COMP 9337 Securing Wireless Networks

T1, 2019

Lab 5

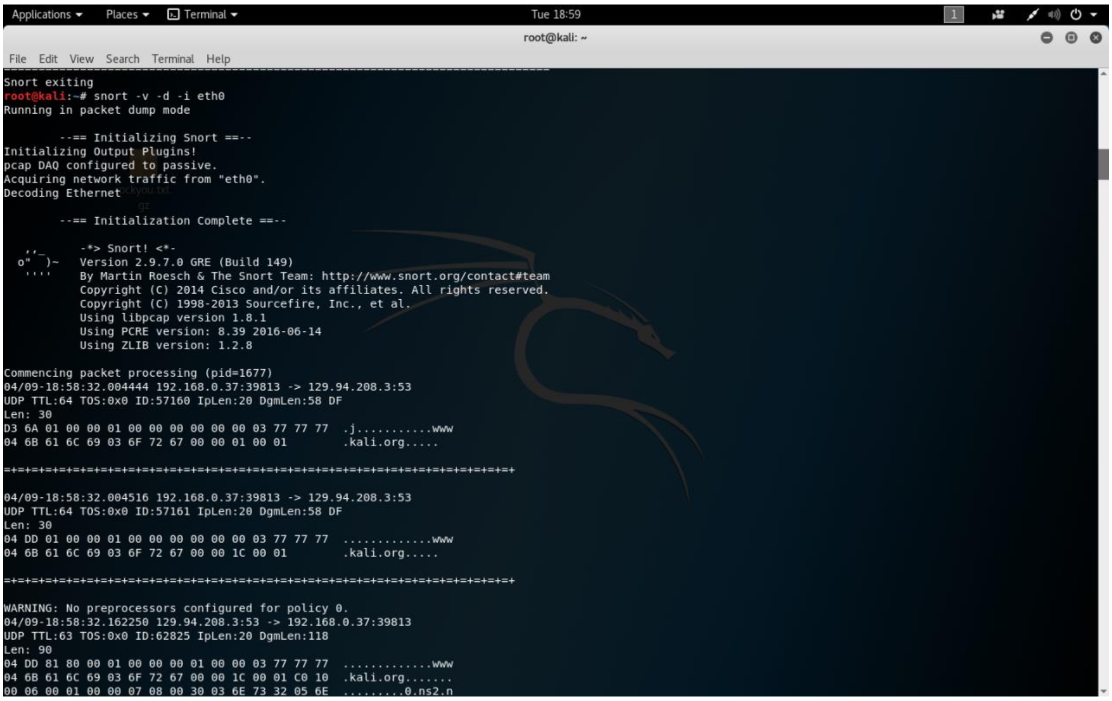
Group: SWN19 AI

Zhou JIANG (z5146092), Wanze LIU (z5137189)

School of Computer Science and Engineering

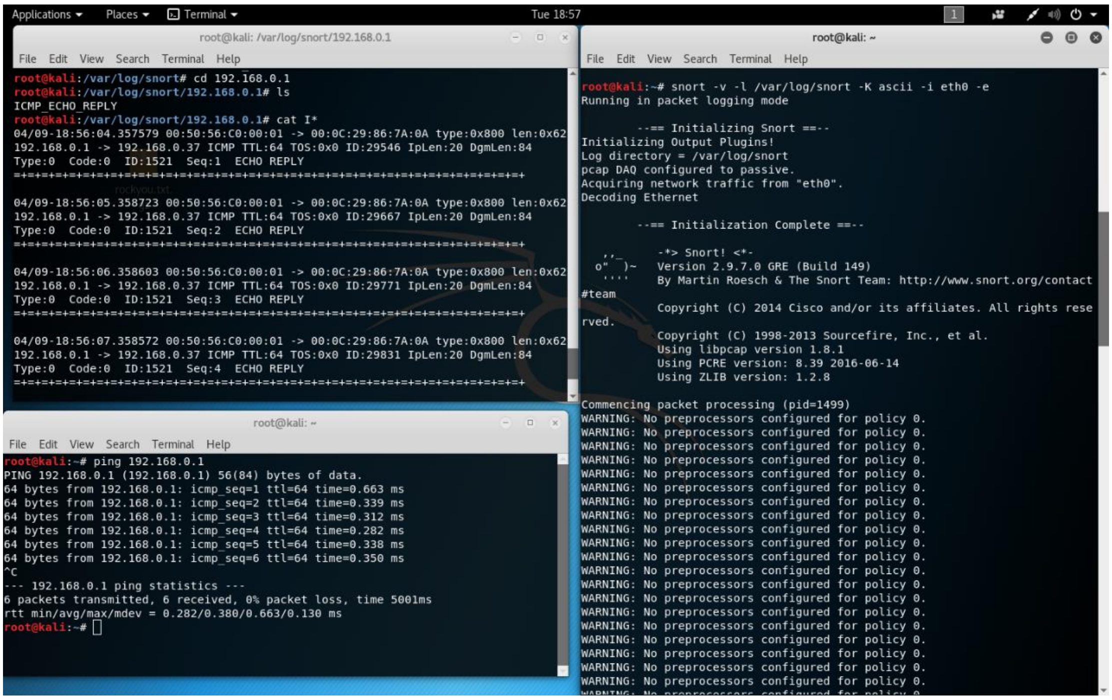
UNSW Sydney

1. Capture application layer data: Give screenshot that shows the command (you use) and the headers and application layer data for a captured packet.



```
Snort exiting
root@kali:~# snort -v -d -i eth0
Running in packet dump mode

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

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  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: 1.2.8

Commencing packet processing (pid=1677)
04/09-18:58:32.004444 192.168.0.37:39813 -> 129.94.208.3:53
UDP TTL:64 TOS:0x0 ID:57160 IpLen:20 DgmLen:58 DF
Len: 30
D3 6A 01 00 00 01 00 00 00 00 00 00 03 77 77 77  .j..........www
04 6B 61 6C 69 03 6F 72 67 00 00 01 00 01        .kali.org.....

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

04/09-18:58:32.004516 192.168.0.37:39813 -> 129.94.208.3:53
UDP TTL:64 TOS:0x0 ID:57161 IpLen:20 DgmLen:58 DF
Len: 30
04 DD 01 00 00 01 00 00 00 00 00 00 03 77 77 77  .............www
04 6B 61 6C 69 03 6F 72 67 00 00 1C 00 01        .kali.org.....

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

WARNING: No preprocessors configured for policy 0.
04/09-18:58:32.162250 129.94.208.3:53 -> 192.168.0.37:39813
UDP TTL:63 TOS:0x0 ID:62825 IpLen:20 DgmLen:118
Len: 90
04 DD 81 80 00 01 00 00 00 01 00 00 03 77 77 77  .............www
04 6B 61 6C 69 03 6F 72 67 00 00 1C 00 01 C0 10  .kali.org.......
00 06 00 01 00 00 07 08 00 30 03 6E 73 32 05 6E  .........0.ns2.n
```

2. Capture Only ICMP: Provide screenshot that shows the command (you use) and the summary of snort packets captured



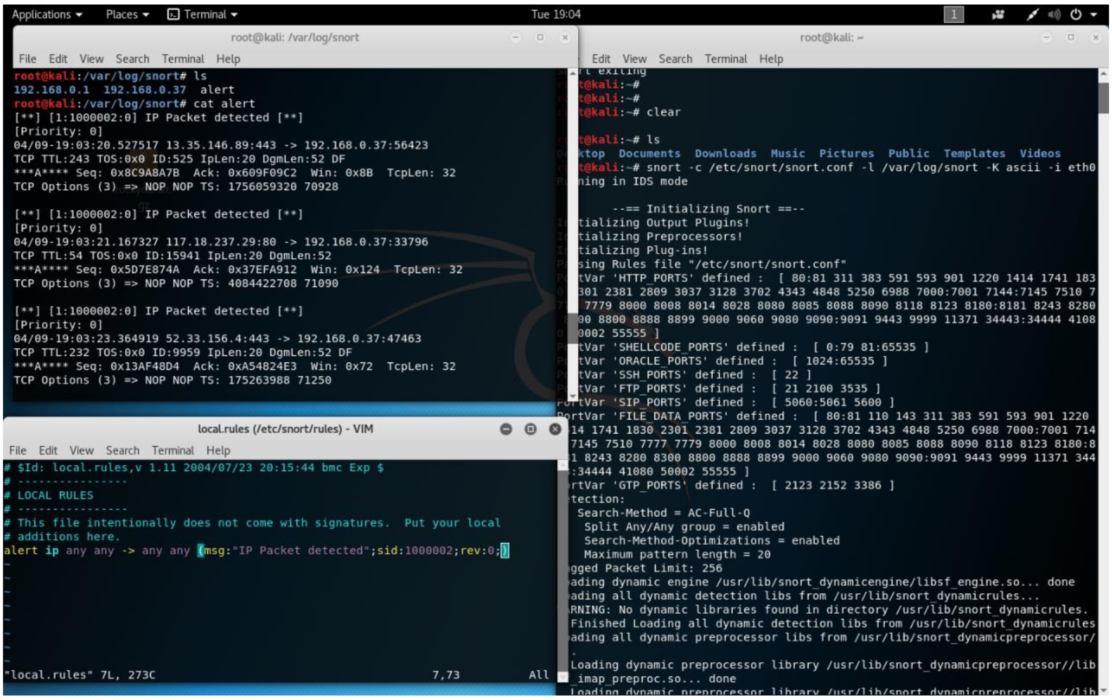
Applications
Places
Terminal
Tue 18:57
root@kali: /var/log/snort/192.168.0.1
File Edit View Search Terminal Help

```
root@kali:/var/log/snort# cd 192.168.0.1
root@kali:/var/log/snort/192.168.0.1# ls
ICMP_ECHO_REPLY
root@kali:/var/log/snort/192.168.0.1# cat I*
04/09-18:56:04.357579 00:50:56:C0:00:01 -> 00:0C:29:86:7A:0A type:0x800 len:0x62
192.168.0.1 -> 192.168.0.37 ICMP TTL:64 TOS:0x0 ID:29546 IpLen:20 DgmLen:84
Type:0  Code:0  ID:1521  Seq:1  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/09-18:56:05.358723 00:50:56:C0:00:01 -> 00:0C:29:86:7A:0A type:0x800 len:0x62
192.168.0.1 -> 192.168.0.37 ICMP TTL:64 TOS:0x0 ID:29667 IpLen:20 DgmLen:84
Type:0  Code:0  ID:1521  Seq:2  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/09-18:56:06.358603 00:50:56:C0:00:01 -> 00:0C:29:86:7A:0A type:0x800 len:0x62
192.168.0.1 -> 192.168.0.37 ICMP TTL:64 TOS:0x0 ID:29771 IpLen:20 DgmLen:84
Type:0  Code:0  ID:1521  Seq:3  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/09-18:56:07.358572 00:50:56:C0:00:01 -> 00:0C:29:86:7A:0A type:0x800 len:0x62
192.168.0.1 -> 192.168.0.37 ICMP TTL:64 TOS:0x0 ID:29831 IpLen:20 DgmLen:84
Type:0  Code:0  ID:1521  Seq:4  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
root@kali:~# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.663 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.339 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.312 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.282 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=0.338 ms
64 bytes from 192.168.0.1: icmp_seq=6 ttl=64 time=0.350 ms
^C
--- 192.168.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5001ms
rtt min/avg/max/mdev = 0.282/0.380/0.663/0.130 ms
root@kali:~# 
```

```
root@kali:~# snort -v -l /var/log/snort -K ascii -i eth0 -e
Running in packet logging mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Log directory = /var/log/snort
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  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 rese
rved.
           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: 1.2.8

Commencing packet processing (pid=1499)
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
```

3. Alert IP: Give screenshot that shows the command (you use) and the output in the alert file (/var/log/snort/alert). Also, provide justification why this rule is a bad rule.

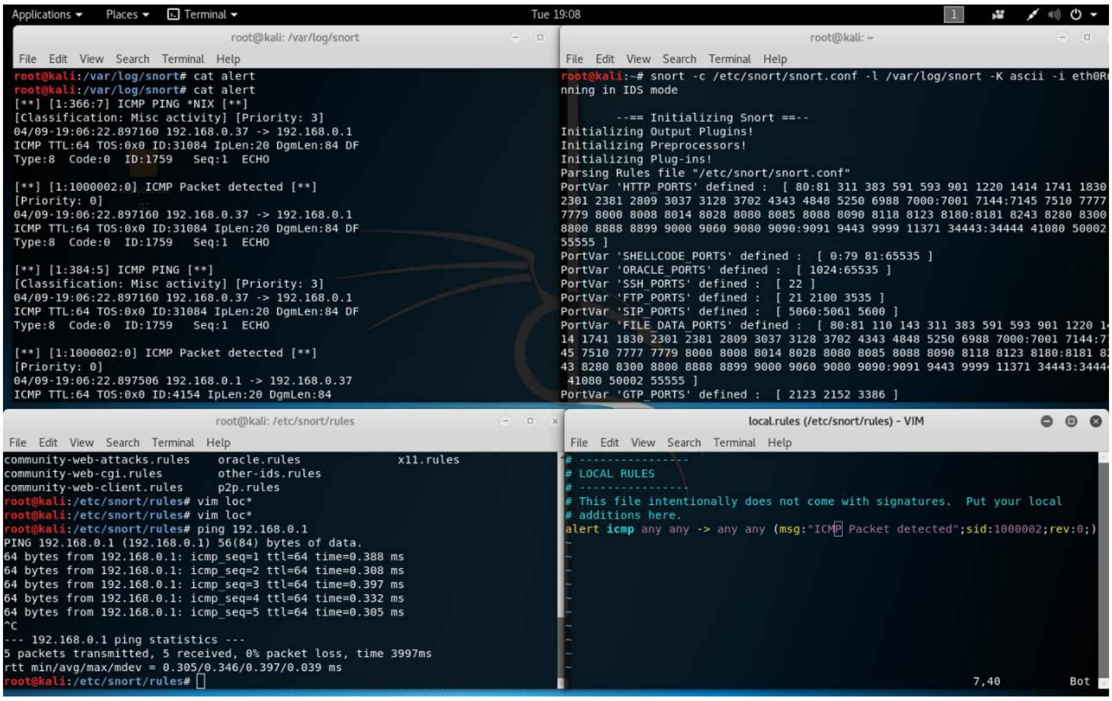

Applications
Places
Terminal
Tue 19:04
root@kali: /var/log/snort
File Edit View Search Terminal Help
root@kali: ~
Edit View Search Terminal Help
local.rules (/etc/snort/rules) - VIM
File Edit View Search Terminal Help

```
root@kali:/var/log/snort# ls
192.168.0.1  192.168.0.37  alert
root@kali:/var/log/snort# cat alert
[**] [1:1000002:0] IP Packet detected [**]
[Priority: 0]
04/09-19:03:20.527517 13.35.146.89:443 -> 192.168.0.37:56423
TCP TTL:243 TOS:0x0 ID:525 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x8C9A8A7B  Ack: 0x609F09C2  Win: 0x8B  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1756059320 70928

[**] [1:1000002:0] IP Packet detected [**]
[Priority: 0]
04/09-19:03:21.167327 117.18.237.29:80 -> 192.168.0.37:33796
TCP TTL:54 TOS:0x0 ID:15941 IpLen:20 DgmLen:52
***A**** Seq: 0x5D7E874A  Ack: 0x37EFA912  Win: 0x124  TcpLen: 32
TCP Options (3) => NOP NOP TS: 4084422708 71090

[**] [1:1000002:0] IP Packet detected [**]
[Priority: 0]
04/09-19:03:23.364919 52.33.156.4:443 -> 192.168.0.37:47463
TCP TTL:232 TOS:0x0 ID:9959 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x13AF48D4  Ack: 0xA54824E3  Win: 0x72  TcpLen: 32
TCP Options (3) => NOP NOP TS: 175263988 71250
```

```
rt exiting
t@kali:~#
t@kali:~#
t@kali:~# clear

t@kali:~# ls
ktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
t@kali:~# snort -c /etc/snort/snort.conf -l /var/log/snort -K ascii -i eth0
ning in IDS mode

        --== Initializing Snort ==--
tializing Output Plugins!
tializing Preprocessors!
tializing Plug-ins!
sing Rules file "/etc/snort/snort.conf"
tVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 183
301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7
 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280
00 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 4108
0002 55555 ]
tVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
tVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
tVar 'SSH_PORTS' defined :  [ 22 ]
tVar '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
14 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 714
7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8
1 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 344
:34444 41080 50002 55555 ]
rtVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
tection:
 Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20
gged Packet Limit: 256
ading dynamic engine /usr/lib/snort_dynamicengine/libsf_engine.so... done
ading all dynamic detection libs from /usr/lib/snort_dynamicrules...
RNING: No dynamic libraries found in directory /usr/lib/snort_dynamicrules.
Finished Loading all dynamic detection libs from /usr/lib/snort_dynamicrules
ading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor/
.
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//lib
_imap_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//lib
```

```
# $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 any any -> any any (msg:"IP Packet detected";sid:1000002;rev:0;)
~
~
~
~
~
~
~
~
"local.rules" 7L, 273C                                     7,73          All
```

4. Alert ICMP: Provide screenshot that shows the rule you used and the command. Also, show the alert file output.


Applications
Places
Terminal
Tue 19:08
root@kali: /var/log/snort
File Edit View Search Terminal Help
root@kali: ~
File Edit View Search Terminal Help
root@kali: /etc/snort/rules
File Edit View Search Terminal Help
local.rules (/etc/snort/rules) - VIM
File Edit View Search Terminal Help

```
root@kali:/var/log/snort# cat alert
root@kali:/var/log/snort# cat alert
[**] [1:366:7] ICMP PING *NIX [**]
[Classification: Misc activity] [Priority: 3]
04/09-19:06:22.897160 192.168.0.37 -> 192.168.0.1
ICMP TTL:64 TOS:0x0 ID:31084 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:1759   Seq:1  ECHO

[**] [1:1000002:0] ICMP Packet detected [**]
[Priority: 0]
04/09-19:06:22.897160 192.168.0.37 -> 192.168.0.1
ICMP TTL:64 TOS:0x0 ID:31084 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:1759   Seq:1  ECHO

[**] [1:384:5] ICMP PING [**]
[Classification: Misc activity] [Priority: 3]
04/09-19:06:22.897160 192.168.0.37 -> 192.168.0.1
ICMP TTL:64 TOS:0x0 ID:31084 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:1759   Seq:1  ECHO

[**] [1:1000002:0] ICMP Packet detected [**]
[Priority: 0]
04/09-19:06:22.897506 192.168.0.1 -> 192.168.0.37
ICMP TTL:64 TOS:0x0 ID:4154 IpLen:20 DgmLen:84
```

```
root@kali:~# snort -c /etc/snort/snort.conf -l /var/log/snort -K ascii -i eth0R
nning 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
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 1
14 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7
45 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8
43 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:3444
 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
```

```
community-web-attacks.rules   oracle.rules            x11.rules
community-web-cgi.rules       other-ids.rules
community-web-client.rules    p2p.rules
root@kali:/etc/snort/rules# vim loc*
root@kali:/etc/snort/rules# vim loc*
root@kali:/etc/snort/rules# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.388 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.308 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.397 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.332 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=0.305 ms
^C
--- 192.168.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.305/0.346/0.397/0.039 ms
root@kali:/etc/snort/rules# 
```

```
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp any any -> any any (msg:"ICMP Packet detected";sid:1000002;rev:0;)
~
~
~
~
~
~
~
~
~
~
                                                          7,40          Bot
```

5. The rule:

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

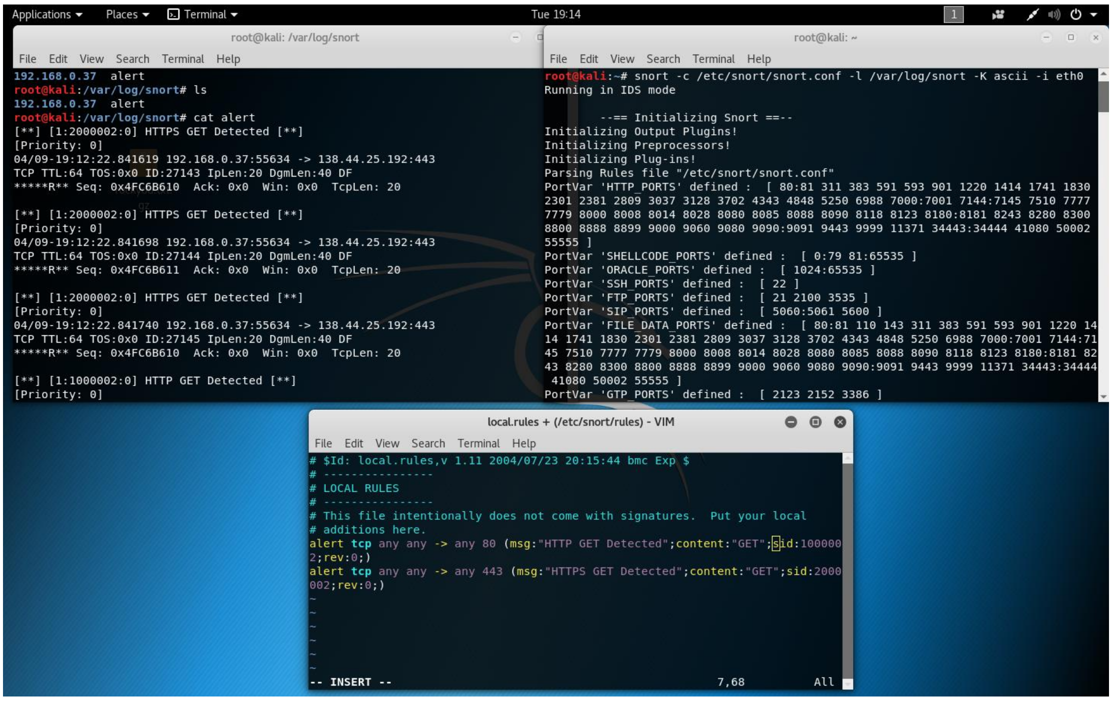
Explain what does the rule specify?

This means only such packet will be alerted:

- Its source address is **not** any of 192.168.1.0/24, and
- Its destination address is any of 192.168.1.0/24, and
- Its destination address is **not** 1024

6. HTTP/S GET matching: Provide the rule, the command used for snort and screenshot of the alert. Also explain how it works.

Explain: It filters out all packets to port 443 or 80, extracts their content as "GET", then captures.

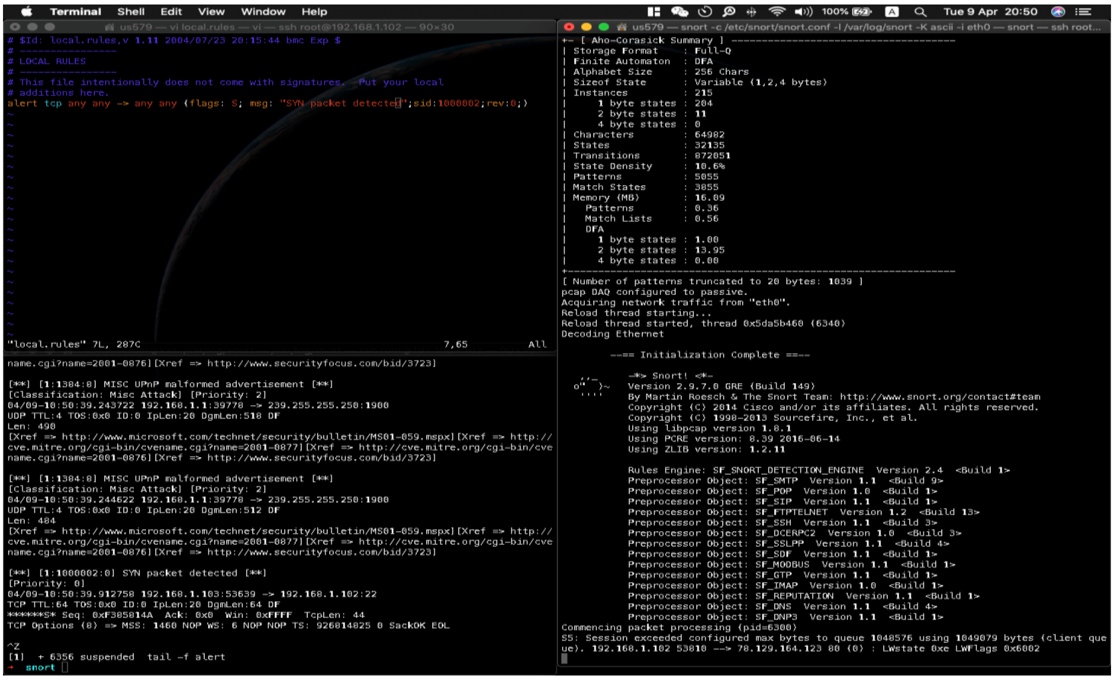

Applications
Places
Terminal
Tue 19:14
root@kali: /var/log/snort
File Edit View Search Terminal Help
root@kali: ~
File Edit View Search Terminal Help
local.rules + (/etc/snort/rules) - VIM
File Edit View Search Terminal Help

```
192.168.0.37  alert
root@kali:/var/log/snort# ls
192.168.0.37  alert
root@kali:/var/log/snort# cat alert
[**] [1:2000002:0] HTTPS GET Detected [**]
[Priority: 0]
04/09-19:12:22.841619 192.168.0.37:55634 -> 138.44.25.192:443
TCP TTL:64 TOS:0x0 ID:27143 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x4FC6B610  Ack: 0x0  Win: 0x0  TcpLen: 20

[**] [1:2000002:0] HTTPS GET Detected [**]
[Priority: 0]
04/09-19:12:22.841698 192.168.0.37:55634 -> 138.44.25.192:443
TCP TTL:64 TOS:0x0 ID:27144 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x4FC6B611  Ack: 0x0  Win: 0x0  TcpLen: 20

[**] [1:2000002:0] HTTPS GET Detected [**]
[Priority: 0]
04/09-19:12:22.841740 192.168.0.37:55634 -> 138.44.25.192:443
TCP TTL:64 TOS:0x0 ID:27145 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x4FC6B610  Ack: 0x0  Win: 0x0  TcpLen: 20

[**] [1:1000002:0] HTTP GET Detected [**]
[Priority: 0]
```

```
root@kali:~# 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
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 14
14 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:71
45 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82
43 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 ]
```

```
# $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 GET Detected";content:"GET";sid:100000
2;rev:0;)
alert tcp any any -> any 443 (msg:"HTTPS GET Detected";content:"GET";sid:2000
002;rev:0;)
~
~
~
~
~
~
-- INSERT --                                           7,68          All
```

7. Alert TCP SYN: Add the screenshots here, which shows the rule (you use). Also, identify the alert generated as a result

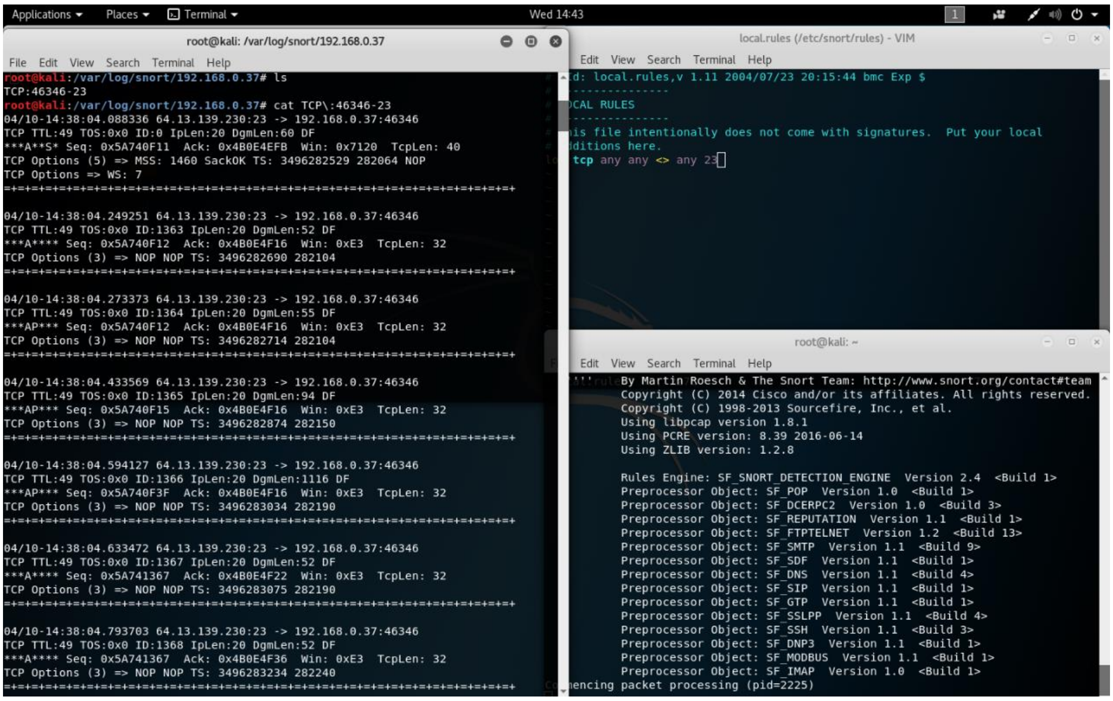

Terminal
Shell
Edit
View
Window
Help
100%
Tue 9 Apr 20:50
us579 — vi local.rules — vi — ssh root@192.168.1.102 — 90×30
us579 — snort -c /etc/snort/snort.conf -l /var/log/snort -K ascii -i eth0 — snort — ssh root...

```
# $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 packet detected";sid:1000002;rev:0;)
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"local.rules" 7L, 287C                                        7,65          All
```

```
name.cgi?name=2001-0876][Xref => http://www.securityfocus.com/bid/3723]

[**] [1:1384:8] MISC UPnP malformed advertisement [**]
[Classification: Misc Attack] [Priority: 2]
04/09-10:50:39.243722 192.168.1.1:39778 -> 239.255.255.250:1900
UDP TTL:4 TOS:0x0 ID:0 IpLen:20 DgmLen:518 DF
Len: 490
[Xref => http://www.microsoft.com/technet/security/bulletin/MS01-059.mspx][Xref => http://
cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0877][Xref => http://cve.mitre.org/cgi-bin/cve
name.cgi?name=2001-0876][Xref => http://www.securityfocus.com/bid/3723]

[**] [1:1384:8] MISC UPnP malformed advertisement [**]
[Classification: Misc Attack] [Priority: 2]
04/09-10:50:39.244622 192.168.1.1:39778 -> 239.255.255.250:1900
UDP TTL:4 TOS:0x0 ID:0 IpLen:20 DgmLen:512 DF
Len: 484
[Xref => http://www.microsoft.com/technet/security/bulletin/MS01-059.mspx][Xref => http://
cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0877][Xref => http://cve.mitre.org/cgi-bin/cve
name.cgi?name=2001-0876][Xref => http://www.securityfocus.com/bid/3723]

[**] [1:1000002:0] SYN packet detected [**]
[Priority: 0]
04/09-10:50:39.912758 192.168.1.103:53639 -> 192.168.1.102:22
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:64 DF
******S* Seq: 0xF385814A  Ack: 0x0  Win: 0xFFFF  TcpLen: 44
TCP Options (8) => MSS: 1460 NOP WS: 6 NOP NOP TS: 926814825 0 SackOK EOL

^Z
[1]  + 6356 suspended  tail -f alert
→  snort
```

```
+-- [ Aho-Corasick Summary ] -------------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 215
|     1 byte states : 204
|     2 byte states : 11
|     4 byte states : 0
| Characters        : 64982
| States            : 32135
| Transitions       : 872051
| State Density     : 10.6%
| Patterns          : 5055
| Match States      : 3855
| Memory (MB)       : 16.09
|   Patterns        : 0.36
|   Match Lists     : 0.56
|   DFA
|     1 byte states : 1.00
|     2 byte states : 13.95
|     4 byte states : 0.00
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1039 ]
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Reload thread starting...
Reload thread started, thread 0x5da5b460 (6340)
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  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

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
Commencing packet processing (pid=6300)
S5: Session exceeded configured max bytes to queue 1048576 using 1049079 bytes (client que
ue). 192.168.1.102 53810 --> 78.129.164.123 80 (0) : LWstate 0xe LWFlags 0x6002
```

8. Alert Telnet: Provide screenshots that shows the rule (you use). Also, identify the alert and the logged packets generated as a result of this rule.



Applications
Places
Terminal
Wed 14:43
1
root@kali: /var/log/snort/192.168.0.37
File Edit View Search Terminal Help
local.rules (/etc/snort/rules) - VIM
Edit View Search Terminal Help
root@kali: ~
Edit View Search Terminal Help

```
root@kali:/var/log/snort/192.168.0.37# ls
TCP:46346-23
root@kali:/var/log/snort/192.168.0.37# cat TCP\:46346-23
04/10-14:38:04.088336 64.13.139.230:23 -> 192.168.0.37:46346
TCP TTL:49 TOS:0x0 ID:0 IpLen:20 DgmLen:60 DF
***A**S* Seq: 0x5A740F11  Ack: 0x4B0E4EFB  Win: 0x7120  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 3496282529 282064 NOP
TCP Options => WS: 7
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/10-14:38:04.249251 64.13.139.230:23 -> 192.168.0.37:46346
TCP TTL:49 TOS:0x0 ID:1363 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x5A740F12  Ack: 0x4B0E4F16  Win: 0xE3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 3496282690 282104
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/10-14:38:04.273373 64.13.139.230:23 -> 192.168.0.37:46346
TCP TTL:49 TOS:0x0 ID:1364 IpLen:20 DgmLen:55 DF
***AP*** Seq: 0x5A740F12  Ack: 0x4B0E4F16  Win: 0xE3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 3496282714 282104
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/10-14:38:04.433569 64.13.139.230:23 -> 192.168.0.37:46346
TCP TTL:49 TOS:0x0 ID:1365 IpLen:20 DgmLen:94 DF
***AP*** Seq: 0x5A740F15  Ack: 0x4B0E4F16  Win: 0xE3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 3496282874 282150
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/10-14:38:04.594127 64.13.139.230:23 -> 192.168.0.37:46346
TCP TTL:49 TOS:0x0 ID:1366 IpLen:20 DgmLen:1116 DF
***AP*** Seq: 0x5A740F3F  Ack: 0x4B0E4F16  Win: 0xE3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 3496283034 282190
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/10-14:38:04.633472 64.13.139.230:23 -> 192.168.0.37:46346
TCP TTL:49 TOS:0x0 ID:1367 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x5A741367  Ack: 0x4B0E4F22  Win: 0xE3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 3496283075 282190
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/10-14:38:04.793703 64.13.139.230:23 -> 192.168.0.37:46346
TCP TTL:49 TOS:0x0 ID:1368 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x5A741367  Ack: 0x4B0E4F36  Win: 0xE3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 3496283234 282240
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
----------------
CAL RULES
----------------
is file intentionally does not come with signatures.  Put your local
dditions here.
 tcp any any <> any 23
```

```
           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: 1.2.8

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
  encing packet processing (pid=2225)
```