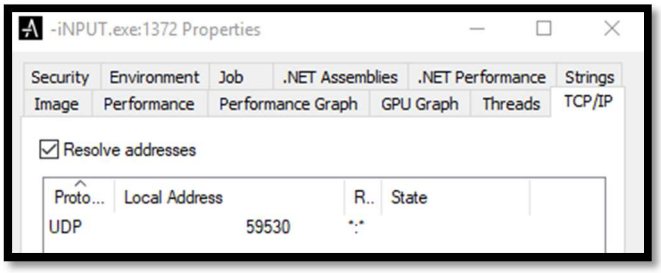
-INPUT-ACE Version 2.2.1

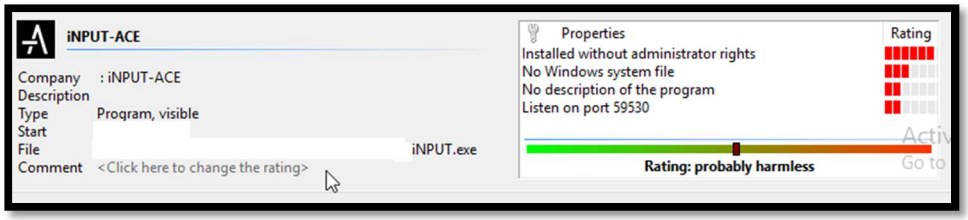
(Review)

Description: This is a review of the -iNPUT-ACE version 2.2.1. The software has a vulnerability that could lead to a denial-of-service (DoS) using a User Datagram Protocol (UDP) flood attack[1]. Other types of attacks using UDP ports may be available.

1. UDP Flood Attack

1.1 The software relies in the use of an UDP port (e.g. 59530):

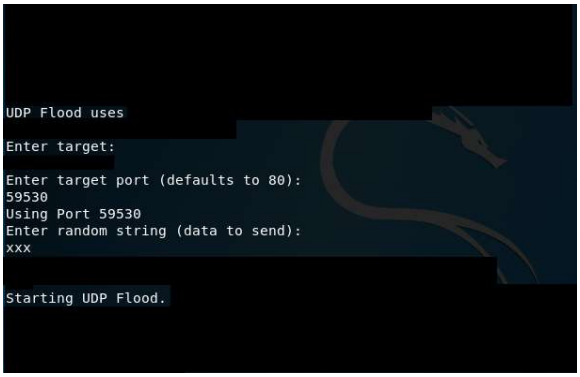




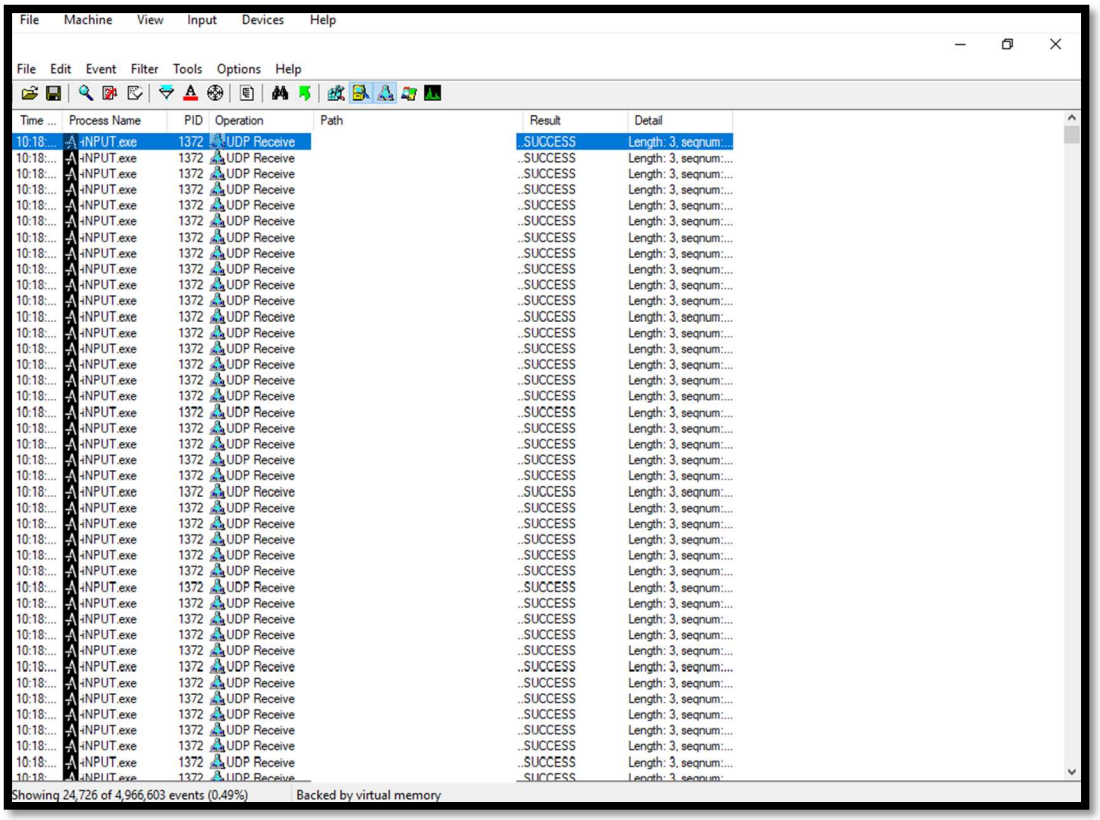
1.2 The port has an open status with a filtered status:

[1] https://en.wikipedia.org/wiki/UDP_flood_attack

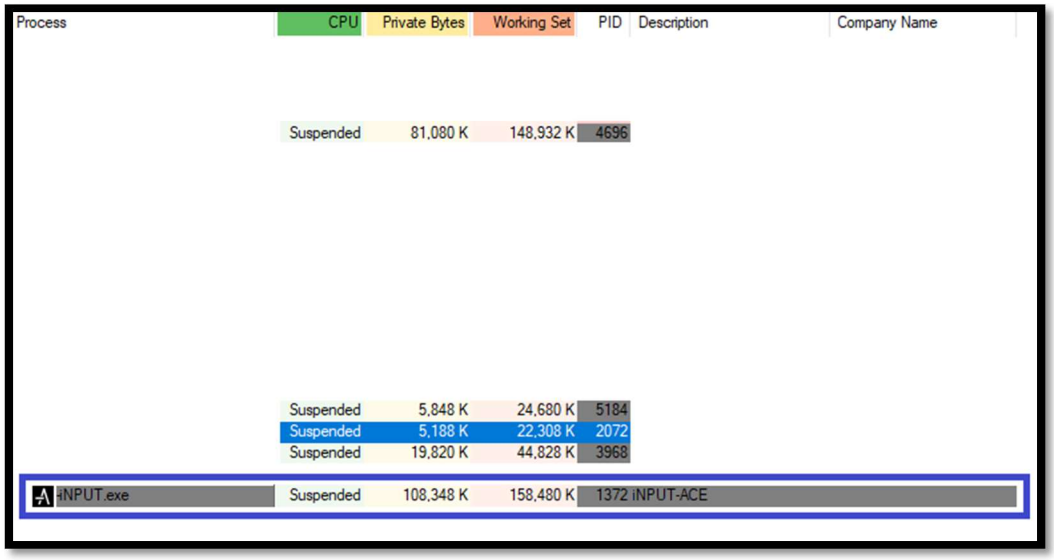
1.3 Then it is possible to send packages to the target port (e.g. 59530) using strings (e.g. “xxx”):



1.4 Confirm the flood in the victim machine (Length:3):



1.5 To finally, suspend the software process and others under execution in the victim machine.



1.6 There is the possibility also to replicate the attack over a Transmission Control Protocol (TCP) as well by using the Remote Address and Remote Port information.