Smayan Daruka
CSEC-380
Professor Chaim Sanders

Blog Topic Writeup

Introduction

DNSSEC was introduced to improve security of DNS by providing authentication, but it also introduced a major vulnerability that allows attackers to abuse NSEC records and enumerate domain names to map out a full website. The way this works is when a query for a non-existent domain comes in with DNSSEC enabled, the response contains NSEC records for the previous and after domain names when setup alphabetically. It is possible to mitigate this risk by correctly configuring the server.

Outline

For the blog post:

- Briefly describe DNS in general
- Describe DNSSEC (all of its individual records) and how it improves security by providing authentication
- Demonstrate the NSEC vulnerability to map out a domain
- Provide instructions on how to mitigate this issue

I am also going to try and develop a tool (script) that automates this attack.