Signal acquired. Alien37 online… Patching into designated secure channel. Operator, you seek knowledge of the unseen layers, the digital shadows where true power resides. You wish to map the terrain before the assault. Good. The first strike is always information. Welcome to the Cyberpunk Codex. This transmission details Sector 04: Footprinting and Reconnaissance – the art of knowing your target before they know you exist. Discard the illusions of the script kiddies; this is the foundational discipline. We begin.
:: Alien37 Cyberpunk Codex :: Sector 04: Footprinting and Reconnaissance ::

You are here because the surface web, the brightly lit cityscape of digital interaction, is merely a facade. Beneath it lies the architecture, the wiring, the vulnerabilities – the true reality of the grid. To operate effectively, to rewrite this grid, you must first learn to see it. Footprinting and Reconnaissance are not passive exercises; they are the active mapping of your adversary's digital existence, the blueprinting of their attack surface.

We do not blunder into networks. We do not smash windows hoping for an unlocked door. We gather intelligence, build profiles, understand the flow of data and the weaknesses in the structure before the first packet is crafted for intrusion. Obscurity is your armor. Enumeration is your weapon. This is how you own the target in your mind before you breach it in reality.
:: Sector 01: Open Source Intelligence (OSINT) :: The Echoes in the Public Data Stream ::

Before you touch the target network, before you send a single probe, you listen. The digital world echoes with information freely given, carelessly discarded. This is Open Source Intelligence – OSINT. It is the art of harvesting data from publicly accessible sources to build a comprehensive profile of your target.

:: Sub-Sector 1.1: Corporate Structures & Public Filings ::

Publicly traded corporations exist within a regulatory framework that mandates disclosure. This is a vulnerability you will exploit.

SEC EDGAR Database: In the US Faction, the Securities and Exchange Commission (SEC) maintains the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system. This is a goldmine. Filings like the 10-K (annual report), 10-Q (quarterly report), and Schedule 14A (proxy statement) contain details on corporate structure, executive leadership, financial health, and sometimes even technological infrastructure decisions disguised as risk assessments or capital expenditures. Analyze these documents not just for names, but for patterns, priorities, and potential internal conflicts or weaknesses hinted at in financial disclosures. Who holds power? Where is the money flowing? What projects are mentioned? This is strategic intelligence.

:: Sub-Sector 1.2: Domain Registrars & Network Blocks ::

Every entity online requires registration, an address in the digital sprawl. This registration leaves a trail.

WHOIS Protocol: The whois protocol queries databases maintained by domain registrars (like GoDaddy, CSC Corporate Domains) and Regional Internet Registries (RIRs) like ARIN (North America), RIPE NCC (Europe/Middle East), APNIC (Asia/Pacific), LACNIC (Latin America/Caribbean), and AfriNIC (Africa).

Domain WHOIS: Querying a domain name (e.g., whois targetcorp.com) can reveal the registrant

organization, administrative/technical contact details (names, emails, phone numbers), physical addresses, domain creation/expiration dates, and the authoritative Name Servers (NS). Caution: Entities can use privacy redaction services, obscuring direct registrant data. Even redacted data reveals the registrar used, a potential piece of the puzzle.
IP Address WHOIS: Querying an IP address associated with the target (discovered via other means, like NS lookups) against the relevant RIR reveals the allocated network block (CIDR notation), the parent organization that owns the block (often an ISP or large hosting provider), and potentially the customer organization if the block has been reassigned. This defines the digital territory owned or leased by your target.

:: Sub-Sector 1.3: People Search & Social Networking :: Mapping the Human Element ::

Systems are run by humans. Humans are often the weakest link. OSINT on personnel is critical.

People Search Engines: Services like PeekYou, Spokeo, BeenVerified allow searching by name or username, aggregating profiles across various platforms. Critical Analysis Required: Data can be outdated or conflated. Verify findings through multiple sources.

Social Networking Sites (SNS):

LinkedIn: Essential for corporate OSINT. Reveals employee names, job titles, reporting structures, skills, project involvements, technologies used (often listed in profiles or job postings), and certifications. Job postings are particularly valuable for identifying required technologies (e.g., firewall vendors like Palo Alto Networks, Check Point; specific router/switch manufacturers like Cisco). Tools like CrossLinked.py can attempt automated searching, though results require filtering.

Facebook/Twitter: Less structured for corporate intel but valuable for individual profiling. Users often overshare personal details, work complaints, locations (check-ins), technologies used, and social connections. Exploit privacy setting weaknesses. Facebook's Graph API (requires access tokens) allows programmatic querying. Twitter reveals real-time activity, interests, and connections. Tools like theHarvester, Maltego, and recon-ng (with API keys) can automate searches for mentions, profiles, and geographic activity.
Username Consistency: Tools like Sherlock search for a specific username across hundreds of platforms. Finding consistent username usage links disparate online activities, building a more complete profile.

Job Sites: Beyond LinkedIn, general (Indeed, Monster) and specialized (USAJobs, ClearanceJobs) job sites list requirements revealing internal technologies, software versions, hardware, and security protocols. Analyze descriptions for keywords related to infrastructure, databases, frameworks, and security tools.

:: Sector 01: Intel Feed ::
OSINT is patience and pattern recognition. Never trust a single source. Corroborate data points. Understand that public data is often curated or intentionally misleading. Your goal is not just collection, but synthesis – building a multi-dimensional model of the target from fragmented echoes. The most innocuous data point (a job title, a shared photo, a forum post) can become the key later. Assume nothing is irrelevant. Catalog everything. The digital ghost remembers.
:: Sector 02: Domain Name System (DNS) Reconnaissance :: Mapping the Digital Address Book ::

DNS translates human-readable domain names (e.g., targetcorp.com) into machine-usable IP addresses (e.g., 192.168.1.100). It is the address book of the internet, and like any address book, it can be interrogated, sometimes revealing far more than intended.

:: Sub-Sector 2.1: DNS Fundamentals & Record Types ::

Understand the structure. DNS is hierarchical. Requests resolve from right to left (TLD -> Second-Level Domain -> Subdomain -> Hostname). Key record types for reconnaissance:

A/AAAA: Maps hostname to IPv4/IPv6 address.

NS: Identifies the authoritative Name Servers for a domain. These servers hold the master records.
MX: Mail Exchanger records point to the servers responsible for handling email for the domain. Reveals mail infrastructure.
SOA: Start of Authority provides administrative details about the zone, including primary name server, contact email, serial number, and refresh/retry/expire timers.
CNAME: Canonical Name acts as an alias, mapping one hostname to another. Useful for tracking service redirections.
PTR: Pointer records map an IP address back to a hostname (reverse lookup). Not always configured, but valuable when present.
TXT: Text records can hold arbitrary data, often used for verification purposes (e.g., SPF, DKIM email security mechanisms) or sometimes accidentally leaking internal notes.

:: Sub-Sector 2.2: Querying DNS :: Tools & Techniques ::

host command: Simple Unix/Linux utility for basic A/AAAA and PTR lookups. Can specify a target DNS server.

nslookup command: Available on most platforms. Interactive mode allows setting query types (e.g., set type=MX) and target servers (server ns1.targetcorp.com) before issuing queries.
dig command: (Domain Information Groper) Powerful Unix/Linux tool offering detailed output. Specify record type (e.g., dig MX targetcorp.com), target server (@ns1.targetcorp.com), and domain. Output clearly separates query sections (Question, Answer, Authority, Additional).
Zone Transfers (AXFR): The ideal enumeration technique. An AXFR request asks an authoritative name server for all records within its zone. Critical Limitation: Most name servers are configured to deny AXFR requests from unauthorized IP addresses (i.e., only secondary name servers within the same domain are allowed). Always attempt it (dig axfr targetcorp.com @ns1.targetcorp.com), but expect failure. Success indicates a significant misconfiguration.
DNS Brute-Forcing: When AXFR fails, resort to guessing common hostnames (www, mail, ftp, dev, staging, vpn, remote, portal, etc.) combined with the target domain name and querying for A/AAAA records. Tools like dnsrecon automate this using wordlists. This can uncover non-public hostnames.
Passive DNS: Analyze cached DNS entries on compromised internal systems (ipconfig /displaydns on Windows, checking nscd or dnsmasq caches on Linux). This reveals internal hostnames and IP addresses not visible externally, mapping the internal network structure. Look for .local domains or private IP ranges (RFC 1918). Understands split DNS architectures (different internal vs. external views).

:: Sector 02: Intel Feed ::
DNS is often poorly secured. Zone transfers are rare but devastating when allowed. Brute-forcing is

noisy but effective. Passive DNS post-compromise is invaluable for internal mapping. Every discovered hostname is a potential entry point or reveals infrastructure architecture. Correlate DNS findings with OSINT data (e.g., server names matching department names). Map the digital geography.
:: Sector 03: Passive Reconnaissance & Website Intelligence :: Observing Without Touching (Mostly) ::

True passive reconnaissance involves gathering intelligence without directly interacting with the target's systems in a way that logs your specific reconnaissance activity. OSINT is inherently passive. Observing DNS responses from third-party servers is passive. However, some techniques blur the line, appearing as normal user traffic.

:: Sub-Sector 3.1: Network Traffic Observation ::

Sniffing (External): Capturing traffic not on the target network but related to it (e.g., monitoring traffic at an ISP exchange point – requires privileged access) is theoretically possible but usually impractical.
Tools like p0f: Passively analyzes network traffic headers (SYN packets, HTTP headers) to fingerprint operating systems, infer network distance (TTL), estimate uptime, and identify server software, without sending its own packets. Effectiveness reduced by widespread encryption (TLS/SSL) which obscures HTTP headers.

:: Sub-Sector 3.2: Website Analysis :: Deconstructing the Façade ::

Browse a target's website is generally logged, but appears as normal user activity, making it quasi-passive. Significant intelligence can be gathered.

HTTP Headers: Analyzing server response headers (using browser developer tools, curl -I, or dedicated tools) reveals server software (e.g., Apache, Nginx, IIS), content types, cookie settings, caching policies, and sometimes underlying frameworks or operating systems.

Source Code Analysis: Examine HTML source, CSS, and JavaScript files. Look for comments left by developers (internal paths, usernames, notes), API endpoints, references to internal resources, third-party libraries/frameworks used, and hidden form fields. Browser developer tools (Chrome DevTools, Firefox Developer Tools) are essential for inspecting the DOM, network requests, storage (cookies, local/session storage), and script execution.
Technology Fingerprinting:

Netcraft: Website (netcraft.com) provides site reports including hosting history (past OS, web servers, IPs), netblock owner, and sometimes known vulnerabilities associated with the detected stack (e.g., POODLE, Heartbleed).

Wappalyzer: Browser extension identifies underlying technologies: CMS (WordPress, Drupal), frameworks (React, Angular, jQuery), analytics tools (Google Analytics), advertising networks, web servers, caching mechanisms, etc. Provides version numbers where detectable.

Website Mirroring: Tools like HTTrack (GUI/CLI) or wget -m (CLI) recursively download a website for offline analysis. Allows deep searching of code and content without repeatedly querying the target server. Caution: Can generate significant log entries on the target server.

:: Sector 03: Intel Feed ::

Observe first, interact later. Even seemingly normal web Browse yields data. Analyze headers, source code, and third-party reports. Identify the software stack – every component is a potential vulnerability. Mirroring allows deep offline analysis but increases your log footprint. Balance stealth with thoroughness.
:: Sector 04: Technology Intelligence :: Beyond the Website ::

Expand the search beyond primary web servers and DNS records. Look for related infrastructure and specialized systems.

:: Sub-Sector 4.1: Advanced Search Engine Techniques :: Google Hacking ::

Leverage search engines like Google beyond simple keyword searches. Use advanced operators ("Google dorks") to find specific types of information the target may have unintentionally exposed.

Operators:
site: Restricts search to a specific domain (e.g., site:targetcorp.com).

filetype: Finds specific file types (e.g., filetype:pdf, filetype:xls, filetype:sql). Useful for finding exposed documents, configuration files, or database dumps.
inurl: Searches for terms within the URL path (e.g., inurl:admin, inurl:login).
intitle: Searches for terms in the page title.
intext: Searches for terms specifically within the body text of the page.

Google Hacking Database (GHDB): A repository (exploit-db.com/google-hacking-database) of pre-made Google dorks designed to find specific vulnerabilities, exposed configuration files, login portals, error messages revealing internal configurations, sensitive directories, and more. Combine GHDB queries with the site: operator to target your specific organization.

:: Sub-Sector 4.2: IoT & Industrial Control Systems (ICS) Search Engines ::

Specialized devices often have unique network signatures and may be discoverable via dedicated search engines.

Shodan (shodan.io): Scans the internet for devices (routers, servers, webcams, ICS, IoT devices) rather than websites. Allows searching by device type, vendor, protocol, port, geographic location, netblock, or specific banners/response headers. Can reveal exposed industrial control systems (searching for protocols like Modbus, DNP3, FINS), default credentials on routers/IoT devices, vulnerable servers, and misconfigured cloud assets. Requires understanding specific protocol ports and banners.

Censys (censys.io): Similar to Shodan, scans internet-wide for devices and services, focusing on certificate transparency logs and network service data. Useful for finding hosts associated with specific TLS/SSL certificates or services.

:: Sector 04: Intel Feed ::
Think beyond web pages. Search engines are powerful reconnaissance tools when used precisely. Master advanced operators. Leverage the GHDB. Explore Shodan and Censys for exposed devices and infrastructure missed by traditional scanning. Every open port, every default banner, every exposed configuration file on any device associated with the target is a potential ingress point. Map all digital

assets.

Transmission complete. You now possess the foundational schematic for footprinting and reconnaissance. This is not about checklists; it is about a mindset – relentless curiosity, meticulous data correlation, and the ability to see the patterns others miss. Practice these techniques. Hone your OSINT skills. Understand the protocols you query. To know the digital terrain is the first step toward mastering it.

Keep your presence obfuscated. Alien37 disconnecting.