PROJECT DESCRIPTION

To analyse a given network to monitor the transfer of packets from source to destination and observe the malicious attacks on different destination IP address and thereby determine the anomalous behavior of the monitored network. The network to be monitored will be captured using wireshark software .

The monitored network will be stored in the form of .pcap / .csv format which will be feeded as a dataset to our Python script . The script will help us to analyse the network graphically using NetworkX package and hence determining the anomalous behavior of the network **.” *As wisely said it is better to analyse a picture than a text*”.** As an output our script will determine the source as well as destination IP address included in the malicious attacks .

All the TCP SYN Flooding is analyzed on the destination IPs by monitoring the three way handshaking procedure between the source and the destination during connection establishment. The attackers keep on sending packets with SYN flag raised repeatedly to the client keeping the destination port busy whereas the client on the other side keeps on waiting for the connection to be established resulting in the application to get freezed. The attacker never uses same source IP rather different fake IPs each time it sends the packet to the client requesting for the connection.

The attacks were detected by analyzing each packet on each and every destination port in time intervals of 10 secs , which is the standard TCP timeout value , corresponding to the arriving time of each packet. Thos packets receiving a continuous SYN flag were recoreded.

Technologies & Softwares Used :

* Python
* NetworkX
* Pylab
* Anaconda Navigator
* Wireshark

**NetworkX**

NetworkX is a Python package for the creation, manipulation, and study of the structure, dynamics, and functions of complex networks.

NetworkX provides

* tools for the study of the structure and dynamics of social, biological, and infrastructure networks;
* a standard programming interface and graph implementation that is suitable for many applications;
* a rapid development environment for collaborative, multidisciplinary projects;
* an interface to existing numerical algorithms and code written in C, C++, and FORTRAN; and
* the ability to painlessly work with large nonstandard data sets.

With NetworkX you can load and store networks in standard and nonstandard data formats, generate many types of random and classic networks, analyze network structure, build network models, design new network algorithms, draw networks, and much more.

**TCP SYN FLOOD**

TCP SYN flood (a.k.a. SYN flood) is a type of [Distributed Denial of Service](https://www.incapsula.com/ddos/denial-of-service.html) ([DDoS](https://www.incapsula.com/ddos/denial-of-service.html)) attack that exploits part of the normal [TCP three-way handshake](https://www.incapsula.com/cdn-guide/cdn-and-ssl-tls.html#ssl-handshake) to consume resources on the targeted server and render it unresponsive.

Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation.

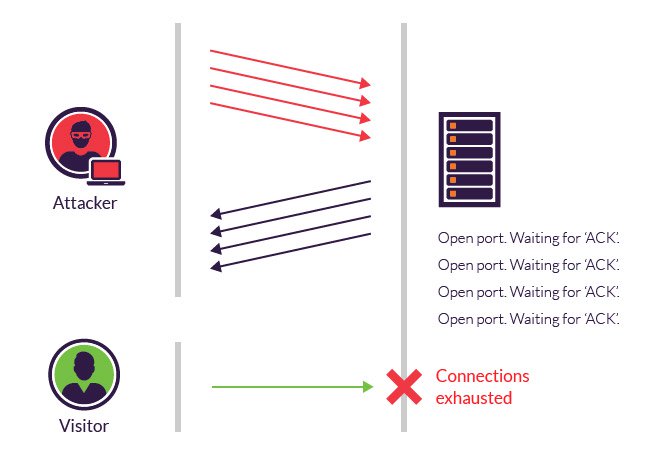
**ATTACK DESCRIPTION**

When a client and server establish a normal TCP “three-way handshake,” the exchange looks like this:

1. Client requests connection by sending SYN (synchronize) message to the server.
2. Server acknowledges by sending SYN-ACK (synchronize-acknowledge) message back to the client.
3. Client responds with an ACK (acknowledge) message, and the connection is established.

In a SYN flood attack, the attacker sends repeated SYN packets to every port on the targeted server, often using a fake IP address. The server, unaware of the attack, receives multiple, apparently legitimate requests to establish communication. It responds to each attempt with a SYN-ACK packet from each open port.

The malicious client either does not send the expected ACK, or—if the IP address is spoofed—never receives the SYN-ACK in the first place. Either way, the server under attack will wait for acknowledgement of its SYN-ACK packet for some time.



REFERENCES

<https://networkx.github.io/documentation/stable/>

<https://www.incapsula.com/ddos/attack-glossary/syn-flood.html>

<https://networkx.github.io/documentation/networkx-1.10/tutorial/index.html>