3-External Recon and Enumeration Principles

Iana: https://www.iana.org/

arin : https://www.arin.net/

RIPE:https://www.ripe.net/

BGP Toolkit: https://bgp.he.net/

Domaintools: https://www.domaintools.com/

PTRArchive: http://ptrarchive.com/

ICANN: https://lookup.icann.org/lookup

https://grayhatwarfare.com/

haveibeenpwned: https://haveibeenpwned.com/

Dashboard: https://www.dehashed.com/

Domaintool: https://whois.domaintools.com/

viewdns.info: https://viewdns.info/

What Are We Looking For?

When conducting our external reconnaissance, there are several key items that we should be looking for. This information may not always be publicly accessible, but it would be prudent to see what is out there. If we get stuck during a penetration test, looking back at what could be obtained through passive recon can give us that nudge needed to move forward, such as password breach data that could be used to access a VPN or other externally facing service. The table below highlights the "`What`" in what we would be searching for during this phase of our engagement.

Data Point	Description
`IP Space`	Valid ASN for our target, netblocks in use for the organization's public-facing infrastructure, cloud presence and the hosting providers, DNS record entries, etc.
`Domain Information`	Based on IP data, DNS, and site registrations. Who administers the domain? Are there any subdomains tied to our target? Are there any publicly accessible domain services present? (Mailservers, DNS, Websites, VPN portals, etc.) Can

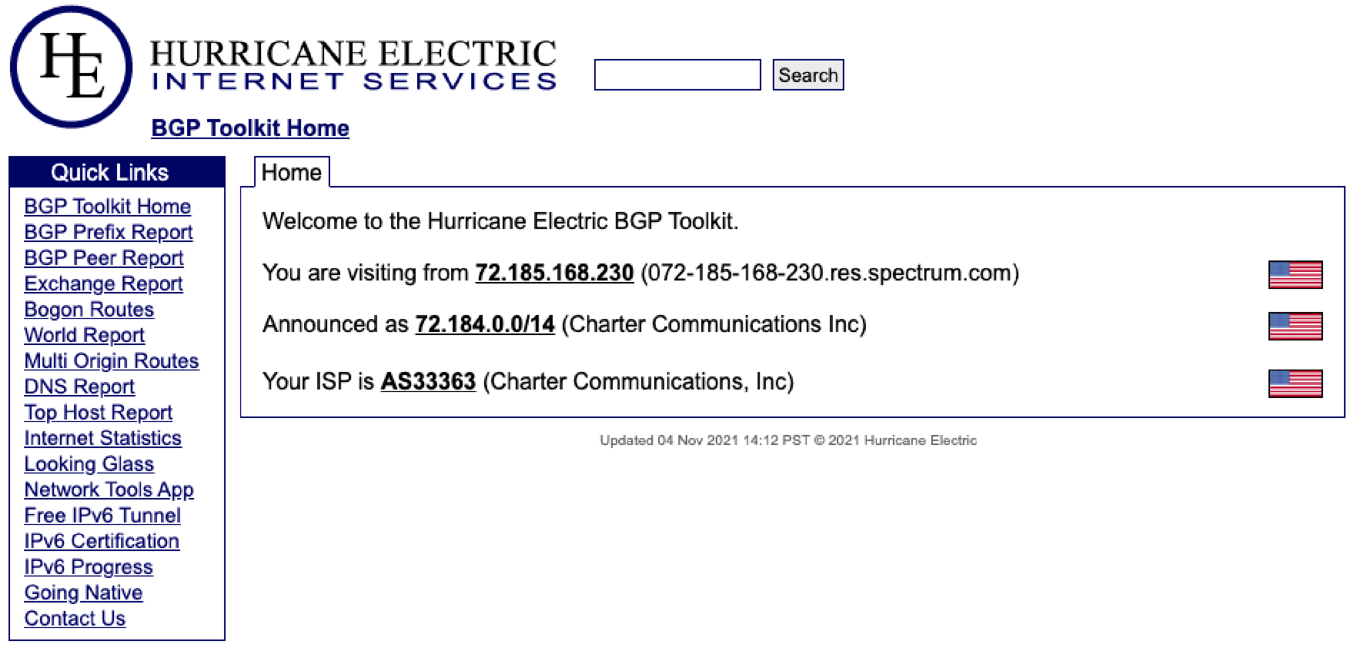
Data Point	Description
	we determine what kind of defenses are in place? (SIEM, AV, IPS/IDS in use, etc.)
`Schema Format`	Can we discover the organization's email accounts, AD usernames, and even password policies? Anything that will give us information we can use to build a valid username list to test external-facing services for password spraying, credential stuffing, brute forcing, etc.
`Data Disclosures`	For data disclosures we will be looking for publicly accessible files (.pdf, .ppt, .docx, .xlsx, etc.) for any information that helps shed light on the target. For example, any published files that contain `intranet` site listings, user metadata, shares, or other critical software or hardware in the environment (credentials pushed to a public GitHub repo, the internal AD username format in the metadata of a PDF, for example.)
`Breach Data`	Any publicly released usernames, passwords, or other critical information that can help an attacker gain a foothold.

We have addressed the `why` and `what` of external reconnaissance; let's dive into the `where` and `how`.

Where Are We Looking?

Our list of data points above can be gathered in many different ways. There are many different websites and tools that can provide us with some or all of the information above that we could use to obtain information vital to our assessment. The table below lists a few potential resources and examples that can be used.

Resource	Examples
`ASN / IP registrars`	IANA, arin for searching the Americas, RIPE for searching in Europe, BGP Toolkit
`Domain Registrars & DNS`	Domaintools, PTRArchive, ICANN, manual DNS record requests against the domain in question or against well known DNS servers, such as `8.8.8.8`.
`Social Media`	Searching Linkedin, Twitter, Facebook, your region's major social media sites, news articles, and any relevant info you can find about the organization.
`Public-Facing Company Websites`	Often, the public website for a corporation will have relevant info embedded. News articles, embedded documents, and the "About Us" and "Contact Us" pages can also be gold mines.
`Cloud & Dev Storage Spaces`	GitHub, AWS S3 buckets & Azure Blog storage containers, Google searches using "Dorks"
`Breach Data Sources`	HaveIBeenPwned to determine if any corporate email accounts appear in public breach data, Dehashed to search for corporate emails with cleartext passwords or hashes we can try to crack offline. We can then try these passwords against any exposed login portals (Citrix, RDS, OWA, 0365, VPN, VMware Horizon, custom applications, etc.) that may use AD authentication.



Welcome to the Hurricane Electric BGP Toolkit.

You are visiting from 72.185.168.230 (072-185-168-230.res.spectrum.com)

Announced as 72.184.0.0/14 (Charter Communications Inc)

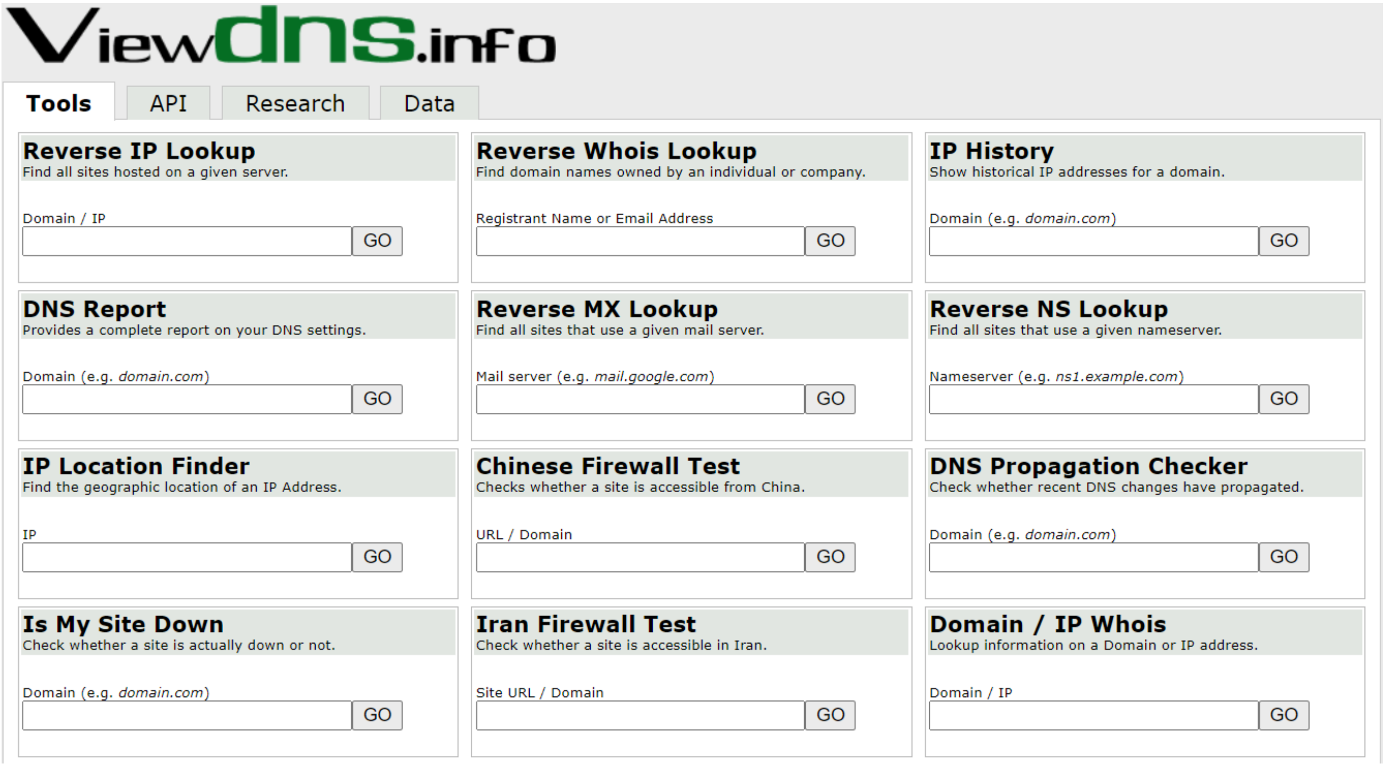
Your ISP is AS33363 (Charter Communications, Inc)

Updated 04 Nov 2021 14:12 PST © 2021 Hurricane Electric

DNS

DNS is a great way to validate our scope and find out about reachable hosts the customer did not disclose in their scoping document. Sites like domaintools, and viewdns.info are great spots to start. We can get back many records and other data ranging from DNS resolution to testing for DNSSEC and if the site is accessible in more restricted countries. Sometimes we may find additional hosts out of scope, but look interesting. In that case, we could bring this list to our client to see if any of them should indeed be included in the scope. We may also find interesting subdomains that were not listed in the scoping documents, but reside on in-scope IP addresses and therefore are fair game

Viewdns.info



Reverse IP Lookup
Find all sites hosted on a given server.
Domain / IP

Reverse Whois Lookup
Find domain names owned by an individual or company.
Registrant Name or Email Address

IP History
Show historical IP addresses for a domain.
Domain (e.g. *domain.com*)

DNS Report
Provides a complete report on your DNS settings.
Domain (e.g. *domain.com*)

Reverse MX Lookup
Find all sites that use a given mail server.
Mail server (e.g. *mail.google.com*)

Reverse NS Lookup
Find all sites that use a given nameserver.
Nameserver (e.g. *ns1.example.com*)

IP Location Finder
Find the geographic location of an IP Address.
IP

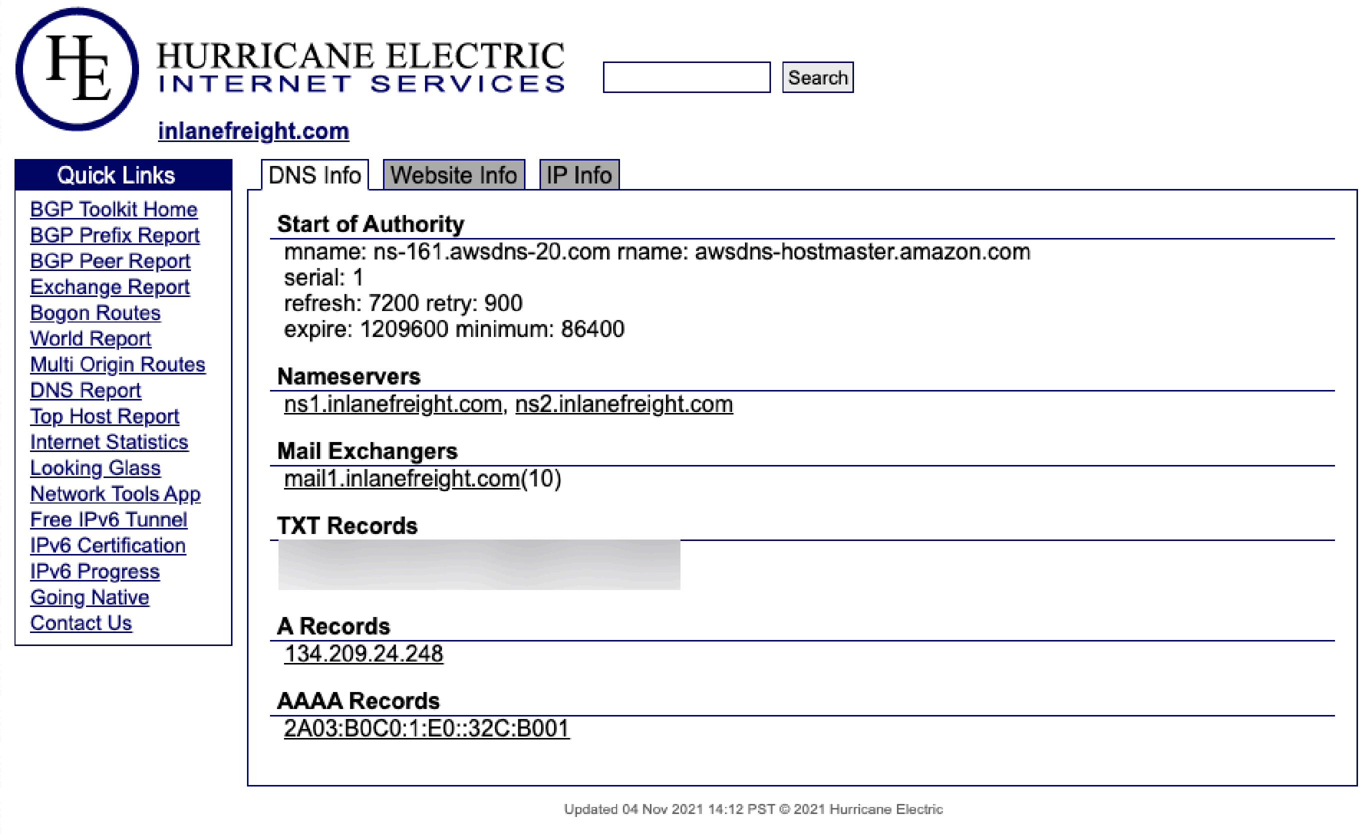
Chinese Firewall Test
Checks whether a site is accessible from China.
URL / Domain

DNS Propagation Checker
Check whether recent DNS changes have propagated.
Domain (e.g. *domain.com*)

Is My Site Down
Check whether a site is actually down or not.
Domain (e.g. *domain.com*)

Iran Firewall Test
Check whether a site is accessible in Iran.
Site URL / Domain

Domain / IP Whois
Lookup information on a Domain or IP address.
Domain / IP



inlanefreight.com

Start of Authority

mname: ns-161.awsdns-20.com rname: awsdns-hostmaster.amazon.com
serial: 1
refresh: 7200 retry: 900
expire: 1209600 minimum: 86400

Nameservers

ns1.inlanefreight.com, ns2.inlanefreight.com

Mail Exchangers

mail1.inlanefreight.com(10)

TXT Records

[redacted]

A Records

134.209.24.248

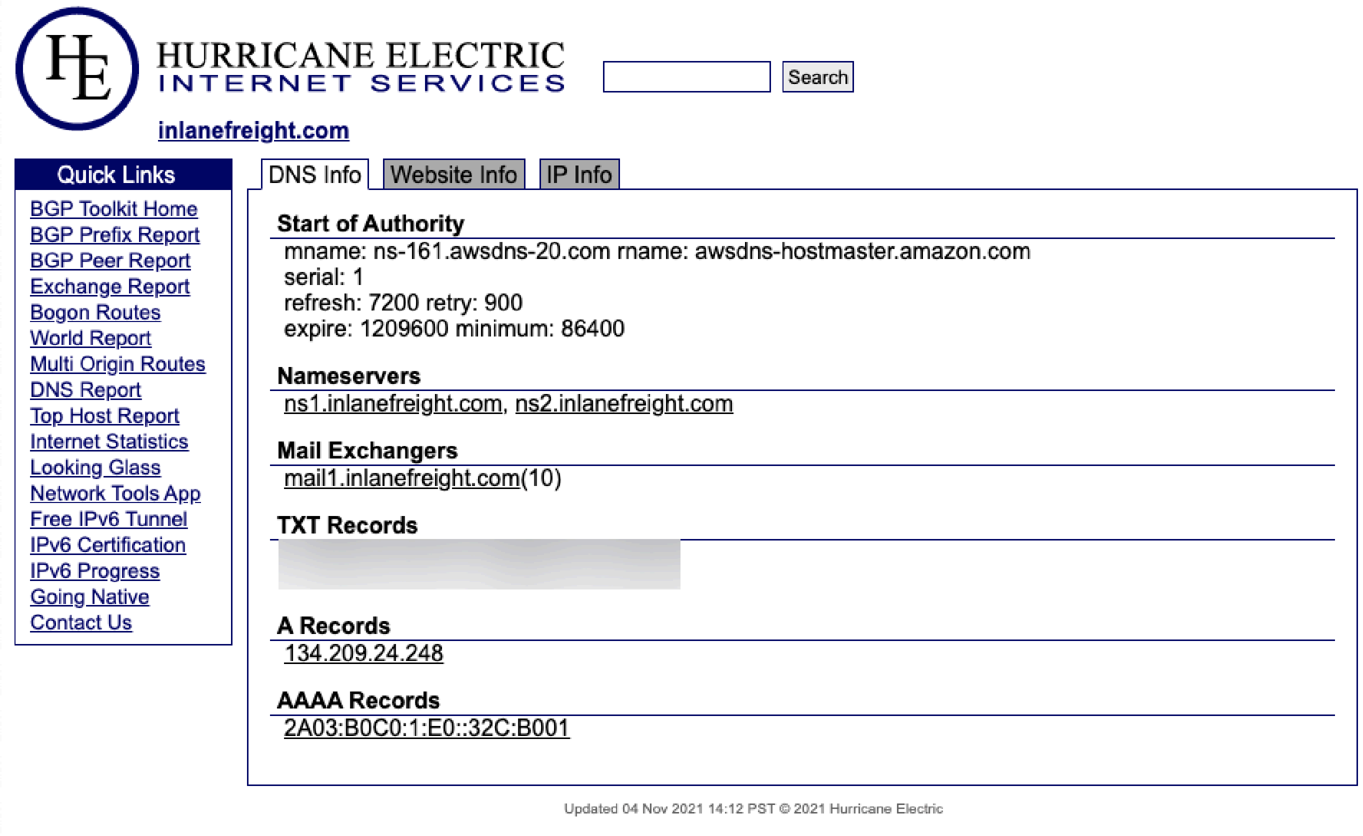
AAAA Records

2A03:B0C0:1:E0::32C:B001

Updated 04 Nov 2021 14:12 PST © 2021 Hurricane Electric

Example Enumeration Process

We have already covered quite a few concepts pertaining to enumeration. Let's start putting it all together. We will practice our enumeration tactics on the `inlanefreight.com` domain without performing any heavy scans (such as Nmap or vulnerability scans which are out of scope). We will start first by checking our Netblocks data and seeing what we can find.


inlanefreight.com

Start of Authority

mname: ns-161.awsdns-20.com rname: awsdns-hostmaster.amazon.com
serial: 1
refresh: 7200 retry: 900
expire: 1209600 minimum: 86400

Nameservers

ns1.inlanefreight.com, ns2.inlanefreight.com

Mail Exchangers

mail1.inlanefreight.com(10)

TXT Records

[redacted]

A Records

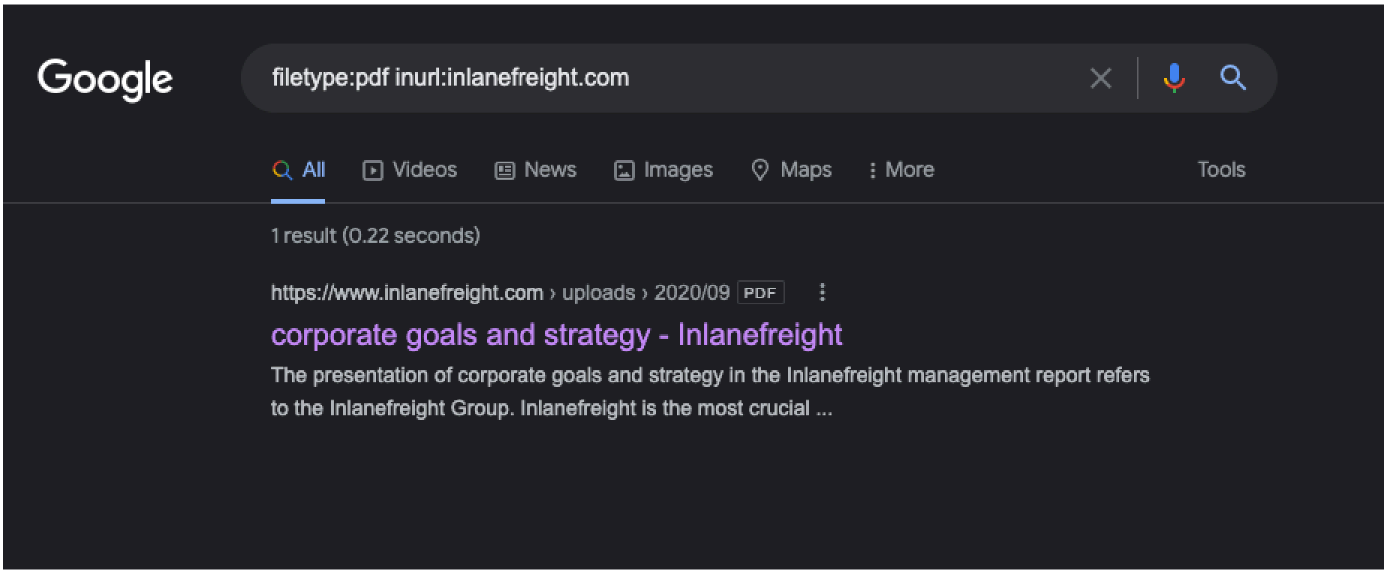
134.209.24.248

AAAA Records

2A03:B0C0:1:E0::32C:B001

Updated 04 Nov 2021 14:12 PST © 2021 Hurricane Electric

Use Google Dorks: The first check we ran was looking for any documents. Using `filetype:pdf inurl:inlanefreight.com` as a search, we are looking for PDFs.



filetype:pdf inurl:inlanefreight.com

1 result (0.22 seconds)

https://www.inlanefreight.com › uploads › 2020/09

corporate goals and strategy - Inlanefreight

The presentation of corporate goals and strategy in the Inlanefreight management report refers to the Inlanefreight Group. Inlanefreight is the most crucial ...

Username Harvesting

We can use a tool such as linkedin2username to scrape data from a company's LinkedIn page and create various mashups of usernames (flast, first.last, f.last, etc.) that can be added to our list of potential password spraying targets.

linkedin2username : https://github.com/initstring/linkedin2username

Credential Hunting

Dehashed is an excellent tool for hunting for cleartext credentials and password hashes in breach data. We can search either on the site or using a script that performs queries via the API. Typically we will find many old passwords for users that do not work on externally-facing portals that use AD auth (or internal), but we may get lucky! This is another tool that can be useful for creating a user list for external or internal password spraying.

Deshashed : http://dehashed.com/

Note: For our purposes, the sample data below is fictional.

```
0xAmr0zZakaria@htb[/htb]$ sudo python3 dehashed.py -q inlanefreight.local -p

id : 5996447501
email : roger.grimes@inlanefreight.local
username : rgrimes
password : Ilovefishing!
hashed_password :
name : Roger Grimes
vin :
```

```
address :
phone :
database_name : ModBSolutions

id : 7344467234
email : jane.yu@inlanefreight.local
username : jyu
password : Starlight1982_!
hashed_password :
name : Jane Yu
vin :
address :
phone :
database_name : MyFitnessPal

<SNIP>
```