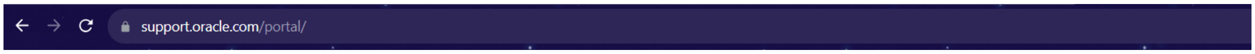
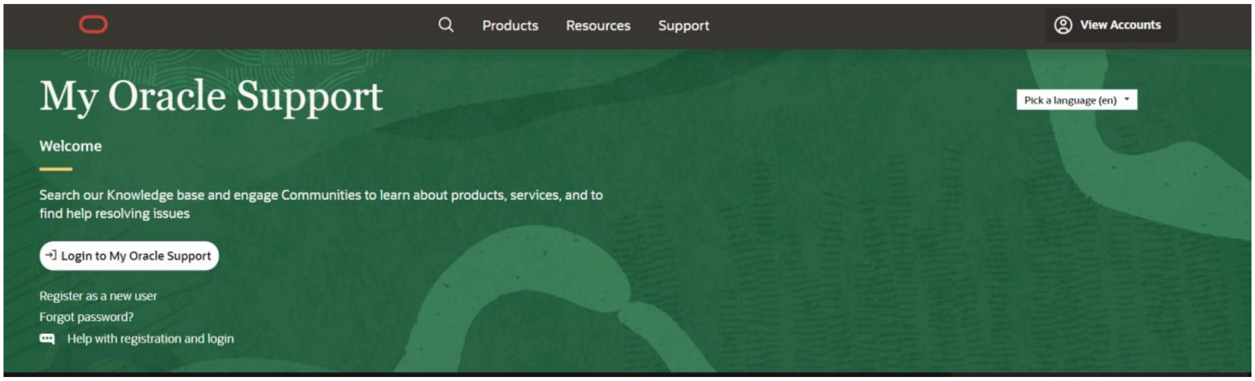
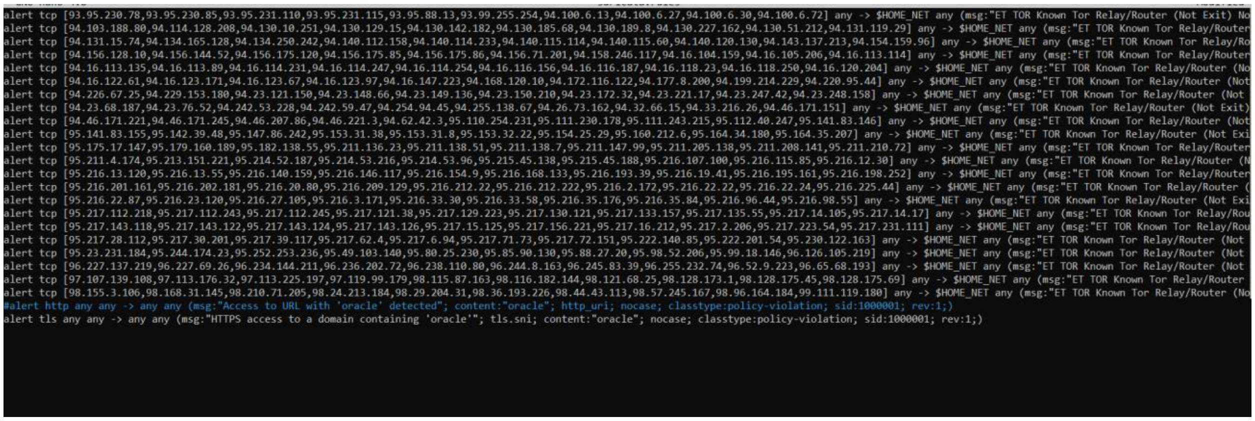
Practical – IDS

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

Screenshots:

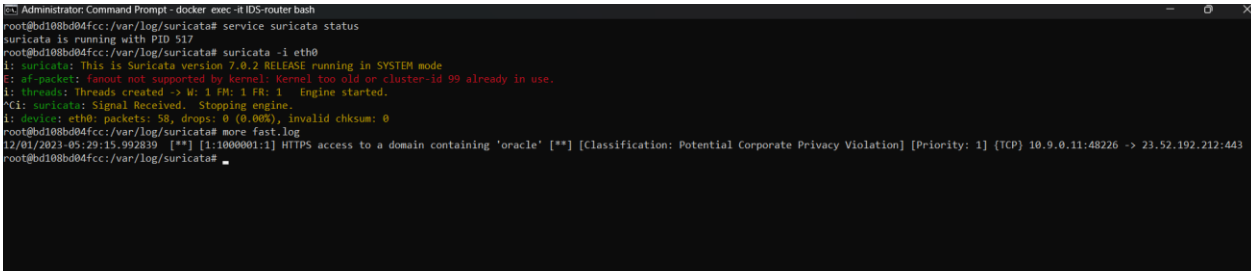



Products
Resources
Support
View Accounts
My Oracle Support
Welcome
Pick a language (en)
Search our Knowledge base and engage Communities to learn about products, services, and to find help resolving issues
Login to My Oracle Support
Register as a new user
Forgot password?
Help with registration and login



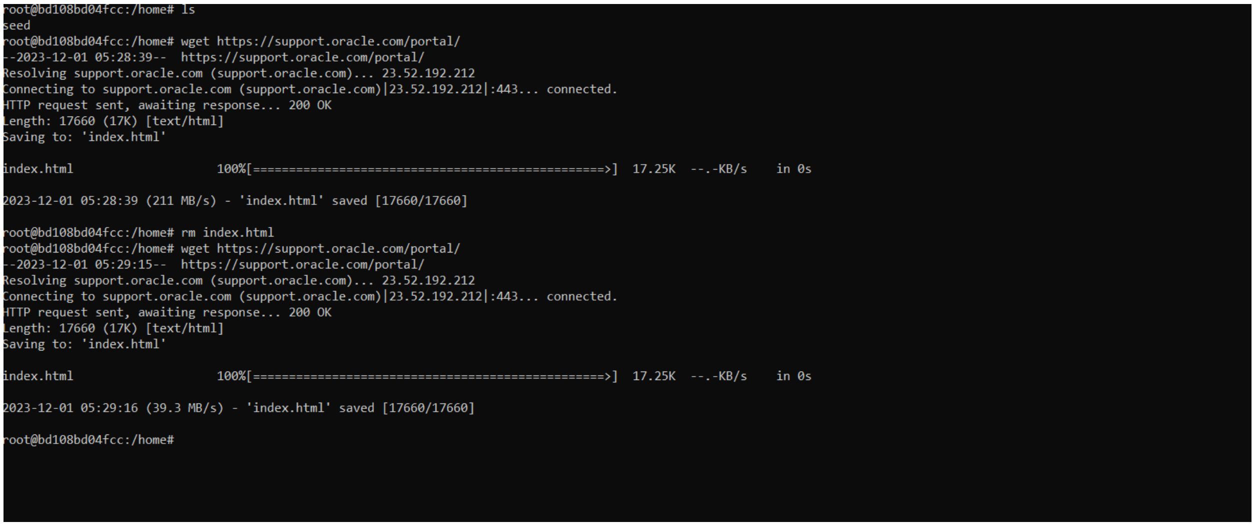
```
alert tcp [93.95.230.78,93.95.230.85,93.95.231.110,93.95.231.115,93.95.88.13,93.99.255.254,94.100.6.13,94.100.6.27,94.100.6.30,94.100.6.72] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exit) No
alert tcp [94.103.188.80,94.114.128.208,94.130.10.251,94.130.129.15,94.130.142.182,94.130.185.68,94.130.189.8,94.130.227.162,94.130.51.212,94.131.119.29] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router
alert tcp [94.131.15.74,94.134.165.128,94.134.250.242,94.140.112.158,94.140.114.233,94.140.115.114,94.140.115.60,94.140.120.130,94.143.137.213,94.154.159.96] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Ro
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (No
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not
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_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exit)
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exi
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (N
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exi
alert tcp [95.217.112.218,95.217.112.243,95.217.112.245,95.217.121.38,95.217.129.223,95.217.130.121,95.217.133.157,95.217.135.55,95.217.14.105,95.217.14.17] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Rou
alert tcp [95.217.143.118,95.217.143.122,95.217.143.124,95.217.143.126,95.217.15.125,95.217.156.221,95.217.16.212,95.217.2.206,95.217.223.54,95.217.231.111] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Rou
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (No
#alert http any any -> any any (msg:"Access to URL with 'oracle' detected"; content:"oracle"; http_uri; nocase; classtype:policy-violation; sid:1000001; rev:1;)
alert tls any any -> any any (msg:"HTTPS access to a domain containing 'oracle'"; tls.sni; content:"oracle"; nocase; classtype:policy-violation; sid:1000001; rev:1;)
```

Rule: alert tls any any -> any any (msg:"HTTPS access to a domain containing 'oracle'"; tls.sni; content:"oracle"; nocase; classtype:policy-violation; sid:1000001; rev:1;)


Administrator: Command Prompt - docker exec -it IDS-router bash

```
root@bd108bd04fcc:/var/log/suricata# service suricata status
suricata is running with PID 517
root@bd108bd04fcc:/var/log/suricata# suricata -i eth0
i: suricata: This is Suricata version 7.0.2 RELEASE running in SYSTEM mode
E: af-packet: fanout not supported by kernel: Kernel too old or cluster-id 99 already in use.
i: threads: Threads created -> W: 1 FM: 1 FR: 1   Engine started.
^Ci: suricata: Signal Received.  Stopping engine.
i: device: eth0: packets: 58, drops: 0 (0.00%), invalid chksum: 0
root@bd108bd04fcc:/var/log/suricata# more fast.log
12/01/2023-05:29:15.992839  [**] [1:1000001:1] HTTPS access to a domain containing 'oracle' [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 10.9.0.11:48226 -> 23.52.192.212:443
root@bd108bd04fcc:/var/log/suricata# _
```

Wget:



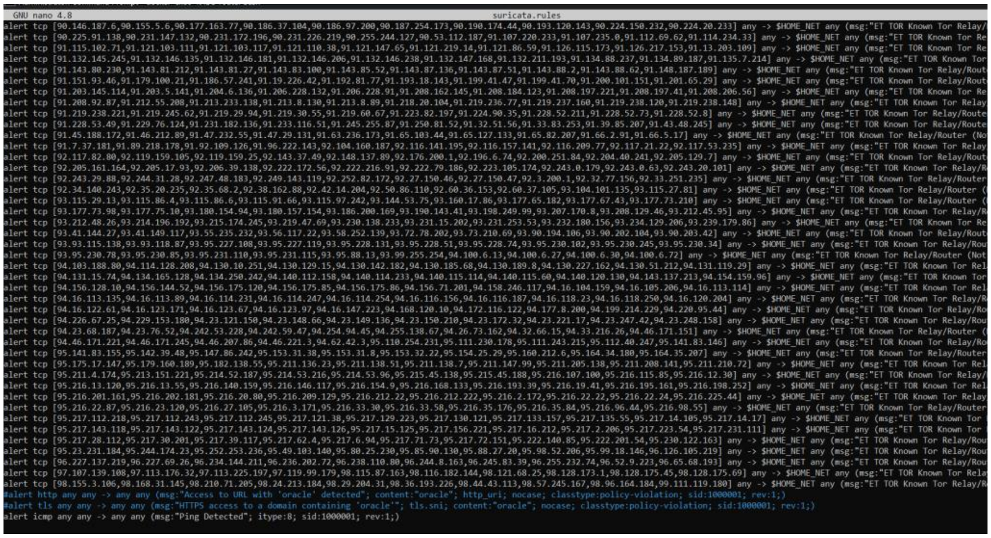
```
root@bd108bd04fcc:/home# ls
seed
root@bd108bd04fcc:/home# wget https://support.oracle.com/portal/
--2023-12-01 05:28:39--  https://support.oracle.com/portal/
Resolving support.oracle.com (support.oracle.com)... 23.52.192.212
Connecting to support.oracle.com (support.oracle.com)|23.52.192.212|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17660 (17K) [text/html]
Saving to: 'index.html'

index.html                 100%[==================================================>]  17.25K  --.-KB/s    in 0s

2023-12-01 05:28:39 (211 MB/s) - 'index.html' saved [17660/17660]

root@bd108bd04fcc:/home# rm index.html
root@bd108bd04fcc:/home# wget https://support.oracle.com/portal/
--2023-12-01 05:29:15--  https://support.oracle.com/portal/
Resolving support.oracle.com (support.oracle.com)... 23.52.192.212
Connecting to support.oracle.com (support.oracle.com)|23.52.192.212|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17660 (17K) [text/html]
Saving to: 'index.html'

index.html                 100%[==================================================>]  17.25K  --.-KB/s    in 0s

2023-12-01 05:29:16 (39.3 MB/s) - 'index.html' saved [17660/17660]

root@bd108bd04fcc:/home#
```

Fast.log file contents:

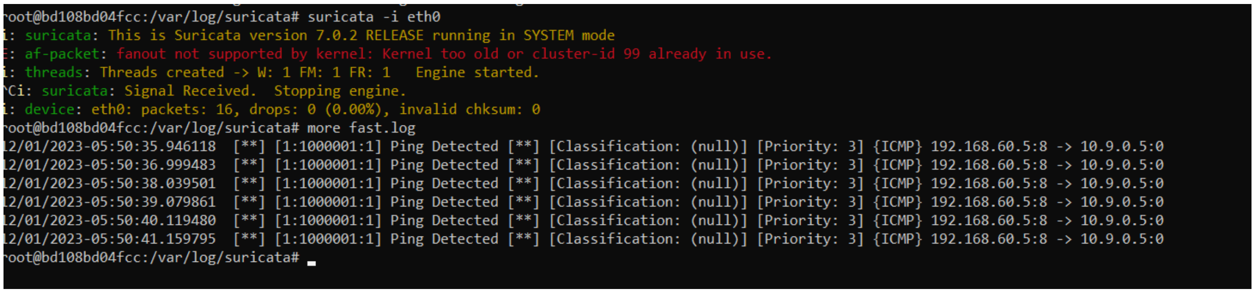
12/01/2023-05:29:15.992839 [**] [1:1000001:1] HTTPS access to a domain containing 'oracle' [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 10.9.0.11:48226 -> 23.52.192.212:443

- (part 2) 25%
    - create a Suricata rule that alerts when any host is pinged
    - submit the rule you create
    - submit the alert log (fast.log) lines that Suricata creates when the rule is triggered

Screenshots:



```
  GNU nano 4.8                                                          suricata.rules
alert tcp [90.146.187.6,90.155.5.6,90.177.163.77,90.186.37.104,90.186.97.200,90.187.254.173,90.190.174.44,90.193.120.143,90.224.150.232,90.224.20.233] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/
alert tcp [90.225.91.138,90.231.147.132,90.231.172.196,90.231.226.219,90.255.244.127,90.53.112.187,91.107.220.233,91.107.235.0,91.112.69.62,91.114.234.33] any -> $HOME_NET any (msg:"ET TOR Known Tor Re
alert tcp [91.115.102.71,91.121.103.111,91.121.103.117,91.121.110.38,91.121.147.65,91.121.219.14,91.121.86.59,91.126.115.173,91.126.217.153,91.13.203.109] any -> $HOME_NET any (msg:"ET TOR Known Tor Re
alert tcp [91.132.145.245,91.132.146.135,91.132.146.181,91.132.146.206,91.132.146.238,91.132.147.168,91.132.211.193,91.134.88.237,91.134.89.187,91.135.7.214] any -> $HOME_NET any (msg:"ET TOR Known Tor
alert tcp [91.143.80.230,91.143.81.212,91.143.81.27,91.143.83.100,91.143.85.52,91.143.87.136,91.143.87.51,91.143.88.2,91.143.88.62,91.148.187.189] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Rout
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Rout
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Re
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Route
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Route
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_NET any (msg:"ET TOR Known Tor Relay/Router (No
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Rout
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/R
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router
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_NET any (msg:"ET TOR Known Tor Relay/Router (
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_NET any (msg:"ET TOR Known Tor Relay/Router (
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/R
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Re
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Rout
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Rou
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_NET any (msg:"ET TOR Known Tor Relay/Router (Not
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Rel
alert tcp [94.131.15.74,94.134.165.128,94.134.250.242,94.140.112.158,94.140.114.233,94.140.115.114,94.140.115.60,94.140.120.130,94.143.137.213,94.154.159.96] any -> $HOME_NET any (msg:"ET TOR Known Tor
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Rel
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/R
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Ro
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Rou
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_NET any (msg:"ET TOR Known Tor Relay/Router (
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Ro
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Rel
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Rel
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router
alert tcp [95.217.112.218,95.217.112.243,95.217.112.245,95.217.121.38,95.217.129.223,95.217.130.121,95.217.133.157,95.217.135.55,95.217.14.105,95.217.14.17] any -> $HOME_NET any (msg:"ET TOR Known Tor
alert tcp [95.217.143.118,95.217.143.122,95.217.143.124,95.217.143.126,95.217.15.125,95.217.156.221,95.217.16.212,95.217.2.206,95.217.223.54,95.217.231.111] any -> $HOME_NET any (msg:"ET TOR Known Tor
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Rou
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Rou
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Rou
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Rela
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/R
#alert http any any -> any any (msg:"Access to URL with 'oracle' detected"; content:"oracle"; http_uri; nocase; classtype:policy-violation; sid:1000001; rev:1;)
#alert tls any any -> any any (msg:"HTTPS access to a domain containing 'oracle'"; tls.sni; content:"oracle"; nocase; classtype:policy-violation; sid:1000001; rev:1;)
alert icmp any any -> any any (msg:"Ping Detected"; itype:8; sid:1000001; rev:1;)
```

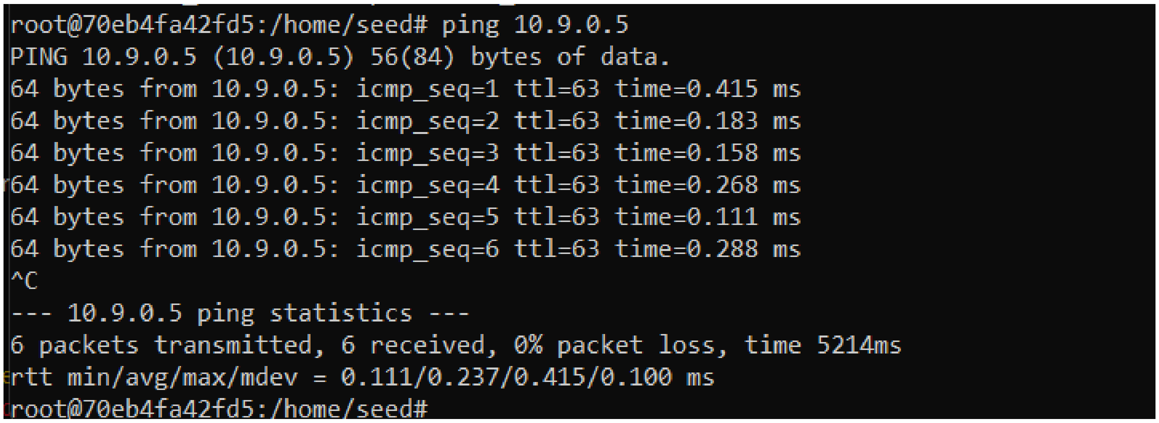


```
root@bd108bd04fcc:/var/log/suricata# suricata -i eth0
i: suricata: This is Suricata version 7.0.2 RELEASE running in SYSTEM mode
E: af-packet: fanout not supported by kernel: Kernel too old or cluster-id 99 already in use.
i: threads: Threads created -> W: 1 FM: 1 FR: 1   Engine started.
^Ci: suricata: Signal Received.  Stopping engine.
i: device: eth0: packets: 16, drops: 0 (0.00%), invalid chksum: 0
root@bd108bd04fcc:/var/log/suricata# more fast.log
12/01/2023-05:50:35.946118  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-05:50:36.999483  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-05:50:38.039501  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-05:50:39.079861  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-05:50:40.119480  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-05:50:41.159795  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
root@bd108bd04fcc:/var/log/suricata# 
```

Rule:

alert icmp any any -> any any (msg:"Ping Detected"; itype:8; sid:1000001; rev:1;)

pinging hostA from host1:



```
root@70eb4fa42fd5:/home/seed# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=63 time=0.415 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.183 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.158 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.268 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.111 ms
64 bytes from 10.9.0.5: icmp_seq=6 ttl=63 time=0.288 ms
^C
--- 10.9.0.5 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5214ms
rtt min/avg/max/mdev = 0.111/0.237/0.415/0.100 ms
root@70eb4fa42fd5:/home/seed#
```

Contents in fast.log file:

12/01/2023-05:50:35.946118 [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0

12/01/2023-05:50:36.999483 [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0

12/01/2023-05:50:38.039501 [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0

12/01/2023-05:50:39.079861 [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0

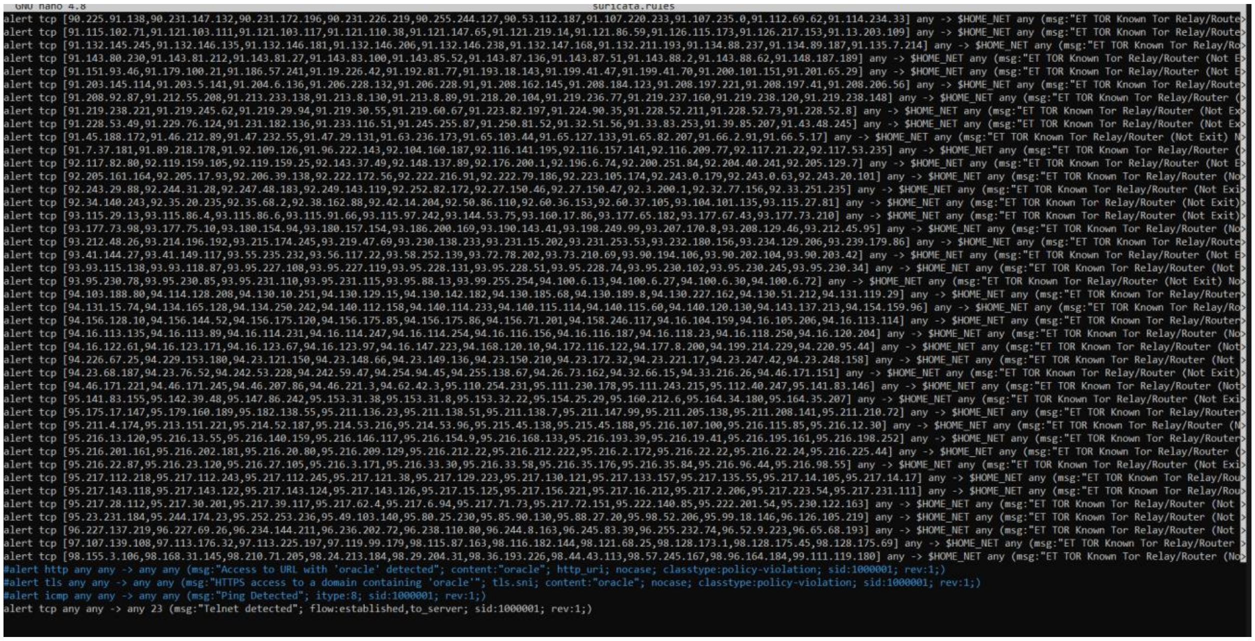
12/01/2023-05:50:40.119480 [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0

- 12/01/2023-05:50:41.159795 [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0

  (part 3) 25%

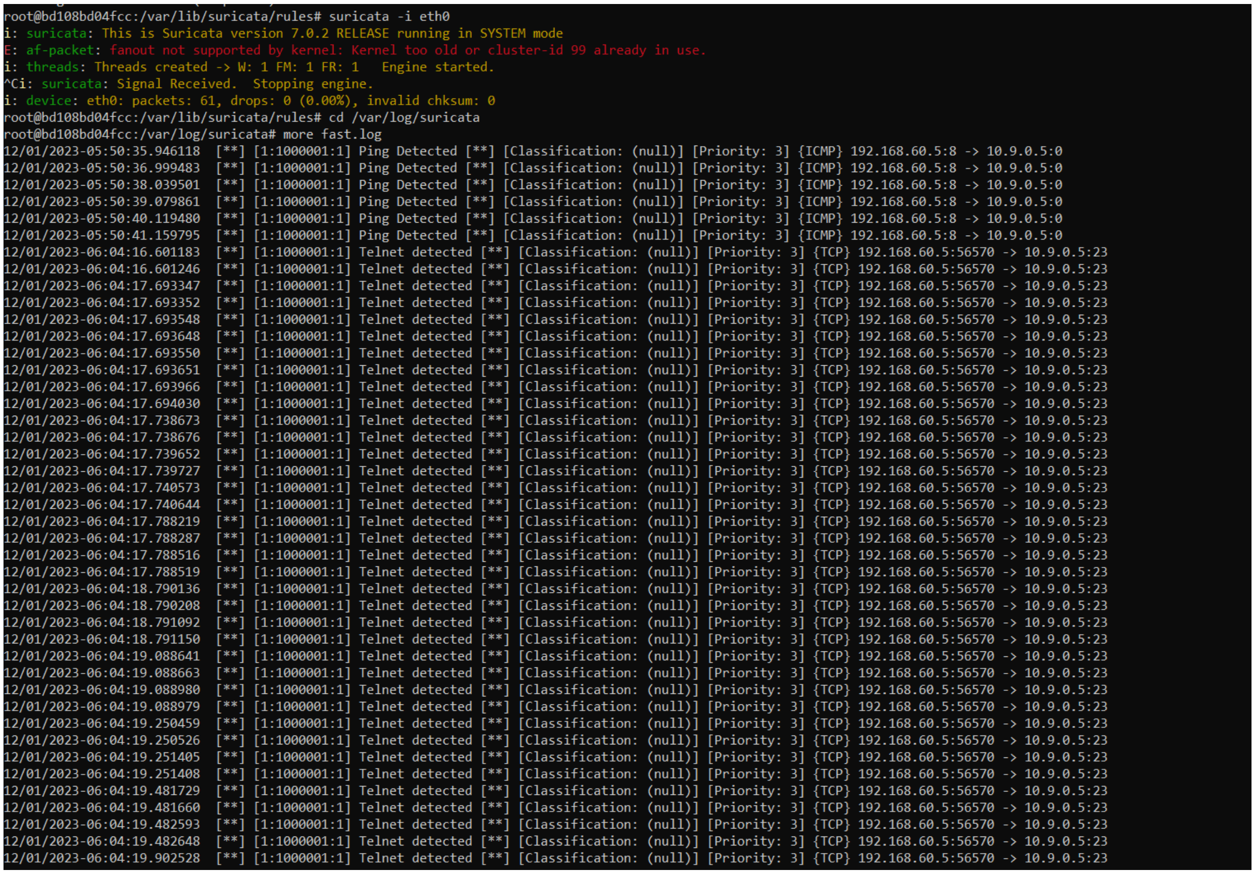
  - ○ create a Suricata rule that alerts when telnet traffic is seen on the network
  - ○ submit the rule you create
  - ○ submit the alert log (fast.log) lines that Suricata creates when the rule is triggered

Screenshots:

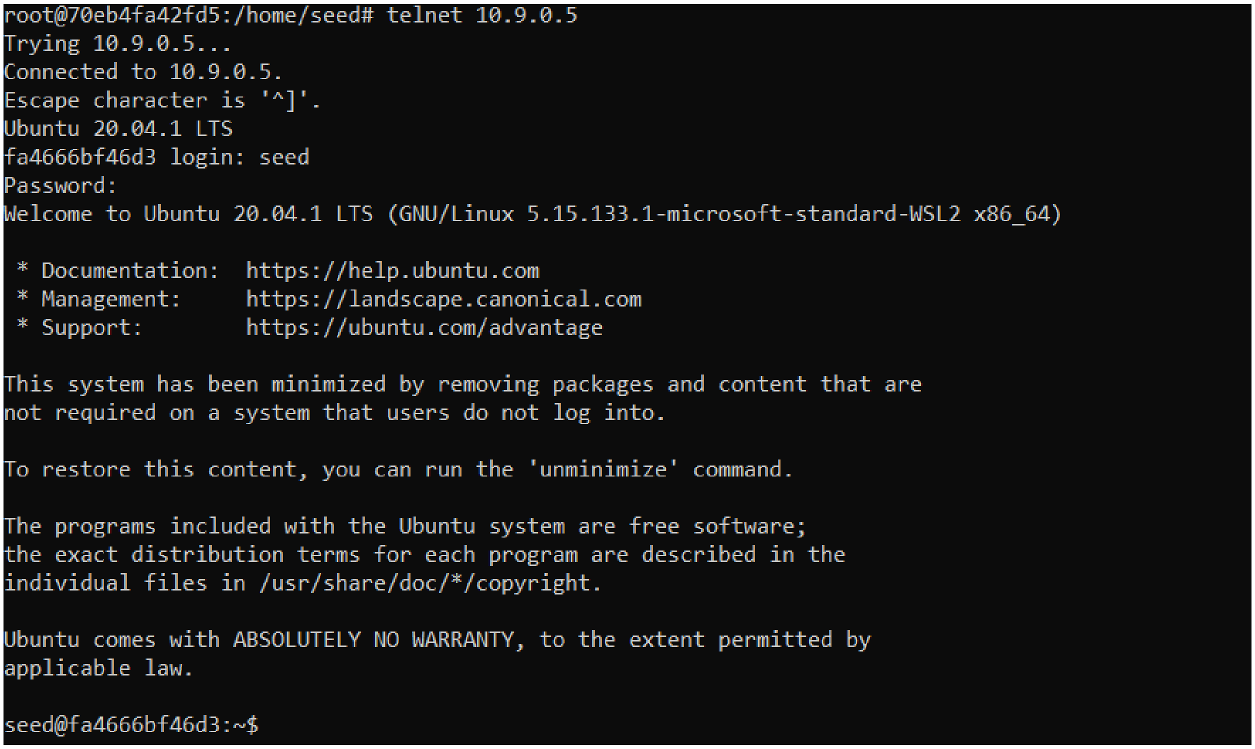


```
  GNU nano 4.8                                                        suricata.rules
alert tcp [90.225.91.138,90.231.147.132,90.231.172.196,90.231.226.219,90.255.244.127,90.53.112.187,91.107.220.233,91.107.235.0,91.112.69.62,91.114.234.33] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Route>
alert tcp [91.115.102.71,91.121.103.111,91.121.103.117,91.121.110.38,91.121.147.65,91.121.219.14,91.121.86.59,91.126.115.173,91.126.217.153,91.13.203.109] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Route>
alert tcp [91.132.145.245,91.132.146.135,91.132.146.181,91.132.146.206,91.132.146.238,91.132.147.168,91.132.211.193,91.134.88.237,91.134.89.187,91.135.7.214] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Ro>
alert tcp [91.143.80.230,91.143.81.212,91.143.81.27,91.143.83.100,91.143.85.52,91.143.87.136,91.143.87.51,91.143.88.2,91.143.88.62,91.148.187.189] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not E>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not E>
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Route>
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not Ex>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not Ex>
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_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exit) N>
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not E>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (No>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exi>
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_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exit)>
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_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exit)>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (No>
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Route>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not E>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not >
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_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exit) No>
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router>
alert tcp [94.131.15.74,94.134.165.128,94.134.250.242,94.140.112.158,94.140.114.233,94.140.115.114,94.140.115.60,94.140.120.130,94.143.137.213,94.154.159.96] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Ro>
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (No>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not >
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_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exit)>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exi>
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (N>
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exi>
alert tcp [95.217.112.218,95.217.112.243,95.217.112.245,95.217.121.38,95.217.129.223,95.217.130.121,95.217.133.157,95.217.135.55,95.217.14.105,95.217.14.17] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Rou>
alert tcp [95.217.143.118,95.217.143.122,95.217.143.124,95.217.143.126,95.217.15.125,95.217.156.221,95.217.16.212,95.217.2.206,95.217.223.54,95.217.231.111] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Rou>
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not >
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not >
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not >
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] any -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router >
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 -> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (No>
#alert http any any -> any any (msg:"Access to URL with 'oracle' detected"; content:"oracle"; http_uri; nocase; classtype:policy-violation; sid:1000001; rev:1;)
#alert tls any any -> any any (msg:"HTTPS access to a domain containing 'oracle'"; tls.sni; content:"oracle"; nocase; classtype:policy-violation; sid:1000001; rev:1;)
#alert icmp any any -> any any (msg:"Ping Detected"; itype:8; sid:1000001; rev:1;)
alert tcp any any -> any 23 (msg:"Telnet detected"; flow:established,to_server; sid:1000001; rev:1;)
```

Rule : alert tcp any any -> any 23 (msg:"Telnet detected"; flow:established,to_server; sid:1000001; rev:1;)



```
root@bd108bd04fcc:/var/lib/suricata/rules# suricata -i eth0
i: suricata: This is Suricata version 7.0.2 RELEASE running in SYSTEM mode
E: af-packet: fanout not supported by kernel: Kernel too old or cluster-id 99 already in use.
i: threads: Threads created -> W: 1 FM: 1 FR: 1   Engine started.
^Ci: suricata: Signal Received.  Stopping engine.
i: device: eth0: packets: 61, drops: 0 (0.00%), invalid chksum: 0
root@bd108bd04fcc:/var/lib/suricata/rules# cd /var/log/suricata
root@bd108bd04fcc:/var/log/suricata# more fast.log
12/01/2023-05:50:35.946118  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-05:50:36.999483  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-05:50:38.039501  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-05:50:39.079861  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-05:50:40.119480  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-05:50:41.159795  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.60.5:8 -> 10.9.0.5:0
12/01/2023-06:04:16.601183  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:16.601246  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.693347  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.693352  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.693548  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.693648  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.693550  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.693651  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.693966  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.694030  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.738673  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.738676  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.739652  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.739727  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.740573  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.740644  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.788219  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.788287  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.788516  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:17.788519  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:18.790136  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:18.790208  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:18.791092  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:18.791150  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:19.088641  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:19.088663  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:19.088980  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:19.088979  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:19.250459  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:19.250526  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:19.251405  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:19.251408  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:19.481729  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:19.481660  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:19.482593  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:19.482648  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
12/01/2023-06:04:19.902528  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:56570 -> 10.9.0.5:23
```



```
root@70eb4fa42fd5:/home/seed# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
fa4666bf46d3 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@fa4666bf46d3:~$
```

Contents in fast.log:

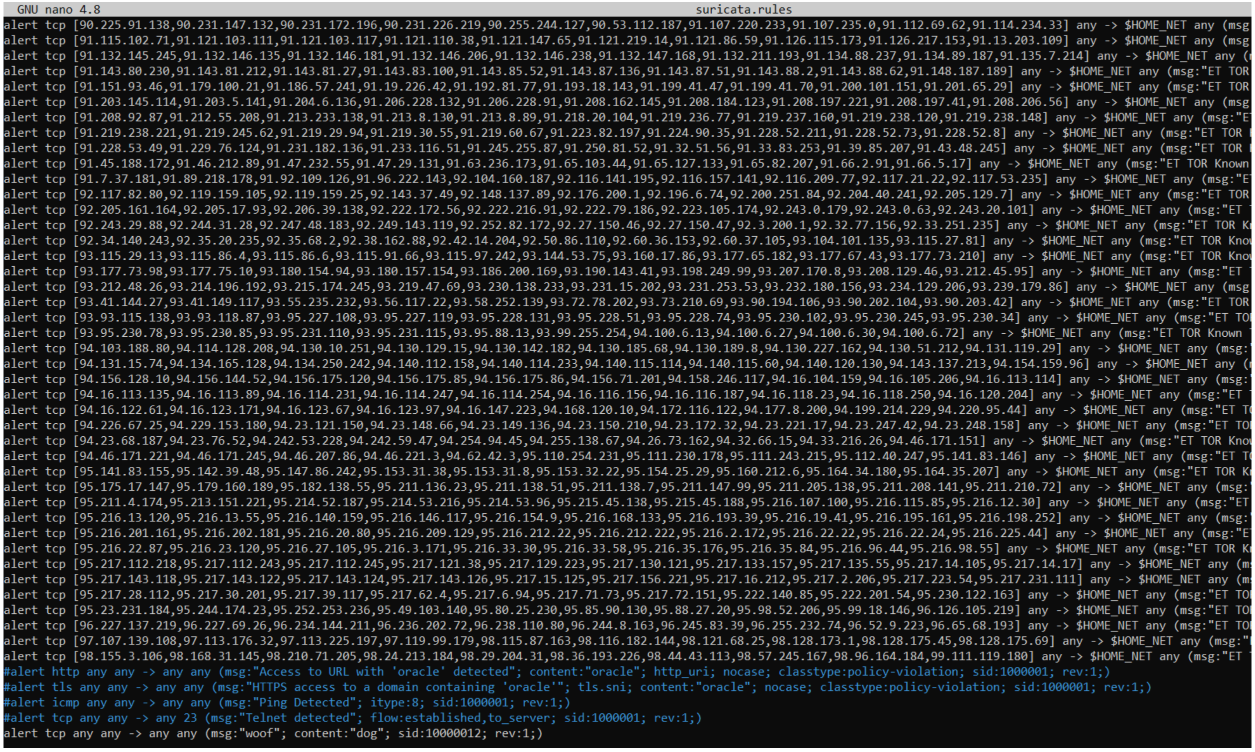
```
12/01/2023-05:50:35.946118  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3]
{ICMP} 192.168.60.5:8 -> 10.9.0.5:0

12/01/2023-05:50:36.999483  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3]
{ICMP} 192.168.60.5:8 -> 10.9.0.5:0

12/01/2023-05:50:38.039501  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3]
{ICMP} 192.168.60.5:8 -> 10.9.0.5:0

12/01/2023-05:50:39.079861  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3]
{ICMP} 192.168.60.5:8 -> 10.9.0.5:0

12/01/2023-05:50:40.119480  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3]
{ICMP} 192.168.60.5:8 -> 10.9.0.5:0

12/01/2023-05:50:41.159795  [**] [1:1000001:1] Ping Detected [**] [Classification: (null)] [Priority: 3]
{ICMP} 192.168.60.5:8 -> 10.9.0.5:0

12/01/2023-06:04:16.601183  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:16.601246  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.693347  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.693352  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.693548  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.693648  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.693550  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.693651  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.693966  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.694030  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.738673  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23
```

```
12/01/2023-06:04:17.738676  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.739652  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.739727  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.740573  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.740644  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.788219  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.788287  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.788516  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:17.788519  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:18.790136  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:18.790208  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:18.791092  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:18.791150  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.088641  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.088663  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.088980  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.088979  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23
```

```
12/01/2023-06:04:19.250459  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.250526  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.251405  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.251408  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.481729  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.481660  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.482593  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.482648  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.902528  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.902590  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.903509  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.903577  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.904621  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:19.904616  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:20.241471  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:20.241518  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

12/01/2023-06:04:20.560477  [**] [1:1000001:1] Telnet detected [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.60.5:56570 -> 10.9.0.5:23

--More--(76%)
```

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

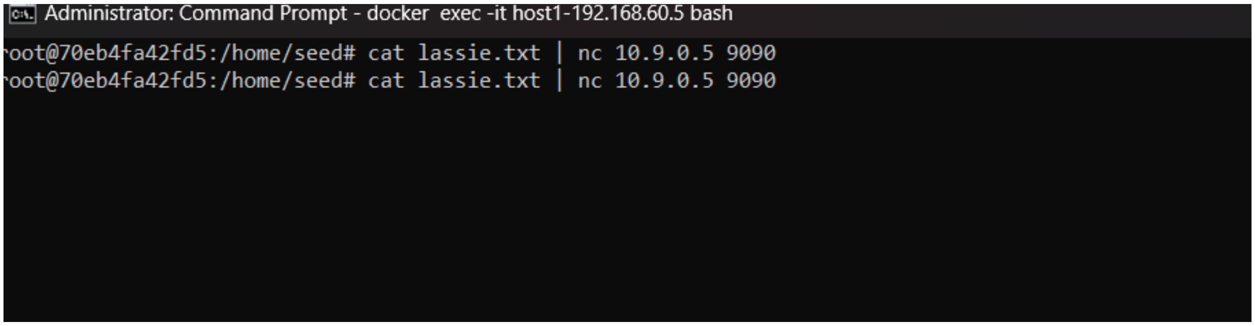
Screenshots:



```
  GNU nano 4.8                                                                                    suricata.rules
alert tcp [90.225.91.138,90.231.147.132,90.231.172.196,90.231.226.219,90.255.244.127,90.53.112.187,91.107.220.233,91.107.235.0,91.112.69.62,91.114.234.33] any -> $HOME_NET any (msg
alert tcp [91.115.102.71,91.121.103.111,91.121.103.117,91.121.110.38,91.121.147.65,91.121.219.14,91.121.86.59,91.126.115.173,91.126.217.153,91.13.203.109] any -> $HOME_NET any (msg
alert tcp [91.132.145.245,91.132.146.135,91.132.146.181,91.132.146.206,91.132.146.238,91.132.147.168,91.132.211.193,91.134.88.237,91.134.89.187,91.135.7.214] any -> $HOME_NET any (
alert tcp [91.143.80.230,91.143.81.212,91.143.81.27,91.143.83.100,91.143.85.52,91.143.87.136,91.143.87.51,91.143.88.2,91.143.88.62,91.148.187.189] any -> $HOME_NET any (msg:"ET TOR
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 -> $HOME_NET any (msg:"ET TOR
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] any -> $HOME_NET any (msg
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] any -> $HOME_NET any (msg:"E
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 -> $HOME_NET any (msg:"ET TOR
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 -> $HOME_NET any (msg:"ET TOR
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_NET any (msg:"ET TOR Known
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] any -> $HOME_NET any (msg:"E
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 -> $HOME_NET any (msg:"ET TOR
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 -> $HOME_NET any (msg:"ET
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 -> $HOME_NET any (msg:"ET TOR K
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_NET any (msg:"ET TOR Kno
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_NET any (msg:"ET TOR Kno
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 -> $HOME_NET any (msg:"ET
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] any -> $HOME_NET any (msg
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 -> $HOME_NET any (msg:"ET TOR
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 -> $HOME_NET any (msg:"ET TO
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_NET any (msg:"ET TOR Known
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] any -> $HOME_NET any (msg:
alert tcp [94.131.15.74,94.134.165.128,94.134.250.242,94.140.112.158,94.140.114.233,94.140.115.114,94.140.115.60,94.140.120.130,94.143.137.213,94.154.159.96] any -> $HOME_NET any (
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] any -> $HOME_NET any (msg:
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 -> $HOME_NET any (msg:"ET
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 -> $HOME_NET any (msg:"ET T
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 -> $HOME_NET any (msg:"ET TO
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_NET any (msg:"ET TOR Kno
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 -> $HOME_NET any (msg:"ET T
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 -> $HOME_NET any (msg:"ET TOR K
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] any -> $HOME_NET any (msg:
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 -> $HOME_NET any (msg:"ET
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] any -> $HOME_NET any (msg:
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 -> $HOME_NET any (msg:"E
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 -> $HOME_NET any (msg:"ET TOR K
alert tcp [95.217.112.218,95.217.112.243,95.217.112.245,95.217.121.38,95.217.129.223,95.217.130.121,95.217.133.157,95.217.135.55,95.217.14.105,95.217.14.17] any -> $HOME_NET any (m
alert tcp [95.217.143.118,95.217.143.122,95.217.143.124,95.217.143.126,95.217.15.125,95.217.156.221,95.217.16.212,95.217.2.206,95.217.223.54,95.217.231.111] any -> $HOME_NET any (m
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 -> $HOME_NET any (msg:"ET TO
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 -> $HOME_NET any (msg:"ET TO
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 -> $HOME_NET any (msg:"ET TO
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] any -> $HOME_NET any (msg:"
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 -> $HOME_NET any (msg:"ET
#alert http any any -> any any (msg:"Access to URL with 'oracle' detected"; content:"oracle"; http_uri; nocase; classtype:policy-violation; sid:1000001; rev:1;)
#alert tls any any -> any any (msg:"HTTPS access to a domain containing 'oracle'"; tls.sni; content:"oracle"; nocase; classtype:policy-violation; sid:1000001; rev:1;)
#alert icmp any any -> any any (msg:"Ping Detected"; itype:8; sid:1000001; rev:1;)
#alert tcp any any -> any 23 (msg:"Telnet detected"; flow:established,to_server; sid:1000001; rev:1;)
alert tcp any any -> any any (msg:"woof"; content:"dog"; sid:10000012; rev:1;)
```

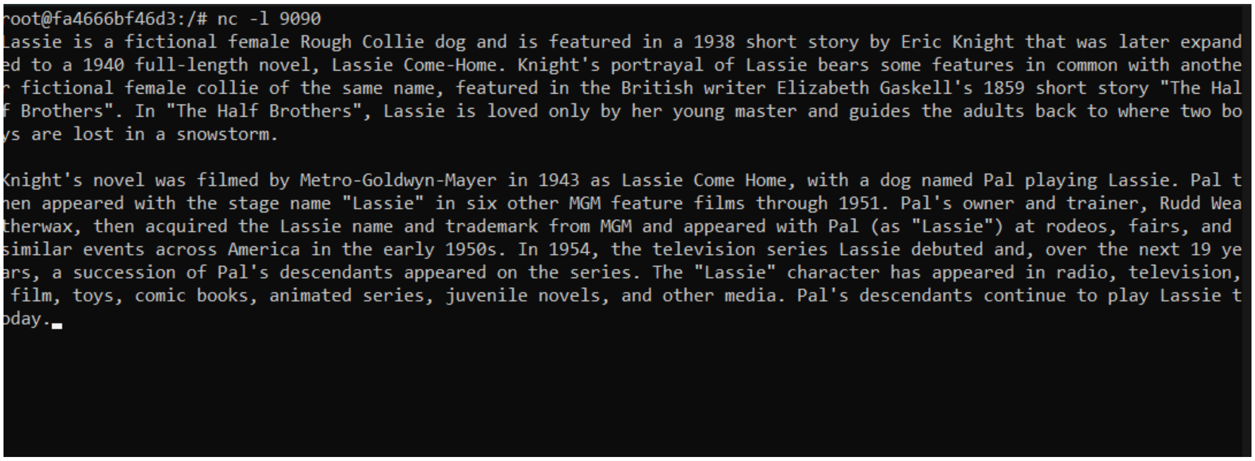
Rule: alert tcp any any -> any any (msg:"woof"; content:"dog"; sid:10000012; rev:1;)

Host1:

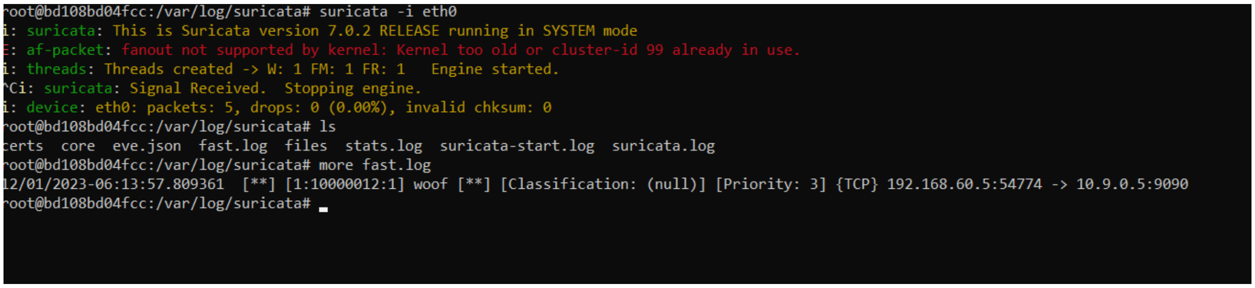


```
Administrator: Command Prompt - docker  exec -it host1-192.168.60.5 bash
root@70eb4fa42fd5:/home/seed# cat lassie.txt | nc 10.9.0.5 9090
root@70eb4fa42fd5:/home/seed# cat lassie.txt | nc 10.9.0.5 9090
```

HostA:



```
root@fa4666bf46d3:/# 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 expand
ed to a 1940 full-length novel, Lassie Come-Home. Knight's portrayal of Lassie bears some features in common with anothe
r fictional female collie of the same name, featured in the British writer Elizabeth Gaskell's 1859 short story "The Hal
f Brothers". In "The Half Brothers", Lassie is loved only by her young master and guides the adults back to where two bo
ys 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 t
hen appeared with the stage name "Lassie" in six other MGM feature films through 1951. Pal's owner and trainer, Rudd Wea
therwax, 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 ye
ars, 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 t
oday.
```



```
root@bd108bd04fcc:/var/log/suricata# suricata -i eth0
i: suricata: This is Suricata version 7.0.2 RELEASE running in SYSTEM mode
E: af-packet: fanout not supported by kernel: Kernel too old or cluster-id 99 already in use.
i: threads: Threads created -> W: 1 FM: 1 FR: 1   Engine started.
^Ci: suricata: Signal Received.  Stopping engine.
i: device: eth0: packets: 5, drops: 0 (0.00%), invalid chksum: 0
root@bd108bd04fcc:/var/log/suricata# ls
certs  core  eve.json  fast.log  files  stats.log  suricata-start.log  suricata.log
root@bd108bd04fcc:/var/log/suricata# more fast.log
12/01/2023-06:13:57.809361  [**] [1:10000012:1] woof [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:54774 -> 10.9.0.5:9090
root@bd108bd04fcc:/var/log/suricata#
```

Contents in fast.log:

12/01/2023-06:13:57.809361 [**] [1:10000012:1] woof [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.60.5:54774 -> 10.9.0.5:9090