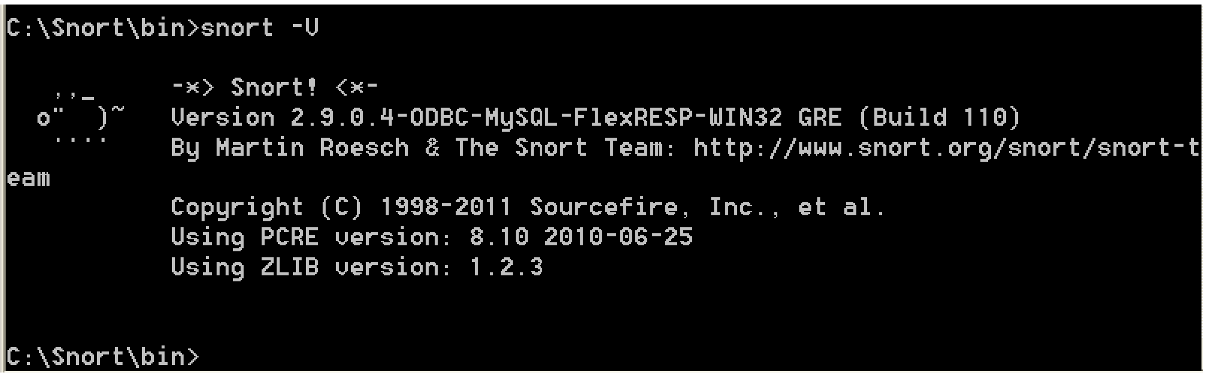
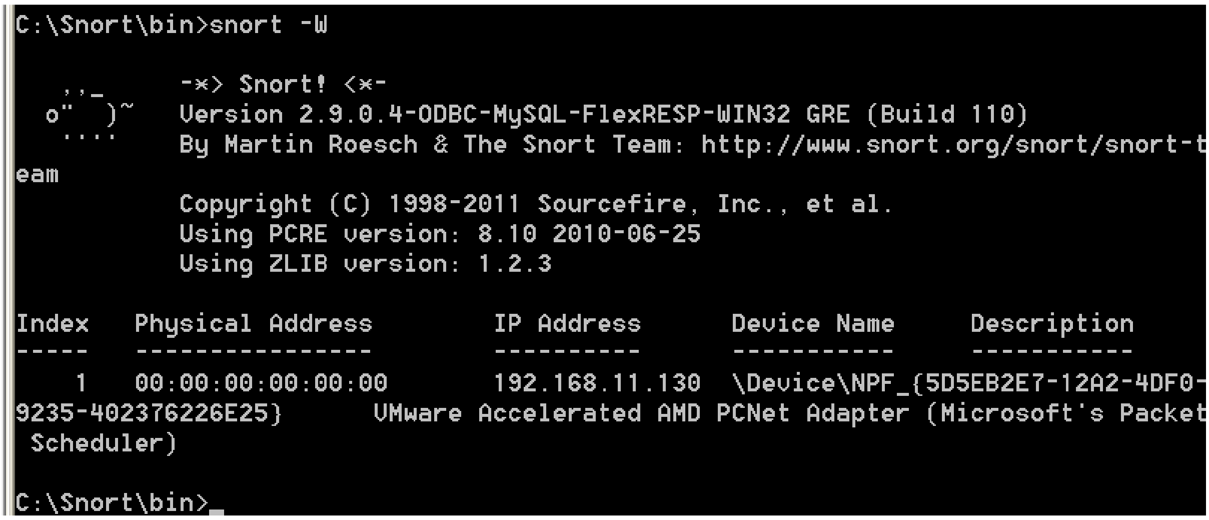
Snort practice

Snort version



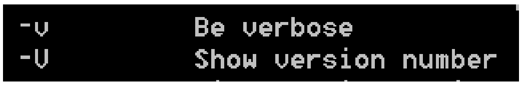
```
C:\Snort\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.0.4-ODBC-MySQL-FlexRESP-WIN32 GRE (Build 110)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort-t
eam
           Copyright (C) 1998-2011 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3


C:\Snort\bin>
```

Snort interface

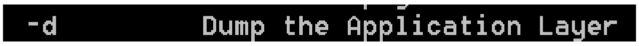


```
C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.0.4-ODBC-MySQL-FlexRESP-WIN32 GRE (Build 110)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort-t
eam
           Copyright (C) 1998-2011 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       192.168.11.130  \Device\NPF_{5D5EB2E7-12A2-4DF0-
9235-402376226E25}      VMware Accelerated AMD PCNet Adapter (Microsoft's Packet
 Scheduler)

C:\Snort\bin>_
```

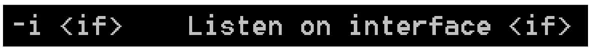
Snort flags



```
-v          Be verbose
-V          Show version number
```



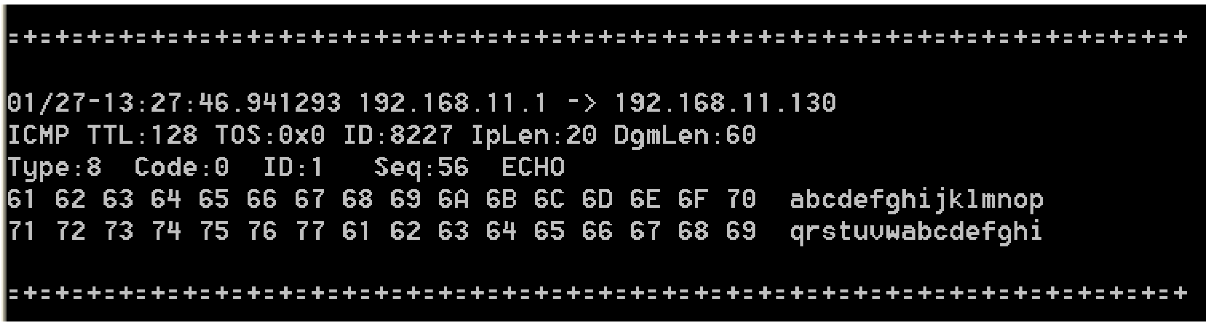
```
 -d          Dump the Application Layer
```



```
-i <if>     Listen on interface <if>
```

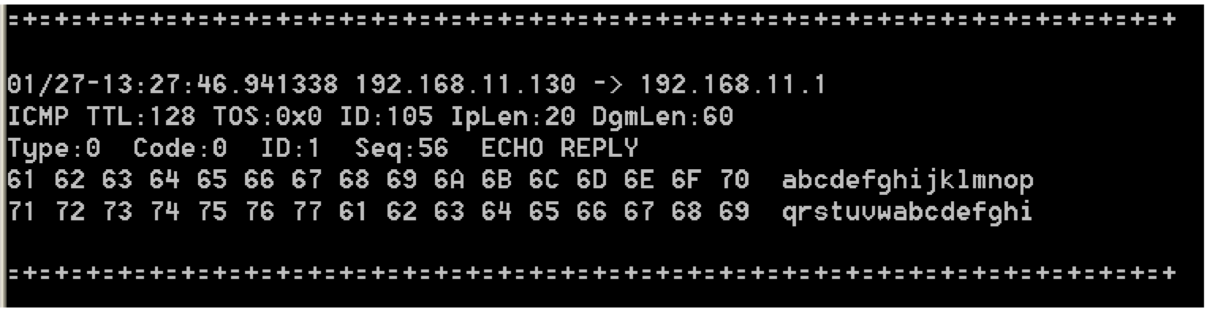
Type "`C:\snort\bin\snort -v -d -iN`" where *N* is the network interface number.

Ping request from host to target



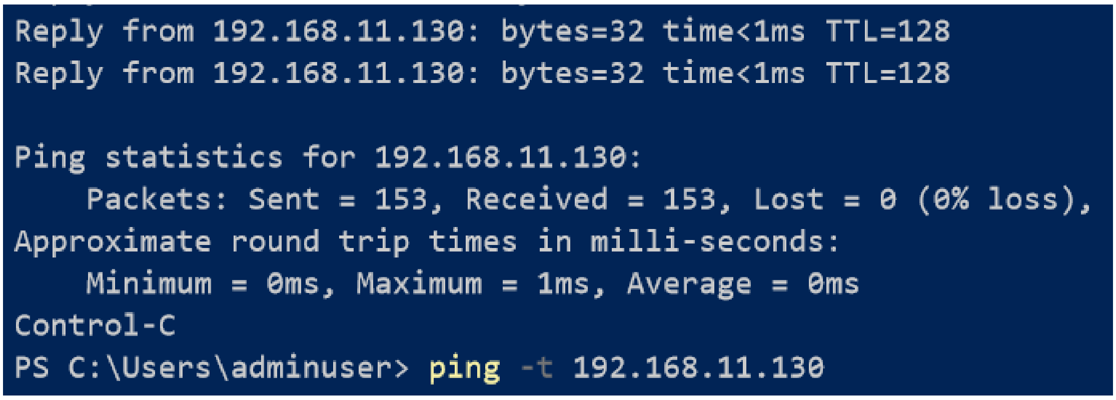
```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

01/27-13:27:46.941293 192.168.11.1 -> 192.168.11.130
ICMP TTL:128 TOS:0x0 ID:8227 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:56  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  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Ping reply from target to host



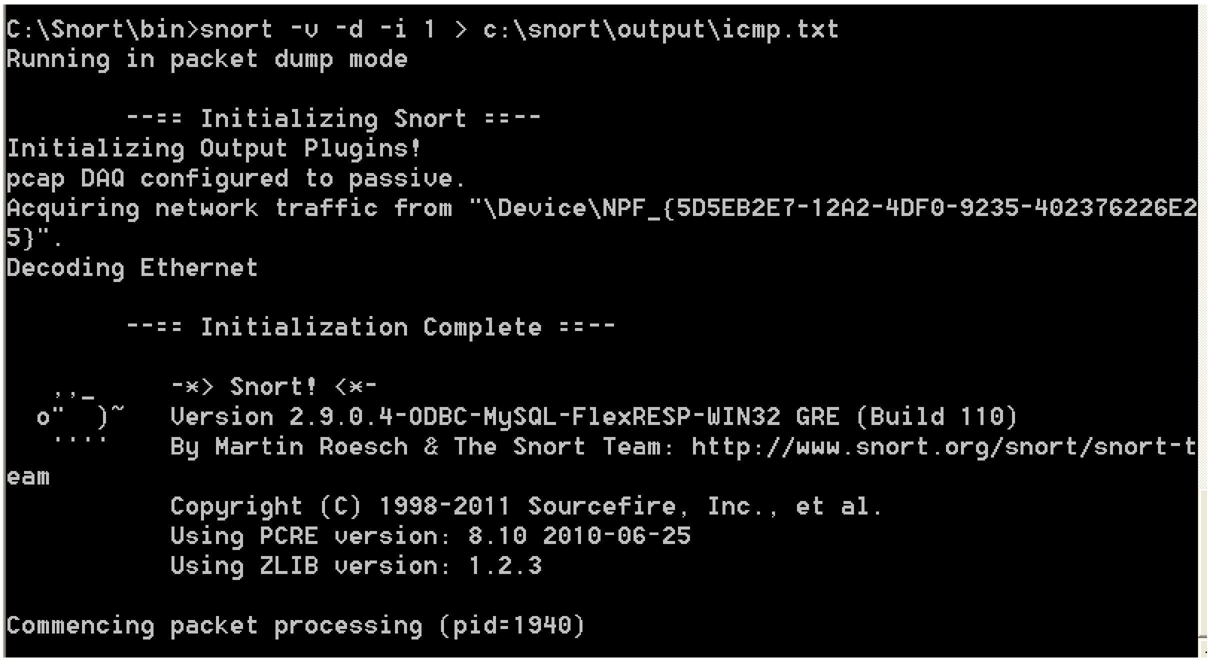
```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

01/27-13:27:46.941338 192.168.11.130 -> 192.168.11.1
ICMP TTL:128 TOS:0x0 ID:105 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1   Seq:56  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  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Continuous ping



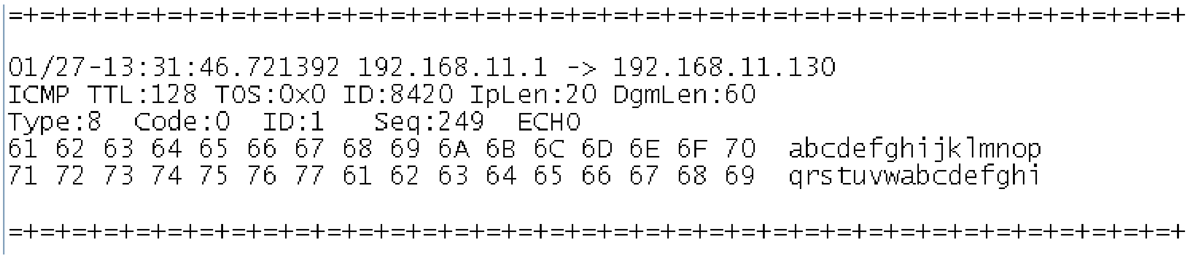
```
Reply from 192.168.11.130: bytes=32 time<1ms TTL=128
Reply from 192.168.11.130: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.11.130:
    Packets: Sent = 153, Received = 153, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
PS C:\Users\adminuser> ping -t 192.168.11.130
```

Verbose, dump application layer, choose interface 1, the output is saved to a file named icmp.txt



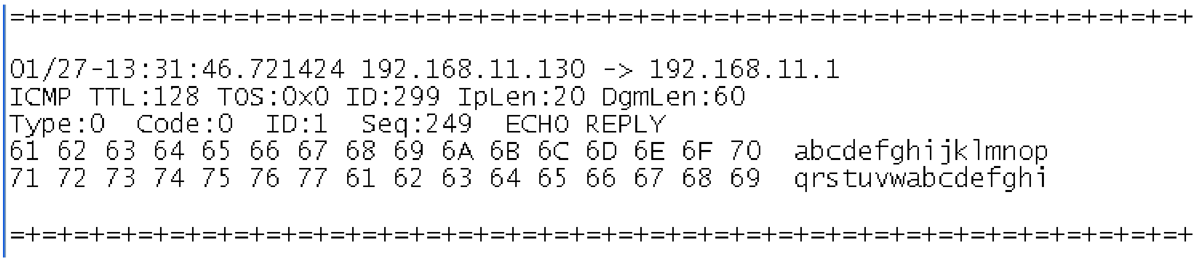
```
C:\Snort\bin>snort -v -d -i 1 > c:\snort\output\icmp.txt
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "\Device\NPF_{5D5EB2E7-12A2-4DF0-9235-402376226E2
5}".
Decoding Ethernet

        --== Initialization Complete ==--

           -*> Snort! <*-
   ,,_
  o"  )~   Version 2.9.0.4-ODBC-MySQL-FlexRESP-WIN32 GRE (Build 110)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 1998-2011 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Commencing packet processing (pid=1940)
```

Indicates ping request to target machine



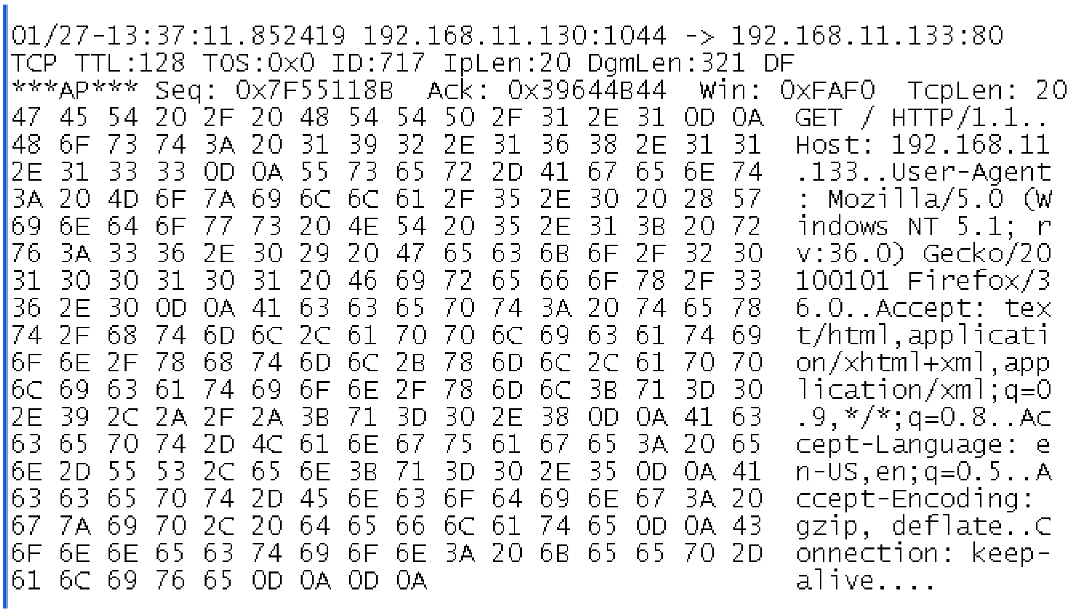
```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

01/27-13:31:46.721392 192.168.11.1 -> 192.168.11.130
ICMP TTL:128 TOS:0x0 ID:8420 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:249  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  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Indicates ping reply from target machine



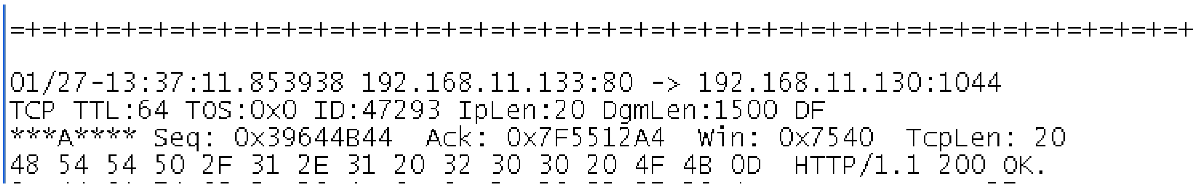
```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

01/27-13:31:46.721424 192.168.11.130 -> 192.168.11.1
ICMP TTL:128 TOS:0x0 ID:299 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:249  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  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

http-get



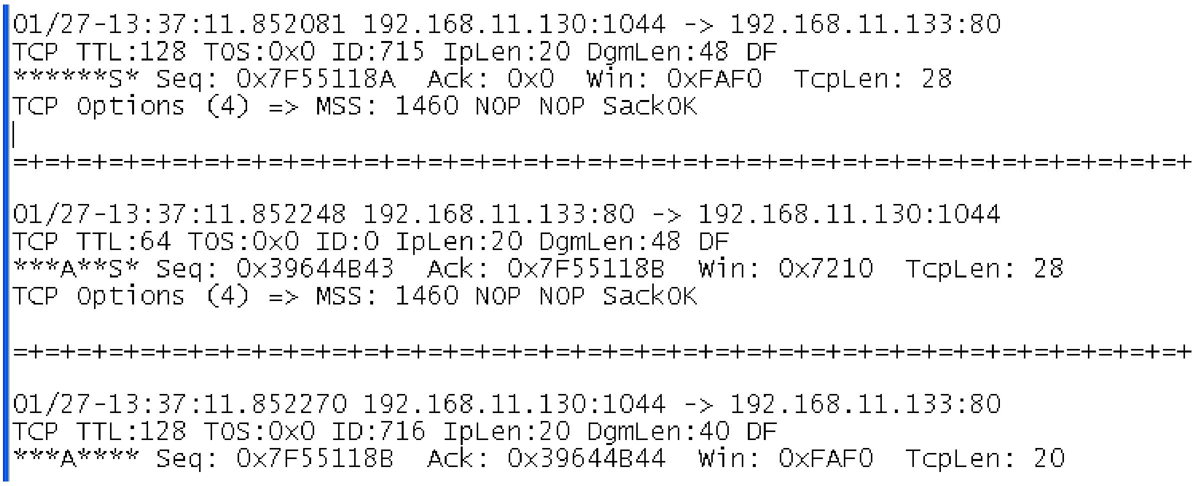
```
01/27-13:37:11.852419 192.168.11.130:1044 -> 192.168.11.133:80
TCP TTL:128 TOS:0x0 ID:717 IpLen:20 DgmLen:321 DF
***AP*** Seq: 0x7F55118B  Ack: 0x39644B44  Win: 0xFAF0  TcpLen: 20
47 45 54 20 2F 20 48 54 54 50 2F 31 2E 31 0D 0A  GET / HTTP/1.1..
48 6F 73 74 3A 20 31 39 32 2E 31 36 38 2E 31 31  Host: 192.168.11
2E 31 33 33 0D 0A 55 73 65 72 2D 41 67 65 6E 74  .133..User-Agent
3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57  : Mozilla/5.0 (W
69 6E 64 6F 77 73 20 4E 54 20 35 2E 31 3B 20 72  indows NT 5.1; r
76 3A 33 36 2E 30 29 20 47 65 63 6B 6F 2F 32 30  v:36.0) Gecko/20
31 30 30 31 30 31 20 46 69 72 65 66 6F 78 2F 33  100101 Firefox/3
36 2E 30 0D 0A 41 63 63 65 70 74 3A 20 74 65 78  6.0..Accept: tex
74 2F 68 74 6D 6C 2C 61 70 70 6C 69 63 61 74 69  t/html,applicati
6F 6E 2F 78 68 74 6D 6C 2B 78 6D 6C 2C 61 70 70  on/xhtml+xml,app
6C 69 63 61 74 69 6F 6E 2F 78 6D 6C 3B 71 3D 30  lication/xml;q=0
2E 39 2C 2A 2F 2A 3B 71 3D 30 2E 38 0D 0A 41 63  .9,*/*;q=0.8..Ac
63 65 70 74 2D 4C 61 6E 67 75 61 67 65 3A 20 65  cept-Language: e
6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 0D 0A 41  n-US,en;q=0.5..A
63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A 20  ccept-Encoding:
67 7A 69 70 2C 20 64 65 66 6C 61 74 65 0D 0A 43  gzip, deflate..C
6F 6E 6E 65 63 74 69 6F 6E 3A 20 6B 65 65 70 2D  onnection: keep-
61 6C 69 76 65 0D 0A 0D 0A                       alive....
```

http-ok



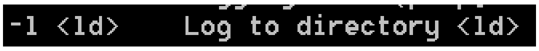
```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

01/27-13:37:11.853938 192.168.11.133:80 -> 192.168.11.130:1044
TCP TTL:64 TOS:0x0 ID:47293 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x39644B44  Ack: 0x7F5512A4  Win: 0x7540  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D  HTTP/1.1 200 OK.
```

Syn, Syn-ack, ack

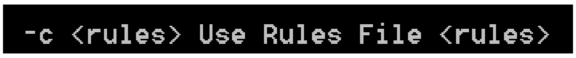


```
01/27-13:37:11.852081 192.168.11.130:1044 -> 192.168.11.133:80
TCP TTL:128 TOS:0x0 ID:715 IpLen:20 DgmLen:48 DF
******S* Seq: 0x7F55118A  Ack: 0x0  Win: 0xFAF0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

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

01/27-13:37:11.852248 192.168.11.133:80 -> 192.168.11.130:1044
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x39644B43  Ack: 0x7F55118B  Win: 0x7210  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

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

01/27-13:37:11.852270 192.168.11.130:1044 -> 192.168.11.133:80
TCP TTL:128 TOS:0x0 ID:716 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x7F55118B  Ack: 0x39644B44  Win: 0xFAF0  TcpLen: 20
```

Snort flags

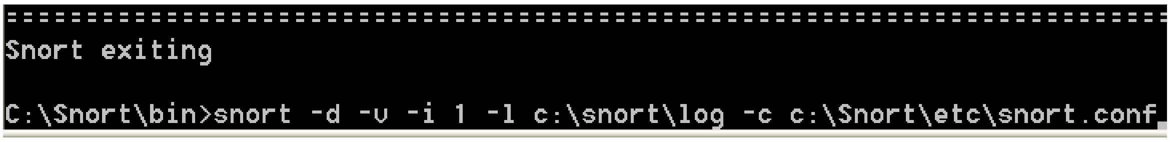


```
-l <ld>     Log to directory <ld>
```



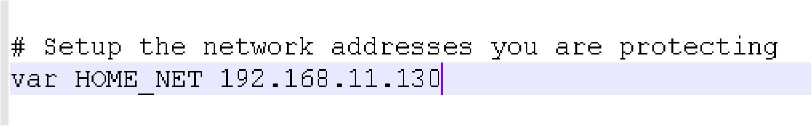
```
 -c <rules> Use Rules File <rules>
```

Dump application layer, verbose, use interface 1, use c:\snort\log as log directory and use config file c:\snort\etc\snort.conf



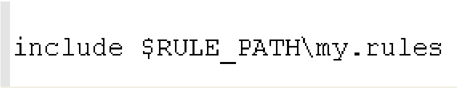
```
===============================================================================
Snort exiting

C:\Snort\bin>snort -d -v -i 1 -l c:\snort\log -c c:\Snort\etc\snort.conf
```

Ip address of winxp vm



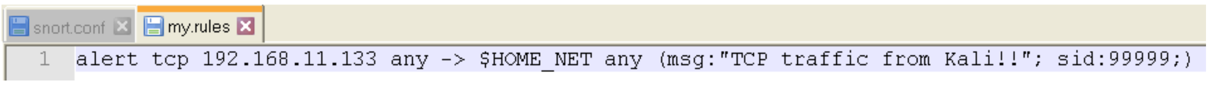
```
# Setup the network addresses you are protecting
var HOME_NET 192.168.11.130
```

Snort.conf file to include custom rules



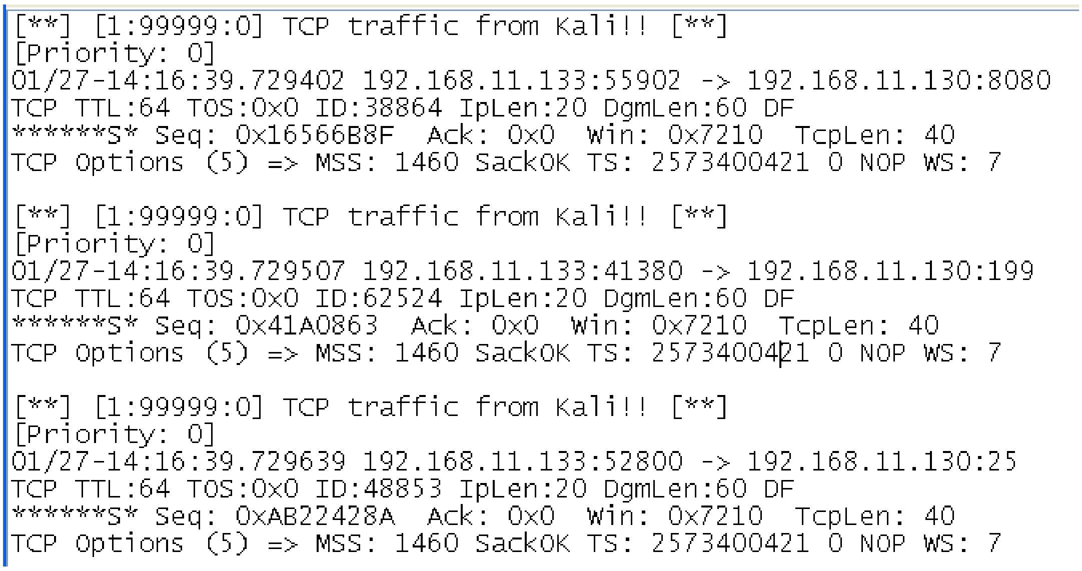
```
include $RULE_PATH\my.rules
```

Any traffic from kali machine is logged



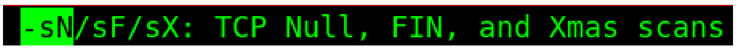
```
alert tcp 192.168.11.133 any -> $HOME_NET any (msg:"TCP traffic from Kali!!"; sid:99999;)
```

Traffic from kali is logged, take note of *s*, it means syn scan



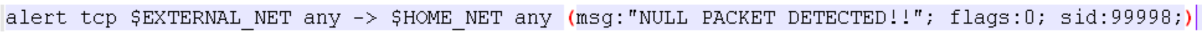
```
[**] [1:99999:0] TCP traffic from Kali!! [**]
[Priority: 0]
01/27-14:16:39.729402 192.168.11.133:55902 -> 192.168.11.130:8080
TCP TTL:64 TOS:0x0 ID:38864 IpLen:20 DgmLen:60 DF
******S* Seq: 0x16566B8F  Ack: 0x0  Win: 0x7210  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 2573400421 0 NOP WS: 7

[**] [1:99999:0] TCP traffic from Kali!! [**]
[Priority: 0]
01/27-14:16:39.729507 192.168.11.133:41380 -> 192.168.11.130:199
TCP TTL:64 TOS:0x0 ID:62524 IpLen:20 DgmLen:60 DF
******S* Seq: 0x41A0863  Ack: 0x0  Win: 0x7210  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 2573400421 0 NOP WS: 7

[**] [1:99999:0] TCP traffic from Kali!! [**]
[Priority: 0]
01/27-14:16:39.729639 192.168.11.133:52800 -> 192.168.11.130:25
TCP TTL:64 TOS:0x0 ID:48853 IpLen:20 DgmLen:60 DF
******S* Seq: 0xAB22428A  Ack: 0x0  Win: 0x7210  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 2573400421 0 NOP WS: 7
```

Nmap null scan



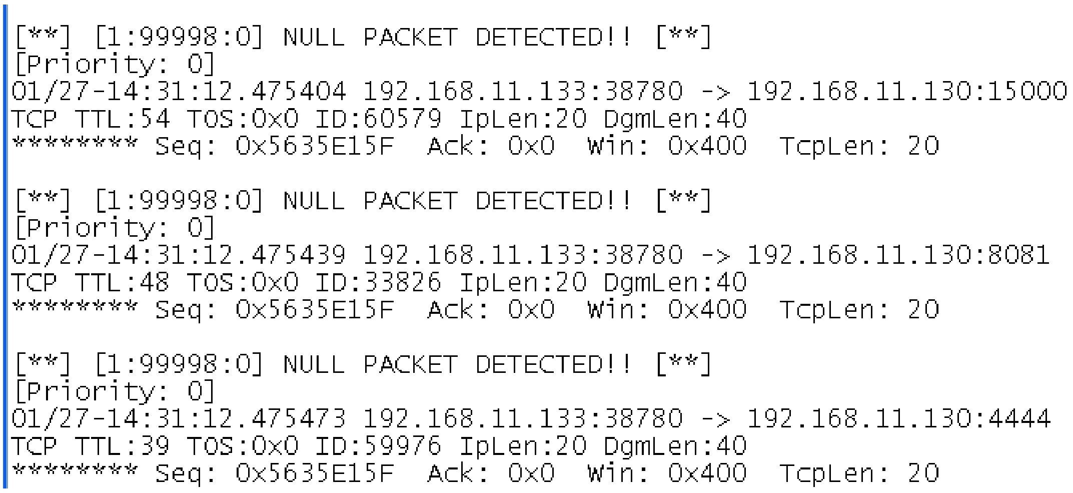
```
-sN/sF/sX: TCP Null, FIN, and Xmas scans
```

Log any null scans



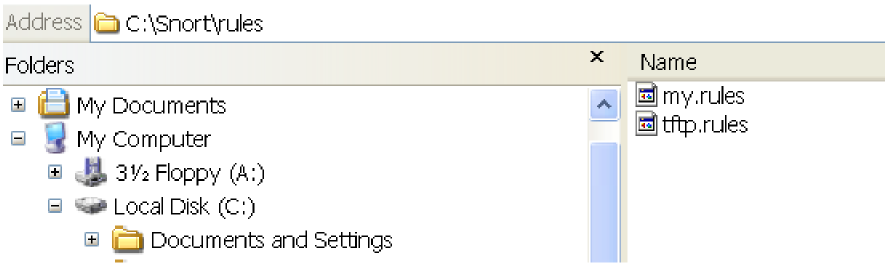
```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"NULL PACKET DETECTED!!"; flags:0; sid:99998;)
```

Null packets logged, take note of all * and no flags



```
[**] [1:99998:0] NULL PACKET DETECTED!! [**]
[Priority: 0]
01/27-14:31:12.475404 192.168.11.133:38780 -> 192.168.11.130:15000
TCP TTL:54 TOS:0x0 ID:60579 IpLen:20 DgmLen:40
******** Seq: 0x5635E15F  Ack: 0x0  Win: 0x400  TcpLen: 20

[**] [1:99998:0] NULL PACKET DETECTED!! [**]
[Priority: 0]
01/27-14:31:12.475439 192.168.11.133:38780 -> 192.168.11.130:8081
TCP TTL:48 TOS:0x0 ID:33826 IpLen:20 DgmLen:40
******** Seq: 0x5635E15F  Ack: 0x0  Win: 0x400  TcpLen: 20

[**] [1:99998:0] NULL PACKET DETECTED!! [**]
[Priority: 0]
01/27-14:31:12.475473 192.168.11.133:38780 -> 192.168.11.130:4444
TCP TTL:39 TOS:0x0 ID:59976 IpLen:20 DgmLen:40
******** Seq: 0x5635E15F  Ack: 0x0  Win: 0x400  TcpLen: 20
```

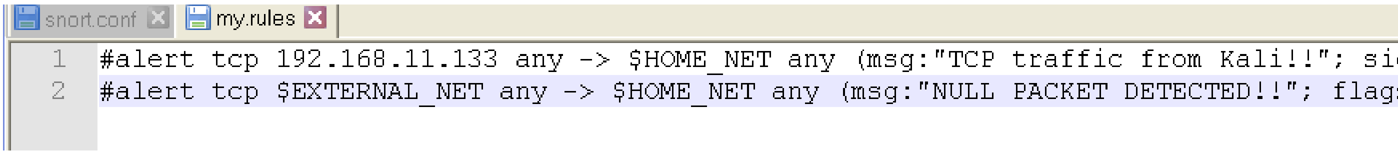
Snort rules for tftp traffic



Include tftp rules in snort.conf

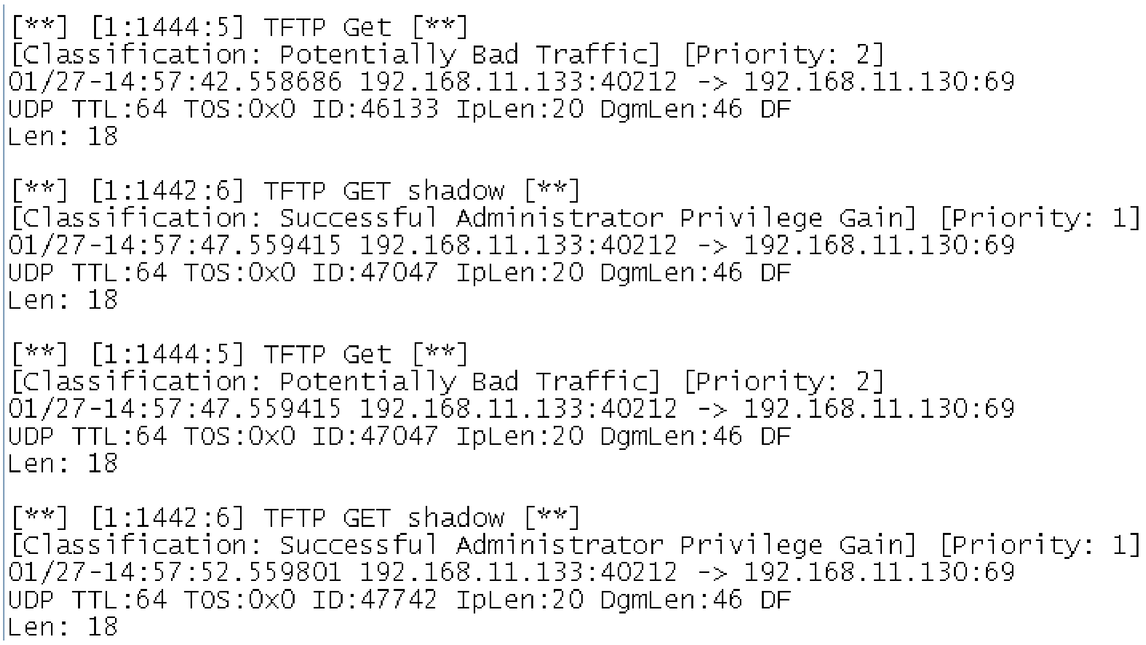
```
include $RULE_PATH\my.rules
include $RULE_PATH\tftp.rules
```

Uncomment any rules in my.rules



```
#alert tcp 192.168.11.133 any -> $HOME_NET any (msg:"TCP traffic from Kali!!"; si
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"NULL PACKET DETECTED!!"; flag
```

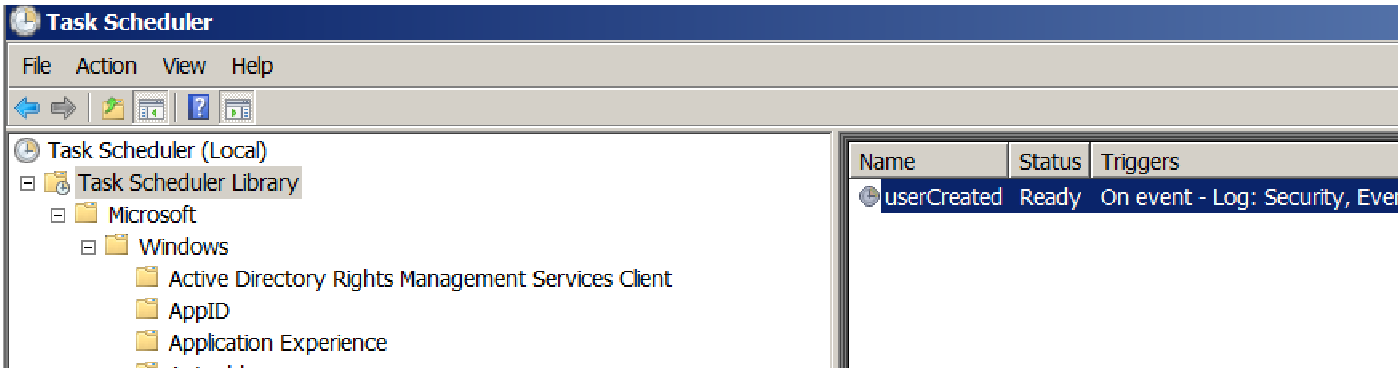
Tftp logs



```
[**] [1:1444:5] TFTP Get [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
01/27-14:57:42.558686 192.168.11.133:40212 -> 192.168.11.130:69
UDP TTL:64 TOS:0x0 ID:46133 IpLen:20 DgmLen:46 DF
Len: 18

[**] [1:1442:6] TFTP GET shadow [**]
[Classification: Successful Administrator Privilege Gain] [Priority: 1]
01/27-14:57:47.559415 192.168.11.133:40212 -> 192.168.11.130:69
UDP TTL:64 TOS:0x0 ID:47047 IpLen:20 DgmLen:46 DF
Len: 18

[**] [1:1444:5] TFTP Get [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
01/27-14:57:47.559415 192.168.11.133:40212 -> 192.168.11.130:69
UDP TTL:64 TOS:0x0 ID:47047 IpLen:20 DgmLen:46 DF
Len: 18

[**] [1:1442:6] TFTP GET shadow [**]
[Classification: Successful Administrator Privilege Gain] [Priority: 1]
01/27-14:57:52.559801 192.168.11.133:40212 -> 192.168.11.130:69
UDP TTL:64 TOS:0x0 ID:47742 IpLen:20 DgmLen:46 DF
Len: 18
```

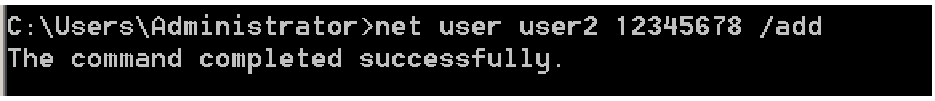
Win2k8 event log

Will display message when new user is created



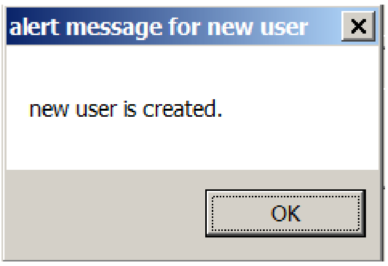
Name	Status	Triggers
userCreated	Ready	On event - Log: Security, Eve

Adding new user



```
C:\Users\Administrator>net user user2 12345678 /add
The command completed successfully.
```

When new user is created, message will pop

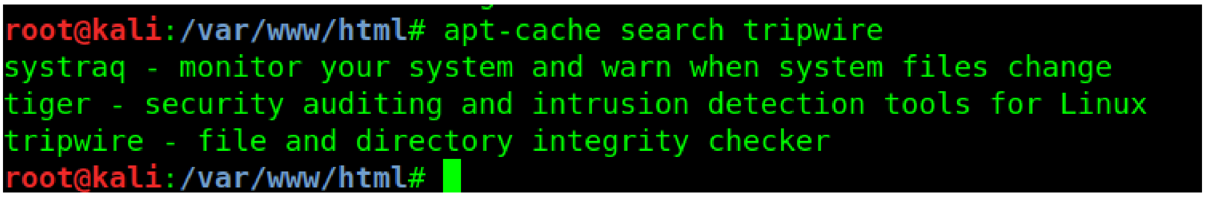


alert message for new user

new user is created.

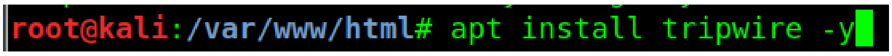
Linux tripwire

Searching for tripwire



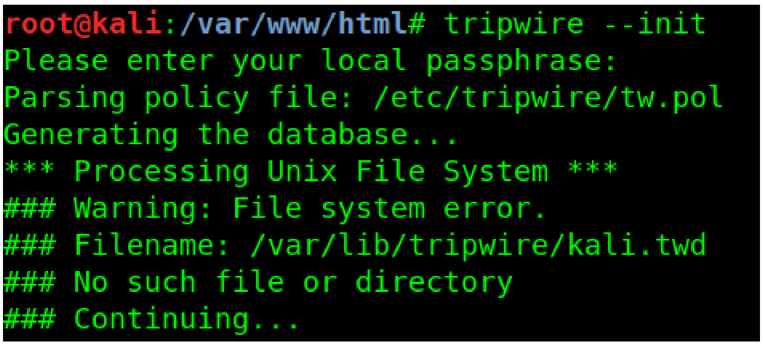
```
root@kali:/var/www/html# apt-cache search tripwire
systraq - monitor your system and warn when system files change
tiger - security auditing and intrusion detection tools for Linux
tripwire - file and directory integrity checker
root@kali:/var/www/html# 
```

Install tripwire



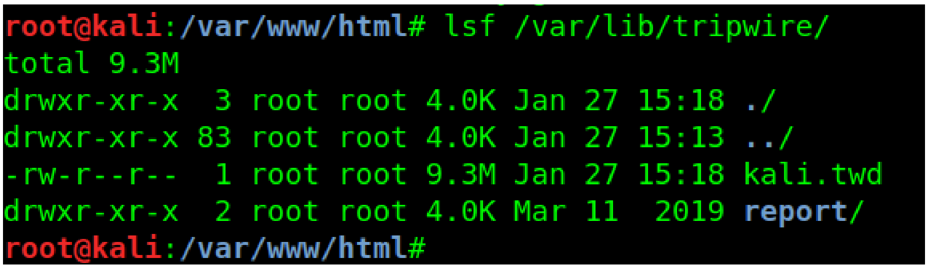
```
root@kali:/var/www/html# apt install tripwire -y
```

Create baseline database

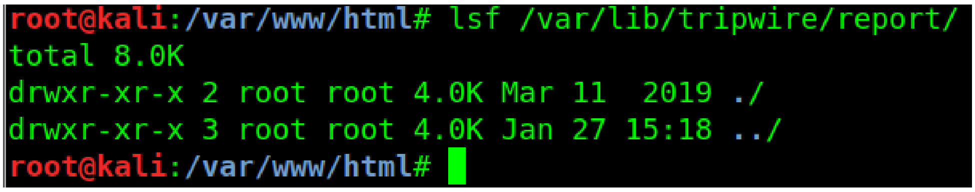


```
root@kali:/var/www/html# tripwire --init
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
### Warning: File system error.
### Filename: /var/lib/tripwire/kali.twd
### No such file or directory
### Continuing...
```

Empty report on first initialization

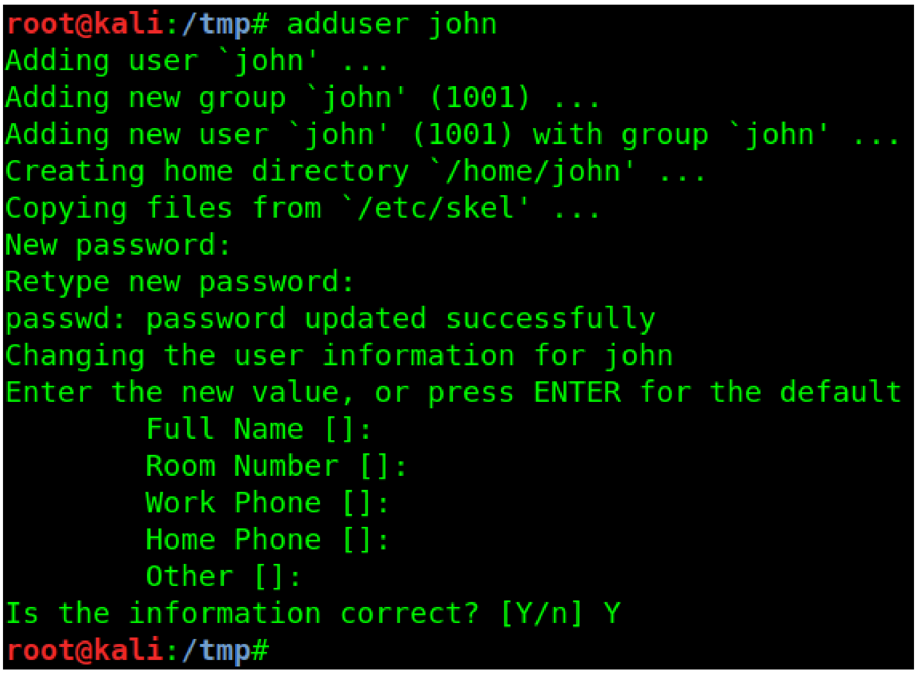


```
root@kali:/var/www/html# lsf /var/lib/tripwire/
total 9.3M
drwxr-xr-x  3 root root 4.0K Jan 27 15:18 ./
drwxr-xr-x 83 root root 4.0K Jan 27 15:13 ../
-rw-r--r--  1 root root 9.3M Jan 27 15:18 kali.twd
drwxr-xr-x  2 root root 4.0K Mar 11  2019 report/
root@kali:/var/www/html#
```



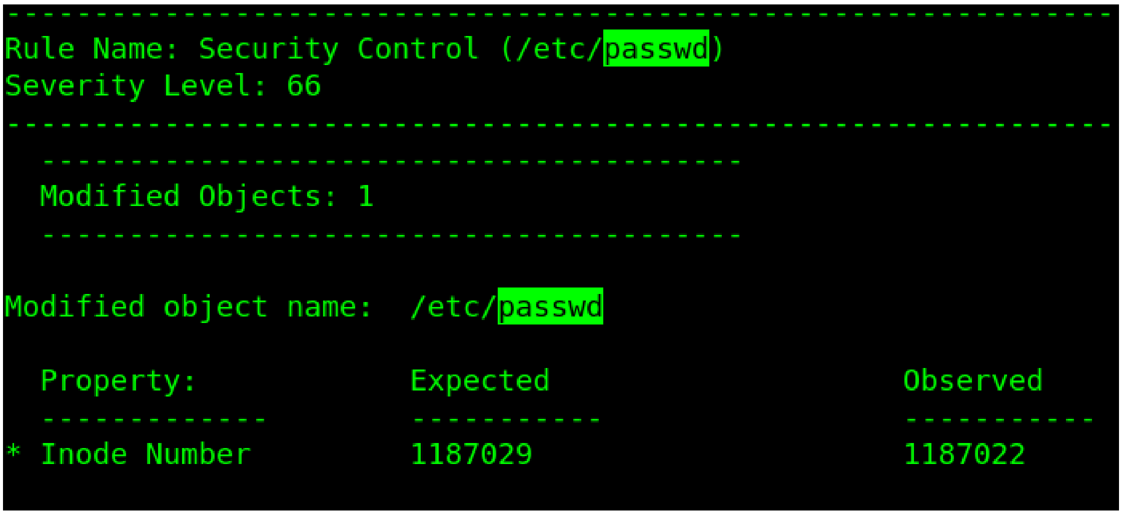
```
root@kali:/var/www/html# lsf /var/lib/tripwire/report/
total 8.0K
drwxr-xr-x 2 root root 4.0K Mar 11  2019 ./
drwxr-xr-x 3 root root 4.0K Jan 27 15:18 ../
root@kali:/var/www/html# 
```

Adduser by the name of john



```
root@kali:/tmp# adduser john
Adding user `john' ...
Adding new group `john' (1001) ...
Adding new user `john' (1001) with group `john' ...
Creating home directory `/home/john' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for john
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
root@kali:/tmp#
```

Notice policy violation



```
-------------------------------------------------------------------------------
Rule Name: Security Control (/etc/passwd)
Severity Level: 66
-------------------------------------------------------------------------------
  ----------------------------------------
  Modified Objects: 1
  ----------------------------------------

Modified object name:  /etc/passwd

  Property:            Expected                    Observed
  -------------        -----------                 -----------
* Inode Number         1187029                     1187022
```