Alice’s Real Identity

Group 8:

1. Amirul Ardy Bin Mohamed Rasi
2. Sng Yu Feng Chester
3. William Ryan Kusnadi
4. Yehezkiel Raymundo Theodoroes

Background

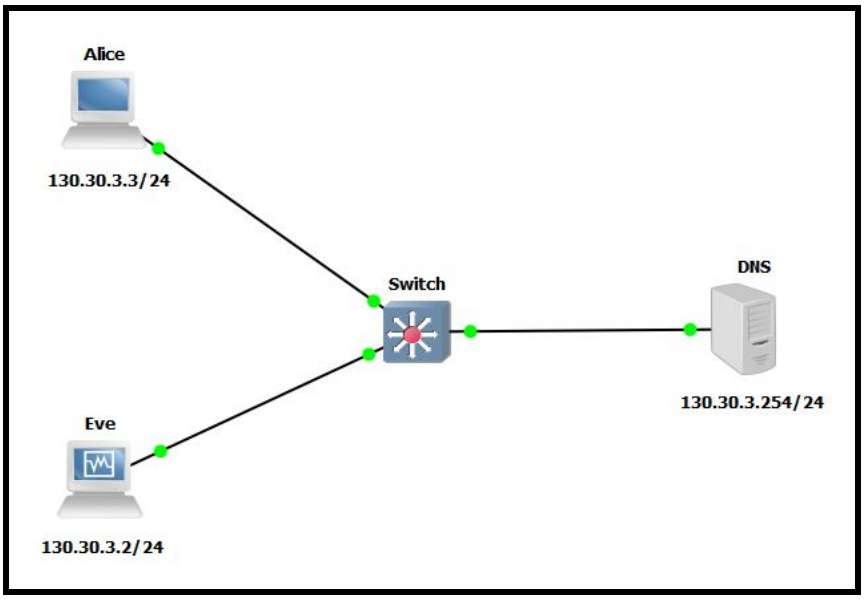
This document outlines our final project for CS3103 AY20/21S1. It was done under the topic of “Create Target System for Security Courses”. Here, we have created a CTF challenge presented in the form of a portable GNS3 project. This project can be used by teaching staff and students for security or networking labs in the future.

About The CTF Challenge

In this challenge, you are taking the role of a host named “Eve” in a network. Your aim is to hack into Alice’s computer and reveal the true identity of Alice!

- You know that Alice uses the same password for her computer for everything else.
- You also know that Alice frequently visits www.bank.com to do secretive transactions.
- Both Eve and Alice access the same DNS Server

The following is the topology of the network:



Note that we have purposely removed the external server from the topology to prevent you from performing a Wireshark capture on their communications. Nonetheless, Alice still repeatedly sends a packet to a destination IP address.

For this challenge, you will only be given the credentials for Eve's host and nothing else. You will win this challenge if you manage to obtain Alice's host password (by inspecting her original message...). To check if you've won the challenge, try to log in to Alice's computer. A surprise awaits you!

Setting Up:

1) Perform the initial setup of GNS3 along with the appliances installation according to the CS3103 AY20/21S1 labs instruction. Minimum appliances required:
    a) Lubuntu
    b) Cisco IOSvL2
2) Go to https://github.com/Yehezkiel01/CS3103_final/releases and download the latest GNS3 project.
3) Import the project into GNS3.
4) Start all nodes in the network.
5) Login to Eve's computer with this password: **Passw0rd!**
6) Start your attempt to steal Alice's password.

SOLUTION

Do not open the next page unless you are stuck and really require some help.
Hints will be given step-by-step and separated into multiple pages.

Step 1

Hint: Access the DNS server’s web interface.

How to do it:
As mentioned before, there is a web interface to query the DNS server. Try to access this page first. You can access it by entering the IP address of the DNS server in a browser.

Step 2

Hint: Bypass the login page.

How to do it:
Inspect the page and see there is a check for username and password, where iIf the username and password match, a JavaScript function will be invoked. You can directly call this function in the console without typing any username/password. Once called, check the source file of the function. You can find a byp4ss1ngL0g1n() function which will bring you to the DNS dashboard.

Step 3

Hint: Redirect the traffic to your own computer by changing the DNS record of “bank.com”.

How to do it:
Perform an SQL Injection attack.

Enter the following query:

```
bank.com'; UPDATE records SET ip ='130.30.3.2' where domain='bank.com';
```

Step 4

Hint: Open port 80 to start listening to HTTP messages.

Enter the following command:

```
sudo netcat -l 80
```

Step 5

Hint: Get the password and login to Alice.

The following is the password:

```
4N4nD1nW0nD3rL4nD
```

You will finally know who the real Alice in Wonderland is...