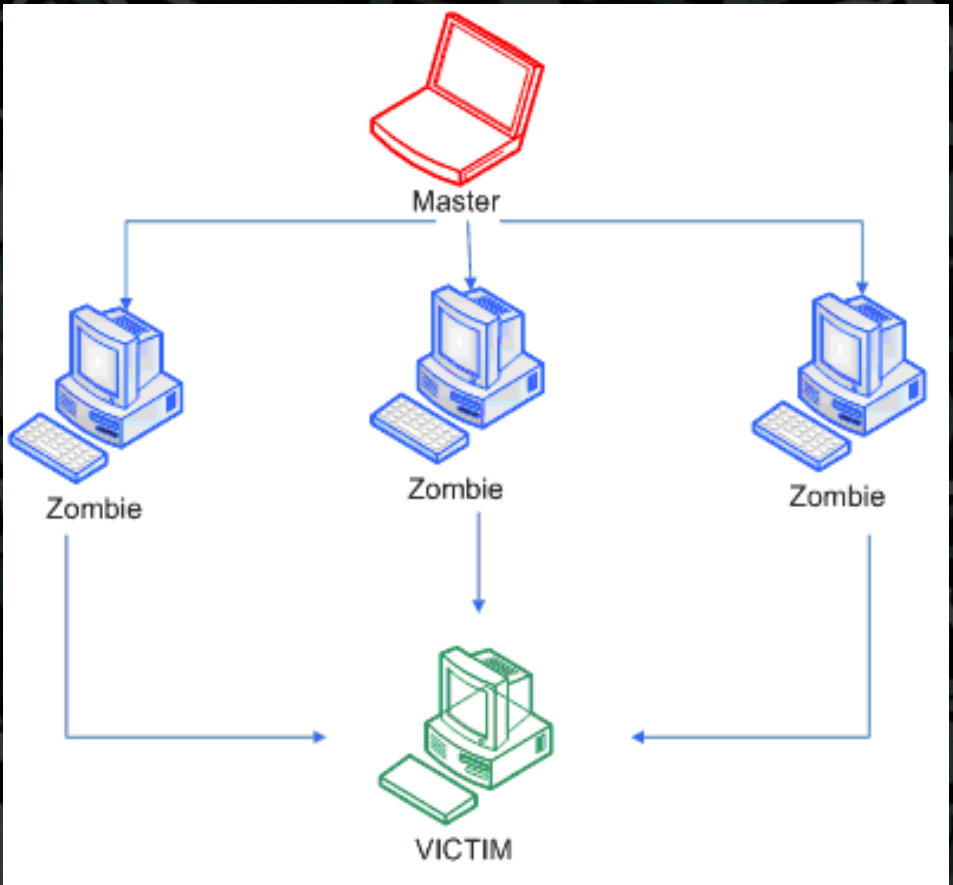
Welcome

Denial of Service Attacks

- One of the attack which causes more losses to the victim
- Easy to carry out by skiddies due to the presence of a lot of point and click tools
- Clogs the Bandwith and results in Network Conjection
- Productivity gets disturbed

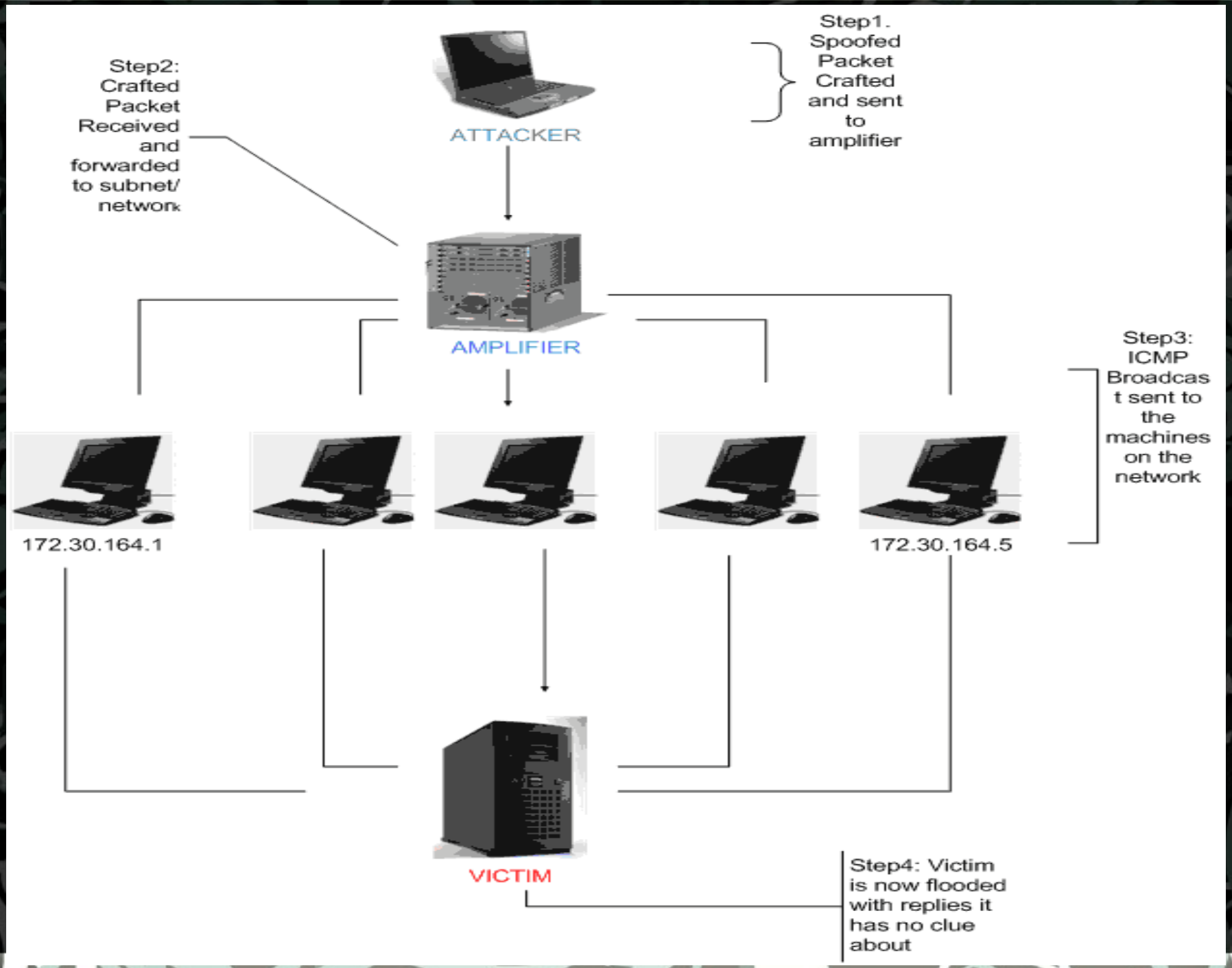
DDoS Attacks



- Highly Profitable attacks
- Group of hacked computers called Botnets (Zombies)
- Yahoo,ebay,Paypal etc. had been DDoSed

BANDWIDTH EXHAUTION

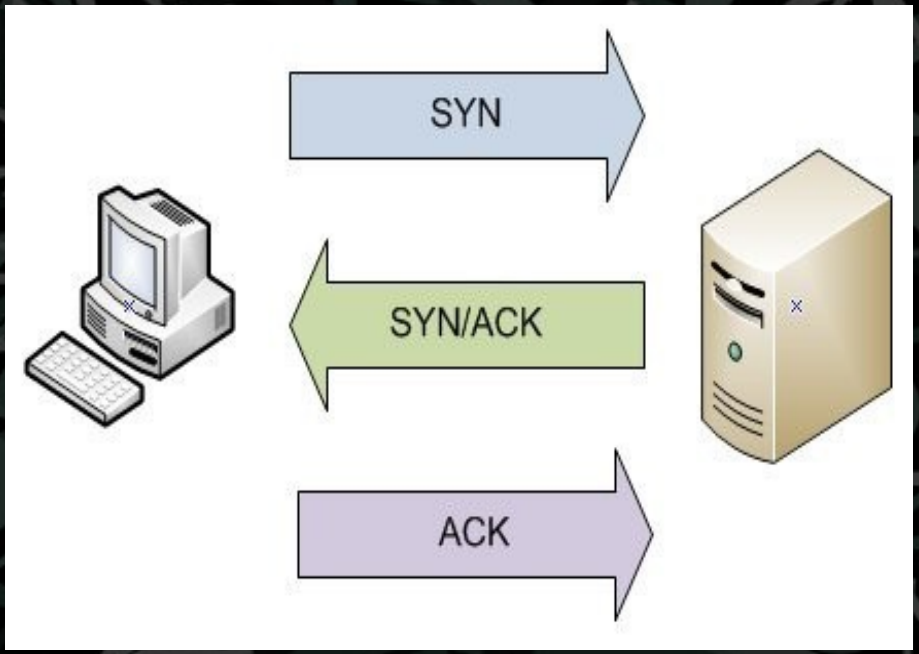
- Smurf
- Spoofed ICMP is sent to Broadcast device
- Victim receives huge amount of traffic from the network.


Step1. Spoofed Packet Crafted and sent to amplifier
ATTACKER
Step2: Crafted Packet Received and forwarded to subnet/ network
AMPLIFIER
Step3: ICMP Broadcast sent to the machines on the network
172.30.164.1
172.30.164.5
VICTIM
Step4: Victim is now flooded with replies it has no clue about

Network Connectivity Attacks

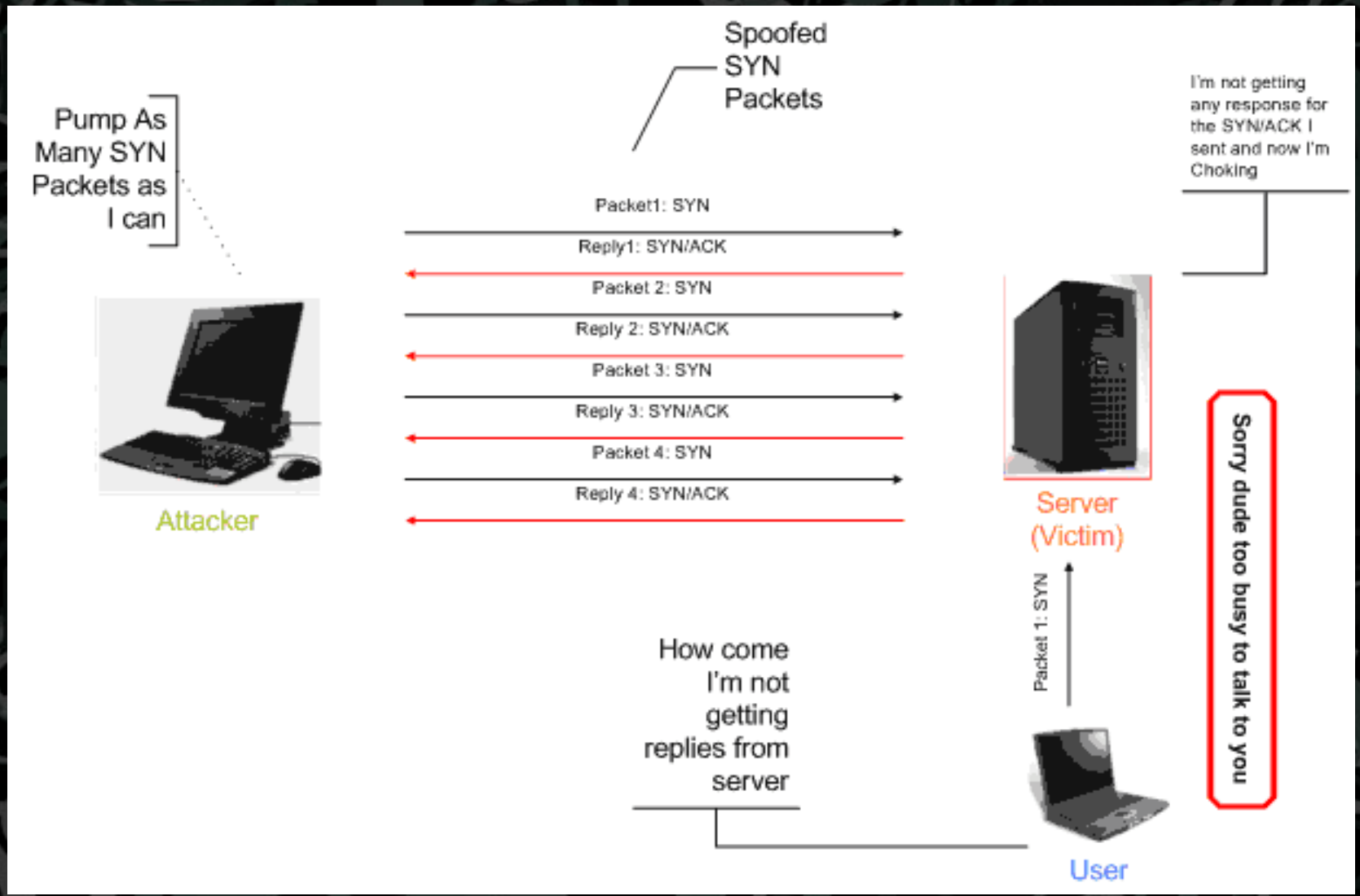
- SYN-FLOODING

SYN Flooding

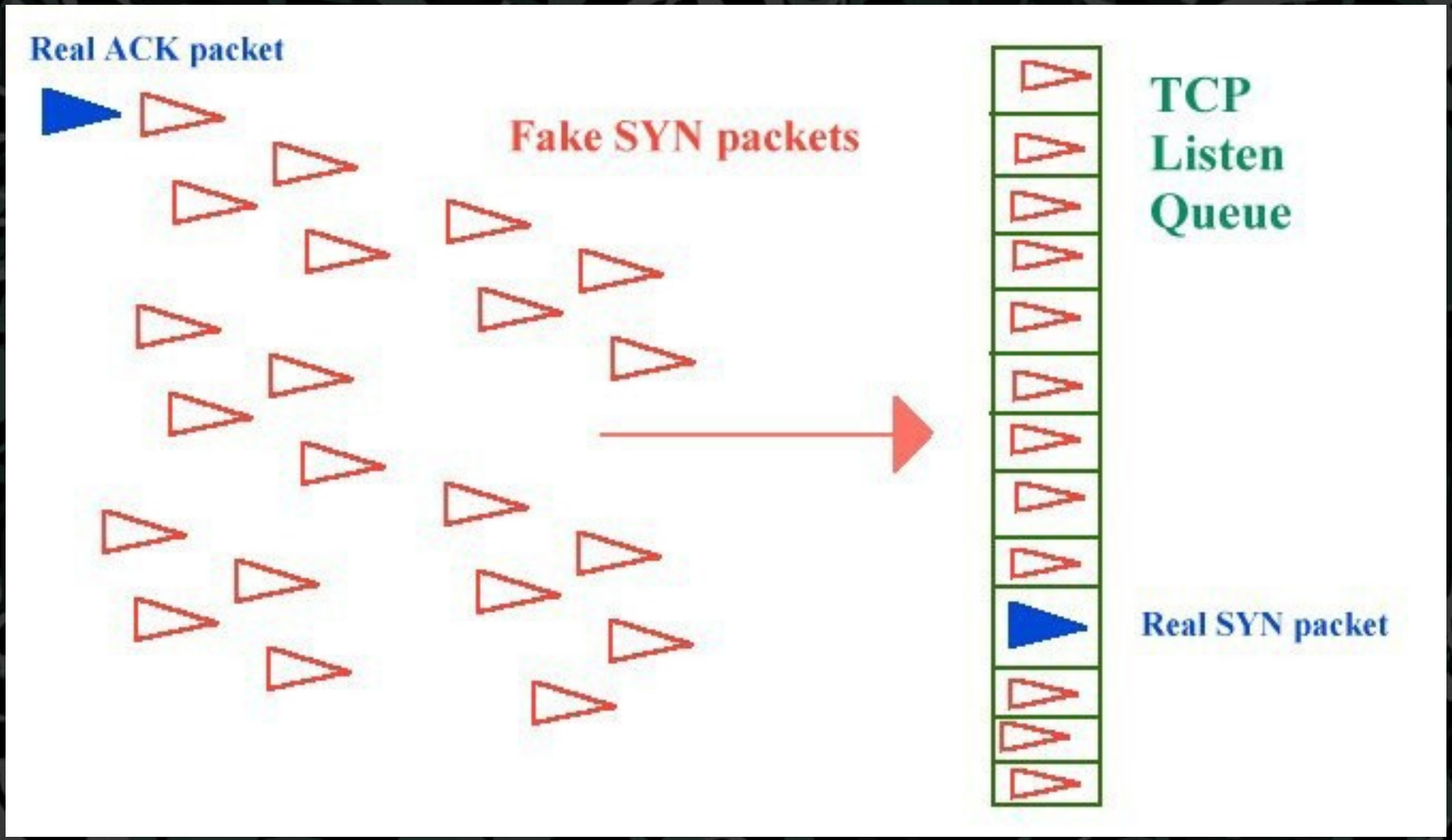


- Basic Flaws in Implementation of TCP/IP
- Retransmission of Packets which is due to Error correcting & Error detecting

A Typical SYN FLOODING scenerio



Backlog Queue



Built in Schemes

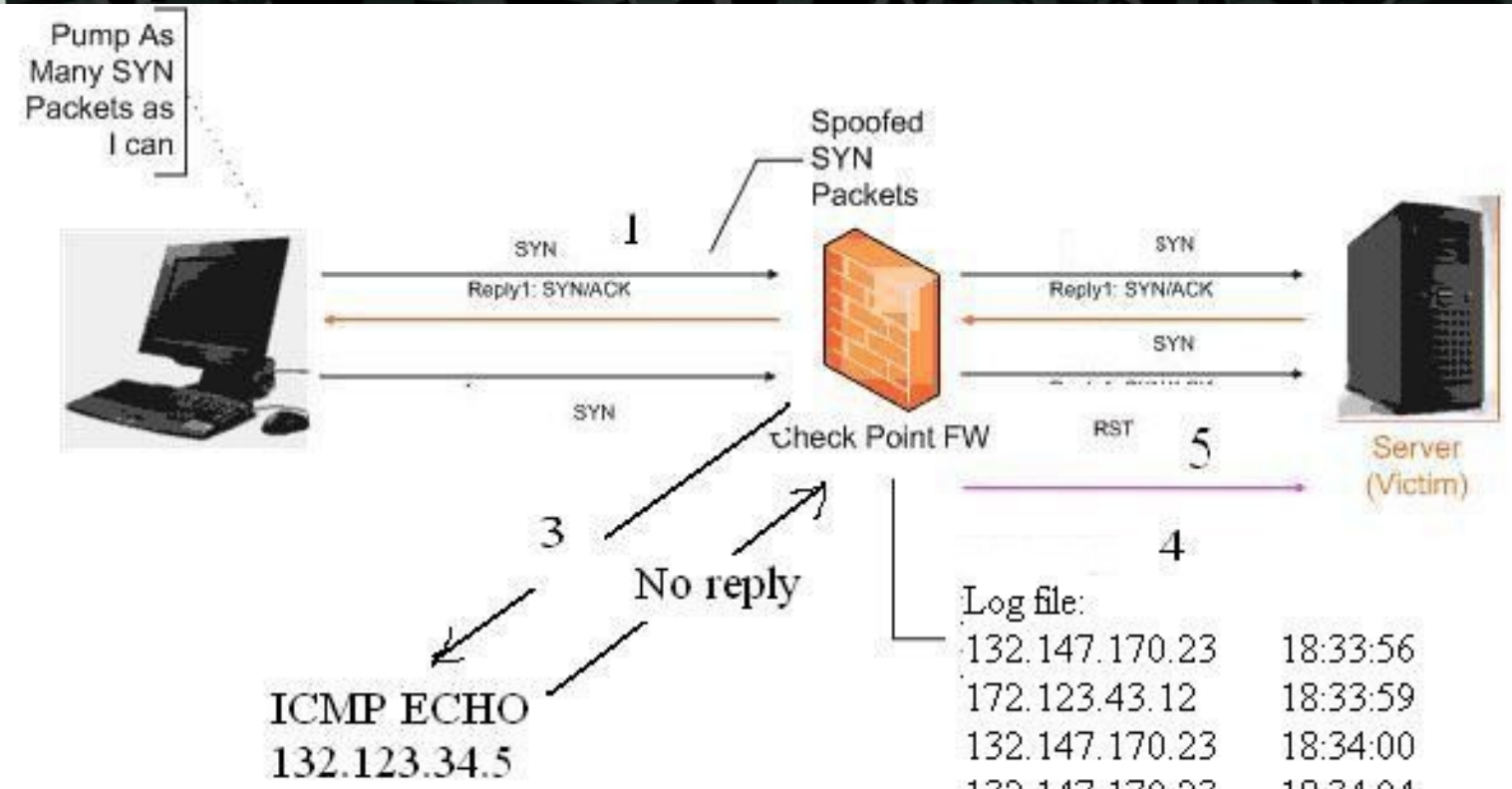
- SYN Cookies in Linux
- SYNAttackProtect in Microsoft Server 03

Our Solution

SYN_Handler

- Identifying the Attacker's SYN Packet from a group of legitimate Packets
- Backup checking
- Isolating the Attacker
- QoS is unaltered
- Using Limited resources to prevent the attack

SYN_Handler



1.Normal SYN pkt
2.75% Backlog queue is full(sme thing happens)
3.ICMP Echo sent to clients trying to connect
4.If no reply is recieved IP adress is Logged alon with time else forwaded to server
5.If another SYN pkt coreesponding to logged IP is found at a time greater than T1 RST is sent to reset all the connections from that IP,and it is added to block list to block further attempts.

Algorithm

- Backlog queue triggers the Transparent firewall
- Firewall logs the incoming requests in logfile
- ICMP request is sent to all clients in the logfile
- If it obtains a valid reply connections takes place as usual
- If reply is not obtained it is logged in ICMP Log

Algorithm

- When ICMP log is not empty firewall monitors for incoming requests from clients in ICMP log
- The time function checks the time in ICMP Log,Log file

THANK YOU

REFRENCES:

Computer Networks By Andrew.S.TanenBaum

PacketStrorm [http://www.packetstorm.com]

SecurityFocus[http://www.securityfocus.com]

Hacking Exposed 5 By StuartMcClure

Bugtraq mailing list.