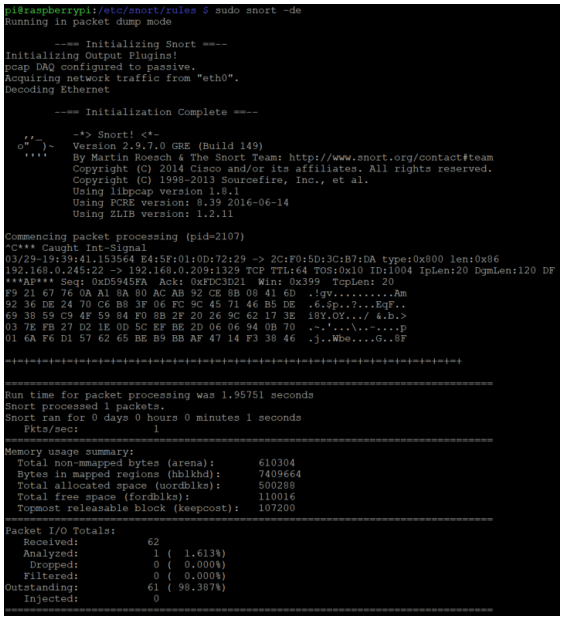
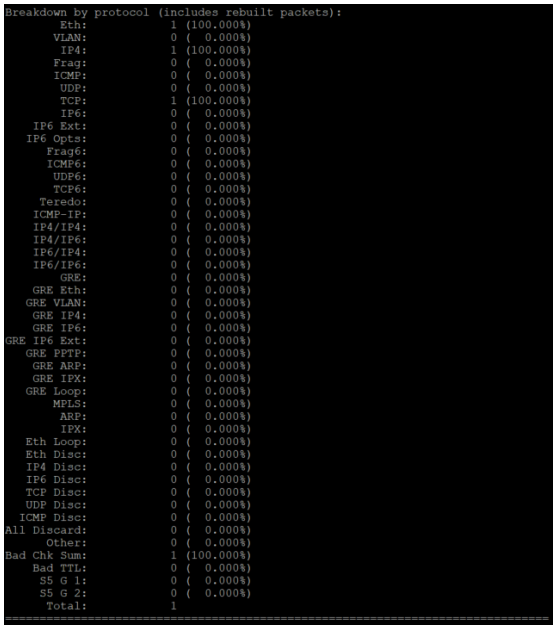
Task 1: Discovery Flag: Display data-link headers and the application layer data

- **Solution:**

Sudo snort -de

  - d: show application data in transit
  - e: show the data link layer headers





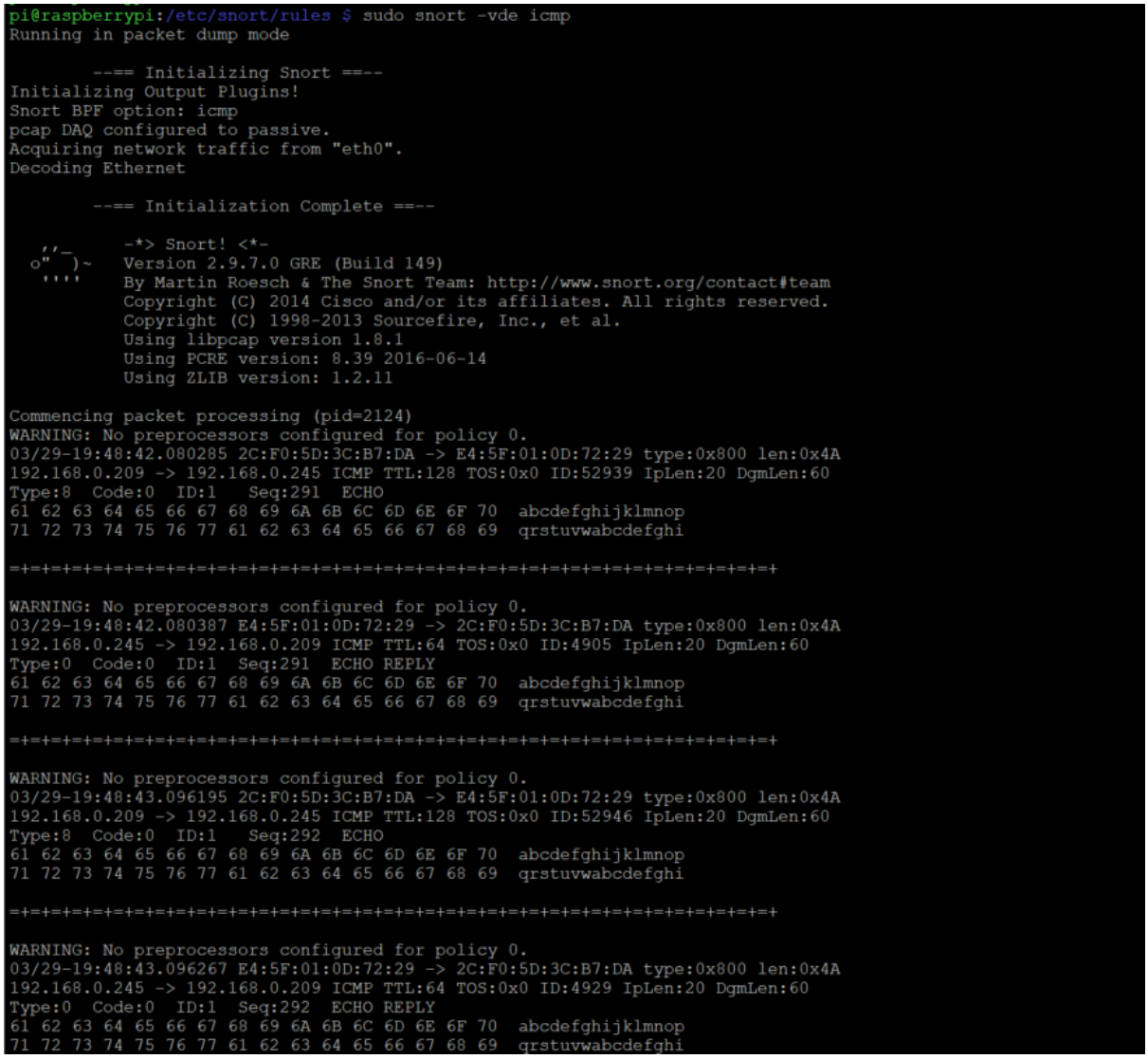
research: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node4.html

Task 2: Capture only ICMP

- **Solution:**

  Sudo snort -vde icmp

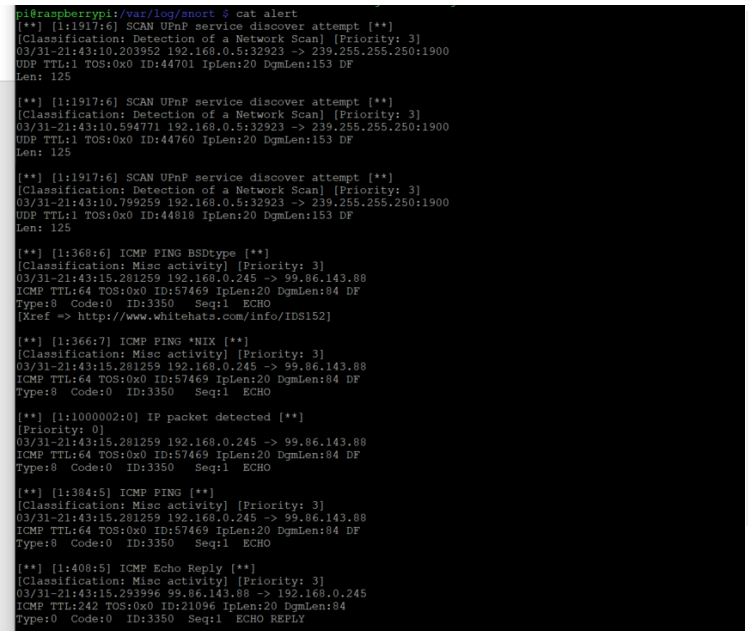
  - Snort use sniffer mode and apply BPF filter that only retrieve ICMP packet.

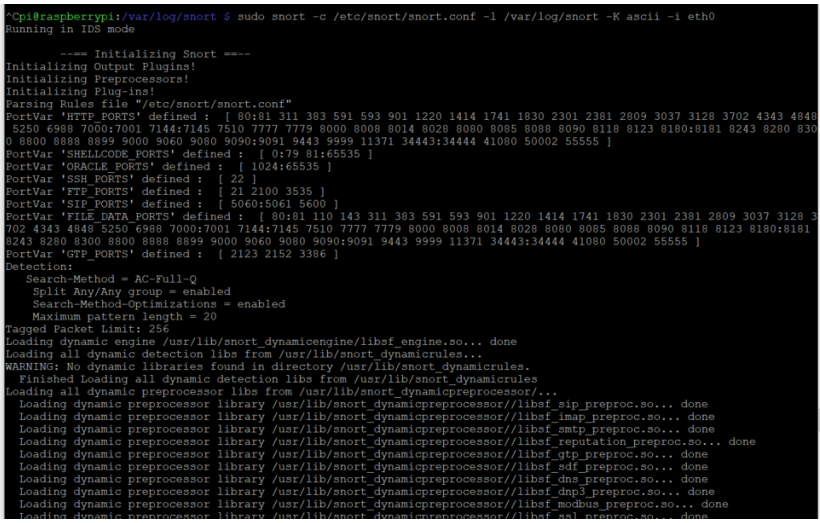


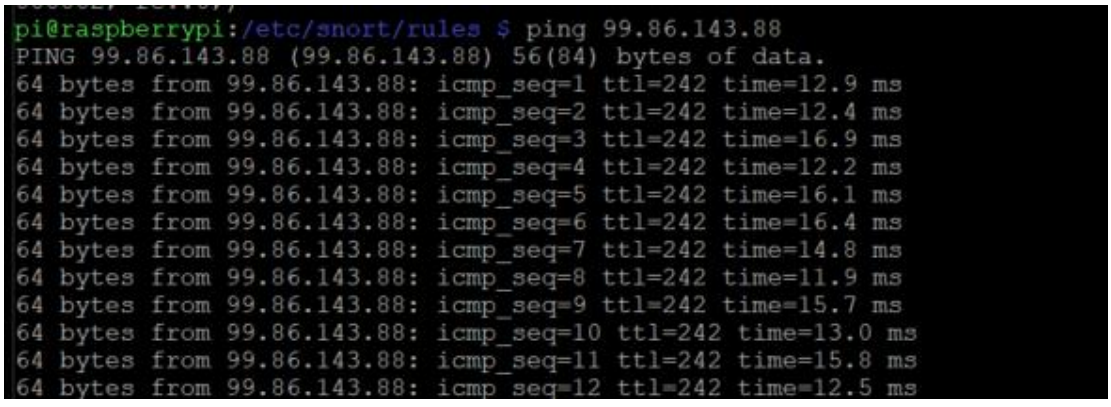
Task 3: Check Alerts

Created Rule:

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert ip 192.168.0.245 any -> 99.86.143.88 any (msg: "IP packet detected"; sid:1000002; rev:0;)
```



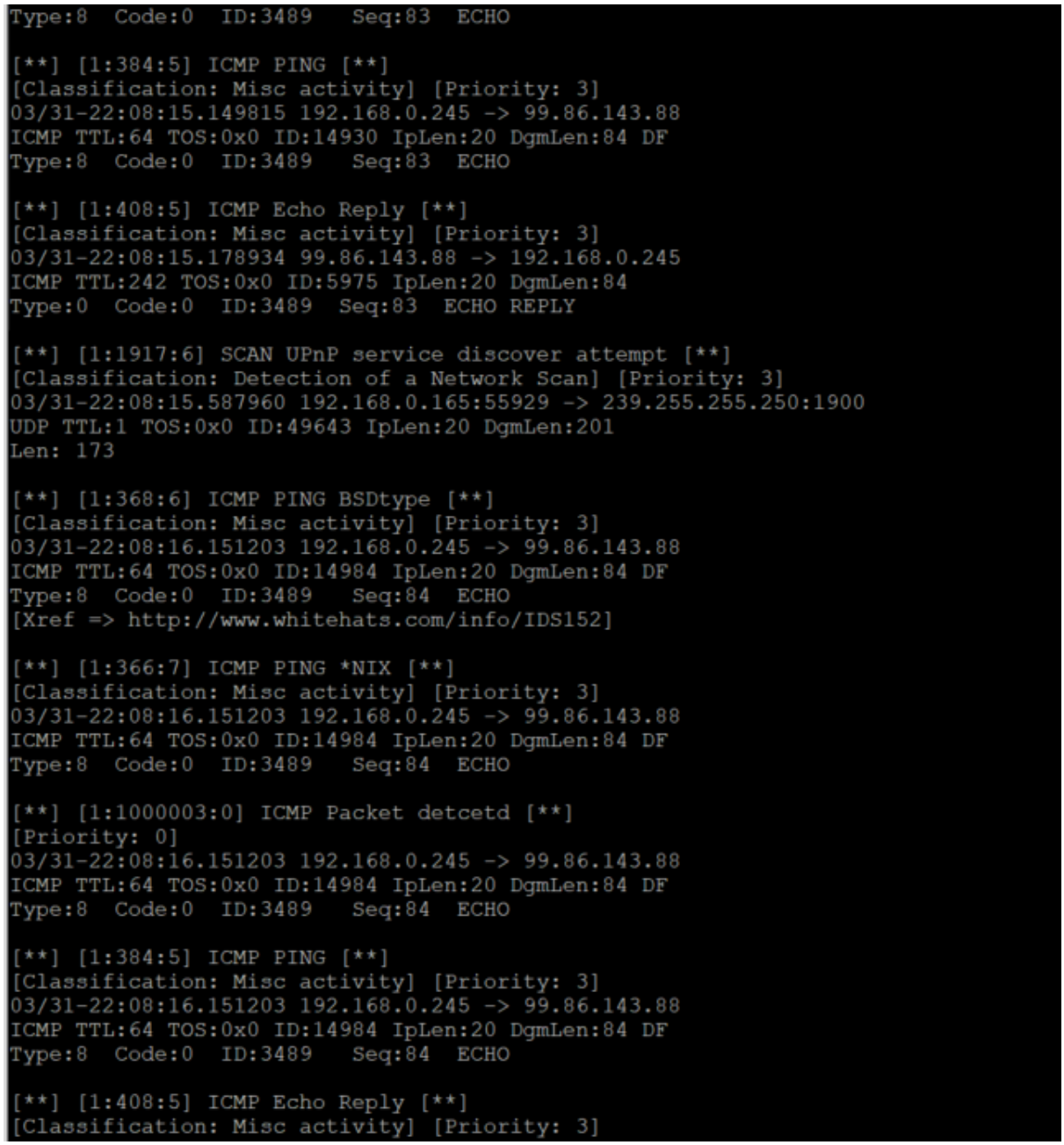




Since this rule will generate an alert message for every single captured IP packet that will used up the disk space. And its hard to find the right message as its loaded with alerts if it keeps capture packets

Task 4: Alert for Only ICMP

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp 192.168.0.245 any -> any any (msg: "ICMP Packet detcetd"; sid:1000003; rev:0;)
```



```
Type:8  Code:0  ID:3489   Seq:83  ECHO

[**] [1:384:5] ICMP PING [**]
[Classification: Misc activity] [Priority: 3]
03/31-22:08:15.149815 192.168.0.245 -> 99.86.143.88
ICMP TTL:64 TOS:0x0 ID:14930 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:3489   Seq:83  ECHO

[**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3]
03/31-22:08:15.178934 99.86.143.88 -> 192.168.0.245
ICMP TTL:242 TOS:0x0 ID:5975 IpLen:20 DgmLen:84
Type:0  Code:0  ID:3489  Seq:83  ECHO REPLY

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
03/31-22:08:15.587960 192.168.0.165:55929 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:49643 IpLen:20 DgmLen:201
Len: 173

[**] [1:368:6] ICMP PING BSDtype [**]
[Classification: Misc activity] [Priority: 3]
03/31-22:08:16.151203 192.168.0.245 -> 99.86.143.88
ICMP TTL:64 TOS:0x0 ID:14984 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:3489   Seq:84  ECHO
[Xref => http://www.whitehats.com/info/IDS152]

[**] [1:366:7] ICMP PING *NIX [**]
[Classification: Misc activity] [Priority: 3]
03/31-22:08:16.151203 192.168.0.245 -> 99.86.143.88
ICMP TTL:64 TOS:0x0 ID:14984 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:3489   Seq:84  ECHO

[**] [1:1000003:0] ICMP Packet detcetd [**]
[Priority: 0]
03/31-22:08:16.151203 192.168.0.245 -> 99.86.143.88
ICMP TTL:64 TOS:0x0 ID:14984 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:3489   Seq:84  ECHO

[**] [1:384:5] ICMP PING [**]
[Classification: Misc activity] [Priority: 3]
03/31-22:08:16.151203 192.168.0.245 -> 99.86.143.88
ICMP TTL:64 TOS:0x0 ID:14984 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:3489   Seq:84  ECHO

[**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3]
```

Task 5: Snort Rule

```
alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 !:1024
```

The subnet 192.168.1.0/24 can send TCP traffic to 192.168.1.0/24 and the port number less and equal than 1024 will not create any alert. Else does.

TASK 6: Alert on HTTP Get

Since HTTP clients generally use TCP connections to communicate to the Server, so that we will monitor the TCP traffic. (As my Raspberry pi cannot use browser, so I changed to Kali)

```
File  Edit  Search  View  Document  Help
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ------------------
# LOCAL RULES
# ------------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert tcp any any -> any 80 (msg: "HTTP request Detected"; sid:1000333; rev:20;)
```

```
03/31-07:35:15.511106  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:15.511303  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:15.617609  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:15.953065  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:16.060848  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:17.183087  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:17.296598  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:17.514069  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51118 → 142.250.66.227:80
03/31-07:35:17.526817  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51118 → 142.250.66.227:80
03/31-07:35:17.532444  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51118 → 142.250.66.227:80
03/31-07:35:17.641594  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51118 → 142.250.66.227:80
03/31-07:35:17.823555  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.0.1:1900 → 239.255.255.250:1900
03/31-07:35:17.874384  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.0.1:1900 → 239.255.255.250:1900
03/31-07:35:17.925421  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.0.1:1900 → 239.255.255.250:1900
03/31-07:35:17.976460  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.0.1:1900 → 239.255.255.250:1900
03/31-07:35:18.027412  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.0.1:1900 → 239.255.255.250:1900
03/31-07:35:18.078548  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.0.1:1900 → 239.255.255.250:1900
03/31-07:35:18.424664  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:18.571176  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:19.891683  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:19.997702  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:20.261576  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:20.366666  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:24.427795  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.0.165:54056 → 239.255.255.250:1900
03/31-07:35:25.438816  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.0.165:54056 → 239.255.255.250:1900
03/31-07:35:25.851353  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40106 → 188.184.21.108:80
03/31-07:35:26.103078  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40108 → 188.184.21.108:80
03/31-07:35:26.158147  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40106 → 188.184.21.108:80
03/31-07:35:26.159191  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40106 → 188.184.21.108:80
03/31-07:35:26.405224  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40108 → 188.184.21.108:80
03/31-07:35:26.451886  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.0.165:54056 → 239.255.255.250:1900
03/31-07:35:26.471150  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40106 → 188.184.21.108:80
03/31-07:35:26.472268  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40106 → 188.184.21.108:80
03/31-07:35:26.674490  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40108 → 188.184.21.108:80
03/31-07:35:26.985834  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40108 → 188.184.21.108:80
03/31-07:35:26.986059  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40108 → 188.184.21.108:80
03/31-07:35:27.460525  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.0.165:54056 → 239.255.255.250:1900
03/31-07:35:27.723157  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51118 → 142.250.66.227:80
03/31-07:35:30.459814  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:37478 → 188.184.99.6:80
03/31-07:35:30.538603  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:51096 → 142.250.66.227:80
03/31-07:35:30.737868  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:53340 → 137.138.153.49:80
03/31-07:35:30.759775  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:37478 → 188.184.99.6:80
03/31-07:35:31.050126  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:53340 → 137.138.153.49:80
03/31-07:35:31.886945  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40114 → 188.184.21.108:80
03/31-07:35:32.165819  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40116 → 188.184.21.108:80
03/31-07:35:32.203149  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40114 → 188.184.21.108:80
03/31-07:35:32.203214  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40114 → 188.184.21.108:80
03/31-07:35:32.473026  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:40116 → 188.184.21.108:80
03/31-07:35:34.813082  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:47584 → 99.86.143.121:80
```

Normally server usually host http request at port 80. So we monitor the destination address with Port 80.

TASK 7: Alert on TCP Flags

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ------------------
# LOCAL RULES
# ------------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert tcp any any -> any any (flags:S; msg:"SYN Packets Detected";sid:1021212;rev:007;)
```

```
SSL Preprocessor:
    SSL packets decoded: 670
            Client Hello: 142
            Server Hello: 109
             Certificate: 18
             Server Done: 50
    Client Key Exchange: 25
    Server Key Exchange: 10
          Change Cipher: 196
               Finished: 0
     Client Application: 116
     Server Application: 143
                  Alert: 2
  Unrecognized records: 220
  Completed handshakes: 0
        Bad handshakes: 0
      Sessions ignored: 73
    Detection disabled: 24
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
IMAP Preprocessor Statistics
  Total sessions                          : 0
  Max concurrent sessions                 : 0
===============================================================================
POP Preprocessor Statistics
  Total sessions                          : 0
  Max concurrent sessions                 : 0
===============================================================================
Snort exiting
```

```
03/31-07:35:34.970796  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:47586 -> 99.86.143.121:80
03/31-07:35:34.970940  [**] [1:1000333:20] HTTP request Detected [**] [Priority: 0] {TCP} 192.168.0.118:47586 -> 99.86.143.121:80
03/31-07:43:20.534713  [**] [1:1021212:7] SYN Packets Detected [**] [Priority: 0] {TCP} 192.168.0.209:2109 -> 20.44.229.112:443
03/31-07:43:23.567305  [**] [1:1021212:7] SYN Packets Detected [**] [Priority: 0] {TCP} 192.168.0.118:50946 -> 142.250.76.99:443
03/31-07:43:23.570341  [**] [1:1021212:7] SYN Packets Detected [**] [Priority: 0] {TCP} 192.168.0.118:50948 -> 142.250.76.99:443
03/31-07:43:23.581359  [**] [1:1021212:7] SYN Packets Detected [**] [Priority: 0] {TCP} 192.168.0.118:50950 -> 142.250.76.99:443
03/31-07:43:23.657199  [**] [1:1021212:7] SYN Packets Detected [**] [Priority: 0] {TCP} 192.168.0.118:57482 -> 142.250.67.14:443
03/31-07:43:23.931343  [**] [1:1021212:7] SYN Packets Detected [**] [Priority: 0] {TCP} 192.168.0.118:48194 -> 142.250.67.2:443
03/31-07:43:23.935893  [**] [1:1021212:7] SYN Packets Detected [**] [Priority: 0] {TCP} 192.168.0.118:34390 -> 142.250.66.234:443
03/31-07:43:24.449914  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.0.165:60081 -> 239.
03/31-07:43:24.451922  [**] [1:1021212:7] SYN Packets Detected [**] [Priority: 0] {TCP} 192.168.0.209:2110 -> 104.68.15.158:80
```

Task 8: Alert on Telnet

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ------------------
# LOCAL RULES
# ------------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert tcp any any -> any 23 (msg:"Telnet Detected";sid:1021212;rev:007;)
```

```
03/31-07:54:36.395044  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.0.1:1900 -> 239.25
03/31-07:55:01.479407  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:01.663981  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:01.860053  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:01.860110  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:02.040670  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:02.046133  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:02.230053  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:02.416722  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:02.416815  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:05.306121  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:05.553253  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:05.597914  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:05.738181  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:05.788216  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:05.972746  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:06.346828  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:06.534200  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:06.712670  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:06.719454  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:06.905598  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:07.090398  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:07.148090  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:07.347778  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:07.352240  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:07.539885  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:07.602367  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:07.721472  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
03/31-07:55:07.787690  [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 -> 64.13.139.230:23
```