IT Security
Written Assignment

DIKU, May 20 2015

This is the written assignment for the 2015 edition of the IT Security course at DIKU. The topic for the assignment is denial of service attacks.

General requirements

- The asignment is available on Absalon on May 20 2015 at 09:00. Solutions must be submitted in PDF format via Absalon on May 29 2015 at 23:59 at the latest.
- Your solution must be documented in a short and precise report no more than 5 pages in length, discounting title page, contents page, pictures, list of references, appendix, etc. Your report should follow the usual structure for scientific reports, starting with a summary followed by a description of the problem and the solution and finishing with a conclusion and a list of references.
- If you are in doubt about the interpretation of some of the requirements, or feel it necessary to make some assumptions, you should explain what you did and why. Be sure to clearly mark work included in your solution that is not your own personal work and make a reference to its source.
- Make clear assumptions of your intended reader and introduce concepts that he/she is assumed unfamiliar with before you use them.
- You may collaborate when solving the assignment, however when writing up the solutions you must do so on your own work and hand in your own report.

- Reports are graded as 'passed' or 'not passed' on June 03 2015 at the latest. You have to pass your report to be able to sit in for the exam. Limited individual written feedback is given via Absalon. Instructors will discuss common key points from the assignment during exercises on June 03.
- Resubmission is allowed if you do not pass your first report and it reflects a serious and whole-hearted effort. Deadlines and requirements for resubmissions will be negotiated individually.
- You may write in English or Danish. If you wish to write in another language, please let us know.

Analysis and discussion of denial of service attacks

This assignment deals with denial of service attacks.

Attack on GitHub

On March 26 2015 open-source code repository Github became the victim of a large and sustained denial of service attack[1]. We would like you to research online material describing the attack and give a short description of the attack, what type of attack, how it was carried out, by whom, to what gain, etc.

On April 30 2015 a group of individuals was convicted of denial of service attacks carried out on the organisations 3F, HK, LO and others in June 2012[2]. Compare the attack on GitHub with the attacks on these organisations in terms of motivations and type of threat actor group carrying out the attacks.

A special type of denial of service attack is the SYN Flood attack. Compare the attack on GitHub with SYN Flood attacks in terms of technical detail, i.e. what commonalities and differences exist in how the attack on GitHub was carried out and how SYN Floods work.

Hands-on with SYN Floods

On Absalon you are given a packet capture of a SYN Flood attack. Analyse it using e.g. Wireshark or `tcpdump` and explain how you can tell the packet capture contains a recording of a SYN Flood attack.

[1] https://status.github.com/messages/2015-03-26

[2] http://www.dr.dk/Nyheder/Indland/2015/04/30/152616.htm

Try to carry out your own SYN Flood attack as described below. We assume you're using a Linux system, but you can carry out the attack on other platforms as well.

SYN Floods flood the victims queue that is used for half-open TCP connections. The state of such connections is `SYN-RECV`. When the queue is full, the victim cannot take any more connections. We would like you:

- Check the system-wide setting for the size of the queue with `sysctl -q net.ipv4.tcp_max_syn_backlog`.
- Set up a listening service on your localhost, e.g. using `nc -l localhost 4444`, `php -S 127.0.0.1:8080 -t /tmp` or similar.
- Use `hping3`, `netwox` or a similar tool to conduct a SYN Flood attack against the listener.
- Record your attack using e.g. Wireshark or `tcpdump`.
- If your attack seems unsuccessful, it may be due to SYN cookies:

  ```
  sysctl -a | grep cookie #displays SYN cookie flag
  sudo sysctl -w net.ipv4.tcp_syncookies=0 #SYN cookies off
  sudo sysctl -w net.ipv4.tcp_syncookies=1 #SYN cookies on
  ```

- While the attack is ongoing, use `netstat` to check usage of the queue.

Describe your observations carrying out the attack. Is your attack successful or not? How can you tell? Run your attacks with the SYN cookie mechanism on and off, and compare the results. Explain why the SYN cookie can or cannot effectively protect your machine against the SYN Flood.