Review of Bachelor's Thesis

Student: Ortiz Caceres Rafael
Title: Detecting DNS Tunneling (id 18265)
Reviewer: Lichtner Ondrej, Ing., UIFS FIT VUT

1. Assignment complexity — **less demanding assignment**

The difficulty of this thesis is closely related to the chosen experiments and methods of detecting DNS tunneling. I imagine that developing and deploying a complex solution for detecting DNS tunneling in a larger network would be quite difficult. The student however chose a much simpler variant of deploying a DNS tunnel and monitoring traffic just on tunnel end points. Because of this I rate the assignment as "easier than average".

2. Completeness of assignment requirements — **assignment fulfilled only partially**

The first part of the thesis that builds the theoretical background on the topic of creating tunnels over DNS is acceptable. However the second part that's focused on deploying security methods detecting DNS tunneling lacks any sort of formal approach. It can be better described as listing of possible indicators of traffic being tunneled over DNS. The author does confirm that these indicators can be seen when manually analyzing network traffic with Wireshark or similar tools. However, manual analysis is only possible on a very small network and drawing conclusions in larger scenarios would require a more formal approach than manually looking for indicators such as "hard to read domain names" or "high frequency of DNS requests".

As far as I understand the student did not actually deploy any security measures that would detect tunnel traffic, he only visually confirmed atypical DNS traffic using Wireshark. This cannot be considered as deployment of security measures since it would be impossible to use in any network other than an experimental one.

3. Length of technical report — **in usual extent**

Length of the reviewed thesis is in normal range. It contains a large amount of screenshots that lower the overall information density, for example Figure 3.2 depicting an instalation window.

4. Presentation level of technical report — **60 p. (D)**

The text of the thesis has a logical flow that follows the individual tasks of the assignment. The structure of the thesis could be improved, for example the Introduction chapter is 18 pages long and corresponds to everything from the first task of the assignment instead of logically separating it into multiple chapters. Another example is chapter "Experiments" where the actual experiments are described in section "How to install Iodine".

5. Formal aspects of technical report — **50 p. (E)**

I didn't find any significant problems with the typography of the thesis. Language quality of the text is bad. The Introduction chapter contains only minor errors, after the second chapter the quality of the text drops significantly. Some parts are barely understandable and need several read-throughs. Most of the text is written in an informal manner that is unsuitable for a thesis.

6. Literature usage — **0 p. (F)**

The student uses mostly internet resources that are relevant to the topic, some resources are in Spanish so I can't comment on them (including Spanish wikipedia). The number of sources is smaller than expected, especially since the listed sources are referenced only in the first chapter. Chapter "Security measures" and "Detecting DNS tunneling" which should be the core of the thesis contain no references in text and only two sources listed in literature are relevant to this topic.

At least sections 1.8 (part describing encodings) and 1.10 are directly copied from SANS Institute InfoSec Reading Room, "Detecting DNS Tunneling" whitepaper that is listed in the References section, but is not cited in related parts of the text. On the other hand, the author also copied the references from original paper and didn't list them in the References section of the thesis.

7. Implementation results — **40 p. (F)**

The assignment didn't require creation of any application. The main part of the technical part of the thesis was experimentation and deployment of security measures capable of detecting traffic tunneled over DNS.

Experiments were performed using the Iodine application, creating a tunnel between two machines. As far as I understand detection of tunneled traffic was done only manually as an administrator watching network traffic with a tool such as Wireshark. This cannot be considered as "deployment of security methods" since such an approach would be highly ineffective, if not impossible, to use in a real network scenario. Performed experiments

involved only tunnel endpoints and were too small to make any conclusions regarding the success rate of detection of DNS tunneled traffic.

8. Utilizability of results

The thesis is mostly a compilation of several internet tutorials and blog posts regarding creation of tunnels over DNS. The performed experiments are too small to be in any way useful. I don't see any added value of this thesis.

9. Questions for defence

1. With regards to task 4 of the assignment, how did you "deploy security methods that can detect DNS tunneling."?

10. Total assessment **40 p. failed (F)**

The student experimented with very simple scenarios of deploying a DNS tunnel in a small network and analysing trafic on tunnel end points. To my understanding he failed in completing the 4th task of the assignment which I consider as the most important part of the thesis. The overall quality of the text is very bad. Finally I found at least two sections that are partially copied from a whitepaper without a reference (even though it is listed in references at the end of the thesis).

Because of these reasons I rate this thesis with F.

In Brno 6. June 2016

.....
signature