CS 333: Network Security and Defense

Role-Playing Game - Remote DNS Attack

Author: Jidong Xiao

1 Introduction

This in-class game is mainly used to engage students in class, and help students to understand how the remote DNS attack works.

1.1 Sketch One

This sketch describes how normally a Kaminsky attack goes. Five roles are involved in this sketch. Attacker (A), Attacker's DNS server (AD), Victim DNS server (VD), Victim client (VC), An authoritative DNS server for some domain (D) (e.g., cnn.com). The script goes like this (no need to follow the lines word by word, they can use their own words, just make sure it's the same meaning.):

- Preparation: The instructor creates the NS record of cnn.com on the board.
- A to VD: Hey, VD, what's the ip address of twysw.cnn.com?
- VD looks at the board, and then turns to D: Hey, D, what's the ip address of twysw.cnn.com?
- D: Hey, VD, actually twysw.cnn.com is not existing.
- A to VD: Hey, VD, I'm D (ip spoofing), so you want to know the ip address of twysw.cnn.com (Query Section)? Well, the ip address of twysw.cnn.com is 1.1.1.1 (Answer Section); and btw, you should remember me, because I'm the authoritative name server for cnn.com, and my domain name is yellowstone.boisestate.edu (Authority Section), also my ip address is 132.178.227.10 (Additional Section).
- VD talks to himself/herself: This is ridiculous, I already have the response. I am gonna disregard this second response. (Attack failed because D responds very fast).
- A to VD: Hey, VD, what's the ip address of abcd.cnn.com?
- VD to D: Hey, D, what's the ip address of abcd.cnn.com?
- D: Keep silent - because this time he/she is too busy or is too far.
- A to VD: Hey, VD, I'm D (ip spoofing), so you want to know the ip address of abcd.cnn.com (Query Section)? Well, the ip address of abcd.cnn.com is 1.1.1.1 (Answer Section); and btw, you should remember me, because I'm the authoritative name server for cnn.com, and my domain name is yellowstone.boisestate.edu (Authority Section), also my ip address is 132.178.227.10 (Additional Section).
- VD writes down the A record for abcd.cnn.com, and also overwrites the existing NS record with the one he/she just received, plus an A record for yellowstone.boisestate.edu. (Cache poisoning attack succeeds)
- VC to VD: Hey, VD, what's the ip address of www.cnn.com?
- VD looks at the board, and realizes he/she should ask AD.
- VD to AD: Hey, AD, what's the ip address of www.cnn.com?
- AD to VD: Hey, VD, the ip address of www.cnn.com is 176.10.250.185.
- VD to VC: Hey, VC, the ip address of www.cnn.com is 176.10.250.185.
- VC uses the computer and types that ip address "176.10.250.185" in the browser.

End.

1.2 Sketch Two

This sketch describes how the Kaminsky attack goes in this classroom. Seven roles are involved in this sketch. Attacker (A), Attacker's DNS server (AD), Victim DNS server (VD), Victim client (VC), Two root DNS server (R1, R2, and R3). The script goes like this (no need to follow the lines word by word, they can use their own words, just make sure it's the same meaning.):

- Preparation: leave nothing on the board (empty cache).
- A to VD: Hey, VD, what's the ip address of twysw.maroon5.com?
- VD to R1: Hey, R1, what's the ip address of twysw.maroon5.com?
- VD to R2: Hey, R2, what's the ip address of twysw.maroon5.com?
- VD to R3: Hey, R3, what's the ip address of twysw.maroon5.com?
- R1, R2, R3: All keep silent - because the responses are somehow blocked in this classroom.
- A to VD: Hey, VD, I'm R1 (ip spoofing), so you want to know the ip address of twysw.maroon5.com (Query Section)? Well, the ip address of twysw.maroon5.com is 1.1.1.1 (Answer Section); and btw, you should remember me, because I'm the authoritative name server for maroon5.com, and my domain name is yellowstone.boisestate.edu (Authority Section), also, my ip address is 132.178.227.10 (Additional Section).
- VD writes down an A record for twysw.maroon5.com, and the NS record for maroon5.com.
- A to VD: Hey, VD, what's the ip address of yellowstone.boisestate.edu?
- VD to R1: Hey, R1, what's the ip address of yellowstone.boisestate.edu?
- VD to R2: Hey, R2, what's the ip address of yellowstone.boisestate.edu?
- VD to R3: Hey, R3, what's the ip address of yellowstone.boisestate.edu?
- A to VD: Hey, VD, I'm R1 (ip spoofing), so you want to know the ip address of yellowstone.boisestate.edu (Query Section)? Well, the ip address of yellowstone.boisestate.edu is 132.178.227.10 (Answer Section). (Authority Section and Additional Section are optional)
- VD writes down an A record of yellowstone.boisestate.edu.
- VC to VD: Hey, VD, what's the ip address of www.maroon5.com?
- VD looks at the board, and realizes he/she should ask AD.
- VD to AD: Hey, AD, what's the ip address of www.maroon5.com?
- AD to VD: Hey, VD, the ip address of www.maroon5.com is 216.18.168.16.
- VD to VC: Hey, VC, the ip address of www.maroon5.com is 216.18.168.16.

End.