
# BGP Hijacking Analysis

**James Hemmings**

## Computer Networking 2 – White Paper

## University of Abertay Dundee

## BSc (Hons) Ethical Hacking

## 2016

*Note that Information contained in this document is for educational purposes.*

# Abstract

The current internet backbone is still primarily using the Border Gateway Protocol (BGP), to connect autonomous systems across cyberspace. However, due to the increased demand and current security threats associated with the internet, it has been noted that BGP has inherited security configuration limitations which have not been addressed, which is not suitable for a more secure internet going forward.

Recent high-profile BGP hijacking attacks have been noted to be exploiting the trusted routing model of BGP, which has demonstrated there are fundamental conceptual flaws with the very foundations of internet infrastructure. The most recent high-profile case of BGP hijacking was where a Pakistani Internet service provider null-routed traffic to YouTube, and leaked the BGP route outside of Pakistan causing YouTube not to be accessible from around the world.

BGP hijacking attacks are limited to performing Denial of Service Attacks (DoS), and man in the middle attacks against plaintext communications. By implementing TLS/SSL technologies across the internet, it ensures that traffic cannot be intercepted easily by this attack.

This white paper will provide the basic underpinning knowledge of BGP, and then identify the existing conceptual flaws in BGP, and highlight the malicious attacks that can be used against the BGP protocol, their security implications and the current methods of preventing such attacks to routers, and internet infrastructure.

# Table of Contents

# Introduction

BGP has been in use as the underpinning routing protocol for the Internet since 1994 and was conceptually developed with a trusted routing model in mind. However as the internet has progressed and malicious cyber-attacks for profit, fun and surveillance have increased, the trusted routing model is obsolete, as all autonomous systems are not to be considered as "trusted" by default.

Recent high profile BGP hijacking attacks have shown the dangers of the attack, such as by Turk Telekom on March 29th, 2014. Turkey attempted to censor Turkish internet by blocking Google DNS, Level 3 DNS, and Open DNS[5]. However, after enforcing the IP null route within Turkey the route was selected by peers as they had a more specific route, this caused the bogus route to be selected and sent to a DNS server within Turkey for interception and then censorship.

Other high profile cases of BGP hijacking have been for monetary gains, such as the February 3rd, 2014 Bitcoin hijacking attack which originated from an autonomous system in Canada, where malicious attackers intercepted traffic from multiple large providers such as Amazon, OVH, Digital Ocean, Lease Web, Alibaba and more [6]. It then resulted in cryptocurrency miners being redirected, to a hijacker-controlled mining pool with the total stolen profit value allotting to over $83,000 over a four-month period [7].

The inherent trust by default model of BGP is not sustainable for the future of the global internet, as there are foreign nation states and individuals who wish to use internet routing infrastructure for censorship, monetary gain, mass surveillance, and other nefarious means.

The aim of this project is to investigate the current methods of BGP Hijacking, their countermeasures as well as providing a demonstration and proof of concept of this attack using virtual Cisco routers and infrastructure with GNS3.

The following objectives were identified for this whitepaper:

- Investigate and describe the BGP 4 protocol.
- Investigate and analyse current BGP hijacking security flaws, and attack vectors.
- Setup up and configure, a proof of concept demonstration using GNS3 and virtual Cisco routers.
- Discuss and analyse currently available countermeasures and their effectiveness.

# BGP Background Information

Border Gateway Protocol (BGP) is the routing protocol of the Internet backbone as we know it today, and is used primarily across the global internet to inter-connect Autonomous Systems (AS's), and thus can handle the complex task of global Internet routing. The current version in use is BGP version 4 based on RFC4271[1].

The main function of the BGP protocol is to exchange routing and network reachability information between other autonomous systems (AS)[2] across the internet. The reachability information is then used for constructing graphs of AS connectivity to other AS's and enables routing loops to be removed from the network, and enforces policy decisions on the AS level. In addition to this, BGP can be used to route within an Autonomous System (AS), commonly referred to as Interior Border Gateway Protocol or Internal BGP, whereas otherwise it is known as eBGP (Exterior Border Gateway Protocol) when routing between another AS.

BGP commonly uses Classless Inter-Domain Routing (CIDR)[3] and supports advertising destinations as an IP prefix, which negates the concept of "Network Class's" within the BGP protocol. In addition to the above, BGP uses TCP (Port 179) as it is a transport protocol to ensure reliability, and eliminates the need for BGP to implement update fragmentation, retransmission, acknowledgement, and sequencing [1]. In addition to this, BGP is a layer four protocol that sits on top of TCP.

## BGP Messages

When BGP establishes a TCP connection, the first message that is sent by each Autonomous System is an "OPEN" message[1], if the message is valid a "KEEPALIVE" message confirming the "OPEN" state is then sent back to the other AS.

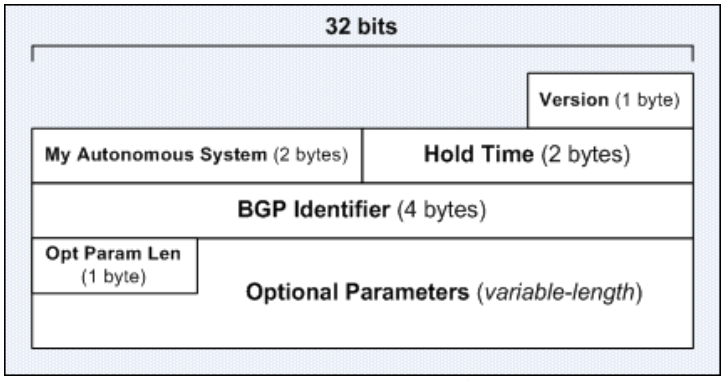


*Figure 1 – BGP OPEN message format [16].*

The route advertisement process of BGP uses a "UPDATE" message to advertise a route between BGP peers, and then once the BGP session is initialized the "UPDATE" messages are sent until the complete BGP table has been exchanged between peers, this causes for the BGP route table version number to be incremented by one each time. Additionally, a route can be withdrawn in the "Withdrawn Routes Field" of the UPDATE message [1]

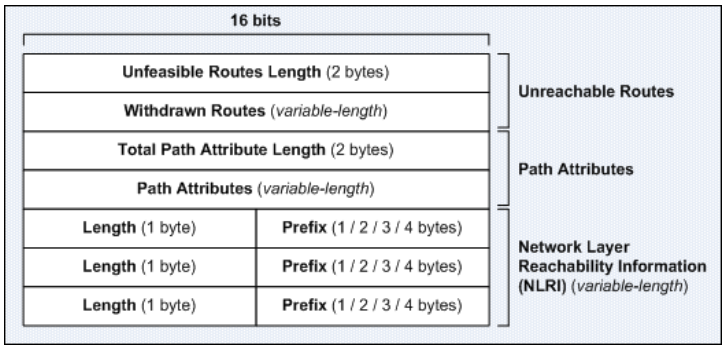


*Figure 2 – BGP UPDATE message format [16].*

BGP "NOTIFICATION" messages are sent by the router when an error condition is detected, causing the connection to be closed immediately.

Prefixes are announced within the BGP protocol to define the path of autonomous systems the traffic must transverse, to reach the announced IPv4 or IPv6 address blocks which contain CIDR block network information and mask. The prefix is usually carried in Network Layer Reachability Information (NLRI) in a BGP UPDATE message. For example, a BGP prefix would be (IPV4): **701 1239 42** 204.10.12.0/24. As identified in the bold text example, the AS numbers have been separated by a space which demonstrates the path network traffic transverses through to reach the specified IP prefix, ensuring the correct route is used to reach the network. The /24 within the prefix is the CIDR mask which indicates the first 24 bits are used for the network part of the address block.

## BGP Path Selection

BGP is also a path vector protocol which is used to span different autonomous systems, the routing table is used to store autonomous systems that are traversed, to reach the destination network, this forms a directed route for packets to travel across the internet from source to destination. Neighbouring autonomous systems also use BGP to exchange update messages about how to reach various AS prefixes. Each AS router decides on the best path to the destination network, which will then be sent to peers along with other metrics. AS's may not advertise the route suggested due to organisation routing policy which is based on path attributes as described below [8].

BGP uses a path selection algorithm which assigns various attributes to each path, it then can be manipulated to control the path that is selected. BGP examines the value of the said attributes in an ordered manner until it can narrow down the possible routes to one path [8].

## BGP Attributes

BGP attributes are sent in the "UPDATE" message and are handled by BGP to pick the best route to a destination AS, which is similar to how metrics are used in OSPF and EIGRP, as they are commonly used as a deciding factor on the selected route.

The four BGP attribute categories and their meanings are listed below:

- **Well-known, Mandatory:** Must exist in the BGP "UPDATE" message, if the attribute is missing then a "NOTIFICATION" error is generated, and the BGP session closed.
- **Well-known, Discretionary:** Attribute must be recognised by BGP, however, it does not need to be included in all BGP "UPDATE" messages.
- **Optional, Transitive:** Not required to be recognised by BGP routers, however, it must be accepted and passed to peers if the transitive flag has been set.
- **Optional, Nontransitive:** Not required to be recognised by BGP routers, however, if the transitive flag has not set then it should be ignored and not passed to peers.

The BGP attributes figure below, describes some of the common path attributes which are used in BGP path selection process:

| Attribute | Meaning |
|---|---|
| AS_PATH | An ordered list of all autonomous systems that the BGP update has been through. Well-known, mandatory. |
| ORIGIN | The origin of how BGP learned of the said network. E.g (i = by network command, e = From EGP , ? = redistributed from another source). Well-known, mandatory. |

| | |
|---|---|
| LOCAL_PREF | Used as a value to tell IBGP peers which path to select for traffic leaving the AS. Well-known, discretionary. |
| MULTI_EXIT_DISC(MED) | MED allows the AS to inform immediate neighbour AS's of its preferred entry points. MED is also used as a metric, and the lowest value of the MED is the most preferred one. Optional, non-transitive. |
| NEXT_HOP | Specifies the next hop IP address to reach the destination, as advertised in the NLRI. Well-known, mandatory. |
| ATOMIC_AGGREGATE | Performs route aggregation on the routes that are non-identical but do point to the same destination, this in effect summarises the routes when being advertised to a BGP peer. Well-known, discretionary. |

*Figure 2 - BGP attributes & meanings [8].*

## Limitations of BGP

BGP has three primary limiting factors which can be used for nefarious means. However, it is not in itself a vulnerability and more of a conceptual flaw in the design of the protocol.

- **BGP Integrity:** Currently there is no protection against the tampering of data within the BGP protocol, or origin authentication of messages and freshness. Integrity usually ensures that a message has not been altered or tampered with, and freshness ensures that the recipient has not revived a new BGP message, or that it has been replayed. In addition to this, the origin authentication ensures the message is not fraudulent.

- **BGP Validation:** BGP does not validate the autonomous system's authority to announce a specific network, and this can cause issues regarding path subversion, as it can announce that it is the shortest path to the route even if it is not directly in the autonomous system destination path.

- **BGP Trust:** BGP does not currently ensure the that the path attributes announced by an AS are authentic. By altering path attributes, a malicious AS or threat actor can manipulate core routing infrastructure.

# BGP Hijacking Overview

BGP hijacking is the process of manipulating BGP routes by nefarious means or misconfiguration, allowing for the interception or modification of traffic. BGP hijacking performed on the internet level is accomplished by configuring a rouge border router to announce prefix's that have not been assigned to that AS. In addition to this, when the malicious BGP prefix is more specific than the legitimate prefix or misrepresents itself as a shorter path, then the prefix will be accepted, and network traffic routed to the malicious AS.

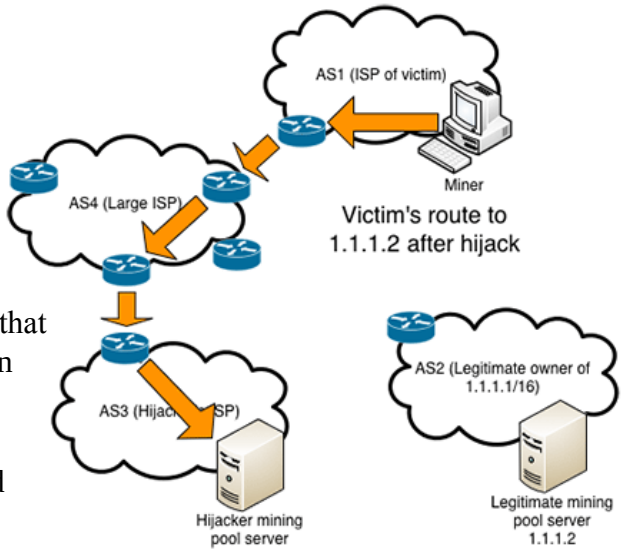


*Figure 3 - BGP hijacking example [7].*

Due to the lack of security with authenticating BGP announcement messages as the true source, then the hijacked prefix can propagate into peer BGP routing tables and poison the Routing Information Base (RIB) of peer AS's which then is further spread to their peers and throughout the global internet. As shown in figure four, it is demonstrated how it can be leveraged to perform a man in the middle attack.

Over the course of several years, there has been a steady amount of BGP hijacking incidents for nefarious means as well as misconfiguration errors, or incidents with unknown intent. It is not uncommon for spammers to use BGP hijacking on unused autonomous systems and IP address space to send out spam email and then rotate to using other hijacked IP address space, which has been primarily used as to avoid detection[9]. In addition to this, other BGP incidents have been for nefarious means such as the bitcoin mining hijack which stole at least $83,000' worth of bitcoins from multiple mining pool websites, by hijacking Bitcoin mining clients onto a hijacked mining pool. During the attack, the threat actor used AS path prepending in an attempt to hide the attack with a range of autonomous systems [6].

It is not only spammers and criminals that use BGP hijacking either, during 2015 it was identified after a breach of Hacking Team company emails, that the Italian government was working with Hacking Team and an Italian ISP to perform BGP hijacking. After the network hosting the command & control (C&C) server went down, the malware communicating with the command and control server were unreachable by the infected machines. After performing the BGP hijack, Hacking Team was able to re-establish access to the command and control server and the infected machines [10]. There have not been any other cases of western government's using BGP hijacking to date, or that was publicly disclosed.

Unfortunately, to this day, there has not been any improvements to the BGP protocol that are feasible and prevent the issues identified above. Although some security countermeasures do exist, they do not prevent all BGP attacks and most ISP's and autonomous systems do not implement them on their networks. However, BGP monitoring services can monitor and detect for BGP hijacking attacks and raise the alarm when this happens, though not all autonomous systems sign up to these services.

## Configuring BGP Environment

The aim of the following section is to walk the reader through the process and configuration, of a virtual network environment in GNS3, using Cisco routers along with Windows and Linux virtual machines. Once this has been achieved, the process of performing a BGP hijacking attack was be demonstrated, by directing the user's request to the malicious web server that has been set up,

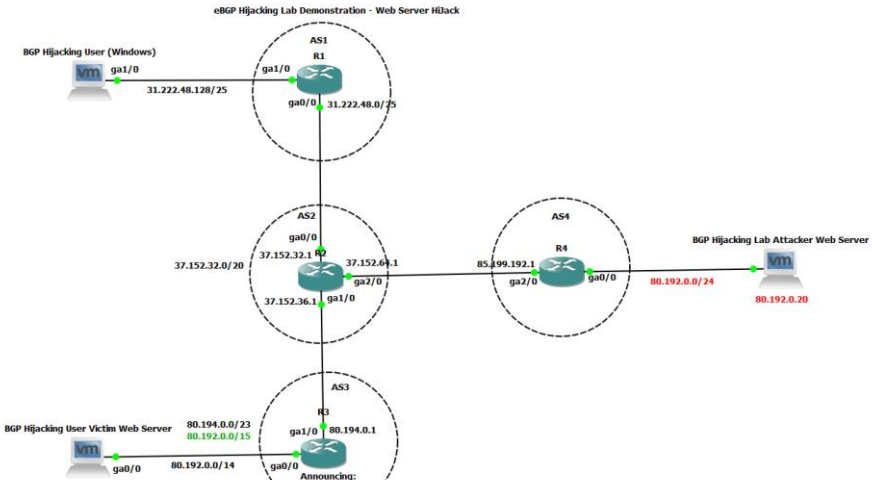


*Figure 4 – GNS3 virtual network topology.*

with the use of malicious BGP route advertisements.

## BGP Network Topology

It was identified for this whitepaper that, to test the functionality and security implications of BGP hijacking, that a lab network using GNS3[11] and virtual machines would be configured, and then a BGP hijacking attack performed to demonstrate the feasibility and effectiveness.

In figure four, the network topology example is using four routers and autonomous systems (AS1000, AS2000, AS3000, and AS4000) along with Cisco C7200 virtual routers running software version 15.2(4)S5.

The victim virtual host PC is running Windows 10 Pro 64bit. In addition to this, both the legitimate web server and malicious web server will be running TurnKey Linux (Debian Jessie 8.4), which includes a prebuilt LAMP stack (Nginx, MySQL, PHP-FastCGI) primarily for ease of setup and speed of configuration. The base hypervisor for the virtual machines will be running VMWare Workstation 12 Pro (12.5.1), along with GNS3 1.5.2 for Cisco network simulation.

## Router 1 BGP Configuration

The first step for configuring BGP routing is by setting the autonomous system number, along with BGP peers (neighbours). The neighbour IP address of 37.152.32.1 is the next hop router IP address. Connectivity checks have to be disabled, due to the router being on a different subnet, and network, without this the neighbour configuration would fail to connect once both sides are configured.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router bgp 1000
R1(config-router)#neighbor 37.152.32.1 remote-as 2000
R1(config-router)#neighbor 37.152.32.1 disable-connected-check
R1(config-router)#end
R1#
```

*Figure 5 – BGP peering configuration.*

After BGP peering has been configured, route advertisements need to be set up for both networks on AS 1000 (37.152.48.0/25, 37.152.48.128/25). This ensures that other autonomous systems, know that AS1000 has the destination of both networks.

```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router bgp 1000
R1(config-router)#network 31.222.48.0 mask 255.255.255.128
R1(config-router)#end
R1#
*Oct 28 23:00:24.103: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

*Figure 6 – Router one, BGP route advertisements.*

```
R1(config)#router bgp 1000
R1(config-router)#network 31.222.48.128 mask 255.255.255.128
R1(config-router)#end
R1#
*Oct 28 23:01:09.123: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

*Figure 7 – Route advertisement.*

Before the routes advertise and route correctly, a static route needs to be created. Without a static route to the next hop network or a route that was previously learned via internal BGP, then the route will not be advertised to other autonomous systems.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 37.152.32.0 255.255.254.0 GigabitEthernet0/0
R1(config)#end
R1#
*Oct 28 20:05:41.275: %SYS-5-CONFIG_I: Configured from console by console
*Oct 28 20:05:42.075: %BGP-5-NBR_RESET: Neighbor 37.152.32.1 active reset (BGP N N
otification sent)
*Oct 28 20:05:42.079: %BGP-5-ADJCHANGE: neighbor 37.152.32.1 Up
```

*Figure 8 – Static route & neighbour configuration.*

## Router 2 BGP Configuration

Firstly, BGP peers (neighbours) need to be configured for the following autonomous systems (AS1000, AS3000, AS4000). Each neighbour IP address is the next hop router IP address from AS2000. Connectivity checks are to be disabled as without the configuration then, the BGP peering session would not establish due to the networks being on different subnets and IP ranges.

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router bgp 2000
R2(config-router)#neighbor 31.222.48.1 remote-as 1000
R2(config-router)#neighbor 31.222.48.1 disable-connected-check
R2(config-router)#neighbor 85.199.192.1 remote-as 4000
R2(config-router)#neighbor 85.199.192.1 disable-connected-check
R2(config-router)#neighbor 80.194.0.1 remote-as 3000
R2(config-router)#neighbor 80.194.0.1 disable-connected-check
R2(config-router)#end
```

*Figure 9 – BGP Neighbour configuration.*

The next step would be to configure BGP route advertisements, three routes need to be advertised on AS 2000 (37.152.36.0/23, 37.152.64.0/23, 37.152.32.0/23).Which ensures that the other autonomous systems have the route to the networks on AS2000.

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router bgp 2000
R2(config-router)#network 37.152.36.0 mask 255.255.254.0
R2(config-router)#network 37.152.64.0 mask 255.255.254.0
R2(config-router)#network 37.152.32.0 mask 255.255.254.0
R2(config-router)#end
R2#
```

*Figure 10 – Route advertisement.*

Before the routes advertise and route correctly, a static route needs to be created, as without a static route to the next hop network or a route that was previously learned via internal BGP, then the route will not be advertised to other autonomous systems.

```
R2(config)#ip route 85.199.192.0 255.255.254.0 Gigabite2/0
R2(config)#ip route 80.194.0.0 255.255.254.0 Gigabite1/0
R2(config)#
```

*Figure 11 – Static route configuration.*

```
R2(config)#ip route 31.222.48.0 255.255.255.128 Gigabite0/0
R2(config)#end
R2#
*Oct 28 23:05:35.239: %SYS-5-CONFIG_I: Configured from console by console
R2#
```

*Figure 12 – Static route configuration.*

## Router 3 BGP Configuration

With the two interfaces being configured, BGP needs to be set up by configuring the BGP peers (neighbours) along with the autonomous system number of the remote AS (AS2000). The neighbour IP address is the next hop router IP address from AS3000. Connectivity checks are to be disabled as without this setting then, the BGP peering session would not establish due to the networks being on different subnets and IP ranges.

Before the routes will advertise and route correctly, a static route needs to be created, as without a static route to the next hop network or a route that was previously learned via internal BGP, then the route will not be advertised to other autonomous systems.

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router bgp 3000
R3(config-router)#neighbor 37.152.36.1 remote-as 2000
R3(config-router)#neighbor 37.152.36.1 disable-connected-check
R3(config-router)#ip route 37.152.36.1 255.255.254.0 GigabitEthernet1/0
%Inconsistent address and mask
R3(config)#ip route 37.152.36.0 255.255.254.0 GigabitEthernet1/0
R3(config)#end
```

*Figure 13 – Neighbour & static route configuration.*

The final step would be to configure BGP route advertisements using the network command, and then two routes need to be advertised on AS 2000 (80.192.0.0/15, 80.194.0.0/23). Which ensures that the other autonomous systems have the route to the networks on AS3000.

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router bgp 3000
R3(config-router)#network 80.192.0.0 mask 255.254.0.0
R3(config-router)#network 80.194.0.0 mask 255.255.254.0
R3(config-router)#end
```

*Figure 14 – Route advertisement.*

## Router 4 BGP Configuration

Next, BGP peering (neighbours) need to be configured on the Cisco router, then the next hop router is 37.152.64.1 with an AS of 2000 as shown below. Connectivity checks are to be

disabled as without this setting, then the BGP peering session would not be established due to the networks being on different subnets and IP ranges.

```
R4#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#router bgp 4000
R4(config-router)#neighbor 37.152.64.1 remote-as 2000
R4(config-router)#neighbor 37.152.64.1 disable-connected-check
R4(config-router)#end
```

*Figure 15 – Neighbour configuration.*

Finally, a static route will need to create to the next hop router interface IP from GigabitEthernet2/0. The static route must be configured, as without this then BGP will not have the route stored in internal routing tables and must be learned by either internal BGP or a static route.

```
R4(config)#ip route 37.152.64.0 255.255.254.0 GigabitEthernet2/0
R4(config)#end
R4#
*Oct 28 20:04:18.867: %SYS-5-CONFIG_I: Configured from console by console
R4#
*Oct 28 20:04:22.211: %BGP-5-NBR_RESET: Neighbor 37.152.64.1 active reset (BGP N
otification sent)
*Oct 28 20:04:22.211: %BGP-5-ADJCHANGE: neighbor 37.152.64.1 Up
```

*Figure 16 – Static route configuration.*

# BGP Hijacking Results

In this section, a BGP Hijacking attack is performed against a pre-configured virtual network in GNS3. The proof-of-concept demonstrates the threats and security implications of BGP hijacking attacks.

The network topology from figure five identified that the target is three hops away from the host machine, and two hops away from our target machine. In addition to this, the victim network/AS is advertising 80.192.0.0/15. By looking at this information, it can be identified that a more specific network advertisement such as "/24" would enable the attacker to perform a BGP Hijacking attack, primarily due to how the Cisco best path selection algorithm determines the best route to an AS [4].

It is important to understand for this proof of concept, that AS4000 is a compromised rouge peer and remote access to the router was obtained. This type of BGP hijacking attack cannot be performed without an attacker compromising a legitimate peer or the legitimate network operators of that AS turn rouge and perform nefarious attacks or accidental misconfiguration of the BGP protocol. BGP attacks without access to a peer can be performed. However, that is not within the scope of this whitepaper.

## Performing BGP Hijacking Attack

The following figure displays all routes in the BGP routing table, after identifying the route from AS 2000 to AS 3000 and the network of 80.192.0.0/15 in the table, then this information can be used to perform the BGP hijacking attack. As a /15 network is less

specific than a /24 network, it's possible to advertise 80.192.0.0/24 and perform the BGP hijack, causing the BGP to select the more specific route.

```
R4#show bgp
BGP table version is 9, local router ID is 85.199.192.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  31.222.48.0/25   37.152.64.1                            0 2000 1000 i
 *>  31.222.48.128/25 37.152.64.1                            0 2000 1000 i
 *>  37.152.32.0/23   37.152.64.1                 0          0 2000 i
 *>  37.152.36.0/23   37.152.64.1                 0          0 2000 i
 r>  37.152.64.0/23   37.152.64.1                 0          0 2000 i
 *>  80.192.0.0/15    37.152.64.1                            0 2000 3000 i
 *>  80.194.0.0/23    37.152.64.1                            0 2000 3000 i
 *>  85.199.192.0/23  0.0.0.0                     0      32768 i
```

*Figure 17 – Cisco Show BGP results.*

In the figure shown below, it displays the AS 4000 IP routes in our control before performing the BGP hijacking attack. In addition to this, the route of 80.192.0.0/24, and 80.192.0.1/32 are displayed in the local routing table. However, the route has not been advertised in BGP, and will not be sent to other autonomous systems.

```
R4#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      31.0.0.0/25 is subnetted, 2 subnets
B        31.222.48.0 [20/0] via 37.152.64.1, 02:20:35
B        31.222.48.128 [20/0] via 37.152.64.1, 02:20:35
      37.0.0.0/23 is subnetted, 3 subnets
B        37.152.32.0 [20/0] via 37.152.64.1, 02:20:35
B        37.152.36.0 [20/0] via 37.152.64.1, 02:20:35
S        37.152.64.0 is directly connected, GigabitEthernet2/0
      80.0.0.0/8 is variably subnetted, 4 subnets, 4 masks
B        80.192.0.0/15 [20/0] via 37.152.64.1, 02:20:35
C        80.192.0.0/24 is directly connected, GigabitEthernet0/0
L        80.192.0.1/32 is directly connected, GigabitEthernet0/0
B        80.194.0.0/23 [20/0] via 37.152.64.1, 02:20:35
      85.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        85.199.192.0/23 is directly connected, GigabitEthernet2/0
L        85.199.192.1/32 is directly connected, GigabitEthernet2/0
```

*Figure 18 – Cisco show route ip results.*

Next, we will perform a trace route using command prompt from the victim host virtual machine to the victim web server at 80.192.0.20. The figure below displays the correct route to the web server with no BGP hijacking attack in place.

```
C:\Users\User>tracert 80.192.0.20

Tracing route to 80.192.0.20 over a maximum of 30 hops

  1     2 ms     9 ms     8 ms  31.222.48.129     AS1000
  2    26 ms    19 ms    17 ms  37.152.32.1       AS2000
  3    37 ms    31 ms    43 ms  80.194.0.1        AS3000
  4    35 ms    41 ms    41 ms  80.192.0.20       AS3000
                                                  (Legitimate Web Server)
Trace complete.
```

*Figure 19 – Windows trace route (pre-hijack).*

The figure below shows the legitimate web server's HTML page before the BGP hijacking attack has been performed.


*Figure 20 – Legitimate web server (Nginx).*

The next step is to advertise the target network, which in this case would be 80.192.0.0, with a subnet mask of 255.255.255.0 which is a /24 network. As the route is more specific than a /15 prefix, then it will be accepted by the next hop and further spread out to other BGP peers, which will poison the routing information base (RIB) of other autonomous systems.

```
R4#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#router bgp 4000
R4(config-router)#network 80.192.0.0 mask 255.255.255.0
R4(config-router)#end
R4#
*Nov  2 17:42:17.762: %SYS-5-CONFIG_I: Configured from console by console
R4#
```

*Figure 21 – Route advertisement configuration.*

After advertising the hijacked BGP route, a static route needs to be created on Router four before the route will be advertised to other autonomous systems, as shown in the figure below.

```
R4#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#ip
*Nov  2 23:08:44.589: %SYS-5-CONFIG_I: Configured from console by console
R4(config)#ip route 80.192.0.0 255.255.255.0 37.152.64.1
R4(config)#end
```

*Figure 22 – Static route configuration.*

After adding a static route in the previous step, then the BGP hijack will have started to poison the RIB (Routing Information Base) of other autonomous systems. As identified below, hop three is now AS4000, rather than AS3000, which confirms the BGP hijack has been successful.

```
C:\Users\User>tracert 80.192.0.20

Tracing route to 80.192.0.20 over a maximum of 30 hops

  1     3 ms     9 ms     9 ms  31.222.48.129      AS1000
  2    21 ms    20 ms    19 ms  37.152.32.1        AS2000
  3    33 ms    30 ms    30 ms  85.199.192.1       AS4000
  4    34 ms    38 ms    39 ms  80.192.0.20        AS4000 (Attacker)

Trace complete.
```

*Figure 23 – Windows trace route (post hijack).*

In the figure below, the final result of the BGP hijacking attack is shown. The victim PC, who could previously access the legitimate web server on 80.192.0.20 is now accessing the

malicious server on the rouge autonomous system (AS4000). Demonstrating the capability threat actors could utilise with BGP hijacking attacks, such as performing any number of man in the middle attacks, serving malicious code/software and stealing login credentials.


*Figure 24 – Attacker web server (Nginx).*

## Discussion

This discussion will focus on the main topics of the BGP hijacking procedure by analysing legitimate BGP routes, advertising the more specific AS prefix, and results of the BGP hijacking attack.

The aim for this whitepaper was to analyse the conceptual security flaws of the BGP protocol and set up and configure a demonstration network using GNS3 along with discussing the BGP hijacking countermeasures and their effectiveness. Firstly, the tools and networking software used in this project was identified. During the practical portion of this whitepaper, feasibility analysis was established to compare GNS3 vs Cisco Packet Tracer, it was identified that Cisco Packet Tracer does not support the extensive internetworking functionality between VMWare Workstation machines, and the virtual network created and for this reason GNS3 was selected for the proof of concept demonstration.

Once the GNS3 environment was configured and deployed, and an IP addressing scheme designed, then it was possible to perform the BGP hijack by advertising the more specific AS prefix. After performing the attack, it was identified that the user could not easily detect that the traffic has been re-routed or intercepted, the real-world effects of this attack could be very devastating due to potentially compromising confidentiality, integrity, and availability. Malicious threat actors could potentially use this attack to perform denial of service attacks, man in the middle attacks and route modification. However, SSL/TLS and associated technologies could defend against man in the middle interception, but due to recent research which was presented at the BlackHat security conference [15], it was demonstrated that the possibility of hijacking certificate authorities and forging SSL certificates exist.

The ease of exploitation for this procedure is a medium level. However, access to a core edge router is needed, which would then enable a threat actor to affect the broader internet if prefix and route filtering is not configured on neighbouring peers, up stream's and customers. However, during the whitepapers research, it was identified that nation-states, as well as rouge autonomous systems, could have the potential and motive to perform this attack for intelligence/surveillance, monetary gain, corporate espionage and further nefarious purposes.

In the case of future BGP hijacking research, man in the middle attacks using interception software such as SSL Strip along with Cisco AS_Path prepending could be further demonstrated and researched. In addition to this, research into forging SSL certificates by hijacking a certificate authority could be looked into and demonstrated.

# Countermeasures

BGP hijacking incidents can usually be mitigated through countermeasures based on public key infrastructure or whitelisting techniques. This section looks at a multitude of countermeasures such as prefix filtering, RPKI (Resource Public Key Infrastructure), BGPSec and current best practices.

## Real Time Monitoring, and Detection

The most current effective method of detecting and responding to BGP hijacking, in addition to prefix/route filtering is to use online services such as BGPMon[13] which can detect "suspicious" routing changes, such as modified AS Path, Origin AS, and Transit AS or any combination of those.

Upon receiving an alert to a BGP hijacking attack, then the organisational NOC/IT teams can contact the relevant upstream providers, and mitigate the attack as necessary.

## Prefix Filtering

Prefix filtering is a basic access control technique which can be used to filter out bogus BGP route advertisements. By enforcing inbound filtering, an autonomous system can ensure that neighbouring networks are only allowed to advertise a prefix, that is on the prefix list, and anything not on the list would be rejected. In addition to this, by configuring outbound prefix filtering, misconfiguration errors can be averted by preventing incorrect routes from being advertised to other autonomous systems, which could cause a non-malicious BGP hijack. It is highly recommended that prefix filtering be enabled for customers, up streams and peers for both ingress and egress traffic [12].

Despite the benefits of prefix filtering, not all autonomous systems deploy BGP filtering, due to the maintenance effort needed to maintain the list on a growing network or simply due to a lack of knowledge. If all network operators where to deploy prefix filtering, then performing a BGP hijacking attack would be very difficult than it is today.

## Resource Public Key Infrastructure (RPKI)

Resource Public Key Infrastructure system is a method to couple an IP prefix, and autonomous system number through the use of cryptographic signatures which is further described in RFC6480[14]. Public key infrastructure is operated by a variety of agencies which comprise the five Regional Internet Registries (RIRs), these organisations provide IP addresses and autonomous system numbers for organisations.

Currently, RIPE NCC operates an RPKI server for autonomous systems to validate BGP routing information using their validator. In addition to this, they have a variety of tools and resources on the subject.

Autonomous systems that hold and operate IP address space generate Route Origination Authorizations (ROAs), which associate the address prefix with an AS number, which gives

that AS permission to advertise the prefix in question and then the ROA is signed with the requesting AS's private key. In addition to this, the ROA does contain a maximum prefix length and expiry date for the ROA.

The certificates and ROA information are publicly accessible for download and verification, which then, in turn, is used to generate lists of prefix's and address prefix owners can be verified to prevent BGP hijacking.

Finally, although RPKI can prevent most BGP hijacking attacks it does not protect against all of them as a malicious threat actor can bypass RPKI protection by adding the authorised AS number to the end of the AS_PATH. RPKI only validates that the AS path is correct. More secure solutions such as BGPSec should be implemented.

### BGPSec

BGPSec is based on path attributes such as BGPSec_Path, which is an optional non-transitive attribute of the BGP protocol when BGPSec is implemented and deployed the BGPSec_Path attribute replaces the AS_PATH attribute. In addition to this, AS_PATH information also transmits a set of digital signatures, which is added in logical sequence to the update messages having left an AS, further to this any alteration in either AS_PATH or NLRI can be detected by the receiving autonomous system.

BGPSec provides a solution to the lack of integrity and authenticity of BGP update messages.

However, as BGPSec seems like an excellent way to solve many of the BGP security issues we face today, the actual implementation of this technology is low and not significant. As there are no regulation, or requirements to deploy BGPSec, many ISPs simply do not implement it. Although, there are disadvantages to this technology, such as the higher memory and processing power footprint that is needed, this is due to the cryptographic overhead, which is the primary reason many organisations have not implemented BGPSec.

### Best Common Practice

In addition to the recommended countermeasures, manufacturer best practices should be followed to ensure defence in depth and protect against more attacks against the BGP protocol. These can usually be found on the router software manufacturers website. Usual recommended best practices can include ACL's, blocking spoofed packets (BCP-38), MD5 neighbour authentication, TTL security check, and AS path length [12].

## Conclusion

In conclusion, it has been identified during this whitepaper, that BGP hijacking on the global internet is quite difficult to perform, due to the requirement of having access to an ISP border edge router. Despite, the difficulty in performing this attack, the consequences of a successful BGP hijack against an autonomous system can be severe which could consist of a man in the middle attack, denial of service attack, and route manipulation. As identified earlier in the paper, major networks have been globally affected by malicious BGP hijacking, which does demonstrate the effect this attack can have on an autonomous system.

Currently, there are a small number of mitigations available to prevent BGP hijacking, though they are not feasible across most autonomous systems due to the cryptographic

overhead and current hardware across internet infrastructure. Despite this, other mitigations can be configured such as prefix filtering, which if used across a large portion of the internet can protect significantly against most BGP hijacking attacks, although not all autonomous systems currently use this in the wild, because of maintenance upkeep or lack of knowledge.

It has been demonstrated through this paper, that the objectives have been achieved by investigating the background of the BGP protocol, describing and analysing current BGP hijacking flaws, and setting up and configuring a proof of concept demonstration along with discussing the available countermeasures and their effectiveness. It was identified that future work and research is possible into this attack vector.

## Further Reading

*H. Patel (2016). BGP Hijack Explained. [Online] Available at: https://www.youtube.com/watch?v=9NBv7lKrG1A [Accessed 5th November 2016].*

*APNIC Training (2014). BGP Basics 19 Mar 2014. [Online] Available at: https://www.youtube.com/watch?v=YBF0vqUhm7s [Accessed 5th November 2016].*

*D. Wendlandt (N.d). BGP Routing Security. [Online] Available at: http://moo.cmcl.cs.cmu.edu/~dwendlan/routing/ [Accessed 5th November 2016].*

*BGP4.as (N.d). BGP: The Border Gateway Protocol Advanced Internet Routing Resources. [Online] Available at: http://www.bgp4.as/security002.bz [Accessed 5th November 2016].*

*A. Gavrichenkov (2015). Breaking HTTPS with BGP Hijacking. [Online] Available at: https://www.blackhat.com/docs/us-15/materials/us-15-Gavrichenkov-Breaking-HTTPS-With-BGP-Hijacking-wp.pdf [Accessed 5th November 2016].*

# References

*[1] Y. Rekhter, T. Li, S. Hares. (Jan 2006). A Border Gateway Protocol 4 (BGP-4). [Online] Available at: https://www.ietf.org/rfc/rfc4271.txt [Accessed: 7th October 2016].*

*[2] G. Huston (Mar 2006). Exploring Autonomous System Numbers. [Online] Available at: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-12/autonomous-system-numbers.html [Accessed: 7th October 2016].*

*[3] Y. Rekhter, T.J. Watson Research Center, IBM Corp, T. Li (1993) An Architecture for IP Address Allocation with CIDR. [Online] Available at: https://tools.ietf.org/html/rfc1518 [Accessed: 7th October 2016].*

*[4] Cisco. (2016). BGP Best Path Selection Algorithm. [Online] Available at: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html [Accessed: 9th October 2016].*

*[5] A. Toonk (2014). Turkey Hijacking IP Address's for Popular Global DNS Providers. [Online] Available at: https://www.bgpmon.net/turkey-hijacking-ip-addresses-for-popular-global-dns-providers/ [Accessed 9th October 2016].*

*[6] A. Toonk (2014). The Canadian Bitcoin Hijack. [Online] Available at: https://www.bgpmon.net/the-canadian-bitcoin-hijack/ [Accessed 9th October 2016].*

*[7] P. Litke, J. Stewart (2014). BGP Hijacking for Cryptocurrency Profit. [Online] Available at: https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit [Accessed 9th October 2016].*

*[8] D. Donohue, B. Stewart (2010). CCNP: Routing and Switching Quick Reference: BGP and Internet Connectivity. [Online] Available at: http://www.ciscopress.com/articles/article.asp?p=1565538&seqNum=4 [Accessed 19th October 2016].*

*[9] A. Toonk (2014). Using BGP data to find Spammers [Online] Available at: https://bgpmon.net/using-bgp-data-to-find-spammers/ [Accessed 23rd October 2016].*

*[10] A. Toonk (2015). How Hacking Team Helped Italian Special Operations Group with BGP Routing Hijack. [Online] Available at: https://bgpmon.net/how-hacking-team-helped-italian-special-operations-group-with-bgp-routing-hijack/ [Accessed 23rd October 2016].*

*[11] GNS3 (2016). The software that empowers network professionals. [Online] Available at: https://www.gns3.com/ [Accessed 5th November 2016].*

*[12] Cisco (N.d). Protecting Border Gateway Protocol for the Enterprise. [Online] Available at: https://www.cisco.com/c/en/us/about/security-center/protecting-border-gateway-protocol.html [Accessed 5th November 2016].*

*[13] BGPMon (2016). BGPMon. [Online] Available at: https://bgpmon.net/ [Accessed 5th November 2016].*

*[14] M. Lepinski, S. Kent (2012). An Infrastructure to Support Secure Internet Routing. [Online] Available at: https://tools.ietf.org/html/rfc6480 [Accessed 5th November 2016].*

*[15] A. Gavrichenkov (2015). Breaking HTTPS with BGP Hijacking. [Online] Available at: https://www.blackhat.com/docs/us-15/materials/us-15-Gavrichenkov-Breaking-HTTPS-With-BGP-Hijacking-wp.pdf [Accessed 5th November 2016]*

*[16] Y. Hoong (2012). BGP Message Types [Online] Available at: http://www.itcertnotes.com/2012/01/bgp-message-types.html [Accessed 7th October 2016].*

# Appendices

## Appendix A - Router 1 Configuration

Firstly, each gigabit interface in use on Router 1 will be configured using Cisco CLI. As identified below, the IP address of 31.222.48.1 was set on interface GigabitEthernet0/0 and will be using the 31.222.48.0/25 network as demonstrated in the figure below.

```
R1(config)#int gigabite0/0
R1(config-if)#ip add 31.222.48.1 255.255.255.128
R1(config-if)#no shutdown
R1(config-if)#end
R1#
*Oct 28 22:59:15.463: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

*Figure 25 – GigabitEthernet0/0 interface configuration.*

The second interface will also be configured using Cisco CLI and will be using the 31.222.48.128/25 network. The IP address 31.222.48.129 was set on interface GigabitEthernet1/0.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int gigabite1/0
R1(config-if)#ip add 31.222.48.129 255.255.255.128
R1(config-if)#no shutdown
R1(config-if)#end
R1#
*Oct 28 23:08:30.003: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

*Figure 26 – GigabitEthernet1/0 interface configuration.*

## Appendix B - Router 2 Configuration

Interface GigabitEthernet0/0 will also be configured using Cisco CLI, using the 37.152.32.0/24 network. The IP address of 37.152.32.1 was set for the interface.

```
R2(config)#int gigabite0/0
R2(config-if)#ip add 37.152.32.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#end
```

*Figure 27 – GigabitEthernet0/0 interface configuration.*

Once the first interface has been configured, GigabitEthernet1/0 needs to be configured using Cisco CLI on the network 37.152.36.0/23, the IP address of the interface being 37.152.36.1.

```
R2(config)#int gigabite1/0
R2(config-if)#ip add 37.152.36.1 255.255.254.0
R2(config-if)#no shutdown
R2(config-if)#end
```

*Figure 28 – GigabitEthernet1/0 interface configuration.*

The third interface, GigabitEthernet2/0 needs to be configured using Cisco CLI on the network 37.152.64.0/23, the IP address of the interface being 37.152.64.1.

```
R2(config-if)#
R2(config-if)#ip add 37.152.64.1 255.255.254.0
R2(config-if)#no shutdown
R2(config-if)#end
```

*Figure 29 – GigabitEthernet2/0 interface configuration.*

## Appendix C - Router 3 Configuration

Interface GigabitEthernet0/0 needs to be configured using Cisco CLI on the network 80.192.0.0/15, the IP address of the interface being 80.192.0.1. It will then be used as the gateway for the legitimate web server virtual machine.

```
R3(config)#int gigabite0/0
R3(config-if)#ip add 80.192.0.1 255.254.0.0
R3(config-if)#no shutdown
R3(config-if)#end
```

*Figure 30 – GigabitEthernet0/0 interface configuration.*

The second interface needs to be configured using Cisco CLI on the network 80.194.0.0/23, and the interface IP address being 80.194.0.1.

```
R3(config)#int gigabite1/0
R3(config-if)#no ip add 46.20.112.1 255.255.254.0
R3(config-if)#ip add 80.194.0.1 255.255.254.0
R3(config-if)#no shutdown
R3(config-if)#end
```

*Figure 31 – GigabitEthernet1/0 interface configuration.*

## Appendix D - Router 4 Configuration

Firstly, interface GigabitEthernet2/0 needs to be configured using Cisco CLI on the network 85.199.192.0/23, and the IP address of the interface being 85.199.192.1, as shown in the figure below.

```
R4(config)#int gigabite2/0
R4(config-if)#ip add 85.199.192.1
R4(config-if)#ip add 85.199.192.1 255.255.254.0
R4(config-if)#no shutdown
R4(config-if)#end
R4#
*Oct 28 19:39:01.815: %SYS-5-CONFIG_I: Configured from console by console
R4#
*Oct 28 19:39:03.163: %LINK-3-UPDOWN: Interface GigabitEthernet2/0, changed stat
e to up
```

*Figure 32 – GigabitEthernet2/0 interface configuration.*

Next, the second interface GigabitEthernet0/0 needs to be configured by using the Cisco CLI on the network 80.192.0.0/24 with the interface IP address being 80.192.0.1, as shown in the

figure below, the hijacked IP space from AS3000 was configured which is used to perform the BGP hijacking attack by announcing a /24 prefix rather than a /15 prefix.

```
R4(config)#int gigabite0/0
R4(config-if)#ip add 80.192.0.1 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#end
R4#
*Oct 31 19:41:20.583: %SYS-5-CONFIG_I: Configured from console by console
R4#
*Oct 31 19:41:21.963: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed stat
e to up
*Oct 31 19:41:22.963: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
ernet0/0, changed state to up
R4#
```

*Figure 33 – GigabitEthernet0/0 interface configuration.*

## Appendix E - Legitimate Web Server Configuration

Firstly, the Linux web server IP address is to be configured on eth0 with the interface IP of 80.192.0.20 and on the network 80.192.0.0/15. The name server has been left blank for the proof of concept demonstration.

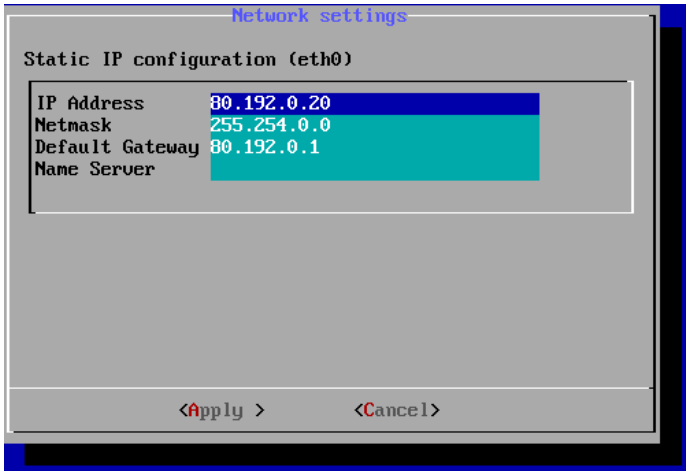


*Figure 34 – GUI eth0 network configuration.*

As identified in the figure below, in the SSH CLI output of interfaces on the system, eth0 is the only interface to be used for this server.

```
root@nginx-php-fastcgi ~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:51:0c:da
          inet addr:80.192.0.20  Bcast:80.193.255.255  Mask:255.254.0.0
          inet6 addr: fe80::20c:29ff:fe51:cda/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:253 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:65615 (64.0 KiB)  TX bytes:1940 (1.8 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:960 errors:0 dropped:0 overruns:0 frame:0
          TX packets:960 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:71040 (69.3 KiB)  TX bytes:71040 (69.3 KiB)
```

*Figure 35 – Linux ifconfig command results.*

## Appendix F - Malicious Web Server Configuration

The malicious web server, networking will be configured using Eth0 with the interface IP address of 80.192.0.20 and on the network 80.192.0.0/24. The name server has been left blank for the proof of concept demonstration.

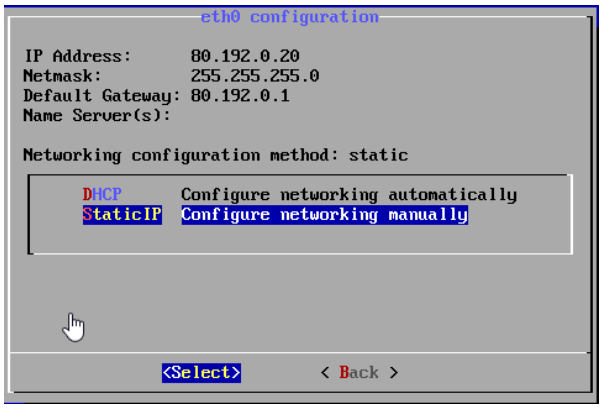


*Figure 36 – GUI eth0 network configuration.*

## Appendix G - Host PC Configuration

The host PC needs to be configured using the interface IP address of 31.222.48.130, and on the network 31.222.48.0/25. The default interface was used for this configuration.

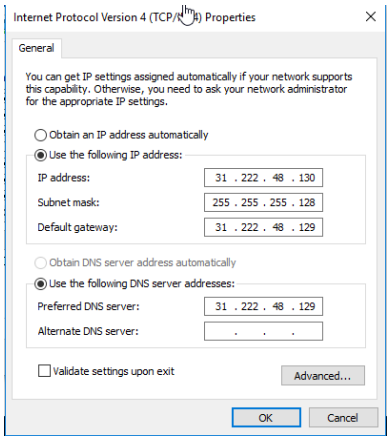


*Figure 37 – Windows Ethernet network configuration.*