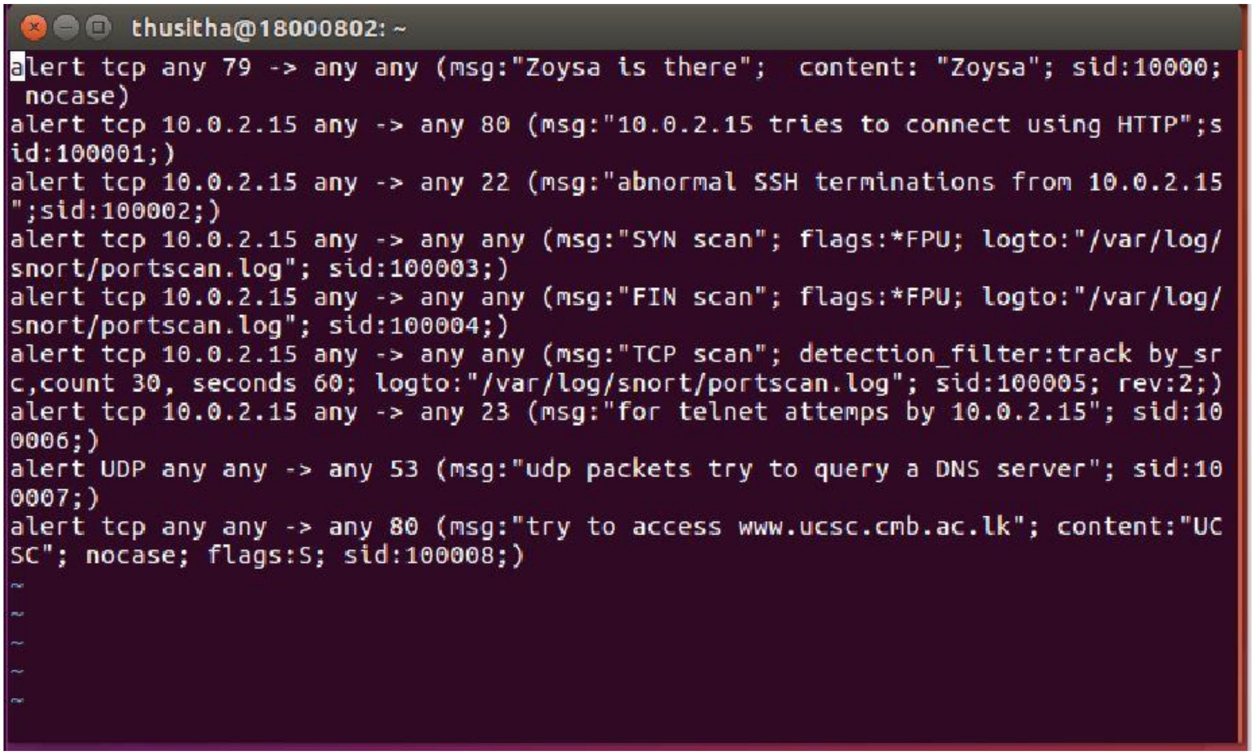
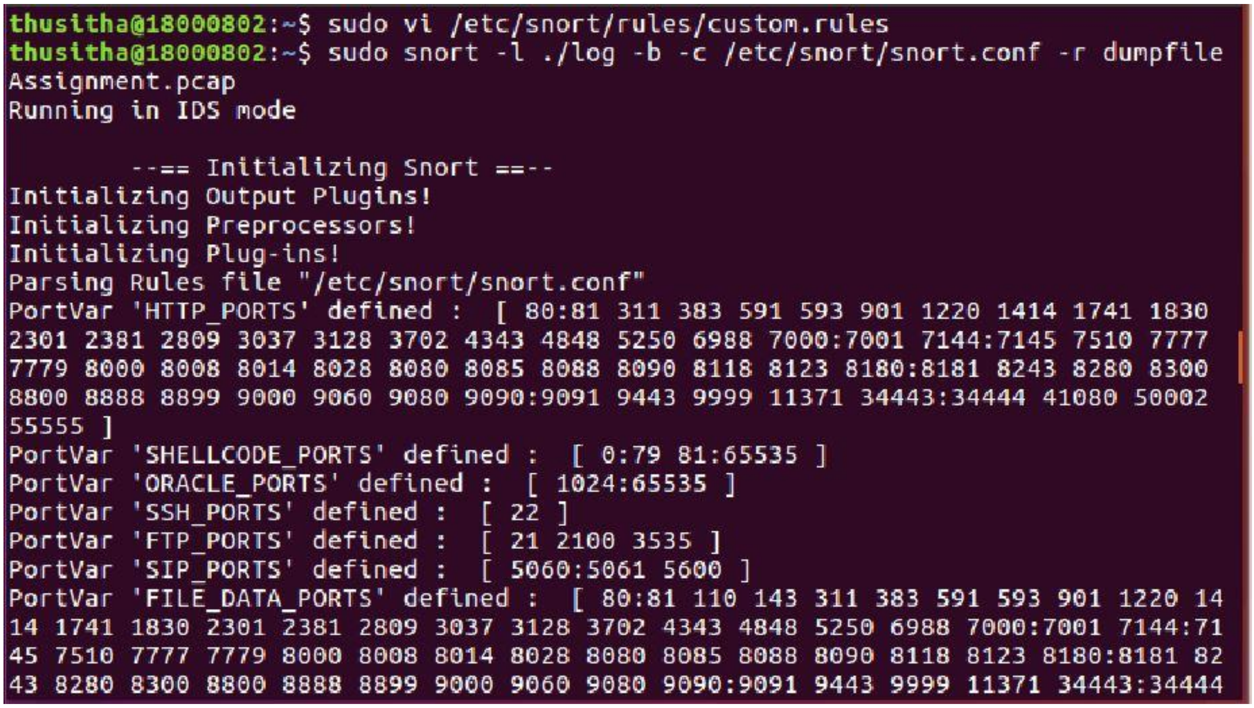
ISS Assignment

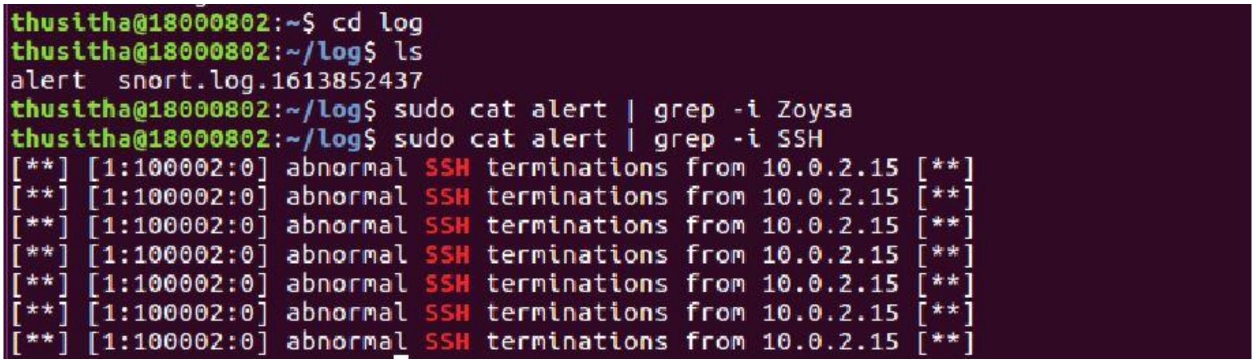
Index No : 18000802



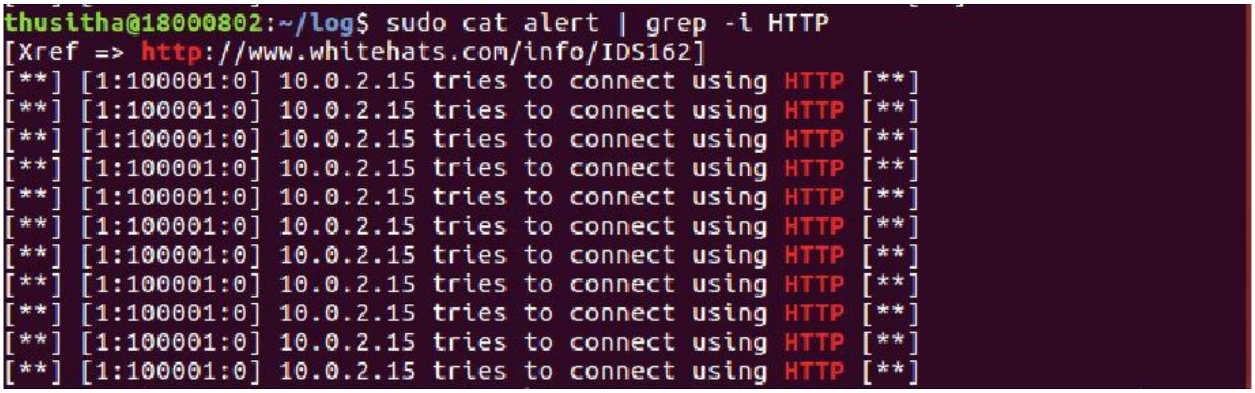
```
alert tcp any 79 -> any any (msg:"Zoysa is there";  content: "Zoysa"; sid:10000;
 nocase)
alert tcp 10.0.2.15 any -> any 80 (msg:"10.0.2.15 tries to connect using HTTP";s
id:100001;)
alert tcp 10.0.2.15 any -> any 22 (msg:"abnormal SSH terminations from 10.0.2.15
";sid:100002;)
alert tcp 10.0.2.15 any -> any any (msg:"SYN scan"; flags:*FPU; logto:"/var/log/
snort/portscan.log"; sid:100003;)
alert tcp 10.0.2.15 any -> any any (msg:"FIN scan"; flags:*FPU; logto:"/var/log/
snort/portscan.log"; sid:100004;)
alert tcp 10.0.2.15 any -> any any (msg:"TCP scan"; detection_filter:track by_sr
c,count 30, seconds 60; logto:"/var/log/snort/portscan.log"; sid:100005; rev:2;)
alert tcp 10.0.2.15 any -> any 23 (msg:"for telnet attemps by 10.0.2.15"; sid:10
0006;)
alert UDP any any -> any 53 (msg:"udp packets try to query a DNS server"; sid:10
0007;)
alert tcp any any -> any 80 (msg:"try to access www.ucsc.cmb.ac.lk"; content:"UC
SC"; nocase; flags:S; sid:100008;)
~
~
~
~
~
```



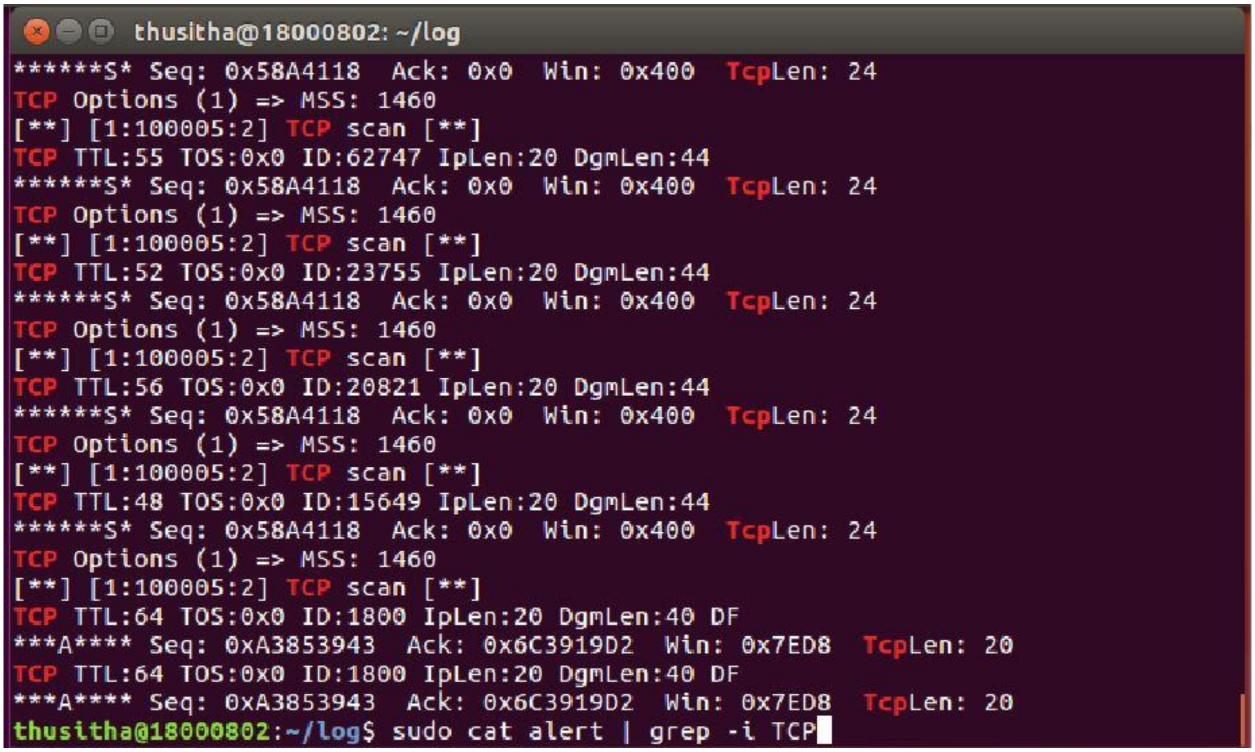
```
thusitha@18000802:~$ sudo vi /etc/snort/rules/custom.rules
thusitha@18000802:~$ sudo snort -l ./log -b -c /etc/snort/snort.conf -r dumpfile
Assignment.pcap
Running in IDS mode

        --== 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 4343 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 14
14 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:71
45 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82
43 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444
```



```
thusitha@18000802:~$ cd log
thusitha@18000802:~/log$ ls
alert   snort.log.1613852437
thusitha@18000802:~/log$ sudo cat alert | grep -i Zoysa
thusitha@18000802:~/log$ sudo cat alert | grep -i SSH
[**] [1:100002:0] abnormal SSH terminations from 10.0.2.15 [**]
[**] [1:100002:0] abnormal SSH terminations from 10.0.2.15 [**]
[**] [1:100002:0] abnormal SSH terminations from 10.0.2.15 [**]
[**] [1:100002:0] abnormal SSH terminations from 10.0.2.15 [**]
[**] [1:100002:0] abnormal SSH terminations from 10.0.2.15 [**]
[**] [1:100002:0] abnormal SSH terminations from 10.0.2.15 [**]
[**] [1:100002:0] abnormal SSH terminations from 10.0.2.15 [**]
```



```
thusitha@18000802:~/log$ sudo cat alert | grep -i HTTP
[Xref => http://www.whitehats.com/info/IDS162]
[**] [1:100001:0] 10.0.2.15 tries to connect using HTTP [**]
[**] [1:100001:0] 10.0.2.15 tries to connect using HTTP [**]
[**] [1:100001:0] 10.0.2.15 tries to connect using HTTP [**]
[**] [1:100001:0] 10.0.2.15 tries to connect using HTTP [**]
[**] [1:100001:0] 10.0.2.15 tries to connect using HTTP [**]
[**] [1:100001:0] 10.0.2.15 tries to connect using HTTP [**]
[**] [1:100001:0] 10.0.2.15 tries to connect using HTTP [**]
[**] [1:100001:0] 10.0.2.15 tries to connect using HTTP [**]
[**] [1:100001:0] 10.0.2.15 tries to connect using HTTP [**]
[**] [1:100001:0] 10.0.2.15 tries to connect using HTTP [**]
[**] [1:100001:0] 10.0.2.15 tries to connect using HTTP [**]
```



```
******S* Seq: 0x58A4118  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460
[**] [1:100005:2] TCP scan [**]
TCP TTL:55 TOS:0x0 ID:62747 IpLen:20 DgmLen:44
******S* Seq: 0x58A4118  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460
[**] [1:100005:2] TCP scan [**]
TCP TTL:52 TOS:0x0 ID:23755 IpLen:20 DgmLen:44
******S* Seq: 0x58A4118  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460
[**] [1:100005:2] TCP scan [**]
TCP TTL:56 TOS:0x0 ID:20821 IpLen:20 DgmLen:44
******S* Seq: 0x58A4118  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460
[**] [1:100005:2] TCP scan [**]
TCP TTL:48 TOS:0x0 ID:15649 IpLen:20 DgmLen:44
******S* Seq: 0x58A4118  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460
[**] [1:100005:2] TCP scan [**]
TCP TTL:64 TOS:0x0 ID:1800 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xA3853943  Ack: 0x6C3919D2  Win: 0x7ED8  TcpLen: 20
TCP TTL:64 TOS:0x0 ID:1800 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xA3853943  Ack: 0x6C3919D2  Win: 0x7ED8  TcpLen: 20
thusitha@18000802:~/log$ sudo cat alert | grep -i TCP
```