C|EH Prep

Certified | Ethical Hacker

Prepared by Youssef Mohamed



Different Techniques for Network & Email Footprinting

CypherPanther

ARIN

American **R**egistry for **I**nternet **N**umbers

When we talk about the structure of the Internet, one of the most important components is the way IP addresses and Autonomous System Numbers (ASNs) are assigned. These resources are not random; they are managed by specialized global authorities known as Regional Internet Registries (RIRs).

ARIN, short for American Registry for Internet Numbers, is one of these registries.

ARIN is the official organization responsible for managing and distributing:

- IPv4 addresses
- IPv6 addresses
- Autonomous System Numbers (ASNs)

Why ARIN Matters in Reconnaissance

During Active Footprinting—a technique Eng. Youssef covered in the sessions—ARIN becomes an important source of intelligence because it can reveal:

- Which organization owns a specific IP address
- Contact information for network administrators
- The assigned ASN
- The organization's network range (CIDR block)
- Registration dates and update history

How ARIN Works

When you enter an IP address or domain into ARIN's lookup service, ARIN checks its database and returns the registered owner.

For example, searching for an IP belonging to a large company like Microsoft might show:

- Organization Name, Network Range, ASN, Abuse Contacts, Technical Contacts, Registration and Update Date

Why ARIN Matters in Reconnaissance

During Active Footprinting—a technique Eng. Youssef covered in the sessions—ARIN becomes an important source of intelligence because it can reveal:

- Which organization owns a specific IP address
- Contact information for network administrators
- The assigned ASN
- The organization's network range (CIDR block)
- Registration dates and update history

How ARIN Works

When you enter an IP address or domain into ARIN's lookup service, ARIN checks its database and returns the registered owner.

For example, searching for an IP belonging to a large company like Microsoft might show:

- Organization Name, Network Range, ASN, Abuse Contacts, Technical Contacts, Registration and Update Date

How ARIN Helps in Active Scanning

Before running DNS scans, port scans, or service enumeration, professionals often use ARIN to confirm:

- Whether the IP block belongs to the expected company
- Whether the infrastructure is internal, external, or hosted by a third-party cloud provider
- Whether the target uses multiple ASNs or multiple geographic regions
- Whether the IP space is shared with other services

Gather information using ping utility

CMD

Copy

```
C:\Users\User..>ping google.com

Pinging google.com [142.250.186.110] with 32 bytes of data:
Reply from 142.250.186.110: bytes=32 time=66ms TTL=112
Reply from 142.250.186.110: bytes=32 time=80ms TTL=112
Reply from 142.250.186.110: bytes=32 time=67ms TTL=112
Reply from 142.250.186.110: bytes=32 time=65ms TTL=112

Ping statistics for 142.250.186.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:

        Minimum = 65ms, Maximum = 80ms, Average = 69ms
```

Gather information using Traceroute

CMD

Copy

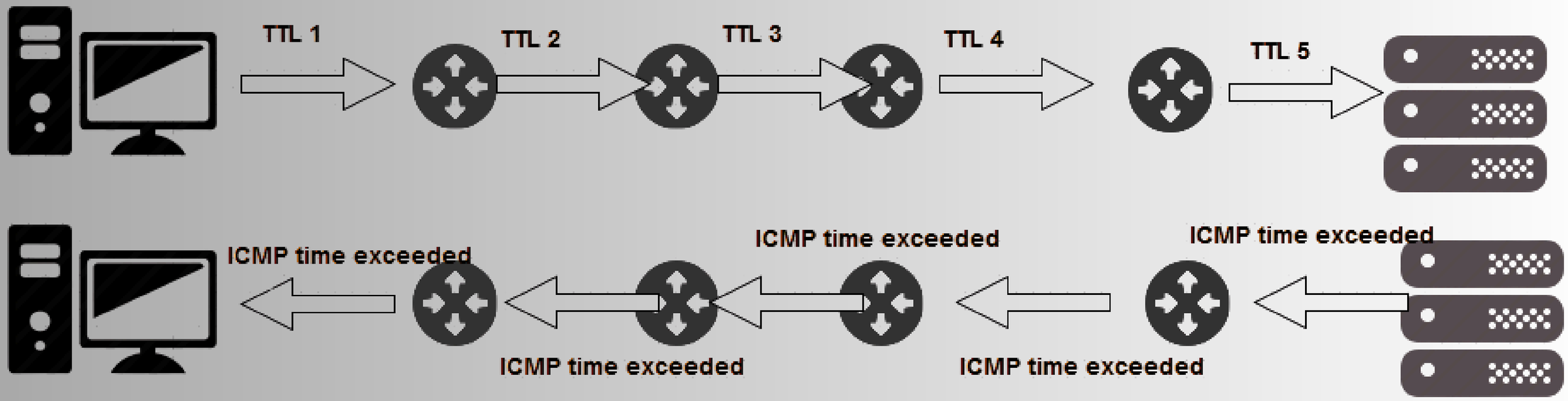
```
C:\Users\youssef.zinhom>tracert google.com

Tracing route to google.com [172.217.171.238]
over a maximum of 30 hops:

  1    12 ms     5 ms     4 ms  192.168.9.21
  2    16 ms     3 ms     4 ms  192.168.103.1
  3    16 ms    16 ms     9 ms  197.133.96.3
  4    20 ms    11 ms    12 ms  172.31.139.5
  5    29 ms    11 ms    29 ms  host-81.10.87.226.tedata.net [81.10.87.226]
  6    52 ms    50 ms    50 ms  et-4-0-16.edge1.Milan1.Level3.net [212.73.241.97]
  7    62 ms    62 ms    61 ms  15169-3356-mln.sp.lumen.tech [4.68.37.166]
  8    63 ms    61 ms    61 ms  72.14.238.234
  9    71 ms    62 ms    62 ms  192.178.104.104
 10    71 ms    62 ms    63 ms  192.178.111.37
 11    78 ms    70 ms    70 ms  172.253.71.227
 12    74 ms    73 ms    68 ms  192.178.85.28
 13    88 ms    69 ms    76 ms  192.178.105.81
 14   177 ms    72 ms    69 ms  172.253.67.151
 15    74 ms    68 ms    68 ms  mrs09s07-in-f14.1e100.net [172.217.171.238]

Trace complete.
```

Traceroute


TTL 1
TTL 2
TTL 3
TTL 4
TTL 5
ICMP time exceeded
ICMP time exceeded
ICMP time exceeded
ICMP time exceeded
ICMP time exceeded



CypherPanther

You can follow us here

Thank you