

The background is a stylized topographic map with contour lines. Overlaid on the map are various technical diagrams: a grid of squares in the top left, a flowchart with hexagons in the top right, a circular diagram with arrows in the bottom left, and a cluster of hexagons in the bottom right. A large, faint green shield with a white question mark is centered behind the title.

Amass: The Recon Tool Behind Real Bug Bounties

A Field Guide to Ethical Attack Surface Mapping

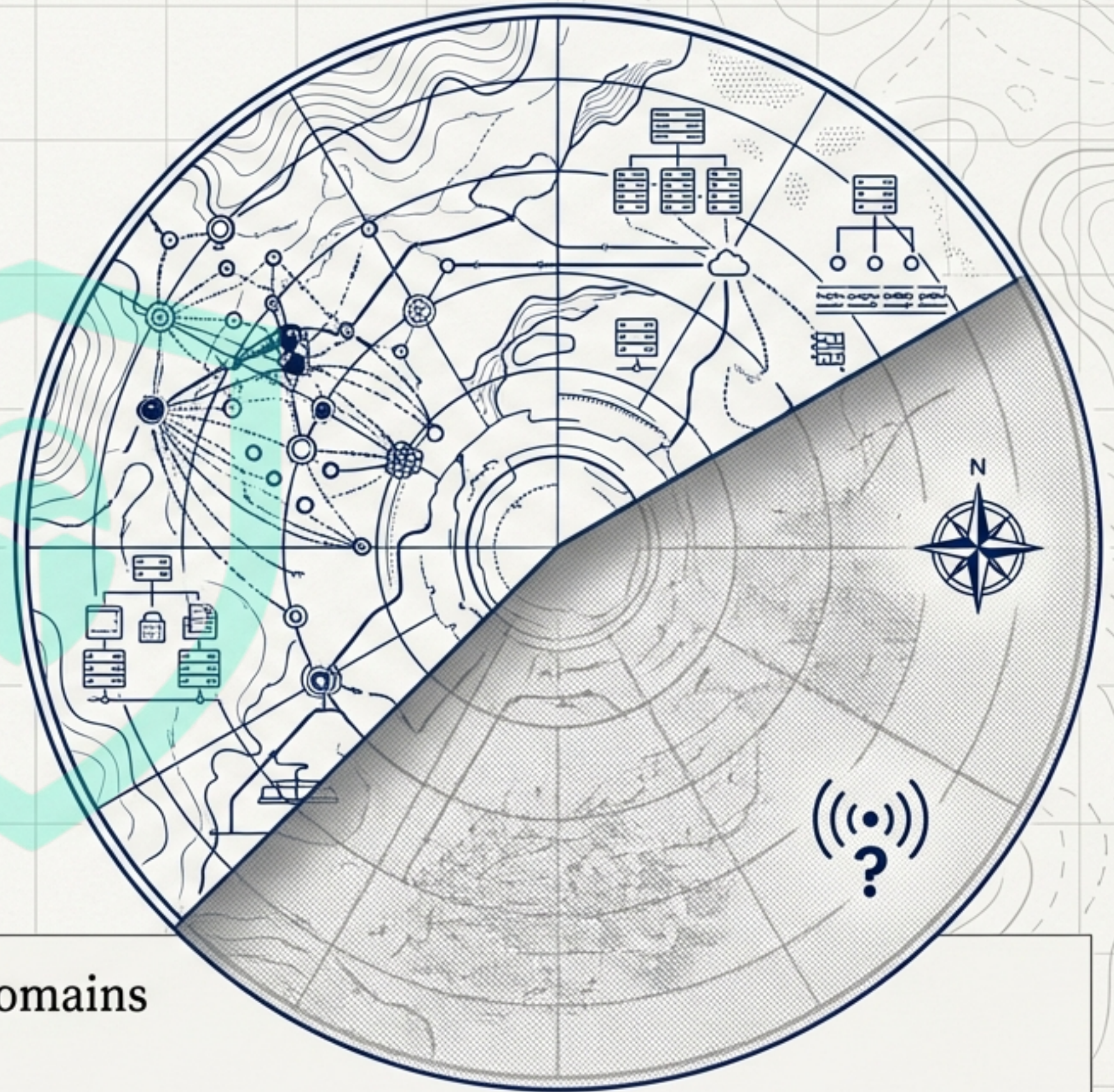
Powered by Bugtrix

Map Smart. Secure Better.

Every Mission Begins with a Map

The modern digital landscape is vast and constantly changing. For defenders, unknown assets create critical blind spots.

Effective security begins with reconnaissance—understanding precisely what assets an organization has so they can be secured. As Red Teams know, you cannot protect what you cannot see.



“Amass works like a satellite map, revealing domains and infrastructure so they can be secured.”

The Digital Cartographer's Instrument: Amass

Amass is an open-source toolset designed for in-depth attack surface mapping and asset discovery.

It provides the ground truth needed for ethical Red Teams and security professionals to help organizations secure their digital footprint.



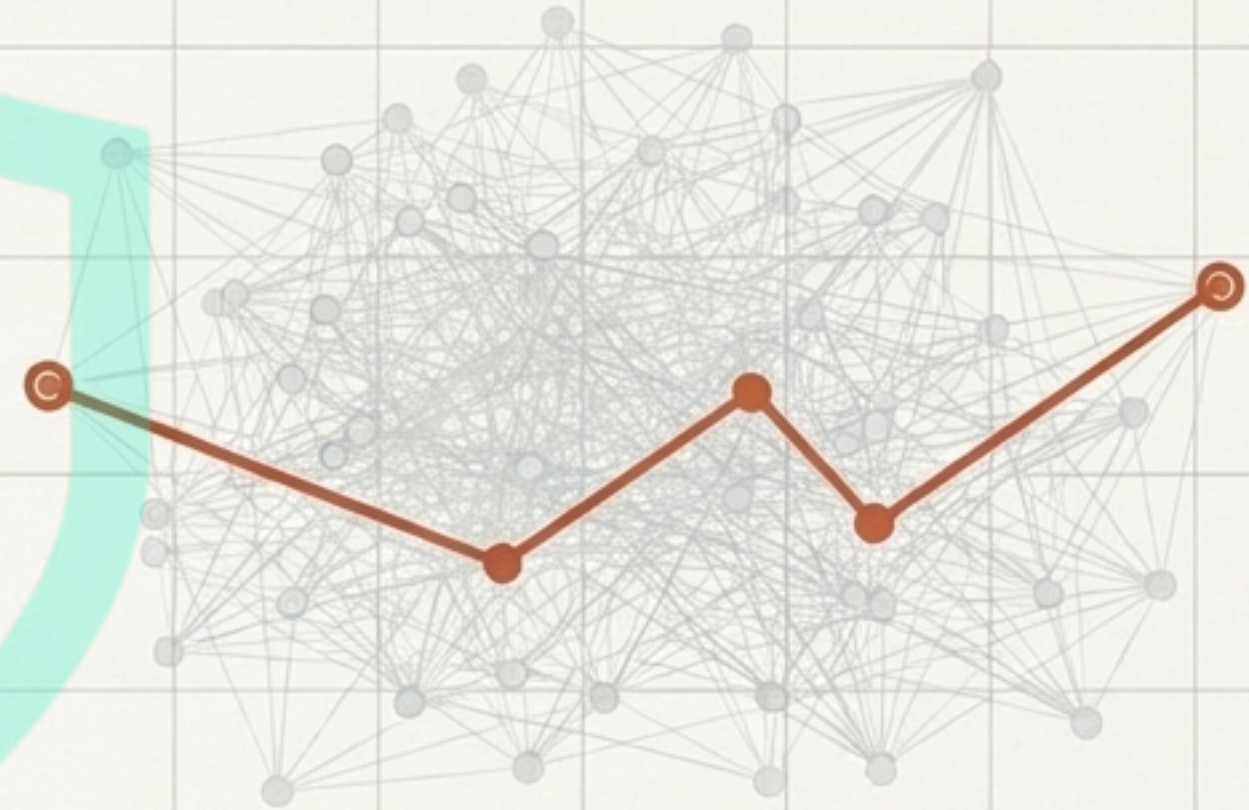
This deck introduces **10 core capabilities** of Amass, treating each as a specialized instrument in your reconnaissance toolkit.

A Tool Is Only as Sharp as Its User

Raw Data



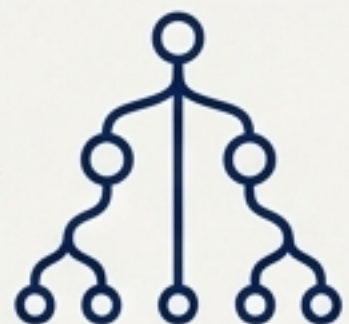
Actionable Insight



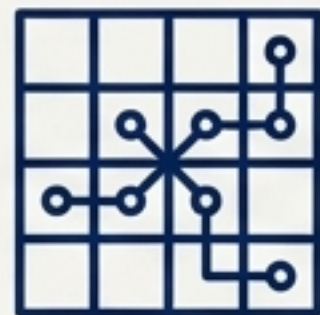
Core Principle: “Amass is incredibly powerful at collecting data, but professional skill determines its relevance. The ultimate goal isn’t data collection; it’s data-driven insight.”

The Bugitrix Method: “Analysis comes before action.”

The Cartographer's Toolkit: 10 Core Capabilities



01 | Subdomain Enumeration



02 | Attack Surface Mapping



03 | Passive Reconnaissance



04 | Active Reconnaissance



05 | DNS Enumeration



06 | Cloud Asset Discovery



07 | Visualization



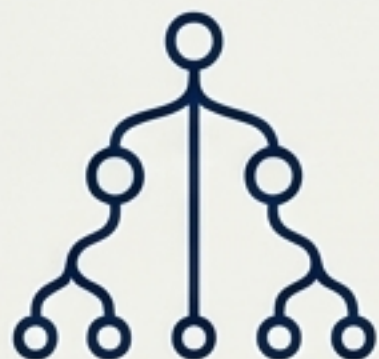
08 | Change Tracking



09 | Scoping Rules



10 | Reporting



Instrument 01 | Subdomain Enumeration

The Mission:

Finds subdomains associated with a target domain.

Strategic Value (Why Defenders Love It):

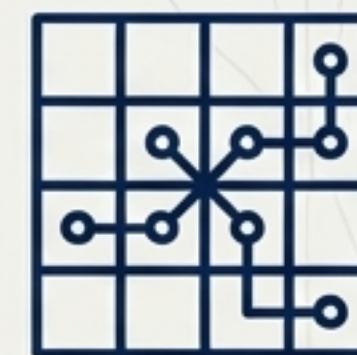
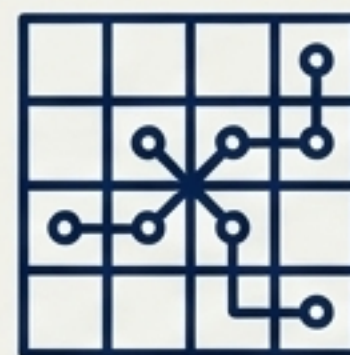
Uncovers **hidden, forgotten, or shadow IT**

Uncovers **hidden, forgotten, or shadow IT assets** that may be vulnerable (e.g., old development servers).

Field Log (Example):

A routine scan reveals `dev-legacy.company.com`, an unpatched server forgotten by the development team.

Skill Focus: DNS Basics.



Instrument 02 | Attack Surface Mapping

The Mission:

Builds a comprehensive inventory of all discovered digital assets.

Strategic Value (Why Defenders Love It):

Creates a **single source of truth**, eliminating blind spots in the security perimeter.

Field Log (Example):

The map reveals an unknown host communicating with a partner network, prompting an immediate policy review.

Skill Focus: Asset Management Principles.

Passive vs. Active Reconnaissance



Instrument 03 | Passive Reconnaissance

The Mission:

Gathers intelligence from publicly available sources without directly engaging the target.

Strategic Value (Why Defenders Love It):

Extremely low-noise and non-intrusive, allowing for safe discovery without alerting potential adversaries.

Field Log (Example):

Public certificates and search engine caches are analyzed to map assets without sending a single packet to the target's network.

Skill Focus: Open-Source Intelligence (OSINT).



Instrument 04 | Active Reconnaissance

The Mission:

Directly interacts with target systems to validate assets and gather precise information.

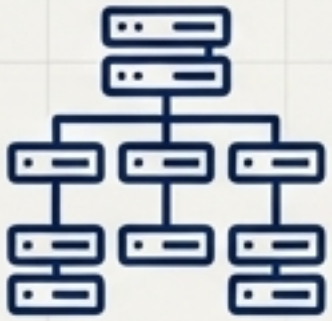
Strategic Value (Why Defenders Love It):

Provides high-fidelity accuracy, confirming which assets are live and filtering out dead hosts or stale data.

Field Log (Example):

An active probe confirms a subdomain from passive recon is no longer in use, preventing wasted time on a dead end.

Skill Focus: Ethical Scanning Techniques.



Instrument 05 | DNS Enumeration

The Mission:

Performs a deep-dive analysis of DNS records (MX, NS, SOA, etc.) to map the target's infrastructure.

Strategic Value (Why Defenders Love It):

Gives critical insight into infrastructure architecture and can reveal **misconfigurations**.

Field Log (Example):

DNS analysis reveals a misconfigured mail server, a potential vector for **spoofing attacks**.

Skill Focus: DNS Fundamentals.



Instrument 06 | Cloud Asset Discovery

The Mission:

Identifies assets hosted within major cloud provider environments (AWS, Azure, GCP).

Strategic Value (Why Defenders Love It):

Prevents **data leaks** from misconfigured or forgotten cloud storage and services.

Field Log (Example):

Amass discovers a publicly accessible **S3 bucket** that was created for a temporary project but never decommissioned.

Skill Focus: Cloud Security Basics.



Instrument 07 | Visualization

The Mission:

Generates interactive graphs and charts of the discovered assets and their relationships.

Strategic Value (Why Defenders Love It):

Provides **instant clarity**, transforming raw text data into an intuitive **visual map** of the attack surface.

Field Log (Example):

A network graph visually highlights a critical server with unexpected connections to less-secure legacy systems.

Skill Focus: Data Interpretation.



Instrument 08 | Change Tracking

The Mission:

Continuously monitors the attack surface and alerts on any changes from a known baseline.

Strategic Value (Why Defenders Love It):

Acts as an **early warning system** for new, potentially unauthorized assets appearing on the network.

Field Log (Example):

Amass detects a new subdomain (**promo-campaign.company.com**) and flags it for immediate security review.

Skill Focus: Security Baselines.



Instrument 09 | Scoping Rules

The Mission:

Limits the reconnaissance operation to a specific, pre-approved set of targets and domains.

Strategic Value (Why Defenders Love It):

Ensures the engagement stays within legal and contractual boundaries, preventing accidental overreach.

Field Log (Example):

A bug bounty program's scope is loaded into Amass to ensure only approved company assets are scanned.

Skill Focus: Rules of Engagement & Ethics.



Instrument 10 | Reporting

The Mission:

Documents all findings in a structured format for analysis and remediation.

Strategic Value (Why Defenders Love It):

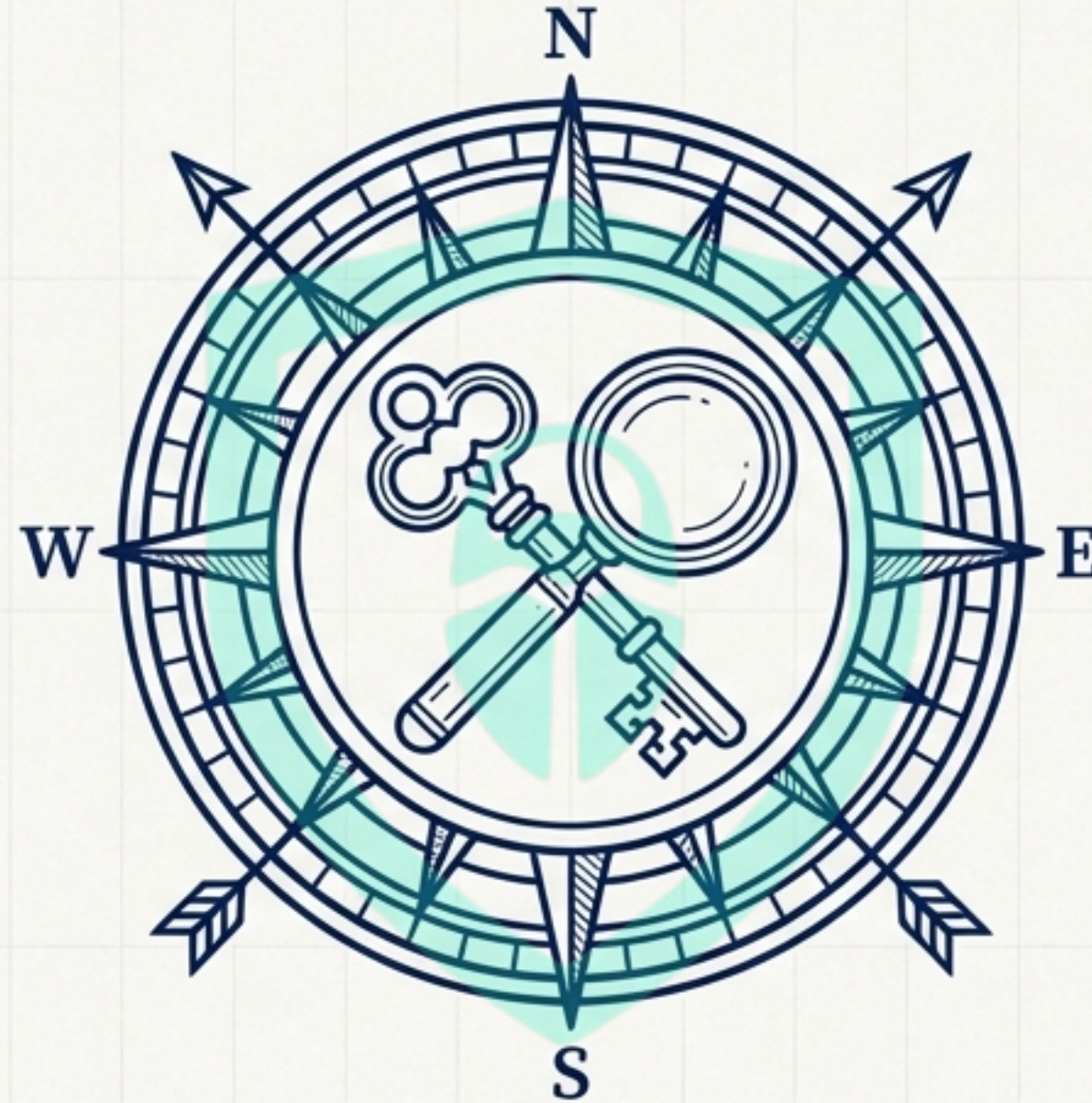
Translates raw discovery data into actionable intelligence that teams can use to prioritize and implement fixes.

Field Log (Example):

A clear report of unmanaged assets is sent to the IT and security teams, enabling them to begin the remediation process.

Skill Focus: Technical Reporting Skills.

The Cartographer's Code



Power demands responsibility. A professional cartographer operates under a strict code of conduct. The most important skills are not technical; they are judgment, ethics, and a commitment to causing no harm. The following are the non-negotiable rules of any reconnaissance mission.

Mission Parameters: Safe Configuration

- ✓ **Respect Boundaries:** Use Amass only on domains you are explicitly authorized to test. Never target systems without permission.
- ✓ **Prioritize Passive Methods:** For initial discovery on sensitive or unknown targets, always prefer passive reconnaissance to minimize your operational footprint.
- ✓ **Adhere to the Scope:** Use Amass's scoping features to strictly enforce the rules of engagement for your project.
- ✓ **Obey the Law:** Understand and comply with all local and international laws regarding computer intrusion and network scanning.

The Ethical & Legal Compact



Unauthorized reconnaissance is illegal and can carry severe consequences.

Amass is a professional tool. Use it exclusively for educational purposes in your own lab environments or on authorized bug bounty and penetration testing programs.

“Bugitrix promotes ethical security.”

Map Smart. Secure Better.



bugitrix.com