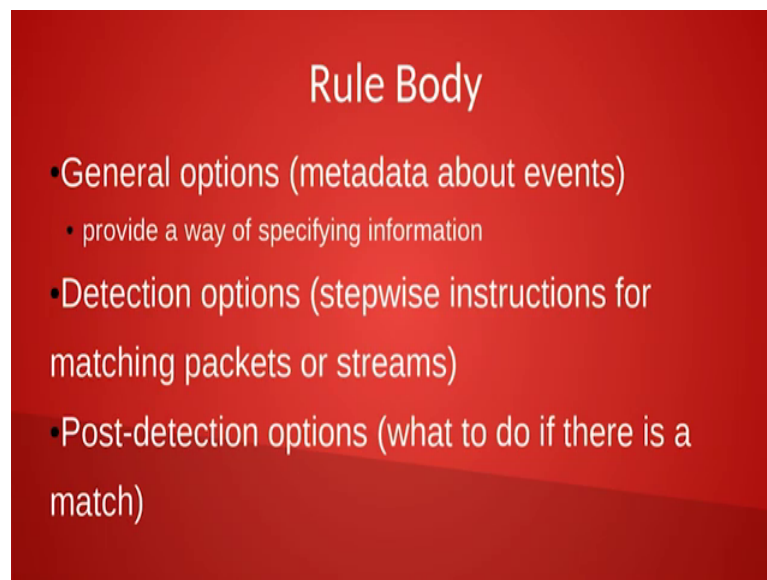


Information security - IV
Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 49
SNORT Rules

Welcome to the session on network security and forensics. In the last session we were briefly reviewing or taking look at snort and we were looking at simple rules of snort. What we will do in this session is we will look into much more details and what is the kind of packets it can capture and all those things.

(Refer Slide Time: 00:33)



Rule Body

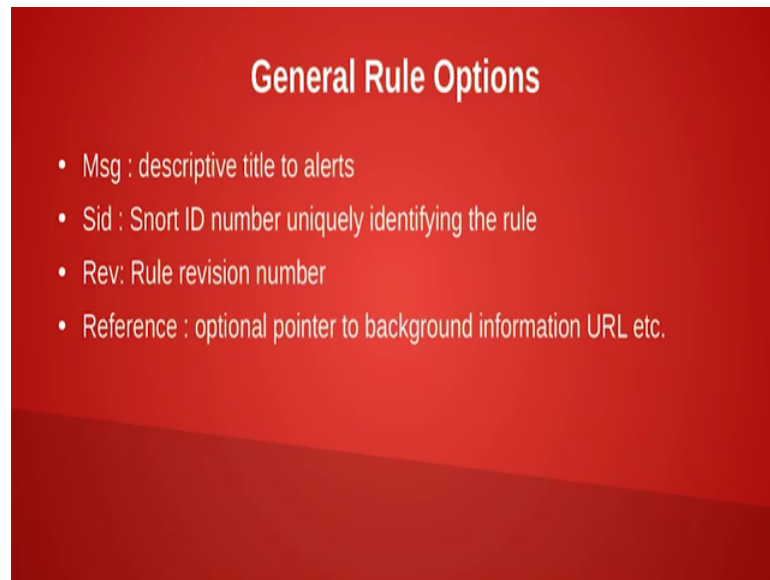
- General options (metadata about events)
 - provide a way of specifying information
- Detection options (stepwise instructions for matching packets or streams)
- Post-detection options (what to do if there is a match)

So, now, coming to rule body of snort ok, you have different options one is you can have a general options were you can have a meta data about events, and you have provide a way of specifying the information. So, the next option is the detection option. So, it says stepwise instruction for matching packets or streams. So, if you look remember our previous rule, it says that I wanted to look at ip, I wanted to look at this port I want to look at this network etcetera etcetera etcetera and then there was something known as post detection options ok.

After I detect what do, I do that was I mean I could either drop or I could either log or I could just send an alert etcetera. So, these were all those what we did ok, so the other than this, in the general rule options ok. So, what it will have is you could have some

messages ok. So, it is something like a descriptive title to alerts and we will see I mean this part might be slightly confusing for you, but what we will do is, when we show some examples of the logs as well as a demo of snort you will understand. So, for time being just understand that there is something like this ok.

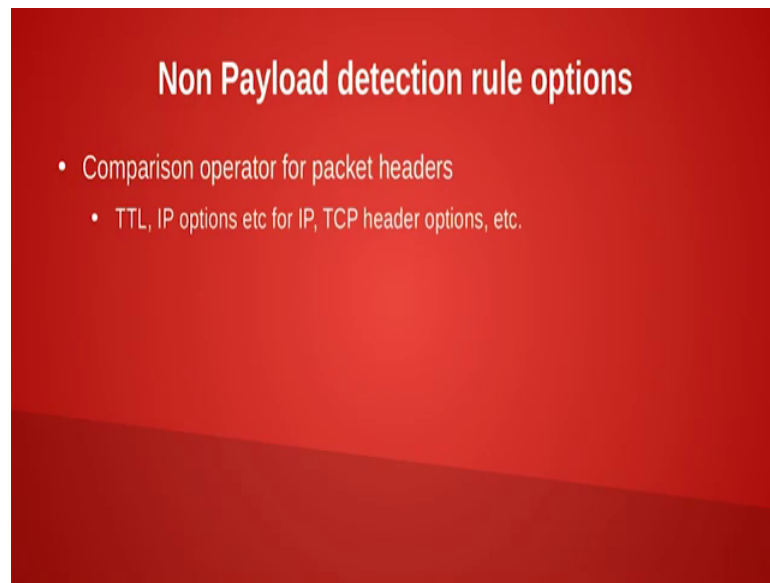
(Refer Slide Time: 01:42)



Like Sid: Snort ID number uniquely identifying the particular rule, that you are implementing then the rule can undergo revisions. So, you can put the rule revision number and then you can also have something a optional pointer to the background informations. So, which URL you should refer to for and why you follow this rules see why is this important because it is sort of command that you provide to rule. See the rules are generated based on policies of your organization.

So, if you have to insert certain rules or if you have to review delete certain rules or review certain rules, then it should or follow the organizations policy and that information must be fed into your rule book of I mean or rules of snort. So, there are other than the general rule options snort also provides something known as non-payload detection rule option ok.

(Refer Slide Time: 02:36)



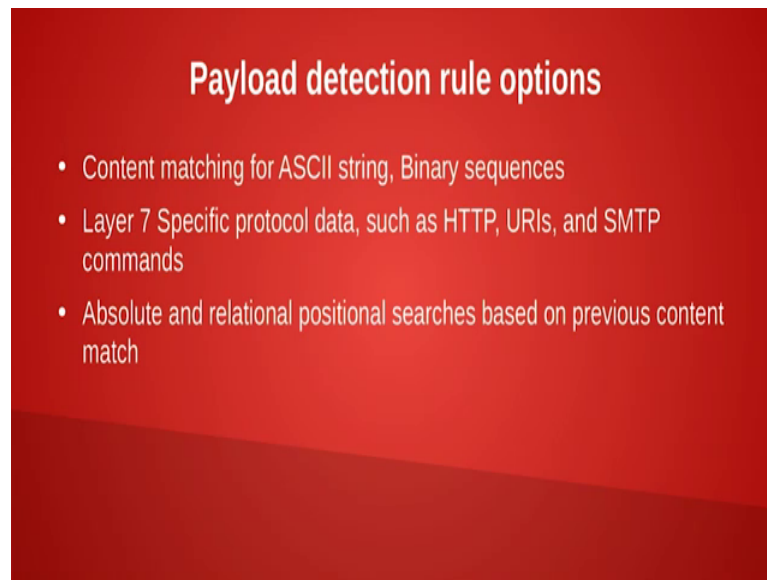
This is with respect to see you have a payload a payload is nothing, but your data and your packet, I mean I could I mean break it into a payload and a header.

Non payload detection rule options talks about how do you detect the patterns based on the header information. For example, whether it is an IP packet or ICMP packet or a TCP packet and if it is an IP packet. Then what about a TTL field ok? If it is a TCP packet then what are where is sin or a sin act. So, these kind of point at details can also be mentioned any rules and this we call them as non-payload detection rule options.

So, in the previous example we did not have we actually found out fifty three we used port number 53, this can be considered as a non-payload detection I mean, but 53 immediately you know the payload will be at ds servers; so dns information. So, I mean this is slightly daisy example, but you could also look at other payload fields like sin fields sin act field ntcp or in IP where its IP v 4 or v 6 etcetera. So, all those things are non-payload detection rule options

So; obviously, then there should be something known as payload detection rule options and with payload detection options what we could do is.

(Refer Slide Time: 04:07)



You can do content matching see whether something matches an ASCII string or whether you are able to see such a binary sequence, and this is very important because in many of worms viruses there is a particular binary pattern that you detect and that comes as a payload ok. So, therefore, the use of this payload detection rule options can be can be utilized, when I want to detect whether any virus or malicious software is entering the network. So, in this way I will I can specify the binary sequences.

You could also look at layer specific protocol data ; that means, whether remember I was talking about your organization banning, you downloading movies or using in our one of the case studies we saw that an uncover was actually trying to send a document ok. So, we could actually block or try to identify whether such documents are being sent ok. So, layer seven specific protocol data I mean we can use this, and along with the binary sequence and then the signatures we can go ahead and find out what exactly happens and how we can do to take any action on when such data is sent out and there is also one more additional feature ok. So, you can have absolute and relational portions such as based on the previous content match ok.

So, sometimes what happens is, I mean for example, certain data packets start at a particular location. So, if the previous is there then we have to start in this location those kind of minor things can be done ok. So, now, combining all this together, I mean its not

becomes very powerful for detecting many of the anomalies then finally, we have something known as a post detection rule option ok.

(Refer Slide Time: 06:01)



Now, here what happens is, you translate the rule the translate rule matches into specific actions on a rule by rule basis ok.

Now, sometimes you could even overwrite this snort configuration for example, you might say that I have to cause an alert. Now the alert can be caused in different ways either you can send the alert to snmp or you can just send it to a particular server as a message and then what I could do is, see in general I can say that log the packet. Now suppose I want to log only a specific areas in the packet, yes then I can apply the post detection rule and apply it to specific areas in the packet ok.

The third one that I can do post rule is for example, it is like taking over the work of a firewall ok. I can go ahead and say that this TCP connection has to be reset because I am getting lot of sin and when I do a sin hack he does not hack therefore, I have to reset this TCP connection. So, this kind of post detection rule options can trigger many of these response mechanisms such as reset of TCP connections etcetera.

Now, I think it is already confusing. So, what will try to do is we will try to look at some examples ok. So, that you we understand all these things. So, here is the first example that we get ok.

(Refer Slide Time: 07:29)

Example

- `alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg : " ICMP PING "; icode : 0; itype : 8; classtype : misc - activity ; sid : 384; rev : 5;)`
- Alert on any inbound ICMP traffic that is of type 8 code 0: an "Echo Request."

```
[**] [1:384:5] ICMP PING [**]
```

```
[ Classification : Misc activity ] [ Priority : 3]
```

```
04/13 -03:12:08.359790 10.0.1.10 -> 10.0.1.254
```

```
ICMP TTL :64 TOS :0 x0 ID :38125 IpLen :20 DgmLen :84
```

```
Type :8 Code :0 ID :32335 Seq :1 ECHO
```

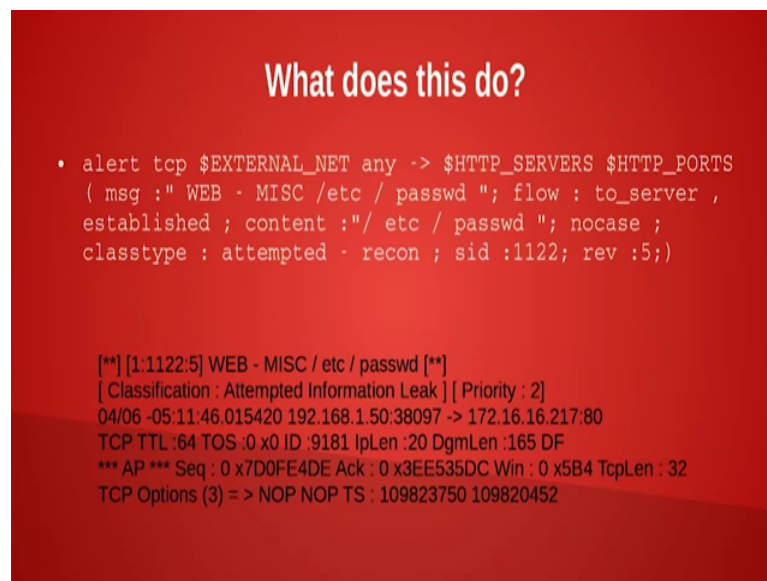
So, this tells you alert ICMP external net any I think you are you are with the first line ok. So, if you take the first line alert so; that means, you have to send the alert then it says ICMP ok. So, this is for the ICMP protocol then external net; that means, any external network and any port to my home network and home and home port any port now this home network and external network can be defined in your snort dot com file I mean we had seen it earlier and then the message that I have to say is that ICMP pin icode 0 itype 8 class type miscellaneous dash activity sid and revision file

Now, if you look at the error message that is prints, look at this it prints classification miscellaneous activity similar to class type miscellaneous activity this part, then it also prints priority is 3. The other thing is this is the one see because its ICMP ping, it prints this ICMP ping and we know what this is because this three 84 is referred to as your snort id and then rule number 5 revision number 5 ok.

So, then it logs ok. So, the person was tried to contact is this, he had tries to send this and if you look at this; what I am talking about icode and itype. So, that is exactly what is printed. So, type 8 and code 0 and the sequence for this is echo and it also prints the other stuff like icp TTL time to leave and. So, all these detail IP length and then data gram length and all those things. So, if you look at this I can configure this and it prints an alert on any inbound as ICMP traffic that is of type 8 and code 0 that is code 0 is an echo request.

So, if someone tries to do a ping then I try I mean I i this I intrusion detection will generate, an alert that ping essentially is an ICMP packet and you try use ping to find out whether someone is live or not. So, if someone tries to find out whether machine is live or not, this guy can snoop inside and then get the data and we can take an action saying that alert someone is trying to snoop I mean come inside the network or snoop what is there in the network

(Refer Slide Time: 09:51)



What does this do?

- alert tcp \$EXTERNAL_NET any -> \$HTTP_SERVERS \$HTTP_PORTS
(msg : " WEB - MISC /etc / passwd "; flow : to_server ,
established ; content : "/ etc / passwd "; nocase ;
classtype : attempted - recon ; sid :1122; rev :5;)

[**] [1:1122:5] WEB - MISC / etc / passwd [**]
[Classification : Attempted Information Leak] [Priority : 2]
04/06 -05:11:46.015420 192.168.1.50:38097 -> 172.16.16.217:80
TCP TTL :64 TOS :0 x0 ID :9181 IpLen :20 DgmLen :165 DF
*** AP *** Seq : 0 x7D0FE4DE Ack : 0 x3EE535DC Win : 0 x5B4 TcpLen : 32
TCP Options (3) => NOP NOP TS : 109823750 109820452

So, similarly it can be slightly more complicated as something like this ok. So, this is slightly more complicated says alert TCP external net any. So, hHTTP servers any port any server any port and then message is web miscellaneous slash etc password flow to server established content etc password nocase classtype attempted recon sid is 1122 and review revision 5.

Now, what does it I mean can you make a guess what it says ok? So, looking at etc password, I think you could make a guess that if someone tries to read the etc password file through some sort of web server sort of interface, then the alert has to be generated yes your correct that is exactly what this rule says ok. So, this rule might look odd we will I mean you have to learn how to write this rules ok, it a session bu itself how to how to write rules using snort, but then let us try to understand the rules. Because if you actually go through the snort conf and other rule file should be able to understand what exactly, see how an organization policy gets converted into this rules ok.

So, this will actually kind of a print a message something like this. So, web server miscellaneous etc password. So, this is the what we want to identify. So, classification information leak and priority to and it says that the person who tried to do this was 192.168.1.50 he was using his port 38097 he was trying to come into our network 172.16.16.21 17 colon 80 and with all TCP and all these things.

Now, the most important stuff is that ok. So, this person was the one I mean he was the one who tried to access this etc password and so, the web content actually had this etc that password the request had is etc dot password and this nocase tells you that it can be any. So, I can give a capital or small or whatever. So, its says nocase and this tells you the other options like what is that TCP sequence number what has acknowledgement number and what was the window size and what is the TCP length and all those details and probably once you get these details you can ge head and start tracking this packets or the tracking this attacker.

So, this is in short how snort works what I mean. So, in conclusion about IDs and IPs one of the things how does forensics analyst use this information first once an alert is triggered it tells the forensic analyzer that you have to actually do an investigation ok.

(Refer Slide Time: 12:48)



Because what this happened is, you had certain policies and someone is violating a policy. So, once you know that yes this has to be investigated then you can start your data collection, which is exactly what we were looking at the previous sessions like

evidence acquisition and once you and remember the evidence acquisition here is much difficult ok. See previously we were looking at putting the data just into the internet and then we are capturing the libpcap file here the pcap file is captured by the ids and he was the one who was giving us alerts.

So, what we have to do is now, we have to closely monitor the ids as well as capture the pcap files and not only that, but only thing is it tells you that there is where to find the needle in the haste tag ok. So, that is exactly the role of IDs. So, it instead of collecting all the data, now we can start collecting targeted data or apply filters such that we identify who is the attacker who is trying to attack us.

So, in that way ids actually reduces the amount of data to be collected by a forensic investigator, and in general in IDs IPs and other things you have something known as false positives and true negatives I mean what happens is sometimes it may not be actually be an attack, but it will be triggered as an attack. So, an alarm could generate and sometimes there will be an attack, but it may not get detected.

Now, the second one is very dangerous, because if there is an attack and its not getting detected, then you have to ensure that your rules are much more stronger and if the first way round yes its ok, but to many I mean false positives also detrimental for your work because every time it will be alerted and. So, that is why getting a balance in writing the rules is also an art ok. So, not only that the rules have to be updated quite frequently, because there are different types of attacks happening the this signatures change quite a lot ok.

So, in order. So, because of this the act of maintaining this ids itself becomes a huge task ok. So, in conclusion, what yes ids is a very very powerful tool and it has to be managed well and once we manage well hopefully will have better security, now this ids tool is very good for forensic analyst because its provides you alerts it removes unnecessary data and it also tells a forensic analyst, where exactly you should start pointing or start your work

So, what we will do until now we have being talking too much. So, what will do in the next session is, we will have a demo of snort we will try to identify some attacks and we will see how the rules have being written for this, how snort has configured and how its start detecting the attacks and then proceed from there and how it sends the logs ok.

Thank you very much.