Assignment 1

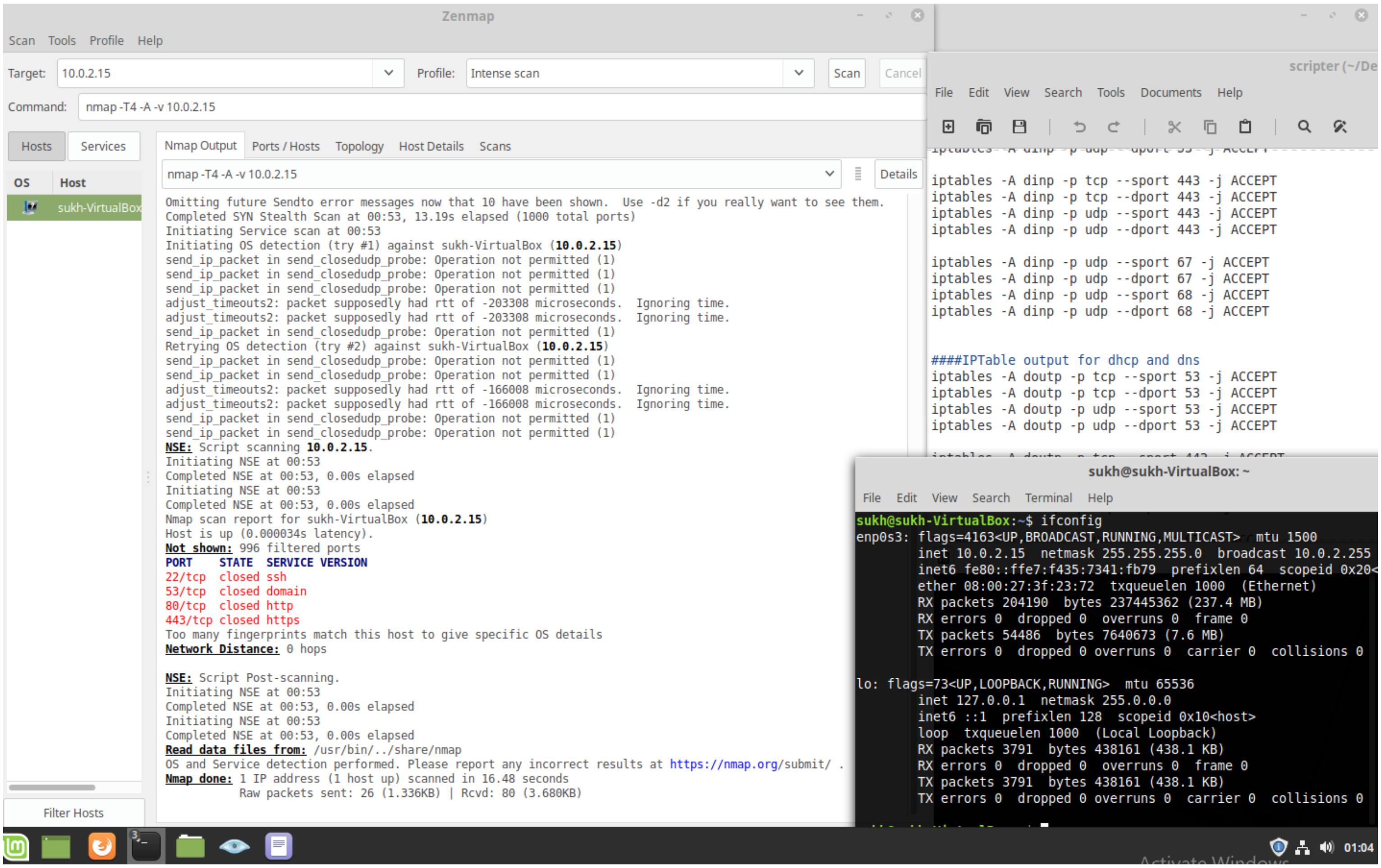
Sukh Atwal, A00907714

Code (Will be using scripts moving forward) with short notes of the rule does, you can copy and paste the following into your Linux terminal as a SU :

```
##Set Default Policies to DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP

##Create user-defined chains for DHCP/DNS, Input/Output to allow inbound/outbound packets
from Port 80 and 22 and Input/Output for dropping.
iptables -N dinp
iptables -N doutp
iptables -N inp
iptables -N outp
iptables -N dropinp
iptables -N dropout

####IPTable input for dhcp and dns
iptables -A dinp -p tcp --sport 53 -j ACCEPT
iptables -A dinp -p tcp --dport 53 -j ACCEPT

iptables -A dinp -p udp --sport 53 -j ACCEPT
iptables -A dinp -p udp --dport 53 -j ACCEPT

iptables -A dinp -p tcp --sport 443 -j ACCEPT
iptables -A dinp -p tcp --dport 443 -j ACCEPT

iptables -A dinp -p udp --sport 443 -j ACCEPT
iptables -A dinp -p udp --dport 443 -j ACCEPT

iptables -A dinp -p udp --sport 67 -j ACCEPT
iptables -A dinp -p udp --dport 67 -j ACCEPT

iptables -A dinp -p udp --sport 68 -j ACCEPT
iptables -A dinp -p udp --dport 68 -j ACCEPT


####IPTable output for dhcp and dns
iptables -A doutp -p tcp --sport 53 -j ACCEPT
iptables -A doutp -p tcp --dport 53 -j ACCEPT
iptables -A doutp -p udp --sport 53 -j ACCEPT
iptables -A doutp -p udp --dport 53 -j ACCEPT

iptables -A doutp -p tcp --sport 443 -j ACCEPT
iptables -A doutp -p tcp --dport 443 -j ACCEPT
iptables -A doutp -p udp --sport 443 -j ACCEPT
iptables -A doutp -p udp --dport 443 -j ACCEPT

iptables -A doutp -p udp --sport 67 -j ACCEPT
iptables -A doutp -p udp --dport 67 -j ACCEPT

iptables -A doutp -p udp --sport 68 -j ACCEPT
iptables -A doutp -p udp --dport 68 -j ACCEPT

####IPTable input for port 22 and 80
iptables -A inp -p tcp --dport 22 -j ACCEPT
iptables -A inp -p tcp --sport 22 -j ACCEPT

iptables -A inp -p tcp --dport 80 -j ACCEPT
iptables -A inp -p tcp --sport 80 -j ACCEPT

####IPTable output for port 22 and 80
iptables -A outp -p tcp --dport 22 -j ACCEPT
iptables -A outp -p tcp --sport 22 -j ACCEPT

iptables -A outp -p tcp --sport 80 -j ACCEPT
iptables -A outp -p tcp --dport 80 -j ACCEPT

####IPTable input for dropping
iptables -A dropinp -p tcp --sport 0:1023 --dport 80 --syn -j DROP
iptables -A dropinp -p tcp --sport 0 -j DROP

####IPTable output for dropping
iptables -A dropout -p tcp --dport 0 -j DROP

##Adding user-defined chains
iptables -A INPUT -p tcp -j dinp
iptables -A OUTPUT -p tcp -j doutp
iptables -A INPUT -p udp -j dinp
iptables -A OUTPUT -p udp -j doutp
iptables -A INPUT -p tcp -j inp
iptables -A OUTPUT -p tcp -j outp
iptables -A INPUT -p tcp -j dropinp
iptables -A OUTPUT -p tcp -j dropout
```

Rule #	**Test Description**	**Tool Used**	**Expected Result**	**Pass/Fail**
1	Permit Inbound / Outbound ssh packets	Nmap	Ssh packets should be allowed both ways	Pass
2	Permit Inbound / Outbound www packets	Nmap	www packets should be allowed both ways	Pass
3	Drop Inbound traffic to Port 80 from Source Ports less than 1024	Nmap/Hping3	Traffic will drop to 80 when the source port is less than 1024 (0:1023)	Pass
4	Drop all incoming packets from reserved port 0 as well as outbound traffic to port 0	Hping3	Anything that’s coming from reserved port 0 is dropped	-

Result



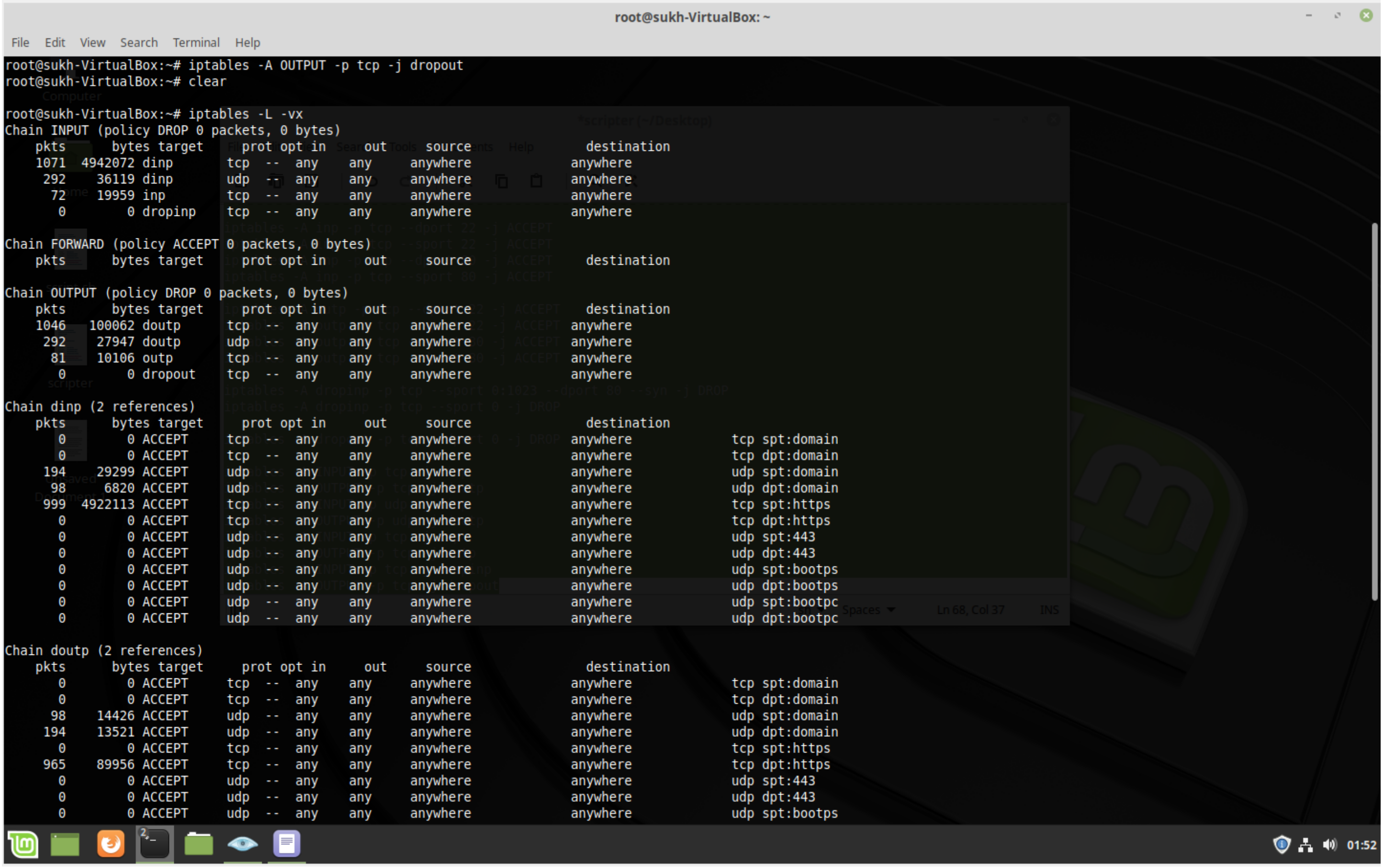
```
Omitting future Sendto error messages now that 10 have been shown.  Use -d2 if you really want to see them.
Completed SYN Stealth Scan at 00:53, 13.19s elapsed (1000 total ports)
Initiating Service scan at 00:53
Initiating OS detection (try #1) against sukh-VirtualBox (10.0.2.15)
send_ip_packet in send_closedudp_probe: Operation not permitted (1)
send_ip_packet in send_closedudp_probe: Operation not permitted (1)
send_ip_packet in send_closedudp_probe: Operation not permitted (1)
adjust_timeouts2: packet supposedly had rtt of -203308 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -203308 microseconds.  Ignoring time.
send_ip_packet in send_closedudp_probe: Operation not permitted (1)
Retrying OS detection (try #2) against sukh-VirtualBox (10.0.2.15)
send_ip_packet in send_closedudp_probe: Operation not permitted (1)
send_ip_packet in send_closedudp_probe: Operation not permitted (1)
adjust_timeouts2: packet supposedly had rtt of -166008 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -166008 microseconds.  Ignoring time.
send_ip_packet in send_closedudp_probe: Operation not permitted (1)
send_ip_packet in send_closedudp_probe: Operation not permitted (1)
NSE: Script scanning 10.0.2.15.
Initiating NSE at 00:53
Completed NSE at 00:53, 0.00s elapsed
Initiating NSE at 00:53
Completed NSE at 00:53, 0.00s elapsed
Nmap scan report for sukh-VirtualBox (10.0.2.15)
Host is up (0.000034s latency).
Not shown: 996 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  closed ssh
53/tcp  closed domain
80/tcp  closed http
443/tcp closed https
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

NSE: Script Post-scanning.
Initiating NSE at 00:53
Completed NSE at 00:53, 0.00s elapsed
Initiating NSE at 00:53
Completed NSE at 00:53, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.48 seconds
           Raw packets sent: 26 (1.336KB) | Rcvd: 80 (3.680KB)
```

```
iptables -A dinp -p tcp --sport 443 -j ACCEPT
iptables -A dinp -p tcp --dport 443 -j ACCEPT
iptables -A dinp -p udp --sport 443 -j ACCEPT
iptables -A dinp -p udp --dport 443 -j ACCEPT

iptables -A dinp -p udp --sport 67 -j ACCEPT
iptables -A dinp -p udp --dport 67 -j ACCEPT
iptables -A dinp -p udp --sport 68 -j ACCEPT
iptables -A dinp -p udp --dport 68 -j ACCEPT


####IPTable output for dhcp and dns
iptables -A doutp -p tcp --sport 53 -j ACCEPT
iptables -A doutp -p tcp --dport 53 -j ACCEPT
iptables -A doutp -p udp --sport 53 -j ACCEPT
iptables -A doutp -p udp --dport 53 -j ACCEPT
```

```
sukh@sukh-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::ffe7:f435:7341:fb79  prefixlen 64  scopeid 0x20<
        ether 08:00:27:3f:23:72  txqueuelen 1000  (Ethernet)
        RX packets 204190  bytes 237445362 (237.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 54486  bytes 7640673 (7.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3791  bytes 438161 (438.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3791  bytes 438161 (438.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

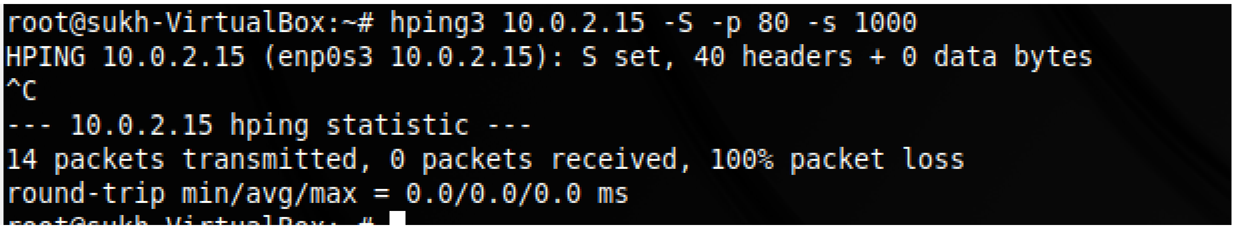
Image shows port 22 (ssh) and 80/443 (http, https) closed.

This is the initial screen when looking at the logs



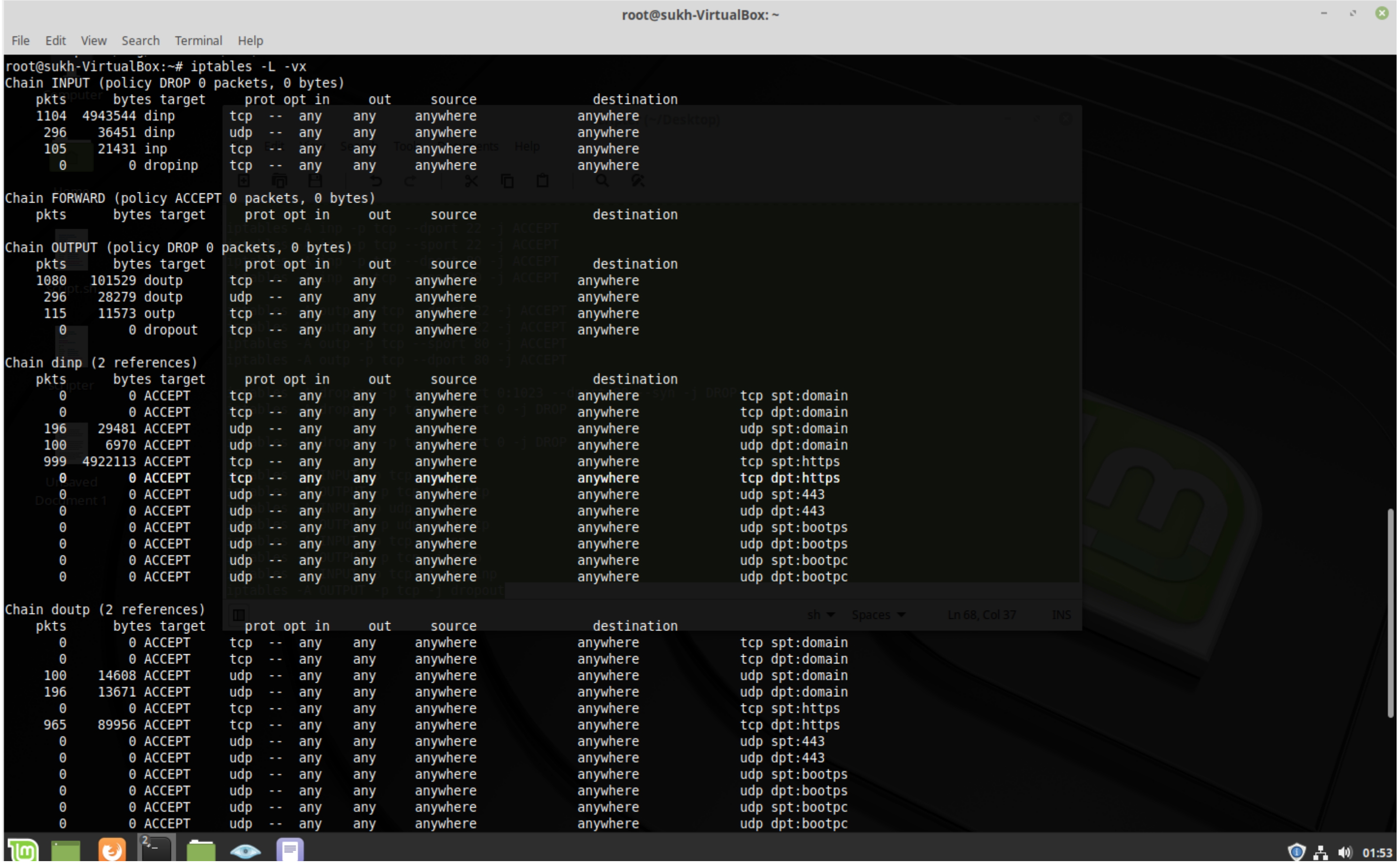
```
root@sukh-VirtualBox:~# iptables -A OUTPUT -p tcp -j dropout
root@sukh-VirtualBox:~# clear

root@sukh-VirtualBox:~# iptables -L -vx
Chain INPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
    1071  4942072 dinp       tcp  --  any    any     anywhere             anywhere
     292    36119 dinp       udp  --  any    any     anywhere             anywhere
      72    19959 inp        tcp  --  any    any     anywhere             anywhere
       0        0 dropinp    tcp  --  any    any     anywhere             anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
    1046   100062 doutp      tcp  --  any    any     anywhere             anywhere
     292    27947 doutp      udp  --  any    any     anywhere             anywhere
      81    10106 outp       tcp  --  any    any     anywhere             anywhere
       0        0 dropout    tcp  --  any    any     anywhere             anywhere

Chain dinp (2 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp spt:domain
       0        0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:domain
     194    29299 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:domain
      98     6820 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:domain
     999  4922113 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp spt:https
       0        0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:https
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:443
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:443
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:bootps
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:bootps
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:bootpc
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:bootpc

Chain doutp (2 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp spt:domain
       0        0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:domain
      98    14426 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:domain
     194    13521 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:domain
       0        0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp spt:https
     965    89956 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:https
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:443
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:443
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:bootps
```

Ran hping3 to test port 80, source port 1000:



```
root@sukh-VirtualBox:~# hping3 10.0.2.15 -S -p 80 -s 1000
HPING 10.0.2.15 (enp0s3 10.0.2.15): S set, 40 headers + 0 data bytes
^C
--- 10.0.2.15 hping statistic ---
14 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@sukh-VirtualBox:~#
```

Resulting in:



```
root@sukh-VirtualBox:~# iptables -L -vx
Chain INPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
    1104  4943544 dinp       tcp  --  any    any     anywhere             anywhere
     296    36451 dinp       udp  --  any    any     anywhere             anywhere
     105    21431 inp        tcp  --  any    any     anywhere             anywhere
       0        0 dropinp    tcp  --  any    any     anywhere             anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
    1080   101529 doutp      tcp  --  any    any     anywhere             anywhere
     296    28279 doutp      udp  --  any    any     anywhere             anywhere
     115    11573 outp       tcp  --  any    any     anywhere             anywhere
       0        0 dropout    tcp  --  any    any     anywhere             anywhere

Chain dinp (2 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp spt:domain
       0        0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:domain
     196    29481 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:domain
     100     6970 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:domain
     999  4922113 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp spt:https
       0        0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:https
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:443
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:443
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:bootps
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:bootps
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:bootpc
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:bootpc

Chain doutp (2 references)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp spt:domain
       0        0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:domain
     100    14608 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:domain
     196    13671 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:domain
       0        0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp spt:https
     965    89956 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:https
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:443
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:443
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:bootps
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:bootps
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:bootpc
       0        0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:bootpc
```