Lab 02

Differentiating Characteristics of Blue, Red & Purple Teams Using Footprinting Techniques from Ping, Fragmentation, Tracert, NSLookup, Etc.

Instructor: Samuel Esan

info@delojik.com

Characteristics of Red, Blue & Purple Teams

Red Team: The red team is in charge of the offensive. They must figure out creative ways to attack the company and to infiltrate it. The red team must do everything (within certain parameters) possible to succeed.

Blue Team: The blue team oversees defending the company. They have to do everything they can to fend off the red team's attacks, including checking infrastructure, updating software, and preventing social engineering attempts from succeeding.

Purple Team: The purple team is a mix of some characteristics of the red and blue teams. In other words, the purple team is a mixture of the other two teams: they join forces after the campaign is over, so they can figure out where the vulnerabilities are and what needs to be improved.

Introduction

From the characteristics that you found above, you will notice that the Red Team has a unique way of looking at simple activities that are performed on a target. In this lab, we would use a few footprinting exercises to demonstrate how to think as part of a red team

What is Footprinting

Footprinting is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.

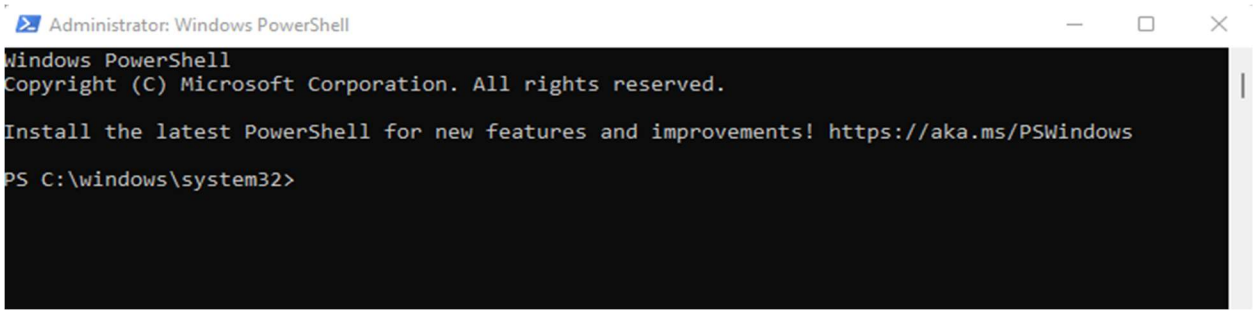
Exercises

A. Ping & Fragmentation

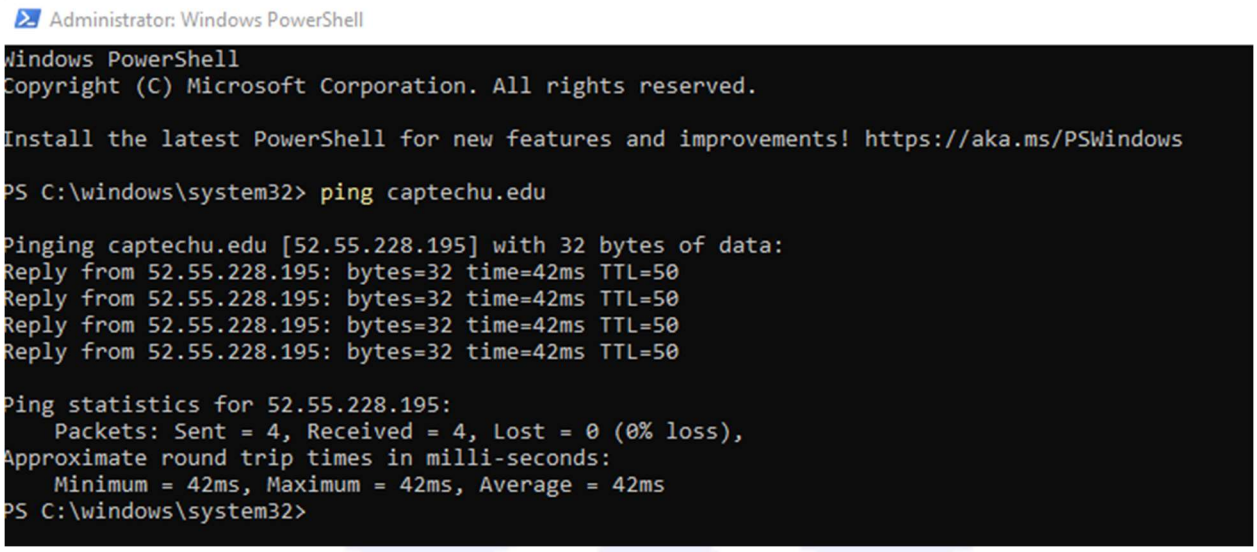
The ping tool gives us the ability to determine three things on a target:

(a) IP
(b) IP Range
(c) Class of IP Blocks which can help us determine the size of the organization

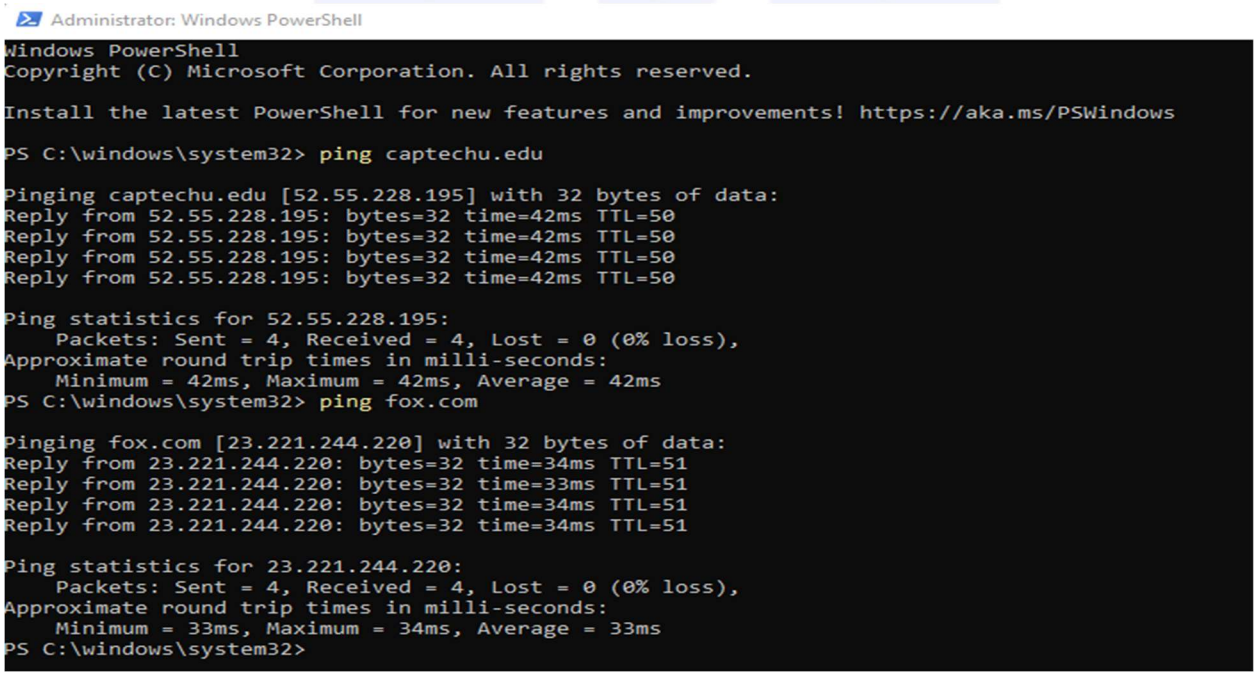
1. Proceed to open your windows PowerShell and run as an admin.



2. Go ahead to ping captechu.edu



3. Ping another site such as fox.com



Exercises

B. Tracert

1. Proceed to trace the route to captechu.edu

```
PS C:\windows\system32> tracert captechu.edu

Tracing route to captechu.edu [52.55.228.195]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  dsldevice.attlocal.net [192.168.1.254]
  2     6 ms     5 ms     6 ms  162-201-24-1.lightspeed.hstntx.sbcglobal.net [162.201.24.1]
  3     5 ms     5 ms     5 ms  71.149.23.168
  4     *        *        *     Request timed out.
  5     6 ms     6 ms     7 ms  32.130.18.117
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    42 ms    41 ms    42 ms  ec2-52-55-228-195.compute-1.amazonaws.com [52.55.228.195]
```

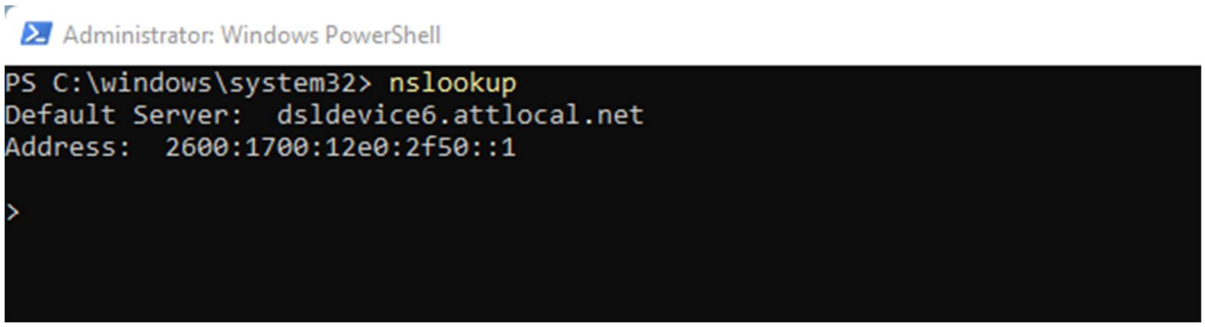
2. Proceed to do the same for fox.com

```
PS C:\windows\system32> tracert fox.com

Tracing route to fox.com [23.221.244.220]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  dsldevice.attlocal.net [192.168.1.254]
  2     4 ms     3 ms     3 ms  162-201-24-1.lightspeed.hstntx.sbcglobal.net [162.201.24.1]
  3     7 ms     5 ms     4 ms  71.149.23.168
  4     *        *        *     Request timed out.
  5    34 ms     *        *     32.130.20.13
  6    32 ms    33 ms    32 ms  32.130.20.14
  7    30 ms    30 ms    30 ms  32.130.20.105
  8    32 ms    32 ms    32 ms  32.130.20.99
  9    33 ms    32 ms    32 ms  32.130.20.101
 10    34 ms    34 ms     *     32.130.20.34
 11    32 ms    31 ms    33 ms  32.130.19.227
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15    33 ms    34 ms    36 ms  a23-221-244-220.deploy.static.akamaitechnologies.com [23.221.244.220]
```

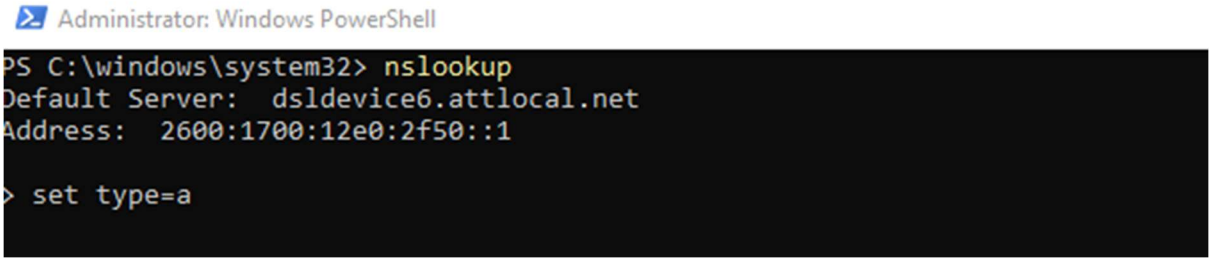
Exercises

C. NSLookup, C-Names and A-Records

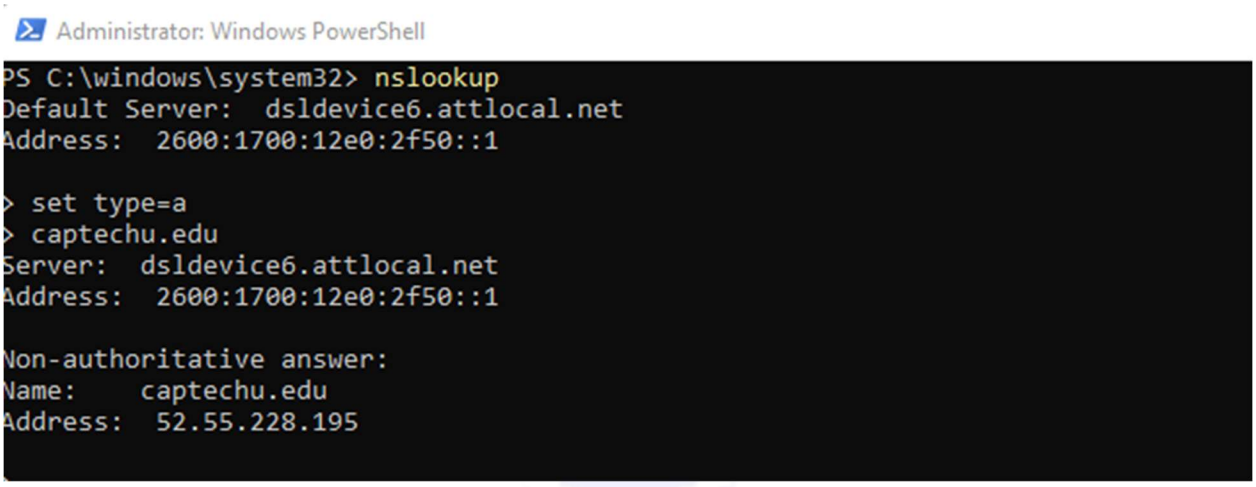
1. Open the NSLookup terminal from your PowerShell Command line.



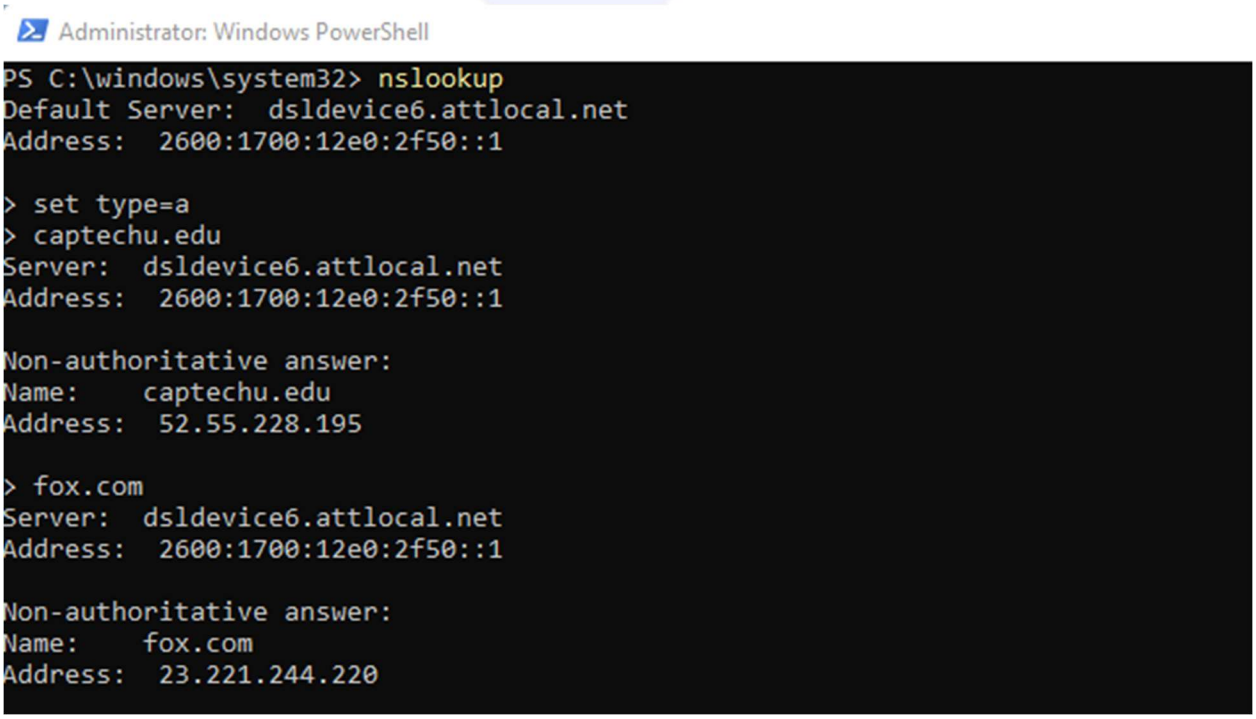
2. Proceed to set the A-record



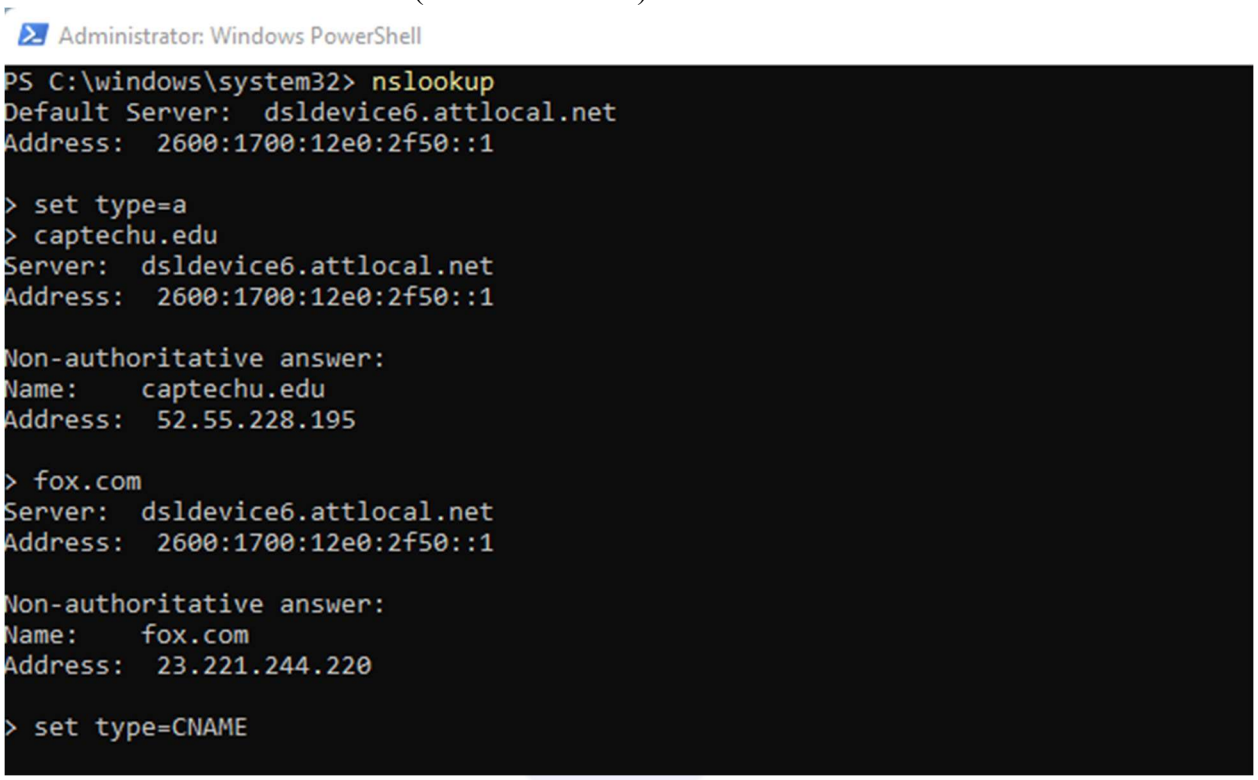
3. Verify the A-Record for captechu.edu



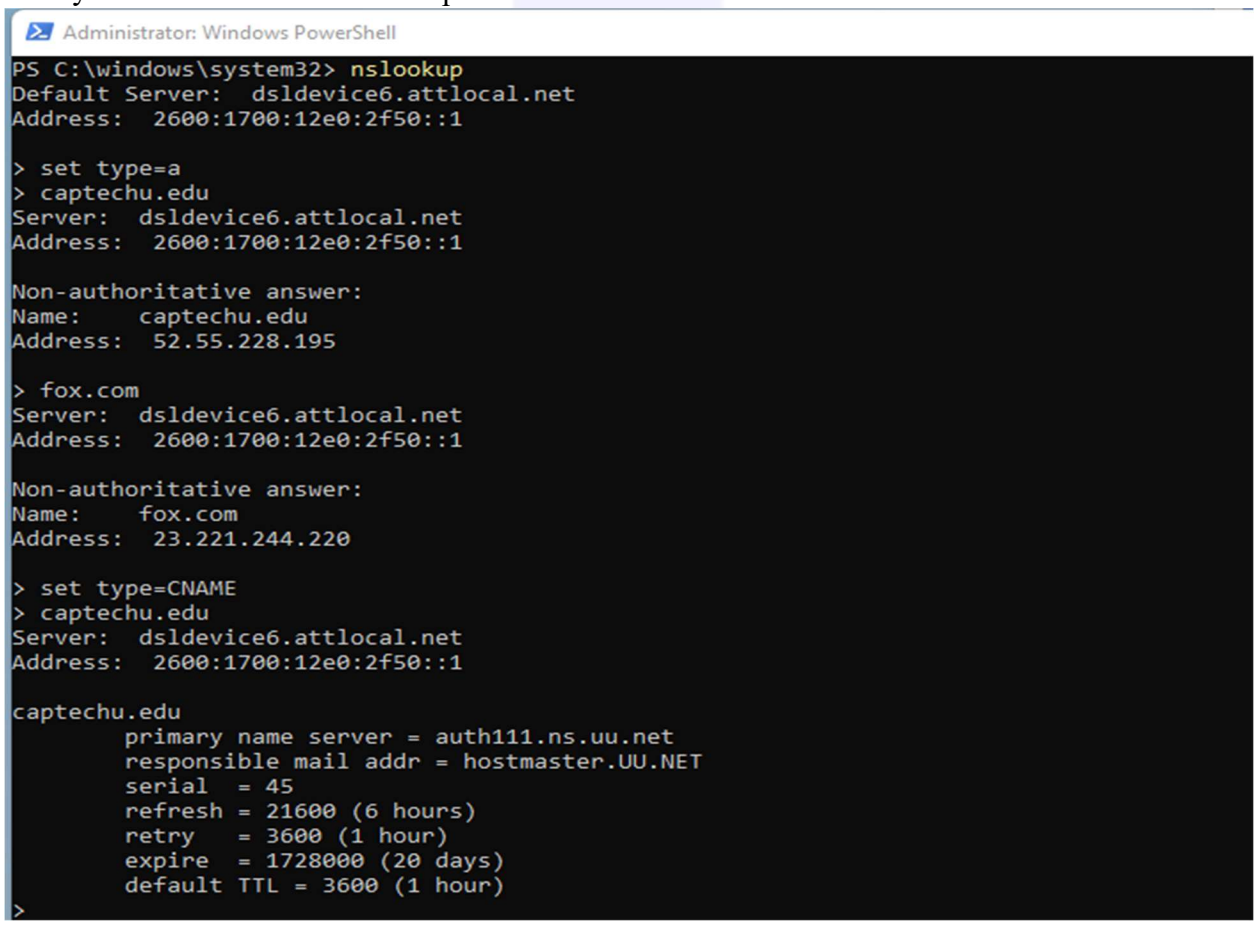
4. Do the same for fox.com



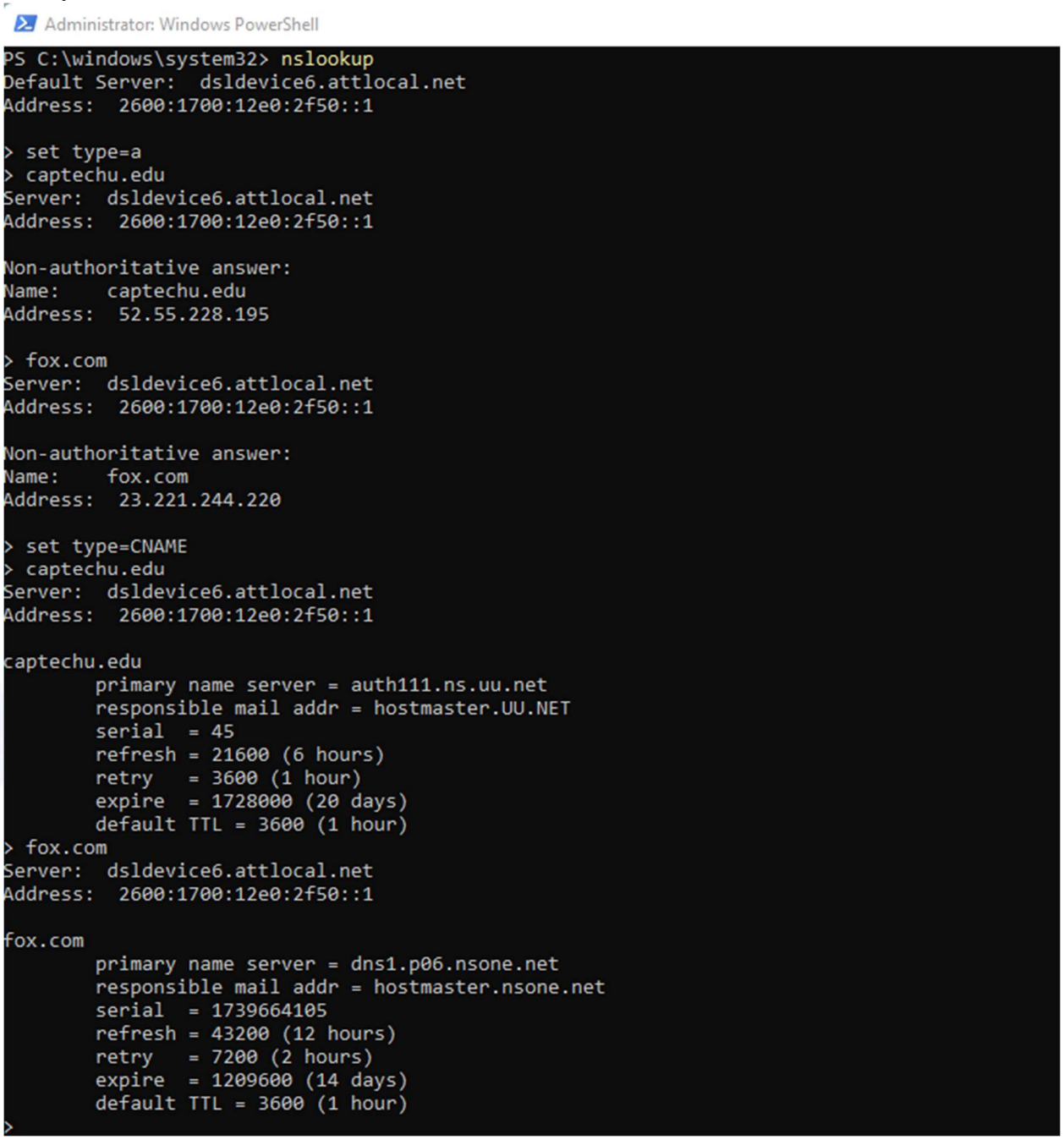
5. Go ahead and set the C-NAME (Canonical Name)



6. Verify the C-NAME results for captechu.edu



7. Verify the CNAME results for fox.com



Questions:

1. **Ping & Fragmentation:**
    a. Analyze the two ICMP requests to captechu.edu and fox.com. What differences does the TTLs tell you about the location and security of these two servers?
    b. Compare the fragmentation sizes and explain what it tells you about the security of the servers and the organization.

2. **Tracert**
    a. From a Red Team's perspective, analyze the differences between both tracert results for captechu.edu and fox.com.

3. **NSLookup, C-Names and A-Records**
    a. Analyze the CNAME results for both servers. What does the default TTL results tell you as a Red Team?
    b. With regards to the entire lab, how would you explain the way a red team approaches simple system and network results in comparison to a blue team?
4. List 5 characteristics that differentiate the red team from the blue and purple teams.
5. List 5 characteristics that differentiate the blue team from the red and purple teams.
6. List 5 characteristics that differentiate the purple team from the blue and red teams

Submit your response to INFO@DELOJIK.COM

SUBMIT BY Thursday February 20 at 6pm US CT.