External Recon Information Gathering

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 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.

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.

Revision #1
Created 2025-02-06 21:18:16 UTC by Ryan
Updated 2025-02-12 01:11:17 UTC by Ryan