Lab № 4

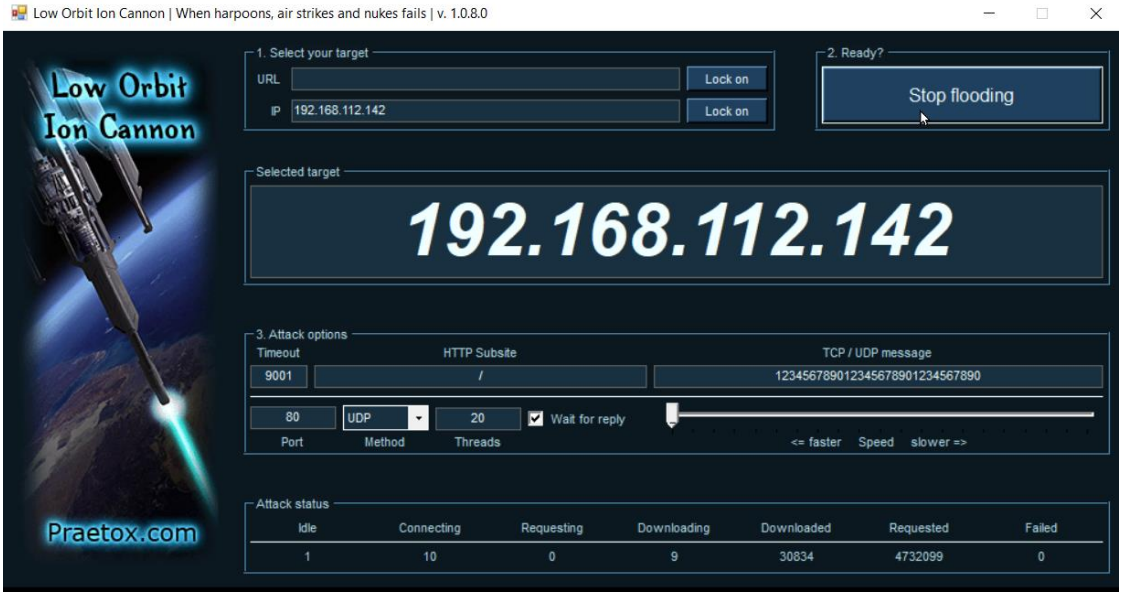
1) I will use during snort IDS during this lab, so first I should install it:

```
root@ubuntu:~# apt install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  snort
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/656 kB of archives.
After this operation, 1,987 kB of additional disk space will be used.
Preconfiguring packages ...
Selecting previously unselected package snort.
(Reading database ... 168249 files and directories currently installed.)
Preparing to unpack .../snort_2.9.7.0-5build1_amd64.deb ...
Unpacking snort (2.9.7.0-5build1) ...
Setting up snort (2.9.7.0-5build1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for systemd (237-3ubuntu10.47) ...
```

2) Different rules were added into local.rules file:

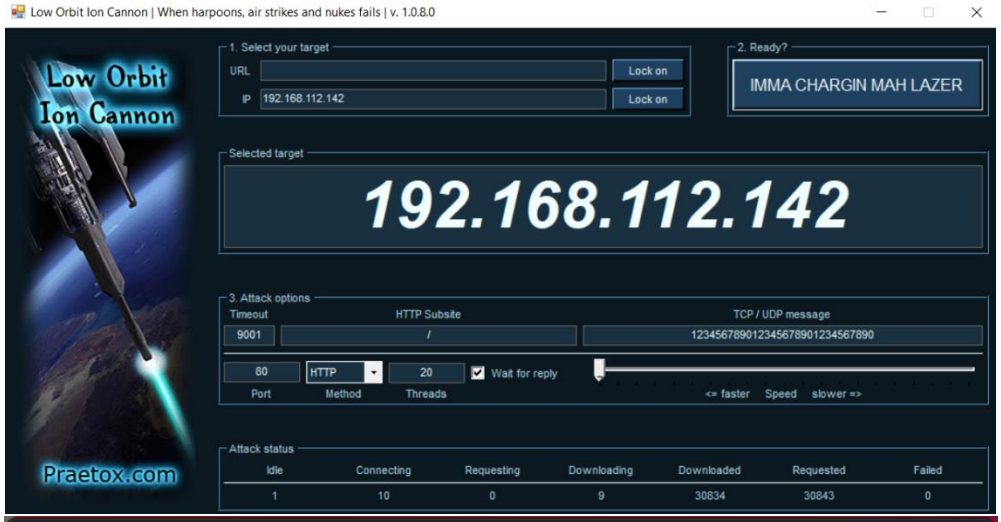
```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP REQUEST TO CONNECT";flow:to_server,established;content:"quit"; \
flags:AP;fragbits:D;\
metadata:service ftp; classtype:tcp-connection; priority:4; sid:1000001;)

#Dos attack detection
alert tcp any any -> $HOME_NET 80 (flags: S; msg:"POSSIBLE TCP DOS"; flow: stateless; detection_filter: track by_src, \
 count 20, seconds 10;sid:1000003; rev:1;)


# Protocol Anomaly
alert udp any any -> any 22,$HTTP_PORTS (msg:"RESTRICTED PROTOCOL TO ACCESS PORT 22,80(UDP)"; classtype:attempted-dos; \
sid:1000011; rev:1;)


#SSH Brute-Force
alert tcp any any -> any 22 (msg:"SSH BRUTE-FORCE ATTACK REJECTED"; flow:established,to_server; content:"SSH"; nocase; \
 offset:0; depth:4; detection_filter:track by_src, count 10, seconds 30; sid:1000015; rev:1;)

#FIN PUSH URGENT Xmas tree attack
alert tcp any any -> any any (msg:"XMAS TREE SCAN"; flags:FPU; sid:1000017; rev:1;)

# Access to root directory
alert tcp any any -> any any (msg:"Command Shell Access"; content:"/root/"; sid:1000025; rev:1;)


# Malware.exe request
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"HTTP Request with filename - malware.exe"; flow:established,\
to_server;content:"malware.exe"; http_uri; fast_pattern:only; pcre:"/malware\.exe$/U"; classtype:trojan-activity; \
sid:1000029; rev:1;)

#App alert
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"WhatsApp";flow:from_client;appid:whatsapp; sid:1000039; classtype: \
misc-activity; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"HTTP Request to domain - illegal.com";
flow:established,to_server; \
content:"Host|3a 20|illegal.com|0d 0a|"; http_header; fast_pattern:only; classtype:trojan-activity; sid:1000049; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 79 (msg:"FIGER 0 QUERY ATTEMPTED";content:"0"; flow:to_server,established;\
 fragoffset:0;fragbits:D; flags:A; classtype:attempted-recon; priority:3; sid:1000053;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP EXPLOIT";flow:to_server, established; content:"|31c031db 41c9b046
cd80 31c031db|";classtype:attempted-admin;sid: 10000057;rev:4;)
```

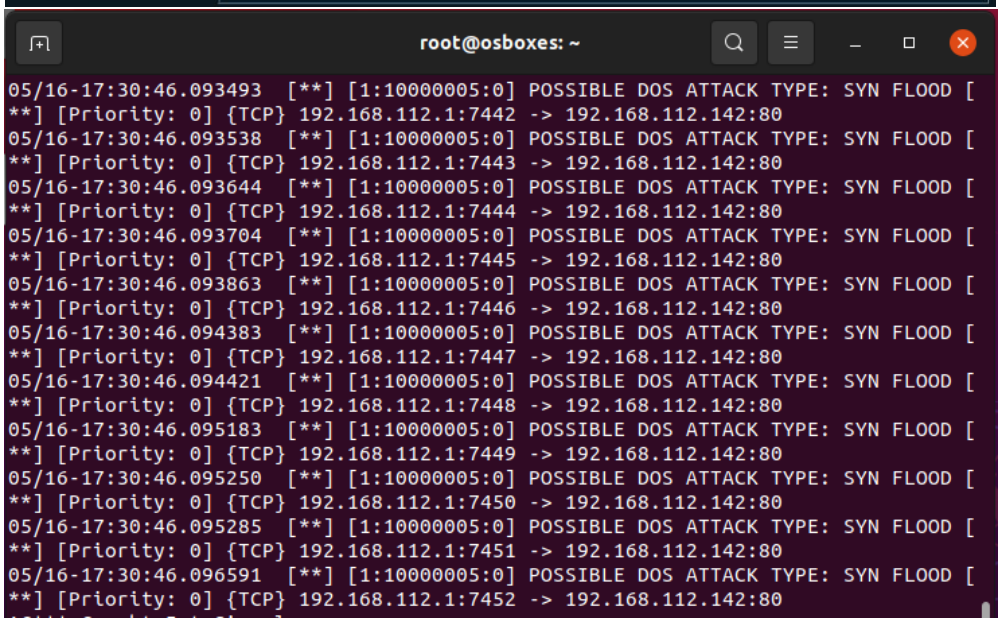
3) Using Low Orbit Ion Canon (LOIC), attack was implemented to port 80, proto UDP in order to invoke Protocol anomaly rule:

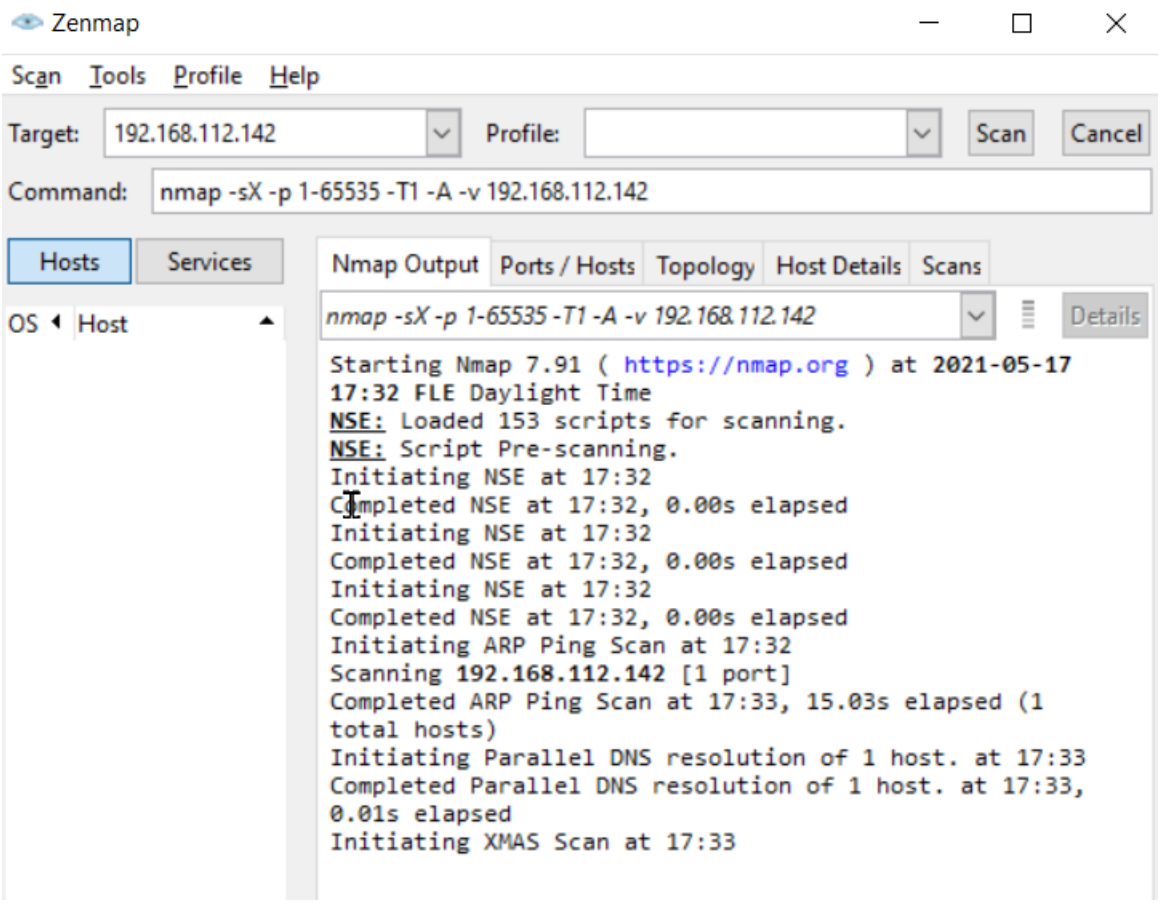


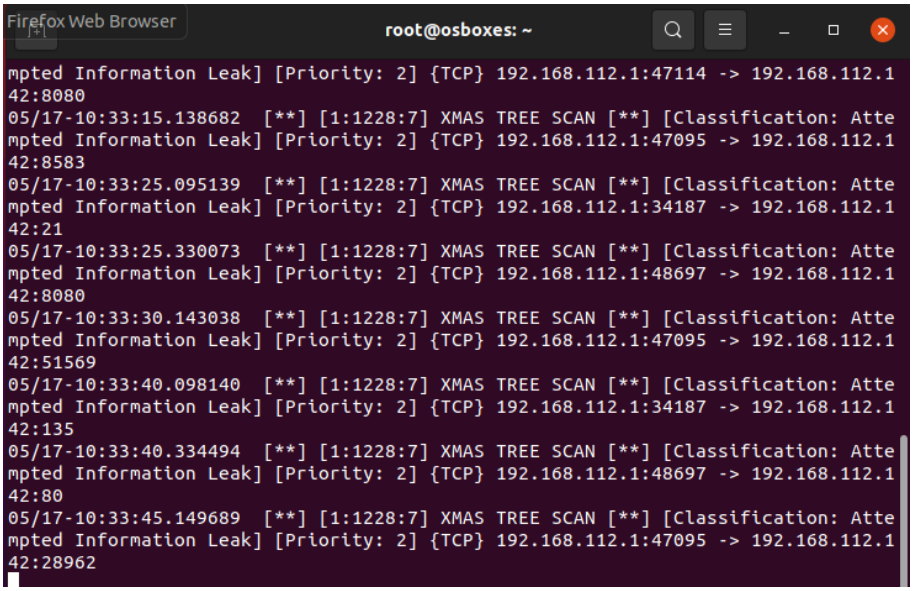

```
05/16-18:06:43.576979  [**] [1:10000013:1] RESTRICTED PROTOCOL TO ACCESS PORT 80
(UDP) [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 192
.168.112.1:65335 -> 192.168.112.142:80
05/16-18:06:43.576980  [**] [1:10000013:1] RESTRICTED PROTOCOL TO ACCESS PORT 80
(UDP) [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 192
.168.112.1:65329 -> 192.168.112.142:80
05/16-18:06:43.576980  [**] [1:10000013:1] RESTRICTED PROTOCOL TO ACCESS PORT 80
(UDP) [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 192
.168.112.1:65335 -> 192.168.112.142:80
05/16-18:06:43.576984  [**] [1:10000013:1] RESTRICTED PROTOCOL TO ACCESS PORT 80
(UDP) [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 192
.168.112.1:65331 -> 192.168.112.142:80
05/16-18:06:43.576984  [**] [1:10000013:1] RESTRICTED PROTOCOL TO ACCESS PORT 80
(UDP) [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 192
.168.112.1:65328 -> 192.168.112.142:80
05/16-18:06:43.576985  [**] [1:10000013:1] RESTRICTED PROTOCOL TO ACCESS PORT 80
(UDP) [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 192
.168.112.1:65336 -> 192.168.112.142:80
05/16-18:06:43.576985  [**] [1:10000013:1] RESTRICTED PROTOCOL TO ACCESS PORT 80
(UDP) [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 192
.168.112.1:65329 -> 192.168.112.142:80
```

Sending http requests to the web server will make snort alert that it is probably DoS attack because number of requests is higher than it is expected to be:






Zenmap
Scan Tools Profile Help
Target: 192.168.112.142
Profile:
Scan
Cancel
Command: nmap -sX -p 1-65535 -T1 -A -v 192.168.112.142
Hosts
Services
OS
Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sX -p 1-65535 -T1 -A -v 192.168.112.142
Details
Starting Nmap 7.91 (https://nmap.org) at 2021-05-17 17:32 FLE Daylight Time
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:32
Completed NSE at 17:32, 0.00s elapsed
Initiating NSE at 17:32
Completed NSE at 17:32, 0.00s elapsed
Initiating NSE at 17:32
Completed NSE at 17:32, 0.00s elapsed
Initiating ARP Ping Scan at 17:32
Scanning 192.168.112.142 [1 port]
Completed ARP Ping Scan at 17:33, 15.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:33
Completed Parallel DNS resolution of 1 host. at 17:33, 0.01s elapsed
Initiating XMAS Scan at 17:33


Firefox Web Browser
root@osboxes: ~
mpted Information Leak] [Priority: 2] {TCP} 192.168.112.1:47114 -> 192.168.112.142:8080
05/17-10:33:15.138682 [**] [1:1228:7] XMAS TREE SCAN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.112.1:47095 -> 192.168.112.142:8583
05/17-10:33:25.095139 [**] [1:1228:7] XMAS TREE SCAN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.112.1:34187 -> 192.168.112.142:21
05/17-10:33:25.330073 [**] [1:1228:7] XMAS TREE SCAN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.112.1:48697 -> 192.168.112.142:8080
05/17-10:33:30.143038 [**] [1:1228:7] XMAS TREE SCAN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.112.1:47095 -> 192.168.112.142:51569
05/17-10:33:40.098140 [**] [1:1228:7] XMAS TREE SCAN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.112.1:34187 -> 192.168.112.142:135
05/17-10:33:40.334494 [**] [1:1228:7] XMAS TREE SCAN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.112.1:48697 -> 192.168.112.142:80
05/17-10:33:45.149689 [**] [1:1228:7] XMAS TREE SCAN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.112.1:47095 -> 192.168.112.142:28962

```
msf6 auxiliary(scanner/ssh/ssh_login) > set StOP_ON_SUCCESS yes
StOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE         C:/10mil.txt     no        File containing passwords, one per line
   RHOSTS            192.168.112.142  yes       The target host(s), range CIDR identifier, or hosts file with syntax '
                                                file:<path>'
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   true             yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per l
                                                ine
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > set username osboxes
username => osboxes
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.112.142:22 - Starting bruteforce
[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

```
root@osboxes: ~
05/17-11:08:12.500258  [**] [1:1000015:1] SSH BRUTE-FORCE ATTACK REJECTED [**] [
Priority: 0] {TCP} 192.168.112.1:13460 -> 192.168.112.142:22
05/17-11:08:15.695656  [**] [1:1000015:1] SSH BRUTE-FORCE ATTACK REJECTED [**] [
Priority: 0] {TCP} 192.168.112.1:13462 -> 192.168.112.142:22
05/17-11:08:16.153660  [**] [1:1228:7] XMAS TREE SCAN [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.112.1:47095 -> 192.168.112.1
42:52621
05/17-11:08:18.876056  [**] [1:1000015:1] SSH BRUTE-FORCE ATTACK REJECTED [**] [
Priority: 0] {TCP} 192.168.112.1:13464 -> 192.168.112.142:22
05/17-11:08:22.058109  [**] [1:1000015:1] SSH BRUTE-FORCE ATTACK REJECTED [**] [
Priority: 0] {TCP} 192.168.112.1:13466 -> 192.168.112.142:22
05/17-11:08:25.305251  [**] [1:1000015:1] SSH BRUTE-FORCE ATTACK REJECTED [**] [
Priority: 0] {TCP} 192.168.112.1:13469 -> 192.168.112.142:22
05/17-11:08:27.136320  [**] [1:1228:7] XMAS TREE SCAN [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.112.1:34187 -> 192.168.112.1
42:3137
05/17-11:08:28.485733  [**] [1:1000015:1] SSH BRUTE-FORCE ATTACK REJECTED [**] [
Priority: 0] {TCP} 192.168.112.1:13471 -> 192.168.112.142:22
05/17-11:08:31.157024  [**] [1:1228:7] XMAS TREE SCAN [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.112.1:47095 -> 192.168.112.1
42:23969
05/17-11:08:31.706933  [**] [1:1000015:1] SSH BRUTE-FORCE ATTACK REJECTED [**] [
Priority: 0] {TCP} 192.168.112.1:13473 -> 192.168.112.142:22
```