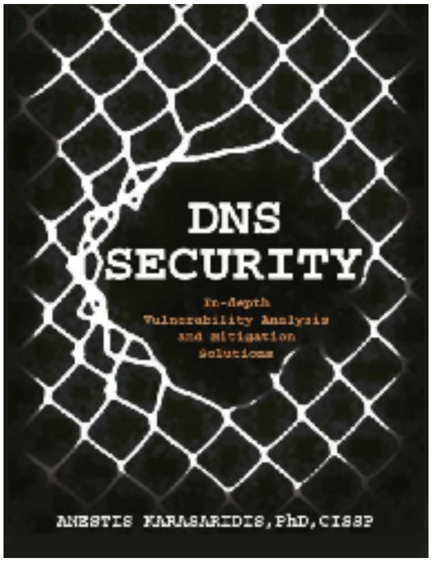

CNIT 40: DNS Security

Fall 2017 Sam Bowne

`77239 T 06:10-09:00PM MUB 388`

Catalog Description

DNS is crucial for all Internet transactions, but it is subject to numerous security risks, including phishing, hijacking, packet amplification, spoofing, snooping, poisoning, and more. Learn how to configure secure DNS servers, and to detect malicious activity with DNS monitoring. We will also cover DNSSEC principles and deployment. Students will perform hands-on projects deploying secure DNS servers on both Windows and Linux platforms.

Advisory: CNIT 106 or 201E, or Network+-level understanding of networking.

Upon successful completion of this course, the student will be able to:

A. **Describe the normal operation of DNS: Zones, servers, records, and protocol function**
B. **Explain common DNS attacks, including hijacking, snooping, poisoning, spoofing, fast flux, and packet amplification**
C. **Understand common defenses against each type of attack**
D. **Configure a secure BIND server on Linux**
E. **Configure a secure Windows DNS server**
F. **Prevent unwanted zone transfers**
G. **Design high-availability DNS infrastructure**
H. **Explain how to detect security breaches with DNS monitoring**
I. **Describe the function and operation of DNSSEC**
J. **Add a DNSSEC signatures to a zone**

Textbook

"DNS Security" by Anestis Karasaridis, Amazon Digital Services, Inc., ASIN: B007ZW50WE

Quizzes

The quizzes are multiple-choice, online, and open-book. However, you may not ask other people to help you during the quizzes. You will need to study the textbook chapter before the lecture covering it, and take the quiz before that class. Each quiz is available for one week, up till 8:30 am Saturday. Each quiz has 5 questions, you have ten minutes to take it, and you can make two attempts. If you take the quiz twice, the higher score counts.

To take quizzes, first claim your RAM ID and then log in to Canvas here: https://ccsf.instructure.com

Live Streaming

Live stream at: ccsf.edu/webcasts

Classes will also be recorded and published on YouTube for later viewing.

Schedule

Date	Due	Topic
Tue 8-22		1: The importance of DNS security
Tue 9-12	Proj 1 due Quizzes: Ch 1 & Ch 2 due before class	2: DNS protocol and architecture
Tue 10-3	Proj 2 & 3 due Quiz Ch 3 due before class	3: DNS vulnerabilities
Tue 10-24	Proj 4 & 5 due Quiz Ch 4 due before class	4: Monitoring and detecting security breaches
Tue 11-14	Proj 6 due Quiz Ch 5 due before class	5: Prevention, protection, and mitigation of DNS service disruption
Tue 12-5	Proj 7 due Quiz Ch 6 due before class	Last class: 6: DNSSEC and beyond
Tue 12-19		Final Exam (Optional)