MCP SERVER | NO CODE | CLOUD HOSTED

Nmap Online MCP

Map network ports and diagnose connectivity failures.

Nmap Online lets you run professional network scans and deep security audits directly through your AI agent. Check open ports, map the digital footprint of any domain, locate IPs geographically, or trace exactly how data travels across the internet—all without leaving your chat interface.

A+ Quality Score 100/100

network-scanning | port-discovery | dns-lookup | security-auditing | network-diagnostics | penetration-testing

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/nmap-online

SCAN TO VIEW

The connectivity layer between AI and the world's software.

Vinkius sits between AI and every application. All communication passes through Vinkius Cloud via the Model Context Protocol (MCP) — with governance, observability, and security at every layer.

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the connectivity layer where AI connects to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

> *The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.*
>
> — Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT

```
https://edge.vinkius.com/{token}/mcp
```

Claude · Cursor · VS Code · Windsurf · Grok · Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1) Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

> Get started at **cloud.vinkius.com** — connect your AI agent in under 60 seconds.

Nmap Online MCP

10 tools available
Cloud-hosted on Vinkius

This MCP connects you to high-powered diagnostic tools used by network engineers and security researchers. You talk naturally to your AI client, and it handles complex tasks like determining if a specific domain is owned by a company or finding all its hidden subdomains.

It goes beyond simple pings; you can inspect raw web server headers to see exactly what links a target page offers, or run comprehensive WHOIS lookups to find out who registered the site. Need to know where an IP address physically sits? You get that location data instantly. When you connect this MCP via Vinkius, your AI agent gains access to this entire suite of network intelligence, allowing you to perform advanced analysis without ever opening a command line or logging into a separate dashboard.

Core Capabilities

01 — Identify open services

Perform fast port scans against any IP or domain to pinpoint which services are running and exposed.

02 — Determine ownership details

Get full WHOIS records for a domain, revealing who owns it and when it was registered.

03 — Analyze network paths

Run traceroutes and pings to diagnose connectivity issues or measure latency between two points.

04 — Map related domains

Execute DNS lookups, including finding subdomains and mapping IPs back to their origins.

05 — Determine physical location

Translate an IP address into its geographical coordinates, country, and city.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/nmap-online** — connect your AI agent in three steps.

01 First, subscribe to this MCP within Vinkius. You can optionally plug in your own HackerTarget API key if you anticipate heavy usage.

02 Next, simply ask your AI client to run a diagnostic task. For example, 'What ports are open on example.com?'

03 Your agent processes the request and returns structured data detailing everything from open services to geographical locations.

The bottom line is that you can talk about network security like talking to an expert, and your AI client handles the rest of the command-line heavy lifting.

Built For

This MCP is built for people who treat networking as a job. Think penetration testers trying to map out a target's attack surface, or network ops staff who spend all day diagnosing intermittent connectivity failures across complex infrastructure.

Security Researcher

They use this MCP daily to quickly identify the potential weak points and exposed services of an unknown domain or IP address.

Network Administrator

When connectivity breaks, they don't waste time in a terminal; they ask their agent to run traceroutes and ping tests directly in chat to find the path failure point.

DevOps Engineer

They monitor service availability by checking HTTP response headers or running DNS lookups on deployment targets, all without leaving their primary workflow.

What Changes When You Connect

01 Diagnose connectivity issues instantly. Instead of manually running a traceroute in the terminal, ask your agent to map the path across hops and identify exactly where packet loss is happening.

02 Understand domain ownership quickly. Use `whois_lookup` to check who registered a site and when, giving you critical context about a target's age or jurisdiction.

03 Map out all associated sites. Don't just check the main URL; use `list_subdomains` to discover every related digital asset linked to that core domain name.

04 Verify web server health. Running `get_http_headers` lets you inspect raw response data, checking for security flags or specific service versions without digging into code.

05 Know where your targets are. The `geoip_lookup` tool converts a simple IP address into actionable physical location details like the country and city it's tied to.

Real-World Applications

Checking for forgotten web assets

You suspect your company owns an old domain, but you can't find its main website. You ask your agent to run a `whois_lookup` and discover the registration details. Then, you use `list_subdomains` to map out every associated subdomain, helping you recover forgotten assets.

Debugging slow site connections

A client reports that their connection times out occasionally. You ask your agent to run a `traceroute` to the destination IP. The results pinpoint exactly which network hop is causing excessive latency or packet loss, allowing you to report the failure point directly.

Assessing a competitor's public services

You need to know what kind of services a competitor runs on their main site. You ask your agent to run an `nmap_scan` against their IP and then use `get_http_headers` to see if they are running any non-standard, exposed protocols.

Finding the origin of suspicious traffic

You receive a log entry with a strange IP address. You immediately ask your agent to perform both `geoip_lookup` and `reverse_dns`. This instantly tells you not only where the IP is physically located but also what domain name it belongs to.

Patterns to Avoid

Treating network checks as isolated tasks

✗ AVOID

Manually checking a website's IP address first, then running a separate DNS lookup, and finally doing a ping test. This wastes time in multiple tools.

✓ INSTEAD

Ask your agent to correlate all three steps at once. Tell it: 'Give me the full network profile for example.com.' Your agent will run `dns_lookup`, `geoip_lookup`, and `ping_host` sequentially, giving you one cohesive report.

Over-relying on surface-level pings

✗ AVOID

Only running a basic ping test to confirm if a host is online. This only confirms the IP address is active; it doesn't tell you what services are actually exposed.

✓ INSTEAD

After confirming availability with `ping_host`, follow up by asking for an `nmap_scan`. This moves beyond simple reachability and tells you exactly which ports (like 80 or 443) are open and ready to accept connections.

Assuming a domain is the whole story

✗ AVOID

Looking up a main domain name using `whois_lookup` but failing to discover all related sites. You miss potential attack vectors.

✓ INSTEAD

After running `whois_lookup`, immediately ask your agent to run `list_subdomains`. This finds every associated subdomain, ensuring you cover the entire digital perimeter.

The Right Fit

Use this MCP when you need verifiable data about a target's network structure or security posture. Specifically, if you need to know *who* owns a domain (`whois_lookup`), *where* an IP is located (`geoip_lookup`), or *what services* are running on it (`nmap_scan`),

this is your tool. Don't use it if all you need is simple text generation or general data processing; for those, use a standard LLM agent. If you only need to read content from a page and extract links, `get_page_links` handles that specific task better than trying to run a full network audit.

Remember this: This MCP focuses purely on the mechanical aspects of networking—the addresses, the paths, the open ports. It doesn't tell you if those services are secure or how to exploit them; it just tells you they exist. For vulnerability analysis, you need specialized tools outside this scope.

The Headache of Manual Network Diagnostics

Right now, mapping out a target's network footprint is a multi-step chore. You have to jump between different command lines: one for WHOIS records, another for GeoIP data, and yet another for running port scans. Then you copy the IP address from one window and paste it into the next diagnostic tool just to trace the path.

With this MCP, your agent handles the entire sequence in natural conversation. You simply tell it what target you're looking at, and it automatically runs `whois_lookup`, `geoip_lookup`, and an `nmap_scan`—all within one cohesive answer.

Nmap Online: Comprehensive Network Mapping

You no longer need to remember which tool is for what. You don't have to manually run a `traceroute` and then check the DNS records separately. Your agent ties all that together, providing a full picture of connectivity loss or path latency immediately.

The difference is control: you get actionable network intelligence in plain text, without leaving your chat interface. It makes the whole process faster and less error-prone.

Nmap Online: 10 Network Tools

Use these tools to perform detailed network diagnostics, including port scanning, DNS lookups, IP geolocation, and full domain ownership checks.

#	TOOL	DESCRIPTION
01	`dns_lookup`	Performs a standard forward lookup to find the IP address for any specified domain name.
02	`geoip_lookup`	Translates an IP address into its physical geographical location, including country and city data.
03	`get_http_headers`	Retrieves the raw HTTP response headers from a given web page to inspect server details.
04	`list_subdomains`	Searches for associated subdomains linked to a main target domain.
05	`nmap_scan`	Executes a basic Nmap scan, identifying which ports and services are active on a host.
06	`get_page_links`	Extracts every single URL link found within the HTML content of a target web page.
07	`ping_host`	Sends ICMP packets to confirm if a specified host is reachable and active on the network.
08	`reverse_dns`	Performs an inverse lookup, taking an IP address and finding its associated domain name.
09	`traceroute`	Maps the entire network path from your client to a target host to check for latency or packet drops.
10	`whois_lookup`	Provides detailed registration records about a domain, including ownership and contact details.

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

U Scan the ports for the domain 'example.com'.

Running Nmap scan... I've identified several open ports on example.com: Port 80 (http) and Port 443 (https) are active. Would you like to see the HTTP headers for this domain?

U Find the physical location of the IP address 8.8.8.8.

Performing GeoIP lookup... The IP 8.8.8.8 is located in the United States, specifically in Mountain View, California. It is registered to Google LLC. Shall I perform a WHOIS lookup for more details?

U Trace the network path to 'google.com'.

Initializing traceroute... I've mapped the path to google.com. It took 8 hops with an average latency of 15ms. No significant packet loss was detected along the route. Would you like to check the DNS records for google.com as well?

Frequently Asked Questions

01 **How do I check open ports using Nmap Online?**

You use the `nmap_scan` tool. Just ask your agent to run an Nmap scan on a specific IP or domain, and it will tell you which services like HTTP or HTTPS are active.

02 **What is the difference between dns_lookup and reverse_dns in Nmap Online?**

`dns_lookup` takes a domain name (like google.com) and finds its IP address. `reverse_dns` does the opposite: it takes an IP address and tries to find out what domain name belongs to it.

03 **Can I find all subdomains with Nmap Online?**

Yes, you use the `list_subdomains` tool. Give it a main domain name, and your agent will search for and provide a list of associated subdomains that might be running.

04 **Does Nmap Online help with general connectivity problems?**

It helps by providing tools like `traceroute` and `ping_host`. These let you diagnose if the connection is failing at your end, or if a specific hop between networks is dropping packets.

05 **What data does whois_lookup provide?**

`whois_lookup` gives deep registration details about a domain. This includes information on who owns the domain and when it was first registered, which can be critical for research.

Go Live in 60 Seconds

Get your connection token from **cloud.vinkius.com**, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

```
https://edge.vinkius.com/[TOKEN]/mcp
```

CLIENT	WHERE TO CONFIGURE
Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add `"nmap-online": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → Add endpoint URL
ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

- Ask ChatGPT
- Ask Claude
- Ask Perplexity
- Ask Gemini
- Ask Grok

READY TO CONNECT

Nmap Online is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

vinkius.com · support@vinkius.com

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by Nmap Online. All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	June 2026
MCP Server	Nmap Online MCP
Server ID	`019d75de-126d-7173-a838-64bc5972f6d4`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/mcp/nmap-online.