INTERNET SECURITY LAB-3

Akarsh Shetty Umesh Mudelkadi
317752264

In the lab I will be referring VM's as VM1, VM2, VM3:
VM1 -IP(10.0.2.15) - MAC(08:00:27:bc:e1:27)
VM2 -IP(10.0.2.4) - MAC(08:00:27:75:b4:1a)
VM3 -IP(10.0.2.5) – MAC (08:00:27:ad:68:6e)

Task 1:

I have made changes in the file /etc/default/ufw, for the field DEFAULT_INPUT_POLICY="DROP" to "ACCEPT". Also, have enabled the firewall by the command: sudo ufw enable.

a) **Prevent A from doing telnet to machine B.**

```
[02/18/2019 13:06]Mudelkadi@VM1:~$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Mon Feb 18 13:04:49 EST 2019 from 10.0.2.15 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

3 packages can be updated.
0 updates are security updates.

[02/18/2019 13:07]Mudelkadi@VM2:~$ exit
logout
Connection closed by foreign host.
[02/18/2019 13:08]Mudelkadi@VM1:~$ sudo ufw deny out from 10.0.2.15 to 10.0.2.4 p
ort 23
Rule added
```

```
[02/18/2019 13:08]Mudelkadi@VM1:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 10.0.2.4 23                DENY OUT    10.0.2.15                  (out)

[02/18/2019 13:08]Mudelkadi@VM1:~$ telnet 10.0.2.4
Trying 10.0.2.4...
telnet: Unable to connect to remote host: Connection timed out
[02/18/2019 13:11]Mudelkadi@VM1:~$
```

Observation: When tried to telnet from VM1 to VM2 it was successful at first. After changing the ufw packet filter and tried doing the telnet again, it doesn't work from VM1 to VM2.

Explanation: UFW is a packet level fileter and checks for each packet and decides to drop and allow it. Since, I set the firewall rule with command : "sudo ufw deny out from 10.0.2.15 to 10.0.2.4 port 23", all the tcp packets are not allowed to be transferred from VM1 to VM2. Used port 23 as tcp runs on that port.

b) **Prevent B from doing telnet to Machine A.**

```
[02/18/2019 13:33]Mudelkadi@VM2:~$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Fri Feb  8 15:25:45 EST 2019 from 10.0.2.4 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

3 packages can be updated.
0 updates are security updates.

[02/18/2019 13:34]Mudelkadi@VM1:~$ exit
logout
```

```
[02/18/2019 13:11]Mudelkadi@VM1:~$ sudo ufw deny in from 10.0.2.4 to 10.0.2.15 po
rt 23
[sudo] password for seed:
Rule added
[02/18/2019 13:36]Mudelkadi@VM1:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 10.0.2.4 23                DENY OUT    10.0.2.15                  (out)
[ 2] 10.0.2.15 23               DENY IN     10.0.2.4

[02/18/2019 13:41]Mudelkadi@VM1:~$
```

```
[02/18/2019 13:34]Mudelkadi@VM1:~$ exit
logout
Connection closed by foreign host.
[02/18/2019 13:36]Mudelkadi@VM2:~$ telnet 10.0.2.15
Trying 10.0.2.15...
telnet: Unable to connect to remote host: Connection timed out
[02/18/2019 13:39]Mudelkadi@VM2:~$
```

Observation: At first it was possible to telnet from VM2 to VM1. After changing the ufw packet filter, telnet from VM2 to VM1 was unsuccessful.

Explanation: Added new rule to the VM1's firewall with the command : "sudo ufw deny in from 10.0.2.4 to 10.0.2.15 port 23". The command states that all the packets from VM2 to VM1 having protocol tcp (tcp uses port 23) must not be entered to VM1.Thus, all the tcp packets are dropped from VM2 to VM1.

c) Prevent A from visiting an external web site. You can choose any web site that you like to block, but keep in mind, some web servers have multiple IP addresses.

```
[02/18/2019 13:53]Mudelkadi@VM1:~$ ping 128.230.18.198
PING 128.230.18.198 (128.230.18.198) 56(84) bytes of data.
64 bytes from 128.230.18.198: icmp_seq=1 ttl=50 time=49.3 ms
64 bytes from 128.230.18.198: icmp_seq=2 ttl=50 time=36.5 ms
64 bytes from 128.230.18.198: icmp_seq=3 ttl=50 time=49.0 ms
64 bytes from 128.230.18.198: icmp_seq=4 ttl=50 time=36.0 ms
64 bytes from 128.230.18.198: icmp_seq=5 ttl=50 time=36.8 ms
^C
--- 128.230.18.198 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 36.042/41.589/49.375/6.249 ms
[02/18/2019 13:53]Mudelkadi@VM1:~$ sudo deny out from 10.0.2.15 to 128.230.18.198
sudo: deny: command not found
[02/18/2019 13:54]Mudelkadi@VM1:~$ sudo ufw  deny out from 10.0.2.15 to 128.230.1
8.198
Rule added
[02/18/2019 13:55]Mudelkadi@VM1:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 10.0.2.4 23                DENY OUT    10.0.2.15                  (out)
[ 2] 10.0.2.15 23               DENY IN     10.0.2.4
[ 3] 128.230.18.198             DENY OUT    10.0.2.15                  (out)

[02/18/2019 13:55]Mudelkadi@VM1:~$ ping 128.230.18.198
PING 128.230.18.198 (128.230.18.198) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 128.230.18.198 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2027ms

[02/18/2019 13:55]Mudelkadi@VM1:~$
```

Observation: When first tried pinging to www.syr.edu IP address from VM1, packets got transmitted and received successfully. After adding the ufw firewall rule, pinging to www.syr.edu was unsuccessful.

Explanation: Added new rule to the VM1's firewall with the command:" sudo ufw deny out from 10.0.2.15 to 128.230.18.198". The rule states that all the packets going from VM1 to www.syr.edu must be dropped/denied. Thus, when trying to ping to the later IP, the packets get dropped.

Task 2:

a) **Prevent A from doing telnet to machine B.**

Code:

```
#include <linux/kernel.h>
#include <linux/module.h>
#include <linux/netfilter.h>
#include <linux/netfilter_ipv4.h>
#include <linux/ip.h>
#include <linux/tcp.h>
#include <linux/inet.h>

static struct nf_hook_ops telnetFilterHook;

unsigned int telnetFilter(void *priv, struct sk_buff *skb,
                const struct nf_hook_state *state)
{
  struct iphdr *iph;
  struct tcphdr *tcph;

  iph = ip_hdr(skb);
  tcph = (void *)iph+iph->ihl*4;

  if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(23) && iph->saddr
==in_aton("10.0.2.15") && iph->daddr==in_aton("10.0.2.4")) {
    printk(KERN_INFO "Dropping telnet packet from %d.%d.%d.%d  to %d.%d.%d.%d\n",
        ((unsigned char *)&iph->saddr)[0],
        ((unsigned char *)&iph->saddr)[1],
        ((unsigned char *)&iph->saddr)[2],
        ((unsigned char *)&iph->saddr)[3],
           ((unsigned char *)&iph->daddr)[0],
        ((unsigned char *)&iph->daddr)[1],
        ((unsigned char *)&iph->daddr)[2],
        ((unsigned char *)&iph->daddr)[3]);
    return NF_DROP;
  } else {
    return NF_ACCEPT;
  }
}


int setUpFilter(void) {
        printk(KERN_INFO "Registering a Telnet filter.\n");
        telnetFilterHook.hook = telnetFilter;
        telnetFilterHook.hooknum = NF_INET_POST_ROUTING;
        telnetFilterHook.pf = PF_INET;
        telnetFilterHook.priority = NF_IP_PRI_FIRST;
```

```
    // Register the hook.
    nf_register_hook(&telnetFilterHook);
    return 0;
}

void removeFilter(void) {
    printk(KERN_INFO "Telnet filter is being removed.\n");
    nf_unregister_hook(&telnetFilterHook);
}

module_init(setUpFilter);
module_exit(removeFilter);

MODULE_LICENSE("GPL");
```

```
[02/18/2019 16:56]Mudelkadi@VM1:~$ sudo subl task2.c
[sudo] password for seed:
[02/18/2019 16:56]Mudelkadi@VM1:~$ sudo subl Makefile
[02/18/2019 16:56]Mudelkadi@VM1:~$ make
make -C /lib/modules/4.8.0-36-generic/build M=/home/seed modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-gener
ic'
  CC [M]  /home/seed/task2.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/seed/task2.mod.o
  LD [M]  /home/seed/task2.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generi
c'
[02/18/2019 16:57]Mudelkadi@VM1:~$ sudo insmod task2.ko
[02/18/2019 16:58]Mudelkadi@VM1:~$ telnet 10.0.2.4
Trying 10.0.2.4...
telnet: Unable to connect to remote host: Connection timed out
[02/18/2019 17:01]Mudelkadi@VM1:~$ sudo rmmod task2.ko
[02/18/2019 17:03]Mudelkadi@VM1:~$ telnet 10.0.2.4
```

```
[02/18/2019 17:01]Mudelkadi@VM1:~$ sudo rmmod task2.ko
[02/18/2019 17:03]Mudelkadi@VM1:~$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Mon Feb 18 16:38:00 EST 2019 from 10.0.2.15 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

3 packages can be updated.
0 updates are security updates.

[02/18/2019 17:03]Mudelkadi@VM2:~$
```

Observation: After compiling the packet filtering file and makefile. Included the kernel module. Couldn't telnet from VM1 to VM2, all the packets get dropped as you can see in the dmesg. Later, removed the kernel module and tried telnet from VM1 to VM2, it worked successfully.

Explanation: Implemented firewall in VM1 by loading the code written above into the kernel and perform the packet filtering. In the function telnetFilter the filter was given such that packets of protocol tcp trying to be transmitted from VM1 to VM2 should be dropped.

b) Prevent B from doing telnet to Machine A.

Code: Same as a), with changes made in filter condition:

if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(23) && iph->saddr ==in_aton("10.0.2.4") && iph->daddr==in_aton("10.0.2.15"))

and

changed hooknum:

icmpFilterHook.hooknum = NF_INET_PRE_ROUTING;

Sequence of testing:

```
[02/18/2019 18:29]Mudelkadi@VM1:~$ sudo subl task2.c
[02/18/2019 18:33]Mudelkadi@VM1:~$ sudo subl Makefile
[02/18/2019 18:34]Mudelkadi@VM1:~$ make
make -C /lib/modules/4.8.0-36-generic/build M=/home/seed modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
  Building modules, stage 2.
  MODPOST 1 modules
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[02/18/2019 18:35]Mudelkadi@VM1:~$ sudo insmod task2.ko
```

```
[02/18/2019 18:35]Mudelkadi@VM2:~$ telnet 10.0.2.15
Trying 10.0.2.15...
^C
```

```
[ 5525.769353] Dropping telnet packet from 10.0.2.4  to 10.0.2.15
[ 5526.796686] Dropping telnet packet from 10.0.2.4  to 10.0.2.15
[ 5528.813052] Dropping telnet packet from 10.0.2.4  to 10.0.2.15
[ 5532.879351] Dropping telnet packet from 10.0.2.4  to 10.0.2.15
[ 5554.189477] Telnet filter is being removed.
[ 6119.650098] Registering a Telnet filter.
[ 6124.913062] Dropping telnet packet from 10.0.2.4  to 10.0.2.15
[ 6125.943589] Dropping telnet packet from 10.0.2.4  to 10.0.2.15
```

```
[02/18/2019 18:37]Mudelkadi@VM1:~$ sudo rmmod task2.ko
```

```
[02/18/2019 18:35]Mudelkadi@VM2:~$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
```

Observation: Compiled the packet filtering file and Makefile. After inserting the module to kernel, when tried to telnet from VM2 toVM1 it was unsuccessful. After removing the packet filtering module telnet worked from VM2 to VM1.

Explanation: Made code changes from that of a) as shown above. Made the filter changes that packets of tcp protocol from VM2 shouldn't be entered inside VM1 and hence dropped. Also made netfilter hook change to NET_INET_PRE_ROUTING for dealing with the incoming packets. Error message is printed in dmssg as shown in the third picture above.

c) Prevent machine A to send packets to any initialized external web address.

Code:

Change in packet filter condition: iph->saddr ==in_aton("10.0.2.15") && iph->daddr==in_aton("128.230.18.198"

Change in netfilter hook : NF_INET_POST_FORWARDING

```
[02/18/2019 19:36]Mudelkadi@VM1:~$ sudo insmod task2.ko
[02/18/2019 19:36]Mudelkadi@VM1:~$ ping 128.230.18.198
PING 128.230.18.198 (128.230.18.198) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 128.230.18.198 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2046ms
```

```
[ 9743.314251] Registering a icmp filter.
[ 9745.400675] Dropping icmp packet from 10.0.2.15  to 128.230.18.198
[ 9746.423358] Dropping icmp packet from 10.0.2.15  to 128.230.18.198
[ 9747.447532] Dropping icmp packet from 10.0.2.15  to 128.230.18.198
[02/18/2019 19:37]Mudelkadi@VM1:~$ ^C
```

```
[02/18/2019 19:37]Mudelkadi@VM1:~$ sudo rmmod task2.ko
[02/18/2019 19:37]Mudelkadi@VM1:~$ ping 128.230.18.198
PING 128.230.18.198 (128.230.18.198) 56(84) bytes of data.
64 bytes from 128.230.18.198: icmp_seq=1 ttl=50 time=37.9 ms
64 bytes from 128.230.18.198: icmp_seq=2 ttl=50 time=38.2 ms
64 bytes from 128.230.18.198: icmp_seq=3 ttl=50 time=36.5 ms
^C
```

Observation: After setting the packet filtering as stated above and adding the module to the kernel, couldn't send packets to external website www.syr.edu. After removing the module, could ping to the external website mentioned.

Explanation: Changed the filter to packet going from VM1 to www.syr.edu IP. Changed the netfilter hook to NF_INET_POST_ROUTING. After changing the module and inserting it into kernel it prevented from sending ICMP packets to external IP.

d) Preventing A from doing ssh to machine B.

Code changes:

if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(22) && iph->saddr ==in_aton("10.0.2.15") && iph->daddr==in_aton("10.0.2.4"))

and

sshFilterHook.hooknum = NF_INET_POST_ROUTING;

```
[02/18/2019 20:10]Mudelkadi@VM1:~$ make
make -C /lib/modules/4.8.0-36-generic/build M=/home/seed modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-gener
ic'
  CC [M]  /home/seed/task2.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/seed/task2.mod.o
  LD [M]  /home/seed/task2.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generi
[02/18/2019 20:11]Mudelkadi@VM1:~$ sudo insmod task2.ko
[sudo] password for seed:
Sorry, try again.
[sudo] password for seed:
[02/18/2019 20:13]Mudelkadi@VM1:~$ ssh 10.0.2.4
^C
[02/18/2019 20:14]Mudelkadi@VM1:~$
```

```
[  556.868741] Registering a ssh filter.
[  564.673229] Dropping ssh packet from 10.0.2.15  to 10.0.2.4
[  565.679625] Dropping ssh packet from 10.0.2.15  to 10.0.2.4
[  567.694980] Dropping ssh packet from 10.0.2.15  to 10.0.2.4
[  571.757074] Dropping ssh packet from 10.0.2.15  to 10.0.2.4
[02/18/2019 20:16]Mudelkadi@VM1:~$
```

```
[02/18/2019 20:16]Mudelkadi@VM1:~$ sudo rmmod task2.ko
[02/18/2019 20:17]Mudelkadi@VM1:~$ ssh 10.0.2.4
The authenticity of host '10.0.2.4 (10.0.2.4)' can't be establishe
d.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1
/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.4' (ECDSA) to the list of known
 hosts.
seed@10.0.2.4's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)
```

Observation: After loading the changed kernel module, couldn't ssh to VM2 from VM1. After remving the module, could ssh to VM2 from VM1.

Explanation: Changing thepacket filter as shown above and changing port to 22, the module blocks ssh call for packets going from VM1 to VM2. Thus, we could see ssh didn't work. We can see the dmesg stating that the packet was dropped.

e) Preventing machine B to send ICMP packet to machine A.

```
[02/18/2019 20:32]Mudelkadi@VM1:~$ make
make -C /lib/modules/4.8.0-36-generic/build M=/home/seed modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-gener
ic'
  Building modules, stage 2.
  MODPOST 1 modules
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generi
c'
[02/18/2019 20:32]Mudelkadi@VM1:~$ sudo insmod task2.ko
[02/18/2019 20:32]Mudelkadi@VM1:~$
```

```
[02/18/2019 20:27]Mudelkadi@VM2:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
^C
--- 10.0.2.15 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2042ms

[02/18/2019 20:33]Mudelkadi@VM2:~$ sc
```

```
[ 1915.924496] Registering a icmp filter.
[ 1929.936567] Dropping icmp packet from 10.0.2.4  to 10.0.2.15
[ 1930.944399] Dropping icmp packet from 10.0.2.4  to 10.0.2.15
[ 1931.967375] Dropping icmp packet from 10.0.2.4  to 10.0.2.15
[ 1932.991216] Dropping icmp packet from 10.0.2.4  to 10.0.2.15
[ 1934.014538] Dropping icmp packet from 10.0.2.4  to 10.0.2.15
```

```
[02/18/2019 20:36]Mudelkadi@VM1:~$ sudo rmmod task2.ko
[02/18/2019 20:37]Mudelkadi@VM1:~$
```

```
[02/18/2019 20:36]Mudelkadi@VM2:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.568 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=1.34 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=1.17 ms
^C
--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2027ms
rtt min/avg/max/mdev = 0.568/1.029/1.342/0.334 ms
```

Observation: After changing the packet filtering and loading the module to kernel, icmp packets were not able to be transmitted from VM2 to VM1. After removing the module, transfer of icmp packets were successful.

Explanation: Changing the filter such tha the packets with protocol icmp are not allowed inside the VM1 from VM2. After setting the netfilter hook to NF_INET_POST_ROUTING. Thus, the packets are not transmitted. We can see from the dmesg that the packets were dropped going coming from VM2 to VM1.

Task 3.a: Telnet to Machine B through the firewall

```
[02/18/2019 22:20]Mudelkadi@VM1:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23/tcp                     DENY OUT    Anywhere
     (out)
[ 2] 23/tcp (v6)                DENY OUT    Anywhere (v6)
     (out)
```

```
[02/18/2019 22:22]Mudelkadi@VM1:~$ ssh -L 8000:10.0.2.5:23 seed@10
.0.2.4
seed@10.0.2.4's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

3 packages can be updated.
0 updates are security updates.

Last login: Mon Feb 18 22:21:16 2019 from 10.0.2.15
[02/18/2019 22:24]Mudelkadi@VM2:~$
```

```
[02/18/2019 22:25]Mudelkadi@VM1:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Mon Feb 18 22:25:34 EST 2019 from 10.0.2.4 on pts/1
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

3 packages can be updated.
0 updates are security updates.

[02/18/2019 22:26]Mudelkadi@VM3:~$
```

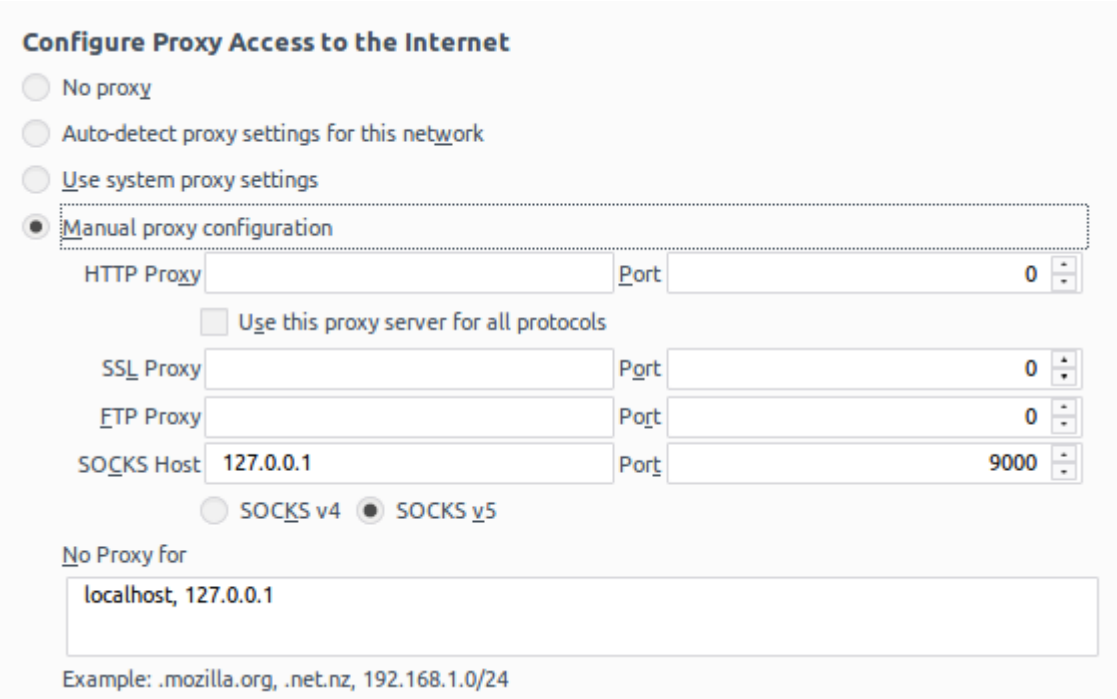
```
 10 2019-02-18 22:25:59.0256597… 10.0.2.15          10.0.2.4           S
 11 2019-02-18 22:25:59.0679330… 10.0.2.4           10.0.2.15          T
 12 2019-02-18 22:26:01.5612800… 10.0.2.15          10.0.2.4           S
 13 2019-02-18 22:26:01.5616991… 10.0.2.4           10.0.2.15          T
 14 2019-02-18 22:26:01.5618797… 10.0.2.4           10.0.2.5           T
 15 2019-02-18 22:26:01.5621793… 10.0.2.5           10.0.2.4           T
 16 2019-02-18 22:26:01.5624210… 10.0.2.4           10.0.2.5           T
```

```
SSH       134 Client: Encrypted packet (len=68)
TCP        66 22 → 53638 [ACK] Seq=1980499596 Ack=2567886297 Win=270 Len=0 …
SSH       158 Client: Encrypted packet (len=92)
TCP        66 22 → 53638 [ACK] Seq=1980499596 Ack=2567886389 Win=270 Len=0 …
TCP        74 46830 → 23 [SYN] Seq=516185801 Win=29200 Len=0 MSS=1460 SACK_…
TCP        74 23 → 46830 [SYN, ACK] Seq=1268487567 Ack=516185802 Win=28960 …
TCP        66 46830 → 23 [ACK] Seq=516185802 Ack=1268487568 Win=29312 Len=0…
```

Observation: Through wireshark result we can conquer that a ssh connection was established from VM1 to VM2, then a tcp connection was established to VM3 delivering the packet sent from VM1. Reverse path is also seen as VM1 receives tcp packet from VM2 sent from VM3.

Explanation: First we set firewall at VM1 such that all tcp packets are dropped going from VM1.Then we create a tunnel to VM2 through SSH. When we set the connection to VM2 through SSH through 8000 port we can then see the packet sent from VM1 to VM2 as ssh is converted to tcp while sending to VM3.VM3 then replies to the received packet and sends back tcp packet to VM2 and thus VM1(since incoming tcp packets are not blocked).

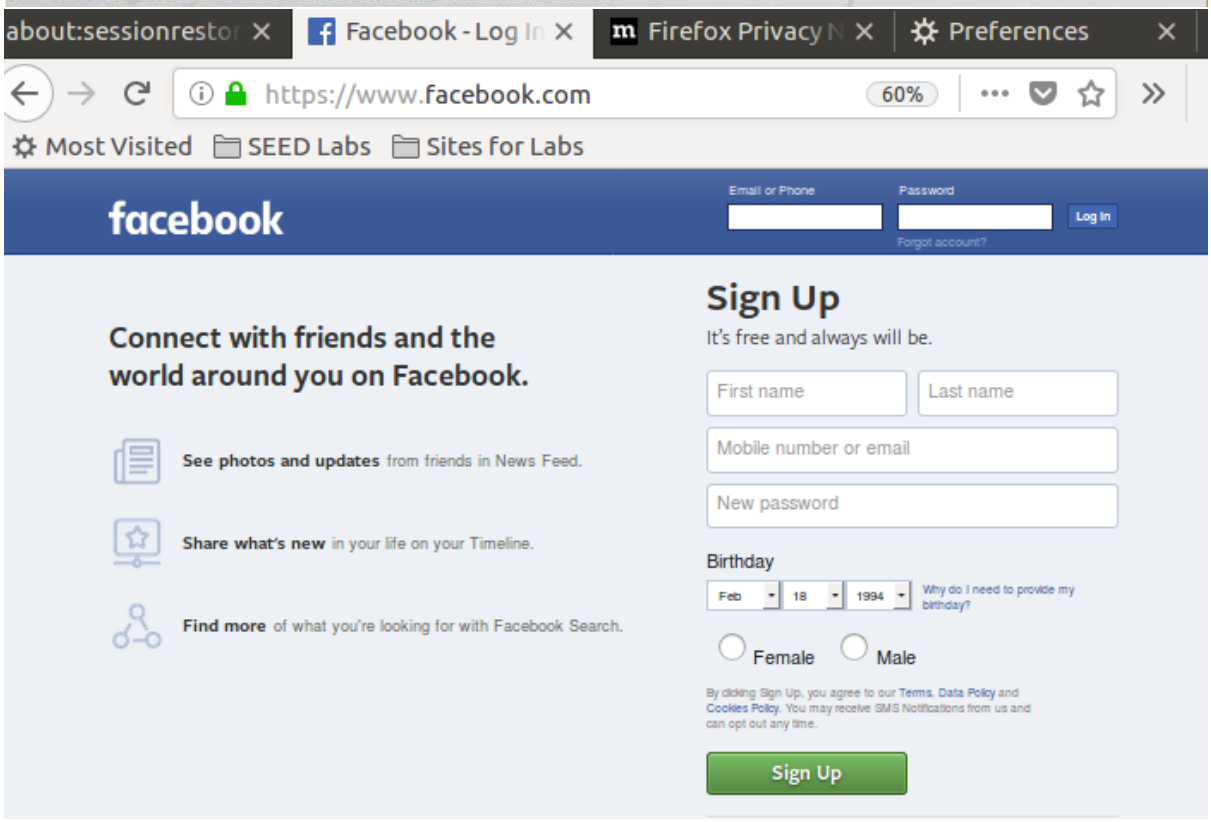
Task 3.b: Connecting to facebook using SSH tunnel.



1. **Run Firefox and go visit the Facebook page. Can you see the Facebook page? Please describe your observation.**

A:

```
^C[02/18/2019 22:53]Mudelkadi@VM1:~$ ssh -D 9000 -C seed@10.0.2.4
seed@10.0.2.4's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

3 packages can be updated.
0 updates are security updates.

Last login: Mon Feb 18 22:24:40 2019 from 10.0.2.15
[02/18/2019 22:54]Mudelkadi@VM2:~$
```

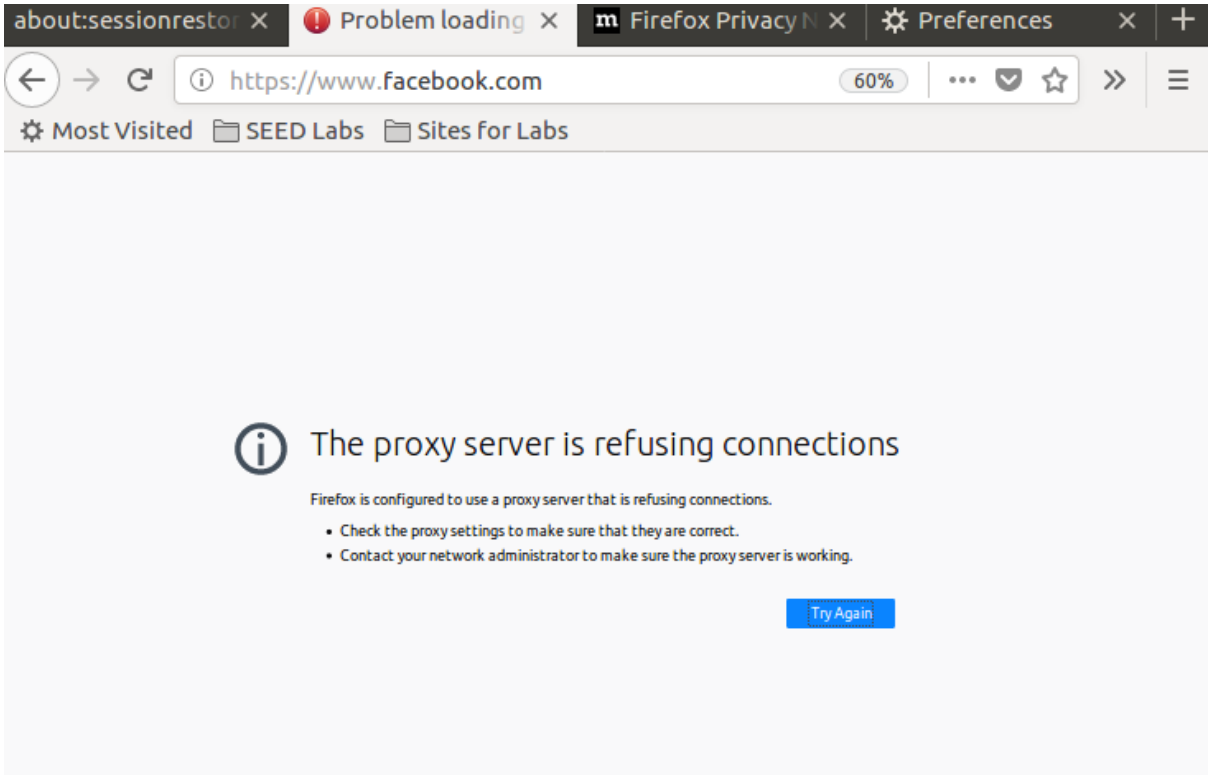


Observation: After setting the ssh tunnel at port at 9000 and making the changes shown above in firefox network settings, we are able open facebook.com successfully.

2. **After you get the facebook page, break the SSH tunnel, clear the Firefox cache, and try the connection again. Please describe your observation.**

A:

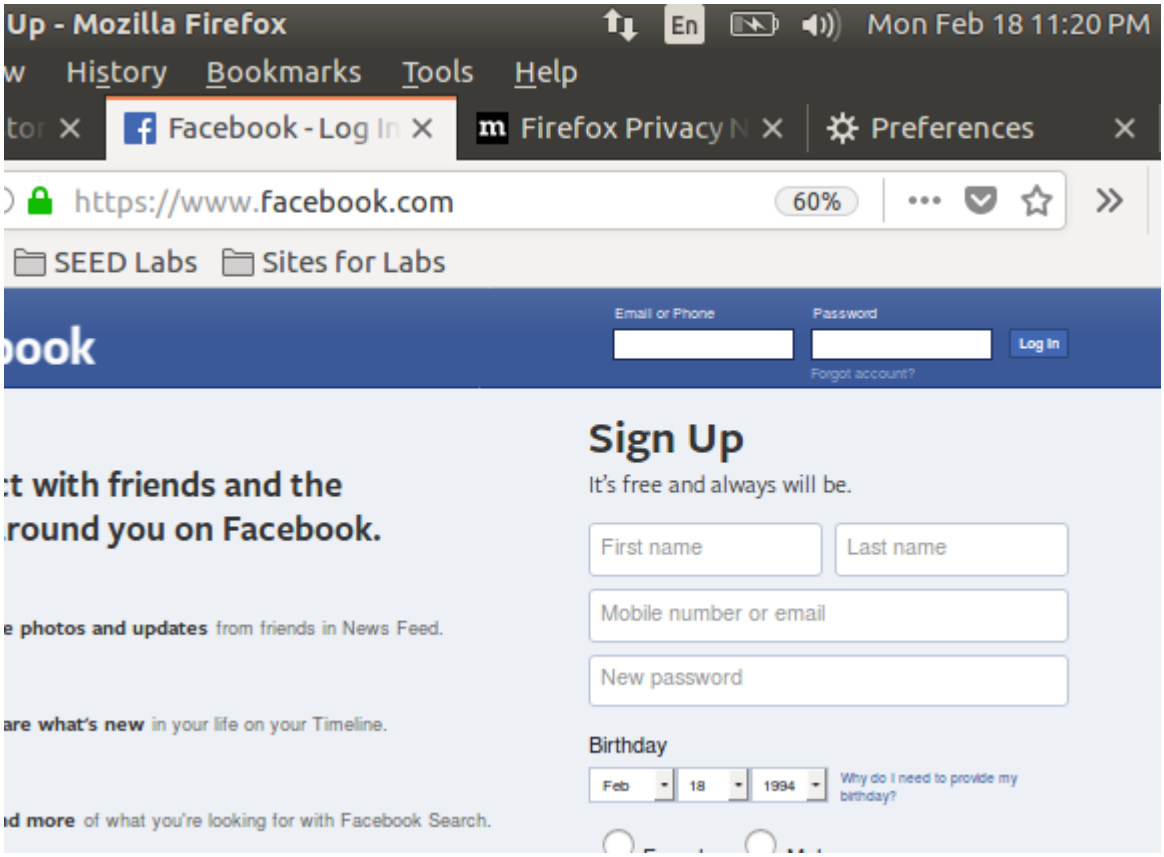
```
Last login: Mon Feb 18 22:24:40 2019 from 10.0.2.15
[02/18/2019 22:54]Mudelkadi@VM2:~$ exit
logout
^C[02/18/2019 23:09]Mudelkadi@VM1:~$
```



Observation: After the ssh tunnel is removed and the firefox network seeting says to use a proxy server which is VM2, which has been disconnected. Since there is not path for http packets to go out as the packet filter breaks all the connection. Hence, we get the above error when we try to open facebook.com.

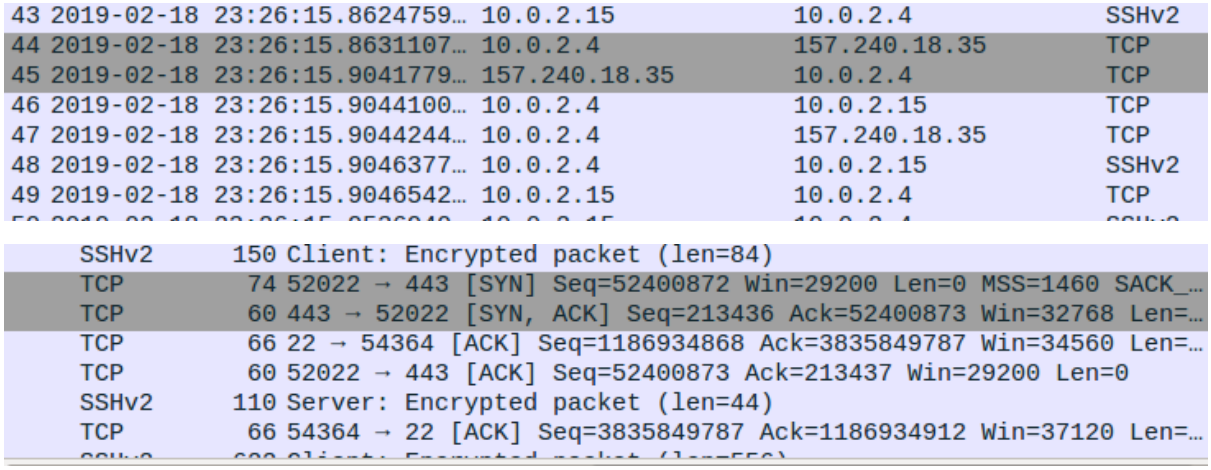
3. **Establish the SSH tunnel again and connect to Facebook. Describe your observation.**

```
^C[02/18/2019 23:09]Mudelkadi@VM1:~$ ssh -D 9000 -C seed@10.0.2.4
seed@10.0.2.4's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

3 packages can be updated.
0 updates are security updates.

Last login: Mon Feb 18 22:54:50 2019 from 10.0.2.15
[02/18/2019 23:17]Mudelkadi@VM2:~$
```



Observation: When the ssh tunnel is set up again, we are able to open facebook.com successfully. Since there is a path now for http packets to go through the tunnel.

4. **Please explain what you have observed, especially on why the SSH tunnel can help bypass the egress filtering. You should use Wireshark to see what exactly is happening on the wire. Please describe your observations and explain them using the packets that you have captured.**

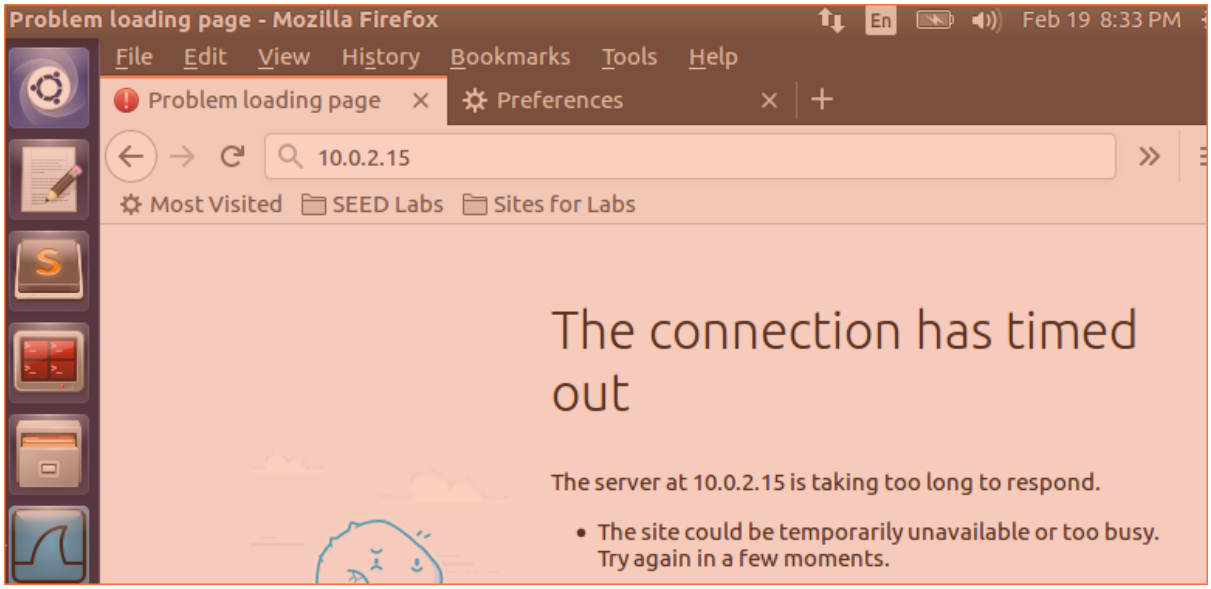


Observation: From above wireshark results we can infer that, when a ssh tunnel is created from VM1 and VM2: First, there is a ssh connection established between VM1 and VM2; Second when we try to open facebook.com VM2 opens a tcp connection to facebook IP and thus gets

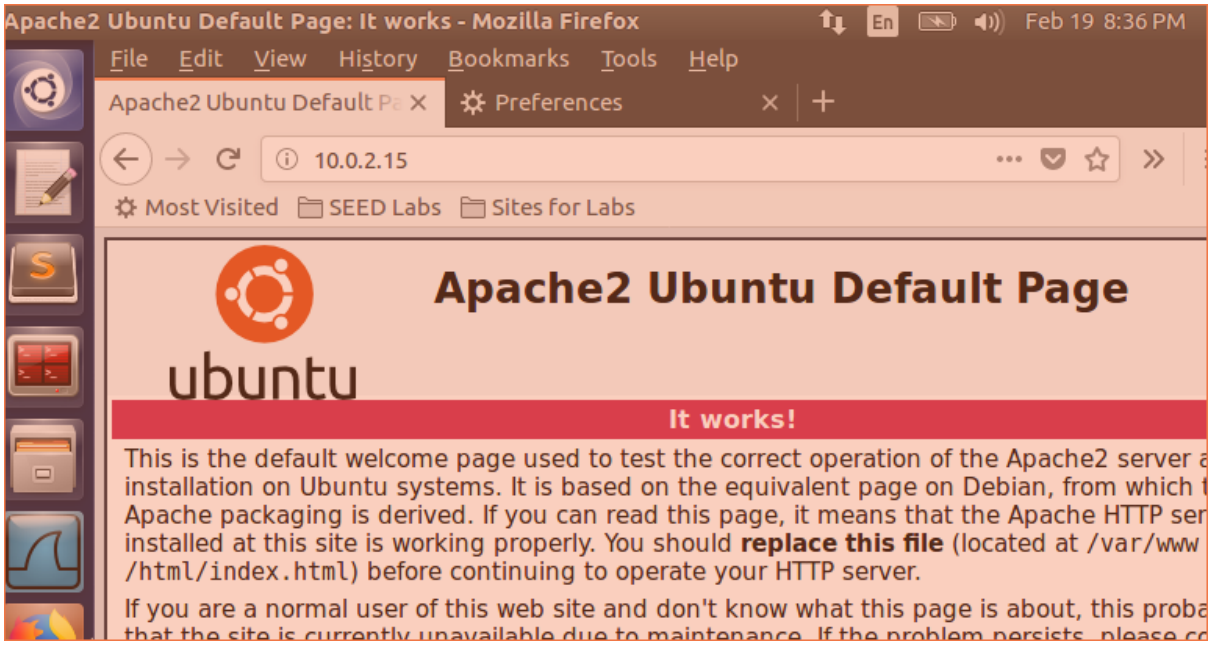
the reply back in tcp; Third the reply is sent back to VM1 as restrictions are not implemented on the incoming packets.

2.4 Task 4: Evading Ingress Filtering:

```
[02/19/2019 20:10]Mudelkadi@VM1:/$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 10.0.2.15 80               DENY IN     Anywhere

[ 2] 10.0.2.15 22               DENY IN     Anywhere
```

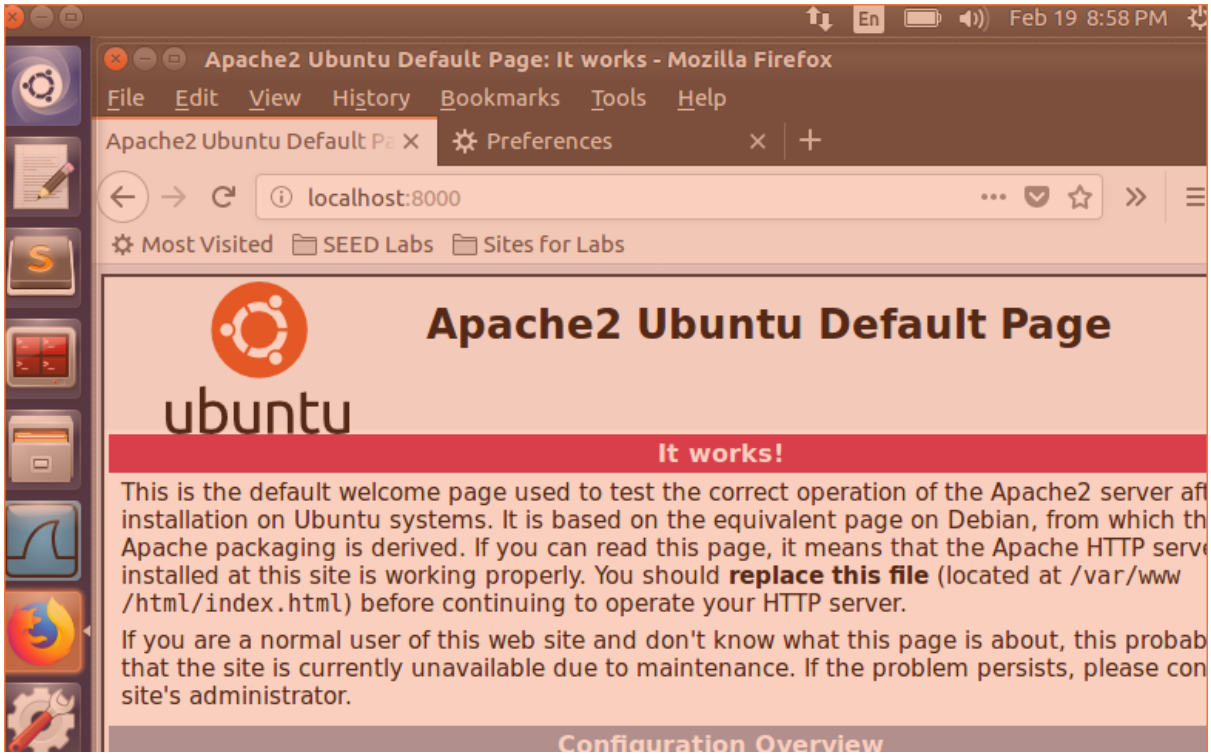



```
[02/19/2019 20:10]Mudelkadi@VM1:/$ sudo ufw disable
[sudo] password for seed:
Firewall stopped and disabled on system startup
[02/19/2019 20:34]Mudelkadi@VM1:/$
```




```
[02/19/2019 20:34]Mudelkadi@VM1:/$ sudo ufw enable
Firewall is active and enabled on system startup
```

```
[02/19/2019 20:56]Mudelkadi@VM1:/$ ssh -R 8000:10.0.2.15:80 seed@
0.0.2.4
seed@10.0.2.4's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

3 packages can be updated.
0 updates are security updates.

Last login: Tue Feb 19 20:56:34 2019 from 10.0.2.4
[02/19/2019 20:57]Mudelkadi@VM2:~$
```



Observation: First, set up firewall rules in VM1 and tried accessing it from VM2 which was unsuccessful. Second, disabled firewall and tried accessing VM1 from VM2 which was successful. Third, again enabled the firewall and did remote port forwarding then VM2 was able to access VM1.

Explanation: Even after setting firewall rules, VM2 was able to connect to VM1 as we have done the setting for remote port forwarding by creating tunnel to VM1's ssh from VM2 through port 8000 with the command : ssh -R 8000:10.0.2.15:80 seed@10.0.2.4.