The Hunt Is On
A practical guide to Internet reconnaissance, by l0gic

Sometimes thirty-two bits are all you need. This is a guide to Internet reconnaissance - a guide to finding out as much as you can concerning a target via the Internet. Utilizing publicly available resources, we can quickly learn a good deal about a suspicious host, such as its service provider and originating country. Coupled with real-world knowledge, we can assess the threat posed by a would-be attacker and react accordingly. Along with a good idea of where to start, this requires some basic working knowledge of the Internet and the communication for which it provides.

The Internet is a cloud. Not literally, of course, but it is often pictured this way due to its vague nature. From the outside, it appears as a single entity, but from within it is impossible to determine its boundaries. The Internet is constantly changing, and there is no giant map to help us get a bearing on where we are. Instead, we rely on routed protocols - specifically IP - for transportation over and between networks.

Now, as with everything, this has good points and bad points. The seemingly infinite size and redundancy of the Internet generally provide for reliable sustained communications. Even though the routes taken by traffic may change, an end-to-end connection appears constant to its users. However, by its very nature, the Internet is an incredibly complex network of networks. It is impossible to consider the Internet as a detailed whole. But with a little know-how, we can traverse this uncharted territory with relative ease.

Hostile Territory

On the routed Internet, we lose certain luxuries taken for granted on local networks. Most obviously, we lose all second-layer functionality (see the OSI Model for a better understanding of the layered anatomy of a network). Any hardware information, such as MAC addresses or interface ID's which would typically prove invaluable on a switched network aren't worth squat outside the border router. We also give up any control we might have had otherwise, such as administrative access to network devices.

To make things even more complicated, we might also have the added limitations of Internet service providers to deal with. Some ISPs filter certain types of traffic in the interest of security or - more often - economy. This is very common among university and corporate networks, and even some less reputable residential providers. One such common practice is to disable ICMP traffic on infrastructure

devices, effectively making ping useless. Similarly, this may also result in abridged or never-ending traceroutes, as with the following IP[1]:

```
C:\>tracert 68.57.30.45

Tracing route to pcp04991434pcs.benslm01.pa.comcast.net [68.57.30.45]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    11 ms    11 ms    10 ms  nv-67-77-38-1.sta.sprint-hsd.net [67.77.38.1]
  3    11 ms    12 ms    11 ms  nv-208-13-128-45.sta.sprint-hsd.net [208.13.128.45]
  4    11 ms    11 ms    11 ms  host114.eseg2.sprintnetops.net [63.164.47.114]
  5    17 ms    17 ms    17 ms  sl-gw23-ana-0-4.sprintlink.net [144.228.170.89]
  6    16 ms    17 ms    17 ms  sl-bb20-ana-3-3.sprintlink.net [144.232.1.45]
  7    18 ms    17 ms    16 ms  sl-bb22-ana-14-0.sprintlink.net [144.232.1.177]
  8    19 ms    17 ms    17 ms  sprint-gw.la2ca.ip.att.net [192.205.32.185]
  9    19 ms    18 ms    19 ms  tbr2-p012101.la2ca.ip.att.net [12.123.29.6]
 10    71 ms    73 ms    70 ms  tbr2-cl2.sl9mo.ip.att.net [12.122.10.13]
 11    70 ms    70 ms    71 ms  tbr2-cl7.cgcil.ip.att.net [12.122.10.45]
 12    71 ms    71 ms    70 ms  tbr1-cl2.cgcil.ip.att.net [12.122.9.133]
 13    85 ms    87 ms    84 ms  tbr1-cl1.n54ny.ip.att.net [12.122.10.1]
 14    84 ms    83 ms    83 ms  gar5-p300.n54ny.ip.att.net [12.123.3.9]
 15    84 ms    84 ms    84 ms  12.118.149.18
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20   137 ms   120 ms   101 ms  pcp04991434pcs.benslm01.pa.comcast.net [68.57.30.45]

Trace complete.
```

The above is an example of an incomplete traceroute - you can see the local hops on the target end have been masked. This can make troubleshooting difficult at times, but some ISPs will restrict ICMP as a measure to mitigate certain types of denial of service attacks. In addition, there may also be limitations placed on other protocols via up-channel firewalls, but these generally won't interfere with our current investigation.

Dissolving the Cloud

So we're reviewing our firewall's intrusion attempt logs one afternoon and one IP in particular stands out from the rest. We see repeated, random attempts at compromising an FTP server. The variations in timing and syntax lead you to believe this to be more than just another virus-infected zombie; the attacks seem to stem from a human source. This certainly warrants investigation, but all we have is an IP: 24.145.180.82. Where do we start?

The first thing we want to do is get an idea of who might be attacking us. Is this just a residential connection, or corporate network, or might it even be coming from a compromised third-party server? A quick reverse DNS lookup should help us out.

```
C:\>nslookup 24.145.180.82
Server:  nv-208-13-143-36.sta.sprint-hsd.net
Address:  208.13.143.36

Name:    user-0c93d2i.cable.mindspring.com
Address:  24.145.180.82
```

We can determine from the lookup that the IP belongs to Mindspring, a provider of Earthlink's broadband Internet service. So, if this turns out to be a malicious attacker, we can at least find out who to contact about a possible Terms of Service violation. This happens to be a United States ISP, but for out-of-country providers, check IANA's top level domain listings at http://www.iana.org/cctld/cctld-whois.htm[2].

Sometimes reverse lookups may not be so helpful, or we require further information. The most reliable sources of IP registration info are the four global IP registries. ARIN serves North America and southern Africa, RIPE serves Europe and northern Africa, APNIC serves Asia and Australia, and LACNIC serves South America. Use your regional registry's WHOIS search to look up the target address. ARIN, for example, returns the following information:

```
Search results for: 24.145.180.82

Earthlink, Inc. ERLK-CABLE-TW-CENTRAL (NET-24-145-128-0-1)
                                  24.145.128.0 - 24.145.255.255
EarthLink, Inc. ERLK-TW-INDIANAPOLIS01 (NET-24-145-178-0-1)
                                  24.145.178.0 - 24.145.181.63
```

However, if we were to WHOIS this address from another registry, it would refer us back to IANA, as that registry would not be responsible for this address block. IANA provides a list of the top-level IP allocation blocks. Your IP may be listed under a specific registry; otherwise, you'll have to check each registry manually until you find the appropriate one.

In our example above, we receive two entries. The first is for a clump of 128 C-blocks[3] allocated to Earthlink, Inc. The second provides greater detail, specifying a more limited range used only in the Indianapolis, Indiana metropolitan area. We're starting to get a clearer picture of our attacker. We now know his general geographic location as well as his service provider. Given this information, we can

make an informed decision whether or not to continue the search.

Let's look at another example. This one is purposefully more complicated, in an effort to stress the importance of detail. Our new target IP is 211.23.250.99. Checking IANA's list of IP blocks, we see that our first octet (211) falls under APNIC, so we head on over to http://www.apnic.net/ and WHOIS the IP:

```
inetnum:      211.23.0.0 - 211.23.255.255
netname:      HINET-TW
descr:        CHTD, Chunghwa Telecom Co.,Ltd.
descr:        Data-Bldg.6F, No.21, Sec.21, Hsin-Yi Rd.
descr:        Taipei Taiwan 100
country:      TW
admin-c:      HN27-AP
tech-c:       HN28-AP
remarks:      This information has been partially mirrored by APNIC from
remarks:      TWNIC. To obtain more specific information, please use the
remarks:      TWNIC whois server at whois.twnic.net.
mnt-by:       MAINT-TW-TWNIC
changed:      hostmaster@twnic.net 20001106
status:       ALLOCATED PORTABLE
source:       APNIC
```

We can see from the above that the IP is registered under Chunghwa Telecom Co., of Taipei, Taiwan. However, this is a very broad listing, whose range is composed of an entire B class - 65,536 IP's. Note that our WHOIS actually returns two separate queries, the second of which is much more localized:

```
inetnum:      211.23.250.96 - 211.23.250.103
netname:      TAIWAN-GUAN-SI-P-KH-TW
descr:        CHTD, Chunghwa Telecom Co., Ltd.
descr:        Data-Bldg. 6F,  No. 21, Sec. 21, Hsin-Yi Rd.,
descr:        Taipei Taiwan
country:      TW
admin-c:      JJ308-TW
tech-c:       JJ308-TW
mnt-by:       MAINT-TW-TWNIC
remarks:      This information has been partially mirrored by APNIC from
remarks:      TWNIC. To obtain more specific information, please use the
remarks:      TWNIC whois server at whois.twnic.net.
changed:      fkchung@ms1.hinet.net 20040108
status:       ASSIGNED NON-PORTABLE
source:       TWNIC
```

The second range spans only eight IPs, but still lists the same parent company. One important detail to note in this case is the addition of administrative comments in the remarks section, indicating that this entry has been mirrored from the local registry of Taiwan, TWNIC. Some countries have elected to run

their own national registries due to political or other motivations. By performing a WHOIS on the same IP at http://whois.twnic.net/ we are provided yet more detail about the address range, including its current owner, Taiwan Guan Si Paint Co.

Putting it All Together

At this point we have a very solid lead for pursuing our investigation. What you decide from this point on should be based on outside information, and relies largely on what your original motive was anyway. The next logical step, should you decide to investigate further, would be target enumeration; port scanning and platform/service analysis. Be aware however that these are proactive steps. Once attempted, you have entered the game and should take appropriate cautions.

The whole WHOIS process is pretty simple, and you should be able to perform every necessary step above and arrive at an answer in just seconds once you're accustomed to it. Keep in mind that the information you find might not always be 100% accurate, or might in fact describe a third-party host an attacker is using as a proxy en route to you. Still, you'll gain a much better footing once you have the means to personify your target. Given a few key pieces of information, the shroud of the Internet begins to thin and makes further progress that much easier.

[1] I would like to stress that the IP addresses provided for demonstration are merely that; several hapless hosts chosen at pseudo-random. When performing traces of your own, try different IP's.

[2] The Internet Assigned Numbers Authority (IANA) is a non-profit organization charged with administering high-level Internet functions. This includes assigning IP address space, TCP/UDP port numbers, etc.

[3] IP addresses are traditionally broken into several distinct classes, which were used to manage routing tables in the early years of the Internet. Each class contains a varying degree of networks versus hosts per network.