DNS Tunneling

Terje Kristoffer H. Skow
terjeks@stud.ntnu.no
TTM4137 Wireless Security Technical Essay

November 11, 2015

1 Introduction

Domain Name System (DNS) is one of the backbone systems of the internet. It is a protocol that is used to lookup a domain name's IP-address, which the network needs to route http traffic. In later years it has been discovered that it has weaknesses that is easy to exploit. The exploit which is going to be looked at in essay is DNS tunneling. DNS tunneling started with people who wanted internet access at hotels and cafs without paying for it. It is now used in "Command and Control" attack where the commands can be sendt encrypted over DNS masked as a regular response, and to transfer data undetected out of a secure network. With the use of smartphones using the internet it is discovered that using DNS tunneling an user could avoid getting charged for the internet use. This essay will first explain some basics of how DNS work and the important elements that is exploited and the use of DNS tunneling, specifically the use on mobile networks.

2 Problem Discussion

2.1 DNS

There are many different record types in the DNS, most commonly is `'A'` and `'AAAA'` records which contains the ipv4 and the ipv6 addresses respectively. You also have a `'CNAME'` record which translate a domain name into another which is associated with an IP-address, e.g. if you enter `www.aftenposten.no` in the browser to visit the website of Aftenposten, the first response of the DNS server is a CNAME which refers you to the domain `aftenposten.no`. The network then send a new request to the DNS with aftenposten.no and receives an 'A' record with the IP-address. Now DNS has over 30 different record types, each has a different purpose and different size of payloads which is an important feature when it comes to DNS tunneling.

DNS has a hierarchical build. Each server sends the request to the next server with more specific information about the domain name you want to reach, going in a postfix order.

2.2 DNS Tunneling

2.3 Requirements of Form

We set the following requirements with respect to format:

1. This LaTeX template must be used.

Figure 1: A "wrapped" figure with the text.

2. The whole document must be limited to 3 A4 pages of text (references not included). A technical essay different from three -3- pages of text will be returned to the author to be cut or enhanced to three pages.

3. One or more illustrations in the form of figures, tables or diagrams must be included (see Figure 1).

4. The entries in your reference should be structured as follows: Author/Origin. *Title.* Where, and when published.

5. The submitted file format must be pdf.

Structure If you want further substructure than sections and subsections, then you can use a paragraph title like here. This will look much better than introducing another numbered level of subsubsection.

2.4 Requirements of Content

The text should be intelligible, logical, interesting and easy to read. Write for your fellow engineering students, and assume that the reader has the same general theoretical background as yourself. Use definitions, facts and logical argumentation.

Interpret and refine the title, discuss the problem and intended scope in the introduction. In the text, do not introduce facts that are not analysed later and that are not relevant to your problem. Bring your *own analysis and thinking* into the essay. If you can, bring in new ideas. When you include tables or figures (see Figure 2), they should be referred to and explained in the text.

While it is allowed to cite Wikipedia or another web page [**?**, **?**], it is not recommended. It is much better if you can refer to a technical article or paper [**?**].

3 Conclusion

The submitted technical essays will be graded and contribute 20% to the final grade of the course. The three best essays will be honoured with publication on ItsLearning, edited if necessary, and become part of this year's syllabus.

(a) Scale=0.20 (b) Scale=0.15 (c) Scale=0.10

Figure 2: The Linksys WRT54G line of routers include both 802.3 Ethernet and 802.11b/g wireless LAN.