Finding and Enumerating ASN

What is an ASN ?

An ASN is a unique number assigned to a network or group of networks that are managed by a single organization and use a common routing policy. These networks are called Autonomous Systems (AS).

Imagine a company has its own internal network with multiple routers and switches. This company network is considered an Autonomous System. Each AS is assigned a special number, called an ASN, to identify it uniquely.

ASNs are used when networks need to communicate with each other on the internet. For example, when your home internet connects to a website hosted by another company, the data has to pass through multiple networks or Autonomous Systems to reach its destination.

Let see how we can get ASN of our target and enumerate it.

- **Finding ASN** - https://bgp.he.net/

```
paytm - AS137614
```

- **Find out the IP ranges that reside inside the ASN.**

```
whois -h whois.radb.net  -- '-i origin AS714' | grep -Eo "([0-9.]+){4}/[0-9]+" | uniq -u > ip_ranges.txt
```

- **Perform a reverse DNS lookup.**

Install MapCIDR

```
# Download MapCIDR

git clone https://github.com/projectdiscovery/mapcidr.git

cd mapcidr/cmd/mapcidr

# Install MapCIDR

go build .
```

```
# Copt binary to bin directory for universal access

sudo cp mapcidr /usr/local/bin
```

Install Dnsx tool

```
# Download Dnsx

git clone https://github.com/projectdiscovery/dnsx.git

cd dnsx/cmd/dnsx

# Install Dnsx

go build .

# Copt binary to bin directory for universal access

sudo cp dnsx /usr/local/bin
```

Perform reverse DNS Lookup:

```
cat ip_ranges.txt | mapcidr -silent | dnsx -ptr -resp-only -o hostname.txt
```
