

**Reconnaissance Report**

***Reconnaissance Report: TechTribe Co Investment Management System***

***Purpose***

*This reconnaissance report aims to provide a comprehensive overview of the TechTribe Co Investment Management System infrastructure, identify potential vulnerabilities, and gather intelligence that malicious actors could exploit. This information can inform further security assessments, penetration testing, and risk mitigation strategies.*

***Scope***

*This reconnaissance effort focused on the following areas:*

* ***Public-facing infrastructure:*** *TechTribe Co’s website, DNS records, and other publicly accessible assets associated with the investment management system.*
* ***Network services:*** *Identify open ports and services running on the system.*
* ***Publicly available information:*** *Gather data from various sources, including social media, public records, and online forums related to TechTribe Co and the investment management system.*

***Reconnaissance Overview: TechTribe Co Investment Management System***

*This reconnaissance report details the findings of an investigation into the TechTribe Co Investment Management System. This effort aimed to gather information about the system’s infrastructure, identify potential vulnerabilities, and provide intelligence for further security assessments.*

*The reconnaissance used passive and active techniques to comprehensively picture the system’s digital footprint. The following sections will outline the specific methods used and the results obtained.*

*Passive reconnaissance techniques:*

* *WHOIS Lookup: To uncover details about the domain registration, including the registrar, contact information, and creation date.*
* *DNS Queries: To identify IP addresses, mail servers (MX records), and nameservers (NS records) associated with the domain. Additionally, any subdomains linked to TechTribe Co will be noted.*
* *Web Searching and Metadata Analysis: Leveraging search engines and tools like metagoofil to locate publicly available documents and extract potentially valuable metadata like usernames, software versions, or document creation dates.*

*Active reconnaissance techniques:*

* *Network Scanning: Using Nmap to scan for open ports and identify the services running on those ports, including their versions. This allows for assessing potential vulnerabilities based on outdated software or misconfigurations.*
* *Banner Grabbing: Examining the service banners displayed by open ports to gain further insights into the target’s infrastructure, such as the operating system used or specific service details.*
* *OSINT (Open-Source Intelligence): Employ tools like the Harvester to gather publicly available information on TechTribe Co and the investment management system, including emails, subdomains, and relevant data from online sources such as social media platforms.*

***The following sections will delve deeper into the findings obtained from each reconnaissance stage and provide recommendations based on the gathered information.***

***Part 1: Passive Reconnaissance***

* ***WHOIS Lookup***

***A computer screen shot of a computer

Description automatically generated***

* ***DNS Queries with nslookup and dig***

***A computer screen shot of a computer code

Description automatically generated***

***A computer screen shot of a program

Description automatically generated***

* ***Web Searching and Metadata Analysis***

***A screenshot of a computer program

Description automatically generated***

***Part 2: Active Reconnaissance***

* ***Network Scanning with Nmap***

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

* ***Banner Grabbing***

***A computer screen shot of a computer error

Description automatically generated***

* ***Exploring OSINT***

***A screenshot of a computer

Description automatically generated***