Denial of Service (DoS) attacks and countermeasures

Pier Luigi Rotondo
IT Specialist
IBM Rome Tivoli Laboratory
Definitions of DoS/DDoS attacks

- Denial of Service is the prevention of authorised access to a system resource or the delaying of system operations and functions [1]

- The main attacker’s objective is to render the target system resource or service inaccessible by legitimate users

- Trivial example: DoS attack to a corporate switchboard

- DDoS are distributed Denial of Service attacks that achieve larger magnitude by launching coordinated attacks by using a framework of “handlers” and “agents”
DoS attacks in the news

- On February 2000, several serious DDoS attacks targeted some of the largest Internet web sites, including Yahoo, Buy.com, Amazon, CNN and eBay.
The DOS phenomenon

- Dollar amount of losses by type

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>Dollar Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of Proprietary Info</td>
<td>70,195,900</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>65,643,300</td>
</tr>
<tr>
<td>Virus</td>
<td>27,382,340</td>
</tr>
<tr>
<td>Insider net abuse</td>
<td>11,767,200</td>
</tr>
<tr>
<td>Financial fraud</td>
<td>10,186,400</td>
</tr>
<tr>
<td>Laptop theft</td>
<td>6,830,500</td>
</tr>
<tr>
<td>Sabotage</td>
<td>5,146,500</td>
</tr>
<tr>
<td>System Penetration</td>
<td>2,754,400</td>
</tr>
<tr>
<td>Active wiretapping</td>
<td>705,000</td>
</tr>
<tr>
<td>Telecom fraud</td>
<td>701,500</td>
</tr>
<tr>
<td>Unauthorised insider access</td>
<td>406,400</td>
</tr>
<tr>
<td>Telecom eavesdropping</td>
<td>76,000</td>
</tr>
</tbody>
</table>

Source: Computer Security Institute
Classification of DoS attacks

1. Bandwidth consumption
   - Attacks will consume all available network bandwidth

2. Resource starvation
   - Attacks will consume system resources (mainly CPU, memory and storage space)

3. Programming flaws
   - Failures of applications or OS components to handle exceptional conditions (i.e. unintended data is sent to a vulnerable component)
   - OS components’ crash
Modes of attacks

1. explicit network connectivity attacks
   - flooding
   - malformed traffic

2. explicit consumption of resources
   - data structures
   - storage (i.e. intentionally generating errors that must be logged)

3. side effect of other forms of attack
   - from a virus (i.e. SQL slammer virus)
   - accounts locked-out during a password cracking
The network layer provides an end-to-end mechanism to move datagrams, independently of the underlying protocols, from the source to the destination host (whence the *end-to-end* definition), in an unreliable and connectionless manner.

Transport layer messages are taken and then split into network layer datagrams (each up to 64KB in the IP network protocol). Each datagram is then transmitted through the Internet, fragmented in smaller chunks if required by the underlying protocols, and reassembled at the other end, where it is delivered to the transport layer.
IP datagrams

- IP (Internet Protocol) is the network layer protocol used in the Internet.

<table>
<thead>
<tr>
<th></th>
<th>ICMP</th>
<th>IGMP</th>
<th>TCP</th>
<th>UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 4 “octets” (32 bit) each address aaa.bbb.ccc.ddd (IPv4)

Sample IP datagram:

```plaintext
Sample IP datagram:

---( 98 bytes transmitted on interface en0 )---
17:08:47.243631253
ETHERNET packet: [00:04:ad:9a:78:e6 -> 00:06:29:fa:da:aa] type 800 (IP)
IP header breakdown:
< SRC = 192.168.1.23 > (source.mydomain.com)
< DST = 192.168.1.19 > (target1.mydomain.com)
ip_v=4, ip_tl=20, ip_tos=0, ip_len=84, ip_id=41600, ip_off=0
ip_ttl=255, ip_sum=7e54, ip_p = 1 (ICMP)
```
ICMP datagrams

- ICMP (Internet Control Message Protocol) datagrams are signaling messages, encapsulated within IP datagrams, used by the network layer to notify special events such as destinations unreachable, redirection, congestion control, testing network connectivity and others.
ICMP “echo” datagrams

- ICMP “echo” datagrams are typically used to test network connectivity.
- A destination host is expected to respond with an ICMP ECHO_REPLY message when “pinged” with an ICMP ECHO_REQUEST message.

```
$ ping target  
PING target: (10.0.7.1): 56 data bytes  
64 bytes from 10.0.7.1 : icmp_seq=0 time=0 ms  
64 bytes from 10.0.7.1 : icmp_seq=1 time=0 ms  

---target PING Statistics---  
0% packet loss  
round-trip min/avg/max = 0/0/0 ms  
$
```
Anatomy of a “ping” command

ETHERNET packet: [00:04:ad:9a:78:e6 -> 00:06:29:fa:da:aa] type 800 (IP)
IP header breakdown:
  < SRC = 192.168.1.23 > (source.mydomain.com)
  < DST = 192.168.1.19 > (target1.mydomain.com)
  ip_v=4, ip_hl=20, ip_tos=0, ip_len=84, ip_id=41600, ip_off=0
  ip_ttl=255, ip_sum=7e54, ip_p = 1 (ICMP)
ICMP header breakdown:
  icmp_type=8 (ECHO_REQUEST)  icmp_id=43894  icmp_seq=0

IP header breakdown:
  < SRC = 192.168.1.19 > (target1.mydomain.com)
  < DST = 192.168.1.23 > (source.mydomain.com)
  ip_v=4, ip_hl=20, ip_tos=0, ip_len=84, ip_id=12029, ip_off=0
  ip_ttl=255, ip_sum=f1d7, ip_p = 1 (ICMP)
ICMP header breakdown:
  icmp_type=0 (ECHO_REPLY)  icmp_id=43894  icmp_seq=0
“Ping of death”

- In the IP specification, the maximum datagram size is 64 KB.

- Some systems react in an unpredictable fashion when receiving oversized (>64 KB) IP datagrams, causing systems crashing, freezing or rebooting, and resulting in a denial of service.

- Example of a DoS that exploits a programming flaw: the IP implementation is unable to deal with the exceptional condition posed by the oversized datagram.

- Exploitable with the “ping” command, as some ping implementations allowed users to send datagrams larger than 64KB. One datagram is enough to crash a vulnerable system.
Yet another simple form of DoS: ICMP (ping) flood

- Attackers flood a network link with ICMP ECHO_REQUEST messages using the “ping” command.

- Exploits a characteristic of the IP layer, that answers with ICMP ECHO_REPLY messages upon reception of ICMP ECHO_REQUEST messages.

- Very simple case of bandwidth consumption DoS.
ICMP (ping) flood

- The attack is successful only if the source host and the channel between source and target have enough network bandwidth to flood the target host.
## IP addressing

<table>
<thead>
<tr>
<th>IP addr class</th>
<th>Network address</th>
<th>Host address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>110</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1110</td>
<td></td>
</tr>
<tr>
<td>Class A</td>
<td>Network address (7 bit)</td>
<td>Host address (24 bit)</td>
</tr>
<tr>
<td>Class B</td>
<td>Network address (14)</td>
<td>Host address (16 bit)</td>
</tr>
<tr>
<td>Class C</td>
<td>Network address (21 bit)</td>
<td>Host address (8 bit)</td>
</tr>
<tr>
<td>Multicast</td>
<td>Multicast address (28 bit)</td>
<td></td>
</tr>
</tbody>
</table>

### 4 IP address classes:

- **Class A**: Network address (7 bit) and Host address (24 bit)
- **Class B**: Network address (14) and Host address (16 bit)
- **Class C**: Network address (21 bit) and Host address (8 bit)
- **Multicast**: Multicast address (28 bit)
**IP subnetting**

- A single network is divided into multiple logical networks (subnets)

<table>
<thead>
<tr>
<th>IP addr class</th>
<th>Network address</th>
<th>Host address</th>
</tr>
</thead>
</table>

151.100.17.13

- **10010111** – class B
- **10 010111 01100100** – network
- **subnet** (with 8-bit subnetting)
- **host**
Directed broadcast addresses

- The *directed broadcast address* is an IP address with all the host address set to 1. It is used to simultaneously address all hosts within the same network.

- I.e. the directed broadcast address for the network class B 151.100.0.0 has IP address 151.100.255.255 and addresses simultaneously all the $2^{16} - 2$ hosts that can be addressed within that network.

- The subnetted networks, the *directed broadcast address* is an IP address with all the host address set to 1 within the same subnet.
“ping” to a directed broadcast address

- All hosts in the broadcast domain answer back

- Network traffic “amplification”: 1 datagram generates $n$ datagrams in response (where $n$ is the number of systems replying to a broadcast ICMP ECHO_REQUEST)
Smurf attack

- In a **Smurf** attack, the attacker sends ping requests directed to a broadcast address, with the source address of the IP datagram set to the address of the target system under attack (spoofed source address)

```
IP header breakdown:
< SRC = 192.168.1.19 > (target.mydomain.com)
< DST = 192.168.1.255 >
ip_v=4, ip_hl=20, ip_tos=0, ip_len=84, ip_id=41600, ip_off=0
   ip_ttl=255, ip_sum=7e74, ip_p = 1 (ICMP)
ICMP header breakdown:
icmp_type=8 (ECHO_REQUEST) icmp_id=43554 icmp_seq=0
```
Smurf attack

- All systems within the broadcast domain will answer back to the target address, thus flooding the target system with ICMP traffic and causing network congestion => little or no bandwidth left for legitimate users

IP header breakdown:
- \( \langle \text{SRC} = 192.168.1.xxx \rangle \) (xxx.mydomain.com)
- \( \langle \text{DST} = 192.168.1.19 \rangle \) (target.mydomain.com)
- \( \text{ip_v}=4, \text{ip_hl}=20, \text{ip_tos}=0, \text{ip_len}=84, \text{ip_id}=41600, \text{ip_off}=0 \)
- \( \text{ip_ttl}=255, \text{ip_sum}=7e74, \text{ip_p} = 1 \) (ICMP)

ICMP header breakdown:
- \( \text{icmp_type}=0 \) (ECHO_REPLY) \( \text{icmp_id}=43554 \) \( \text{icmp_seq}=0 \)

IBM Software Group
Smurf attack – putting things together

ICMP ECHO_REQUEST

192.168.1.0

target.mydomain.com

192.168.1.19

ICMP ECHO_REPLY
Smurf attack highlights

- Traffic amplification: strength to the attack is given by the amplification factor provided by all affected systems in the broadcast domain.

- By using the amplification effect, systems with limited network resources may generate a large amount of network traffic towards sophisticated sites.

- Hidden source address (IP spoofing). The source address of the 1st datagram (from attacking system to the broadcast address) corresponds to the address of the attacked system.
Smurf attack protection

- Prevent being used as an intermediary
  - Hosts can be configured not to respond to ICMP datagrams directed to IP broadcast addresses. Most OSes have specific network settings to enable/disable the response to a broadcast ICMP ping message
  - Disable IP-directed broadcasts at your leaf routers: to deny IP broadcast traffic onto your network from other networks (in particular from the Internet)

- Block users of your network from attacking other systems
  - A forged source is required for the attack to succeed. Routers must filter outgoing packets that contain source addresses not belonging to local subnetworks

- Install IDS (Intrusion Detection Systems) capable of detecting Smurf attacks
Smurf attack protection

- Configure ICMP traffic rate limiting
Fraggle attack

- A variant of Smurf: uses UDP packets instead of ICMP datagrams
- Attackers send spoofed UDP packets of the broadcast address of the amplifying network, typically towards UDP port 7 (echo)
Fraggle attack

- For a successful Fraggle attack, the attacker needs systems with the UDP echo service enabled.

- If UDP echo is enabled, *the system will respond* with an another UDP echo packet back to the system under attack.

- If UDP echo is not enabled, *the system will respond* with an ICMP PORT_UNREACHABLE datagram, still consuming bandwidth.

- By using the amplification effect, systems with limited network resources may generate a large amount of network traffic towards sophisticated sites.
Fraggle attack protection

- Identify vulnerable systems within your network and prevent being used as an intermediary
  - Perform regular network vulnerability scans and disable UDP/9 (echo) service

- Block users of your network from attacking other systems
  - A forged source is required for the attack to succeed. Routers must filter outgoing packets that contain source addresses not belonging to local subnetworks

- Install IDS (Intrusion Detection Systems) capable of detecting Fraggle attacks
Fraggle attack protection

- Configure UDP traffic rate limiting
TCP’s three-way handshake

- The "three-way handshake" is the procedure used to establish (open) a connection.
TCP’s three-way handshake

IP header breakdown:

< SRC = 192.168.1.23 >  (source.mydomain.com)
< DST = 192.168.1.19 >  (target.mydomain.com)

TCP header breakdown:

<source port=61538, destination port=23(telnet) >
flags <SYN>

IP header breakdown:

< SRC = 192.168.1.19 >  (target.mydomain.com)
< DST = 192.168.1.23 >  (source.mydomain.com)

TCP header breakdown:

<source port=23(telnet), destination port=61538 >
flags <SYN | ACK>

IP header breakdown:

< SRC = 192.168.1.23 >  (source.mydomain.com)
< DST = 192.168.1.19 >  (target.mydomain.com)

TCP header breakdown:

<source port=61538, destination port=23(telnet) >
flags <ACK>
TCP SYN flood

- A TCP SYN flood is an attack based on bogus TCP connection requests, created with a spoofed source IP address, sent to the attacked system. *Connections are not completed*, thus soon it will fill up the connection request table of the attacked system, preventing it from accepting any further valid connection request.

- The source host for the attack sends a SYN packet to the target host. The target host replies with a SYN/ACK *back to the legitimate user of the forged IP source address*. Since the spoofed source IP address is unreachable, the attacked system will never receive the corresponding ACK packets in return, and the connection request table on the attacked system will soon be filled up.
TCP SYN flood

Non reachable IP address

SYN / ACK
SYN / ACK are not acknowledged

connection request table

... SYN-RECEIVED
... SYN-RECEIVED
... SYN-RECEIVED
... SYN-RECEIVED
... SYN-RECEIVED
... SYN-RECEIVED
... SYN-RECEIVED
... SYN-RECEIVED

IBM Software Group
TCP SYN flood

- The attack works if the spoofed source IP address is not reachable by the attacked system. If the spoofed source IP address _where reachable by the attacked system_, then the legitimate owner of the source IP address would respond with a RST packet back to the target host, closing the connection and defeating the attack.

- TCP SYN flood is a denial of service attack that sends a host more TCP SYN packets than the protocol implementation can handle.

- This is a resource starvation DoS attack because once the connection table is full, the server is unable to service legitimate requests.
TCP SYN flood protection

- Apply Operating System fixes:
  - systems periodically check incomplete connection requests, and randomly clear connections that have not completed a three-way handshake. This will reduce the likelihood of a complete block due to a successful SYN attack, and allow legitimate client connections to proceed.

- Configure TCP SYN traffic rate limiting

- Install IDS (Intrusion Detection Systems) capable of detecting TCP SYN flood attacks
TCP SYN flood protection

Filter network traffic:

- Use circuit level firewalls (*stateful inspection*) to monitor the handshake of each new connection and maintain the state of established TCP connections. The filtering system must be able to distinguish harmful uses of a network service from legitimate uses.

- Static packet filtering (*stateless*) does not protect from TCP SYN flood attacks.
Distributed Denial of Service (DDoS)

- The attacking host is replicated through an handler-agent distributed framework.

Attack preparation: as many more systems as possible are compromised with classic system penetration techniques and DDoS agents are installed.

Great amplification factor

Agents attack the target, all together

Attack is launched from the handler

Once the attack has been launched, the handler can be taken offline (i.e. if it’s detected) with the agents able to independently continue with the attack.
DDoS highlights

- Innovative in the form of *coordination* of the attack

- By using the amplification effect given by the handler-agent framework, systems with limited network resources may generate a large amount of network traffic towards sophisticated sites.

- Two kinds of victims:
  - agents (compromised using common weaknesses to install DDoS agents code), likely to be identified guilty during the first stage of the investigation
  - end targets (during the attack)
DDoS highlights

- Agents may be residing on several networks
  - attacks difficult to trace back from once the attack has commenced

- Attacks continue even if the handler, or some (but not all) agents are identified and taken offline
DDoS protection

- Configure routers to filter network traffic
  - Filter RFC 1918 address space
  - Perform ingress filtering\(^7\)
  - Configure traffic rate limiting (ICMP, SYN, UDP, etc)

- Deploy firewalls at the boundaries of your network
  - The filtering system must be able to distinguish harmful uses of a network service from legitimate uses.

- Perform regular network vulnerability scans
  - common vulnerabilities could be exploited to install DDoS agents
  - Identify the agents that are listening to the handler’s commands
DDoS protection

- Install IDS (Intrusion Detection Systems) capable of detecting
  - DDoS handler-to-agent communication
  - DDoS agent-to-target attacks
Risk level of DoS attacks

- A Denial of Service denies a service but does not directly allow unauthorised access.

- Systems under a DoS attacks fail in such a way that they deny access to an attacker rather then letting the attacker in (fail-safe stance)

- Under the above conditions, DoS attacks are typically considered low risk threats.
References


References


Thank you!