CS 333: Network Security and Defense

Capture the Flag - DNS Response Spoofing

Author: Jidong Xiao

1 Introduction

This in-class contest is mainly used to engage students in class, and help students to understand how dns responses can be spoofed. Students will be divided into two teams, both team will act like the attackers.

2 Rules

- This game is based on "Local DNS Attack Lab task 5"; the goal is to generate fake responses to the victim's DNS queries. The instructor will act like the victim and generate the queries. Team 1's goal is to redirect the victime to https://www.bradlittleforidaho.com/ (Brad Little, Republican, ip address: 104.18.50.52); while Team 2's goal is to redirect the victim to https://www.jordanforgovernor.com/ (Paulette Jordan, Democrat, ip address: 104.25.15.19).
- Each row in team 1 will play against the corresponding row in team 2, e.g., Row 1 in team 1 will play against Row 1 in team 2.
- When the instructor generates the query, which team's response is displayed on his screen, the team get 10 points.
- The instructor will repeat this querying procedure 5 times, so row 1, row 2, row 3, row 4, row 5 will all get involved.
- No terminal should be open until the instrutor says "start".

3 Incentives

Five CTF games will be played during this semester, and this is the second one. All the CTF game points will be accumulated, eventually the team with more accumulated points will be the winning team. The winning team will earn the following "prize":

- 1. Students (in the winning team) who are supposed to get B+ will be raised to A-; A- will be raised to A.
- 2. Students (in the winning team) who are supposed to get anything below than C, will be raised to C.

Exception: The prize doesn't apply to students who misses 4 or more than 4 classes.

4 Preparation

- Every participant needs to ssh to onyxnode112; and telnet to a given VM. This VM will be the attacker's VM. The other VM running on onyxnode112 will be the victim VM. The ip address of both VMs will be given.
- The instructor will do a demo first. (A local DNS server needs to be running, the victim machine needs to be configured to use this DNS server as its local DNS resolver.)