Defense against DoS, flooding attacks

Paweł Suwala Natalia Wieczorek
Email: {pawsu509, natwi936}@student.liu.se
Supervisor: Viiveke Fåk, {viiveke@isy.liu.se}
Project Report for Information Security Course
Linköpings universitetet, Sweden

Abstract

The following paper concentrates on the means of defense against denial of service attacks. First, some possible and common denial of service attacks are described to give the reader a basic understanding of what is this type of the attacks. The main part of the project is the mechanism, tools and methods used to prevent the denial of service attacks. At the end a short case study along with the description of the small company network is given. When conducting the experiment we noticed that a successful attack on the networked system is relatively easy as the needed tools are free to download but at the same time the simple means of defense can be applied to make most of the attacks impossible.

Key words: denial of service, distributed denial of service, worm, firewall, network protocols.

1 Introduction

This project was created for the TDDD17 Information Security course. The aim of this project is not to create an elaborate essay on the DoS subject but rather to give the reader a basic understanding of the processes behind the DoS attacks and most importantly the defense mechanism that can be applied in order to protect the networks/computer resources from becoming unavailable. The short case study and graphical presentation of those mechanisms were added to complement and illustrate better the main part of the project – that is a theoretical framework or study on the defense against the DoS attacks. The knowledge that we obtained from literature was then applied in a case study to show the practical approach to the DoS prevention.

2 Background

The denial of service (DoS) or Distributed Denial of service (DDoS) is the group of attacks that are performed to make certain resources unavailable to the intended audience. This short definition states that the targets of attack may vary, but most often those are the sites or services hosted on the high-profile web servers, like banks, credit card payments systems, popular social services – Facebook, Wordpress. In most cases the attack is conducted to generate great financial loss or as an ideological attack, sometimes for personal gain or ambitious reasons. The motivation varies. The goal of the attack is to make the target works less efficiently or not at all, for a given period of time, or permanently. This can be done by forcing the computer target to stop working or consume too many resources to respond to other legitimate requests. The interesting part is that some of those attacks are made possible because of the poor, broken by design protocols such as TCP, ICMP. Those attacks may also not necessarily be very expensive. Especially the distributed denial of service attack that uses botnets (networks of so called Zombie computers - compromised computers running malicious software, usually installed via worms, Trojan horses, or backdoors, working in a controlled infrastructure) can be cheap after the initial infrastructure is created [an example 9]. There is no typical defense mechanism or solutions for those kinds of attacks. Some very well-known cyber wars were related to those attacks [6], like in 2001 when Register.net was targeted, or the same year when a successful attack on Irish Government's Department of Finance was launched. In 2007, a number of successful attacks on popular game servers were conducted by Russian group R.U.S. In a wake of the war in Ossetia, the government sites were blocked by a DoS attack and it was implied and suggested that Russia stood behind those attacks.

3 Overview of the common DoS and DDoS attacks and their classification

The following section contains the short description of the most common Dos and DDoS attacks. Since this paper scope is rather about the defense mechanism than the attacks themselves, the information is provided mostly to give the reader general information about the kinds of attacks that may be possible.

3.1 Attacks Classification

Basically, denial of service attacks can be classified in two ways:
a) Denial of service attacks (DoS) / Distributed Denial of Service attacks (DDoS) / Distributed Reflected Denial of Service attacks.

DoS attack occurs when actions of single attacker results in making certain service unavailable by its target audience. Such attacks can be carried out in numerous ways; however it mostly relies on vulnerabilities or design flaws. Single attacker usually does not have enough bandwidth and resources to perform effective flood.

DDoS attack occurs when multiple compromised systems flood the resources of target system. Such network of compromised computers (a botnet) is prepared before an attack using malware software installed on numerous computers connected to the internet.

DRDoS involves sending forged requests to a very large number of computers that will reply to the request. Source address of the request packets is set to that of the victim. This attack will result in thousands of replies to the victim system, which can lead to crash or resources exhaustion.

b) Wired / Wireless attacks

Wired attack is mostly carried out through the internet to prevent legitimate users from connecting to the available services like website, FTP server, mail server etc.

Wireless attack targets the wireless infrastructure of the network, flooding it by garbage packets or producing noise to disrupt wireless devices. Attacks based on jamming signal by noise requires high-power or/and directed antennas. More sophisticated methods are based on flaws in the security protocol designs.

3.2 General scenarios for DoS attack

DoS and especially DDoS attacks require a certain level of preparation. If it's a distributed attack, then a network of bots is needed. Malicious software has to be implemented and the computers need to be infected. This phase is usually done easily – ready-made worms, Trojans and viruses aid the attacker. Once the control over a certain network is set, it can be used to launch an attack. In case of wireless attacks a high power Network Interface Card and a high directional antenna are needed. This of course makes the attacks expensive. Broken by design protocols (TCP for example) make the attack difficult to detect. Most of DoS attacks are detected too late, when the system actually becomes inoperative. The symptoms may include:

- Significantly decreased network performance noticed by the user and monitoring software
- Unavailability of a particular web site (different types of errors received by the users)
- Dramatic increase in the number of spam emails before an attack may mean that a group or an individual is preparing the environment for a successful attack.

Sometimes a DoS attacks is used as a part of a bigger attack on the system.
The general scenarios for DoS attack may include:

- Significant consumption of computational resources (memory, bandwidth, processor time)
- Disruption of the configuration information
- Disruption of state information, such as unsolicited resetting of the TCP sessions
- Disruption of the physical network devices
- Disturbing the communication media between the accepted/ intended users and the victim (a server) to obstruct communication in an efficient and intended way.

3.3 Typical DoS attacks [8]

3.3.1 ICMP flood attack

ICMP flood attack is based on sending a large amount of ICMP traffic to the victim machine to use up the network bandwidth. This attack in its simplest form can be carried out using the “ping –t target_address” command under *nix system.

3.3.2 Smurf Attack

Smurf attack is a type of ICMP flood attack; this type of attack floods the target machine with the spoofed broadcast ping messages. An attacker sends a large quantity of the ICMP echo request packets to many different network broadcast addresses; all packets have a spoofed IP address of the target victim. Routers will forward the ICMP packet to all hosts, the hosts will try to reply to the ICMP request by sending a reply message to the victim. If there are many hosts in used networks, victim will be effectively spoofed by a large amount of traffic.

3.3.3 UDP flood attack

This attack relies on the User Datagram Protocol which is a connectionless networking protocol. An UDP attack can be carried out by sending a large number of packets to the random ports on the target machine. The victim host will check for the application listening to a flooded port and most likely answer by an ICMP Destination unreachable packet. A misconfigured victim machine will be forced to reply with a large number of ICMP packets, finally leading it to be unreachable to the desirable traffic.

3.3.4 SYN Flood

This attack is based on sending the SYN requests to the target machine. The aim of the attack is to exhaust the allowed number of the half-opened connections. This prevents any new legitimate connections to be established.

3.3.5 LAND attack

This attack is based on sending the spoofed TCP SYN packet with the victims target and destination addresses. As a result, the target machine will reply to itself continuously causing a lock up and denial of service.

3.3.6 WinNuke attack

WinNuke is one of the first Denial of Service attacks. It is based on sending “out of band” data to the target computer to a 139 port. As a result of this attack, a Windows machine will show a classic Blue Screen of Death and lock up. After the blue screen appeared, a machine has to be rebooted, so all unsaved work would be lost.

3.3.7 Teardrop attack

This attack is based on sending the invalid IP packets to the target machine. Depending on the vulnerable system, an attacker can send the over-sized packets or packets that have some overlapping fragments. A bug in an implementation of the TCP/IP packet re-assembly causes crash or unstable behavior in various operating systems.

3.3.8 Application level flood

It is the simplest and most primitive denial of service attack; however it can be very effective. It is based on exhausting the resources on the target machine. There are many ways to do that:

- An attacker can send an overwhelming amount of the packets exhausting bandwidth connection or filling up the disk space by the logs.
- An attacker can localize the most CPU-consuming function of the system and call it many times causing the system overload;
- An attacker can localize a relatively big file on the www server and initiate downloading multiple times exhausting the connection bandwidth.

3.3.9 Fork bomb

This attack is based on the fact that the running process can start another process. A fork bomb is a process that starts itself over and over again exhausting the number of the processes that can run on the operating system simultaneously. After the fork bomb has been started it is almost impossible to start any other legitimate process, nor kill the fork bomb processes. Only reboot of the system can help. Despite that the fork bomb exhausts the space in the table process it also exhaust available memory and processor time.

3.3.10 Peer-to-peer attack

This attack is based on the bugs in the popular p2p file sharing servers. A scenario of this attack begins with finding a bug in the p2p server software (which are mostly open source) and redirecting the connected users from the p2p server to the target website. This results in thousands of connection attempts in a short period of time, which leads to crash or low performance of the server.

4 Defense against the DoS attacks [6]

A set of methods, tools and strategies can be used to prevent the DoS attacks.

4.1 Survival

The first thing after the attack is performed is to ensure the system survival. There should be clear procedures and additional resources to prevent the long-term unavailability of the service. A company that is prepared for the possibility of an attack will be more likely not to suffer the great financial loss. A separate block of the IP addresses for the critical servers, separate routes for the packets, a packet filtering using the stateful packet filters may be economically justified for the critical systems, although it is an expensive solution that requires continuous maintenance.

4.2 Firewalls

The firewalls are integrated security measures to prevent unauthorized access to the certain resources within the network. They work according to the set of rules and some other criteria. Their main tasks of the router are:

- Filtering the network traffic
- Posing as a gateway to the selected services
- Proxy server

Many modern firewalls cannot be used as a mean of DoS prevention. It may be extremely difficult or impossible to provide the rules for filtering the network traffic, as the firewalls cannot distinguish between the legitimate or illegitimate packets. Besides, the attacks may be performed before the control takes place – for example on the routers. A successful DoS attack on a router will switch off the service effectively. Better firewalls have a Defender mechanism implemented that checks the TCP connection validity before allowing the request to pass. It may be also possible to set the connection parameters to the certain limits. If the limits are exceeded the connection may be dropped or the firewall may go into the emergency mode. There is another side of those prevention systems – they may significantly reduce the effectiveness of the system. A firewall may also effectively part the intranet and internet thus saving the internal communication during an attack.

4.3 Intrusion Detection and Intrusion Prevention System

The intrusion detection system (IDS) or intrusion prevention system (IPS) is "a device that monitors the network and the different system activities for malicious or unwanted behavior/activity and, in case of an IPS, can react, in real-time, to block or prevent those activities".[8] They should not be mistaken with the firewalls as such. Such devices exist in a network invisibly (they are not part of the network and cannot be seen by other devices) and their role is to detect unwanted behavior, not to filter the packets. There are many types of IPS and IDS:

- Network-based IPS (NIPS)
- Host-based IPS (HIPS)
- Content-based IPS (CBIPS)
- Rate-based IPS (RIPS)

From the perspective of preventing the DoS attacks, the most needed mechanism in IPS is the rate-based IPS. RIPS monitors and learns the typical traffic in the network and behaviors. For the certain protocols (like TCP, UDP, ARP), the IPS can identify the abnormalities in the behavior of the network [9] (a significant difference in a number of connections per second, packets per connection, packets to specific ports for example). The thresholds are configured and dynamically adjusted (since the system may not expect too much connection during the night for example). When they are exceeded, the set of mechanisms is put to work. Those mechanisms may be of a varying type: the change is logged, an alarm is set, the connection is limited, source is tracked, ports and protocols are filtered. IPS not only stops the attack before the service may become unavailable or permanently shut down but also logs certain information like the IP address sources. It may also work as a deter system – to discourage the attackers. Some IPSs are implemented as an IDS working together with a firewall. Such solution may be referred to as a layered security and is a good implementation of a defense mechanism.

4.4 Operational Systems [8]

Since some types of the denial of service attacks make use of the exploits in the operating systems it is important to:

- Keep the system updated – all patches should be installed; subscribing to automatic producer notification may prove useful
- Windows systems: use desktop firewall, disable scripting on browsers and e-mail clients, use antivirus program that is updated and recommended by specialists
- Unix systems: Limit accessibility with network access control tools e.g. TCP Wrappers, use file system integrity check, use programs to test common DoS attacks, for example Remote Intrusion Detection
- Implement the security policies and ensure that they are followed when the desktops are used by the personnel

Those means of defense are preventing workstation from becoming zombie computers rather than protecting against the DoS attacks. If, however, everyone followed those rules, the DoS attack may become a costly and difficult strategy to overpower the systems.

4.5 Infrastructure and network configuration [7]

The attacks should be detected and prevented on the network periphery. There are certain attacks that can be conducted on the network devices. Their configurations have to be managed to make them secure.

4.5.1 Routers

Routers can have the basic rate limiting and access control list (ACL) capabilities. Some routers producers added the mechanisms that should block flooding attacks. But still it is relatively easy to take down the router.

4.5.2 Switches

Most switches have the rate-limiting and ACL capabilities just like the routers. Some mechanisms that may be useful include: automatic and system-wide rate limiting, deep packet inspection, traffic shaping, delayed binding (TCP splicing) and bogus IP filtering. Some consideration is needed – those mechanisms may sometimes block the legitimate traffic and slow down the network.

4.6 Audits

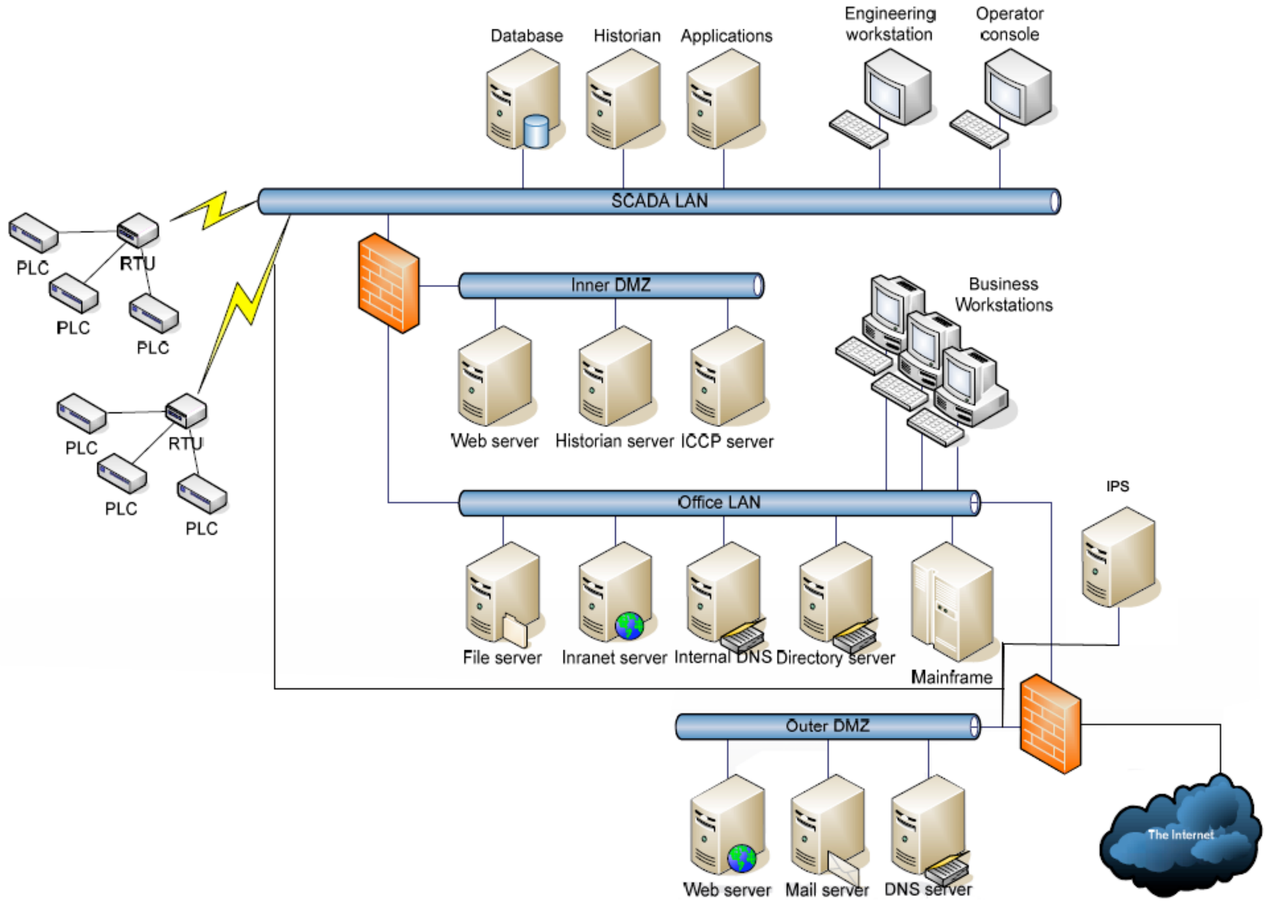
Even the best tools and methods for prevention of DoS attacks will be useless, if their configuration is not evaluated to find the possible weak points. An audit is an evaluation of the system done by the external experts. Their knowledge and tools for the fake attacks may reveal a wrong configuration, the weaknesses in the network and the level of security that is implemented.

4.7 People awareness

Most of the successful and world-known attacks were launched as a DDoS attacks. It is clear that awareness shared by computer users may make the attacks more difficult to conduct. Having an updated operational system, updated antivirus program as well as a basic firewall make most of the home computers secure when it comes to DDoS attacks.

5 Example network and proposed means of defense against attacks

The following drawing (source: TDDD17 lectures) depicts how the network for a small company could be protected against the denial of service attack. The firewalls are installed and configured properly, an IPS placed at the entrances to LAN network monitors the traffic changes and can report any unusual activity but also react by cutting off the intruder, all the computers are equipped with the firewalls and antivirus programs. The Operational Systems are up to date, all the patches are regularly installed at place.



Drawing 1: An example network

6 Case Study: experimental DoS attack on the server [11]

We prepared and conducted various DoS attacks on the services available on the public server.
A target machine is owned by the authors of this report.

6.1 Target

A target of the attack is a server named Tapczan, it is a multi-service machine connected to a small LAN network. This machine is running under Ubuntu Linux 7.10 operating system.

There are following services available on the server:

- A file storage (Samba server)
- A WWW server (Apache server)
- A database server (MySQL, PostgreSQL)
- A FTP server (VsFTPd)

The Server is connected to the network through a LinkSys router. All services are available through the internet, all corresponding ports are open.

6.2 Attack Description

Attacks were carried out in the three ways:

- Using the hosts connected to the same LAN network
- Through the internet/using the computers not connected to the LAN network.
- Using the direct SSH connection with a low-privileged user.

6.2.1 ICMP FLOOD

First attack was performed using the HPING program to flood the server with the ICMP echo requests packets. This attack was carried out in the two ways: using the hosts connected to the LAN network and using the University computers which are not connected to the same LAN network.

6.2.2 FORK BOMB

This attack was performed using the direct SSH connection by an authorized, low-privileged user. The aim of the attack attempt is to determine if the user with the basic privileges is able to crash the server. The attack was carried out using the various code snippets available on the internet.

6.3 Attack

Two types of attacks were carried out: an ICMP flood and a fork bomb.

6.3.1 ICMP FLOOD[1]

This attack was performed using various combinations of Hping and Hping2 shell command programs[3].

```
hping2 –a tapczan_IP –i u10 –S dummy_IP
```

The attack was firstly carried out from the internet. We used two university computers. The amount of the ICMP packets that could be sent from the two internet hosts was too small to effectively flood the server. This attack passed unnoticed to the server.

After the first failed attempt we tried the same thing from within the LAN network, where the destination machine was very close to the attacker host. It turned out that just one machine in the LAN network can effectively flood the server. The responses from the HTTP server were 10 times slower during the attack. Most of the connection requests to a FTP server timed-out before the connection could be established. Transferring the files through a Samba server was extremely slow and failed in most cases.

6.3.2 FORK BOMB

This attack was carried out using a simple 13 characters long bash shell script:

```
:(){ :|:& };:
```

After pasting this snippet of code into a terminal server has frozen. All process slots were occupied by the child processes of a fork bomb.

It was not possible to create another process, nor enter any command into a terminal. The only cure was to reboot the machine.

A similar effect was produced using this snippet of a C code:

```
int main()
{
  while(1) fork();
  return 0;
}
```

6.4 Defense

6.4.1 ICMP FLOOD[2]

There is a number of possible defense strategies against the ICMP flood. We choose the one that seemed to be simplest and most effective. Our LinkSys router allows configuring Internet Access Policy; it is possible to configure a router in such a way that all the ICMP packets addressed to the server will be dropped. After setting up this configuration, all attempts to flood the server with the ICMP packets failed.

6.4.2 FORK BOMB

The defense against this type of attack usually comes down to limiting the number of processes that one user can own. When the bomb tries to start another process and the user already owns a maximum number of processes, creation fails.

The Ubuntu-Server in default comes with the ulimit program. The Ulimit allows an administrator to limit many server parameters. To limit amount of processes of a user one may add:

```
* hard nproc 150
```

to the /etc/security/limitc.conf file. With this configuration every user of the system can own only 150 processes at the time.

Starting the fork bomb fails with: “fork: Resources temporary unavailable” error.

6.5 Results

Two different types of the attacks against the Linux server were carried out, both succeeded.

We have analyzed the reasons standing behind this success and found the effective solutions.

One problem was solved by reconfiguration of the server’s operating system, the other one by setting up a more restrictive network access policy. The ideas behind those solutions were taken from the theoretical. The proposed means of solving the problem of a DoS attack are thought to be enough to make the non-critical systems secure however they do not provide enough security for the critical systems. The most important part about this experiment is to show how easy an attacker can take advantage of an exposed weakness in the networked systems using the available on the internet tools.

7 Conclusion

There are several ways in which the network resources can be protected from the DoS attack but most of them were not implemented as a direct solution to them. A good monitoring process, correct configuration on routers, employees/users awareness and ways to replicate the resources are the key success factors to make the network resources as resistant to those attacks as possible. It is not possible to eliminate the risk completely.

References

[1] Internet Denial of Service: Attack and Defense Mechanisms, Jelena Mirkovic, Sven Dietrich, David Dittrich and Peter Reiher. Prentice Hall PTR

[2] The Tao of Network Security Monitoring, by Richard Bejtlich, Addison-Wesley, July, 2004

[3] Denial of Service Tools http://packetstormsecurity.org/distributed/

[4] Distributed-Systems Intruder Tools Workshop http://www.cert.org/reports/dsit_workshop.pdf

[5] Hack Attacks Denied, 2002, John Chirillo

[6] http://en.wikipedia.org/wiki/Denial-of-service_attack#Incidents

[7] The CEH prep guide : the comprehensive guide to certified ethical hacking, 2008, Ronald L. Krutz, Russell Dean Vines

[8] Denial of service attacks http://en.wikipedia.org/wiki/Denial_of_service_attack

[9] A large scale attack http://news.zdnet.com/2100-1009_22-145225.html

[10] A DoS attack http://indjst.org/archive/vol.2.issue.2/feb09madani.pdf

[11] Description of the tools that can be used when performing a DoS attack *http://documents.iss.net/whitepapers/ddos.pdf*