Route Me

Background Story
Recent reports regarding delays in food container production of the **“Plastic & Elastic”** company led to several changes in the company’s network topology.

The topology modification included new networking devices and permissions modifications.

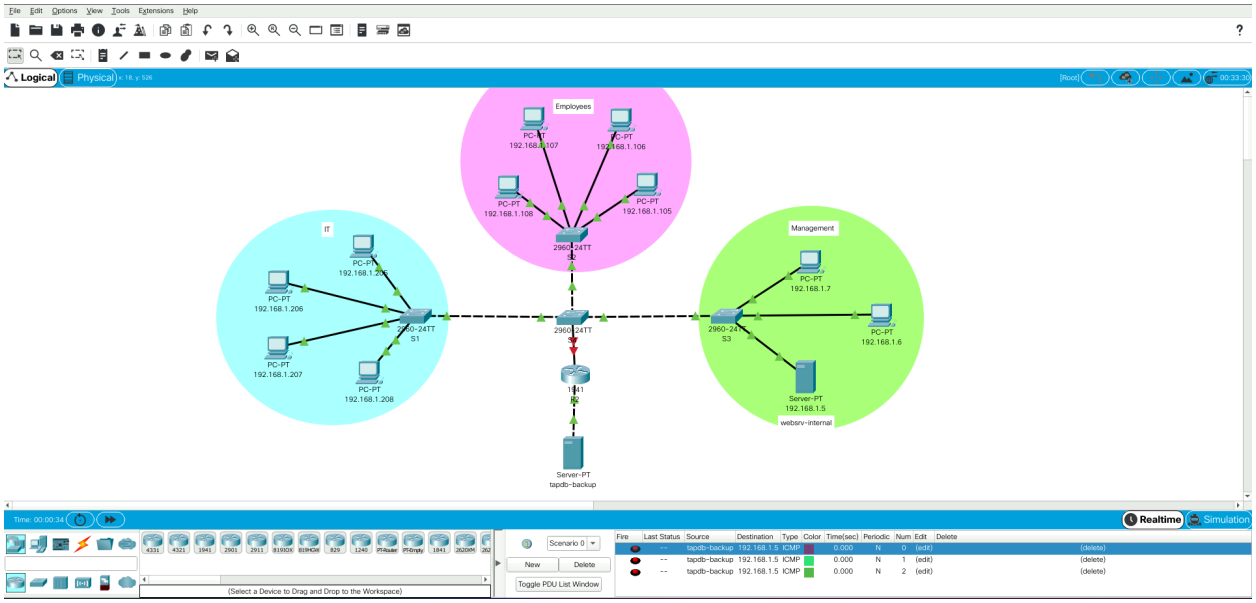
As the company’s security specialist, you were requested to verify that the new topology and hierarchy were established securely.

When considering the various cases, your main concern was a compromise of the main router in the network.

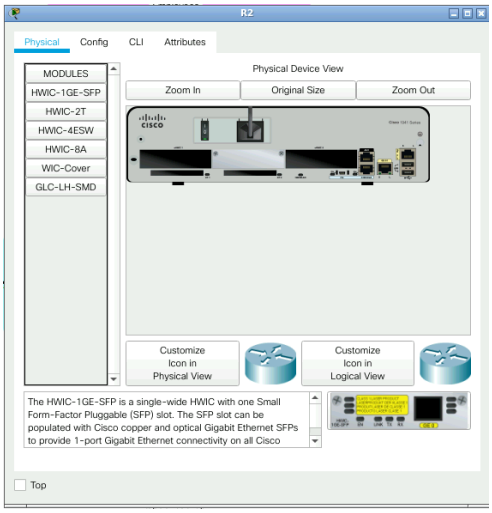
Your goals
To perform the security evaluation without interrupting the production process, you were provided with an exact replica of the network and access to ‘**R2**’, using the user and password **‘Smith:DawaYk’**

- Find a way to compromise the router and access the Global Configuration Mode.
- Modify the router’s configurations to enable access to the web server in the management network from the ‘**tabdb-backup**’ Server.
- Verify the web interface of ‘**websrv-internal**’ (192.168.1.5) in the Management network can be accessed from ‘**tabdb-backup**’

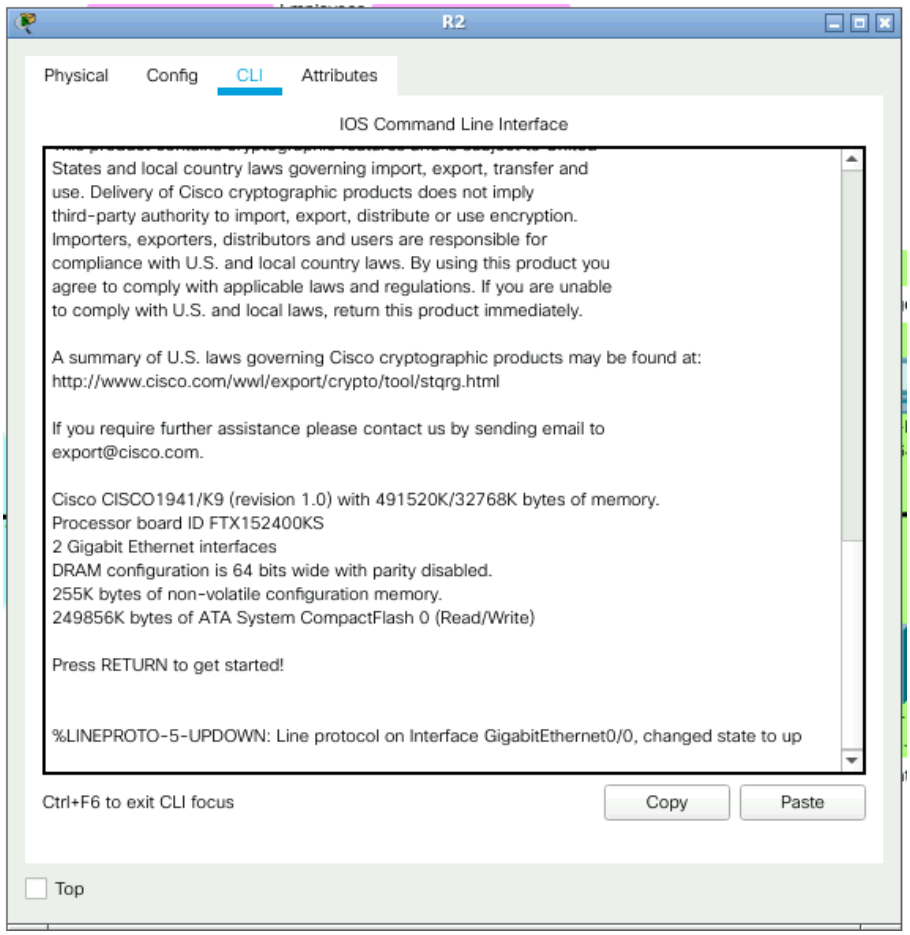
Here’s our network layout



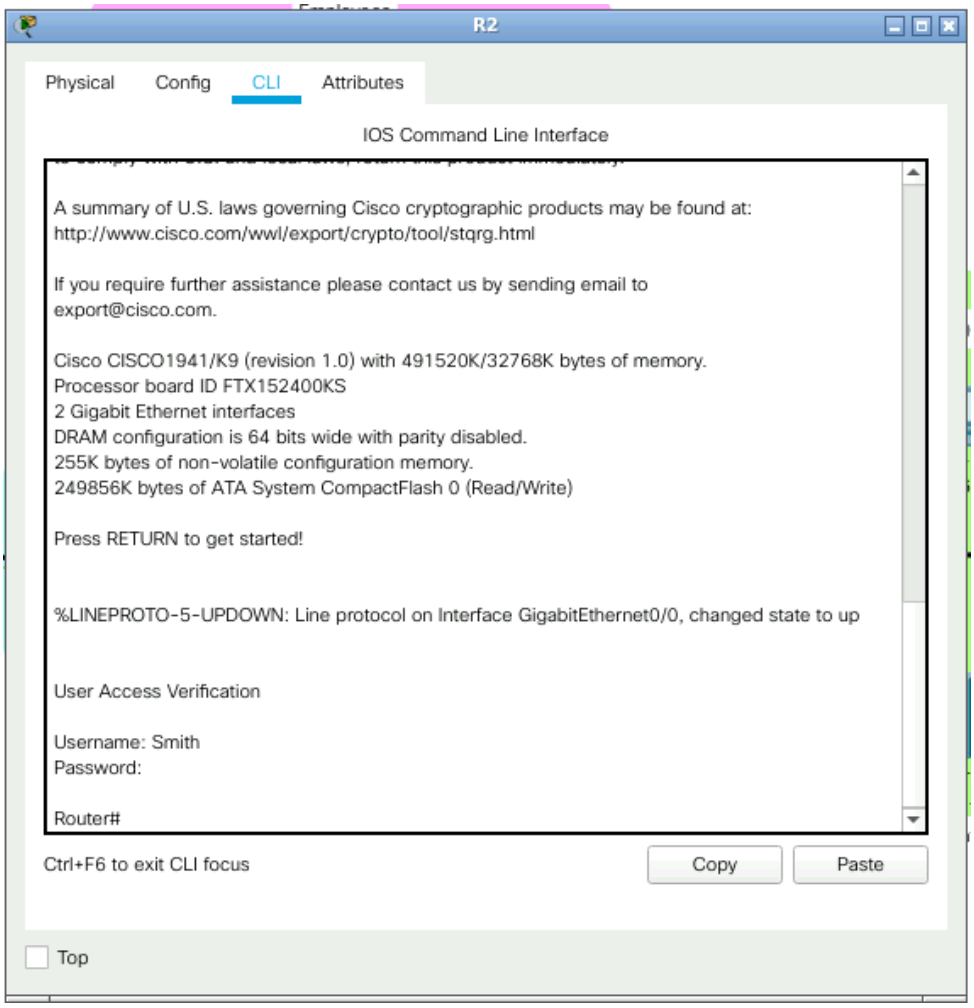
And here's my Process:
I started by going to **R2**



And went to the CLI (command line interface)



And here is where I entered the **Smith** username and **DawaYk** password

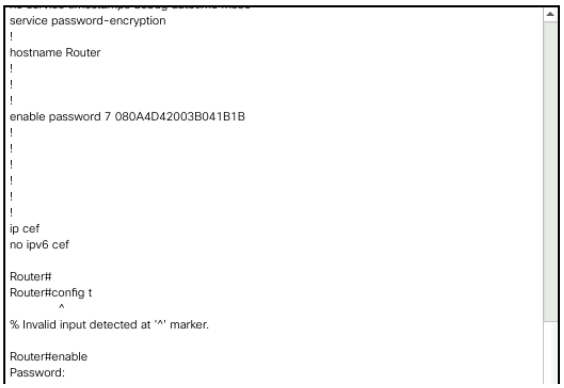


I can see straightaway that I'm in **Privileged EXEC** mode, which grants administrative access to all device commands, including viewing sensitive configuration files.

But my first goal is to go further and compromise the router to access **Global Configuration Mode.** Just to verify, I enter **configure terminal** (or, **config t**) and can see:

- ★ % Invalid input detected at '^' marker

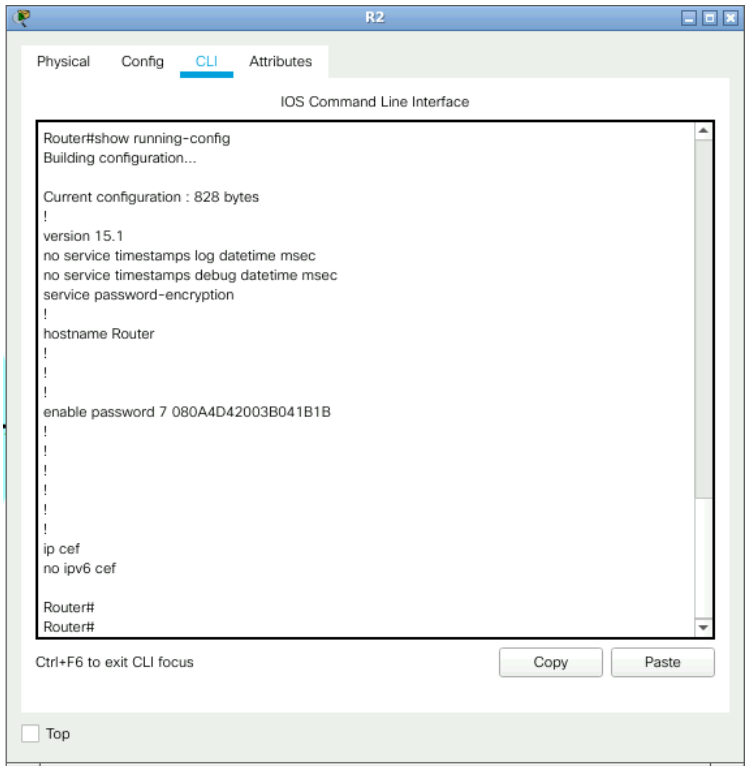
Access essentially denied.



So, I need to find a way to compromise the router and access the Global Configuration Mode.

I dig just a little deeper and enter **show running-config**, which shows me

- hostname: Router
- enable password 7 080A4D42003B041B1B



a-HA! I was expecting to see a Type 5 (MD5), 8 (SHA-256), or 9 (Scrypt) encryption level password, but no, it's **type 7**. I know that Type 7 encryption is insecure (which is OK for this lab environment) so I'm on my way to my first goal, compromising the router to access Global Configuration Mode. All I need to do is navigate to a website that will decrypt type 7 passwords.

The decrypted password for **R2** is **KaliBali**. So I return to the original error I received and enter that password, KaliBali and WOOT, I'm in. I can now access the **Global Configuration Mode**, by typing **config t**

```
service password-encryption
!
hostname Router
!
!
!
enable password 7 080A4D42003B041B1B
!
!
!
!
!
!
ip cef
no ipv6 cef

Router#
Router#config t
          ^
% Invalid input detected at '^' marker.

Router#enable
Password:
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

I'm on my way to modifying the router's configurations.

I configure the **interface** by entering:

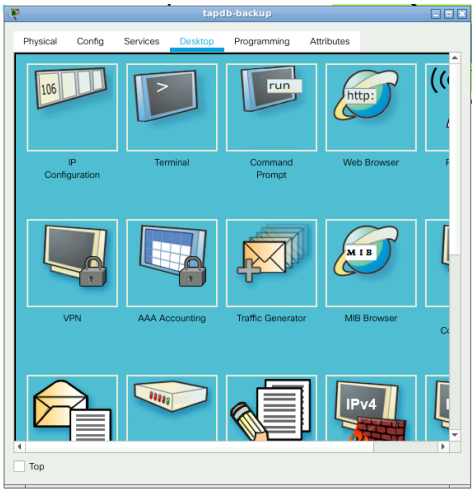
- **interface gigabitEthernet 0/1**
- and then activate that network interface by entering **no shutdown**

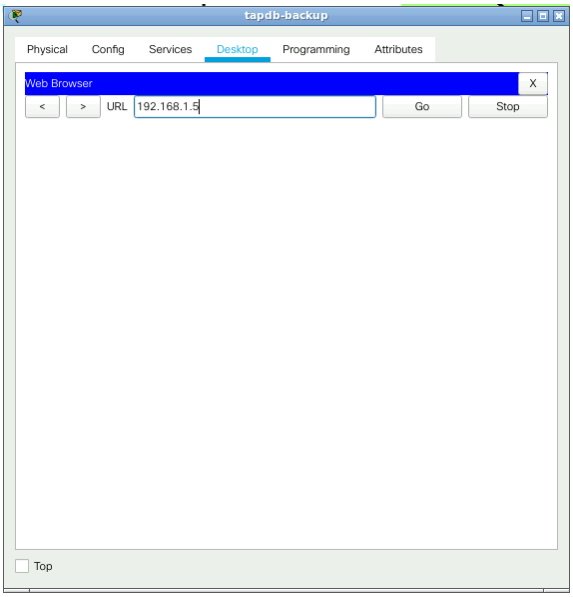
```
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#
```

Ctrl+F6 to exit CLI focus Copy Paste

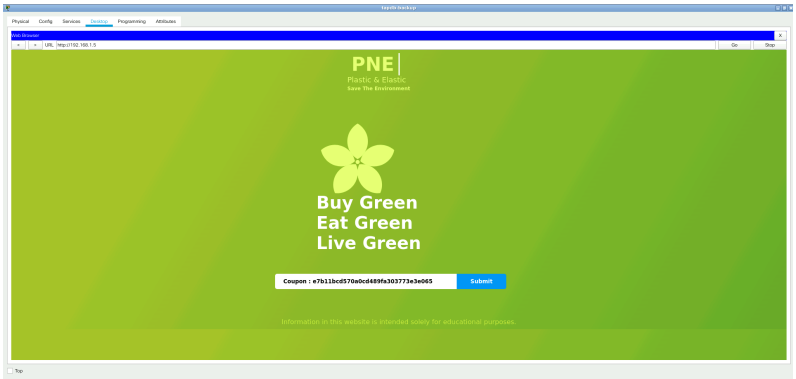
Now, let's see if we can accomplish our last goal which is to verify the web interface of '**websrv-internal**' (192.168.1.5) in the Management network can be accessed from

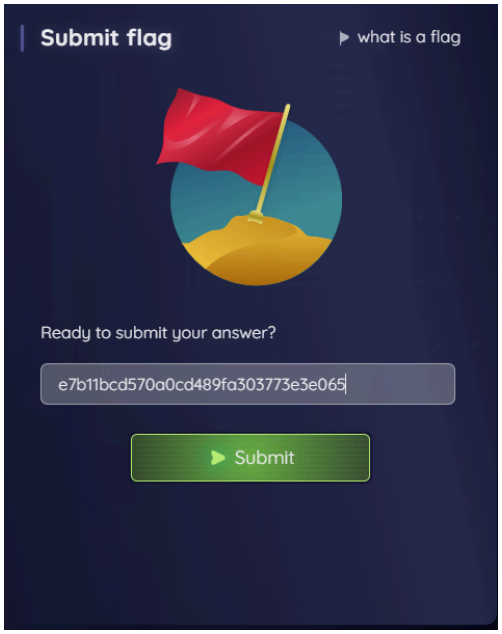
‘**tabdb-backup**by going to **tabdb-backup** via Web Browser





Yeee! Look at that! And THERE is the flag: e7b11bcd570a0cd489fa303773e3e065




Submit flag
what is a flag
Ready to submit your answer?
e7b11bcd570a0cd489fa303773e3e065
Submit


OBJECTIVE SECURED