OSINT Investigation Report – example.com

# Project Overview

This OSINT (Open Source Intelligence) investigation simulates reconnaissance on a public domain using passive information-gathering techniques only. The goal is to identify publicly available data such as emails, subdomains, and DNS records — without any direct interaction with the target.

# Target Details

* Domain: example.com
* Scan Type: Passive OSINT scan
* Tools Used: theHarvester, SpiderFoot

# Tools Used

* theHarvester: Used to collect publicly available emails and subdomains via the Bing search engine.
* SpiderFoot: Performed a comprehensive passive scan to extract WHOIS data, DNS information, SSL certificate metadata, and other publicly exposed intelligence.

# Emails Found

* coolguy123@example.com
* name@example.com
* test@example.com
* irock@example.com
* partyqueen@example.com
* user@example.com

# Subdomains Discovered

* www.example.com
* static.example.com
* sub1.example.com
* sub2.example.com

# Notable Findings from SpiderFoot Scan

* WHOIS: Domain owned by IANA (Internet Assigned Numbers Authority)
* Name Servers: A.IANA-SERVERS.NET, B.IANA-SERVERS.NET
* Certificates: SSL certificate metadata retrieved
* Other: Numerous passive DNS and metadata artifacts uncovered

# Exported Results

* CSV
* JSON
* Excel
* GEXF (for graph-based visualization with tools like Gephi)

# Observations and Applications

* Even a placeholder domain like example.com reveals interesting surface-level information through passive OSINT. In real-world scenarios, such findings could:
* - Support phishing or spoofing risk assessments
* - Inform network/infrastructure mapping
* - Feed into broader red team reconnaissance workflows

# Ethical Disclaimer

This investigation was conducted on a non-malicious, publicly accessible test domain (example.com) strictly for educational and ethical cybersecurity research purposes.