

**IDS detection system:**

- set up the following four Suricata scenarios and submit the results to Canvas.
- (part 1) 25%
  - create a Suricata rule that alerts when a browser attempts to access a URL with the string "oracle" in the URL.
  - submit the rule you create.

IDS-Router:

[illegible]

```

root@8b25e32f830b:/home# wget -O - https://www.oracle.com
--2023-12-02 01:39:05-- https://www.oracle.com/
Resolving www.oracle.com (www.oracle.com)... 104.92.230.120, 104.92.230.120, 2600:141b:1c00:2289::a15, ...
Connecting to www.oracle.com (www.oracle.com)[104.92.230.120]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'STDOUT'

-
[<=>] 0 --.-KB/s
!DOCTYPE html><html lang="en-US"><head><meta charset="utf-8"><meta name="referrer" content="no-referrer-when-downgrade"><meta name="viewport" device-width, initial-scale=1.0"/><meta name="facebook-domain-verification" content="oijeioeqkuqvqoqfgdyhfdyjsnsvgf"><meta name="title" | Cloud Applications and Cloud Platform"/><meta name="description" content="Oracle offers a comprehensive and fully integrated stack of cloud cloud platform services."/><meta name="keywords" content="enterprise, applications, software, database, middleware, fusions, business, h><meta name="robots" content="index, follow"/><meta name="site" content="CustomerStory"/><meta name="siteid" content="us"/><meta name="count S"/><meta name="country" content="United States"/><meta name="Language" content="en"/><meta name="page_type" content="Home"/><title>Oracle ons and Cloud Platform/<title><link rel="preconnect" href="https://tms.oracle.com/" crossorigin="anonymous"><link rel="preconnect" href="https://n.com/" crossorigin="anonymous"><link rel="preconnect" href="https://consent.trustarc.com/" crossorigin="anonymous"><link rel="preconnect" href="https://oracleinfinity.io/" crossorigin="anonymous"><link rel="dns-prefetch" href="https://dc.oracleinfinity.io/" crossorigin="anonymous"/><link rel="prefetch" href="https://oracle.112.267.net/" crossorigin="anonymous"/><link rel="dns-prefetch" href="https://s.go-mpulse.net/" crossorigin="anonymous"/><efetch" href="https://c.go-mpulse.net/" crossorigin="anonymous"/><link rel="preload" href="https://www.oracle.com/asset/web/fonts/oraclesans

```

- submit the alert log (fast.log) lines that Suricata creates when the rule is triggered.

IDS-router:

```
certs core eve.json fast.log files stats.log suricata-start.log suricata.log
root@8b25e32f830b:/var/log/suricata# cat fast.log
12/02/2023-01:39:05.763988  [**] [1:1000001:1] HTTPS access to a domain containing 'oracle' [**] [Classification: Potential Co
iority: 1] {TCP} 10.9.0.11:48582 -> 104.92.230.120:443
12/02/2023-01:39:05.763988  [**] [1:1000001:1] HTTPS access to a domain containing 'oracle' [**] [Classification: Potential Co
iority: 1] {TCP} 10.9.0.11:48582 -> 104.92.230.120:443
root@8b25e32f830b:/var/log/suricata# cd /var/lib/suricata/
root@8b25e32f830b:/var/lib/suricata# cd rules/
```

part 4) 25%

- create a Suricata rule that detects a content text string from the lassie.txt file on Host 1
- submit the rule you create.

IDS-Router:

```
GNU nano 4.8 suricata.rules
#alert tcp [91.151.93.46,91.179.100.21,91.186.57.241,91.19.226.42,91.192.81.77,91.193.18.143,91.199.41.47,91.199.41.70,91.200.101.151,91.201.65.29] any ->
#alert tcp [91.203.145.114,91.203.5.141,91.204.6.136,91.206.228.132,91.206.228.91,91.208.162.145,91.208.184.123,91.208.197.221,91.208.197.41,91.208.206.56]
#alert tcp [91.208.92.87,91.212.55.208,91.213.233.138,91.213.8.130,91.213.8.89,91.218.20.104,91.219.236.77,91.219.237.160,91.219.238.120,91.219.238.148] an
#alert tcp [91.219.238.221,91.219.245.62,91.219.29.94,91.219.30.55,91.219.60.67,91.223.82.197,91.224.90.35,91.228.52.211,91.228.52.73,91.228.52.8] any -> $
#alert tcp [91.228.53.49,91.229.76.124,91.231.182.136,91.233.116.51,91.245.255.87,91.250.81.52,91.32.51.56,91.33.83.253,91.39.85.207,91.43.48.245] any -> $
#alert tcp [91.45.188.172,91.46.212.89,91.47.232.55,91.47.29.131,91.63.236.173,91.65.103.44,91.65.127.133,91.65.82.207,91.66.2.91,91.66.5.17] any -> $HOME
#alert tcp [91.7.37.181,91.89.218.178,91.92.109.126,91.96.222.143,92.104.160.187,92.116.141.195,92.116.157.141,92.116.209.77,92.117.21.22,92.117.53.235] an
#alert tcp [92.117.82.80,92.119.159.105,92.119.159.25,92.143.37.49,92.148.137.89,92.176.200.1,92.196.6.74,92.200.251.84,92.204.40.241,92.205.129.7] any ->
#alert tcp [92.205.161.164,92.205.17.93,92.206.39.138,92.222.172.56,92.222.216.91,92.222.79.186,92.223.105.174,92.243.0.179,92.243.0.63,92.243.20.101] any
#alert tcp [92.243.29.88,92.244.31.28,92.247.48.183,92.249.143.119,92.252.82.172,92.27.150.46,92.27.150.47,92.3.200.1,92.32.77.156,92.33.251.235] any -> $H
#alert tcp [92.34.140.243,92.35.20.235,92.35.68.2,92.38.162.88,92.42.14.204,92.50.86.110,92.60.36.153,92.60.37.105,93.104.101.135,93.115.27.81] any -> $HOME
#alert tcp [93.115.29.13,93.115.86.4,93.115.86.6,93.115.91.66,93.115.97.242,93.144.53.75,93.160.17.86,93.177.65.182,93.177.67.43,93.177.73.210] any -> $HOME
#alert tcp [93.177.73.98,93.177.75.10,93.180.154.94,93.180.157.154,93.186.200.169,93.190.143.41,93.198.249.99,93.207.170.8,93.208.129.46,93.212.45.95] any
#alert tcp [93.212.48.26,93.214.196.192,93.215.174.245,93.219.47.69,93.230.138.233,93.231.15.202,93.231.253.53,93.232.180.156,93.234.129.206,93.239.179.86]
#alert tcp [93.41.144.27,93.41.149.117,93.55.235.232,93.56.117.22,93.58.252.139,93.72.78.202,93.73.210.69,93.90.194.106,93.90.202.104,93.90.203.42] any ->
#alert tcp [93.93.115.138,93.93.118.87,93.95.227.108,93.95.227.119,93.95.228.131,93.95.228.51,93.95.228.74,93.95.230.102,93.95.230.245,93.95.230.34] any ->
#alert tcp [93.95.230.78,93.95.230.85,93.95.231.110,93.95.231.115,93.95.88.13,93.99.255.254,94.100.6.13,94.100.6.27,94.100.6.30,94.100.6.72] any -> $HOME
#alert tcp [94.103.188.80,94.114.128.208,94.130.10.251,94.130.129.15,94.130.142.182,94.130.185.68,94.130.189.8,94.130.227.162,94.130.51.212,94.131.119.29]
#alert tcp [94.131.15.74,94.134.165.128,94.134.250.242,94.140.112.158,94.140.114.233,94.140.115.114,94.140.115.60,94.140.120.130,94.143.137.213,94.154.159
#alert tcp [94.156.128.10,94.156.144.52,94.156.175.120,94.156.175.85,94.156.175.86,94.156.71.201,94.158.246.117,94.16.104.159,94.16.105.206,94.16.113.114]
#alert tcp [94.16.113.135,94.16.113.89,94.16.114.231,94.16.114.247,94.16.114.254,94.16.116.156,94.16.116.187,94.16.118.23,94.16.118.250,94.16.120.204] any
#alert tcp [94.16.122.61,94.16.123.171,94.16.123.67,94.16.123.97,94.16.147.223,94.168.120.10,94.172.116.122,94.177.8.200,94.199.214.229,94.220.95.44] any ->
#alert tcp [94.226.67.25,94.229.153.180,94.23.121.150,94.23.148.66,94.23.149.136,94.23.150.210,94.23.172.32,94.23.221.17,94.23.247.42,94.23.248.158] any ->
#alert tcp [94.23.68.187,94.23.76.52,94.242.53.228,94.242.59.47,94.254.94.45,94.255.138.67,94.26.73.162,94.32.66.15,94.33.216.26,94.46.171.151] any -> $HOME
#alert tcp [94.46.171.221,94.46.171.245,94.46.207.86,94.46.221.3,94.62.42.3,95.110.254.231,95.111.230.178,95.111.243.215,95.112.40.247,95.141.83.146] any ->
#alert tcp [95.141.83.155,95.142.39.48,95.147.86.242,95.153.31.38,95.153.31.8,95.153.32.22,95.154.25.29,95.160.212.6,95.164.34.180,95.164.35.207] any -> $H
#alert tcp [95.175.17.147,95.179.160.189,95.182.138.55,95.211.136.23,95.211.138.51,95.211.138.7,95.211.147.99,95.211.205.138,95.211.208.141,95.211.210.72]
#alert tcp [95.211.4.174,95.213.151.221,95.214.52.187,95.214.53.216,95.214.53.96,95.215.45.138,95.215.45.188,95.216.107.100,95.216.115.85,95.216.12.30] any
#alert tcp [95.216.13.120,95.216.13.55,95.216.140.159,95.216.146.117,95.216.154.9,95.216.168.133,95.216.193.39,95.216.19.41,95.216.195.161,95.216.198.252]
#alert tcp [95.216.201.161,95.216.202.181,95.216.20.80,95.216.209.129,95.216.212.22,95.216.212.222,95.216.2.172,95.216.22.22,95.216.22.24,95.216.225.44] any
#alert tcp [95.216.22.87,95.216.23.120,95.216.27.105,95.216.3.171,95.216.33.30,95.216.33.58,95.216.35.176,95.216.35.84,95.216.96.44,95.216.98.55] any -> $H
#alert tcp [95.217.112.218,95.217.112.243,95.217.112.245,95.217.121.38,95.217.129.223,95.217.130.121,95.217.133.157,95.217.135.55,95.217.14.105,95.217.14.1
#alert tcp [95.217.143.118,95.217.143.122,95.217.143.124,95.217.143.126,95.217.15.125,95.217.156.221,95.217.16.212,95.217.2.206,95.217.223.54,95.217.231.11
#alert tcp [95.217.28.112,95.217.30.201,95.217.39.117,95.217.62.4,95.217.6.94,95.217.71.73,95.217.72.151,95.222.140.85,95.222.201.54,95.230.122.163] any ->
#alert tcp [95.23.231.184,95.244.174.23,95.252.253.236,95.49.103.140,95.80.25.230,95.85.90.130,95.88.27.20,95.98.52.206,95.99.18.146,96.126.105.219] any ->
#alert tcp [96.227.137.219,96.227.69.26,96.234.144.211,96.236.202.72,96.238.110.80,96.244.8.163,96.245.83.39,96.255.232.74,96.52.9.223,96.65.68.193] any ->
#alert tcp [97.107.139.108,97.113.176.32,97.113.225.197,97.119.99.179,98.115.87.163,98.116.182.144,98.121.68.25,98.128.173.1,98.128.175.45,98.128.175.69] a
#alert tcp [98.155.3.106,98.168.31.145,98.210.71.205,98.24.213.184,98.29.204.31,98.36.193.226,98.44.43.113,98.57.245.167,98.96.164.184,99.111.119.180] any
alert tcp any any -> any any (msg:"woof"; content:"dog"; sid:10000012; rev:1;)
```

- submit the alert log (fast.log) lines that Suricata creates when the rule is triggered.

## IDS-Router

```
root@ee8af94c5362:/var/lib/suricata/rules# suricata -i eth1
i: suricata: This is Suricata version 7.0.2 RELEASE running in SYSTEM mode
i: threads: Threads created -> W: 12 FM: 1 FR: 1 Engine started.
^Ci: suricata: Signal Received. Stopping engine.
i: device: eth1: packets: 14, drops: 0 (0.00%), invalid checksum: 0
root@ee8af94c5362:/var/lib/suricata/rules# cd /var/log/suricata/
root@ee8af94c5362:/var/log/suricata# ls
certs eve.json files suricata-start.log
core fast.log stats.log suricata.log
root@ee8af94c5362:/var/log/suricata# more fast.log
12/01/2023-19:39:09.518251 [**] [1:10000012:1] woof [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:50874 -> 10.9.0.5:9090
12/01/2023-19:39:45.919956 [**] [1:10000012:1] woof [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:53860 -> 10.9.0.5:9090
```

## Host A

```
root@d6f5f1bae98e:/# nc -l 9090
Lassie is a fictional female Rough Collie dog and is featured in a 1938 short story by Eric Knight that was later expanded to a 1940 full-length novel, Lassie Come-Home. Knight's portrayal of Lassie bears some features in common with another fictional female collie of the same name, featured in the British writer Elizabeth Gaskell's 1859 short story "The Half Brothers". In "The Half Brothers", Lassie is loved only by her young master and guides the adults back to where two boys are lost in a snowstorm.

Knight's novel was filmed by Metro-Goldwyn-Mayer in 1943 as Lassie Come Home, with a dog named Pal playing Lassie. Pal then appeared with the stage name "Lassie" in six other MGM feature films through 1951. Pal's owner and trainer, Rudd Weatherwax, then acquired the Lassie name and trademark from MGM and appeared with Pal (as "Lassie") at rodeos, fairs, and similar events across America in the early 1950s. In 1954, the television series Lassie debuted and, over the next 19 years, a succession of Pal's descendants appeared on the series. The "Lassie" character has appeared in radio, television, film, toys, comic books, animated series, juvenile novels, and other media. Pal's descendants continue to play Lassie today.root@d6f5f1bae98e:/# nc -l 9090
Lassie is a fictional female Rough Collie dog and is featured in a 1938 short story by Eric Knight that was later expanded to a 1940 full-length novel, Lassie Come-Home. Knight's portrayal of Lassie bears some features in common with another fictional female collie of the same name, featured in the British writer Elizabeth Gaskell's 1859 short story "The Half Brothers". In "The Half Brothers", Lassie is loved only by her young master and guides the adults back to where two boys are lost in a snowstorm.

Knight's novel was filmed by Metro-Goldwyn-Mayer in 1943 as Lassie Come Home, with a dog named Pal playing Lassie. Pal then appeared with the stage name "Lassie" in six other MGM feature films through 1951. Pal's owner and trainer, Rudd Weatherwax, then acquired the Lassie name and trademark from MGM and appeared with Pal (as "Lassie") at rodeos, fairs, and similar events across America in the early 1950s. In 1954, the television series Lassie debuted and, over the next 19 years, a succession of Pal's descendants appeared on the series. The "Lassie" character has appeared in radio, television, film, toys, comic books, animated series, juvenile novels, and other media. Pal's descendants continue to play Lassie today.
```

## Host1

```
^C
root@e742bd5b2d56:/home/seed# cat lassie.txt | nc 10.9.0.5 9090
root@e742bd5b2d56:/home/seed# cat lassie.txt | nc 10.9.0.5 9090
```

## part 2 25%

- create a Suricata rule that alerts when any host is pinged.
- submit the rule you create.



[illegible]

Alert log:

```
root@ee8af94c5362:/var/log/suricata# suricata -i eth1
i: suricata: This is Suricata version 7.0.2 RELEASE running in SYSTEM mode
i: threads: Threads created -> W: 12 FW: 1 FR: 1 Engine started.
^Ci: suricata: Signal Received. Stopping engine.
i: device: eth1, packets: 445, drops: 0 (0.00%), invalid checksum: 0
root@ee8af94c5362:/var/log/suricata# more fast.log
12/01/2023-22:21:30.647367 [**] [1:10000002:1] ICMP Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-22:21:30.647676 [**] [1:10000002:1] ICMP Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 10.9.0.5:0 -> 192.168.60.5:0
12/01/2023-22:21:51.439393 [**] [1:10000002:1] ICMP Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-22:21:51.439449 [**] [1:10000002:1] ICMP Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 10.9.0.5:0 -> 192.168.60.5:0
root@ee8af94c5362:/var/log/suricata#
```

(part 3) 25%

- create a Suricata rule that alerts when telnet traffic is seen on the network.
- submit the rule you create.
- submit the alert log (fast.log) lines that Suricata creates when the rule is triggered.

Host1:

```
root@e742bd5b2d56:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d6f5f1bae98e login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.133.1-microsoft-standard-WSL2 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Dec 1 22:31:49 UTC 2023 from 192.168.60.5 on pts/2
seed@d6f5f1bae98e:~$
```

Host A:

```
root@d6f5f1bae98e:/# nc -l -p 9090
```

## IDS-Router

```
GNU nano 2.8 /var/lib/suricata/rules/suricata.rules
!alert tcp [91.208.92.0/24,91.212.55.200,91.213.233.138,91.213.8.130,91.213.8.89,91.218.20.104,91.219.237.77,91.219.237.160,91.219.238.120,91.219.238.140]
!alert tcp [91.219.238.221,91.219.205.62,91.219.219.94,91.219.30.55,91.219.60.67,91.223.82.197,91.224.90.35,91.228.52.211,91.228.52.73,91.228.52.81] any
!alert tcp [91.228.53.49,91.229.76.124,91.231.182.136,91.233.116.51,91.245.255.87,91.250.01.22,91.32.51.66,91.33.83.253,91.39.85.207,91.43.48.240] any
!alert tcp [91.45.188.172,91.46.212.89,91.47.232.55,91.47.29.131,91.63.236.173,91.65.183.44,91.65.127.133,91.65.82.207,91.66.2.91,91.66.5.17] any -> $H
!alert tcp [91.7.37.181,91.89.218.178,91.92.109.126,91.96.222.143,92.104.160.187,92.116.141.195,92.116.157.141,92.116.209.77,92.117.21.22,92.117.53.230]
!alert tcp [92.117.42.0/24,92.119.159.185,92.119.159.25,92.143.37.49,92.148.137.89,92.176.200.1,92.196.6.74,92.200.251.84,92.204.40.241,92.205.159.71] any
!alert tcp [92.205.161.164,92.205.17.93,92.206.39.118,92.222.172.56,92.222.216.91,92.222.79.186,92.223.185.174,92.243.0.179,92.243.0.63,92.243.20.101]
!alert tcp [92.243.29.88,92.244.31.28,92.247.48.183,92.249.143.119,92.252.82.172,92.27.150.46,92.27.150.47,92.3.200.1,92.32.77.156,92.33.251.235] any ->
!alert tcp [92.30.100.243,92.35.70.235,92.35.68.2,92.38.163.80,92.42.14.208,92.50.66.110,92.60.36.153,92.60.37.109,91.104.101.135,93.115.27.43] any ->
!alert tcp [93.115.29.13,93.115.46.4,93.115.46.4,93.115.91.66,93.115.97.242,93.144.53.75,93.160.17.86,93.177.65.182,93.177.67.43,93.177.73.210] any ->
!alert tcp [93.177.73.98,93.177.75.10,93.180.154.94,93.180.157.154,93.186.200.169,93.190.143.41,93.198.249.99,93.207.170.8,93.208.129.46,93.212.45.95]
!alert tcp [93.212.48.26,93.214.196.192,93.215.174.205,93.219.47.60,93.230.138.233,93.231.15.202,93.231.253.53,93.232.108.156,93.234.129.206,93.239.179]
!alert tcp [93.41.140.77,93.41.149.117,93.55.255.233,93.56.117.22,93.58.252.139,93.72.70.202,93.72.210.69,93.90.194.186,93.94.202.104,93.98.203.421] any
!alert tcp [93.93.115.138,93.93.118.87,93.95.227.108,93.95.227.119,93.95.228.131,93.95.228.51,93.95.228.74,93.95.230.182,93.95.230.245,93.95.230.34] any
!alert tcp [93.95.230.78,93.95.230.85,93.95.231.110,93.95.231.115,93.95.88.13,93.99.255.284,94.100.6.13,94.100.6.27,94.100.6.30,94.100.6.72] any -> $H
!alert tcp [94.103.188.80,94.110.120.208,94.130.16.253,94.130.129.15,94.130.142.182,94.130.185.68,94.130.189.0,94.130.227.162,94.139.51.212,94.131.119]
!alert tcp [94.131.15.74,94.134.165.128,94.134.250.242,94.140.112.158,94.140.114.233,94.140.115.114,94.140.115.69,94.140.120.130,94.143.137.213,94.154]
!alert tcp [94.156.128.10,94.156.144.52,94.156.175.120,94.156.175.85,94.156.175.86,94.156.71.201,94.158.246.117,94.16.104.159,94.16.105.206,94.16.113.3]
!alert tcp [94.16.113.135,94.16.113.89,94.16.114.211,94.16.114.247,94.16.114.254,94.16.116.116,94.16.116.157,94.16.118.21,94.16.118.250,94.16.120.200]
!alert tcp [94.16.122.61,94.16.123.171,94.16.123.67,94.16.123.97,94.16.147.223,94.160.120.10,94.172.116.122,94.177.8.200,94.199.214.229,94.220.95.44] any
!alert tcp [94.226.67.25,94.229.153.180,94.23.121.150,94.23.148.66,94.23.149.136,94.23.150.210,94.23.172.32,94.23.221.17,94.23.247.42,94.23.248.158] any
!alert tcp [94.23.60.107,94.23.96.82,94.202.53.228,94.202.69.47,94.250.94.85,94.255.138.67,94.26.73.162,94.32.66.15,94.33.216.26,94.46.171.153] any ->
!alert tcp [94.46.171.221,94.46.171.205,94.46.207.86,94.46.221.1,94.42.42.3,94.110.204.231,95.111.230.179,95.111.243.215,95.112.46.247,95.141.83.146] any
!alert tcp [95.141.83.155,95.142.39.48,95.147.86.242,95.153.31.38,95.153.31.8,95.153.32.22,95.154.25.29,95.160.212.6,95.164.34.108,95.164.35.207] any ->
!alert tcp [95.175.17.107,95.179.160.189,95.182.138.55,95.211.136.23,95.211.188.51,95.211.188.7,95.211.147.99,95.211.248.138,95.211.208.101,95.211.210]
!alert tcp [95.211.4.174,95.211.151.221,95.218.52.187,95.210.53.216,95.216.53.96,95.216.55.96,95.216.55.138,95.215.45.188,95.215.45.188,95.216.107.180,95.216.115.85,95.216.12.38]
!alert tcp [95.216.13.120,95.216.13.55,95.216.140.159,95.216.146.117,95.216.154.9,95.216.168.133,95.216.193.39,95.216.19.41,95.216.195.161,95.216.198.2]
!alert tcp [95.216.201.161,95.216.202.181,95.216.20.80,95.216.209.129,95.216.212.22,95.216.212.222,95.216.212.172,95.216.22.22,95.216.22.24,95.216.225.40]
!alert tcp [95.216.22.07,95.216.23.120,95.216.27.189,95.216.3.173,95.216.31.30,95.216.33.88,95.216.35.176,95.216.35.84,95.216.40.95,95.216.88.53] any ->
!alert tcp [95.217.112.210,95.217.112.243,95.217.112.245,95.217.121.38,95.217.129.223,95.217.129.223,95.217.130.121,95.217.133.157,95.217.135.55,95.217.14.105,95.217]
!alert tcp [95.217.143.118,95.217.143.122,95.217.143.124,95.217.143.126,95.217.15.125,95.217.156.221,95.217.16.212,95.217.2.206,95.217.223.84,95.217.23]
!alert tcp [95.217.25.112,95.217.30.203,95.217.30.117,95.217.62.4,95.217.6.94,95.217.71.72,95.217.72.151,95.222.140.85,95.222.201.54,95.230.122.163] any
!alert tcp [95.23.231.184,95.240.174.23,95.252.253.236,95.40.103.140,95.80.25.230,95.85.90.130,95.88.27.20,95.98.52.206,95.99.18.146,95.96.126.105.219] any
!alert tcp [96.227.137.219,96.227.69.26,96.234.144.211,96.236.202.72,96.238.110.88,96.244.8.163,96.245.83.39,96.255.232.74,96.52.9.223,96.65.68.193] any
!alert tcp [97.107.139.100,97.113.174.32,97.113.225.197,97.119.99.179,98.115.87.163,98.116.102.144,98.121.60.25,98.122.171.1,98.128.175.45,98.128.175.6]
!alert tcp [98.155.3.106,98.168.31.145,98.210.71.205,98.24.213.184,98.29.204.31,98.36.193.226,98.44.43.113,98.57.245.167,98.96.164.104,99.111.119.180]
!alert tcp any any -> any any (msg:"woof",content:"dog",sid:100000012;rev:1;)
!alert http any any -> any any (msg:"URL contains oracle",content:"oracle",http_uri:sid:100000001;rev:1;)
!alert icmp any any -> any any (msg:"icmp Ping Detected",sid:100000002;rev:1;)
alert tcp any any -> any 23 (msg:"Telnet Traffic Detected";sid:100000003;rev:1;)
```

## Alert:

```
root@eeBaf94c5362:/var/log/suricata# suricata -i eth1
i: suricata: This is Suricata version 7.0.2 RELEASE running in SYSTEM mode
i: threads: Threads created -> W: 12 FM: 1 FR: 1 Engine started.
^Ci: suricata: Signal Received. Stopping engine.
i: device: eth1: packets: 386, drops: 0 (0.00%), invalid checksum: 0
root@eeBaf94c5362:/var/log/suricata# more fast.log
12/01/2023-22:32:44.295731 [**] [1:10000003:1] Telnet Traffic Detected [**] [Classification: (null)] [Priority: 3] [TCP] 192.168.60.5:34558 -> 10.9.0.5:23
12/01/2023-22:32:47.976537 [**] [1:10000003:1] Telnet Traffic Detected [**] [Classification: (null)] [Priority: 3] [TCP] 192.168.60.5:35760 -> 10.9.0.5:23
root@eeBaf94c5362:/var/log/suricata#
```