Name : Nikita Shukla
Intern ID : 134

Proof of Concept Report:

Search Engines Name: Ahmia & Aleph OpenSearch

Description of the Tool

Ahmia and Aleph OpenSearch are specialized search engines designed to index and provide access to content on the Dark Web. These tools operate primarily through the Tor network, a privacy-focused system that allows anonymous browsing and hosting of websites (".onion" domains). While traditional search engines like Google or Bing cannot access .onion sites due to their non-standard domain structure and network protocols, tools like Ahmia and Aleph fill this gap by indexing Dark Web content in a secure and ethical manner.

- **Ahmia** is an open-source search engine focused on indexing Tor hidden services while filtering out abusive or illegal content. It provides a user-friendly interface accessible via clearnet (https://ahmia.fi) and .onion link.
- **Aleph OpenSearch** is a tool developed by OCCRP (Organized Crime and Corruption Reporting Project) for indexing leaked databases, public records, and dark web content to support investigative journalism.

Why It's Useful

These search engines serve critical purposes in cybersecurity, research, journalism, and digital forensics:

- **Privacy and Anonymity**: Allow anonymous searching of Dark Web content without compromising user privacy.
- **Law Enforcement and Cybersecurity**: Enable tracking of leaked data, illicit marketplaces, and illegal activities.
- **Research and Intelligence Gathering**: Used by journalists, researchers, and analysts to uncover hidden networks, compromised credentials, and structured crime data.
- **Ethical Indexing**: Unlike conventional scraping, Ahmia applies filters to exclude illegal material and promotes transparency.
- **Data Aggregation**: Aleph connects multiple structured datasets into a single searchable interface, helping in investigations.

How It’s Used

Stage 1: Accessing the Tool

- For Ahmia, visit: https://ahmia.fi
- For Aleph OpenSearch, visit: https://aleph.occrp.org
  Both tools can also be accessed through the Tor browser for enhanced anonymity.

Stage 2: Searching

- Enter keywords, leaked emails, organization names, or file types.
- Ahmia fetches indexed .onion results, and Aleph pulls from structured databases and documents.

Stage 3: Analyzing Results

- Users examine summaries or full content of indexed data.
- Metadata and source information are often provided, aiding in validation.

When to Use It

- **Investigating Data Leaks**: Journalists or security professionals tracing breached databases.
- **Threat Intelligence**: Cybersecurity teams identifying exposed credentials or infrastructure threats.
- **Digital Forensics**: Gathering evidence from hidden services for criminal cases.
- **Educational Purposes**: Demonstrations in cybercrime awareness training.
- **Compliance Checks**: Verifying exposure of company data or identities.

Who Should Use It

- **Cybersecurity Analysts**
- **Digital Forensic Investigators**
- **Journalists & Researchers**
- **Intelligence Officers**
- **Academic Institutions** teaching cybersecurity, OSINT, and digital ethics.

Advantages

- Free and Open Source

- Enables anonymous search on Dark Web
- Supports both clearnet and Tor access
- Filters illegal content (Ahmia)
- Structured query and dataset linking (Aleph)
- Useful for threat detection and investigative reporting
- Supports export and collaboration (Aleph)

Flaws or Limitations

- Limited Coverage: Not all onion services are indexed.
- Latency: Search can be slower due to Tor network dependency.
- Legal Sensitivity: Users must ensure compliance with laws when accessing or analyzing content.
- Aleph requires some technical skill to filter/search effectively.
- Some results may become outdated due to site volatility on the Dark Web.
- May be blocked or restricted in some jurisdictions.