**Student Name:** **Weight: \_\_\_\_2.5\_\_\_\_%**

**Student ID:** **Marks: \_\_\_\_\_\_\_\_\_\_**

Lab 3: Advanced Routing Protocols

# Learning Outcomes

* Configure BGP.
* Learn how to do basic security of the BGP protocol.

# Tools

* Cisco Switches Configuration (Setup document)
* Cisco Routers Configuration (Setup document)
* Win10 with Loki (Setup document)

# Topology

|  |
| --- |
|  |

Reading

RFC4271 BGP Protocol 4 <https://tools.ietf.org/html/rfc4271>

Cisco documentation https://www.cisco.com/c/en/us/about/security-center/protecting-border-gateway-protocol.html

BGP Wiki <https://en.wikipedia.org/wiki/Border_Gateway_Protocol>

References

<https://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t2/htmsdpmd.html>

<https://security.stackexchange.com/questions/56069/what-security-mechanisms-are-used-in-bgp-and-why-do-they-fail>

Introduction

1. Perform setup instructions from ITSC\_M3\_Lab3\_AdvancedRoutingProtocol-Setup.docx using Initial BGP Switch Setup steps
2. Confirm connectivity between routers by issuing the ping command from one router to the next:

RouterA#ping 10.200.100.2

Are you getting a response? If not troubleshoot up the IP stack:

1. Question: Physical cable between both routers? \_\_\_\_\_\_\_\_
2. Question: Is the interface on the router up? \_\_\_\_\_\_\_\_\_\_
3. Question: Is the mask set to 8 bit? \_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. If you issue the command sh ip route on RouterA, you should see in your routing table

|  |
| --- |
| Insert evidence here |

# Loki.exe

Before you begin the lab activities, perform the steps below to set up your computer.

1. Ensure Kali with Loki is connected to switch with the following parameters.

* Network Adapter: LAN Segment 1
* Configure the IP address to: 172.16.0.4/24
* Configure the gateway to: 172.16.0.254

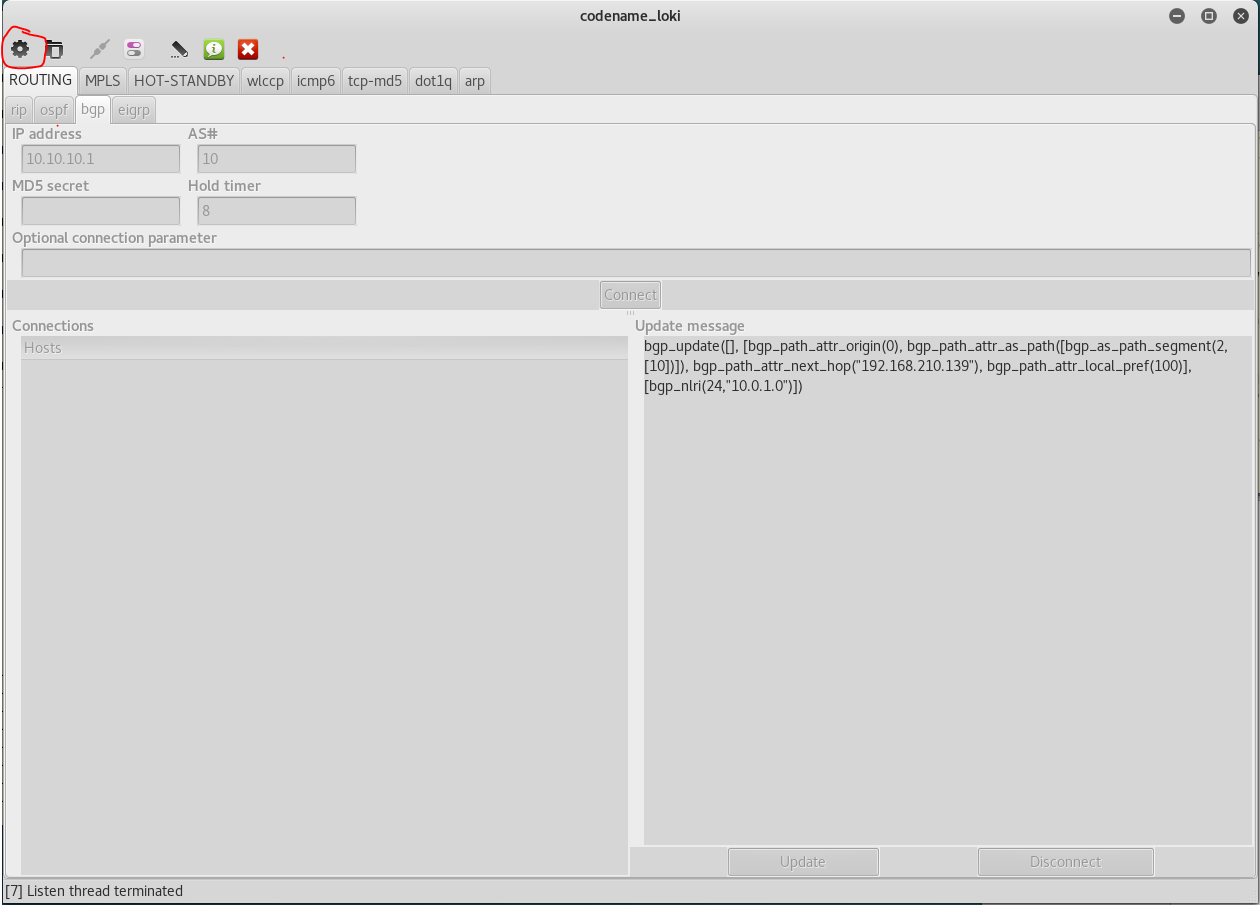
1. Run Loki: **from desktop loki.exe of Win10**.

BGP Attack

Using Loki to Attack BGP

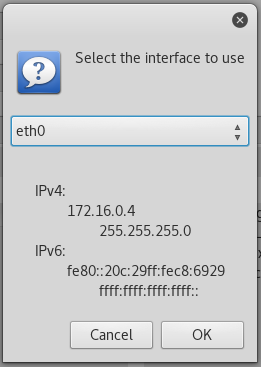
1. BGP does not have any native security mechanisms

* there are no mechanisms internal to BGP that protect against attacks that modify, delete, forge, or replay data, any of which has the potential to disrupt overall network routing behavior. As a TCP/IP protocol, BGP is subject to all TCP/IP attacks, e.g., IP spoofing, session stealing, etc. Any outsider can inject believable BGP messages into the communication between BGP peers, and thereby inject bogus routing information;
* When a router advertise new routing information, BGP does not ensure that it uses the AS number it has been allocated, which means a BGP router can advertise routes with any AS number;
* An AS can advertise a prefix from address space unassigned by or belonging to another AS. This is called prefix hijacking and it can be used to perform man-in-the-middle attack which was initially demonstrated at DefCon 16 by Alex Pilosov and Anton "Tony" Kapela;
* BGP does not provide a shared, global view of correct routing information that would make it much easier to detect invalid or malicious routes.

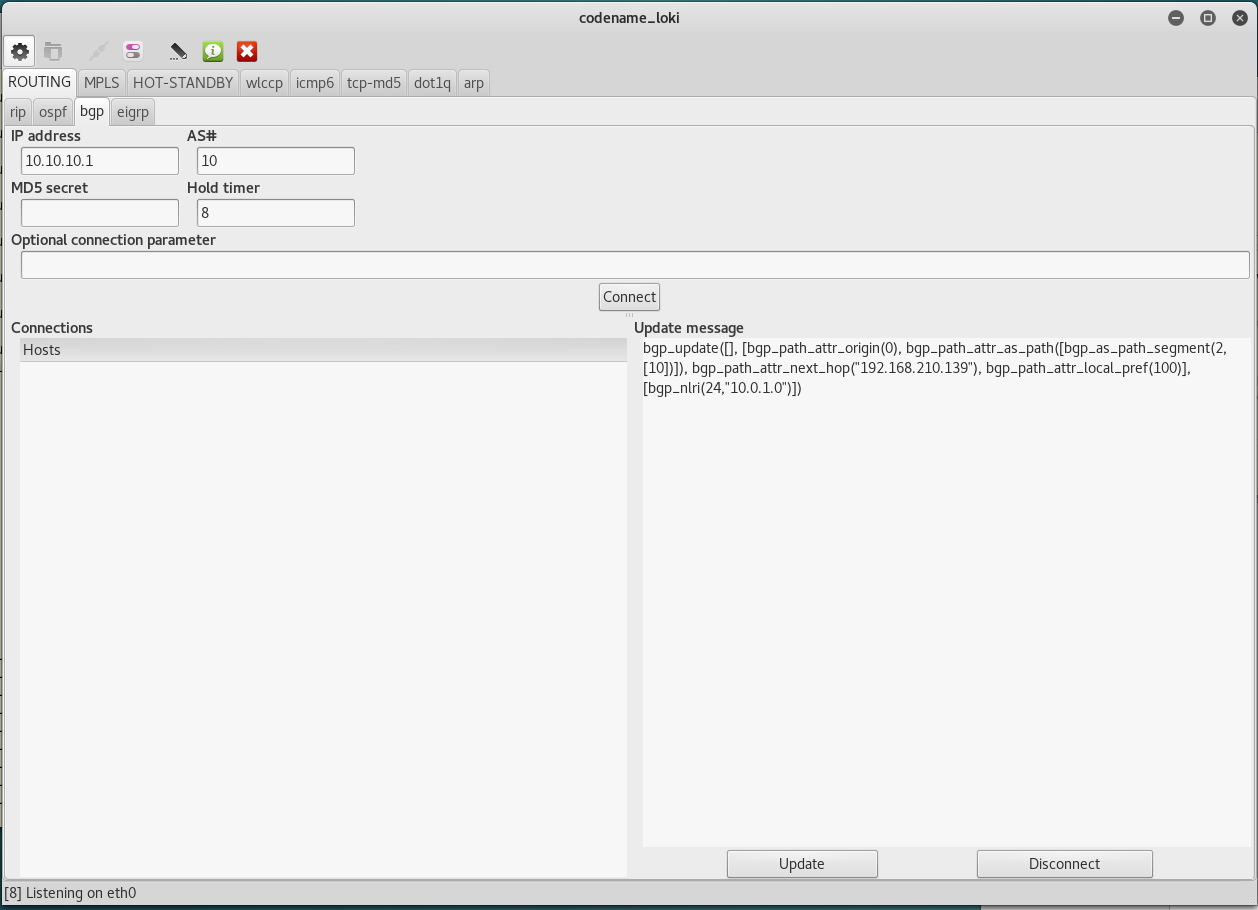


Loki on initialization, click on Run (top left)

Select the working network interface



Select interface associated with correct IP



If it is working properly, sniffing BGP connections, there will be host in the lower left pane else it will be empty, edit the IP address (top left) with 10.200.200.1 or 10.100.200.1 and click Connect (middle center).

Gather evidence to prove Loki worked otherwise

If this isn’t working for you, review the pcaps for the questions below.

From bgp.pcap

1. Question: What protocol & port (layer 4) does BGP communicate on: TCP or UDP \_\_\_\_\_\_
2. Question: First Open Message contains what AS: \_\_\_\_\_
3. Question: Within the update message, what is the Aggregator AS and origin: \_\_\_\_\_\_\_\_\_\_
4. From bgp\_shutdown\_communication.pcap

Question: In the Keepalive message, is there anything that identifies the source AS: \_\_\_\_\_\_\_\_\_\_

Question: In the notification message, is there any ISP or contact details: \_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

BGP Hardening

1. We can authenticate the neighboring peers

On RouterA and Router B add the following commands:

RouterA#conf t

RouterA(config)#ip msdp peer 10.200.200.1

RouterA(config)#ip msdp password peer 10.200.200.1 0 bgppasswd

RouterA(config)#end

RouterB#conf t

RouterA(config)#ip msdp peer 10.100.200.1

RouterA(config)#ip msdp password peer 10.100.200.1 0 bgppasswd

RouterA(config)#end

1. Additionally, there is TTL security (read about it http://packetlife.net/blog/2009/nov/23/understanding-bgp-ttl-security/)

This is ensuring that the routers you peer with are using the number of hops between yourselves as an authentication factor. This works if the network is static and there are no changes to the hops required.

Gather evidence to prove Loki worked after implemented hardening

OSPF Attack

Using Loki to Attack OSPF

# Purpose

In this lab, you will look at route manipulation using a tool called Loki to inject routes into OSPF routing protocols.

# Tools

* Cisco Switch Configuration (Setup document)
* Cisco Router Configuration (Setup document)
* Kali with Loki (Setup document)

# Topology

|  |
| --- |
|  |

1. Lab Outcomes

* Configure OSPF.
* Learn how to do basic security of the OSPF protocol.

Reading

RFC2328. OSPF Version 2. <http://www.ietf.org/rfc/rfc2328.txt>

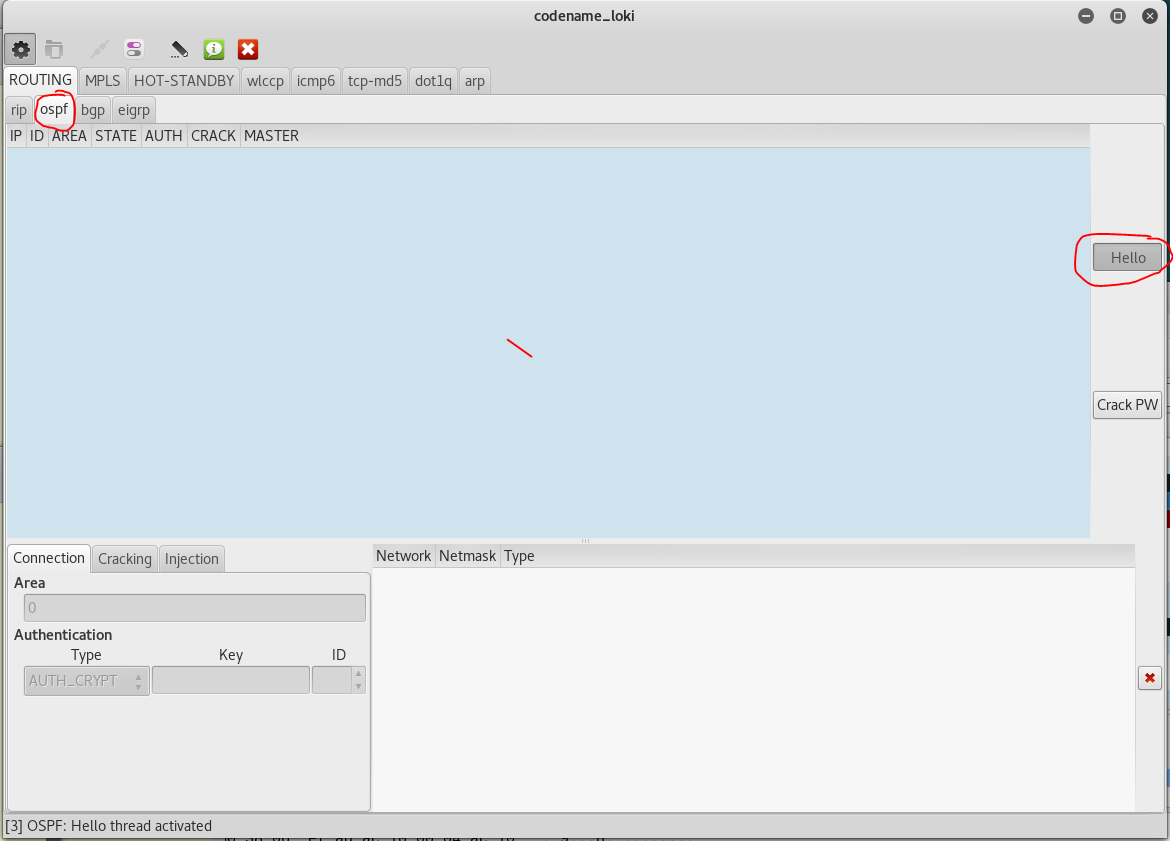
Cisco documentation. <http://www.cisco.com> and <http://www.cisco.com/warp/public/104/2.html#6.0>

RFC1321. The MD5 Message-Digest Algorithm - <http://www.ietf.org/rfc/rfc1321.txt>

OSPF: Anatomy of a Routing Protocol. John T. Moy. Addison-Wesley. 1998.

## Perform OSPF LSA Injection

1. Use Loki as above to listen to the OSPF exchange routing information. (injection of LSAs)



1. Demonstrate that you can use Loki to poison a route to 8.8.8.8/32 with a next hop of 172.16.4.254 and a metric of 16.
2. From an IOS device, issue a ping to 8.8.8.8.
3. Demonstrate in Wireshark that the ping to 8.8.8.8 does not arrive at the Kali network interface.
4. If the above doesn’t work then answer the following questions:

From ospf.cap

* 1. Question: Notice Hello packets, how many are there? \_\_\_\_\_
  2. Question: What is the area ID? \_\_\_\_\_\_\_\_
  3. Question: What is the highest sequence number? \_\_\_\_\_\_\_\_\_\_
  4. Question: What is the metric associated with above update? \_\_\_\_

## Configure an OSPF MD5 Authentication Cracking

1. Configure the OSPF routing protocol on your IOSv devices.

Note: Include networks 172.16.0.0/22 on Area 0.

1. Do not configure authentication.
2. Demonstrate in the routers that the OSPF routing protocol is exchanging routing information.
3. Gather evidence to prove Loki worked

## Perform OSPF Injection

1. Use Loki to listen to the OSPF exchange routing information.
2. Set Loki to use Area 0 and AUTH\_NONE.
3. Send Hello to OSPF routers.
4. Wait for Loki to establish OSPF routing with OSPF routers.

Note: The State should be FULL.

1. Confirm that Loki can see all routing information from the OSPF routers.
2. Demonstrate that you can use Loki to inject a route to 0.0.0.0/0.
3. Gather evidence to prove Loki worked

OSPF Hardening

1. Now, we have to secure the OSPF interfaces as ANY router on the same network as FastEthernet0 or FastEthernet1 can inject routes into the OSPF tables, and learn routes as well.

We will introduce passive interfaces that donot need to participate in an OSPF area and we will introduce authentication for OSPF neighbours.

On RouterA and Router B add the following commands:

RouterA#conf t

RouterA(config-router)#router ospf 10

RouterA(config-router)#passive-interface default

RouterA(config-router)#int Fa0

RouterA(config-if)#ip ospf authentication message-digest

RouterA(config-if)#ip ospf message-digest-key 1 md5 ospfpasswd

RouterA(config-if)#end

RouterB#conf t

RouterB(config-router)#router ospf 10

RouterB(config-router)#passive-interface default

RouterB(config-router)#int Fa0

RouterB(config-if)#ip ospf authentication message-digest

RouterB(config-if)#ip ospf message-digest-key 1 md5 ospfpasswd

RouterB(config-if)#end

Gather evidence to prove Loki worked after implemented hardening

Other Tools – extra points

Attempt to use Scapy with scapy\_ospf.py with ospf.cap file to learn more tools. See link to use add-on <http://scapy.readthedocs.io/en/latest/extending.html> and <https://bitbucket.org/secdev/scapy/wiki/contrib/code/OSPF>, hint #python scapy\_ospf.py