Network Security

Optional assignment DNS, Friday, May 24, 2019, version 1.0

Handing in your answers: Submission via Brightspace (`https://brightspace.ru.nl`)

Deadline: Friday, May 31, 23:59:59 (midnight)

Teaching assistants. Please email *all* of us if you have a question.

- Daan Sprenkels `<d.sprenkels@cs.ru.nl>`
- Alireza Vahdad `<alireza.vahdad@gmail.com>`
- Jos Craaijo `<jos635@outlook.com>`

This assignement is *optional*, i.e. you don't have to do it[1]! Please prioritize the mandatory assignments over this one.

In this assignment you will be using dig, or a similar DNS query tool:
`http://www.isc.org/downloads/bind/`
Again, do not compile this program from source, but install it using your distribution's package manager.

This assignment contains only the practical exercise of crafting a DNS query with a large DNS amplification.

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. *Optional.* 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 *UDP*[2] 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 Brightspace 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` or `drill` 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 *non-NATing* 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`.

[1] Except if you want to win the book.

[2] Since TCP is useless for amplification attacks. Switching the entire DNS infrastructure over to TCP would effectively stop the issue of DNS DDoS, but introduces other issues in turn.

2. Place the files and directories `exercise1` and all their contents in a folder called `netsec-assignment_dns-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-assignment_dns-STUDENTNUMBER1-STUDENTNUMBER2` directory and submit this archive in Brightspace.