[Destroying the Internet (BGP routers) EP 1 // BGP Python scapy DoS script](https://www.youtube.com/watch?v=39DGVpMt7eQ)

A person in a black shirt

Description automatically generated

Internetworking

A diagram of a network

Description automatically generated

A diagram of a network

Description automatically generated

BGP attacks can take down internetwork spots

A close-up of a computer screen

Description automatically generated

Topology

A diagram of a machine

Description automatically generated

A diagram of a network

Description automatically generated

**BGP uses TCP port 179**

Layer2 relationship is NOT important in this scenario

Kali sniffing packets from BGP routers => sending back to Network

A diagram of a diagram of a router

Description automatically generated with medium confidence

A diagram of a network

Description automatically generated

BGP router to BGP router = **TCP unicast**

**Switch by default would NOT forward traffic to Kali**

A diagram of a diagram

Description automatically generated with medium confidence

Thus, we need to use 'Wiretaps'

A black box with a white text

Description automatically generated

The port

A person holding a device

Description automatically generated

It does NOT allow traffic to be sent back into the network

A hand holding a box with two ports

Description automatically generated

Then sniff the traffic and monitor the traffic out of that port

Problem of Wiretaps

A close up of a device

Description automatically generated

yet, Wiretaps do NOT allow us to send traffic back into the network

**We wanna monitor traffic between BGP routers,**

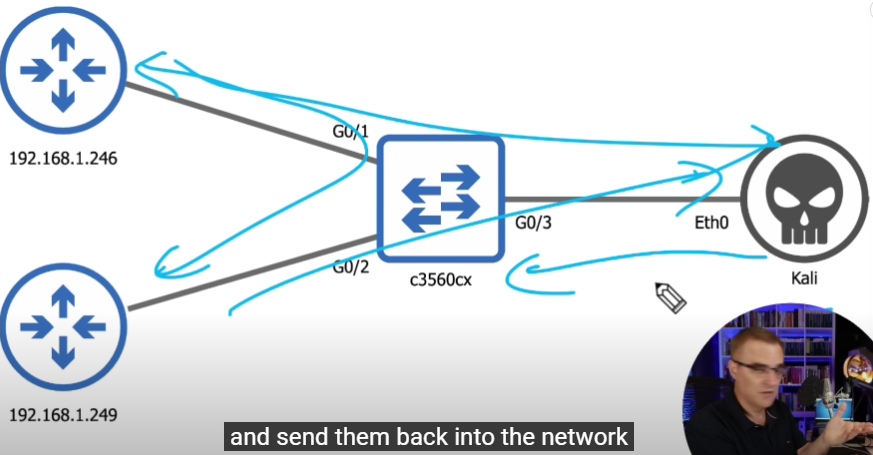
**receive the traffic & then manipulate the packets,**

**then send manipulated packets back into the network,**

**to get BGP routers do things for us**

A diagram of a router

Description automatically generated



In order to remove Routes from Switch to BGP Router 192.168.1.249

We must pretend our Kali to be BGP router 192.168.1.246 to send packets to BGP router 192.168.1.249 (Internet Access),

and get 192.168.1.249 to remove Routes from its routing tables

A diagram of a router

Description automatically generated

**Set-up of Port Mirroring to mirror traffic from BGP Router 192.168.1.246 via Gi0/1 to Switch c3560cx then to our Kali, and**

**configure Gi0/3 to NOT only just mirror traffic, but also receive traffic**

A diagram of a connection

Description automatically generated with medium confidence

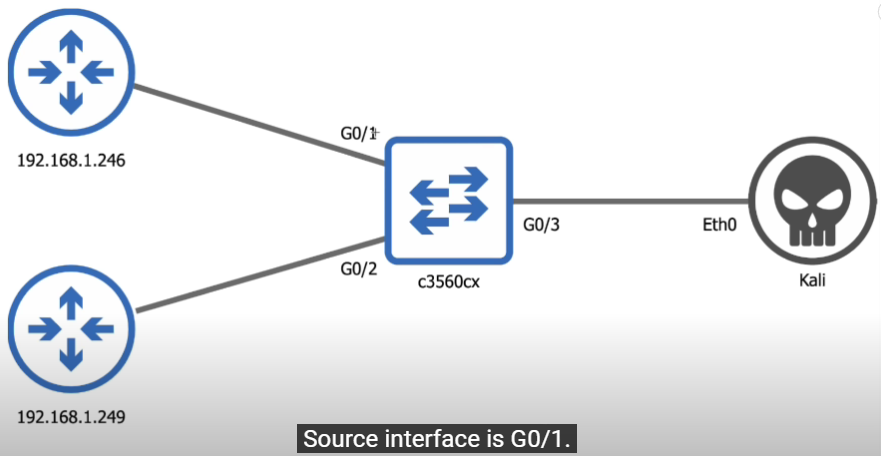
**Connecting to c3560cx Switch**

sh run | include monitor

A black background with white text

Description automatically generated

**Source of traffic from BGP Router 192.168.1.246 to Switch c3560cx is via Gi0/1**



**Network traffic between Switch c3560cx and Kali is via Gi0/3**

**\*\*\* We need access to the Switch to basically tap the network \*\*\***

**\*\*\* or We need a Hub/Wiretap to see traffic between BGP Routers \*\*\***

**\*\*\* To start intercepting traffic between Switch & BGP Routers**

**We Bridge Kali's network adapter on any Devices (Windows?) connecting to the Switch that connects to any BGP routers \*\*\***

A computer screen shot of a computer

Description automatically generated

**Now, we can start injecting traffic to the network**

1st script = bgp-dos-reset-neighbors.py to Reset the neighbor relationships between BGP routers

2nd script = bgp-remove-route.py to Remove routes out of the routing table

3rd script = bgp-add-fake-routes.py to Inject fake routes into BGP routing table

1st script =

**bgp-dos-reset-neighbors.py**

Reset the neighbor relationships between BGP routers

**BGP Hacking Topology**

# Let's say there's a computer (compA) connects to a Switch

# in which, that Switch also connects to some BGP Routers

A diagram of a network

Description automatically generated

# Once you've connected your laptop (Kali VM host) to compA using LAN cables

# You 'bridge' your Kali's network adapter to compA NIC

A computer screen shot of a computer

Description automatically generated

# Asking for a BGP Router IP:

# Use Ettercap & Wireshark to sniff all the devices in the network

# Find out all BGP Routers IP

# Enter 1 BPG Router IP for further sniffing

bgp\_IP = input('Enter BGP Router dst IP [192.168.1.249]: ')

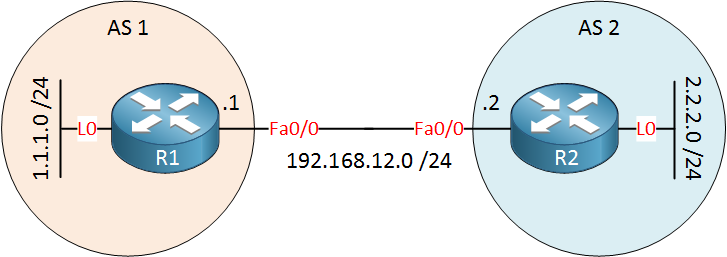
# This captures 1 packets from Switch to Internet BGP Router

# In order to make this BGP hack work

**# We need to know Src & Dst ports**

# BGP uses TCP port 179

# Yet this depends on which BGP Router initiates the session



# Assume we have 2 BGP Routers

# BGP Router A (left) & BGP Router B (right)

# If BGP Router A (left) initiates the session to BGP Router B (right)

# BGP Router B (right) has dstPort = 179 on itself

# If BGP Router B (right) initiates the session to BGP Router A (left)

# BGP Router A (left) has dstPort = 179 on itself

**# Simply saying:**

**# The BGP Router that initiates Session to another BGP Router**

**# has a randomPort, while the BGP Router that receives initiation of a Session has dstPort**