Exposys Data Labs

FROM: DEEP PARMAR

Introduction

Denial of Service (DoS) attack is executed to determine a specific category of information warfare where a malicious user blocks legitimate users from accessing network services by exhausting the resources of the victim system. Without hacking the password files or stealing sensitive data, a DoS attacker creates network congestion by generating a large volume of traffic in the area of the targeting system.

Existing Method

Inferring of Internet Denial-of-Service Activity is extremely difficult for even system administrators because the current Internet protocol does not require a mechanism for the current packets to be pre-verified before leaving from a source network, during traversing through inter-networks and finally to be authenticated after arriving at any machines of the destination network. This anonymity is the most beautiful of the Internet in spite of leaving unfavourable security issues.

Proposed Method

Establishing a defence mechanism which provides a powerful security against resource consumption attacks namely denial of service attacks. Before the successful attack the attacker's traffic consumes much network resources which lead to congestion over the network. This mechanism is a hybrid model consisting of a pushback mechanism with client puzzles.

Methodology

The proposed work is a hybrid model for providing the defence against DoS/DDoS attacks. A router based client puzzle to suppress the attack traffic at the edge router itself is introduced. Intelligent routers have the responsibility of authenticating the host requests and allocating the network resources. This router based model is integrated with the pushback method. With this a very powerful defence against both the DoS/DDoS attacks can be provided.

Implementation

To simulate the proposed system, we have to create the network. This network consists of LAN's connected with ISP's. This Network layout was created in Network Simulator. Figure 4 shows the network layout structure.

1. Attack Traffic Generation Phase
2. Pushback Mechanism Phase

Conclusion

This proposed method provides a strong defence against the malicious hosts in the network, and it easily identifies the attacker hosts by their traffic nature and blocks all the traffic from the attacker hosts. Client puzzles give the advantage to validate the suspected hosts in order to confirm whether the suspected hosts are from an attacker or from a legitimate user.