

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

- Solution:

```
Sudo snort -de
```

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

```
root@kali:~/src/snort# sudo snort -de
Running in packet dump mode

--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

--== Initialization Complete ==--

o' )- Version 2.9.7.0 GRE (Build 149)
    '--- By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
        Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
        Copyright (C) 1998-2013 Sourcefire, Inc., et al.
        Using libpcap version 1.8.1
        Using PCRE version: 8.39 2016-06-14
        Using ZLIB version: 1.2.11

Commencing packet processing (pid=2107)
^C*** Caught Int-Signal

03/29/19:39:41.153564 E4:5F:01:0D:72:29 -> 2C:F0:5D:3C:B7:DA type:0x800 len:0x86
192.168.0.245:22 -> 192.168.0.209:1329 TCP TTL:64 TOS:0x10 ID:1004 Iplen:20 DgmLen:120 DF
*** Seq: 0x05945FA Ack: 0x00C3D21 Win: 0x356 TopLen: 20
F9 21 67 76 0A A1 8A 80 AC AB 92 C8 8B 08 41 6D .!gv.....Am
92 36 DE 24 70 C6 B8 3F 06 FC 9C 45 71 46 B5 DE .6.Sp...?..EqF..
59 39 59 C9 4F 59 84 F0 BB 2F 20 26 5C 62 17 3E iRY.Ox.../ t.b->
03 7E FB 27 D2 1F 0D 5C EF BE 2D 06 06 94 0B 70 -.\'.....P
01 6A F6 D1 57 62 65 BE B9 BB AF 47 14 F3 38 46 .j..Wbe....G..8F

-----
Run time for packet processing was 1.95751 seconds
Snort processed 1 packets.
Snort ran for 0 days 0 hours 0 minutes 1 seconds
Pkts/sec: 1

-----
Memory usage summary:
Total non-mapped bytes (arena): 610384
Bytes in mapped regions (abkbks): 7409664
Total allocated space (uordbks): 500288
Total free space (fordbks): 110016
Topmost releasable block (keepcost): 107200

-----
Packet I/O Totals:
Received: 62
Analyzed: 1 ( 1.613%)
Dropped: 0 ( 0.000%)
Filtered: 0 ( 0.000%)
Outstanding: 61 ( 99.387%)
Injected: 0
```

```
Breakdown by protocol (includes reinit packets):
Eth: 1 (100.000%)
VLAN: 0 ( 0.000%)
IP4: 1 (100.000%)
Frag: 0 ( 0.000%)
ICMP: 0 ( 0.000%)
UDP: 0 ( 0.000%)
TCP: 1 (100.000%)
IP6: 0 ( 0.000%)
IP6 Ext: 0 ( 0.000%)
IP6 Opt: 0 ( 0.000%)
Frag6: 0 ( 0.000%)
ICMP-IP: 0 ( 0.000%)
UDPF: 0 ( 0.000%)
TCP6: 0 ( 0.000%)
Teredo: 0 ( 0.000%)
ICMP-IP6: 0 ( 0.000%)
IP4/IP4: 0 ( 0.000%)
IP4/IP6: 0 ( 0.000%)
IP6/IP4: 0 ( 0.000%)
IP6/IP6: 0 ( 0.000%)
GRE: 0 ( 0.000%)
GRE Eth: 0 ( 0.000%)
GRE VLAN: 0 ( 0.000%)
GRE IP4: 0 ( 0.000%)
GRE IP6: 0 ( 0.000%)
GRE IP6 Ext: 0 ( 0.000%)
GRE PTP: 0 ( 0.000%)
GRE ARP: 0 ( 0.000%)
GRE IPX: 0 ( 0.000%)
GRE Loop: 0 ( 0.000%)
MPLS: 0 ( 0.000%)
ARP: 0 ( 0.000%)
IPX: 0 ( 0.000%)
Eth Loop: 0 ( 0.000%)
Eth Disc: 0 ( 0.000%)
IP4 Disc: 0 ( 0.000%)
IP6 Disc: 0 ( 0.000%)
TCP Disc: 0 ( 0.000%)
UDF Disc: 0 ( 0.000%)
ICMP Disc: 0 ( 0.000%)
All Discard: 0 ( 0.000%)
Other: 0 ( 0.000%)
Bad Chk Sum: 1 (100.000%)
Bad TTL: 0 ( 0.000%)
SS G 1: 0 ( 0.000%)
SS G 2: 0 ( 0.000%)
Total: 1
```

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

- **Solution:**

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

```
pi@raspberrypi:/etc/snort/rules $ sudo snort -vde icmp
Running in packet dump mode

==== Initializing Snort ====
Initializing Output Plugins!
Snort BPF option: icmp
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

---- Initialization Complete ----

''~
'''-
-*> Snort! <*~
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Commencing packet processing (pid=2124)
WARNING: No preprocessors configured for policy 0.
03/29-19:48:42.080285 2C:F0:5D:3C:B7:DA -> E4:5F:01:0D:72:29 type:0x800 len:0x4A
192.168.0.209 -> 192.168.0.245 ICMP TTL:128 TOS:0x0 ID:52939 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:291 ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcedefghi

+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-19:48:42.080387 E4:5F:01:0D:72:29 -> 2C:F0:5D:3C:B7:DA type:0x800 len:0x4A
192.168.0.245 -> 192.168.0.209 ICMP TTL:64 TOS:0x0 ID:4905 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:291 ECHO REPLY
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcedefghi

+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-19:48:43.096195 2C:F0:5D:3C:B7:DA -> E4:5F:01:0D:72:29 type:0x800 len:0x4A
192.168.0.209 -> 192.168.0.245 ICMP TTL:128 TOS:0x0 ID:52946 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:292 ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcedefghi

+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/29-19:48:43.096267 E4:5F:01:0D:72:29 -> 2C:F0:5D:3C:B7:DA type:0x800 len:0x4A
192.168.0.245 -> 192.168.0.209 ICMP TTL:64 TOS:0x0 ID:4929 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:292 ECHO REPLY
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcedefghi
```

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;)
```

```
pi@raspberrypi:/var/log/snort $ cat alert
[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
03/31-21:43:10.203952 192.168.0.5:32923 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:44701 Iplen:20 Dgmlen:153 DF
Len: 125

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
03/31-21:43:10.594771 192.168.0.5:32923 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:44760 Iplen:20 Dgmlen:153 DF
Len: 125

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
03/31-21:43:10.799259 192.168.0.5:32923 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:44818 Iplen:20 Dgmlen:153 DF
Len: 125

[**] [1:368:6] ICMP PING BSDtype [**]
[Classification: Misc activity] [Priority: 3]
03/31-21:43:15.281259 192.168.0.245 -> 99.86.143.88
ICMP TTL:64 TOS:0x0 ID:57469 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:3350 Seq:1 ECHO
[Xref => http://www.whitehats.com/info/IDS152]

[**] [1:366:7] ICMP PING *NIX [**]
[Classification: Misc activity] [Priority: 3]
03/31-21:43:15.281259 192.168.0.245 -> 99.86.143.88
ICMP TTL:64 TOS:0x0 ID:57469 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:3350 Seq:1 ECHO

[**] [1:1000002:0] IP packet detected [**]
[Priority: 0]
03/31-21:43:15.281259 192.168.0.245 -> 99.86.143.88
ICMP TTL:64 TOS:0x0 ID:57469 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:3350 Seq:1 ECHO

[**] [1:384:5] ICMP PING [**]
[Classification: Misc activity] [Priority: 3]
03/31-21:43:15.281259 192.168.0.245 -> 99.86.143.88
ICMP TTL:64 TOS:0x0 ID:57469 Iplen:20 Dgmlen:84 DF
Type:8 Code:0 ID:3350 Seq:1 ECHO

[**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3]
03/31-21:43:15.293996 99.86.143.88 -> 192.168.0.245
ICMP TTL:242 TOS:0x0 ID:21096 Iplen:20 Dgmlen:84
Type:0 Code:0 ID:3350 Seq:1 ECHO REPLY
```

```
pi@raspberrypi:/var/log/snort $ sudo snort -c /etc/snort/snort.conf -l /var/log/snort -K ascii -i eth0
Running in IDS mode

----- Initializing Snort -----
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300
0 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3
702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181
8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
Search-Method - AC-Full-Q
Split Any/Any group = enabled
Search-Method-Optimizations = enabled
Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort_dynamicengine/libaf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort_dynamicrules.
Finished Loading all dynamic detection libs from /usr/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor...
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libaf_gip_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libaf_imap_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libaf_ftp_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libaf_gtp_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libaf_sdf_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libaf_dns_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libaf_dnp3_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libaf_modbus_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libaf_spl_preproc.so... done
```

```
pi@raspberrypi:/etc/snort/rules $ ping 99.86.143.88
PING 99.86.143.88 (99.86.143.88) 56(84) bytes of data.
64 bytes from 99.86.143.88: icmp_seq=1 ttl=242 time=12.9 ms
64 bytes from 99.86.143.88: icmp_seq=2 ttl=242 time=12.4 ms
64 bytes from 99.86.143.88: icmp_seq=3 ttl=242 time=16.9 ms
64 bytes from 99.86.143.88: icmp_seq=4 ttl=242 time=12.2 ms
64 bytes from 99.86.143.88: icmp_seq=5 ttl=242 time=16.1 ms
64 bytes from 99.86.143.88: icmp_seq=6 ttl=242 time=16.4 ms
64 bytes from 99.86.143.88: icmp_seq=7 ttl=242 time=14.8 ms
64 bytes from 99.86.143.88: icmp_seq=8 ttl=242 time=11.9 ms
64 bytes from 99.86.143.88: icmp_seq=9 ttl=242 time=15.7 ms
64 bytes from 99.86.143.88: icmp_seq=10 ttl=242 time=13.0 ms
64 bytes from 99.86.143.88: icmp_seq=11 ttl=242 time=15.8 ms
64 bytes from 99.86.143.88: icmp_seq=12 ttl=242 time=12.5 ms
```

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
03/31-07:35:26.674400 ** [1:1000333:20] HTTP request Detected ** [Priority: 0] [TCP] 192.168.0.118:40108 -> 188.184.21.108:80
03/31-07:35:26.985824 ** [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
03/31-07:35:31.869645 ** [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
03/31-07:43:24.510130 [**] [1:1021212:7] SYN Packets Detected [**] [Priority: 0] {TCP} 192.168.0.118:47586 → 99.86.143.121:80
```

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 → 239.252.0.3:1900
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
03/31-07:55:07.905313 [**] [1:1021212:7] Telnet Detected [**] [Priority: 0] {TCP} 192.168.0.118:48370 → 64.13.139.230:23
```