ACN Mininet Assignment: BGP Path Hijacking

In this group assignment, you are going to recreate a "BGP path hijacking attack" inside Mininet by making use of the code base available at this link. Please follow the instructions step-by-step and answer the questions along the way in your report. Do not forget to insert screenshots of outputs seen at different nodes and wireshark logs to support your answers, wherever needed.

Setup:

1. Download the virtual machine at: link
2. Use VirtualBox to import the virtual machine. The VM is GUI enabled.
3. Start the VM.
4. Type in login id as “mininet and password also as “mininet”. You should be able to see a desktop.
5. Verify that in /home/mininet, you see a bgp folder.

Any questions up to here can be posted in google classroom or the private chats if you have trouble setting the above up. Please verify this as soon as possible and well before the deadline so that you are not hindered by setup issues.

Assignment sequence starts here:

The assignment requires that you start the mininet environment. In the tutorial we did so explicitly with a command “sudo mn”. However, here we are going to start a custom topology using a pre-written script available at https://bitbucket.org/jvimal/bgp/src/master/
To do so, follow the steps given below:

Open a terminal and navigate to /home/mininet/bgp

Once inside, execute the command “`sudo python bgp.py`”. This brings up a custom mininet topology. You should be able to see the familiar screen as shown below.

```
mininet@mininet-vm:~/bgp$ sudo python bgp.py
*** Creating network
*** Adding controller
*** Adding hosts:
h1-1 h1-2 h1-3 h2-1 h2-2 h2-3 h3-1 h3-2 h3-3 h4-1 h4-2 h4-3
*** Adding switches:
R1 R2 R3 R4
*** Adding links:
```

```
(R1, R2) (R1, R4) (R1, h1-1) (R1, h1-2) (R1, h1-3) (R2, R3) (R2, h2-1) (R2,
h2-2) (R2, h2-3) (R3, h3-1) (R3, h3-2) (R3, h3-3) (R4, h4-1) (R4, h4-2) (R4,
h4-3)
*** Configuring hosts
h1-1 h1-2 h1-3 h2-1 h2-2 h2-3 h3-1 h3-2 h3-3 h4-1 h4-2 h4-3
*** Starting controller
*** Starting 4 switches
R1 R2 R3 R4
Waiting 3 seconds for sysctl changes to take effect...
Starting zebra and bgpd on R1
Starting zebra and bgpd on R2
Starting zebra and bgpd on R3
Starting web servers
*** Starting CLI:
mininet>
```

Q1: Draw the topology diagram used for this demo. How many hosts are there and how many Routers are present in the emulated network inside mininet? How many hosts are present in each subnet? (Hint: Each router here represents an autonomous system)

Q2: What are all the available interfaces (on both routers and hosts) and what are their IP addresses? (hint: use xterm to log into the host and find the answer). Include the IP addresses also in the topology diagram. If an interface does not have an IP address yet, mention it.

Q3: Check the reachability for host “h3-1” from at least three other hosts. Post screenshots as proof that you are able to communicate with “h3-1”. (hint: use xterm “hostname” to log in the host and test reachability)

Now let us learn how to look into the bgp routing table of the routers. For example, to look into the router R1, open a new terminal and execute the following command: `sudo python run.py --node R1 --cmd "telnet localhost bgpd`. This brings up a series of prompts as shown below. Now type “en” in all the prompts to reach the bgpd-R1 shell as shown below

```
mininet@mininet-vm:~/bgp$ sudo python run.py --node R1 --cmd "telnet
localhost bgpd"
Connecting to R1 shell
Trying ::1...
Connected to localhost.
Escape character is '^]'.

Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification
Password: (type password "en" (without quotes))
Now, type the "en" command to get to the admin shell:
```

```
bgpd-R1> en
Password: (type password "en" (without quotes))
bgpd-R1#
```

Now type in the command "`sh ip bgp`" to view the routing table.

Q4: What do you see at the router R1 (AS1). Explain your interpretation of the entries in the BGP table with screenshots.

Q5: Perform the same for the router R2. Post screenshot. Are the entries in the routers different from each other? Why? What do they signify?

Q6. Post contents of forwarding tables at R1 and R2 using "route -n" command by logging into respective routers. Explain the difference between R1's BGP table and its forwarding table and how the BGP table is used to populate entries in the forwarding table of R1.

Now let's continue on with the experiment. When you executed bgp.py, along with the topology, the script also started a webserver in the host "h3-1", now we will access a default page on this webserver from host "h1-1". To do so open a new terminal (keep the mininet terminal open) and execute the following script: "`./website.sh`". You should see continuous messages as below.

```
mininet@mininet-vm:~/bgp$ ./website.sh
Sun Aug 10 09:56:39 PDT 2014 -- <h1>Default web server</h1>
Sun Aug 10 09:56:40 PDT 2014 -- <h1>Default web server</h1>
Sun Aug 10 09:56:41 PDT 2014 -- <h1>Default web server</h1>
```

The script website.sh automatically logs into host h1-1 and continuously sends GET requests to the host h3-1.

Q7: Open wireshark and listen to an interface (you have to choose the appropriate one). Post screenshots of the HTTP GET requests and the response you received. This should correspond to the output seen on the terminal window. (hint: to open wireshark: xterm into a host and type "`sudo wireshark &`"; ignore any error messages that pop up. Then choose an interface and listen to it.)

At this point, it should be clear that the topology is alive with a webserver running on h3-1 and a host h1-1 actively accessing it.

Q8: Modify `website.sh` (call it `website2.sh`) by choosing one of the hosts in AS2 to send GET requests to the webserver running on h3-1. Post a screenshot of CLI output and wireshark log as the proof.

Now open a new terminal. Navigate into the bgp folder and run the following script: "`start_rogue.sh`". You should be able to see the following output.

```
mininet@mininet-vm:~/bgp$ ./start_rogue.sh
Killing any existing rogue AS
Starting rogue AS
```

The script starts a rogue AS with the border router R4. This AS4 has malicious intent to hijack BGP paths of AS3 to itself and launches a fake website mimicking the web server deployed on the host h3-1.

Q9: Do you see any change in the CLI output where you ran website.sh? If yes, post the screenshot. If not, post the screenshot. What do you think has happened?

Q10: Do you see any change in the CLI output where you ran the modified script, website2.sh? If yes, post the screenshot. If not, post the screenshot. What do you think has happened?

Q11: Log into the routers R1, R2. Are their BGP tables and forwarding tables different from before? If so, what is the difference? What has happened after bogus BGP advertisements by AS4 at AS1 and AS2?

Now to have a fine grained look and investigate what could have happened, we are going to repeat the experiment. For that run the script `stop_rogue.sh` to stop the rogue autonomous system as shown below:

```
mininet@mininet-vm:~/bgp$ ./stop_rogue.sh
<switch to the other terminal>

mininet@mininet-vm:~/bgp$ ./website.sh
Sun Aug 10 10:08:15 PDT 2014 -- <h1>*** Attacker web server ***</h1>
Sun Aug 10 10:08:16 PDT 2014 -- <h1>*** Attacker web server ***</h1>
<R4 killed at this point>
Sun Aug 10 10:08:17 PDT 2014 -- <h1>Default web server</h1>
Sun Aug 10 10:08:18 PDT 2014 -- <h1>Default web server</h1>
Sun Aug 10 10:08:19 PDT 2014 -- <h1>Default web server</h1>
```

Q12: But this time open the xterm of the appropriate hosts and listen to the appropriate interfaces (figure out these interfaces) on wireshark in order to listen to the traffic. Now run the `start_rogue.sh` script. Do you see any BGP message sequence in the wireshark captures? Pin point which BGP message contains the rogue BGP update and post the screenshot. Expand the packet and post the screenshot. Explain the message contents, especially prefixes being advertised. Correlate this message with the screenshot taken earlier.

Q13: Now put the sequence of events together and explain in clear steps what has occurred from start to finish. Has rogue AS succeeded in fooling the hosts (and then directing them to a fake website running at the hijacked host/web server) present in all other ASs or only a subset of them? List out the hosts that got fooled by the rogue AS.

Q14. When hosts present in AS1 ping hosts in AS3, observe RTT before running `start_rogue.sh` script and after running `start_rogue.sh` script. Do you find any difference, explain. Did the rogue AS (AS4) hijack all the hosts in AS3 or a subset of them?

Q15. This is an advanced task. Modify the scripts given in the code base in a way the rogue attacker (AS4) only hijacks the host "h3-1" but not other hosts present in AS3. Explain how to launch this targeted BGP path hijack attack on the target host "h3-1" and demonstrate it with step-by-step instructions with screenshots. Note that this part of the assignment (Q15) carries 1/3 of the total marks.

What to Hand in?

Deliverables in a tar ball or ZIP on GC

1. Folder having various scripts referred from the code base and those written by your group for answering the questions asked in this assignment.

2. Readme.txt (Contains detailed Instructions to run this assignment)

3. Report.pdf (Detailed explanations for the questions asked and screenshots used)

No late submissions allowed on GC.

ANTI-PLAGIARISM Statement <Include it in your report>

We certify that this assignment/report is our own work, based on our personal study and/or research and that we have acknowledged all material and sources used in its preparation, whether they be books, articles, packages, datasets, reports, lecture notes, and any other kind of document, electronic or personal communication. We also certify that this assignment/report has not previously been submitted for assessment/project in any other course lab, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that we have not copied in part or whole or otherwise plagiarized the work of other students and/or persons. Additionally, we acknowledge that we may have used AI tools, such as language models (e.g., ChatGPT, Bard), for assistance in generating and refining my assignment, and we have made all reasonable efforts to ensure that such usage complies with the academic integrity policies set for the course. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, we understand our responsibility to report honour violations by other students if we become aware of it.

Names <Roll Nos>:
Date:
Signatures: <keep your initials here>

Note: Max 3 students per group. No change in the group composition from the previous (programming) assignment. One submission per group on GC suffices.

References:

- https://github.com/mininet/mininet/wiki/BGP-Path-Hijacking-Attack-Demo
- https://bitbucket.org/jvimal/bgp/src/master/