

IMPLEMENTATION AND INVESTIGATION OF DNS VULNERABILITIES AND EXPLOITS

Mircea-Radu-Serban Dobrau

University of Wales Trinity Saint David
serb348@gmail.com



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Introduction

The IoT concept is slowly becoming a reality, with tens of billions of connected devices and increasing [1, p. v], as well as 26 billion expected by 2020 [2, p. 114] and 7 billion devices connected over cellular networks expected by 2025. [3, p. 35] As a result, cybersecurity poses a much greater risk. [4, p. 156] [5, p. 153]

DNS attacks in particular are increasingly prevalent, reaching a very large number of organisations in the past years. [6, p. 1] [7, p. 17] Furthermore, it may also target end-user devices due to most users being unfamiliar with DNS and DNS settings. [8, p. 2] Finally, the large DDoS attack on the Dyn DNS service provider [9, p. 5] proved to be fatal to hundreds of services such as Netflix and Twitter, making use of up to 100,000 devices.

As such, it can be asserted that DNS is a vital component of the Internet's infrastructure. This project will detail the investigation and implementation of DNS vulnerabilities and/or exploits.

Aim and Objectives

The aim of this project is to investigate and implement various DNS vulnerabilities and/or exploits. Its objectives are to:

- Research DNS design, operation, and vulnerabilities
- Design a live-network simulation and implement vulnerabilities in the simulated environment
- Evaluate results

Literature review

DNS can be both understood as a hierarchical, redundant and distributed database [10, p. 1] and as an application protocol used for exchanging domain name information between DNS servers and clients. It helps users abstract from a host's IP address by binding it to a host-name and/or domain-name. [11, p. 1]

There exist various types of DNS exploits, such as:

- DNS poisoning
- Domain typosquatting
- Name server typosquatting
- Name server bitsquatting
- DNS spoofing
- Zone poisoning
- DNS domain hi-jacking
- and others

Methodology: Design and Experiment

The methodology is to implement exploits using ready-made programs and/or code, with the help of VM software for simulating a real network, DNS server/client software, penetration testing distributions and/or other independently acquired tools/exploits.

Additionally, an originally-written implementation of an exploit and/or a wrapper for multiple exploit implementations is to be implemented.

Outcomes and deliverables

A thoroughly written research of DNS vulnerabilities is to be provided.

Furthermore, one or some of the following is to be achieved:

- Originally hand-written implementation of exploit
- Wrapper for multiple already-existing code implementations

References

- [1] S. Ziegler, Internet of Things Security and Data Protection, ser. Internet of things. Springer Nature, 2019.
- [2] S. S. Ammar Rayes, Internet of Things From Hype to Reality: The Road to Digitization, 2nd ed. Springer International Publishing, 2019.
- [3] A. A. Waleed Ejaz, Internet of Things for Smart Cities: Technologies, Big Data and Security, 1st ed., ser. SpringerBriefs in Electrical and Computer Engineering. Springer International Publishing, 2019.
- [4] M. J. Carey, Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World. Threatcare Press, 2019.
- [5] J. Warfare, Journal of Law & Cyber Warfare Vol. 4:3 Winter 2015. Lulu.com, 2016.
- [6] "Sharp rise in costs and damage from dns-related attacks." Network Security, vol. 2018, no. 6, pp. 1-3, June 2018.
- [7] C. Marrison, "Understanding the threats to dns and how to secure it," Network Security, vol. 2015, no. 10, pp. 8-10, 2015.
- [8] D. Winder, "So what should you be doing to mitigate the iot botnet threat? start with a network audit," PC Pro, no. 288, pp. 118-120, 2018.
- [9] S. Mohan, M. Asplund, G. Bloom, A.-R. Sadeghi, A. Ibrahim, N. Salajageh, P. Griffioen, and B. Sinopoli, "The future of iot security: Special session," in Proceedings of the International Conference on Embedded Software, ser. EMSOFT '18. Piscataway, NJ, USA: IEEE Press, 2018, pp. 16:1-16:7.
- [10] A. Liska and G. Stowe, DNS Security: Defending the Domain Name System. Elsevier Science, 2016.
- [11] M. Jeftovic, Managing Mission - Critical Domains and DNS: Demystifying nameservers, DNS, and domain names. Packt Publishing, 2018.