

Activity 5.2 Snort Part-2

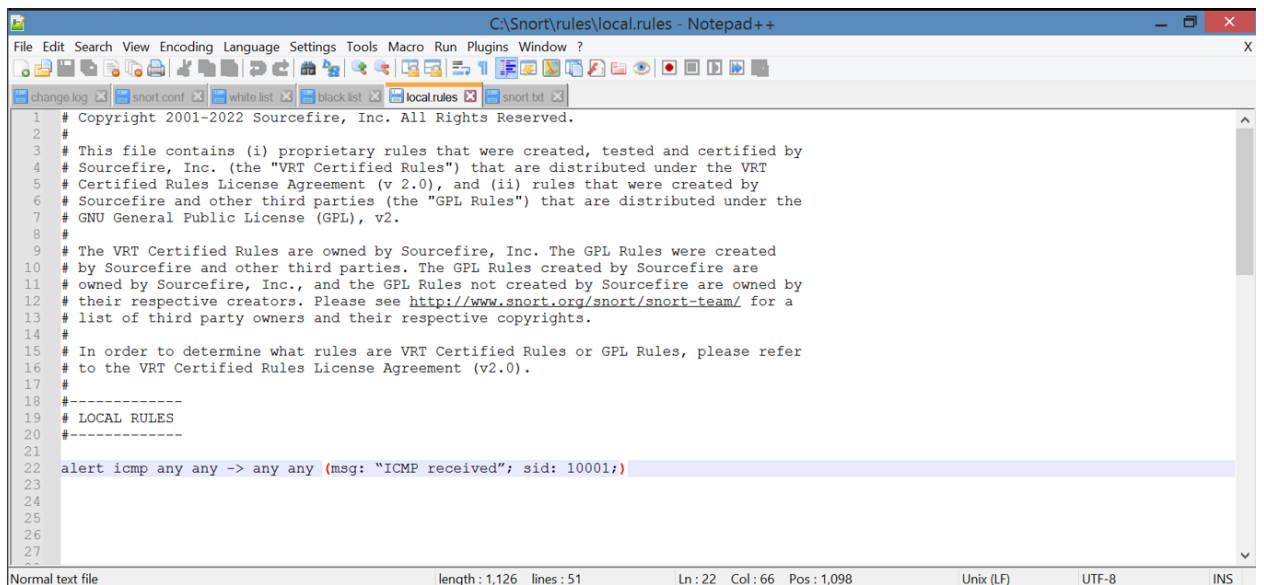
Dominik Gonzales

Connor Carroll

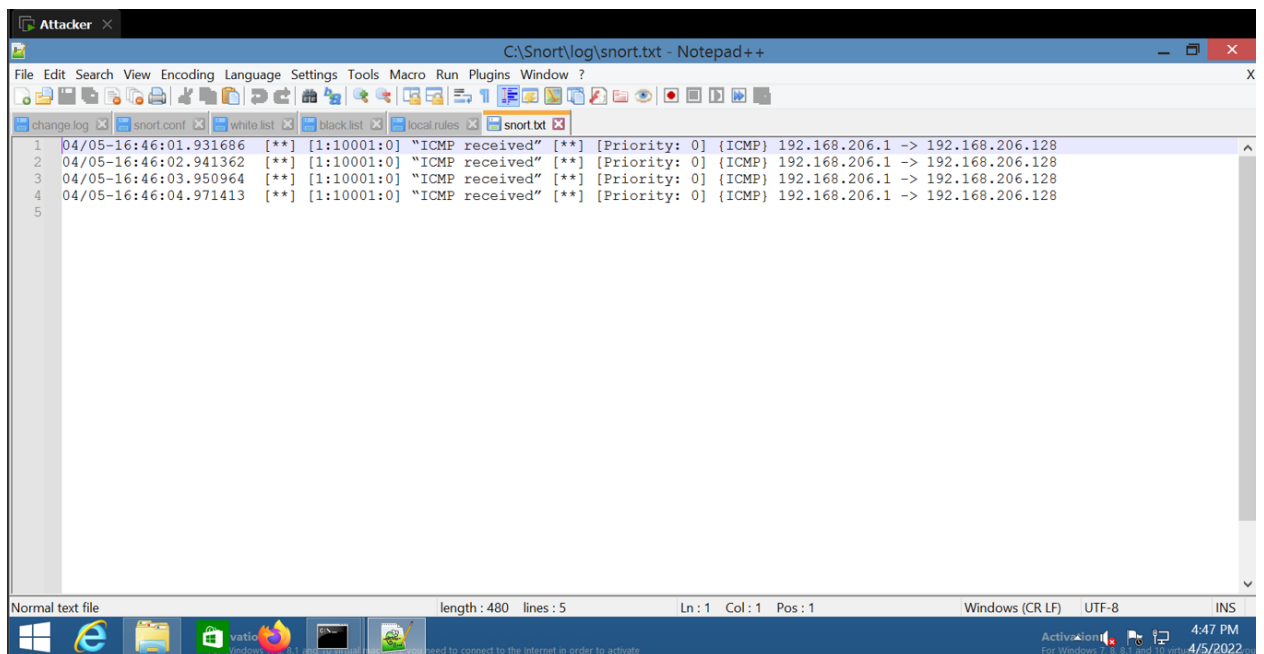
Will Zhang

Shashank Mondrati

1.

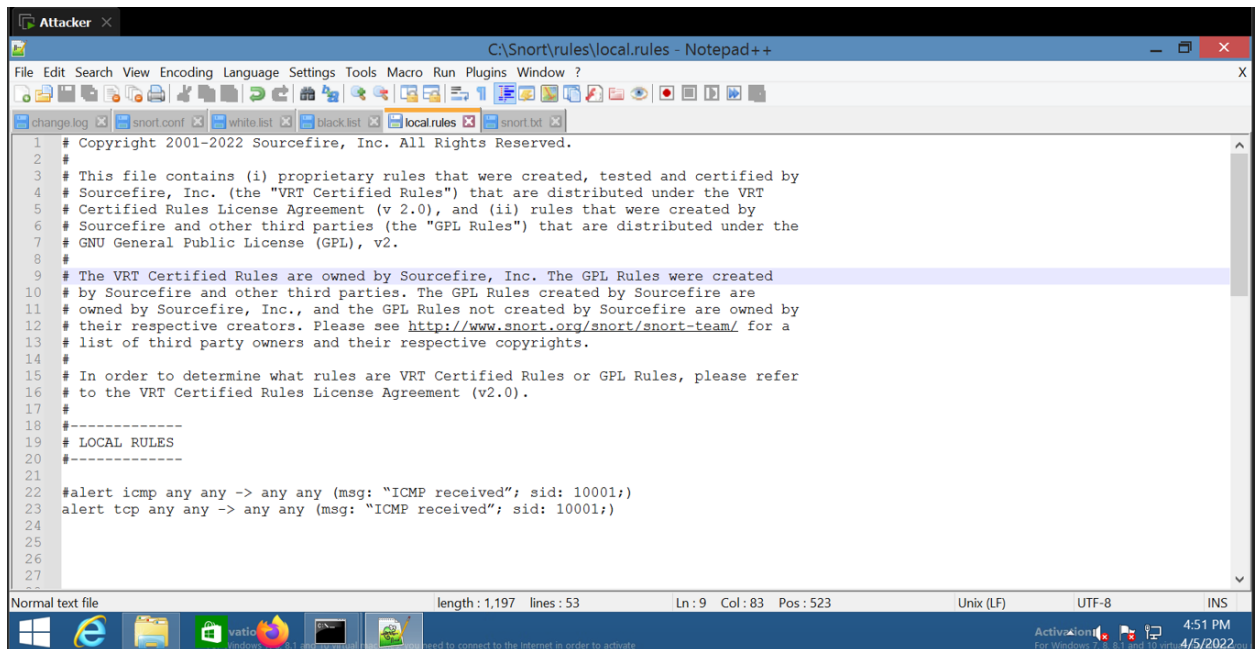


```
1 # Copyright 2001-2022 Sourcefire, Inc. All Rights Reserved.
2 #
3 # This file contains (i) proprietary rules that were created, tested and certified by
4 # Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
5 # Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
6 # Sourcefire and other third parties (the "GPL Rules") that are distributed under the
7 # GNU General Public License (GPL), v2.
8 #
9 # The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
10 # by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
11 # owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
12 # their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
13 # list of third party owners and their respective copyrights.
14 #
15 # In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
16 # to the VRT Certified Rules License Agreement (v2.0).
17 #
18 #-----
19 # LOCAL RULES
20 #-----
21
22 alert icmp any any -> any any (msg: "ICMP received"; sid: 10001;)
23
24
25
26
27
28
```



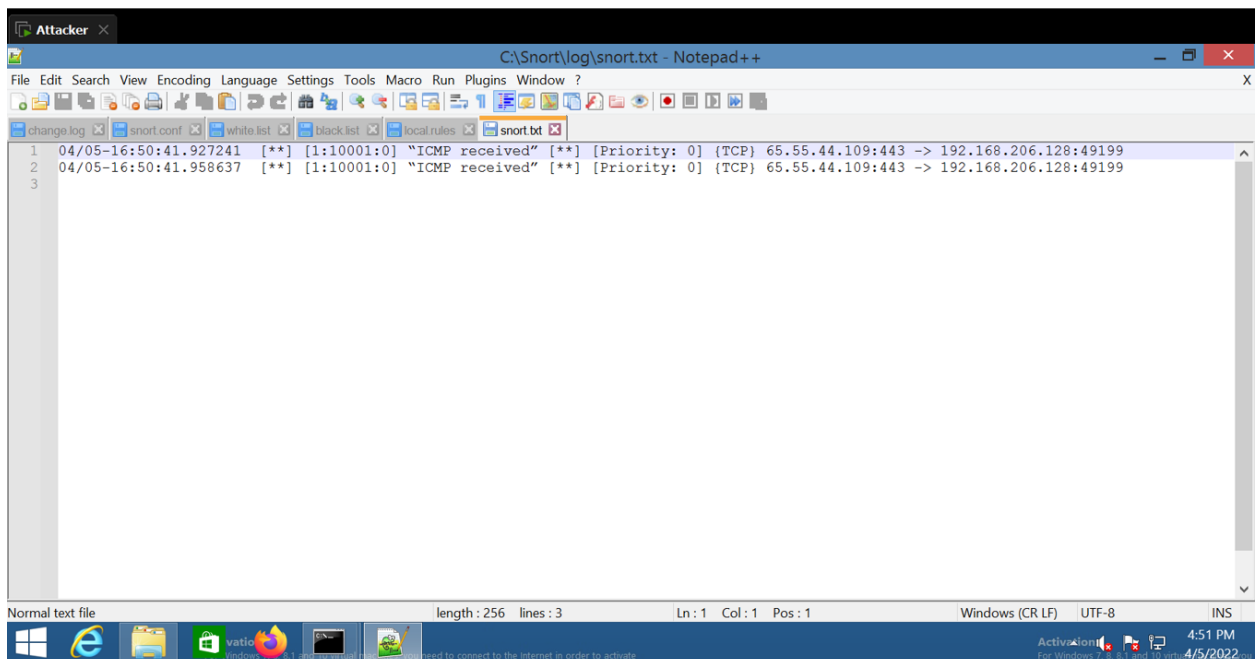
```
1 04/05-16:46:01.931686 [**] [1:10001:0] "ICMP received" [**] [Priority: 0] (ICMP) 192.168.206.1 -> 192.168.206.128
2 04/05-16:46:02.941362 [**] [1:10001:0] "ICMP received" [**] [Priority: 0] (ICMP) 192.168.206.1 -> 192.168.206.128
3 04/05-16:46:03.950964 [**] [1:10001:0] "ICMP received" [**] [Priority: 0] (ICMP) 192.168.206.1 -> 192.168.206.128
4 04/05-16:46:04.971413 [**] [1:10001:0] "ICMP received" [**] [Priority: 0] (ICMP) 192.168.206.1 -> 192.168.206.128
5
```

2. **Alert:** Rule action. Snort will generate an alert when the set condition is met.
icmp: Protocol we use can be TCP, ICMP, or HTTP
Any:Source IP. Snort will look at all sources.
Any:Source IP. Snort will look at all ports.
->: from source to destination
msg:"ICMP received" : Snort message will be displayed in alert
Sid: 10001: Snort rule ID. Remember all numbers smaller than 1,000,000 are reserved; this is why we are starting with 1,000,001. (You may use any number, as long as it's greater than 1,000,000.)

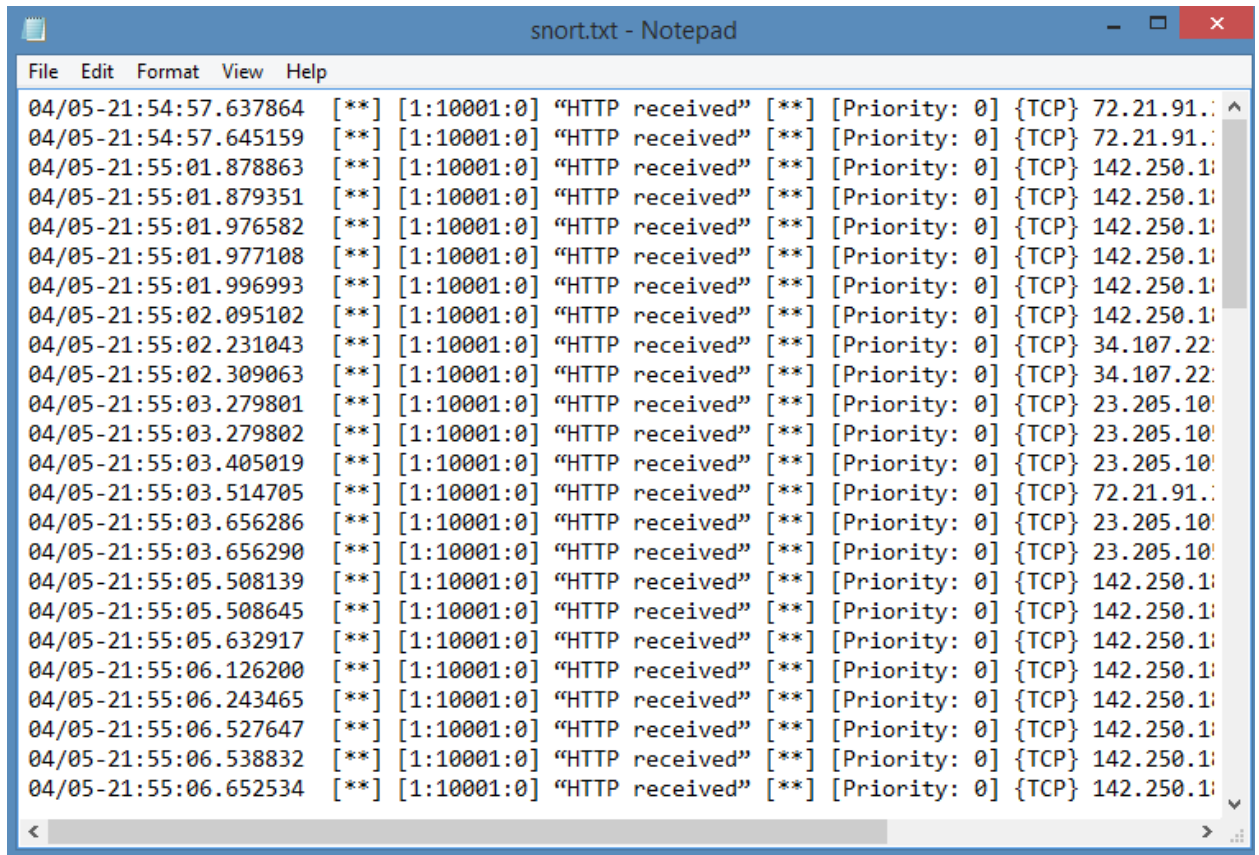


```
1 # Copyright 2001-2022 Sourcefire, Inc. All Rights Reserved.
2 #
3 # This file contains (i) proprietary rules that were created, tested and certified by
4 # Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
5 # Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
6 # Sourcefire and other third parties (the "GPL Rules") that are distributed under the
7 # GNU General Public License (GPL), v2.
8 #
9 # The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
10 # by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
11 # owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
12 # their respective creators. Please see http://www.snort.org/snort-team/ for a
13 # list of third party owners and their respective copyrights.
14 #
15 # In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
16 # to the VRT Certified Rules License Agreement (v2.0).
17 #
18 #-----
19 # LOCAL RULES
20 #-----
21
22 #alert icmp any any -> any any (msg: "ICMP received"; sid: 10001;)
23 alert tcp any any -> any any (msg: "ICMP received"; sid: 10001;)
24
25
26
27
```

3.



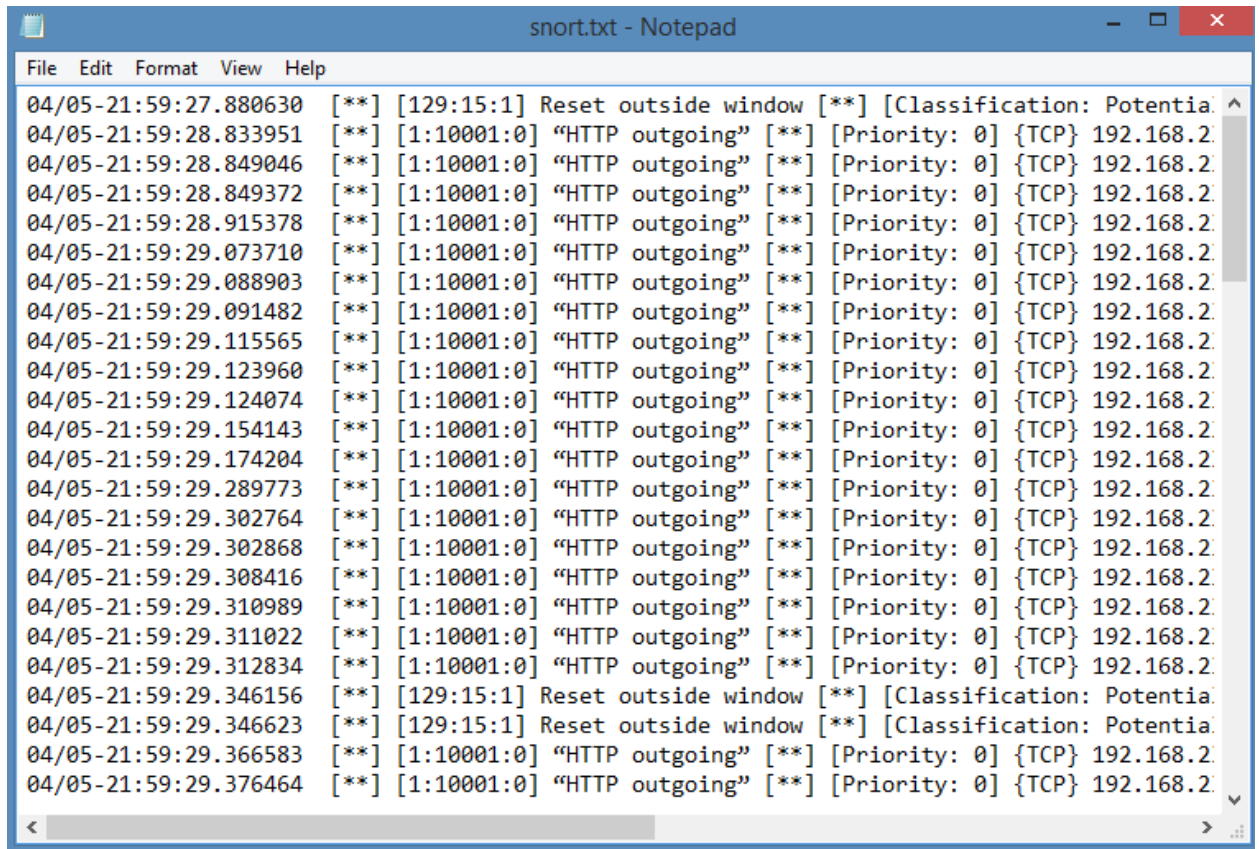
```
1 04/05-16:50:41.927241 [**] [1:10001:0] "ICMP received" [**] [Priority: 0] (TCP) 65.55.44.109:443 -> 192.168.206.128:49199
2 04/05-16:50:41.958637 [**] [1:10001:0] "ICMP received" [**] [Priority: 0] (TCP) 65.55.44.109:443 -> 192.168.206.128:49199
3
```



```
04/05-21:54:57.637864  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 72.21.91.1
04/05-21:54:57.645159  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 72.21.91.1
04/05-21:55:01.878863  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
04/05-21:55:01.879351  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
04/05-21:55:01.976582  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
04/05-21:55:01.977108  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
04/05-21:55:01.996993  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
04/05-21:55:02.095102  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
04/05-21:55:02.231043  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 34.107.22
04/05-21:55:02.309063  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 34.107.22
04/05-21:55:03.279801  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 23.205.10
04/05-21:55:03.279802  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 23.205.10
04/05-21:55:03.405019  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 23.205.10
04/05-21:55:03.514705  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 72.21.91.1
04/05-21:55:03.656286  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 23.205.10
04/05-21:55:03.656290  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 23.205.10
04/05-21:55:05.508139  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
04/05-21:55:05.508645  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
04/05-21:55:05.632917  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
04/05-21:55:06.126200  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
04/05-21:55:06.243465  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
04/05-21:55:06.527647  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
04/05-21:55:06.538832  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
04/05-21:55:06.652534  [**] [1:10001:0] "HTTP received" [**] [Priority: 0] {TCP} 142.250.1
```

4.

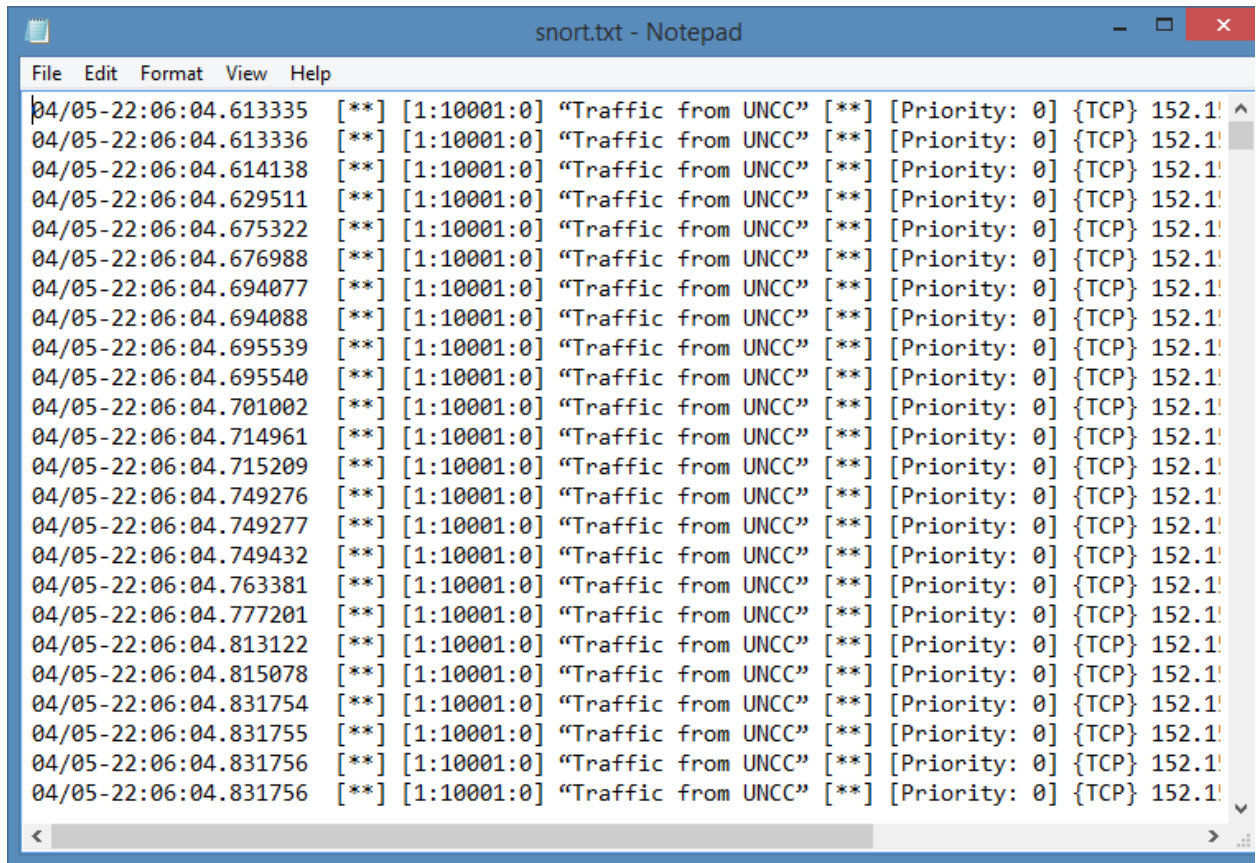
Rule: alert tcp any 80 -> any any (msg: "HTTP received"; sid: 10001;)



```
04/05-21:59:27.880630  [**] [129:15:1] Reset outside window [**] [Classification: Potentia
04/05-21:59:28.833951  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:28.849046  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:28.849372  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:28.915378  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.073710  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.088903  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.091482  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.115565  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.123960  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.124074  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.154143  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.174204  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.289773  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.302764  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.302868  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.308416  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.310989  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.311022  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.312834  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.346156  [**] [129:15:1] Reset outside window [**] [Classification: Potentia
04/05-21:59:29.346623  [**] [129:15:1] Reset outside window [**] [Classification: Potentia
04/05-21:59:29.366583  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
04/05-21:59:29.376464  [**] [1:10001:0] "HTTP outgoing" [**] [Priority: 0] {TCP} 192.168.2
```

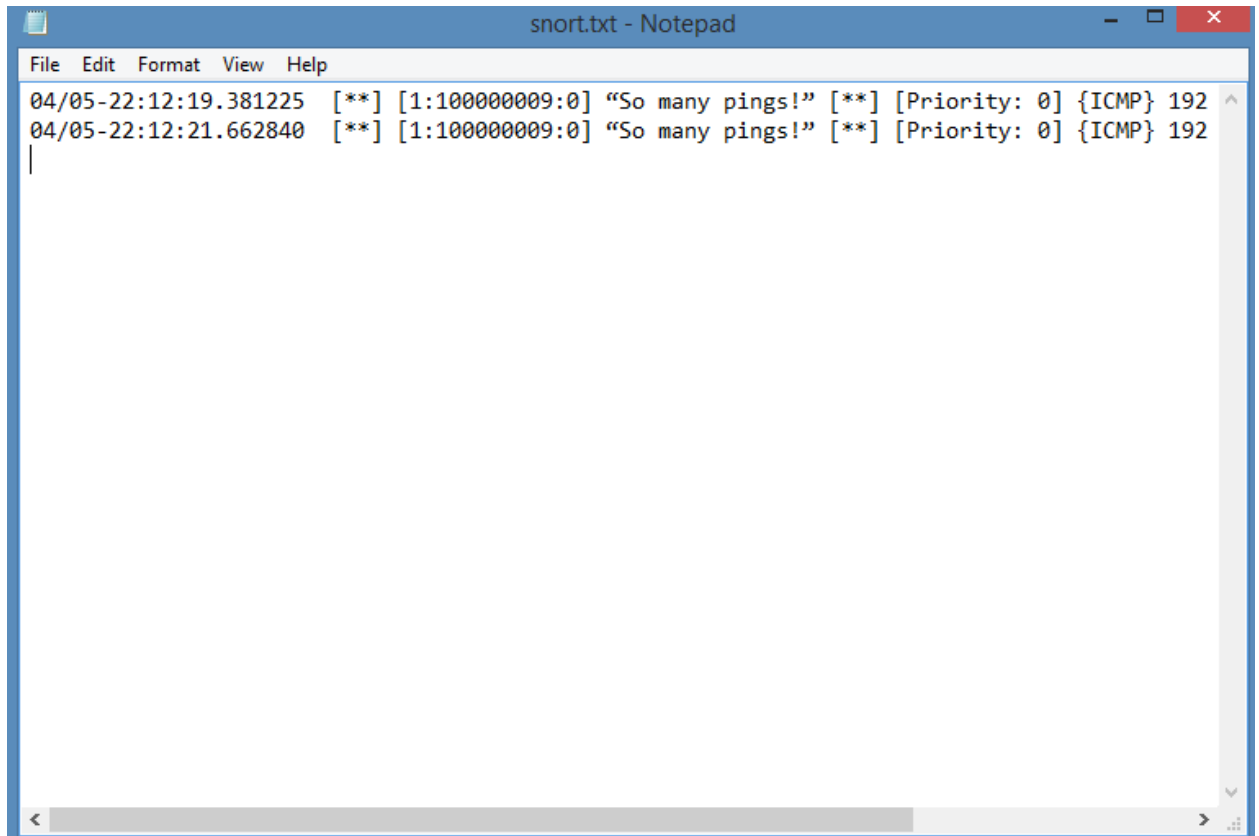
5.

Rule: alert tcp any any -> any 80 (msg: "HTTP outgoing"; sid: 10001;)



```
snort.txt - Notepad
File Edit Format View Help
04/05-22:06:04.613335 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.613336 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.614138 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.629511 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.675322 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.676988 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.694077 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.694088 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.695539 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.695540 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.701002 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.714961 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.715209 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.749276 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.749277 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.749432 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.763381 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.777201 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.813122 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.815078 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.831754 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.831755 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.831756 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
04/05-22:06:04.831756 [**] [1:10001:0] "Traffic from UNCC" [**] [Priority: 0] {TCP} 152.15.38.60
```

6. Rule: **alert tcp 152.15.38.60 any -> \$HOME_NET any (msg: "Traffic from UNCC"; sid: 10001;)**
7. The log file does not show any logs because there has to be 8 pings for the filter to detect it.
8. Yes, there are logs in the log file because we reached the threshold of 8 pings. The detection filter detected pings past 8.



```
snort.txt - Notepad
File Edit Format View Help
04/05-22:12:19.381225 [**] [1:100000009:0] "So many pings!" [**] [Priority: 0] {ICMP} 192
04/05-22:12:21.662840 [**] [1:100000009:0] "So many pings!" [**] [Priority: 0] {ICMP} 192
|
```

9. The reason that there are no logs for 2 pings and logs for 10 pings is because there is a rule in the detection filter that makes it so that 8 pings is the threshold required before logs are made.