Josh Keahey

Lacey Rone

4.11.19

Deter Lab 2 Questions

1. When a client and server want to initially connect with each other, what’s called the TCP three-way handshake takes place. The client sends the server a SYN request, asking to sync with the server. The server responds with a SYN/ACK response, saying that it has received the client’s SYN, and is ready to connect. Normally, the client would then send one last ACK back to server to complete the handshake and establish a connection. Except what the attacker does is, when sending its SYN request, spoofs a fake IP address, so when the server responds with its SYN/ACK, it sends it to a client that doesn’t exist. The server then waits for the response from the client forever, or for long enough that it takes up the server’s resources, and legitimate traffic can’t get through.
2. Blah blah
3. #!/bin/bash

while :

do

curl –output /dev/null <http://5.6.7.8/index.html>

sleep 1

done

1. sudo flooder –dst 5.6.7.8 –highrate 15 –proto 6 –dportmin 80 –dportmax 80 –src 1.1.3.4 –srcmask 255.255.255.0
2. Without SYN cookies:



With SYN cookies:



1. In the first case, when there are no cookies, we can clearly see when the attack starts at 30 seconds in. It tries to recover after the initial incoming of new packets, but it deteriorates quickly and stays clogged until the attack stops at around 90 seconds. When the SYN cookies are turned back on again however, there is a noticeable difference