# 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

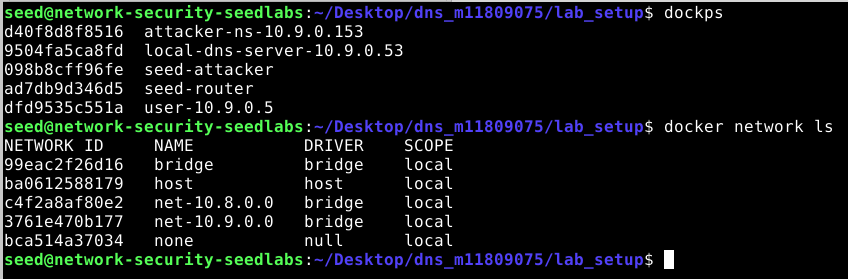


Hardware: Google Cloud E2 Instance

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



## Assumptions

* 1. User Machine (10.0.2.18) = user-10.9.0.5 (10.9.0.5)

Graphical user interface, text, application

Description automatically generated

* 1. Attacker (10.0.2.17) = seed-attacker (10.9.0.1)

A screenshot of a computer

Description automatically generated

* 1. Local DNS Server (10.0.2.16) = local-dns-server-10.9.0.53 (10.9.0.53)Graphical user interface, text, application

     Description automatically generated

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

### User Machine (Task 1)

1. Look at the contents of */etc/resolv.conf*.

Graphical user interface, text, application

Description automatically generated

1. It appears that the SEED Labs Docker Image is already configured to use the local-dns-server-10.9.0.53 as the DNS server. Note that *resolvconf* is not installed in this image. Verify using the *dig* command that 10.9.0.53 is the DNS server in use.

Text

Description automatically generated

***Note:*** *as seen above, the server used by dig is 10.9.0.53, the IP address of local-dns-server-10.9.0.53*.

### Server Machine (Task 2)

1. Look at the contents of */etc/bind/named.conf*.

Text

Description automatically generated

1. Look at the contents of */etc/bind/named.conf.options*.

Text

Description automatically generated

1. Dump the DNS cache to the file specified by the *dump-file* line in step 2 (*/var/cache/bind/dump.db*).

Graphical user interface, text, application

Description automatically generated

1. Flush the DNS cache.

Graphical user interface, text, application

Description automatically generated

1. Turn off DNSSEC by modifying the */etc/bind/named.conf.options* file to comment out *dnssec-validation auto;* and add *dnssec-enable no;*.

Text

Description automatically generated

***Note:*** *this appears to already be configured in the SEED Labs Docker Images provided.*

1. From the seed-user, test that DNS is working properly using *dig*.

Text

Description automatically generated

1. Use Wireshark to verify a DNS query is made when running *dig* on seed-user.

Graphical user interface, application

Description automatically generated

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

## Screenshots of each step

See screenshots shown with steps in “How do you setup the User machine and Server machine?” and “How do you perform the attack in your VM?”

## 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