VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Information Security Management
CSE3502

Lab Assignment 6
SNORT Revision & Social Engineering Tools

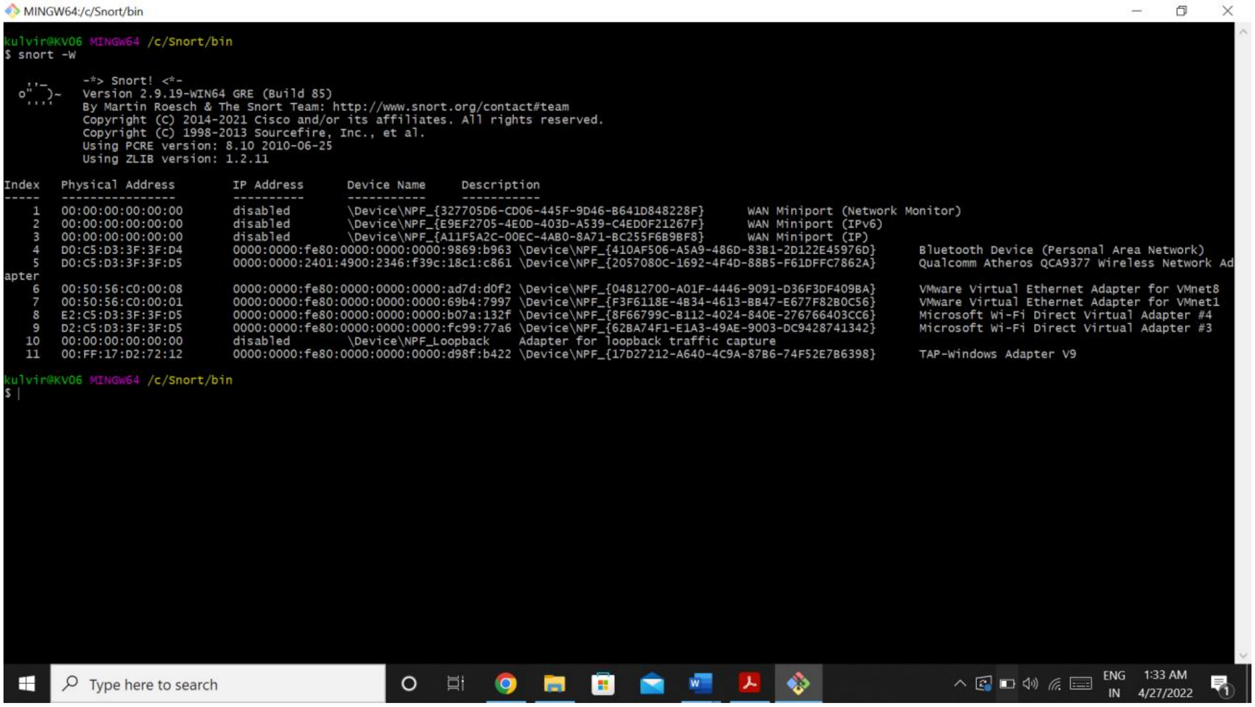
Slot : L25+L26

Name : Kulvir Singh

Register Number : 19BCE2074

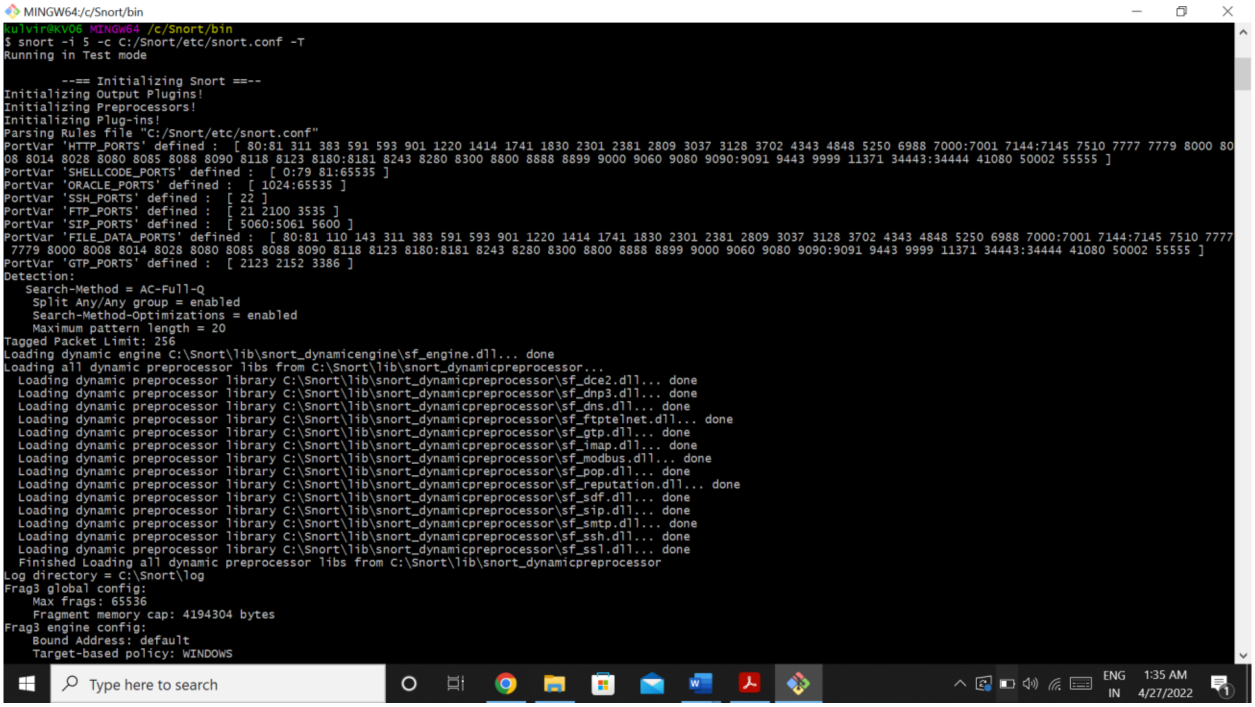
SNORT Experiment :

Command 1-> snort -W



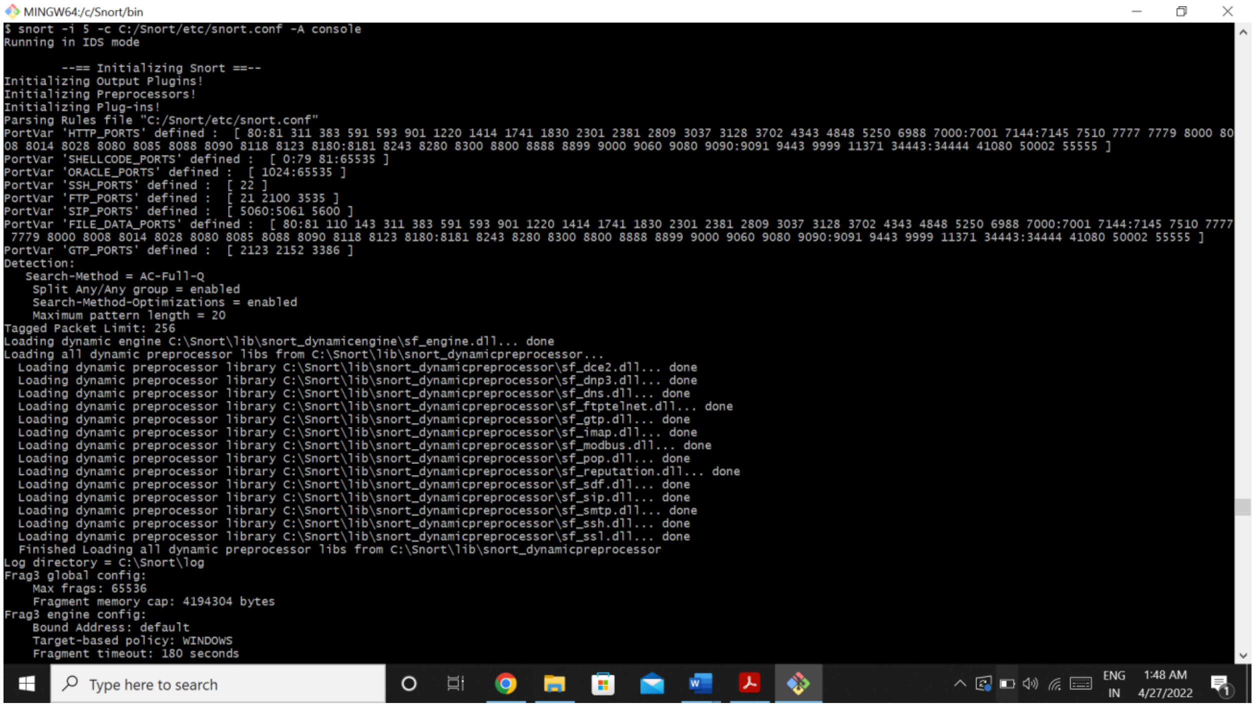
```
kulvir@KV06 MINGW64 /c/Snort/bin
$ snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 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

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{327705D6-CD06-445F-9D46-B641D848228F}      WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{E9EF2705-4E0D-403D-A539-C4ED0F21267F}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{A11F5A2C-00EC-4AB0-8A71-BC255F6B9BF8}      WAN Miniport (IP)
    4   D0:C5:D3:3F:3F:D4       0000:0000:fe80:0000:0000:0000:9869:b963 \Device\NPF_{410AF506-A5A9-486D-83B1-2D122E45976D}      Bluetooth Device (Personal Area Network)
    5   D0:C5:D3:3F:3F:D5       0000:0000:2401:4900:2346:f39c:18c1:c861 \Device\NPF_{2057080C-1692-4F4D-88B5-F61DFFC7862A}      Qualcomm Atheros QCA9377 Wireless Network Ad
apter
    6   00:50:56:C0:00:08       0000:0000:fe80:0000:0000:0000:ad7d:d0f2 \Device\NPF_{04812700-A01F-4446-9091-D36F3DF409BA}      VMware Virtual Ethernet Adapter for VMnet8
    7   00:50:56:C0:00:01       0000:0000:fe80:0000:0000:0000:69b4:7997 \Device\NPF_{F3F6118E-4B34-4613-BB47-E677F82B0C56}      VMware Virtual Ethernet Adapter for VMnet1
    8   E2:C5:D3:3F:3F:D5       0000:0000:fe80:0000:0000:0000:b07a:132f \Device\NPF_{8F66799C-B112-4024-840E-276766403CC6}      Microsoft Wi-Fi Direct Virtual Adapter #4
    9   D2:C5:D3:3F:3F:D5       0000:0000:fe80:0000:0000:0000:fc99:77a6 \Device\NPF_{62BA74F1-E1A3-49AE-9003-DC9428741342}      Microsoft Wi-Fi Direct Virtual Adapter #3
   10   00:00:00:00:00:00       disabled        \Device\NPF_Loopback    Adapter for loopback traffic capture
   11   00:FF:17:D2:72:12       0000:0000:fe80:0000:0000:0000:d98f:b422 \Device\NPF_{17D27212-A640-4C9A-87B6-74F52E7B6398}      TAP-Windows Adapter V9

kulvir@KV06 MINGW64 /c/Snort/bin
$ |
```

Command 2-> snort -i 5 -c C:/Snort/etc/snort.conf -T



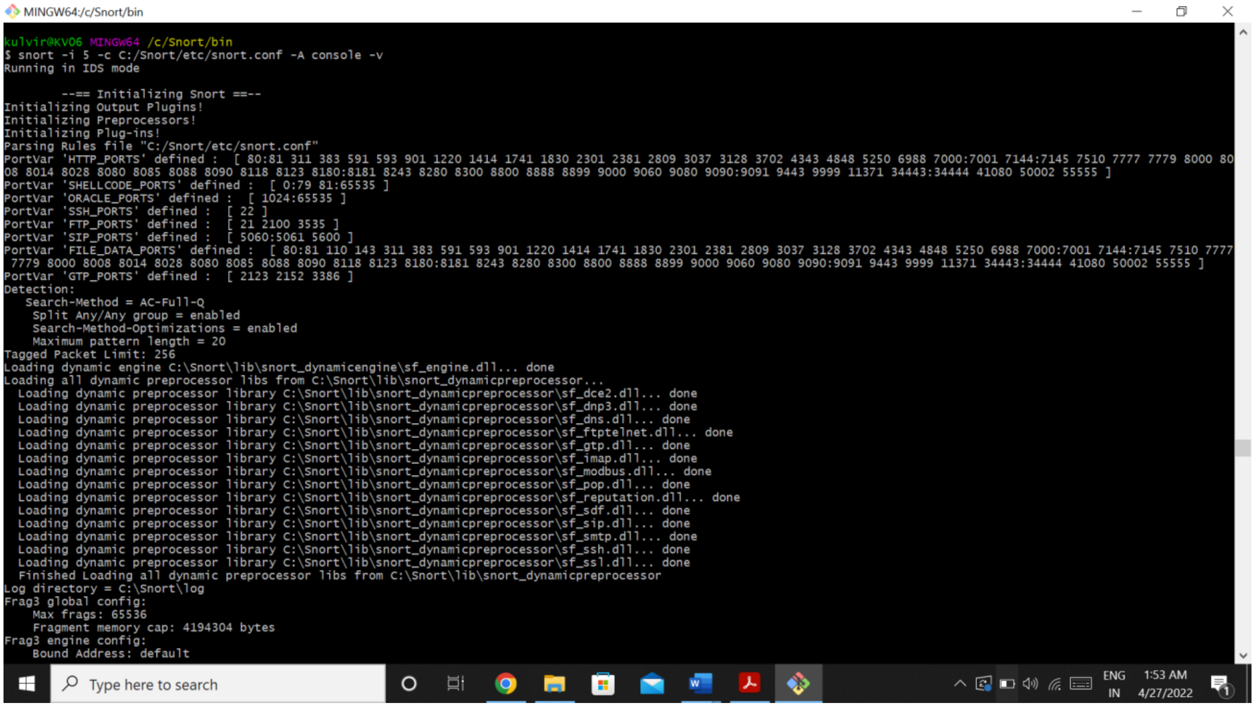
```
kulvir@KV06 MINGW64 /c/Snort/bin
$ snort -i 5 -c C:/Snort/etc/snort.conf -T
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:/Snort/etc/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 80
08 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 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 '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 C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
  Finished Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor
Log directory = C:\Snort\log
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
    Bound Address: default
    Target-based policy: WINDOWS
```

Command 3-> snort -i 5 -c C:/Snort/etc/snort.conf -A console

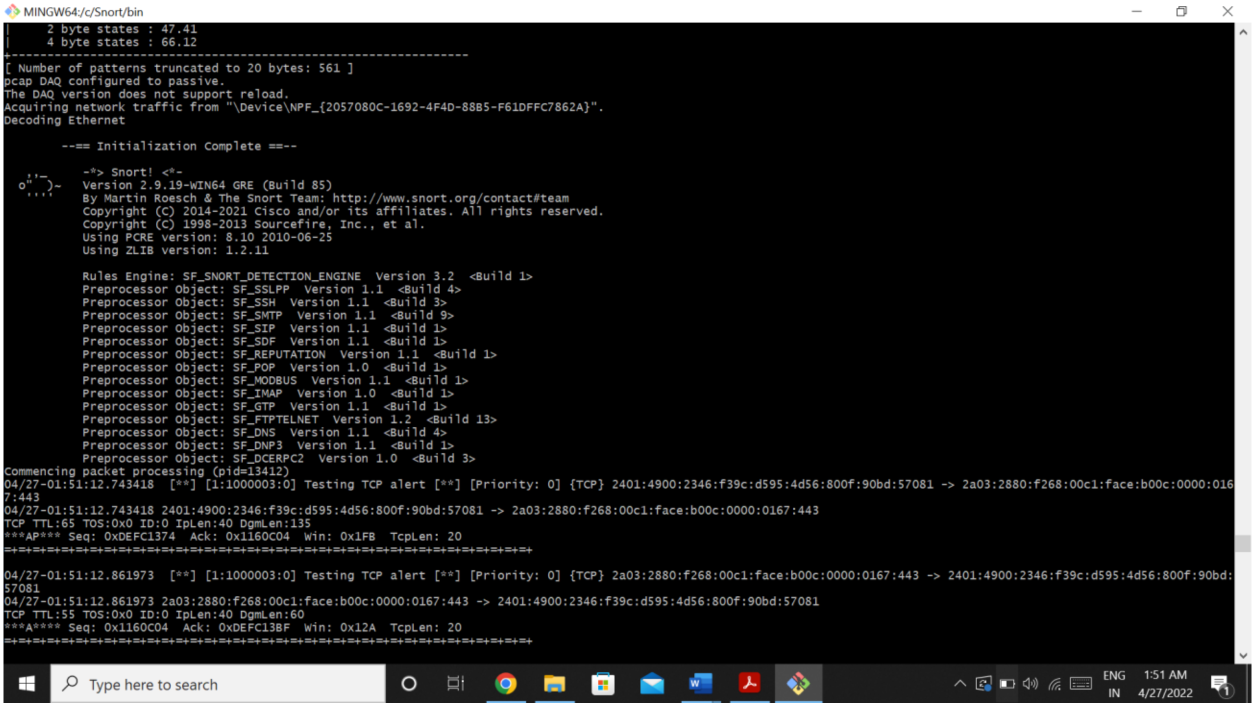


```
$ snort -i 5 -c C:/Snort/etc/snort.conf -A console
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:/Snort/etc/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 80
08 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 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 '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 C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
  Finished Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor
Log directory = C:\Snort\log
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
    Bound Address: default
    Target-based policy: WINDOWS
    Fragment timeout: 180 seconds
```

Command 4-> snort -i 5 -c C:/Snort/etc/snort.conf -A console -v

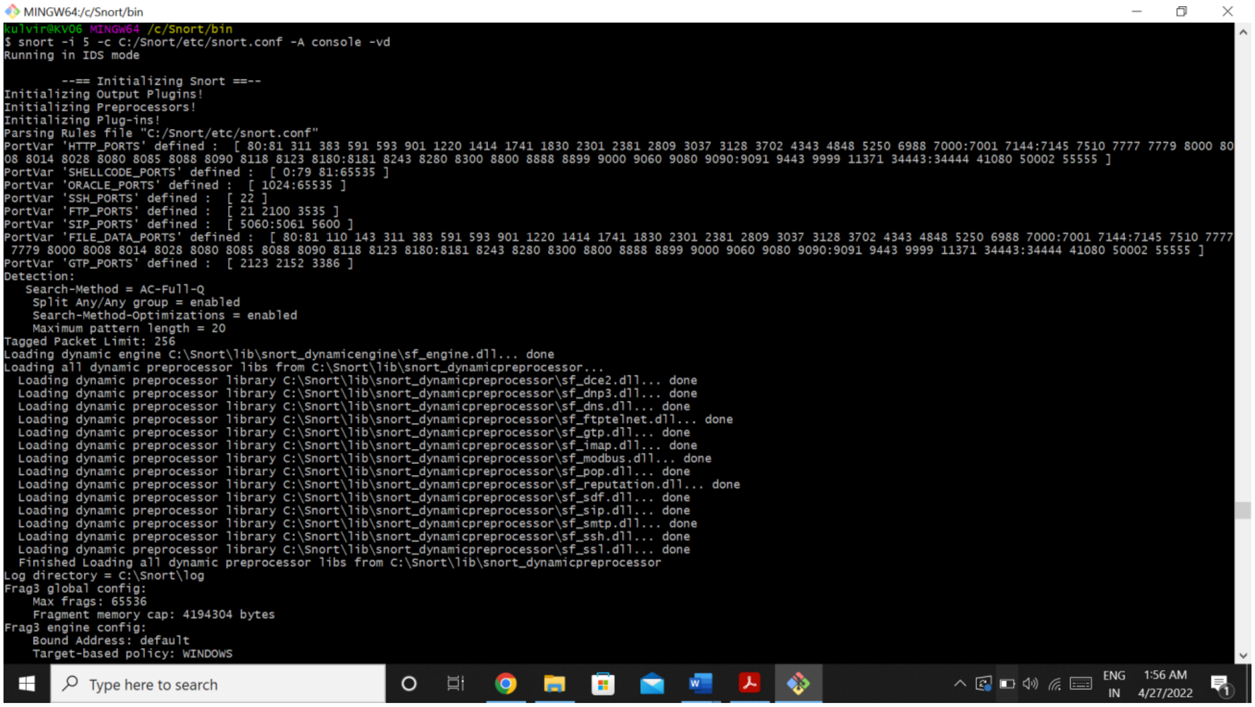


```
kulvir@KV06 MINGW64 /c/Snort/bin
$ snort -i 5 -c C:/Snort/etc/snort.conf -A console -v
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:/Snort/etc/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 80
08 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 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 '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 C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
  Finished Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor
Log directory = C:\Snort\log
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
    Bound Address: default
```

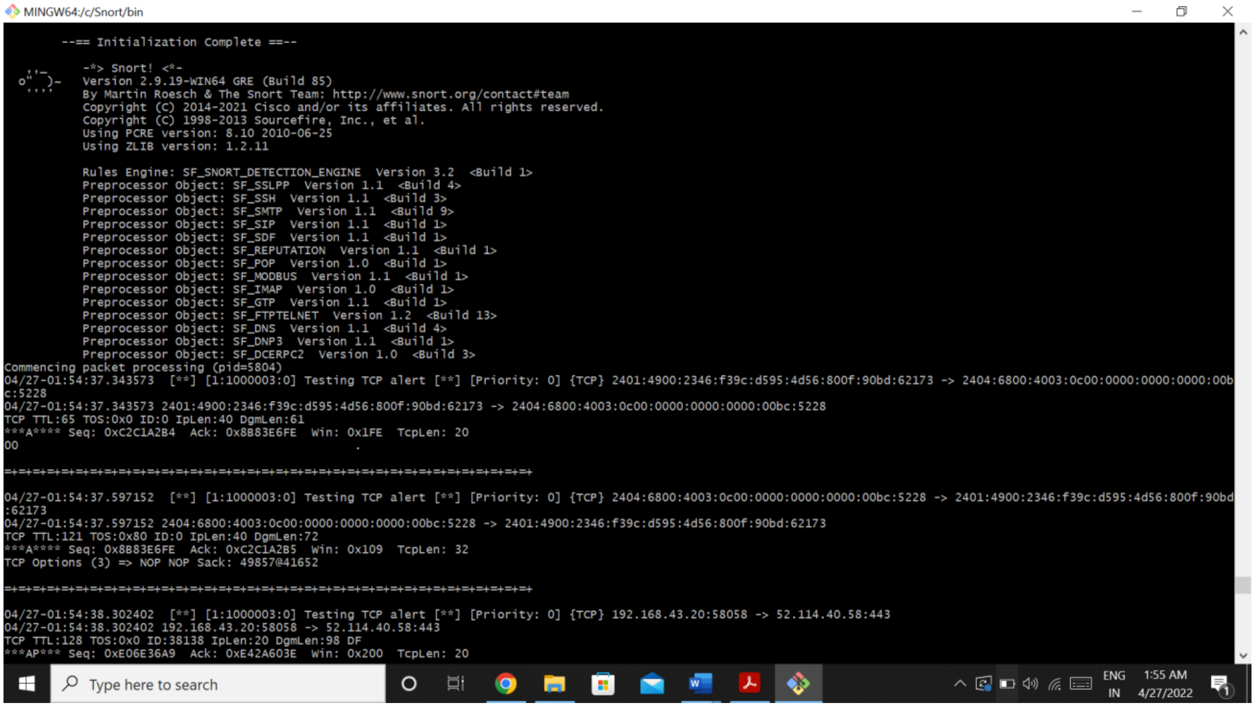


```
|     2 byte states : 47.41
|     4 byte states : 66.12
+-----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 561 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{2057080C-1692-4F4D-88B5-F61DFFC7862A}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 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 3.2  <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=13412)
04/27-01:51:12.743418  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2401:4900:2346:f39c:d595:4d56:800f:90bd:57081 -> 2a03:2880:f268:00c1:face:b00c:0000:016
7:443
04/27-01:51:12.743418 2401:4900:2346:f39c:d595:4d56:800f:90bd:57081 -> 2a03:2880:f268:00c1:face:b00c:0000:0167:443
TCP TTL:65 TOS:0x0 ID:0 IpLen:40 DgmLen:135
***AP*** Seq: 0xDEFC1374  Ack: 0x1160C04  Win: 0x1FB  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/27-01:51:12.861973  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a03:2880:f268:00c1:face:b00c:0000:0167:443 -> 2401:4900:2346:f39c:d595:4d56:800f:90bd:
57081
04/27-01:51:12.861973 2a03:2880:f268:00c1:face:b00c:0000:0167:443 -> 2401:4900:2346:f39c:d595:4d56:800f:90bd:57081
TCP TTL:55 TOS:0x0 ID:0 IpLen:40 DgmLen:60
***A**** Seq: 0x1160C04  Ack: 0xDEFC13BF  Win: 0x12A  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

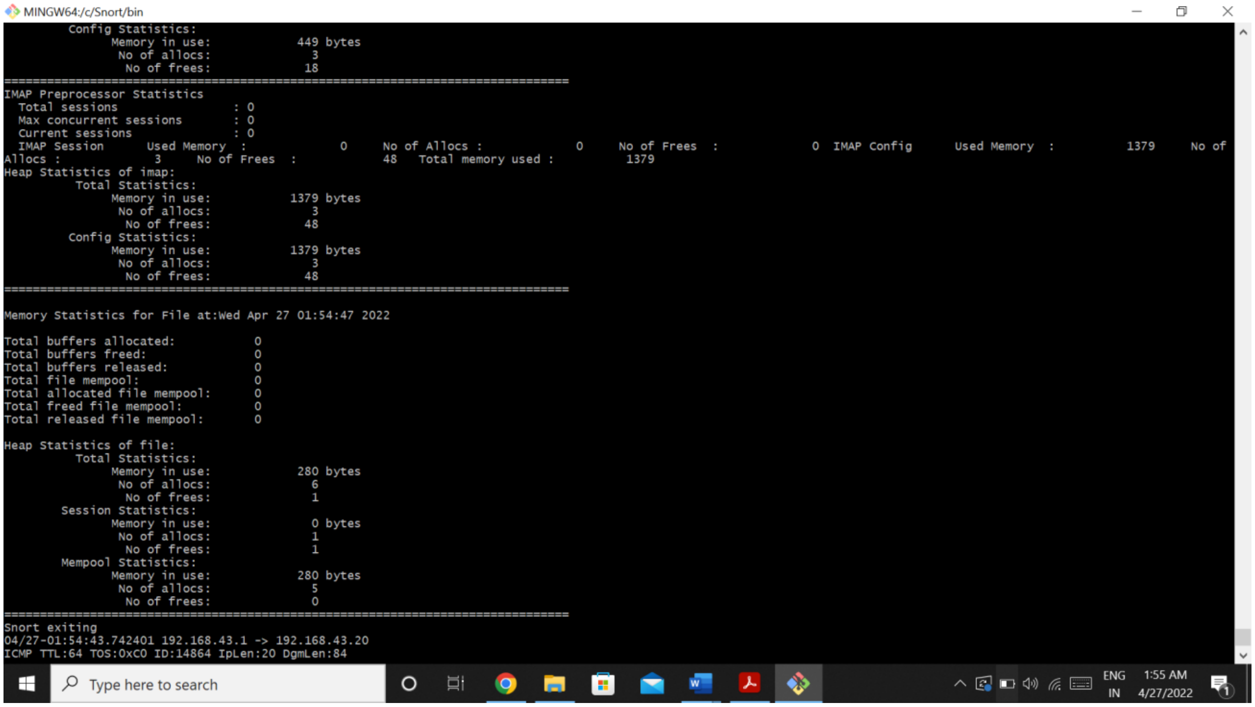
Command 5-> snort -i 5 -c C:/Snort/etc/snort.conf -A console -vd



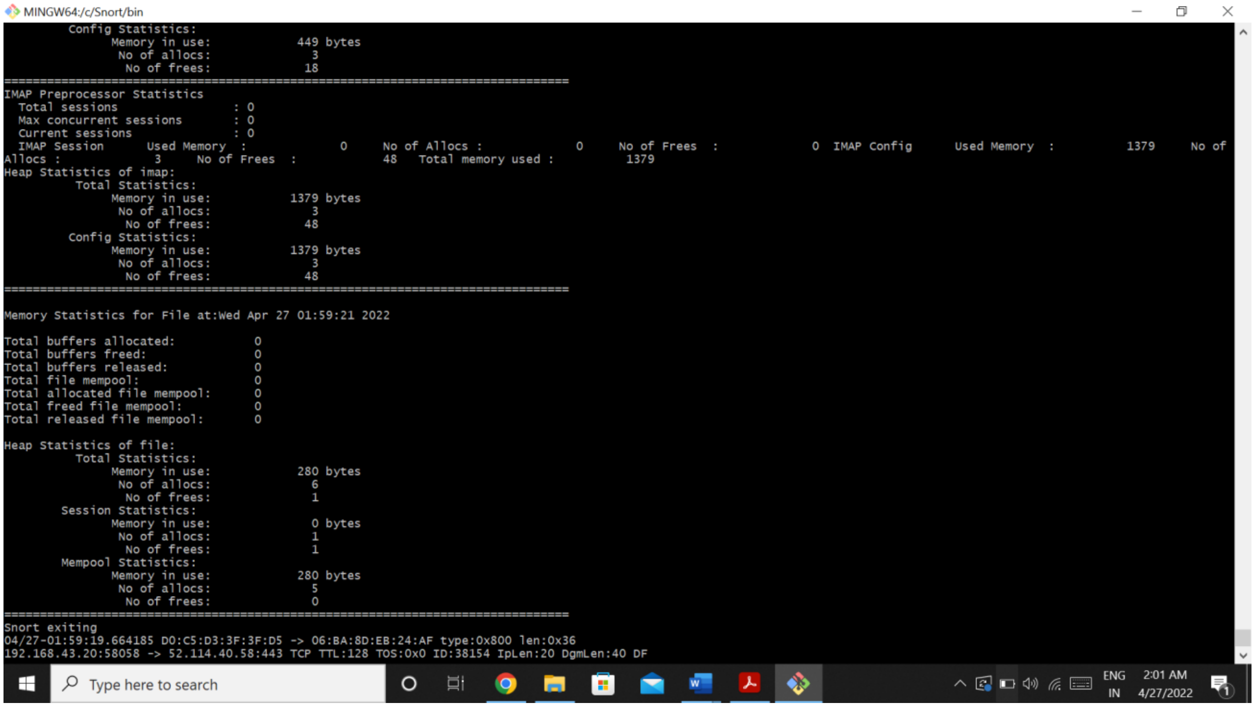
```
kulvir@KV06 MINGW64 /c/Snort/bin
$ snort -i 5 -c C:/Snort/etc/snort.conf -A console -vd
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:/Snort/etc/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 80
08 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 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 '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 C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
  Finished Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor
Log directory = C:\Snort\log
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
    Bound Address: default
    Target-based policy: WINDOWS
```



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

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 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 3.2  <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=5804)
04/27-01:54:37.343573  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2401:4900:2346:f39c:d595:4d56:800f:90bd:62173 -> 2404:6800:4003:0c00:0000:0000:0000:00b
c:5228
04/27-01:54:37.343573 2401:4900:2346:f39c:d595:4d56:800f:90bd:62173 -> 2404:6800:4003:0c00:0000:0000:0000:00bc:5228
TCP TTL:65 TOS:0x0 ID:0 IpLen:40 DgmLen:61
***A**** Seq: 0xC2C1A2B4  Ack: 0x8B83E6FE  Win: 0x1FE  TcpLen: 20
00                                                    .

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

04/27-01:54:37.597152  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2404:6800:4003:0c00:0000:0000:0000:00bc:5228 -> 2401:4900:2346:f39c:d595:4d56:800f:90bd
:62173
04/27-01:54:37.597152 2404:6800:4003:0c00:0000:0000:0000:00bc:5228 -> 2401:4900:2346:f39c:d595:4d56:800f:90bd:62173
TCP TTL:121 TOS:0x80 ID:0 IpLen:40 DgmLen:72
***A**** Seq: 0x8B83E6FE  Ack: 0xC2C1A2B5  Win: 0x109  TcpLen: 32
TCP Options (3) => NOP NOP Sack: 49857@41652

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

04/27-01:54:38.302402  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 192.168.43.20:58058 -> 52.114.40.58:443
04/27-01:54:38.302402 192.168.43.20:58058 -> 52.114.40.58:443
TCP TTL:128 TOS:0x0 ID:38138 IpLen:20 DgmLen:98 DF
***AP*** Seq: 0xE06E36A9  Ack: 0xE42A603E  Win: 0x200  TcpLen: 20
```

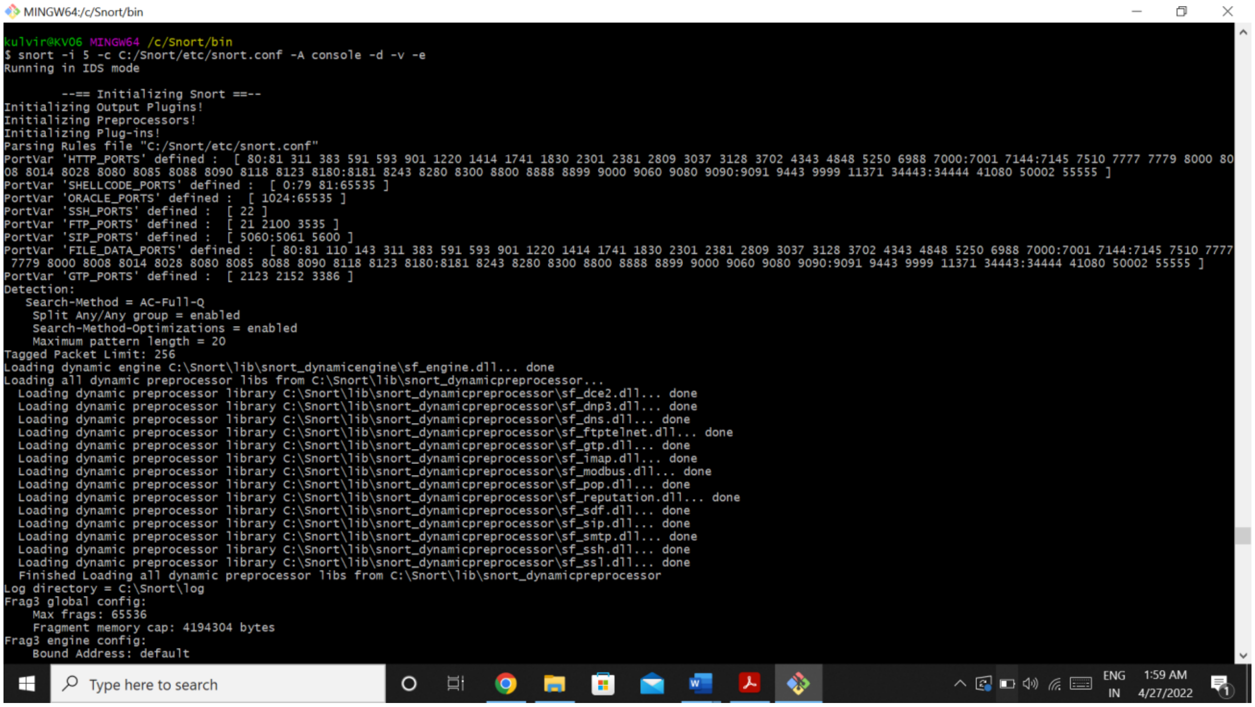


```
         Config Statistics:
               Memory in use:            449 bytes
                No of allocs:              3
                 No of frees:             18
===============================================================================
IMAP Preprocessor Statistics
  Total sessions                  : 0
  Max concurrent sessions         : 0
  Current sessions                : 0
  IMAP Session      Used Memory  :             0     No of Allocs :             0     No of Frees  :             0  IMAP Config      Used Memory  :          1379     No of
Allocs :             3     No of Frees  :            48   Total memory used :          1379
Heap Statistics of imap:
          Total Statistics:
               Memory in use:           1379 bytes
                No of allocs:              3
                 No of frees:             48
         Config Statistics:
               Memory in use:           1379 bytes
                No of allocs:              3
                 No of frees:             48
===============================================================================

Memory Statistics for File at:Wed Apr 27 01:54:47 2022

Total buffers allocated:           0
Total buffers freed:               0
Total buffers released:            0
Total file mempool:                0
Total allocated file mempool:      0
Total freed file mempool:          0
Total released file mempool:       0

Heap Statistics of file:
          Total Statistics:
               Memory in use:            280 bytes
                No of allocs:              6
                 No of frees:              1
        Session Statistics:
               Memory in use:              0 bytes
                No of allocs:              1
                 No of frees:              1
        Mempool Statistics:
               Memory in use:            280 bytes
                No of allocs:              5
                 No of frees:              0
===============================================================================
Snort exiting
04/27-01:54:43.742401 192.168.43.1 -> 192.168.43.20
ICMP TTL:64 TOS:0xC0 ID:14864 IpLen:20 DgmLen:84
```

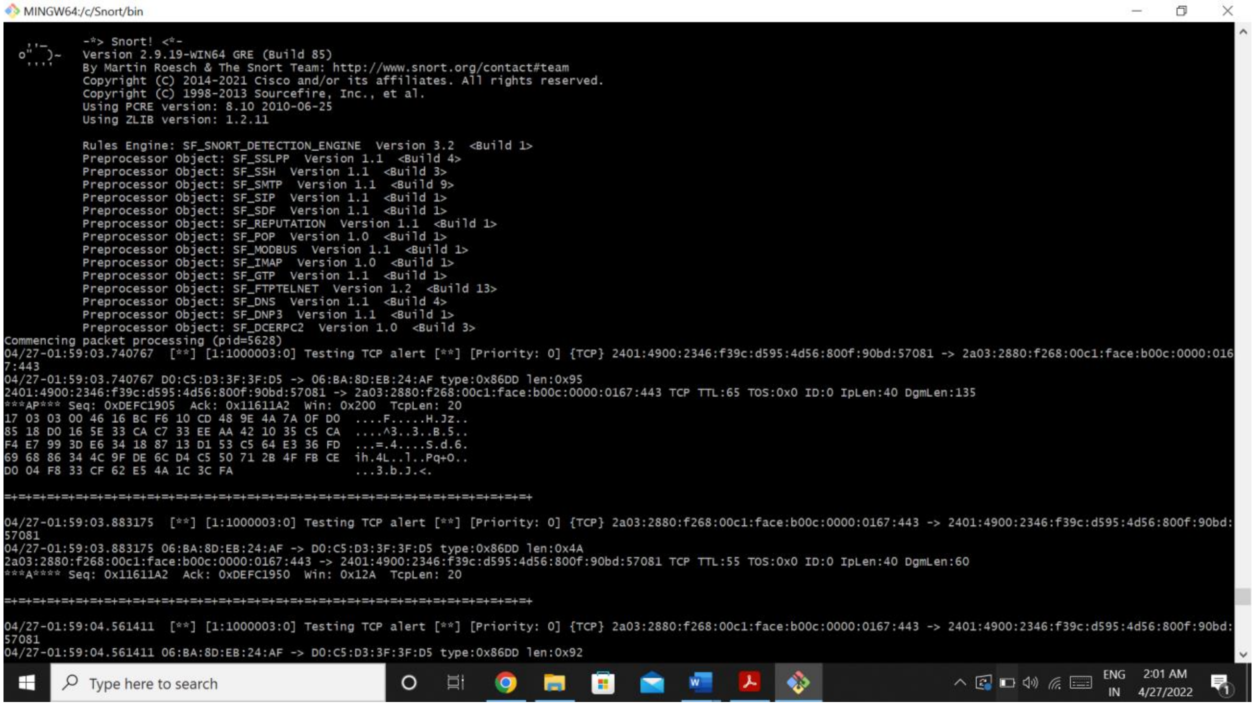


```
         Config Statistics:
               Memory in use:            449 bytes
                No of allocs:              3
                 No of frees:             18
===============================================================================
IMAP Preprocessor Statistics
  Total sessions                  : 0
  Max concurrent sessions         : 0
  Current sessions                : 0
  IMAP Session      Used Memory  :             0     No of Allocs :             0     No of Frees  :             0  IMAP Config      Used Memory  :          1379     No of
Allocs :             3     No of Frees  :            48   Total memory used :          1379
Heap Statistics of imap:
          Total Statistics:
               Memory in use:           1379 bytes
                No of allocs:              3
                 No of frees:             48
         Config Statistics:
               Memory in use:           1379 bytes
                No of allocs:              3
                 No of frees:             48
===============================================================================

Memory Statistics for File at:Wed Apr 27 01:59:21 2022

Total buffers allocated:           0
Total buffers freed:               0
Total buffers released:            0
Total file mempool:                0
Total allocated file mempool:      0
Total freed file mempool:          0
Total released file mempool:       0

Heap Statistics of file:
          Total Statistics:
               Memory in use:            280 bytes
                No of allocs:              6
                 No of frees:              1
        Session Statistics:
               Memory in use:              0 bytes
                No of allocs:              1
                 No of frees:              1
        Mempool Statistics:
               Memory in use:            280 bytes
                No of allocs:              5
                 No of frees:              0
===============================================================================
Snort exiting
04/27-01:59:19.664185 D0:C5:D3:3F:3F:D5 -> 06:BA:8D:EB:24:AF type:0x800 len:0x36
192.168.43.20:58058 -> 52.114.40.58:443 TCP TTL:128 TOS:0x0 ID:38154 IpLen:20 DgmLen:40 DF
```

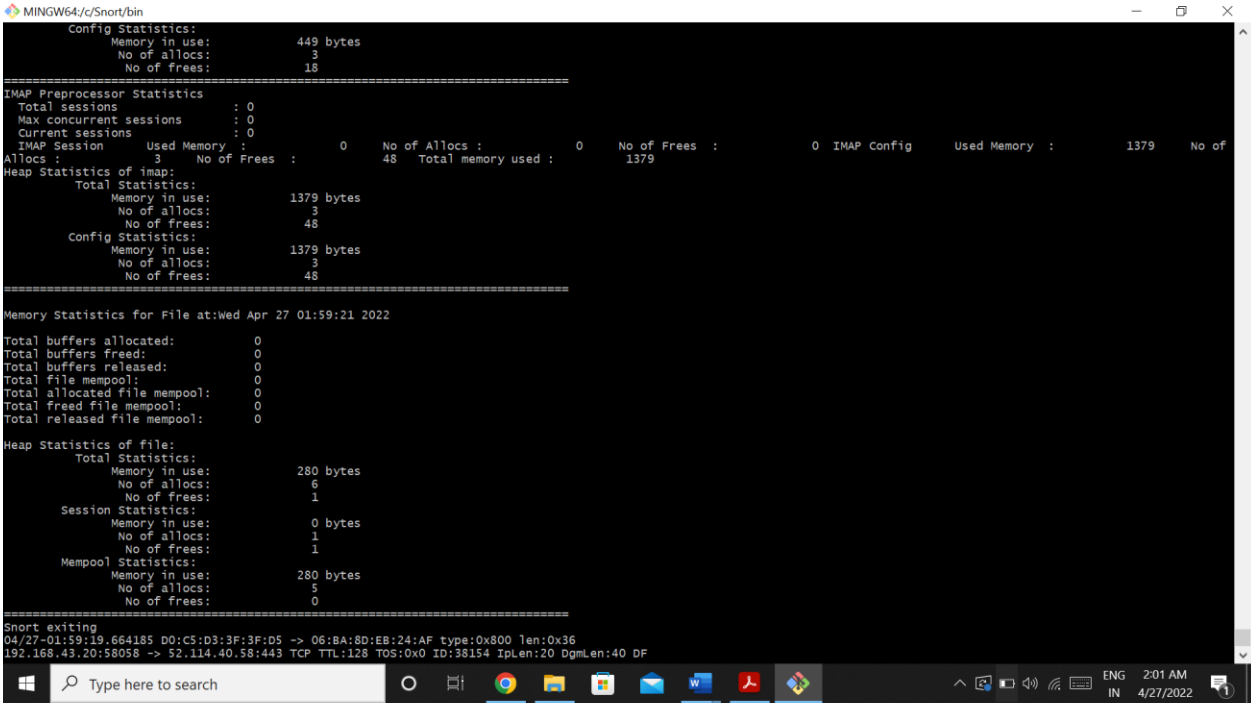
Command 6-> snort -i 5 -c C:/Snort/etc/snort.conf -A console -d -v -e



```
kulvir@KV06 MINGW64 /c/Snort/bin
$ snort -i 5 -c C:/Snort/etc/snort.conf -A console -d -v -e
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:/Snort/etc/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 80
08 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 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 '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 C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
  Finished Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor
Log directory = C:\Snort\log
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
    Bound Address: default
```



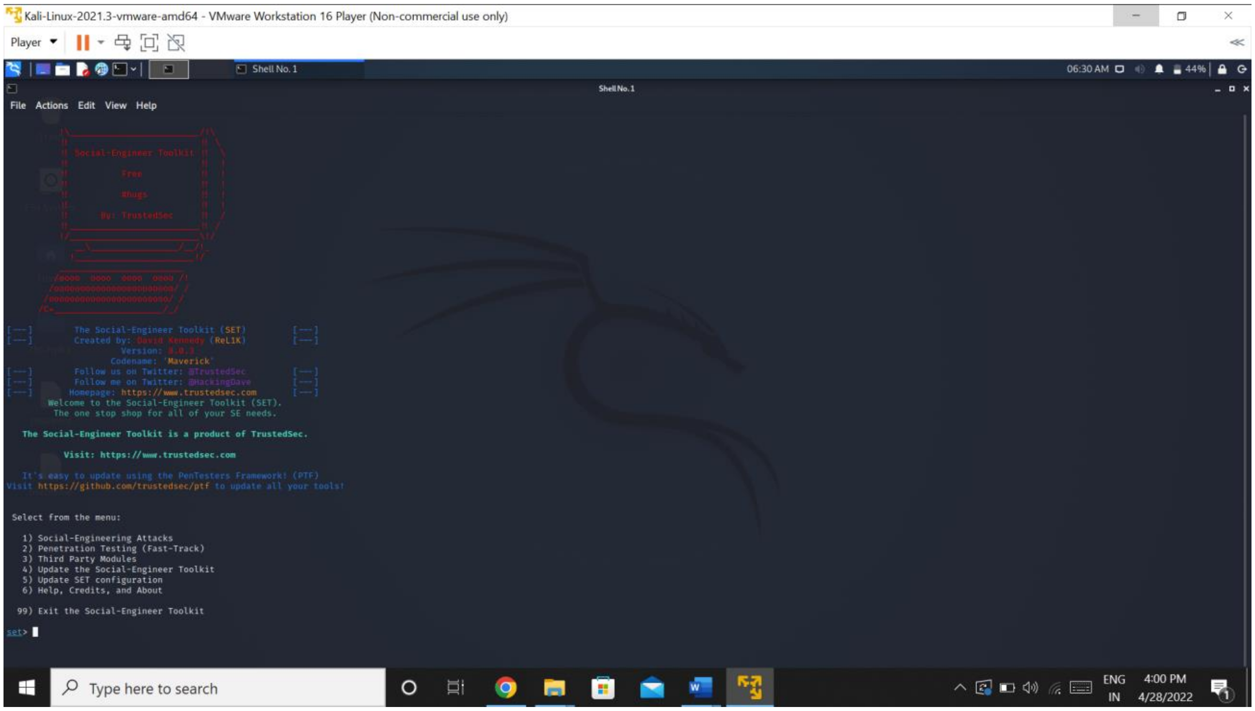
```
   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <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=5628)
04/27-01:59:03.740767  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2401:4900:2346:f39c:d595:4d56:800f:90bd:57081 -> 2a03:2880:f268:00c1:face:b00c:0000:016
7:443
04/27-01:59:03.740767 D0:C5:D3:3F:3F:D5 -> 06:BA:8D:EB:24:AF type:0x86DD len:0x95
2401:4900:2346:f39c:d595:4d56:800f:90bd:57081 -> 2a03:2880:f268:00c1:face:b00c:0000:0167:443 TCP TTL:65 TOS:0x0 ID:0 IpLen:40 DgmLen:135
***AP*** Seq: 0xDEFC1905  Ack: 0x11611A2  Win: 0x200  TcpLen: 20
17 03 03 00 46 16 BC F6 10 CD 48 9E 4A 7A 0F D0  ....F.....H.Jz..
85 18 D0 16 5E 33 CA C7 33 EE AA 42 10 35 C5 CA  ....^3..3..B.5..
F4 E7 99 3D E6 34 18 87 13 D1 53 C5 64 E3 36 FD  ...=.4....S.d.6.
69 68 86 34 4C 9F DE 6C D4 C5 50 71 2B 4F FB CE  ih.4L..l..Pq+O..
D0 04 F8 33 CF 62 E5 4A 1C 3C FA                 ...3.b.J.<.

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

04/27-01:59:03.883175  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a03:2880:f268:00c1:face:b00c:0000:0167:443 -> 2401:4900:2346:f39c:d595:4d56:800f:90bd:
57081
04/27-01:59:03.883175 06:BA:8D:EB:24:AF -> D0:C5:D3:3F:3F:D5 type:0x86DD len:0x4A
2a03:2880:f268:00c1:face:b00c:0000:0167:443 -> 2401:4900:2346:f39c:d595:4d56:800f:90bd:57081 TCP TTL:55 TOS:0x0 ID:0 IpLen:40 DgmLen:60
***A**** Seq: 0x11611A2  Ack: 0xDEFC1950  Win: 0x12A  TcpLen: 20

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

04/27-01:59:04.561411  [**] [1:1000003:0] Testing TCP alert [**] [Priority: 0] {TCP} 2a03:2880:f268:00c1:face:b00c:0000:0167:443 -> 2401:4900:2346:f39c:d595:4d56:800f:90bd:
57081
04/27-01:59:04.561411 06:BA:8D:EB:24:AF -> D0:C5:D3:3F:3F:D5 type:0x86DD len:0x92
```



```
         Config Statistics:
                Memory in use:           449 bytes
                 No of allocs:             3
                  No of frees:            18
===============================================================================
IMAP Preprocessor Statistics
  Total sessions                : 0
  Max concurrent sessions       : 0
  Current sessions              : 0
  IMAP Session      Used Memory  :             0     No of Allocs :              0     No of Frees   :              0  IMAP Config      Used Memory  :           1379     No of
Allocs :          3     No of Frees   :            48   Total memory used :         1379
Heap Statistics of imap:
          Total Statistics:
                Memory in use:          1379 bytes
                 No of allocs:             3
                  No of frees:            48
         Config Statistics:
                Memory in use:          1379 bytes
                 No of allocs:             3
                  No of frees:            48
===============================================================================

Memory Statistics for File at:Wed Apr 27 01:59:21 2022

Total buffers allocated:          0
Total buffers freed:              0
Total buffers released:           0
Total file mempool:               0
Total allocated file mempool:     0
Total freed file mempool:         0
Total released file mempool:      0

Heap Statistics of file:
          Total Statistics:
                Memory in use:           280 bytes
                 No of allocs:             6
                  No of frees:             1
        Session Statistics:
                Memory in use:             0 bytes
                 No of allocs:             1
                  No of frees:             1
        Mempool Statistics:
                Memory in use:           280 bytes
                 No of allocs:             5
                  No of frees:             0
===============================================================================
Snort exiting
04/27-01:59:19.664185 D0:C5:D3:3F:3F:D5 -> 06:BA:8D:EB:24:AF type:0x800 len:0x36
192.168.43.20:58058 -> 52.114.40.58:443 TCP TTL:128 TOS:0x0 ID:38154 IpLen:20 DgmLen:40 DF
```

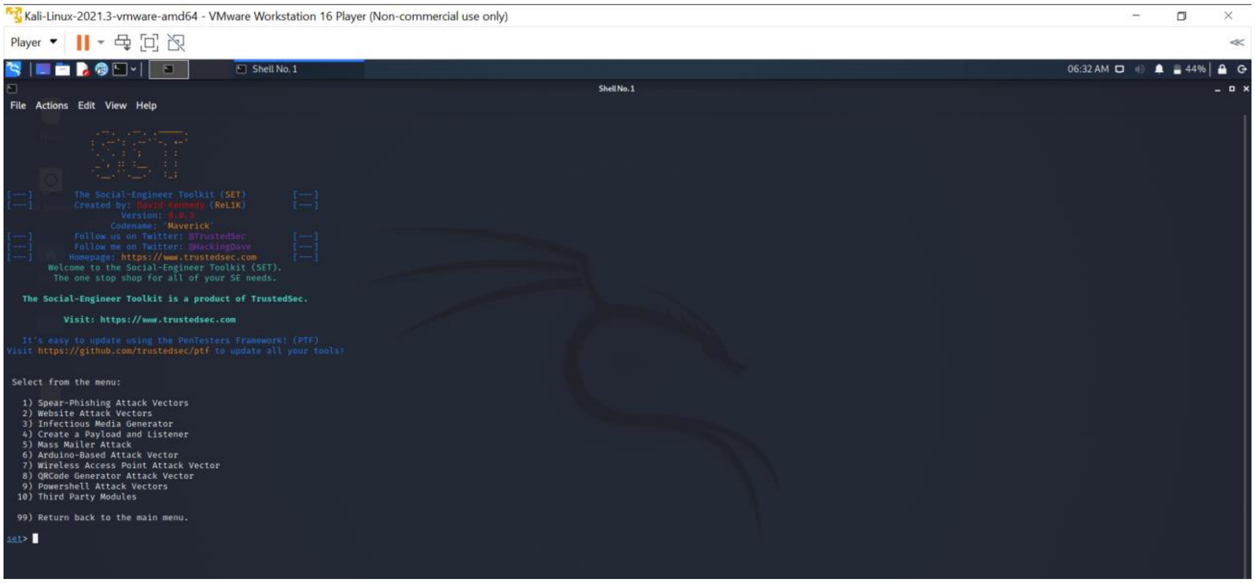
Social Engineering Tool

SET installed :


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Shell No. 1
06:30 AM
44%
File Actions Edit View Help
Type here to search
ENG
IN
4:00 PM
4/28/2022

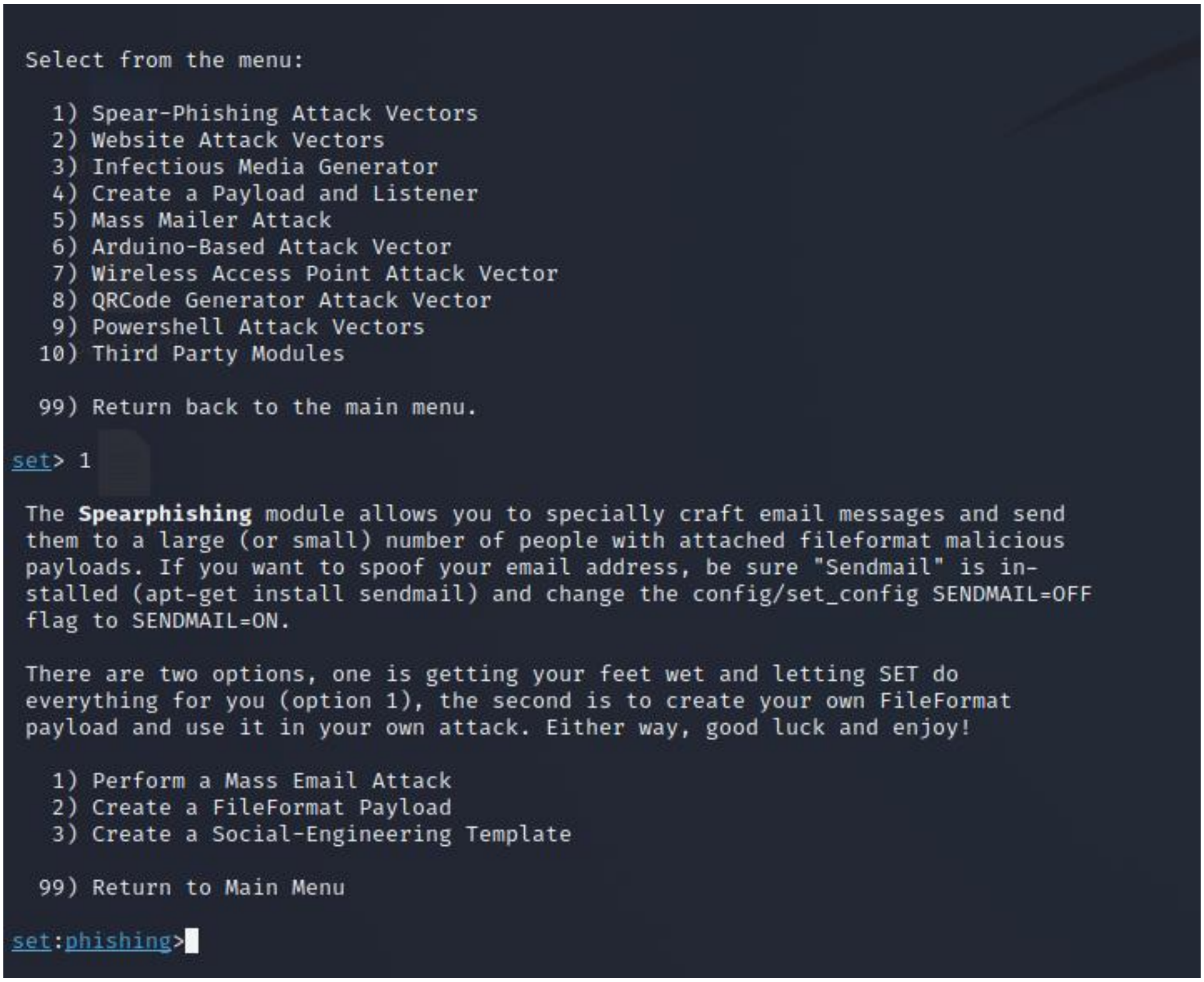
```
Social-Engineer Toolkit

        Free

        #hugs

   By: TrustedSec

[---]        The Social-Engineer Toolkit (SET)        [---]
[---]        Created by: David Kennedy (ReL1K)        [---]
                    Version: 8.0.3
                  Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec        [---]
[---]        Follow me on Twitter: @HackingDave       [---]
[---]       Homepage: https://www.trustedsec.com      [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 
```

Social Engineering Attacks option selected :


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Shell No. 1
06:32 AM
44%
File Actions Edit View Help

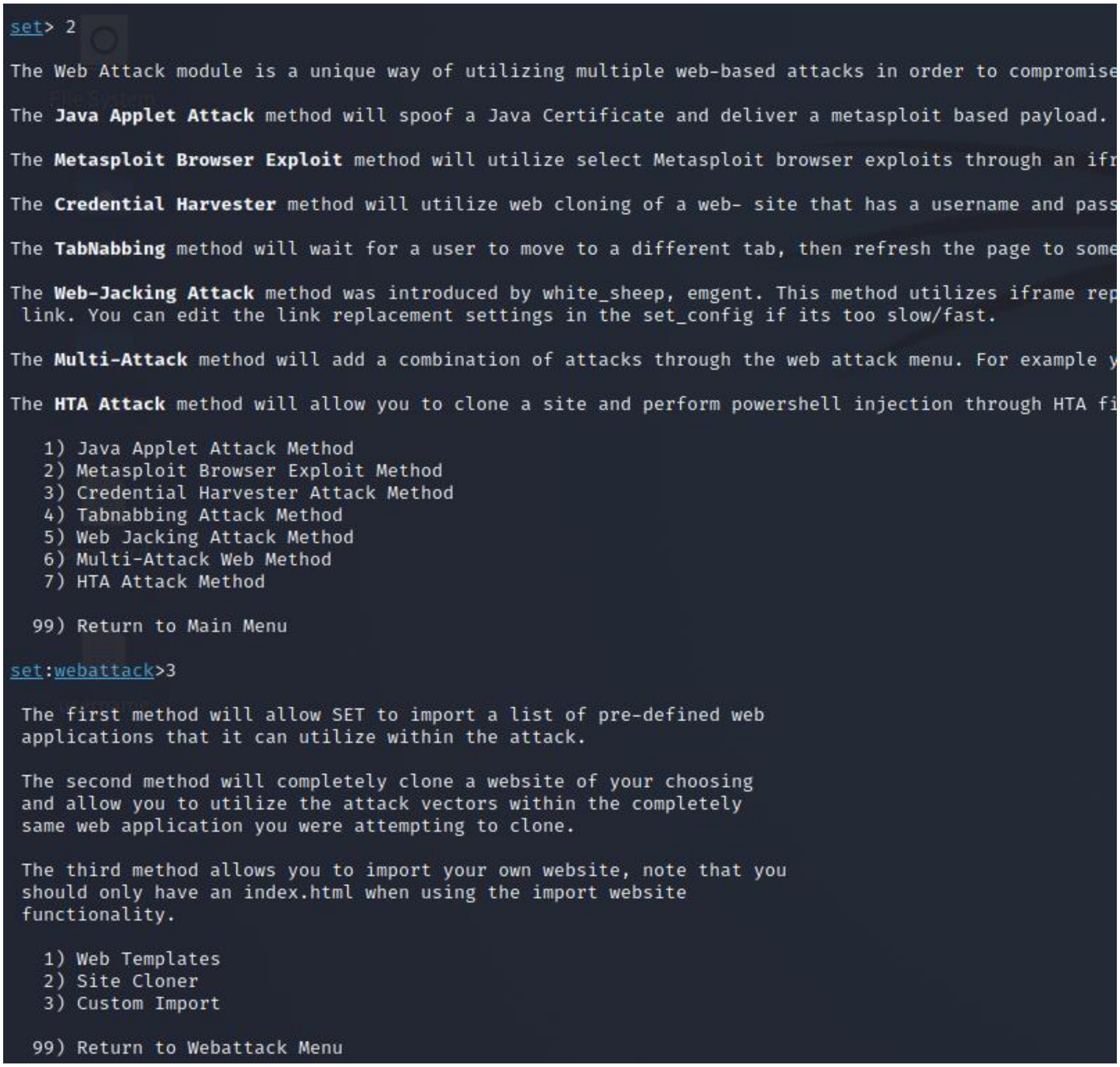
```
[---]        The Social-Engineer Toolkit (SET)        [---]
[---]        Created by: David Kennedy (ReL1K)        [---]
                    Version: 8.0.3
                  Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec        [---]
[---]        Follow me on Twitter: @HackingDave       [---]
[---]       Homepage: https://www.trustedsec.com      [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 
```

Select Phishing :



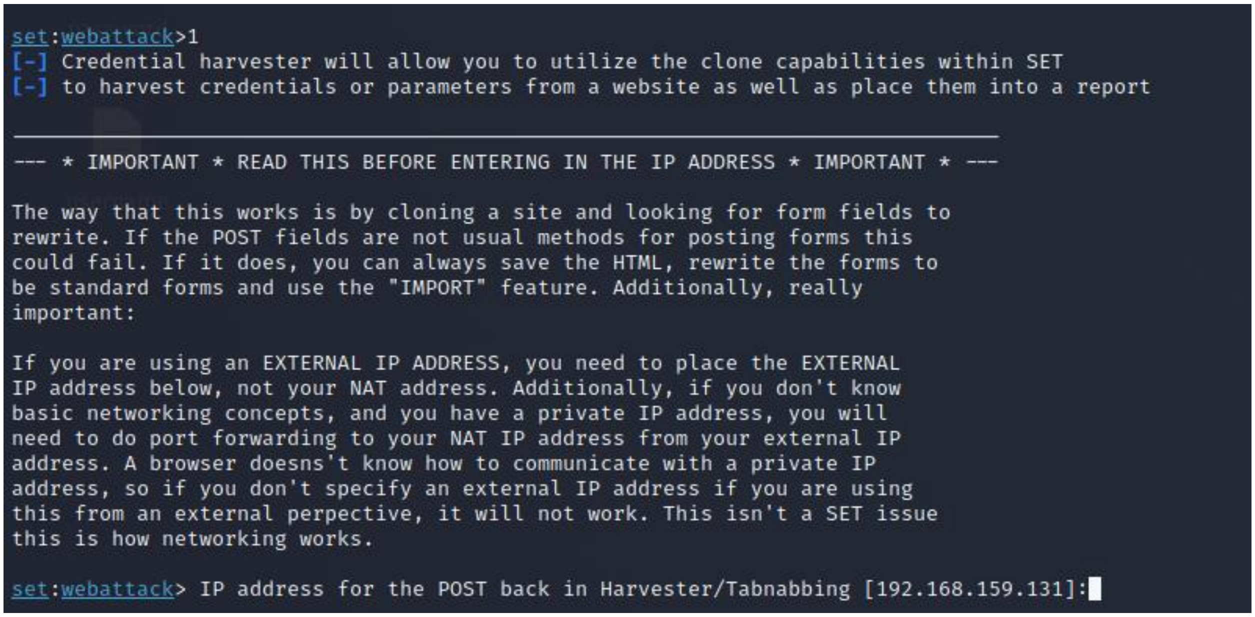
```
 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 1

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached fileformat malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own FileFormat
 payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>
```

Now we will select the web attack vector from SET
We need to select option 2 from the main menu
Once option 2 is selected a list of attacks will be visible. Out of that select the credential harvester option :



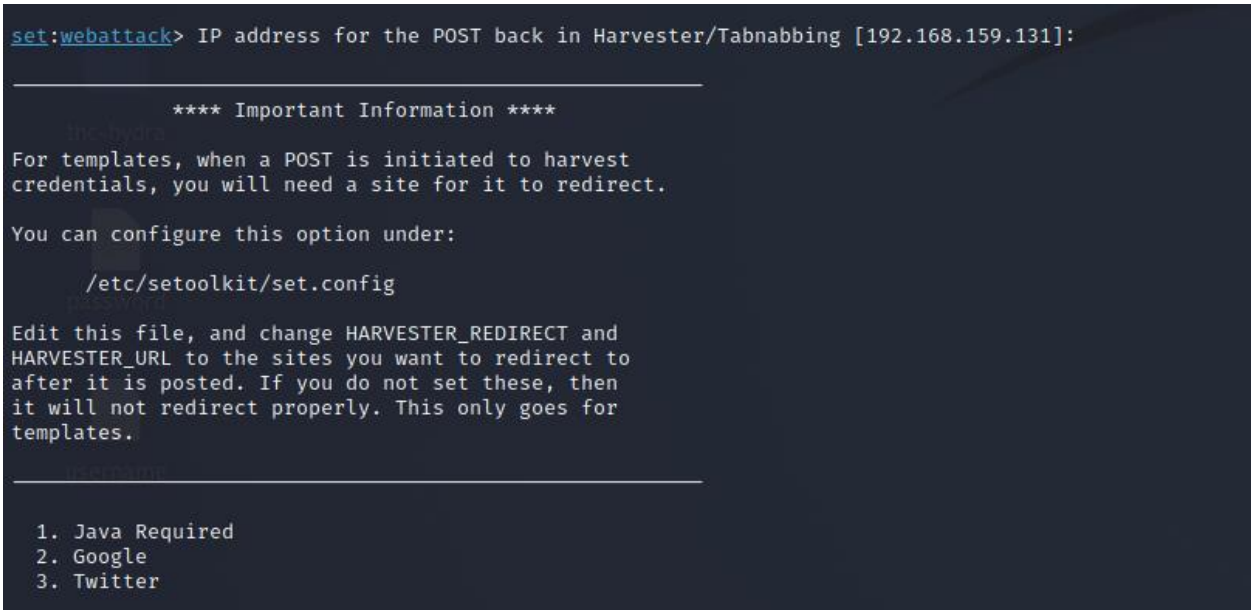
```
set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an ifr

The Credential Harvester method will utilize web cloning of a web- site that has a username and pass

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to some

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe rep
 link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example y

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA fi

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu
```

Once that is done, select the template to be designed for the attack :



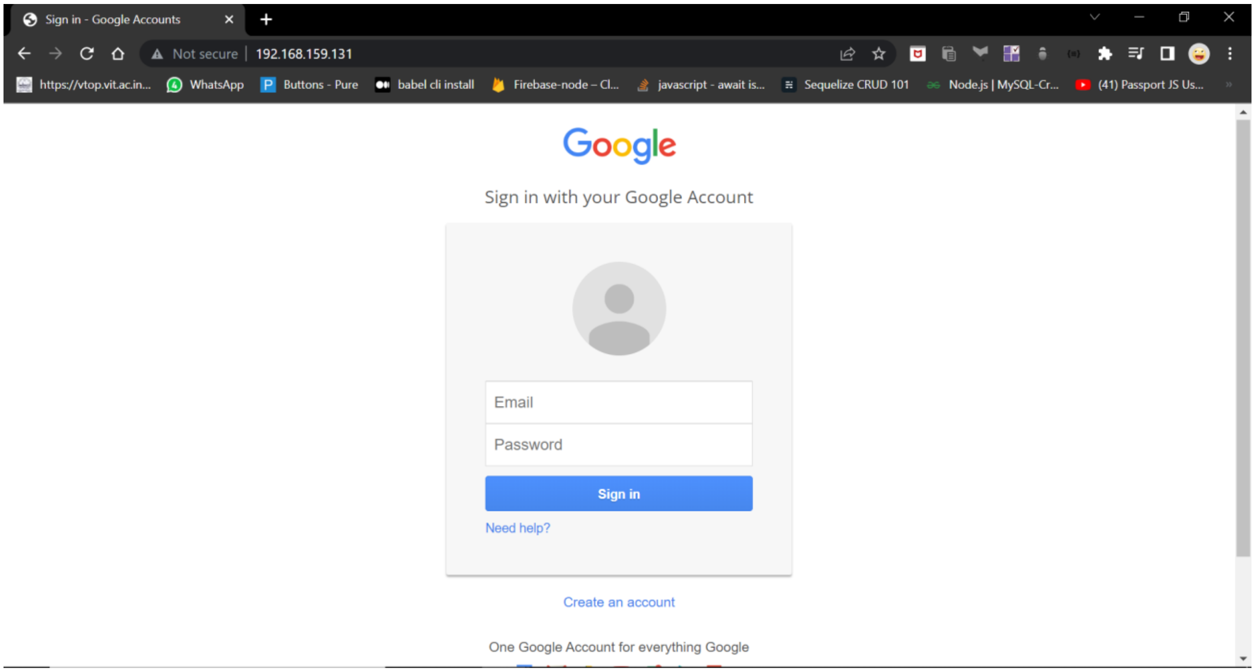
```
set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.159.131]:
```

Google is selected as the template :

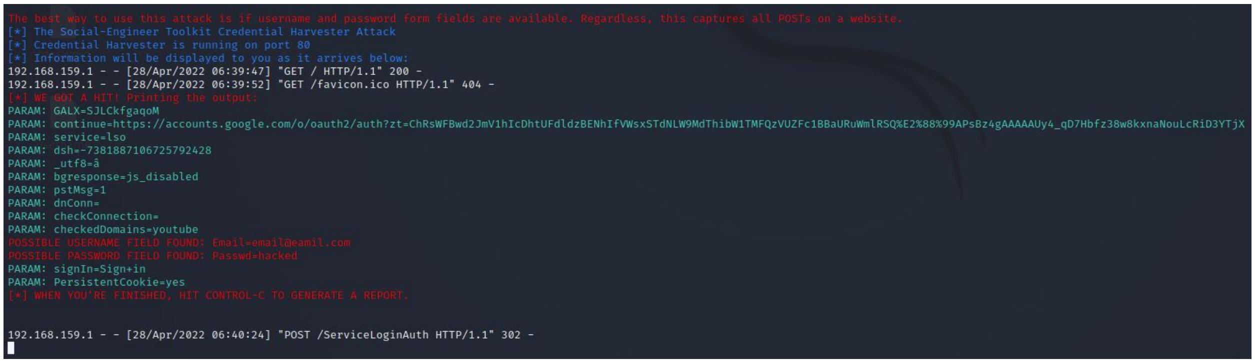


```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.159.131]:
_______________________________________________________

             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.
_______________________________________________________

  1. Java Required
  2. Google
  3. Twitter
```

Finally we get the template selected and a clone is created. On entering the id and password, we can receive it at the terminal as seen below :



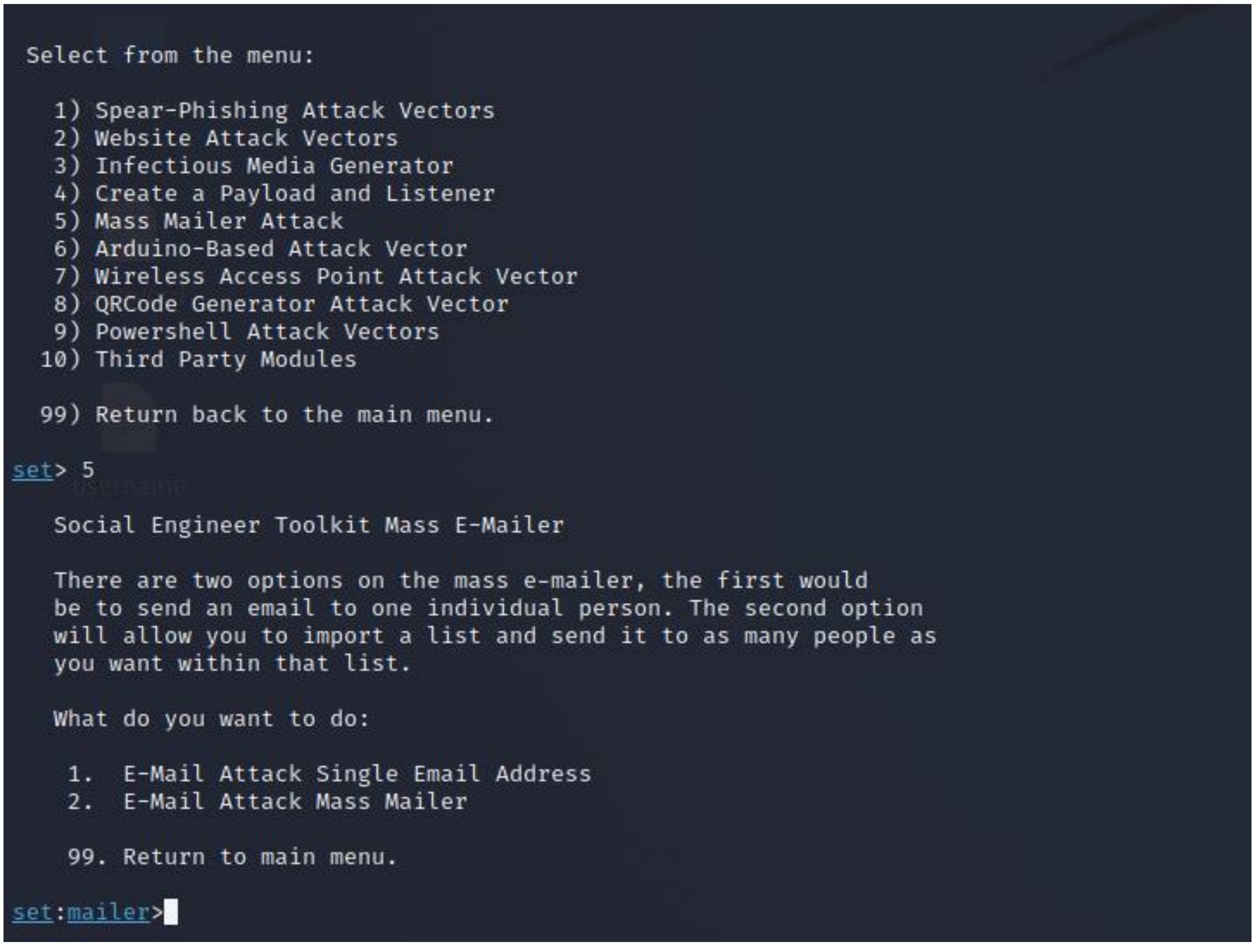
ID and password entered is retrieved here :



```
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.159.1 - - [28/Apr/2022 06:39:47] "GET / HTTP/1.1" 200 -
192.168.159.1 - - [28/Apr/2022 06:39:52] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=email@eamil.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=hacked
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.159.1 - - [28/Apr/2022 06:40:24] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

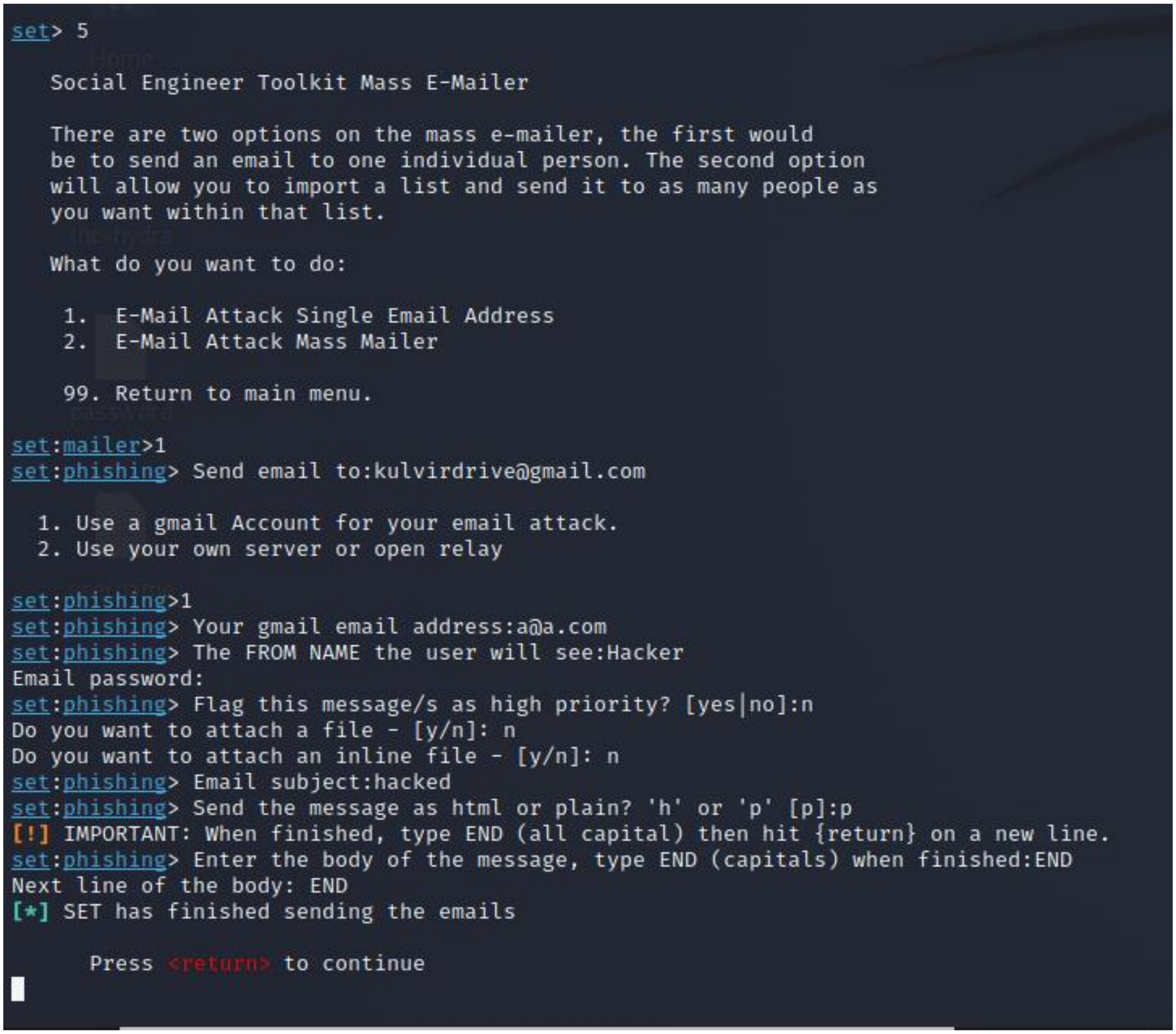
Mass mailer attack

Another attack option is mass mailer attack



```
 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 5

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

    1.  E-Mail Attack Single Email Address
    2.  E-Mail Attack Mass Mailer

    99. Return to main menu.

set:mailer>
```

We volley multiple emails to a single user by selecting that option. Once that is done, we fill in the false email details and attack the victim as shown below :



```
set> 5

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

    1.  E-Mail Attack Single Email Address
    2.  E-Mail Attack Mass Mailer

    99. Return to main menu.

set:mailer>1
set:phishing> Send email to:kulvirdrive@gmail.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:a@a.com
set:phishing> The FROM NAME the user will see:Hacker
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:n
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:hacked
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:END
Next line of the body: END
[*] SET has finished sending the emails

      Press <return> to continue
```