

Network Security

Assignment 5, Friday, October 3, 2014, version 1.0

Handing in your answers: Submission via Blackboard (<http://blackboard.ru.nl>)

Deadline: Friday, October 10, 23:59:59 (midnight)

This assignment consists of some theoretical questions and a practical exercise. Please turn in all your work in plain text files (program source files are also plain text). If you prefer a document with formatting for whatever reason, like including images, use the PDF format to turn in your work (most editors allow you to export to PDF). Note that it's okay to include images separately and then refer to them from within the text files.

Commands that need to be run with root rights are denoted by a prefix `#`. When a command should be run without root rights, it will be prefixed with `$`. Do not include the prefix when typing the command.

1. This exercise is about DDOS attacks using DNS amplification. Create a folder `exercise1` to contain the files with your answers.
 - (a) Using any tool, script or program you want, figure out the DNS query that gives you the largest DNS amplification. E.g. a query that's 100 bytes and generates a response of 1000 bytes gives you an amplification factor of 10. You are not allowed to use DNS servers under your own control for this, but apart from that you are free to pick any server and any query you want. To make sure that we can verify your answer, make a packet capture of the outgoing query and the incoming response. Members of the group with the largest amplification will get a prize: a copy of "Ghost in the Wires: My Adventures as the World's Most Wanted Hacker" by Kevin Mitnick. In the case of a tie, the first submission in Blackboard wins. Don't spend all your time doing this, however. Find a reasonable query, then do the other exercises before coming back to improve on this answer.
Write your answer, preferably as a `dig` query, to `exercise1a`. Also store the packet capture as `exercise1a.cap`. If you programmed something for this, include the source code.
 - (b) Now imagine that you are in a LAN with a gateway router. Explain how you would use this DNS query to take down a server which has been annoying you for a while, e.g. `blackboard.ru.nl`. Describe the packet you need to craft, and its relevant features, at DNS level, UDP level, IP level and ethernet level. Do not actually perform the attack. Write your answer to `exercise1b`.
 - (c) Suppose you are the administrator of this network. You want to make sure that, from the LAN, nobody can use this kind of DNS amplification attack. The LAN network is `203.0.113.0/24`, the gateway's internal IP address is `203.0.113.1`, and its external IP address is `198.51.100.78`.
What firewall measures (iptables rules) would be effective in preventing this kind of attack *without* impeding normal operation of the network? Describe these measures in detail, and also try to come up with actual iptables rules for them. Write your answer to `exercise1c`.

2. Create a folder called `exercise2`.

Assume you're an attacker who wants to trick a DNS cache into believing your server is actually hosting `blackboard.ru.nl`. You try to race a legitimate DNS server to provide the answer faster.

- (a) How would you ensure that you can predict the queries that the cache is going to produce? Describe the setup and/or process. Write your answer to `exercise2a`.
- (b) QID randomization and port randomization are (somewhat) effective countermeasures against cache poisoning. What are the odds that you guess right if the DNS cache is using QID randomization in its queries? Assuming your response always arrives first, how many queries do you need the cache to make on average to have a 90% chance of successfully poisoning the cache?

What are the odds and how many queries do you need if the cache is also using source port randomization?

Write your answers to **exercise2b**.

- (c) Imagine that on top of that, these DNS servers also deploy 0x20 randomization (see slides, the random capital letters in the query). What are the odds now that you will guess right on a query for the blackboard.ru.nl host? Write your answer to **exercise2c**.
 - (d) Explain, in your own words, why all these countermeasures do not work against the easy DNS attack, i.e. against a passive MitM attacker. Write your answer to **exercise2d**.
3. The firewall configuration you made in assignment 4, exercise 1a, should still allow DNS conversations. However, DNS usually runs over UDP and UDP is a connectionless protocol. Try to explain how the firewall still knows that it should allow this DNS traffic. Write your answer to **exercise3**.
4. Place the files and directories **exercise1**, **exercise2**, and **exercise3** and all their contents in a folder called **netsec-assignment5-STUDENTNUMBER1-STUDENTNUMBER2**. Replace **STUDENTNUMBER1** and **STUDENTNUMBER2** by your respective student numbers, and accomodate for extra / fewer student numbers. Make a **tar.gz** archive of the whole **netsec-assignment5-STUDENTNUMBER1-STUDENTNUMBER2** directory and submit this archive in Blackboard.