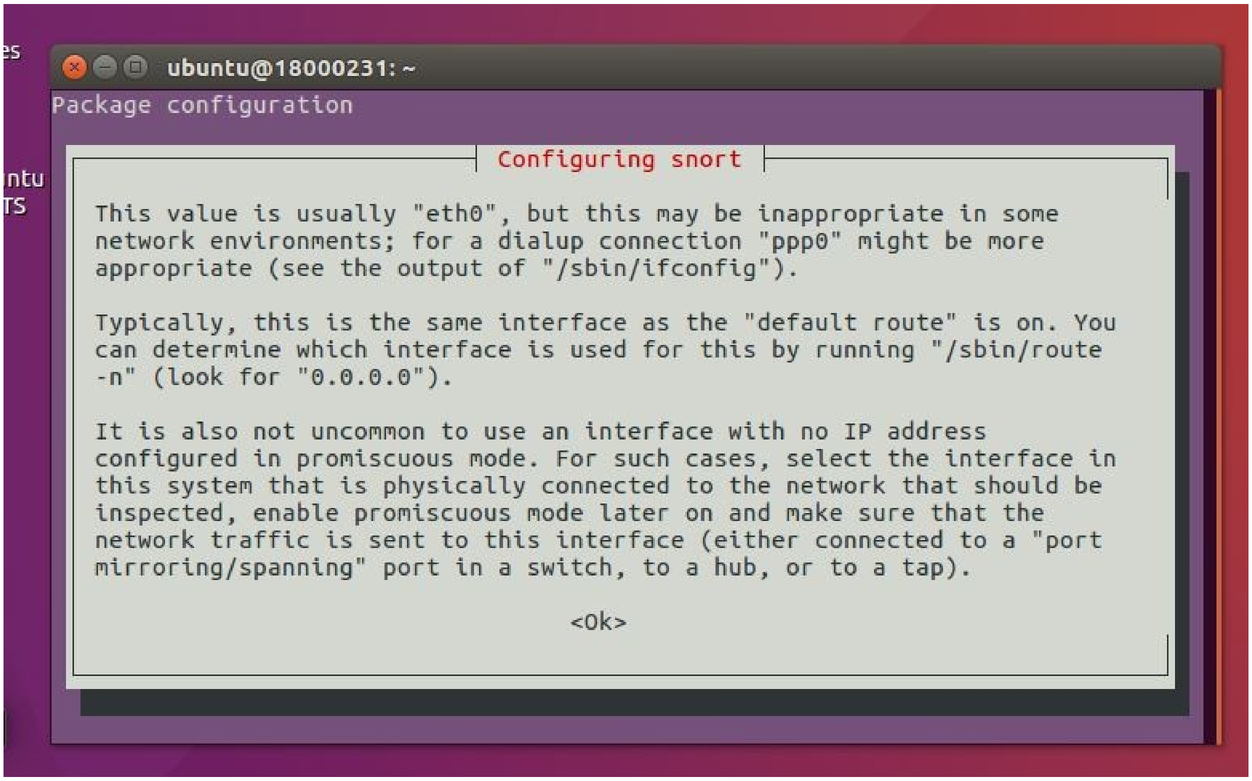
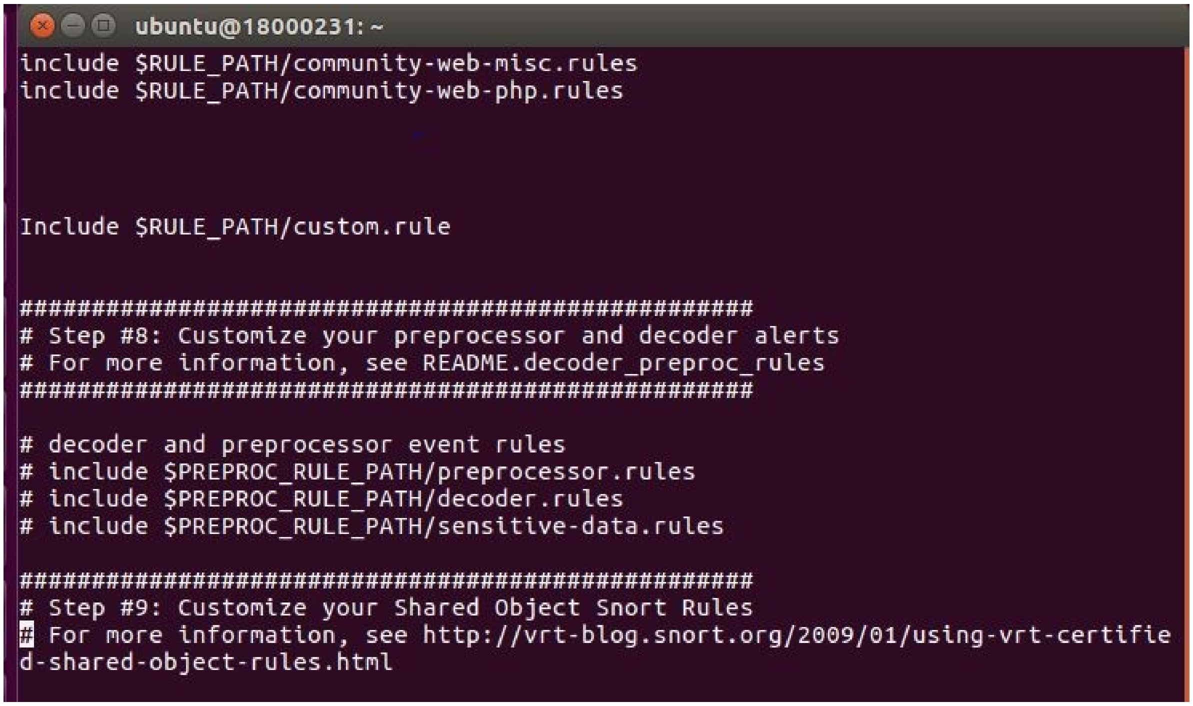
SCS2214 Information System Security

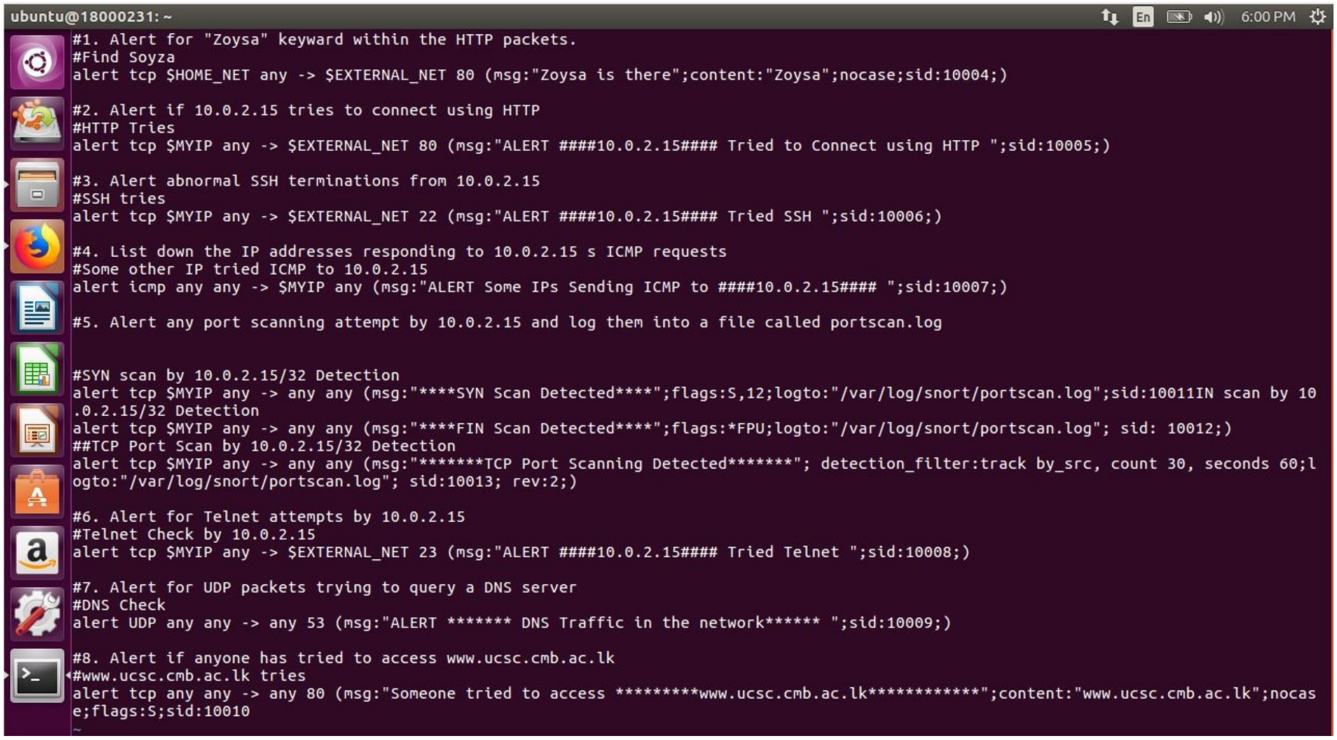
Index number 18000231



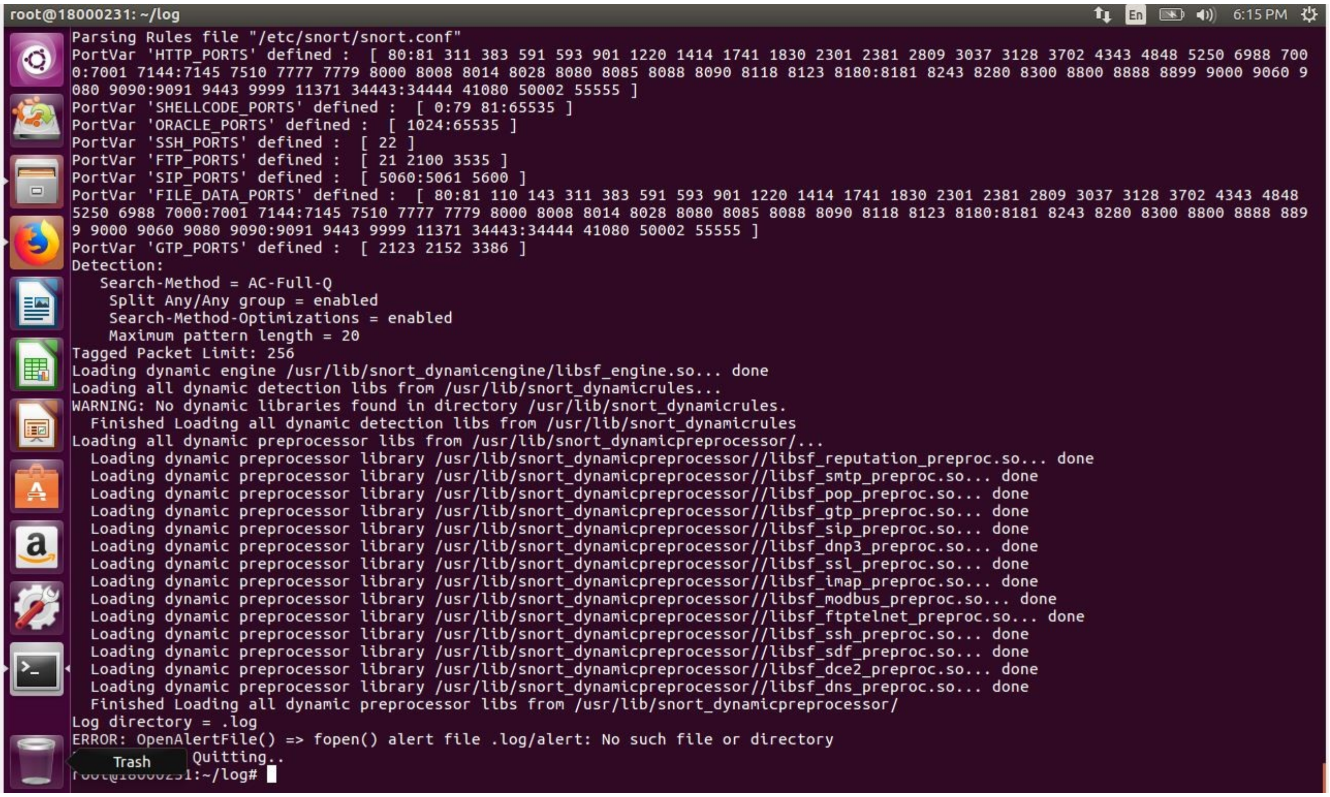
```
Package configuration

Configuring snort

This value is usually "eth0", but this may be inappropriate in some
network environments; for a dialup connection "ppp0" might be more
appropriate (see the output of "/sbin/ifconfig").

Typically, this is the same interface as the "default route" is on. You
can determine which interface is used for this by running "/sbin/route
-n" (look for "0.0.0.0").

It is also not uncommon to use an interface with no IP address
configured in promiscuous mode. For such cases, select the interface in
this system that is physically connected to the network that should be
inspected, enable promiscuous mode later on and make sure that the
network traffic is sent to this interface (either connected to a "port
mirroring/spanning" port in a switch, to a hub, or to a tap).

                              <Ok>
```



```
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules




Include $RULE_PATH/custom.rule


###################################################
# Step #8: Customize your preprocessor and decoder alerts
# For more information, see README.decoder_preproc_rules
###################################################

# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH/preprocessor.rules
# include $PREPROC_RULE_PATH/decoder.rules
# include $PREPROC_RULE_PATH/sensitive-data.rules

###################################################
# Step #9: Customize your Shared Object Snort Rules
# For more information, see http://vrt-blog.snort.org/2009/01/using-vrt-certifie
d-shared-object-rules.html
```



```
#1. Alert for "Zoysa" keyward within the HTTP packets.
#Find Soyza
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"Zoysa is there";content:"Zoysa";nocase;sid:10004;)

#2. Alert if 10.0.2.15 tries to connect using HTTP
#HTTP Tries
alert tcp $MYIP any -> $EXTERNAL_NET 80 (msg:"ALERT ####10.0.2.15#### Tried to Connect using HTTP ";sid:10005;)

#3. Alert abnormal SSH terminations from 10.0.2.15
#SSH tries
alert tcp $MYIP any -> $EXTERNAL_NET 22 (msg:"ALERT ####10.0.2.15#### Tried SSH ";sid:10006;)

#4. List down the IP addresses responding to 10.0.2.15 s ICMP requests
#Some other IP tried ICMP to 10.0.2.15
alert icmp any any -> $MYIP any (msg:"ALERT Some IPs Sending ICMP to ####10.0.2.15#### ";sid:10007;)

#5. Alert any port scanning attempt by 10.0.2.15 and log them into a file called portscan.log


#SYN scan by 10.0.2.15/32 Detection
alert tcp $MYIP any -> any any (msg:"****SYN Scan Detected****";flags:S,12;logto:"/var/log/snort/portscan.log";sid:10011IN scan by 10
.0.2.15/32 Detection
alert tcp $MYIP any -> any any (msg:"****FIN Scan Detected****";flags:*FPU;logto:"/var/log/snort/portscan.log"; sid: 10012;)
##TCP Port Scan by 10.0.2.15/32 Detection
alert tcp $MYIP any -> any any (msg:"*******TCP Port Scanning Detected*******"; detection_filter:track by_src, count 30, seconds 60;l
ogto:"/var/log/snort/portscan.log"; sid:10013; rev:2;)

#6. Alert for Telnet attempts by 10.0.2.15
#Telnet Check by 10.0.2.15
alert tcp $MYIP any -> $EXTERNAL_NET 23 (msg:"ALERT ####10.0.2.15#### Tried Telnet ";sid:10008;)

#7. Alert for UDP packets trying to query a DNS server
#DNS Check
alert UDP any any -> any 53 (msg:"ALERT ******* DNS Traffic in the network****** ";sid:10009;)

#8. Alert if anyone has tried to access www.ucsc.cmb.ac.lk
#www.ucsc.cmb.ac.lk tries
alert tcp any any -> any 80 (msg:"Someone tried to access *********www.ucsc.cmb.ac.lk************";content:"www.ucsc.cmb.ac.lk";nocas
e;flags:S;sid:10010
~
```



```
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 700
0:7001 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 9
080 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 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 889
9 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_reputation_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_smtp_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_pop_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_gtp_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_sip_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_dnp3_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_ssl_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_imap_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_modbus_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_ftptelnet_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_ssh_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_sdf_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_dce2_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_dns_preproc.so... done
  Finished Loading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor/
Log directory = .log
ERROR: OpenAlertFile() => fopen() alert file .log/alert: No such file or directory
             Quitting..
root@18000231:~/log# 
```

I got an error.I tried to solve it but it is not working sir!