# CS 5153/5053 Network Security, Spring 2023

## Project 4: Local DNS Cache Poisoning

## Report

### Student: Austin Tyler Conn

Contents

[Link to Source Code 3](#_Toc131178888)

[Host Environment Used 3](#_Toc131178889)

[Docker Information 3](#_Toc131178890)

[Assumptions 3](#_Toc131178891)

[How do you setup the User and Server machine? 4](#_Toc131178892)

[How do you perform the attack in your VM? 4](#_Toc131178893)

[Screenshots of each step 4](#_Toc131178894)

[Was the attack successful? 4](#_Toc131178895)

Link to Source Code <https://github.com/austinc3030/dns_m11809075>

## Host Environment Used

Operating System: Ubuntu 20.04 LTS



Hardware: Google Cloud E2 Instance

Links Used for Environment Setup:

* [seed-labs/seedvm-cloud.md at master · seed-labs/seed-labs (github.com)](https://github.com/seed-labs/seed-labs/blob/master/manuals/cloud/seedvm-cloud.md)
* [seed-labs/create\_vm\_gcp.md at master · seed-labs/seed-labs (github.com)](https://github.com/seed-labs/seed-labs/blob/master/manuals/cloud/create_vm_gcp.md)

## Docker Information

Text

Description automatically generated

Text

Description automatically generated

## Assumptions

1. Mapping between PDF document and docker containers provided:
   1. Client (10.0.2.5) = user1-10.9.0.6 (10.9.0.6)
   2. Server (10.0.2.6) = victim-10.9.0.5 (10.9.0.5)
   3. Attacker (10.0.2.7) = seed-attacker (10.9.0.1)

## How do you setup the User and Server machine?

## How do you perform the attack in your VM?

## Screenshots of each step

## Was the attack successful?

### Include screenshots to show the attack is successful and can render an incorrect IP on both the User machine and Server machine