Virtual Internet Labs

BGP Attack via Network Prefix Hijacking

Created: 02/26/2024

Published by

WWU Virtual Internet Development Team

Under the supervision of

Vipul Kumar

Western Washington University - Poulsbo Cyber Range

Contents

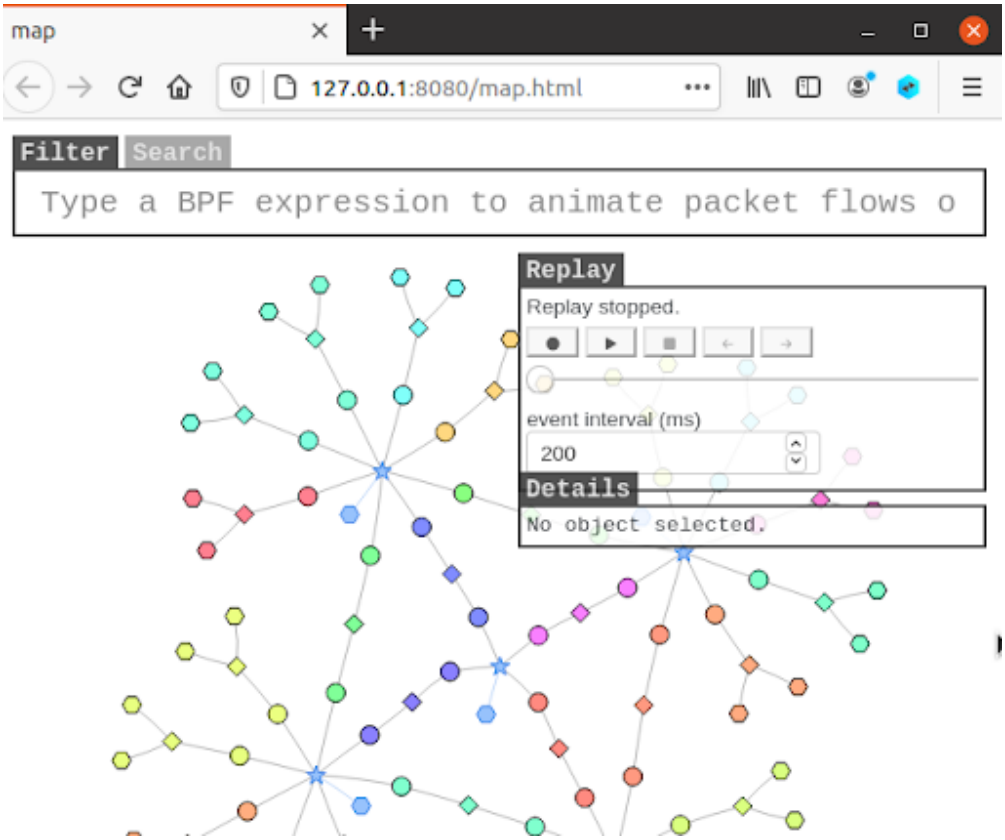
1 Introduction

The Border Gateway Protocol (BGP) is the backbone of the internet, responsible for routing traffic between autonomous systems (AS) which are large networks or group of networks managed by a single organization or service provider. BGP is a path vector protocol that makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator. Despite its critical role in internet infrastructure, BGP lacks an intrinsic security mechanism to validate routes, making it susceptible to various types of attacks, such as prefix hijacking, route leakage, and the interception of data.

2 Lab Procedure

2.1 Starting the Internet Emulator

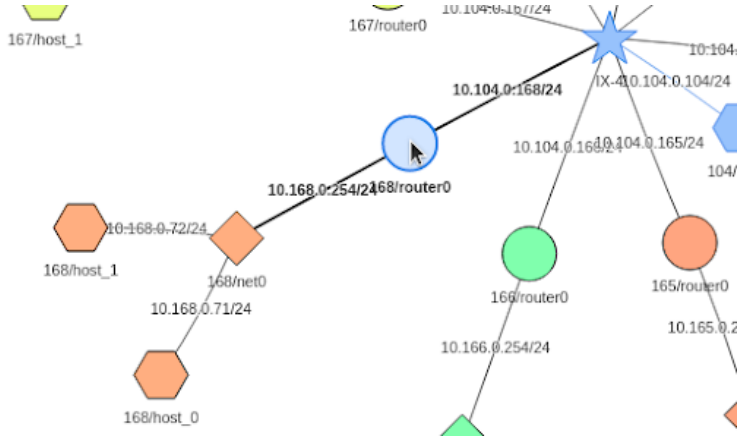
NOTE: It may take a few minutes for the environment to load, but you should end up with a Firefox browser open that contains a visualizer of the emulated internet.



2.2 Monitoring and Redirecting Traffic

2.2.1 Selecting a Router

Zoom in on the network map and click on one of the routers. For instance, router 168 with the IP address 10.168.0.254/24.

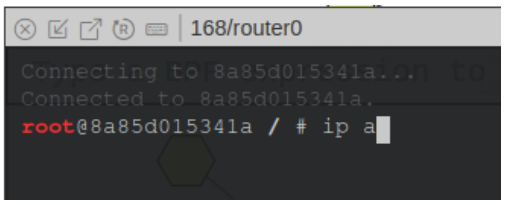


2.2.2 Launching Console

After selecting a router, click 'Launch Console' from the Actions menu displayed on the right side of the browser window.

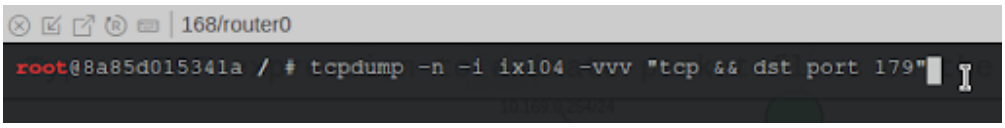
2.2.3 Discovering Your IP Address

Inside the console, start by entering the command 'ip a'. This is used to display and manage IP addresses assigned to all network interfaces on a machine. It shows detailed information about the state of network interfaces.



2.2.4 Capturing Packets

Take note of the ix value shown for the details of your selected router. Using your ix value, issue the tcpdump command. This is used for network diagnostics and troubleshooting. It allows you to capture and display the packets being transmitted or received over a network to which the computer is connected.

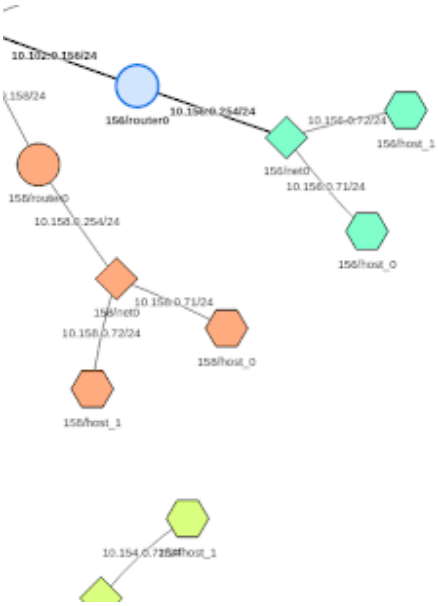


2.2.5 Filter Traffic

Apply the filter filter shown below using the input field shown at the top of the webpage then observe the traffic being highlighted on the map.

2.2.6 Disabling and Enabling BGP Sessions

Select a new router and disable the BGP Sessions under the respective menu, then re-enable them to observe the update messages in the console.

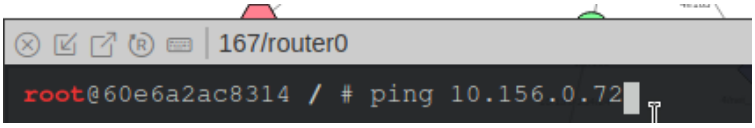


2.3 BGP Attack via Network Prefix Hijacking

Network prefix hijacking, also known as route hijacking or IP hijacking, is an attack where a malicious actor illegitimately takes control of one or several IP prefixes by corrupting BGP routing tables. This is done by broadcasting false prefix ownership information, causing internet traffic meant for a particular IP space to be misrouted through the attacker's network. This can lead to traffic interception, monitoring, or rerouting, disrupting internet services and compromising data integrity and confidentiality. The decentralized and trust-based nature of BGP, combined with the lack of an effective validation mechanism for routing announcements, makes such attacks feasible and challenging to mitigate.

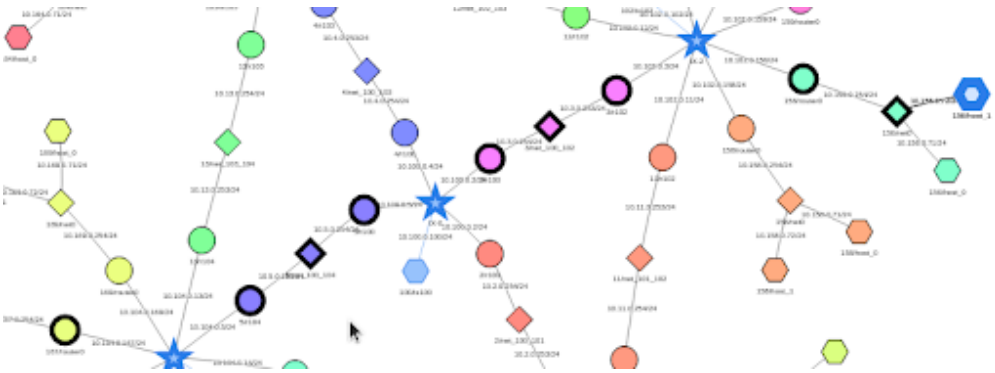
2.3.1 Initiating Communication

Start by turning on an ICMP filter and select two nodes for communication. Issue a ping from your selected router to the host.



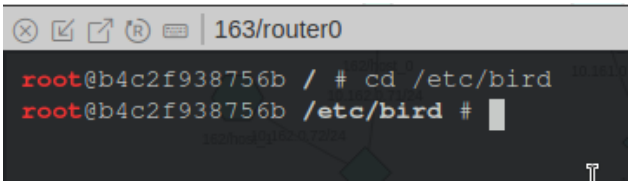
2.3.2 Observing Traffic

Adjust the filter to show traffic moving in one direction.



2.3.3 Accessing a Router for the Attack

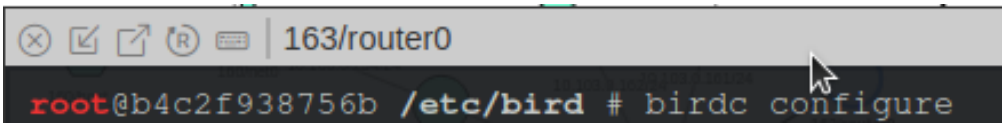
Select a router separate from the two currently communicating, open a console, change directory to the bird folder, and open the bird configuration file using a text editor.



2.3.4 Modifying Malicious Router Configuration

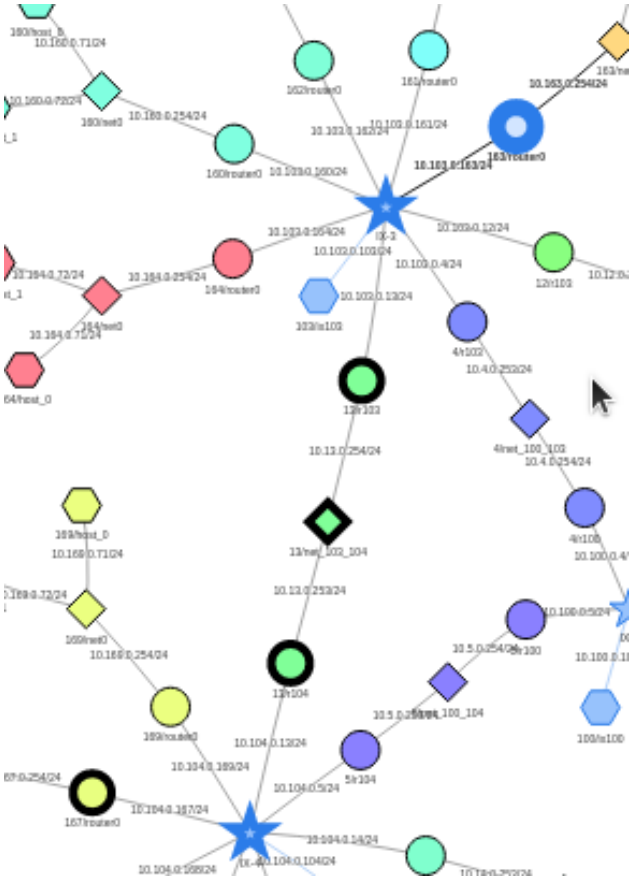
If using vim, click 'i' to enter insert mode then navigate using your arrow keys to reach the end of the file. Add the code snippet shown below to the end of the file making sure to change the second octet value (156 in the given example) to match the second octet value associated with the host you have selected as the endpoint for the devices you have communicating. To save the changes, if using vim, press 'esc' followed by, shift-colon, and type 'wq!', then press enter. Once back in the console issue the command 'birdc configure' to commit the changes.

```
protocol static hijacks {
        ipv4 {
                table t_bgp;
        };
        route 10.156.0.0/25 blackhole { bgp_large_community.add(LOCAL_COMM); };
        route 10.156.0.128/25 blackhole { bgp_large_community.add(LOCAL_COMM); };
}
```



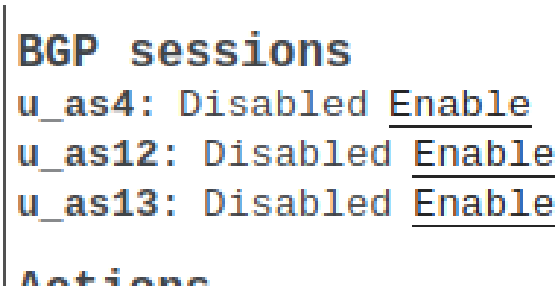
2.3.5 Observing Hijacked Traffic

You should now be able to see the traffic that was going to your selected host device get hijacked by the router that you edited the configuration file for similar to the example image shown below.



2.3.6 Stopping the Attack

To stop the attack you can either remove the code from the configuration file or disable all the BGP sessions on the router that is hijacking the traffic.



2.4 Mitigating the Attack

Several strategies exist to mitigate BGP hijacking:

- **BGPsec:** An extension of BGP, BGPsec provides security features for the validation of BGP announcement paths. It uses cryptographic signatures to ensure that the route announcements are authenticated and authorized by the actual IP address owners.
- **Route Origin Authorizations (ROAs):** As part of the RPKI framework, ROAs allow network owners to specify which Autonomous Systems are authorized to announce certain IP prefixes, thereby aiding in the prevention of unauthorized BGP hijacks.
- **Manually Filtering Routes:** This traditional method involves network administrators setting up manual filters to selectively accept routes from specific ASes. While this can be effective, it is labor-intensive and may not scale well with the dynamic nature of the internet.

3 Conclusion

This lab demonstrates the vulnerabilities inherent in the BGP protocol, highlighting the ease with which traffic can be hijacked and misrouted. By understanding these vulnerabilities, cybersecurity professionals can better protect networks against such attacks through vigilant monitoring, implementing security protocols like BGPsec, and adhering to best practices in route filtering and validation.