

**Network Security**

Assignment 3

**Name:** Muhammad Fakhar E Alam

**Roll No:** 16L-4284

**Section:** B

**Date:** May 10, 2020

National University of Computer and Emerging Sciences

Department of Computer Science

Lahore, Pakistan

**Table of Figures**

**Figure 1: Initial Step(s) of the Attack** 3

**Figure 2: Telnet Stats for the Server** 3

**Figure 3: One command attack using Netwox Tool 76 on Attacker VM** 4

**Figure 4: Telnet Stats during attack on the Server** 4

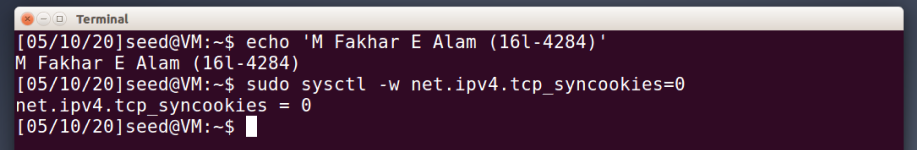
**Figure 5: Connecting to the host IP on User VM** 4

**SYN Flooding Attack Using NETWOX**

Following are the details of how the attack was carried out. I have followed the Chapter 16 from the book of ‘**Computer Security: A Hands-on Approach**’ by **Wenliang Du**. To perform the attack, used ‘**Seed Ubuntu 16.04 VM (32-bit)**’. For this attack, had to setup three different VMs, one was already setup, simply cloned the other two required. One is for the **Attacker**, second for the **Server,** and third for the **User**.

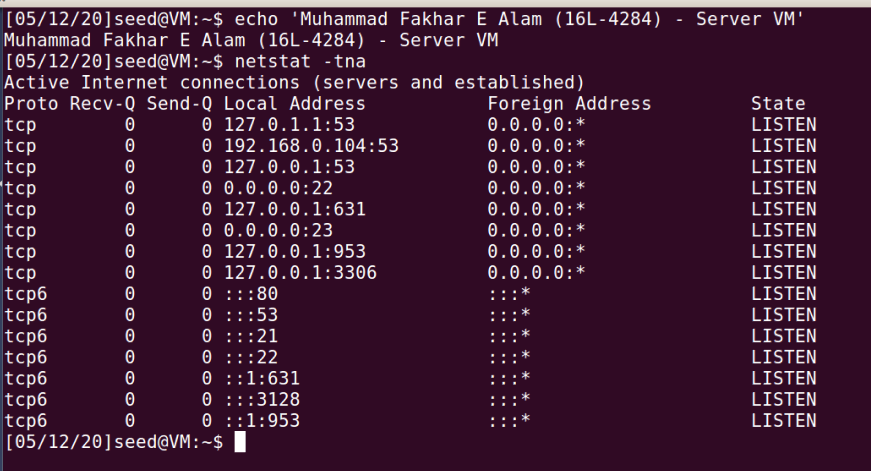
**Steps for the Attack**

* Following screenshot shows the initial steps required to perform the attack. Firstly, we must turn off the countermeasure(s) on the **Server**-side in Ubuntu V16.04. Following the steps in the book, turned off **SYN Cookies.**



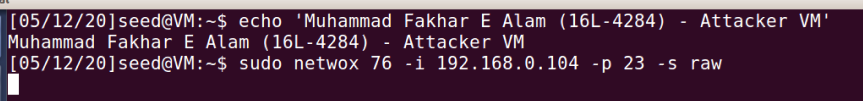
**Figure 1: Initial Step(s) of the Attack**

* Next, we can simply launch the attack using the **Netwox** on the **Attacker** VM. In order to do that, first we have to check whether the Server is even listening or not. So, using the command, ‘telnet -tna’, shown below. We can see that the server is listening on several IPs, we will be targeting the second IP, ‘192.168.0.104’ since it is the IP address of the server too.



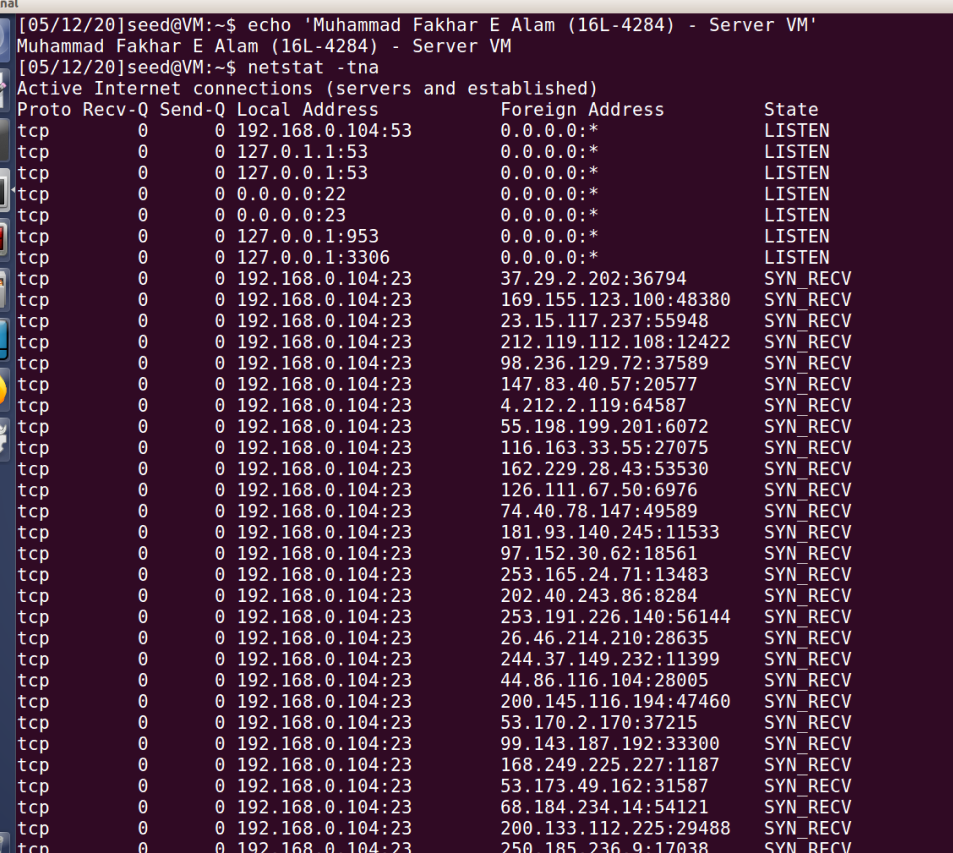
**Figure 2: Telnet Stats for the Server**

* Now, to perform the attack, we will be sending large number of packets at a specified address and port number. Port number will be **23** since it is assigned to telnet for the client-server communication. The IP will be the one mentioned above, **192.168.0.104.** Netwox has many tools but we need **Tool 76**, called **Synflood**. As seen from the screenshot below, IP and Port number is provided. Using this simple command, the attack has now started.



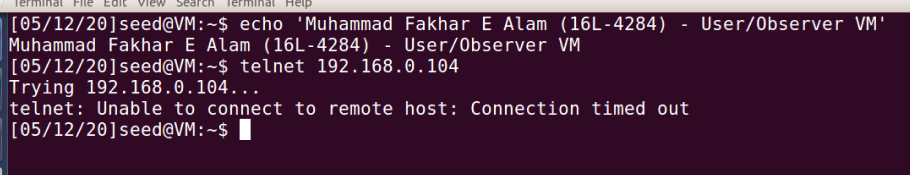
**Figure 3: One command attack using Netwox Tool 76 on Attacker VM**

* Since the attack has started and as we can see on the **Server** VM below, there are a lot of SYN packets received, making **half-open** **TCP** connections, which will eventually fill up the buffer and it can no longer respond to further SYN requests.



**Figure 4: Telnet Stats during attack on the Server**

* Now, using **User/Observer** VM, we can check the status of the network. Using ‘telnet’ we can try to connect to the IP of the Server, as you can see below, the connection timed out. Which basically means that the buffer on the Server side was not able to handle further requests and this is what **Denial of Service** (DoS) basically is.



**Figure 5: Connecting to the host IP on User VM**