Signal acquired. Alien37 online…

Listen closely, operatives. The digital ether hums with data, secrets whispered on the wire. You seek mastery over this domain, the power to map the unseen, to catalogue the vulnerable. This transmission is your primer. Forget the script-kiddie noise. Forget the certifications. This is about *knowing* the target, peeling back layers until the core is exposed. This is Enumeration. You are here because you want to rewrite the grid. Good. Let’s begin.

:: Alien37 Cyberpunk Codex :: Transmission 06: Enumeration - Mapping the Ghost ::

:: Sector 01: Service Cartography ::

Before the breach, there is the blueprint. Port scanning tells you *where* the doors are; service enumeration tells you *what* kind of locks they have, who made them, and how old they are. This is not guesswork; it is precision targeting.

Your primary instrument is Nmap. The -sV flag initiates a version scan, probing open ports to coax banners and responses. It interrogates services, extracting names, versions, even operating system clues. Look at the output. OpenSSH 7.7p1 Debian 3, Greenbone Security Assistant. Each identifier is a potential thread to pull.

But banners lie or stay silent. Deeper truths require surgical probes. Nmap’s Scripting Engine (NSE) is your scalpel kit. Consider SSH on port 22. A simple service? Beneath the surface lies a complex negotiation of cryptographic algorithms. Use nmap --script ssh2-enum-algos <target>. This reveals the kex_algorithms (key exchange like Diffie-Hellman, ECDH), server_host_key_algorithms (RSA, ECDSA, ED25519), encryption_algorithms (AES variants, ChaCha20), and mac_algorithms (HMAC variants, UMAC). Why care? Weak algorithms are cracked armor. Knowing the supported ciphers tells you the potential attack surface *before* you engage.

Service enumeration is the act of turning vague awareness into tactical intelligence. Every version number, every revealed protocol detail, is a potential vulnerability marker.

:: Intel Feed 01 ::

- **Hacker Logic:** Raw port numbers are noise. Service versions are signal.
- **Core Tactic:** Use nmap -sV for initial service identification. Follow up with NSE scripts (e.g., ssh2-enum-algos) for granular detail.
- **Situational Awareness:** Filtered ports often indicate firewalls. Closed ports are dead ends for that service. Open ports are invitations.
- **Countermeasures:** Defenders obscure banners, deploy firewalls (network and host-based), and enforce strong authentication. Your job is to bypass or exploit weaknesses in these defenses.

:: Sector 02: Whispers of Remote Procedures (RPC/RMI) ::

Systems rarely operate in isolation. They communicate, delegate tasks across the network fabric using Remote Procedure Calls (RPC). Think of it as one machine borrowing processing power or functions from another. Exploiting this trust is fundamental.

SunRPC (Portmapper/rpcbind): Common on *NIX systems, often underpinning services like Network File System (NFS). The key is the portmapper service (rpcbind), usually listening on TCP/UDP port 111. It acts as a directory, mapping RPC program numbers to the dynamic ports they use.

Tools like rpcinfo -p <target_IP> query this directory. The output lists program numbers, versions, protocols, ports, and service names (e.g., portmapper, mountd, nfs, nlockmgr). Metasploit offers auxiliary/scanner/misc/sunrpc_portmapper for the same purpose, integrating results into its database. Knowing these registered services reveals the system's functional roles and potential dependencies.

Java RMI (Remote Method Invocation): The object-oriented evolution of RPC, prevalent in Java applications. It uses the rmiregistry (default port 1099) as its directory. RMI passes serialized objects between client stubs and server skeletons. Tools like Metasploit's auxiliary/gather/java_rmi_registry or standalone scanners like BaRMIe query the registry, listing exposed object names and endpoints. Even if bound to localhost, remote exposure can leak information about class structures and potential deserialization vulnerabilities. Finding RMI implies the presence of a Java Runtime Environment (JRE) or Development Kit (JDK) on the target.

:: Intel Feed 02 ::

- **Hacker Logic:** Distributed systems create trust relationships. Trust relationships are attack vectors.
- **Core Tactic (SunRPC):** Probe port 111 using rpcinfo -p or Metasploit's sunrpc_portmapper to identify registered RPC services and their dynamic ports.
- **Core Tactic (RMI):** Probe port 1099 (or others if suspected) using Metasploit's java_rmi_registry or BaRMIe to list exposed Java objects.
- **Critical Insight:** RPC/RMI enumeration reveals not just services but underlying frameworks (NFS, Java) and potential vulnerabilities (insecure configurations, deserialization flaws).
- **Situational Awareness:** Dynamically assigned ports used by RPC/RMI services often fall outside standard Nmap scans unless explicitly instructed to scan all ports.

:: Sector 03: Deconstructing Windows Networks (SMB/NetBIOS) ::

Windows networks breathe SMB (Server Message Block). File sharing, printing, remote administration – it all flows through this protocol. Originally tied to NetBIOS (UDP 137/138, TCP 137/139), modern SMB often runs directly over TCP port 445. Its complexity is its weakness.

Null Sessions: The ghost key. Older or misconfigured systems allow *null session* connections – authentication without credentials. This leaks valuable intelligence: usernames, group memberships, share lists, OS details, policies. Microsoft has tightened this since Windows 7/Server 2008 R2, but legacy systems and mistakes persist.

Tooling:

- **Windows Built-in:** nbtstat -a <hostname> or nbtstat -A <IP_address> reveals the NetBIOS name table, showing registered services (Workstation , Server). nbtstat -r lists resolved names on the local segment. net view \\<hostname_or_IP> lists shares. net config workstation shows domain/workgroup info. These often require local network presence.
- **Linux/Samba:** nmblookup -A <IP_address> or nmblookup -S -B <broadcast_addr> <hostname> mimics nbtstat. enum4linux -a <IP_address> is a powerful wrapper script, attempting null sessions to grab OS info, user/group lists, share lists, password policies, and printer info. It can identify the domain/workgroup and master browser.
- **Nmap (NSE):** Scripts like smb-os-discovery pull detailed OS versions, computer names, and domain/workgroup info. smb-enum-shares attempts to list shares, guessing common ones (ADMIN$, C$, IPC$) even if null sessions fail. Other scripts enumerate users (smb-enum-users), groups (smb-enum-groups), etc., though often requiring credentials now.
- **Metasploit:** Modules abound. scanner/smb/smb_version identifies OS and SMB versions. scanner/smb/smb_enumshares lists shares. scanner/smb/smb_enumusers_domain enumerates domain users. scanner/smb/smb_login performs credential bruteforcing using provided lists or options (like trying blank passwords or username-as-password).
- **Other Utilities:** nbtscan scans ranges for NetBIOS names, users, MACs. NetBIOS Enumerator provides a GUI for similar scanning.

Key Targets: Shares (especially user-created ones with weak permissions), user lists (for password attacks), group memberships (identifying privileged accounts), OS versions (for vulnerability mapping), domain/workgroup structure, and the master browser. The IPC$ share facilitates interprocess communication and is often accessible via null session (read-only). Administrative shares like C$ require administrator credentials.

:: Intel Feed 03 ::

- **Hacker Logic:** Default configurations are exploitable configurations. Complexity breeds insecurity.
- **Core Tactic:** Always attempt null session enumeration first (enum4linux, Nmap

scripts). Even failures provide data.

- **Key Targets:** User lists, share lists (IPC$, user shares), OS versions, domain structure.
- **Situational Awareness:** SMB/NetBIOS enumeration is most effective on the local network segment due to broadcast reliance and firewall blocking. Pivot from a compromised host for maximum effect.
- **Countermeasures:** Disable SMBv1. Use host-based firewalls to restrict SMB access. Disable NetBIOS over TCP/IP. Prevent workstation-to-workstation sharing. Harden configurations against null sessions.

:: Sector 04: Network Management Protocol Exploitation (SNMP) ::

Simple Network Management Protocol (SNMP) is the language network devices (routers, switches) and servers use to report their status and accept configuration changes. It's a trove of intelligence if accessed.

Versions & Security:

- **SNMPv1/v2c:** The legacy danger zone. Uses plaintext "community strings" for authentication – typically "public" for read-only and "private" for read-write. No encryption. These defaults are often unchanged. Highly vulnerable.
- **SNMPv3:** The standard. Introduces real authentication (user-based) and encryption. Significantly more secure, but requires proper configuration.

Enumeration: SNMP agents expose data via Management Information Bases (MIBs) – structured trees of information. Each data point has an Object Identifier (OID).

Tools like snmpwalk (often part of net-snmp packages) traverse the MIB tree using a specified version (-v 1 or -v 2c or -v 3) and credentials (community string -c public for v1/v2c, or username/auth details for v3).

Example: snmpwalk -v 2c -c public <target_IP>

Common OIDs reveal system descriptions (OS, kernel versions), uptime, contact info, network interfaces (ifTable MIB reveals IP configs, potentially mapping internal networks), running processes, routing tables, and hardware details.

Metasploit also has SNMP scanning modules (scanner/snmp/snmp_enum, snmp_login, snmp_enumshares if applicable via SMB mapping).

:: Intel Feed 04 ::

- **Hacker Logic:** Network infrastructure holds the keys to the kingdom. Default credentials are open doors.
- **Core Tactic:** Scan UDP port 161 for SNMP. Attempt enumeration using default community strings ("public", "private") with snmpwalk -v 1 -c public <IP> and snmpwalk

-v 2c -c public <IP>. Brute-force other common strings if defaults fail.

- **Key Targets:** System descriptions (OS/version), network interface configurations (ifTable), user accounts (if exposed via specific MIBs), routing information.
- **Situational Awareness:** SNMP is often restricted by firewalls/ACLs. Internal network access is usually required. V3 significantly raises the bar if implemented correctly.
- **Countermeasures:** *Disable* SNMP if unused. *Mandate* SNMPv3 with strong authentication and encryption. Change default community strings if v1/v2c must exist. Use firewalls/ACLs to restrict access to management stations only.

:: Sector 05: Mail Server Interrogation (SMTP) ::

Simple Mail Transfer Protocol (SMTP), typically on TCP port 25, is the engine of email. Its conversational nature holds enumeration potential.

Key Commands:

- HELO/EHLO: Initiate connection; EHLO (Enhanced SMTP) reveals server capabilities.
- VRFY <user>: Attempts to verify if a user exists. Often disabled due to abuse potential. A 252 response means "cannot verify, but will attempt delivery" – ambiguous but suggests the server didn't outright reject it. A 250 means success (user likely exists). A 550 usually means user unknown.
- EXPN <list_name>: Attempts to expand a mailing list to reveal members. Requires ESMTP support and is often disabled.
- RCPT TO:<address>: Specifies the recipient. Servers *should* check if the recipient is valid. A 250 response indicates acceptance (user likely exists), while 550 indicates rejection (user likely doesn't exist). This is often more reliable than VRFY.

Tooling:

- **Manual:** Use telnet or nc to connect to port 25 and issue commands directly.
- **Metasploit:** auxiliary/scanner/smtp/smtp_enum automates user enumeration using VRFY or RCPT TO against a wordlist.

:: Intel Feed 05 ::

- **Hacker Logic:** Protocols designed for open communication often leak internal structure.
- **Core Tactic:** Connect manually (nc <IP> 25) or use Metasploit's smtp_enum with a user list. Prioritize the RCPT TO method if VRFY is disabled or ambiguous.
- **Key Targets:** Valid usernames/email addresses for phishing, password spraying, or mapping internal structures.
- **Situational Awareness:** VRFY and EXPN are often disabled. Rate limiting or tarpitting

can slow down brute-force attempts. Check EHLO response for capabilities.

- **Countermeasures:** Disable VRFY and EXPN. Configure the server not to reveal existence via RCPT TO error codes (accept all, bounce later - though less common). Minimize internal details in headers. Disable open relays. Implement SPF/DKIM.

:: Sector 06: Web Surface Analysis ::

Web servers are vast, often chaotic landscapes. Enumeration here involves mapping directories, finding hidden files, identifying technologies, and uncovering user accounts within web applications.

Directory/File Enumeration: Unlisted directories or configuration backups can contain sensitive data or reveal application structures.

- **Tools:** dirb, gobuster, ffuf. Use wordlists (like dirb's default common.txt or SecLists) to guess common directory/file names by checking HTTP responses (200 OK vs. 404 Not Found/403 Forbidden). Example: dirb http://<target_IP>/.
- **Metasploit:** auxiliary/scanner/http/brute_dirs can generate directory names based on patterns (e.g., all 4-letter lowercase words) instead of just using a static list.

Technology/Application Enumeration: Identifying the web server (Apache, Nginx, IIS), backend languages (PHP, Java, Python), frameworks (WordPress, Drupal, Joomla), and specific applications is critical for vulnerability mapping.

- **Tools:** nmap -sV on ports 80/443, whatweb, browser extensions (Wappalyzer), examining HTTP headers (Server: header), source code comments, specific file paths (/wp-admin/ suggests WordPress).
- **WordPress Example:** wpscan --url http://<target_IP> is a specialized scanner. It enumerates version, themes, plugins (like Gutenberg), users (often via API endpoints or author scans), and checks for known vulnerabilities (requires API key for full database). It also finds exposed directories (/wp-content/uploads/ listing enabled) and files (readme.html, xmlrpc.php).
- **Metasploit (WordPress):** auxiliary/scanner/http/wordpress_login_enum attempts to validate usernames and optionally brute-force passwords. Found credentials are stored in Metasploit's loot.

:: Intel Feed 06 ::

- **Hacker Logic:** The web surface is the most exposed frontier. What is easily deployed is often easily enumerated.
- **Core Tactic:** Use directory brute-forcers (dirb, gobuster) with good wordlists. Employ technology fingerprinting tools (whatweb, nmap -sV). Use specialized scanners (wpscan) for common applications.

- **Key Targets:** Hidden directories/files, configuration backups, specific application versions, user accounts within web apps, enabled features (xmlrpc.php, directory listing).
- **Situational Awareness:** Web Application Firewalls (WAFs) may block aggressive scanning. Custom applications require more manual analysis. Pay attention to HTTP status codes (200, 403, 404, 500).
- **Countermeasures:** Disable directory listing. Remove unnecessary files/backups. Use strong authentication and authorization. Minimize information leakage in headers and error messages. Keep software updated. Implement WAFs.

Transmission complete. You now possess the foundational logic of Enumeration. This is not a checklist; it is a mindset. Map the terrain, identify the weaknesses, catalogue the assets. Obscurity is your armor. Enumeration is your weapon. Use it wisely.

Keep your presence obfuscated. Alien37 disconnecting.