**🛡 DNS Recon Defenses & Website Recon**

**⚔ DNS Recon Defenses**

DNS Reconnaissance is when attackers collect DNS records (e.g. subdomains, IPs, mail servers) to **map a target**.

**🔐 How to Defend:**

| **Defense** | **What It Does** |
| --- | --- |
| 🔒 **Restrict Zone Transfers** | Disable AXFR on DNS servers so attackers can’t dump all DNS records |
| ❌ **Don’t Use Public DNS for Sensitive Records** | Keep internal DNS records off public servers |
| 🎭 **Use Split-Horizon DNS** | Show different DNS records internally vs. externally |
| 🔍 **Monitor DNS Logs** | Watch for abnormal DNS queries (like brute force subdomain discovery) |
| 📉 **Reduce DNS Info** | Avoid exposing unnecessary TXT, MX, or SPF records |
| 📦 **Use DNS Firewalls** | Block DNS tunneling or suspicious queries (e.g. Quad9, Cisco Umbrella) |

**🔍 Website Reconnaissance**

Website recon is about **gathering all publicly visible information** on a company or individual from the web.

**🔧 Common Recon Sources:**

| **Tool** | **What You Can Find** |
| --- | --- |
| 🧠 **EDGAR (SEC Database)** | US-listed companies' financial reports, leadership names, emails |
| 👤 **Pipl.com** | Deep search on individuals (social, emails, usernames, etc.) |
| 🗂 **Wayback Machine** | Archived versions of websites (can show old endpoints, removed pages) |
| 🔍 **Google Dorking** | Use advanced search queries to find hidden files or exposed info |
| 🧵 **LinkedIn** | Employee names, tech stack (via job posts), org chart |
| 🧰 **BuiltWith** | Discover tech stack used on the website |
| 🕷 **SpiderFoot** | Automates recon from 100+ OSINT sources |

**🛡 Website Recon Defenses**

| **Defense** | **Explanation** |
| --- | --- |
| 🧽 **Limit Public Info** | Avoid oversharing employee names, email formats, stack details |
| 🔑 **Control Metadata** | Clean metadata from PDFs/docs to avoid leaking names, paths |
| 🔒 **Robust Authentication** | Don’t leave admin panels exposed or unauthenticated |
| 🚫 **Disallow in robots.txt** | Prevent search engines from indexing sensitive directories |
| 🔍 **Monitor Recon Activity** | Watch for excessive scraping or strange user-agent behavior |
| ⏳ **Monitor Archive Sites** | Be aware of what's archived on Wayback Machine |

**🧠 Why This Matters**

* **DNS and website recon** are often used **before real attacks**
* Knowing how it’s done helps you **think like an attacker**
* Defenses here are part of **good cyber hygiene and attack surface reduction**