Information security - IV

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

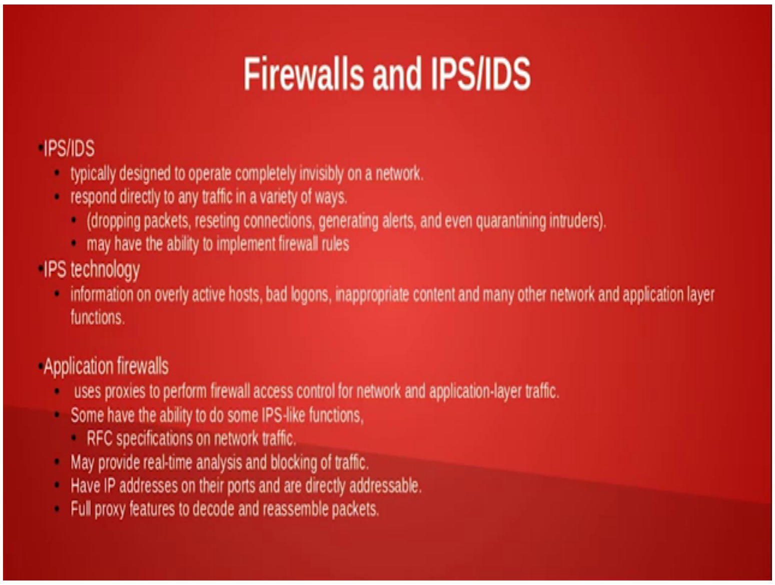
Lecture – 47
Network Security Devices – IDS

As a forensic expert, we saw that use of software tools for analysis is very useful for us. As you are able to converge on solutions or converge on what has happened on the on the attacker or crime very quickly, we saw that in case study that was given in the last session, what we will do from now on is we are going to look at some of the network intrusion detection prevention and devices such as firewalls which could be hardware or software. These kinds of products, ok, we will try to analyze them. We will try to become hands on in some of the products, we will try to understand, how they work, what is they behavior, why these tools are used all these things, we will learn in the next few sessions.

And we will also see; how these devices; some of these devices or some of these software can be configured by forensic expert to gather more data, see one of the thing is one is gathering data and analyzing ok. Until now, we have being trying to gather some kind of live data. Now, what happens see one is one part of it is if something bad has happened, you go and investigate what has bad has happened and you try to get the data out of it the other one is to protect the network itself or even if the network fails, I try to identify whether someone is trying to hack into my network.

So, in this case, you will be able to use this kind of network intrusion, detection and prevention tool, protection tools and as well as something like firewalls.

(Refer Slide Time: 01:53)



Firewalls and IPS/IDS

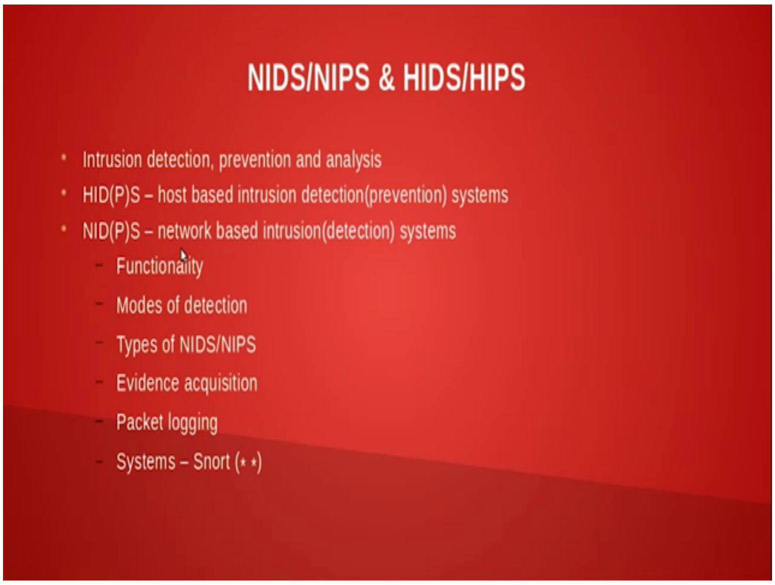
- IPS/IDS
  - typically designed to operate completely invisibly on a network.
  - respond directly to any traffic in a variety of ways.
    - (dropping packets, reseting connections, generating alerts, and even quarantining intruders).
    - may have the ability to implement firewall rules
- IPS technology
  - information on overly active hosts, bad logons, inappropriate content and many other network and application layer functions.
- Application firewalls
  - uses proxies to perform firewall access control for network and application-layer traffic.
  - Some have the ability to do some IPS-like functions,
    - RFC specifications on network traffic.
  - May provide real-time analysis and blocking of traffic.
  - Have IP addresses on their ports and are directly addressable.
  - Full proxy features to decode and reassemble packets.

So, first will look at network intrusion detection and then we will take a look at what is this intrusion detection, what is intrusion prevention, then will take briefly overview of what is the difference between firewall and IPS, IDS are both same or they different then we will probably take a look at the software we might look at the ip tables for firewalls and probably this snort for IPS and IDS and all these were see you have to become expert in actually programming these devices, ok.

So, what these software configuration do is they will have a configuration file and in that configuration file you have to write a bunch of rules ok. So, suppose you see this pattern, you have to take this action, suppose, you see this pattern you have to take this action and so on. So, you have to be familiar in writing small sort of scripts to configure these devices.

Let us start up with network intrusion detection and what is host intrusion detection ok.

(Refer Slide Time: 02:54)



NIDS/NIPS & HIDS/HIPS

- Intrusion detection, prevention and analysis
- HID(P)S – host based intrusion detection(prevention) systems
- NID(P)S – network based intrusion(detection) systems
  - Functionality
  - Modes of detection
  - Types of NIDS/NIPS
  - Evidence acquisition
  - Packet logging
  - Systems – Snort (* *)

So, the whole aim behind network security is to have intrusion detection prevention and analysis. So, if something had gone wrong we had to do some sort of analysis now there are two types of intrusion detection systems one is known as the host based intrusion detection and prevention systems known as HIDS or HIPS and then the next one is the network based intrusion detection system or network based intrusion prevention system, ok. So, we will be concentrating mostly on NIDS and NIPS, ok. The first thing is the intrusion detection, they have functionality. So, it the functionality is that it needs to identify, whether any intrusion has happened or is there any anomaly in the data that is transferring on the network that is the first thing.

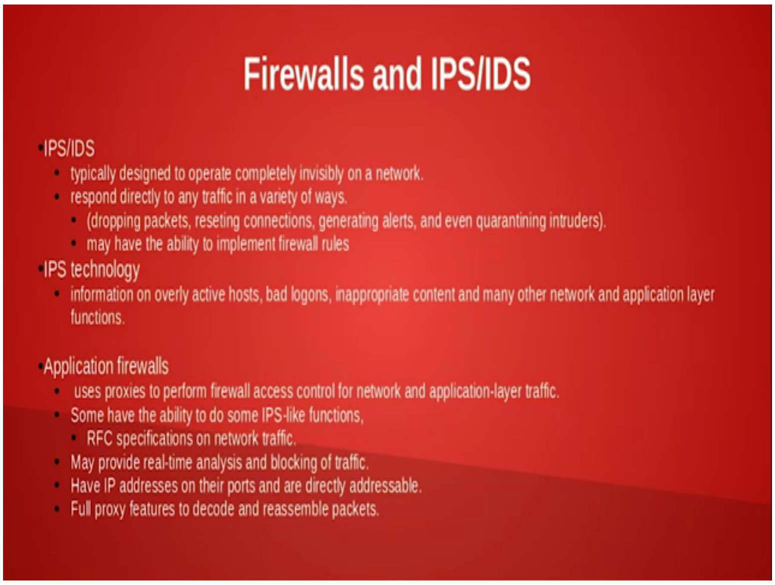
The second one is; what are the modes by which you can detect that there is an anomaly during in the network say for example, if someone trying to scan all the ports if someone is trying to scan all the ports should I send an alert and where should I send the alert ok. So, you would use you know that the attackers before the actually attack a system they do something known as reconeson so; that means, what they do is they go head and try to this is done usually by thieves before they want to steal in a house actually they look at the surroundings, they look at who are all the people there at what time, they wake up at what time they go to sleep what all these things ok. So, this is very important and if you are going to use intrusion detecting or prevention systems prevention protection systems, what you could do is you could go head and then identify this kind of pattern because if I mean hope many of you would have seen old in the old movies the villain will always be rotating his eyes and showing that he is a villain.

So, similarly you have certain mannerism that happens with this that we call it has the pattern ok. So, we would use there are many ways by which you can detect this kind of patterns whether you are trying to enter into the network for example, I mean many a time they will use something known as a honeypot. A honeypot is a system that was that is left vulnerable and you try it and when attacker comes in he will try to see this vulnerable system and then start attacking.

So, in that way you will be able to identify because you are just letting the system be taken by a person and then you are allowing him to steal a house and then once he steals you catch him. So, this is you could use this sort of methodology to catch the person also, but at the end of the day I mean you have you prevention is much better ok. So, when I use this type of network intrusion detection and prevention system, you could have, you could use commercially available systems or you could use open source. So, we will see some of the commercially available systems as well as the open source systems.

The most important part of network intrusion detection is evidence acquisition. So, essentially this be in terms of log and since these devices are made for network security, they are capable of generating logs that different levels, I mean if you could have a course grind log or you could get a fine grind log, etcetera. So, this has a very good packet logging or flow logging flow logging mechanisms and one of the ways by with which we can use systems such as not to actually do all these activities. So, we will look about not later in the session.

(Refer Slide Time: 06:28)



Firewalls and IPS/IDS

- IPS/IDS
  - typically designed to operate completely invisibly on a network.
  - respond directly to any traffic in a variety of ways.
    - (dropping packets, reseting connections, generating alerts, and even quarantining intruders).
    - may have the ability to implement firewall rules
- IPS technology
  - information on overly active hosts, bad logons, inappropriate content and many other network and application layer functions.
- Application firewalls
  - uses proxies to perform firewall access control for network and application-layer traffic.
  - Some have the ability to do some IPS-like functions,
    - RFC specifications on network traffic.
  - May provide real-time analysis and blocking of traffic.
  - Have IP addresses on their ports and are directly addressable.
  - Full proxy features to decode and reassemble packets.

Then we will now try to differentiate between firewall IPS and IDS, I mean many a times, these are of confuse with each other. So, if it is an IPS intrusion prevention intrusion detection system, it is typically designed to cooperate completely invisibly on a network. So, see for example, if I know that there is a policeman in my house 24 hours, ok, it will prevent many people from entering my house. So, similarly, if someone tells you that there is intrusion prevention or detection system there, I mean at least some people will resist to attack the system. So, that is the general psychology or some people actually be very interested if such a systems there because they want to see you whether who is intelligent, whether the person attacking is intelligent or the person who put the system is intelligent.

So, whatever may be the case and if the policeman is visible; obviously, people will not attack I mean hopefully, but if the policeman is invisible then it gives an advantage for the policeman similarly a intrusion prevention or intrusion detection system if it is invisible to the external world ok. So, for example, you could actually block ARP packets or so that if someone pings this IP address, you do not get a response ok, something like that it can be done and in order to put a mask like that one could use firewall ok.

So, for example, I do not have to send any data out of IPS or IDS to an external world. So, someone tries to do a http 80 on my IPS or IDS, I should not actually get back a response to person ok. So, I would only be sitting on the network observing the data. So, in this way when I want to apply a filter I might use a firewall ok.

The second thing is see one of the ways I can do is that suppose someone tries to attack I since it is also a intrusion prevention system ok, for example, if someone starts to do port scanning then you can configure a rules saying that any data from that ip address which is doing port scanning should be blocked and I can send this instruction to firewall and tell the firewall that please block any of these or I myself might have the capability to block this now this is where there is a confusion because there is IPS at sometimes acts as a firewall and sometimes firewalls have to prevent IPS from getting exposed. So, so it is a kind of relationship slight relationship that exists between. So, sometimes the IPS and IDS may have the ability to implement firewall rules ok.

Or the other thing is they can instruct the firewall to stop the packets. So, something like this can be done in a prevention technology in IPS actually it see IPS if someone is extra active for example, poor scanning activity is someone extra active or is someone trying to send lot packets to your machine ok, in order to suppressive your processing ability like dos attack ok.

So, a prevention system will study this and then it can it can pass information about bag logins or inappropriate content that is coming through the network or many other network and application layer function for example, movie downloads for example, if you tell an organization that do not download movies people may not really listen to you the second one is you could go head and install this or prevent movies from getting downloaded in each one of the employees pc, but that is going to be to difficult for you because if there are as a number of employees grow then you have to install more and more application and remember more the application more the vulnerabilities and more the security problems ok.

So, one way is that you could make the IPS or IPS system block downloading of movies. So, a firewall can also do this. So, once you do this you need not set it up for all the employees in the organization, you could actually just put it in one place. So, maintenance and other things becomes much more easy coming to application firewalls ok. So, uses proxys to perform firewall access control for network and application layer traffic and some of the ability to do a IPS function, I think I think, we saw that before sort of preventing access for a particular website or preventing people from downloading movies either you could do with an IPS or you can do it with a firewall so.

So, there is actually a sort of overlap there are some common functions between these two and there are functions where these two are independent and one of the things with application firewalls is see, you could actually look whether the RFC have being implemented properly ok. So, with application firewall for example, http suppose, I send a request then you should send a response and if their response as an error, whether it sends a correct error code and not the correct error code at least, it sends an error and things like that these can be checked and one of the things with firewalls is that it might provide real time analysis and blocking of traffic.

So, so, and major difference is that firewall is visible to the external world one of the things firewall can do is it can also reassemble the packets ok. So, it is it is much more capabilities than a intrusion prevention and detection system ok. So, what is the functionality of a IDS, we will now look take a look at IDS.

(Refer Slide Time: 12:03)

Functionality

- IDS's are rule based
- Issues alerts
- Configured to capture suspicious packet sequences
- Sniffing
  - Multiple layer inspection
  - Protocol awareness
  - Protocol reassembly
- In a NIPS processing time is critical
- In a NIDS offline analysis and alerting is tolerable
  - Deep packet analysis is possible
- Some sort of normalization of packet contents may be required

Then, we will later go to firewalls IDS are rule based ok. So, you detects certain pattern and then in order to prevent or detect an attack you have to use certain rules for example, do you want to block some packets do you want to redirect some packets all these things can be specified by rules ok, the rules will usually be dictated by the organizational policy ok. So, if the organizational policy says that if any employee downloads the movie block it, but download the movie to the administrator. So, that he can watch the movie you can put you can even do that ok.

So, any employee wanting to download a movie the administrator can watch the movie or he can sell that movie. So, something like this I mean such kind of things can be done, but hopefully your organization does not have such kind of policy ok. So, second one is it also. So, the policy could also be like issue an alert that this employee is spending more time on go Gmail, rather than working at working with a company's email. So, such type of alerts can be configured you could also configure or look at suspicious packets we had already seen the example of port scanning as one of the example.

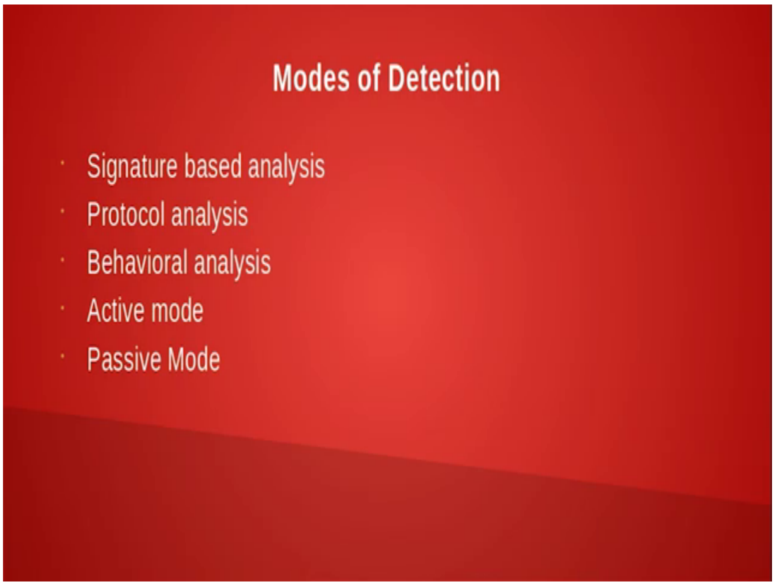
Now, other thing that IDS or IPS can do is sniffing and it can do sniffing and multilayer inspection like you know it can inspect for IP traffic or it can inspect for TCP traffic etcetera and based on IP and TCP traffic, it can take some action one of the simplest thing, I could do is I need not response for any ping suppose I do a broadcast ping, I mean if you remember the previous the case study we were looking at firewall logs and one of the firewall logs I mean if you would observed that they are trying to a broadcast from 192 168 one dot address the broadcast was 255 and the firewall actually detected that kind of broadcast someone see broadcast actually wears the bandwidth I mean if someone is interested what are the machines that are available in the local net and he will do a ping minus b and then do a broadcast and identify who are all the machines ok.

Those activities the firewall was trying to stop and it was logging it ok. So, it; so, in this way you once you sniff the packets you will be able to have protocol awareness, you can look at protocol reassembly and things like that, but most important thing is this prevention systems and detection system must be more or less real time ok. So, you I mean because the detection systems has to identify before an attacker takes over control ok, similarly a prevention system has to prevent before the attacker takes over control, which means it needs very high amount of processing power ok.

The difficulty is that see in order to do such kind of processing power you might have to go for de packet analysis de packet analysis means that you analyze the whole packet along with the flow not just the headers or the meta data which we were talking about in the past few classes now de packet analysis will provide you lot of information, but the same time, it is extremely difficult because it has to if especially, if you are running at line rate that is speed of de packet inspection should be equivalent to speed of the data packet that is sent its virtually impossible unless you have some mechanisms to do this ok.

Usually what these kinds of IDS and IPS do is that they have some sort of normalization mechanism ok, for example, only taking specific meta data or dropping some packets which are really not useful, etcetera. So, they will try to do this kind of analysis. So, this is functionality of IDS or IPS and the most important thing is it needs good performance the next point is how does IDS or IPS detect that something has gone wrong ok.

(Refer Slide Time: 16:07)



Modes of Detection

- Signature based analysis
- Protocol analysis
- Behavioral analysis
- Active mode
- Passive Mode

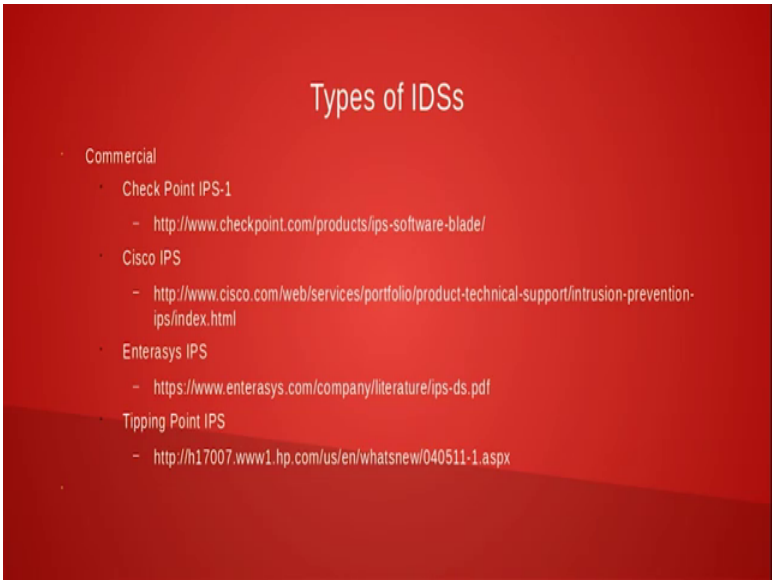
The very easy way of detection is signature based analysis ok. So, one of the things one the detection can be done either in the active mode or passive mode I think active mode is being live passive mode is being watchful and reading from some other logs and things like that ok.

But once I do the detection, I mean I can do I mean the way I can detect is from these after collecting the data is one is signature based analysis ok. So, if some organizations for example, have a criteria that you are not supposed to send any word document outside even to your private email id because document might have confidentiality requirements, etcetera ok. So, in that case what this IDS or IPS will do is that it will always monitor I mean you could do it even with firewalls, but it start monitoring the packets whether the practical or signature is available and if you remember we were looking at signatures for the word document if that is the case it actually logs this, that this and it actually tracks the header signature and the trail signature and then within that it takes the document and then puts it and then logs which person has sent. In fact, in one of the organization, I was working this person had actually wanted to review a document and. So, he sent it to his private email id and the organization found and they actually terminated him.

So, some of this can be taken up very seriously the second one is you can do some sort of protocol analysis I think we discussed that I mean you follow the RFC and then see whether the messages are exchanged according to the RFCs and the third one is as I told you the behavior analysis with someone is trying to look into all the ports I mean a person has no business to find out whether all the ports are occupied or not ok. So, unless he is an network administrator or is a system architect who tries to do something. So, so this kind of behavior analysis can also be done with this IDS or IPS.

We will look at some before we close this session we look at some types of IDS.

(Refer Slide Time: 18:13)

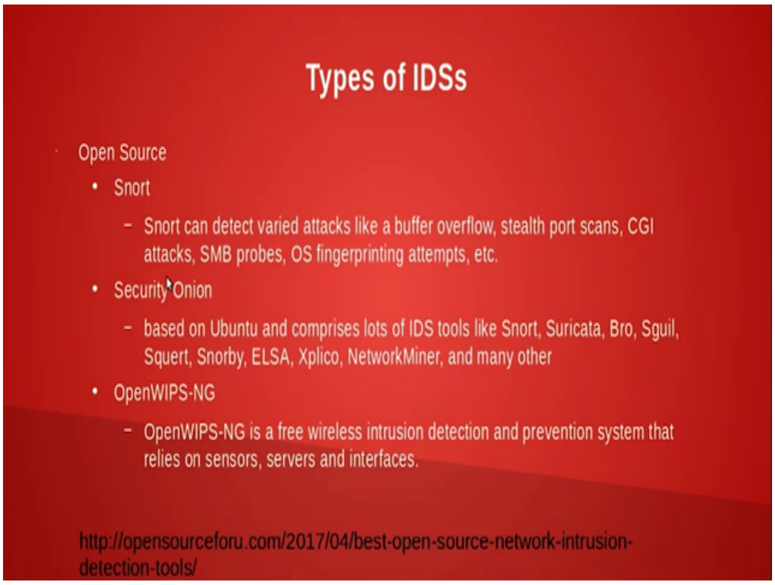


Types of IDSs

- Commercial
  - Check Point IPS-1
    - http://www.checkpoint.com/products/ips-software-blade/
  - Cisco IPS
    - http://www.cisco.com/web/services/portfolio/product-technical-support/intrusion-prevention-ips/index.html
  - Enterasys IPS
    - https://www.enterasys.com/company/literature/ips-ds.pdf
  - Tipping Point IPS
    - http://h17007.www1.hp.com/us/en/whatsnew/040511-1.aspx

You have commercial IPS systems like check point you have Cisco IPS you have Enterasys IPS and then tipping point IPS these are some commercial vendor IPS that you can see in the market an dah there are different types of IDS ok.

(Refer Slide Time: 18:30)



Types of IDSs

- Open Source
  - Snort
    - Snort can detect varied attacks like a buffer overflow, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, etc.
  - Security Onion
    - based on Ubuntu and comprises lots of IDS tools like Snort, Suricata, Bro, Sguil, Squert, Snorby, ELSA, Xplico, NetworkMiner, and many other
  - OpenWIPS-NG
    - OpenWIPS-NG is a free wireless intrusion detection and prevention system that relies on sensors, servers and interfaces.

http://opensourceforu.com/2017/04/best-open-source-network-intrusion-detection-tools/

So, in open source you have IDS IDS can also I mean if when I say IDS IPS IDS can also be use for IPS activities most of the IPS activities and vice versa ok. So, and. So, the open source we have snort and snort can detect varied attacks like buffer overflow stealth port scans and then CGI attacks SMB probes and OS fingerprinting attempts etcetera whether someone is trying to see whether you are using what type of OS are you trying to use ok.

So, when you try to do this kind of fingerprinting then snort can actually help you out there is a product called security onion it is it combines many tools together. So, this is actually much more effective because it also includes snort ok. So, it comprises lot of IDS tools ok. So, you could look at this security onion or you can use open VIPS engine this is essentially for wireless intrusion detection. So, we had seen in the previous sessions that wireless systems are slightly different from wired systems. So, you really have a different intrusion detection technology for wireless systems we would say that you go to this website that is given below and try to see what are all other types of ideas and especially open source ideas that are available the idea is to have detection prevention.

So, we are not recommending that use only snort or use only security onion I mean you should feel comfortable with the tool that you that you use. So, the best thing is to try out some of these tools and see your comfort level then you look at the features that this tool provides which other do not provide since its open source if this tool lacks certain features and you can write your own programs and include it well and good that will raise your capability of doing forensic analysis and prevention and detection we will look at the other features of IDS in the next session.

Thank you very much.