

# Discovering Intel from Network Reconnaissance/Footprinting

---



**Dale Meredith**

MCT/CEI/CEH/Speaker/Security Dude



@dalemeredith



:daledumbsITdown



:daledumbsITdown



:dalemeredith

www.daledumbsITdown.com

Who is Arin?

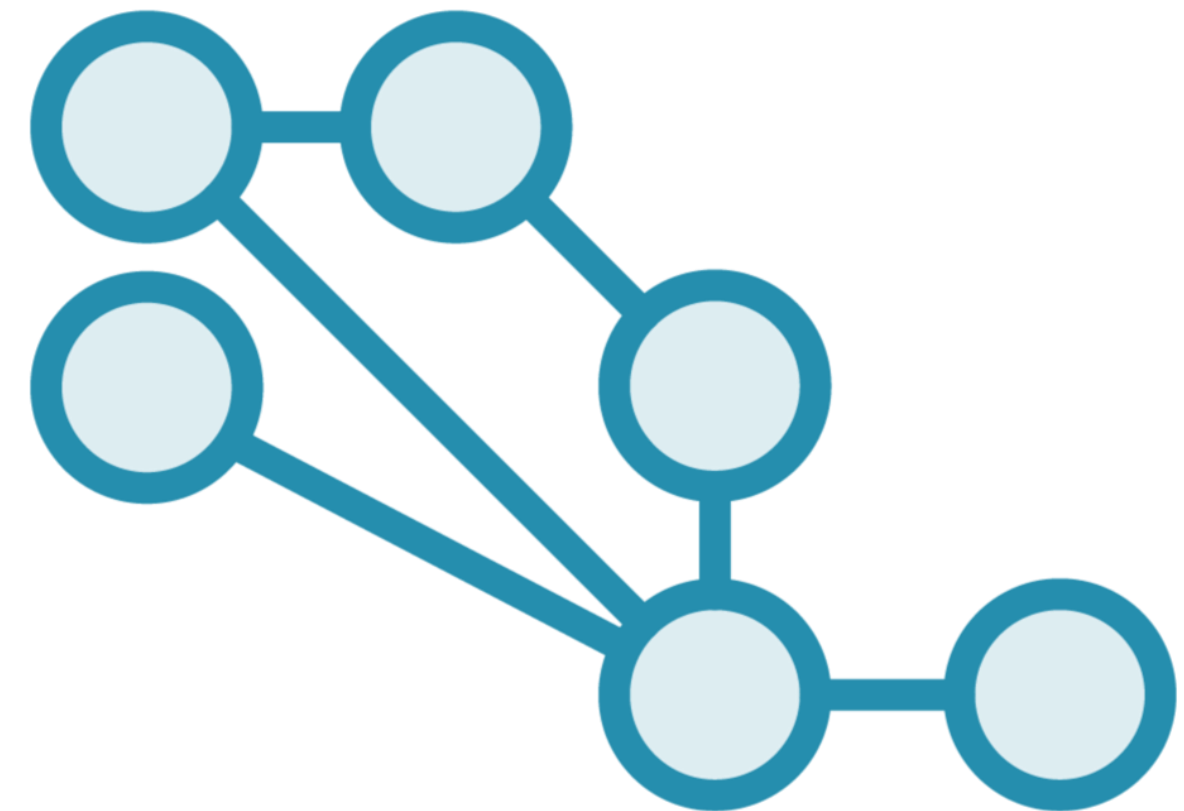
---

# Who is Arin?


**Expose other targets**

**IP addresses and  
subnet masks**

**Map out the target's network**



# Who is Arin?

 **ARIN**  
American Registry for Internet Numbers

Search Site or Whois

[Home](#) [IP Addresses & ASNs](#) [Policy & Participation](#) [Reference & Tools](#) [About](#)

## ARIN Whois/RDAP

54.186.147.214

» Search [www.arin.net](http://www.arin.net) instead

► Search Filter: **Automatic**

all requests subject to terms of use

"54.186.147.214"

### Network: NET-54-184-0-0-1

<b>Source Registry</b>	ARIN
<b>Net Range</b>	54.184.0.0 - 54.187.255.255
<b>CIDR</b>	54.184.0.0/14
<b>Name</b>	AMAZO-ZPDX7
<b>Handle</b>	NET-54-184-0-0-1
<b>Parent</b>	NET-54-144-0-0-1 <a href="https://t.me/learningnets">https://t.me/learningnets</a>

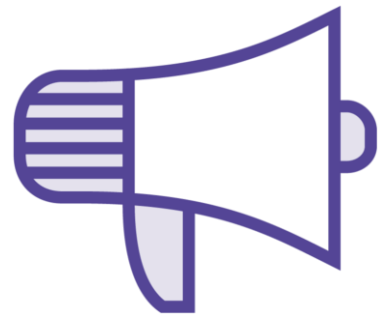
# Using Traceroute

---

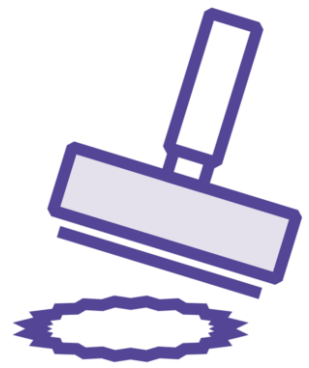
# Using Traceroute



**UDP Traceroute**



**ICMP Traceroute**



**TCP Traceroute**

# ICMP Traceroute

```
PS C:\> tracert hackthissite.org

Tracing route to hackthissite.org [137.74.187.104]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  BATROUTER [10.10.10.1]
  2   1 ms   1 ms   1 ms  192.168.0.1
  3   8 ms   8 ms   9 ms  slcy-dsl-gw16.slcy.qwest.net [207.108.176.16]
  4   9 ms  10 ms  10 ms  slcy-agw1.inet.qwest.net [207.108.177.121]
  5   9 ms  20 ms  19 ms  4.68.38.161
  6   *     *     *     Request timed out.
  7  35 ms  32 ms  32 ms  sjo-sv5-bb1-a9.ca.us [142.44.208.133]
  8  69 ms  67 ms  67 ms  be102.pdx-pdx02-sbb1-nc5.oregon.us [198.27.73.197]
  9  67 ms  66 ms  69 ms  142.44.208.227
 10   *     *     *     Request timed out.
 11  70 ms  66 ms  66 ms  pdx1-hil1-vac1-a75-1-firewall.ovh.us [147.135.34.8]
 12  67 ms  67 ms  66 ms  pdx1-hil1-vac1-a75-2-shield.ovh.us [147.135.34.9]
 13  67 ms  66 ms  66 ms  pdx1-hil1-vac1-a75-3.ovh.us [147.135.34.7]
 14   *     *     *     Request timed out.
 15   *     *     *     Request timed out.
 16   *     *     *     Request timed out.
 17   *     *     *     Request timed out.
 18   *     *     *     Request timed out.
 19   *     *     *     Request timed out.
 20 182 ms 180 ms 179 ms  hackthissite.org [137.74.187.104]

Trace complete.
```

# TCP Traceroute

```
(bwayne@Windows10-Targete)-[~/mnt/c/Users/dmeredith]
$ sudo tcptraceroute hackthissite.org
Running:
      traceroute -T -0 info hackthissite.org
traceroute to hackthissite.org (137.74.187.101), 30 hops max, 60 byte packets
 1  Windows10-Targete.mshome.net (172.21.48.1)  0.485 ms  0.227 ms  0.398 ms
 2  10.10.10.1 (10.10.10.1)  1.174 ms  1.132 ms  0.778 ms
 3  192.168.0.1 (192.168.0.1)  3.543 ms  4.231 ms  2.929 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  sjo-sv5-bb1-a9.ca.us (142.44.208.133)  66.170 ms  72.933 ms  85.381 ms
 9  be102.pdx-pdx02-sbb1-nc5.oregon.us (198.27.73.197)  109.979 ms  109.060 ms  110.672 ms
10  142.44.208.227 (142.44.208.227)  110.333 ms  109.929 ms  111.636 ms
11  * * *
12  pdx1-hil1-vac1-a75-1-firewall.ovh.us (147.135.34.8)  110.945 ms  113.746 ms  113.484 ms
13  * * pdx1-hil1-vac1-a75-2-shield.ovh.us (147.135.34.9)  100.572 ms
14  pdx1-hil1-vac1-a75-3.ovh.us (147.135.34.7)  110.509 ms  112.685 ms  112.677 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  hackthissite.org (137.74.187.101) <syn,ack>  288.950 ms  183.606 ms  183.374 ms

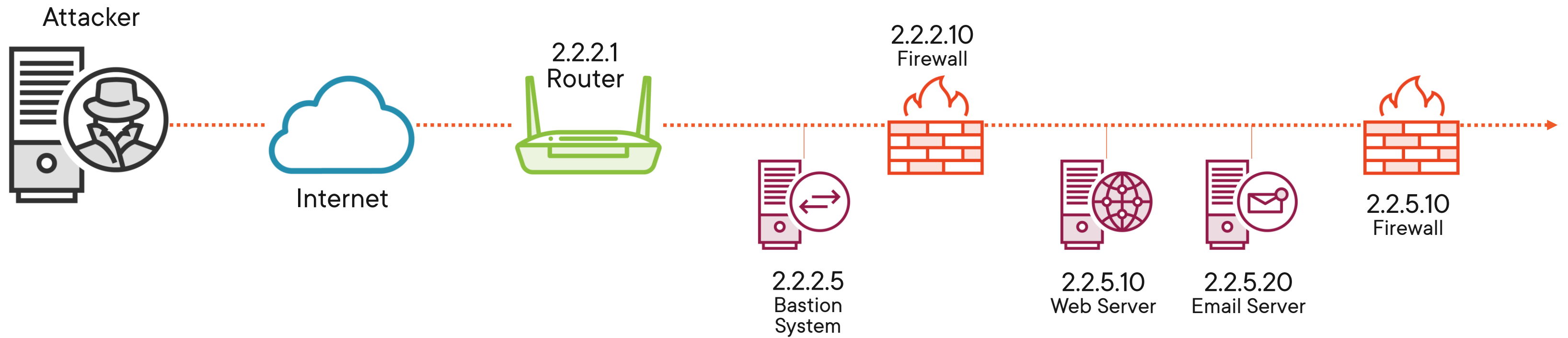
(bwayne@Windows10-Targete)-[~/mnt/c/Users/dmeredith]
$ |
```

# UDP Traceroute

```
(bwayne@Windows10-Targete)-[~/mnt/c/Users/dmeredith]
$ traceroute hackthissite.org
traceroute to hackthissite.org (137.74.187.101), 30 hops max, 60 byte packets
 1  Windows10-Targete.mshome.net (172.21.48.1)  2.072 ms  1.865 ms  1.844 ms
 2  10.10.10.1 (10.10.10.1)  1.735 ms  1.168 ms  1.009 ms
 3  192.168.0.1 (192.168.0.1)  3.918 ms  3.755 ms  3.379 ms
 4  slcy-dsl-gw16.slcy.qwest.net (207.108.176.16)  11.431 ms  11.425 ms  11.835 ms
 5  slcy-agw1.inet.qwest.net (207.108.177.121)  12.791 ms  10.483 ms  12.884 ms
 6  4.68.38.161 (4.68.38.161)  11.055 ms *  126.433 ms
 7  * * *
 8  sjo-sv5-bb1-a9.ca.us (142.44.208.133)  139.704 ms  33.506 ms  35.974 ms
 9  be102.pdx-pdx02-sbb1-nc5.oregon.us (198.27.73.197)  70.899 ms  71.843 ms  68.978 ms
10  142.44.208.227 (142.44.208.227)  70.191 ms  69.597 ms  70.812 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

```
(bwayne@Windows10-Targete)-[~/mnt/c/Users/dmeredith]
$
```

# Traceroute



# Demo



**Keycdn online tool**

**GeoTraceroute**

Up Next:

Employing Social Engineering Tactics

---