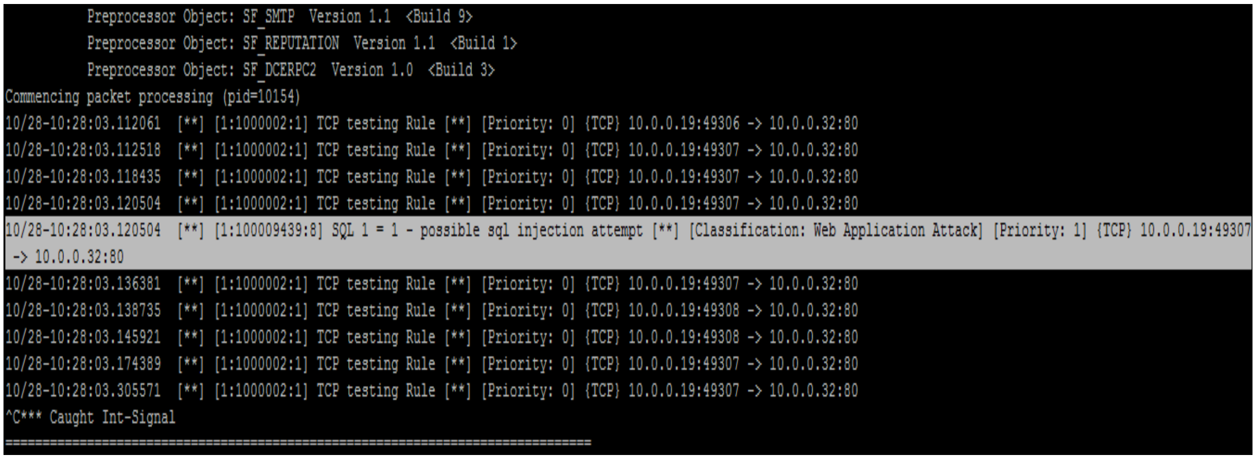
1. **Submit your Snort configuration file. You need only include your main snort.conf, not the downloaded signatures.**
   ➔ snort.conf file has been included in the folder.

2. **Which signature did you select to test Snort? Include a snippet of the log showing when the alert was triggered.**
   ➔ a. SQL Injection from sql.rules (defined in /etc/snort/rules/snort.rules)

   alert tcp any any -> any 80 (msg:"SQL 1 = 1 - possible sql injection attempt"; flow:to_server,established; content:"1=1"; fast_pattern:only; http_uri; pcre:"/(and|or)[\s\x2f\x2A]+1=1/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:url,ferruh.mavituna.com/sql-injection-cheatsheet-oku/; classtype:web-application-attack; sid:100009439; rev:8;)

   HTTP URL used in the Windows Web Browser: http://strawman.nslab/?arg1=hello’ and 1=1#

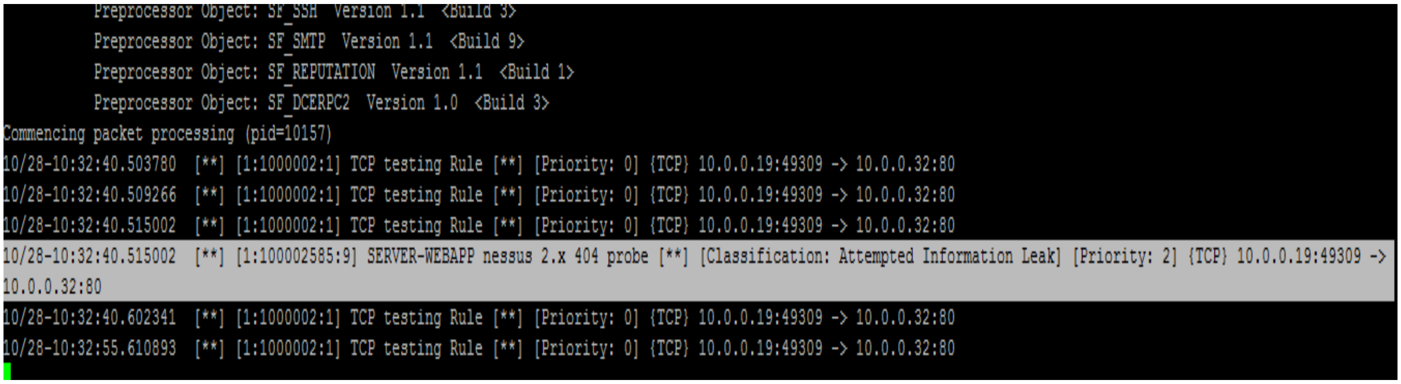


```
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=10154)
10/28-10:28:03.112061  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49306 -> 10.0.0.32:80
10/28-10:28:03.112518  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49307 -> 10.0.0.32:80
10/28-10:28:03.118435  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49307 -> 10.0.0.32:80
10/28-10:28:03.120504  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49307 -> 10.0.0.32:80
10/28-10:28:03.120504  [**] [1:100009439:8] SQL 1 = 1 - possible sql injection attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 10.0.0.19:49307
 -> 10.0.0.32:80
10/28-10:28:03.136381  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49307 -> 10.0.0.32:80
10/28-10:28:03.138735  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49308 -> 10.0.0.32:80
10/28-10:28:03.145921  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49308 -> 10.0.0.32:80
10/28-10:28:03.174389  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49307 -> 10.0.0.32:80
10/28-10:28:03.305571  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49307 -> 10.0.0.32:80
^C*** Caught Int-Signal
================================================================================
```

   b. NessusTest from server-webapp.rules

   alert tcp any any -> any 80 (msg:"SERVER-WEBAPP nessus 2.x 404 probe"; flow:to_server,established; content:"/NessusTest"; fast_pattern:only; http_uri; metadata:ruleset community, service http; reference:nessus,10386; classtype:attempted-recon; sid:100002585; rev:9;)

   HTTP URL used on the Windows Web browser: http://strawman.nslab/NessusTest



```
        Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
        Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
        Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
        Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=10157)
10/28-10:32:40.503780  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49309 -> 10.0.0.32:80
10/28-10:32:40.509266  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49309 -> 10.0.0.32:80
10/28-10:32:40.515002  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49309 -> 10.0.0.32:80
10/28-10:32:40.515002  [**] [1:100002585:9] SERVER-WEBAPP nessus 2.x 404 probe [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 10.0.0.19:49309 ->
10.0.0.32:80
10/28-10:32:40.602341  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49309 -> 10.0.0.32:80
10/28-10:32:55.610893  [**] [1:1000002:1] TCP testing Rule [**] [Priority: 0] {TCP} 10.0.0.19:49309 -> 10.0.0.32:80
```

3. **Suppose you are the administrator of a webserver that hosts a large eCommerce application. For security, your webserver is configured to communicate with all clients over SSL for every request. Your boss asks you to set up Snort to monitor attacks against the web server and application. He believes that the SSL implementation is secure and isn't concerned about monitoring the SSL tunnel itself. Propose a network design that would allow you to monitor this traffic without installing Snort on the webservers themselves. Draw a simple diagram that illustrates your design. NOTE: You do not need to worry about specific products and whether or not there exist products that do what you need for your design. If you need a router/server/etc that does something, assume you could build it.**

   ➔ Instead of installing Snort on the webservers themselves, it can be installed on the strategic points of the network along with firewall which can monitor the traffic on the webservers and the application.

   Diagram to illustrate this design :
   Please refer the image uploaded in the folder. DesignDiagram.pdf