Punished for Others SYNs

Research Assignment, TCP/IP Network Fall 2016

1 Prologue

October 22, 2015
Team Zero, Google Zurich

Congratulations on being the latest member of the Google family and welcome to Project Zero. We at Google, deliver solutions that affect the experiences of millions of users, everyday. The Project Zero team aims to improve the security of the Internet and reduce targeted attacks by conducting leading network security research.

2 The Case of X

An evaluation of one of our divisions, "X" has shown that, during a period of two hours on every Tuesday and Friday in the past month, not a single user was able to start using Xs service. Users who were already using the server did not complain of any problems.

A preliminary analysis by Alice has shown that the network is adequately provisioned and the bottleneck is at Xs webserver. Alice has also verified the configuration of the webserver to establish that our usual network security best practices such as encryption, authentication and firewall settings were already in place. On doing a wireshark trace, Alice found the following peculiar behavior:

"... from 4pm-6pm on every Tuesday and 11am -1pm on every Friday, I noticed a ***flood of TCP-SYN*** *messages with a wide-range of different source-IP address targeted towards the port 80 of Xs webserver. Incidentally, it is during these periods of time, that Xs service was reported unavailable ..."*

3 SYN flood attacks and SYN cookies

SYN flood attacks [1] are denial of service (DoS) attacks wherein a large number of SYN packets are sent to a specific port of TCP server by an attacker, thereby leaving the server with not enough resources to serve other clients.

To understand how the attack works, it is important to understand what are the different states of the server and client in a TCP session, and how these states evolve with time.

There are several techniques of mitigation of SYN flood attacks [2]. The focus of this exercise will be on one of these techniques called SYN cookies [3, 4].

4 Your Task

Your task in this research exercise is to:

1. Perform a survey of how SYN flood attacks work and how are they mitigated

2. Demonstrate a SYN flood attack and mitigation using SYN cookies in GNS3

4.1 Survey

Your survey should describe: 1) what is the problem with SYN floods and 2) how does the SYN cookies solution address this problem. Specifically, your survey should address the following non-exhaustive list of details:

Problem

1. What are the different states of a TCP client and a server during the lifetime of a TCP session?
2. How do SYN floods affect the TCP state machine at the server?
3. How do SYN flood attacks result in a DoS attack?

Solution

1. What is the central idea behind SYN cookies?
2. How do SYN cookies mitigate SYN flood attacks?
3. How do the SYN cookies solution compare with other solutions?

4.2 Demonstration in GNS3

For the demo, you should set up a network in GNS3 with a webserver, a client and an attacker. To establish a simple webserver, you may use node.js [5]. To perform a SYN flood attack, you can use hping3 [6], a network security tool that is pre-installed on the attackers image.

SYN cookies are a part of Linux kernel since version 2.6.26 and you will be able to turn them on or off using the command line. You should demonstrate the effect of the attack on existing and new TCP connections between the server and the client, when SYN cookies are enabled and disabled. You will show it on the day of your defense.

In your report, you should clearly describe your setup and the various configuration details required to realize the attack. You should also comment on:

1. When SYN cookies are disabled, for how long is the effect of the attack perceived after the flooding has stopped?
2. When SYN cookies are enabled, how long before the effect of the attack vanishes?
3. number of TCP connection on the server before the flood, during the flood and long after the flood, when SYN cookies are used and not used. (Use netstat -tn [7])
4. Do you notice any change in the servers CPU and memory usage when SYN cookies are used as opposed to when they are not used?

Feel free to write about any more interesting observations that you see.

4.3 Optional

Do not work on this before completing the compulsory tasks!

Your manager was very happy with your work. Thanks to you, our division X now has uninterrupted service on all days of the week. However, it has come to her knowledge that when SYN cookies were enabled, some of the users were experiencing degraded performance, largely characterized by a high-latency in the service. Could you comment on what might be the problem and propose a possible solution?

5 Research Assignment organization

- You can work alone or in groups of two.
- You should upload your report on Moodle before **Wednesday, November 11, 23:59**. It should be maximum 6 pages long in double-column format. Please use the templates provided on Moodle (LaTeX or Word) for the reports. Submissions within 24h after the deadline will be penalized (-20% of the grade). After that, no submissions will be possible.
- On **November 19 2015**, there will be an optional quiz on this topic which will add to the theory grade.
- On **December 3, 2015** we will announce grades and the two winning teams. Winning teams will have a chance to present their solution during the class on **Friday, December 18, 2015**. For this step they will receive guidance from Professor Le Boudec.

Contact:

Maaz Mohiuddin maaz.mohiuddin@epfl.ch

References

[1] *SYN flood*. October 2015, `https://en.wikipedia.org/wiki/SYN_flood`.

[2] W. Eddy *TCP SYN Flooding Attacks and Common Mitigations*. August 2007, `https://tools.ietf.org/html/rfc4987`.

[3] D. J. Bernstein *SYN Cookies*. `http://cr.yp.to/syncookies.html`.

[4] W. Eddy *Defenses Against TCP SYN Flooding Attacks*. December 2006, `http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-4/syn_flooding_attacks.html`.

[5] *node.js*. October 2015, `https://nodejs.org/en/`.

[6] *hping3*. October 2015, `http://linux.die.net/man/8/hping3`.

[7] *Netstat*. October 2015, `http://linux.die.net/man/8/netstat`.