Simulating Network Intrusion in NS-2

Palash Verma, John DeDourek, Przemyslaw Pochec
Faculty of Computer Science, University of New Brunswick, Fredericton, NB, Canada E3B 5A3

Introduction

▪ An Intrusion can be defined as any set of actions to compromise the integrity, confidentiality and/or availability of a resource. Intrusion attacks on Computer Networks have become a very common scenario.

▪ Denial of Service (DoS) & Distributed Denial of Service (DDoS) Intrusion attacks are very easily generated and are tough to detect as they are similar to the normal traffic packets.

▪ Network Simulation provides as a very convenient tool to model and study such intrusion attacks.

▪ In our research, we tried to observe as to how the network properties change during a DoS and DDoS attack, on a wired network.

Methodology

▪ We started by creating a model for the normal network. The network consisted of 64 wired nodes, highly meshed, to simulate a switched network, where every node is connected to the other nodes in the network. All links have 1 Mbps bandwidth, with a delay of 100 ms. The legitimate nodes are defined as UDP agents sending packets of size 600 bytes. All nodes use Constant Bit Rate (CBR) Traffic. TCL was used to model the network. A dormant attacker node is also created with 10Mbps bandwidth and 100ms delay (Node 64 visible in red hexagon on the right)

▪ Next we modeled our malicious node which is used to simulate Intrusion. This was modeled by using ICMP agent so that we can mimic a DoS attack. This node when activated sends ping messages to the compromised node, in a flood mode, i.e. as fast as possible. This is shown by red packets being sent to Node 0 on the right. Due to overwhelming ping traffic the node starts dropping packets. As a result, legitimate nodes are denied access to the compromised node.

▪ To further extend our study, we created 5 more malicious nodes (namely n65 – n69) having exactly the same characteristics as of the earlier malicious node. In this simulation, all the malicious nodes are activated together to create a DDoS attack. Once activated all the nodes send malicious ping packets in flood mode to the compromised node, denying access to other legitimate nodes.

▪ Once the modelling is completed we will run the three simulations and create respective nam files. Then we use an awk script to extract data out of the nam files

Goals

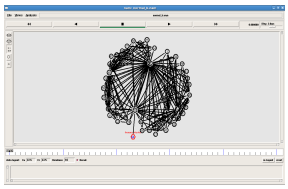
▪ We want to analyze the use of NS-2 simulations as a possible tool for studying Intrusion in networks.

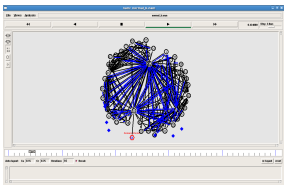
▪ We would like to consider questions such as: can we run these simulations in a reasonable time and space?

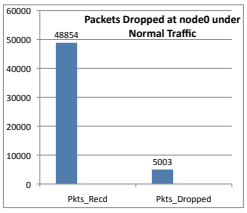
▪ Analyze the network behaviour from simulation results. Network behaviour is expected to change once an attack begins.

Experiments and Results

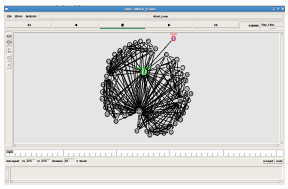
Simulation with normal traffic

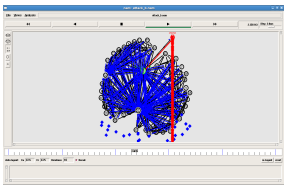


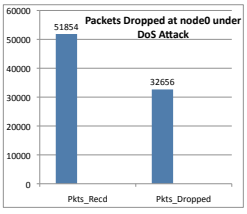




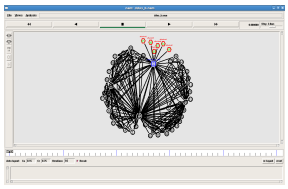
Simulation of DoS attack

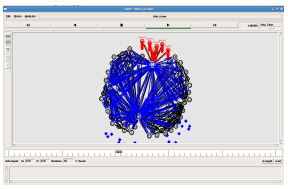


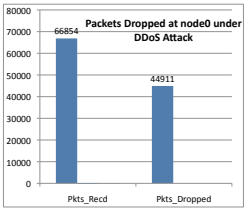




Simulation of DDoS Attack







Network Simulator *v2* (NS-2)

▪ NS-2 is a object oriented, discreet event driven network simulator, developed by UC Berkeley, written in C++ and OTcl (Tcl script language with Object-oriented Extensions). It can simulate real network structures and characteristics in the network structure.

▪ C++ defines the internals of the simulator objects where as, the OTcl is responsible for assembling, configuring and running the discreet events in the simulator environment

▪ It simulates actual network protocols such as TCP and UPD, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and much more.

▪ NS-2 also implements multicasting and some of the MAC layer protocols for LAN simulations.

▪ Once simulations are complete, NS-2 outputs either text based or animation based results.

Denial of Service (DoS)

▪ DoS is a complex and fascinating form of computer attack that impacts the confidentiality, integrity, and availability of millions of computers worldwide.

▪ The sole purpose of launching such an attack is to stop the victim computer from serving legitimate requests.

▪ Most DoS attacks exploit flaws related to the implementation of a TCP/IP model protocol.

▪ DoS can be classified in two forms namely
  • Denial of service by saturation, which involves flooding a machine with requests so it can no longer respond to actual requests
  • Denial of service by vulnerability exploitation, which involve exploiting a flaw in the remote system so as to make it unusable.

Distributed Denial of Service (DDoS)

▪ DDoS is an extensive form of DoS. In this attack multiple compromised hosts in the network attack the victim.

▪ To amplify the effect and hide real attackers, DDoS attacks can be generated in two different ways:
  • In one, the attacker compromises a number of agents and manipulates the agents to send attack traffic to the victim.
  • In other form the attacker uses reflectors. A reflector is any host that responds to a packet if it receives a packet.

▪ ICMP flooding based attack uses ICMP protocol. Usually ICMP REQUEST and ECHO REPLY messages are used for carrying control information for network management.

▪ In a typical attack the source address field of a ICMP ECHO REQUEST message is set as the victim address. Therefore, the ICMP ECHO REPLY message will be sent to the victim instead of the real request message sender (the attack agent).