**Assignment 3**

Mininet & BGP Routing

**Security Tools Lab 1**

Gowtham Baskar   
1006523

**Mininet**

After installing the Mininet as per the assignment. We have successfully designed a network diagram based on the information found in each host and router as show in the screenshot below.

Timeline

Description automatically generated

Following Network Diagram illustrates the detailed flow of network

Diagram, schematic

Description automatically generated

**BGP**

As per this Task, I’ve taken screenshot for both BGP propagated route and compared each routes with its routers.

A picture containing text

Description automatically generated

From the above screenshot we can see that the

After coonecting to R1 using BGP route Table. “Enable” was entered to access the admin mode and a wireshark was established using R1 router. When “clear bgp external” was entered, the following packets were captured showing the other 2 types of message (OPEN Message and NOTIFICATION Message) other than “keepalive”. A screenshot is added below for reference.

Table

Description automatically generated

Next...

**BGP Attack 1**

After reading and understanding the configurations, I’ve modified the “bgpd-R4.conf” file where instead of 14.0.0.0/8 as it’s default, I’ve broadcasted to advertise about victim route to network 13.0.0.0/8.

Text

Description automatically generated

After that I’ve tried to perform the attack and I’ve managed to successfully compromise the website present in 13.0.1.1 (AS3) as shown below.

**Graphical user interface, application

Description automatically generated**

I’ve also recorded the Wireshark packets and TCP packets are retransmitted as shown below.

**A picture containing background pattern

Description automatically generated**

After that, I’ve compared the route from Switch R1 to 13.0.1.1 before and after the attack and now the AS is broadcasting to the neighbour 13.0.1.1 which was modified in AS4 configuration.

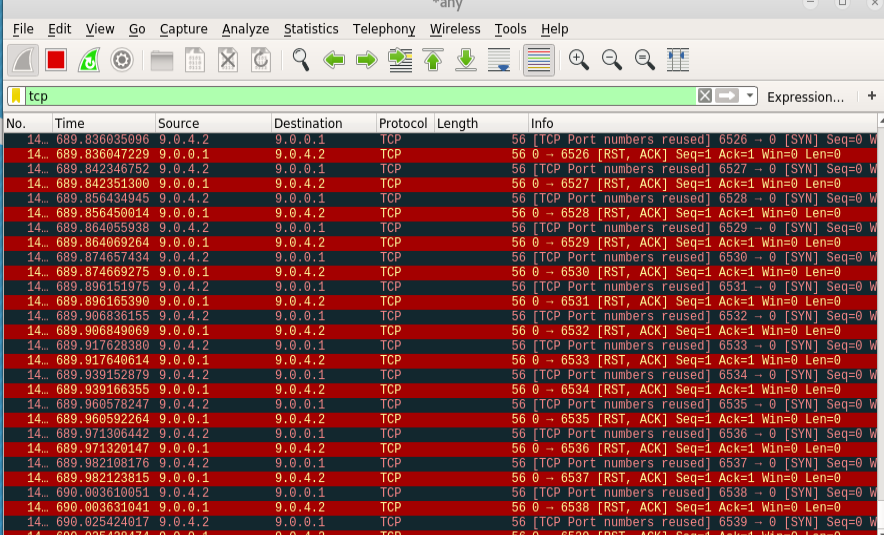
**Text

Description automatically generated**

**BGP Attack 2**

Firstly, I’ve opened a Wireshark on R1 and scanned the all the interfaces.

I’ve done <hping3 -I u1 -S 9.0.0.1> as 9.0.0.1 is the router IP that is being passed to other AS’s (AS2 and AS 3). I’ve included the Wireshark screenshot for reference below. I can also do a --flood command, but by doing so freezes the machine but successfully creating a DOS attack.



By adding null0 to the static route, we will be able to protect the route from any DoS attack.

I’ve tried to add a null route in the <R1-bgpd.conf> file.

Text

Description automatically generated

I was unsuccessful as the service was not detected when I make changes to the AS1 config and cuts the AS4 config from the routing.