CES571S - L1 - TCP/IP Attack

467261 - Yifu Wang

2018 - 09 - 05

1 Lab Environment

We need 3 machines to accomplish this lab, one **Attacker**, one **Client**, one **Server**. I choose to create 3 VM with VirtualBox. In order to connet all 3 VM to internet and connet them with each others and the host, I create a bridge to share the Ethernet in the host, so they all under the 192.168.137.***.

2 Lab Tasks

2.1 SYN Flooding Attack

In order to observe the attack result easily. I used a tool called **tcpping**, which is similar to ping but using tcp protocol. So hopefully my attack will jam the **tcpping**. And every thing worked smoothly.
With `"netwox 76 -i 192.168.137.167 -p 80"`, the **Attacker** attacked the **Server** at port 80.
With `"tcpping 192.168.137.167 80"`, the **Client** is able to send tcp request to **Server** at the same port. So we can find out if our attack were successful.
And by the way, though the `"netwox 76"` won't log no matter it's success or not, we can still tell the difference physically. When the SYN cookie is turned on, this command won't do anything. But when the SYN cookie is turned off, this command will cause the cooling fan to make a huge noise.
Screenshot: Server, Client, Attacker