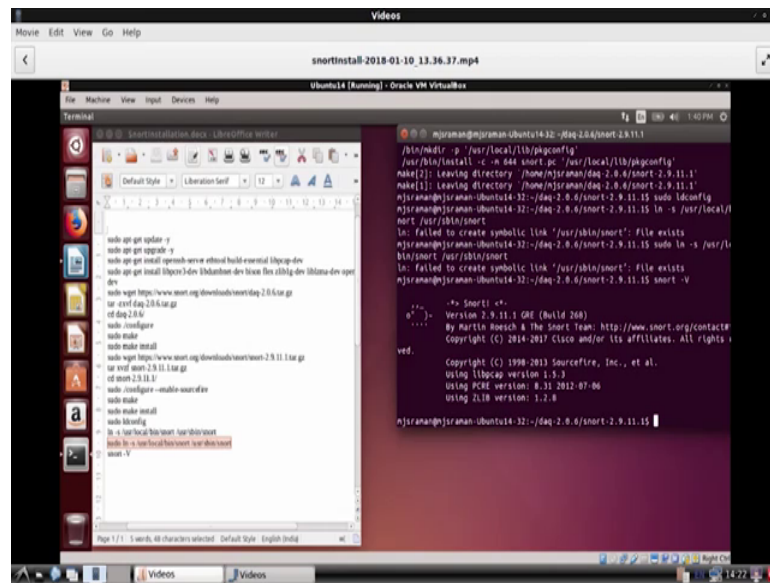
(Refer Slide Time: 12:42)



So, you just provide a link from snort. So, in this case also you might have use link minus now in our case it will say it is already available, because we already tested it. So, the file already exist.

And finally, here is the last step if you are done everything correctly hopefully then you can use this command called snort and then minus capital V.

(Refer Slide Time: 13:11)



So, you go ahead and issue this command and then it should say something like this the version 2.9.11.1 and then it has source fare and part of cisco, all these copyright messages what libpcap version it uses what zlip version uses and all that. So, if you have done this; then, you are on the safe side. You have installed it properly. What then, what should we do after this that is a next question?

So, we had seen that you have to configure snort. So, if you want to configure snort you have to get a bunch of rules for snort to work on. So, what should snort capture what should it do once it capture a package, I think we did a quite an amount of spent quite an amount of spent quite an amount of time regarding the rules of snort.

So, the next step after this is to configure the snort rules and we have to come up with certain policies, what we want to do will have to configure the snort rules based on the policy. So, these have to be written into specific directories of snort and you could have something known as a white list which means whatever you allow you could have something known as a black list, whatever you do not allow then you can have bunch of rules for filtering and all these things what we will do is will do will see that in a separate section.

So, until now you should got this correct once you got this right you have got your intrusion detection system in short and feel happy about it. So, in the next session actually, we will look at getting some snort rules and see how to make snort works.

Thank you very much.