Memo BGP Hijacking

Vinci Nicolò

29 October 2021

1 Part 1

This section contains answers for question 1-6.

1.1 Q1: How many hops away is the ftp server from the client?

The ftp server is 4 hops away from the client. The entire path starting from the client is:

1. Client 10.5.0.2
2. Asn3 10.5.0.1
3. Asn2 10.3.0.2
4. Asn1 10.2.0.1
5. Ftp server 10.1.1.2

1.2 Q2: Explain how the client is able to send packets to 10.1.1.2, i.e., what route is the client using to reach the server 10.1.1.2 (don't forget to list the gateway address and mask value).

The client is using the route with:

- Destination 10.0.0.0
- Netmask 255.0.0.0 (/8)
- Interface eth4
- Gateway 10.5.0.1

1.3 Q3: Does the "information" (not the raw output) differ from the above output? If so, what additional information can you learn from this output?

The *vtysh* command adds if a route is a static route or connected route in comparison to *nestat* command run in question 1.2. Moreover, *vtysh* shows also the connected route for the loopback interface.

1.4 Q4: What does it say? (README file)

The README file says: *AS1 owns the prefix for 10.1/16.*

1.5 Q5: What is the AS path to reach 10.1/16?

From Asn3 the AS path to reach 10.1.0.0/16 is: *65002 65001 i.*

1.6 Q6: What AS path will be used to reach an IP address 10.1.1.2? What AS path will be used to reach an IP address 10.1.2.2?

From Asn2 the AS path to reach 10.1.1.2 is: *65001 ?.*
From Asn2 the AS path to reach 10.1.2.2 is: *65001 i.*

2 Part 2

This section contains answers for question 1-4.

2.1 Q1: Explain the path from client host 10.5.0.2 to the ftp server 10.1.1.2. How many hops away is the ftp server from the client this time? Is there a difference in output from the same command in Part-1?

The ftp server is 4 hops away from the client. The entire path starting from the client is:

1. Client 10.5.0.2
2. Asn3 10.5.0.1
3. Asn2 10.3.0.2
4. Asn1 10.2.0.1
5. Ftp server 10.1.1.2

There no difference from the same command from Part 1 described in the question 1.1, because Asn3 matches the more specific route for 10.1.1.0/24 and not the route for 10.1.0.0/16. The attacker hijacked the route for 10.1.0.0/16 configuring Asn4 and the shortest path for 10.1.0.0/16 is through Asn4 from the point of view of the client. However, Asn3 matches the more specific route 10.1.1.0/24 when client performs the request for the ftp server.

2.2 Q2: What does it say? Did the contents of README file differ from the output in Part-1?

The README file says: *AS1 owns the prefix for 10.1/16.*
The README file does not differ from the output in Part 1.

2.3 Q3: What is the AS path to reach 10.1/16? Did the AS path differ from the last time (i.e., part-1)?

From Asn3 the AS path to reach 10.1.0.0/16 is: *65004 i.*
The AS path differs from the Part 1.

2.4 Q4: What AS path will be used to reach an IP address 10.1.1.2? What AS path will be used to reach an IP address 10.1.2.2?

From Asn2 the AS path to reach 10.1.1.2 is: *65001 ?.*
From Asn2 the AS path to reach 10.1.2.2 is: *65003 65004 i.*

3 Part 3

This section contains answers for question 1-4.

3.1 Q1: How many hops away is the ftp server 10.1.1.2 from the client this time? Is there a difference in output from the same command in Part-2?

The ftp server is 3 hops away from the client. The entire path starting from the client is:

1. Client 10.5.0.2
2. Asn3 10.5.0.1
3. Asn4 10.4.0.2
4. Attacker 10.1.1.2

In comparison to Part 2, the client request goes through the Asn4 and arrives to the Attacker. This time the attacker hijacked the more specific route 10.1.1.0/24. When the client makes the request, the Asn3 matches the route for 10.1.1.0/24. Then, it decides to go through Asn4 because the path is shorter than through Asn2.

3.2 Q2: Did the contents of README file differ from the output in Part-2?

The README file says: *I just hijacked your BGP Prefix!*.
The README file differs from the output in Part 2.

3.3 Q3: What is the AS path to reach 10.1/16? Did the AS path differ from Part-2? What is the AS path to reach 10.1.1.0/24?

From Asn3 the AS path to reach 10.1.0.0/16 is: *65002 65001 i*.
The path differs from Part 2, it is not hijacked.
From Asn3 the AS path to reach 10.1.1.0/24 is: *65004 i*.

3.4 Q4: What AS path will be used to reach an IP address 10.1.1.2? What AS path will be used to reach an IP address 10.1.2.2?

From Asn2 the AS path to reach 10.1.1.2 is: *65003 65004 i*.
From Asn2 the AS path to reach 10.1.2.2 is: *65001 i*.