



ASSIGNMENT NO 1

INFORMATION GATHERING

TOPIC : FIND OUT THE TARGET BY USING NMAP AND PING

DOMAIN NAME : Hero.com

NAME : HITESH SAGAR WAGH

EMAIL : hiteshswagh001@gmail.com

DATE : 01/11/2022

Host discovers

<https://bgp.he.net/>

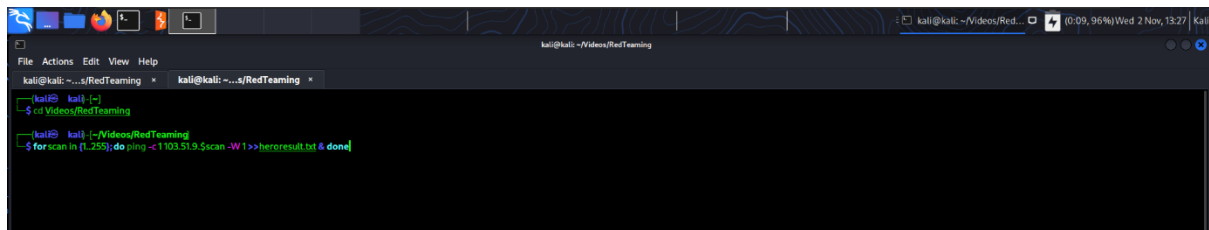
The screenshot shows the Hurricane Electric BGP Toolkit search results for the query 'hero'. The search results table lists various ASes and their descriptions. The AS132135 Hero MotoCorp Ltd is highlighted in green.

Result	Description
hero	
AS399250	Name Hero, LLC
AS37596	HERO TELECOMS (PTY) LTD
AS37439	HERO TELECOMS (PTY) LTD
AS37417	HERO TELECOMS (PTY) LTD
AS36953	HERO TELECOMS (PTY) LTD
AS328471	HERO TELECOMS (PTY) LTD
AS328232	HERO TELECOMS (PTY) LTD
AS328130	HERO TELECOMS (PTY) LTD
AS328064	HERO TELECOMS (PTY) LTD
AS327957	HERO TELECOMS (PTY) LTD
AS327858	HERO TELECOMS (PTY) LTD
AS327826	HERO TELECOMS (PTY) LTD
AS327781	HERO TELECOMS (PTY) LTD
AS327715	HERO TELECOMS (PTY) LTD
AS206041	Network Hero, S.L.
AS150113	HERO LINE LIMITED
AS135284	LUCKY HERO TECHNOLOGY DEVELOPMENT LIMITED
AS132135	Hero MotoCorp Ltd
61.51.0.0/20	Beijing Jingxin Hero Telecommunication
45.41.235.0/24	Name Hero, LLC
45.221.47.0/24	HERO TELECOMS (PTY) LTD
45.221.45.0/24	HERO TELECOMS (PTY) LTD
45.221.42.0/24	HERO TELECOMS (PTY) LTD
45.221.41.0/24	HERO TELECOMS (PTY) LTD
45.221.40.0/24	HERO TELECOMS (PTY) LTD

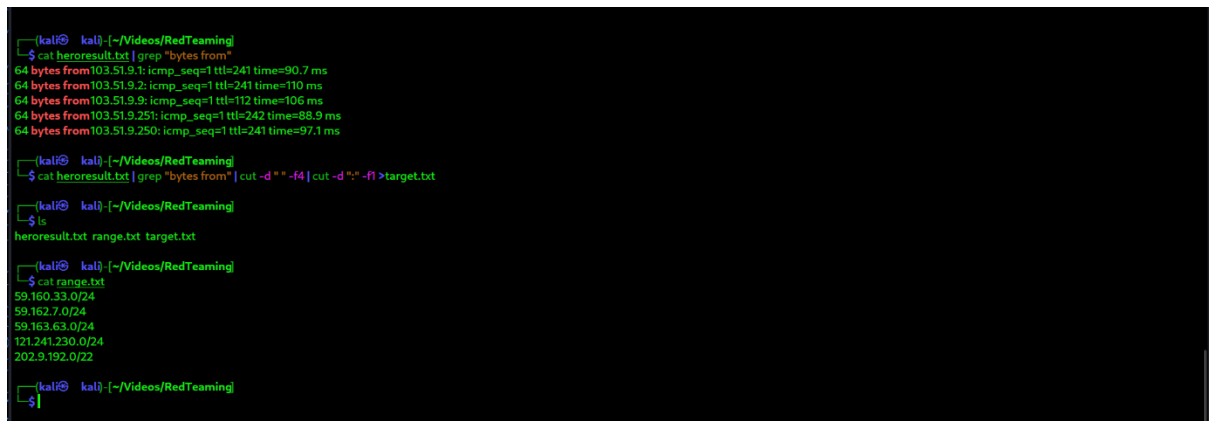
The screenshot shows the Hurricane Electric BGP Toolkit page for AS132135 Hero MotoCorp Ltd. The page displays the AS's prefixes and their descriptions. The AS132135 Hero MotoCorp Ltd is highlighted in green.

Prefix	Description
103.34.13.0/24	Hero MotoCorp Ltd
103.247.208.0/24	Hero MotoCorp Ltd

Getting all the open IP addresses and checking which of they and they stored in the target.txt



```
kali@kali: ~/Videos/RedTeaming
File Actions Edit View Help
kali@kali: ~/Videos/RedTeaming
$ cd Videos/RedTeaming
kali@kali: ~/Videos/RedTeaming
$ for scan in {1..255}; do ping -c 1 103.51.9.$scan -W 1 >> heroresult.txt & done
```



```
kali@kali: ~/Videos/RedTeaming
$ cat heroresult.txt | grep "bytes from"
64 bytes from 103.51.9.1: icmp_seq=1 ttl=241 time=90.7 ms
64 bytes from 103.51.9.2: icmp_seq=1 ttl=241 time=110 ms
64 bytes from 103.51.9.9: icmp_seq=1 ttl=112 time=106 ms
64 bytes from 103.51.9.251: icmp_seq=1 ttl=242 time=88.9 ms
64 bytes from 103.51.9.250: icmp_seq=1 ttl=241 time=97.1 ms

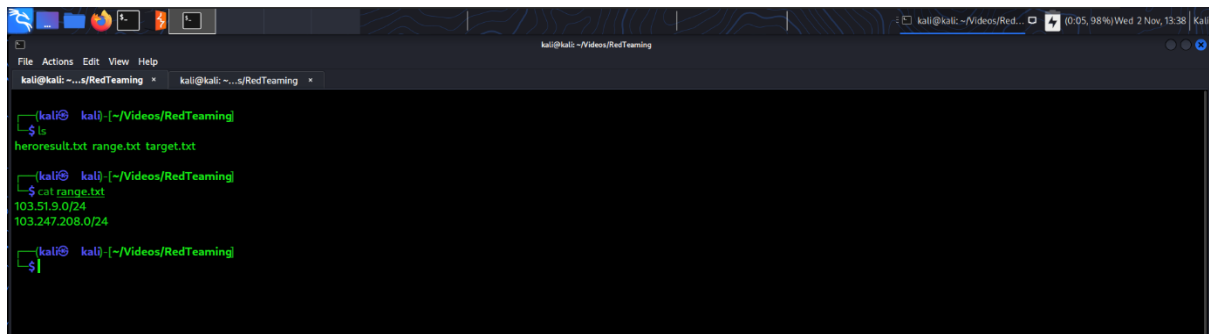
kali@kali: ~/Videos/RedTeaming
$ cat heroresult.txt | grep "bytes from" | cut -d " " -f4 | cut -d "." -f1 > target.txt

kali@kali: ~/Videos/RedTeaming
$ ls
heroresult.txt range.txt target.txt

kali@kali: ~/Videos/RedTeaming
$ cat range.txt
59.160.33.0/24
59.162.7.0/24
59.163.63.0/24
121.241.230.0/24
202.9.192.0/22

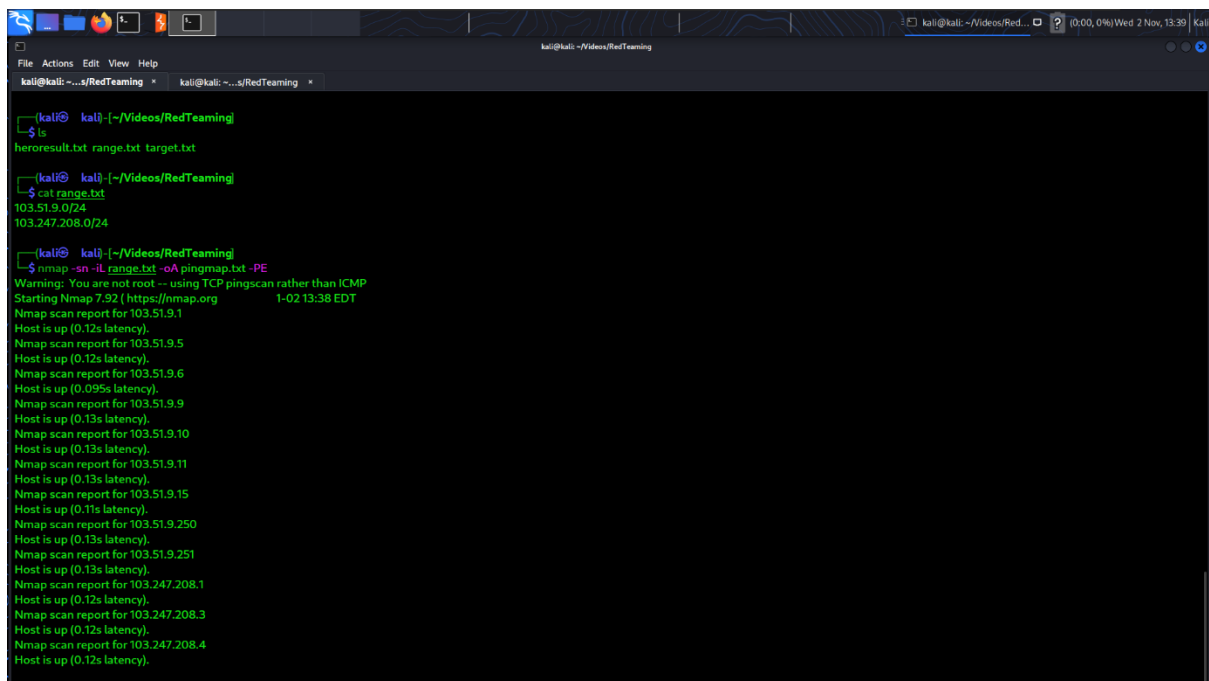
kali@kali: ~/Videos/RedTeaming
$
```

BY USING THE NMAP FOR THE OPEN PORTS AND LIVE IP'S



```
kali@kali: ~/Videos/RedTeaming
File Actions Edit View Help
kali@kali: ~/Videos/RedTeaming
$ ls
heroresult.txt range.txt target.txt
$ cat range.txt
103.51.9.0/24
103.247.208.0/24
$
```

IT SHOWS ONLY LIVE IP'S



```
kali@kali: ~/Videos/RedTeaming
File Actions Edit View Help
kali@kali: ~/Videos/RedTeaming
$ ls
heroresult.txt range.txt target.txt
$ cat range.txt
103.51.9.0/24
103.247.208.0/24
$ nmap -sn -iL range.txt -oA pingmap.txt -PE
Warning: You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.92 ( https://nmap.org ) 1-02 13:38 EDT
Nmap scan report for 103.51.9.1
Host is up (0.12s latency).
Nmap scan report for 103.51.9.5
Host is up (0.12s latency).
Nmap scan report for 103.51.9.6
Host is up (0.095s latency).
Nmap scan report for 103.51.9.9
Host is up (0.13s latency).
Nmap scan report for 103.51.9.10
Host is up (0.13s latency).
Nmap scan report for 103.51.9.11
Host is up (0.13s latency).
Nmap scan report for 103.51.9.15
Host is up (0.11s latency).
Nmap scan report for 103.51.9.250
Host is up (0.13s latency).
Nmap scan report for 103.51.9.251
Host is up (0.13s latency).
Nmap scan report for 103.247.208.1
Host is up (0.12s latency).
Nmap scan report for 103.247.208.3
Host is up (0.12s latency).
Nmap scan report for 103.247.208.4
Host is up (0.12s latency).
```

TO EXTRACT ONLY LIVE IPS



```
kali@kali: ~/Videos/RedTeaming
$ cat pingmap.txt.nmap | grep "Nmap" | cut -d " " -f 5 |>>target.txt
$
```

```
kali@kali: ~/Videos/RedTeaming
File Actions Edit View Help
kali@kali: ~/Videos/RedTeaming
kali@kali: ~/Videos/RedTeaming

kali@kali: ~/Videos/RedTeaming
$ cat target.txt
103.51.9.1
103.51.9.2
103.51.9.9
103.51.9.251
103.51.9.250
initiated
103.51.9.1
103.51.9.5
103.51.9.6
103.51.9.9
103.51.9.10
103.51.9.11
103.51.9.15
103.51.9.250
103.51.9.251
103.247.208.1
103.247.208.3
103.247.208.4
103.247.208.5
103.247.208.16
103.247.208.25
103.247.208.32
103.247.208.33
103.247.208.34
103.247.208.35
103.247.208.48
103.247.208.51
103.247.208.52
103.247.208.55
103.247.208.57
103.247.208.58
103.247.208.60
103.247.208.61
103.247.208.64
103.247.208.66
```

FINDING THE SPECIFIC IP'S USING PORTS:

```
kali@kali: ~/Videos/RedTeaming
$ nmap -Pn -p 22,80,443,2222,3389 -iL range.txt -oA portrange.txt
```

```
kali@kali: ~/Videos/RedTeaming
File Actions Edit View Help
kali@kali: ~/Videos/RedTeaming
kali@kali: ~/Videos/RedTeaming

Nmap scan report for 103.247.208.255
Host is up.

PORT      STATE SERVICE
22/tcp    filtered ssh
80/tcp    filtered http
443/tcp   filtered https
2222/tcp   filtered EtherNetIP-1
3389/tcp   filtered ms-wbt-server

# Nmap done at Wed Nov 2 13:55:31 2022 -- 512 IP addresses (512 hosts up) scanned in 453.35 seconds

kali@kali: ~/Videos/RedTeaming
$ cat portrange.txt.nmap | grep "Nmap" | cut -d " " -f 5 >> targetport.txt

kali@kali: ~/Videos/RedTeaming
$ ls
herosresult.txt pingmap.txt.gnmap pingmap.txt.nmap pingmap.txt.xml portrange.txt.gnmap portrange.txt.nmap portrange.txt.xml range.txt targetport.txt target.txt

kali@kali: ~/Videos/RedTeaming
$ cat targetport.txt
initiated
103.51.9.0
103.51.9.1
103.51.9.2
103.51.9.3
103.51.9.4
103.51.9.5
103.51.9.6
103.51.9.7
103.51.9.8
103.51.9.9
103.51.9.10
103.51.9.11
103.51.9.12
103.51.9.13
103.51.9.14
```