4η Εργαστηριακή Εργασία στην Ασφάλεια Υπολογιστών

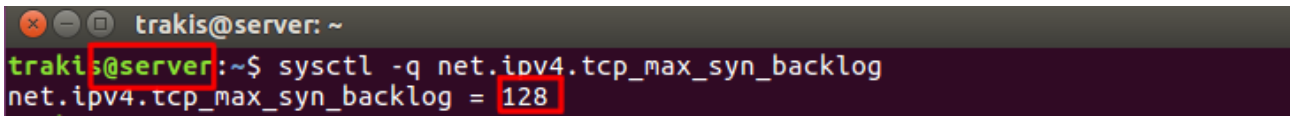
Αξελός Χρήστος
Αεμ 1814

System Configuration

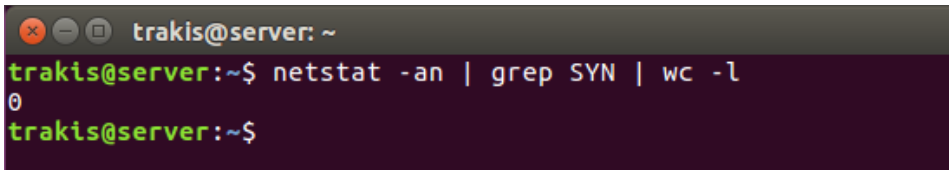
- Χρησιμοποιώ τον **Host**(192.168.2.8) ως **attacker**
- Έπειτα ένα **VM1**(172.16.48.130) ως **server/victim**
- Τέλος, άλλο ένα **VM**(172.16.48.131) ως **client/victim**

Task 1: SYN Flooding Attack

- Για το attack αυτό χρησιμοποιώ το **VM1** συν τον **Host**.
- Σαν 1ο βήμα, βλέπουμε το μέγεθος του queue στον **server/victim**



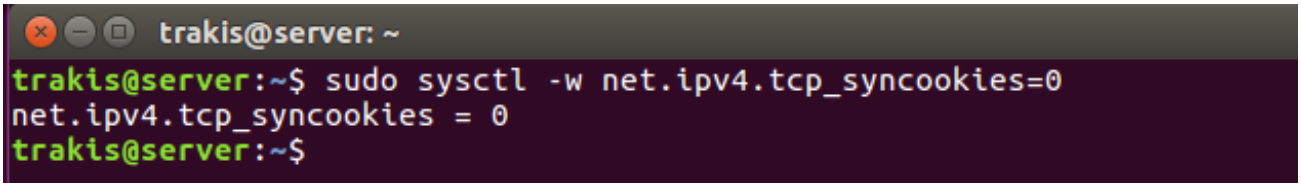
*- Έπειτα, εκτυπώνουμε στην οθόνη όσες **συνδέσεις** υπάρχουν στο Queue και βρίσκονται σε κατάσταση **SYN-RECV** πριν το attack χρησιμοποιώντας την εντολή **netstat***



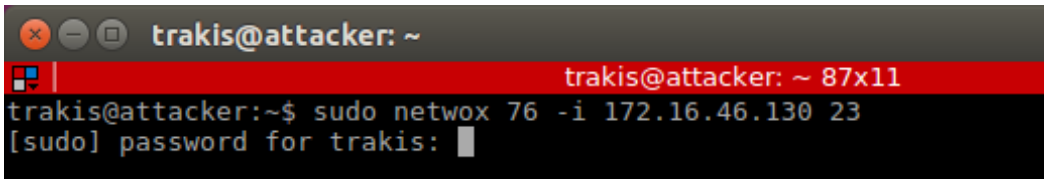
- Παρατηρούμε πως δεν υπάρχουν τέτοιες συνδέσεις πριν το attack

a) SYN Flooding χωρίς τα Cookies

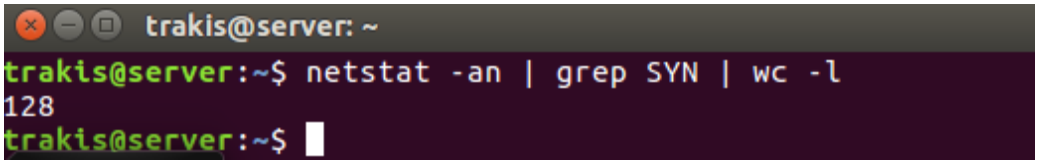
*- Απεργοποιούμε τα Cookies του Queue χρησιμοποιώντας την παρακάτω εντολή στον **server/victim***



- Έπειτα ξεκινάω από τον host/attacker την επίθεση χρησιμοποιώντας ως port το ***telnet*** *χρησιμοποιώντας την εντολή*

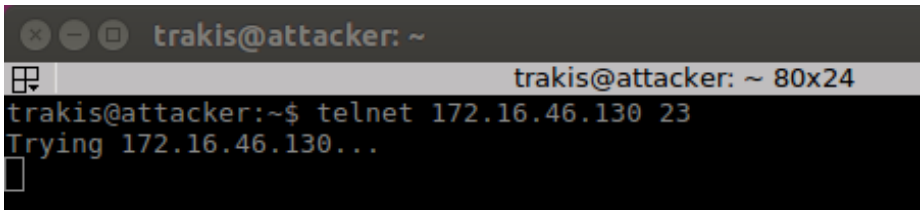


- Έπειτα ελέγχουμε πάλι με την εντολή netstat την κατάσταση του Queue στον server/victim.



- Παρατηρούμε ότι η χρήση του Queue έχει φτάσει το ***max όριο συνδέσεων****. Τα υπόλοιπα* ***SYN πακέτα*** *που δεν χωράνε στο Queue* ***χάνονται****. Ταυτόχρονα, το σύστημα του Server/Victim γίνεται πιο* ***αργό****.*

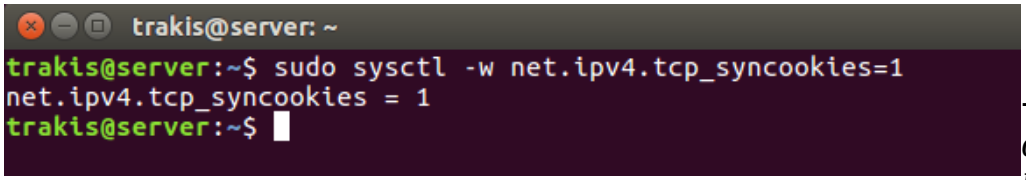
- Ελέγξαμε πως το SYN FLOODING όντως λειτουργεί σωστά, προσπαθώντας να κάνουμε telnet στον Server/Victim από τον attacker σε ένα 2ο terminal



- Ωστόσο η σύνδεση δεν πετυχαίνει

a) SYN Flooding με τα Cookies ενεργοποιημένα

- Επαναλαμβάνουμε όλα τα βήματα που κάναμε, ενεργοποιώντας αυτή την φορά τα Cookies



- Τρέχουμε πάλι από τον ***host/attacker*** *την εντολή* ***sudo netwox 76 -i 172.16.46.130 23*** *και έπειτα θα συμβούν τα εξής πράγματα:*

*a) Πάλι η εντολή **netstat** θα βγάλει πως θα έχουμε **128 SYN_RECV συνδέσεις** στο backlog*

b) Δεν πετυχαίνει το Denial Of Service αυτήν την φορά, διότι τελικά θα καταφέρουμε να κάνουμε telnet, έστω και με μεγάλη καθυστέριση

- Σε αντίθεση με την προηγούμενη περίπτωση όπου ο Server είχε απενεργοποιημένα τα SYN COOKIES, ο Server δεν απορρίπτει τα SYN πακέτα, αλλά συμπεριφέρεται λες και έχει μεγαλώσει το SYN Queue

*- Η μεγάλη αυτή **καθυστέριση** οφείλεται στο ότι μόλις γεμίσει το Queue από SYN συνδέσεις, πρέπει ο Server να απαντήσει με **SYN_ACK + τα Cookies**. Τότε, μπορεί ο Server να αφαιρέσει μία SYN_ACK σύνδεση και να βάλει μια άλλη.*