Passive Reconnaissance Report: infosys.com

Date of Assessment: September 2, 2025
Author: Ishaan Malhotra
Classification: Confidential

1. Executive Summary

This report outlines the findings of a passive reconnaissance assessment conducted on the domain `infosys.com`. The objective was to gather publicly available information to understand the organization's external attack surface without directly interacting with its systems.

The investigation successfully identified a significant amount of information, including hundreds of subdomains, multiple IP addresses and network blocks, employee email addresses, and server port/service information. Furthermore, Google dorking techniques revealed potentially sensitive documents and exposed login panels.

The findings, supported by the evidence in the appendix, indicate a large and complex digital footprint that could present multiple avenues for a potential attacker. Key areas of concern include exposed services like the Remote Desktop Protocol (RDP) and the public availability of documents marked as "confidential."

2. Scope & Methodology

- **Target Domain:** `infosys.com`
- **Methodology:** The assessment was strictly passive, utilizing Open Source Intelligence (OSINT) techniques. Data was gathered from public search engines, DNS records, and specialized security search engines.
- **Tools Used:**
    - theHarvester
    - Recon-ng (with `hackertarget` module)
    - Shodan
    - Amass
    - Google Dorking

3. Findings

The following sections detail the information discovered during the assessment. For direct tool outputs and screenshots, please refer to **Appendix A: Evidence**.

3.1. Email Addresses

The `theHarvester` tool identified several email addresses associated with the `infosys.com` domain.

- **Emails Found:**
  - 0_10_@infosys.com
  - anny_liu@infosys.com
  - arunacnewton@infosys.com
  - china_freshers@infosys.com
  - connect-china@infosys.com
  - infy-rec_helpdesk@infosys.com
  - infy.zhaopin@infosys.com
  - instep_team@infosys.com

Impact: These addresses could be used in targeted phishing campaigns or social engineering attacks against Infosys employees.

3.2. Domain & Subdomain Enumeration

A vast number of subdomains were discovered, indicating a wide digital presence.

- **Hosts Found:** `theHarvester` reported finding **845 hosts**.
- **Key Subdomains Identified (from Amass, Recon-ng, theHarvester):**
  - admin.infosys.com
  - blogs.infosys.com
  - forms.infosys.com
  - jamfadcs.infosys.com
  - oic.infosys.com
  - rec-test.infosys.com
  - usasbc01-ext.infosys.com
  - usasbc02-ext.infosys.com

Impact: Each subdomain represents a potential entry point. Subdomains like `rec-test` may have weaker security configurations than production environments, posing a significant risk.

3.3. IP Addresses & Network Infrastructure

Multiple IP addresses, netblocks, and Autonomous System Numbers (ASNs) were identified.

- **Identified IPs:**
  - infosys.com -> 35.71.178.178
  - usasbc01-ext.infosys.com -> 122.98.130.127
  - usasbc02-ext.infosys.com -> 122.98.118.127
  - jamfadcs.infosys.com -> 122.98.14.176
- **Identified ASNs:**
  - 38191 (Infosys Technologies Ltd)
  - 16509 (Amazon.com, Inc.)
  - 55410 (Vodafone Idea Ltd, IN)

Impact: This information maps out the company's network infrastructure and reveals its hosting partners (e.g., Amazon AWS).

3.4. Open Ports & Services (Shodan)

Shodan identified 13 internet-facing devices, primarily located in the United States and India.

- **Common Open Ports:** 443 (HTTPS), 25 (SMTP), 465 (SMTPS).

- **High-Risk Open Ports: 3389 (Remote Desktop Protocol - RDP)** was identified on at least two devices.
- **Identified Technologies:** NGINX web servers, MailEnable SMTP servers.

Impact: Exposed RDP ports are a primary target for brute-force and ransomware attacks. If not properly secured with strong passwords, MFA, and access controls, they present a critical vulnerability.

3.5. Sensitive Information Exposure (Google Dorking)

Advanced Google searches revealed potentially sensitive data.

- **Confidential Documents:** A search for `site:infosys.com filetype:pdf "confidential"` returned several documents, including `enterprise-data-protection.pdf` and others related to cloud security and data analytics that contain the word "confidential".
- **Exposed Login Pages:** A search for `site:infosys.com inurl:login` identified a generic login portal and a related user manual.

Impact: The public availability of documents labeled "confidential" suggests a potential breakdown in data classification and handling procedures. Exposed login pages provide clear targets for credential stuffing and brute-force attacks.

4. Recommendations

Based on these passive findings, the following actions are recommended:

1. **Reduce Attack Surface:** Conduct an internal audit of all discovered subdomains. Decommission any that are no longer required, especially non-production environments like `rec-test`.
2. **Secure Exposed Services:** Immediately review the security of all devices with port 3389 (RDP) open. Enforce strong, unique passwords, enable Multi-Factor Authentication (MFA), and restrict access to trusted IP addresses only.
3. **Data Leakage Prevention:** Review all publicly accessible files on the `infosys.com` domain to ensure that no internal or sensitive information is inadvertently exposed. Implement a web application firewall (WAF) rule to block crawling of sensitive directories.
4. **Employee Training:** Enhance security awareness training for employees, focusing on the risks of phishing, using the discovered email address formats as examples.

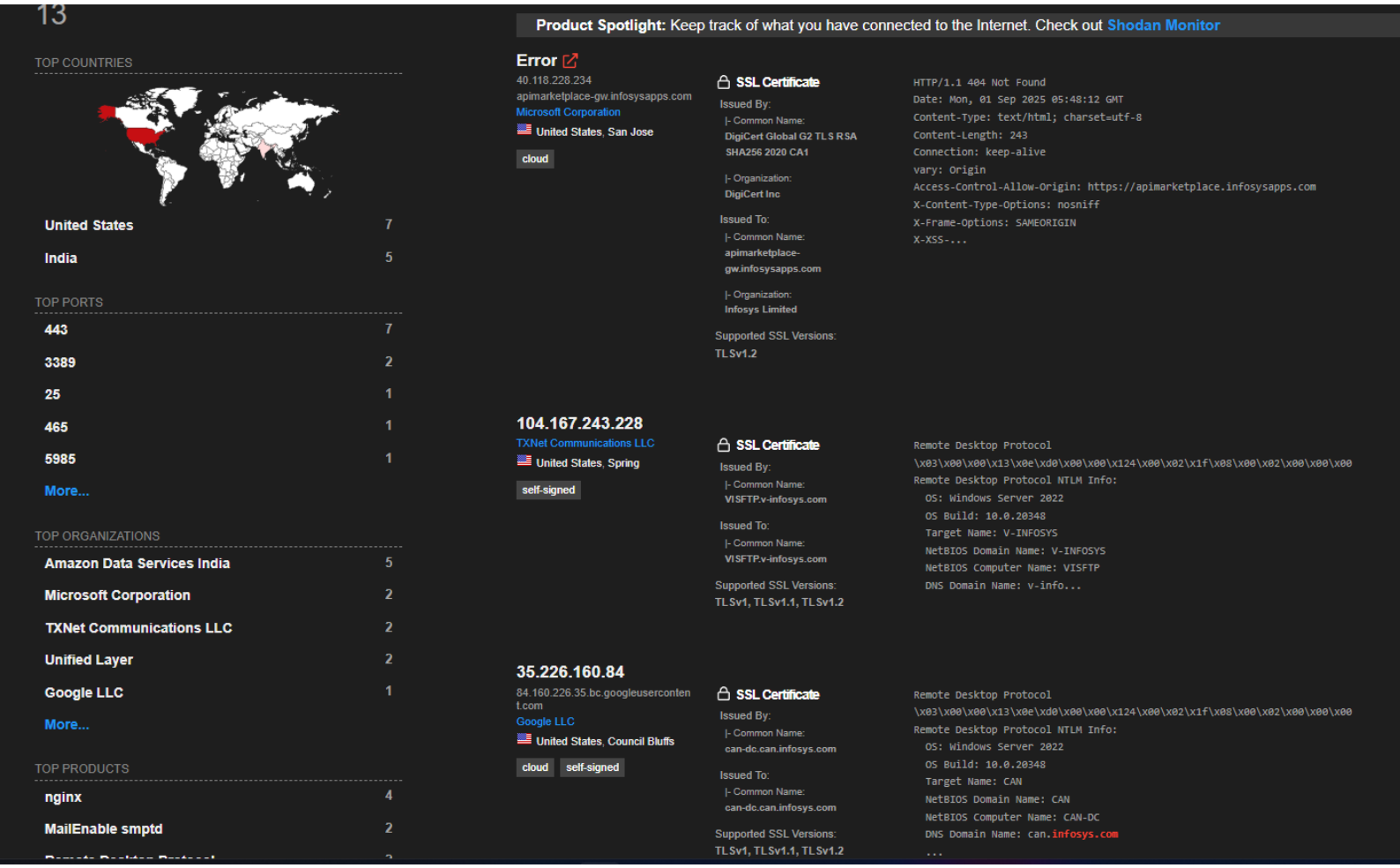
5. Conclusion

The passive reconnaissance of `infosys.com` reveals a significant and varied external attack surface. The volume of subdomains, combined with exposed high-risk services and potentially sensitive documents, provides a fertile ground for a malicious actor to begin a more targeted attack. It is strongly recommended that the organization proceeds with a comprehensive vulnerability assessment and penetration test to actively identify and remediate the security weaknesses suggested by this report.

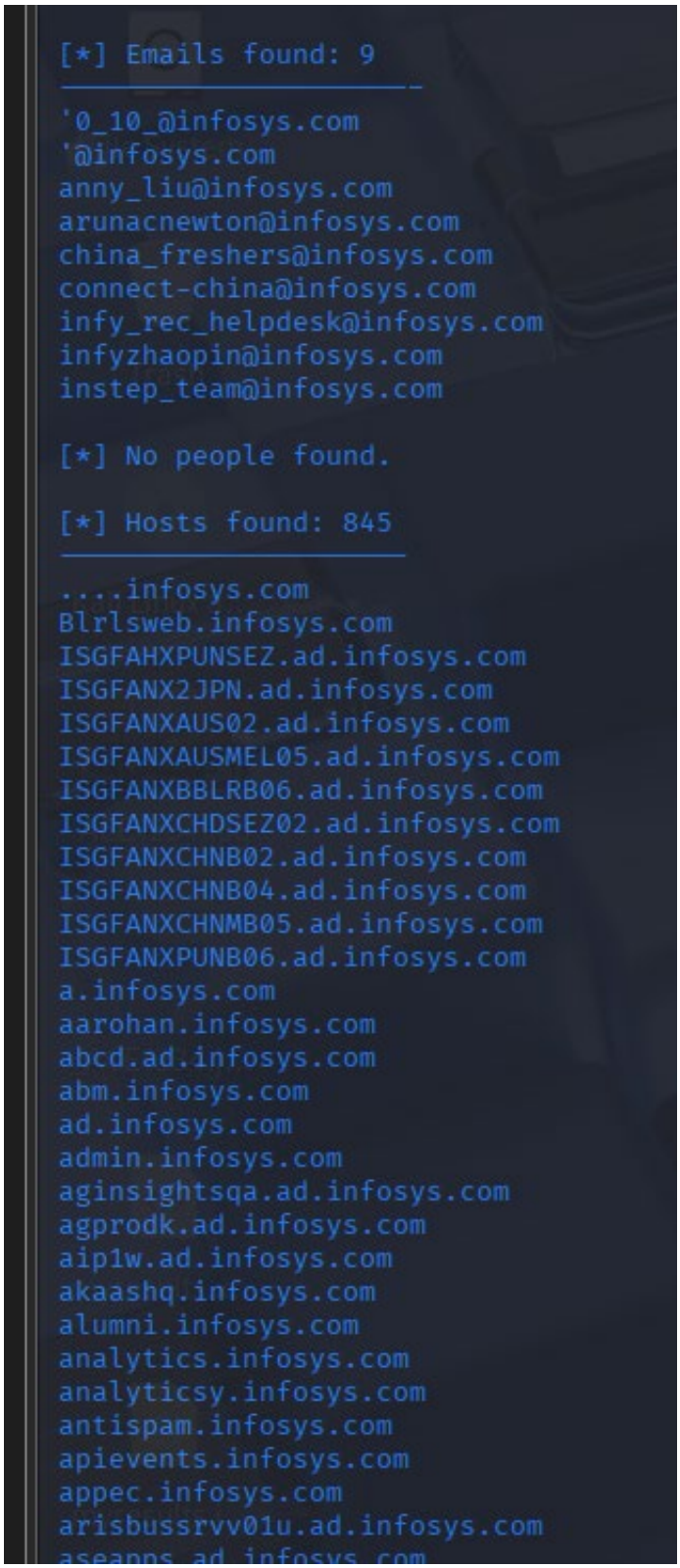
Appendix A: Evidence

This appendix contains references to the screenshots captured during the assessment, which serve as evidence for the findings in Section 3.

- **EVD-01: Shodan Scan Results**
  - **Description:** Shodan dashboard showing 13 total results for `infosys.com`, with details on top countries (United States, India), open ports (443, 3389), and organizations.

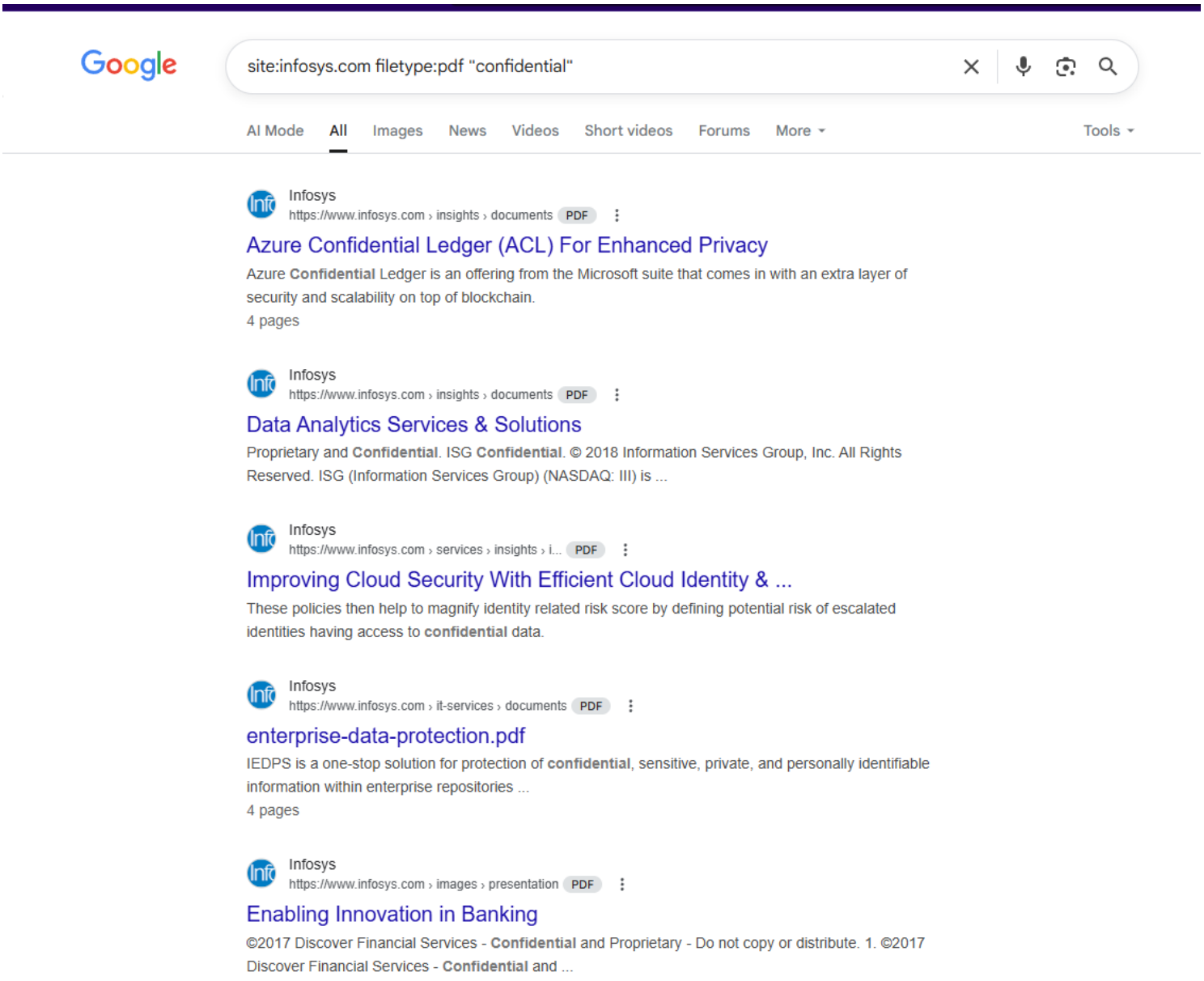


- **EVD-02: theHarvester Scan Results**
  - **Description:** Console output from theHarvester showing 9 emails found and a partial list of 845 subdomains discovered.

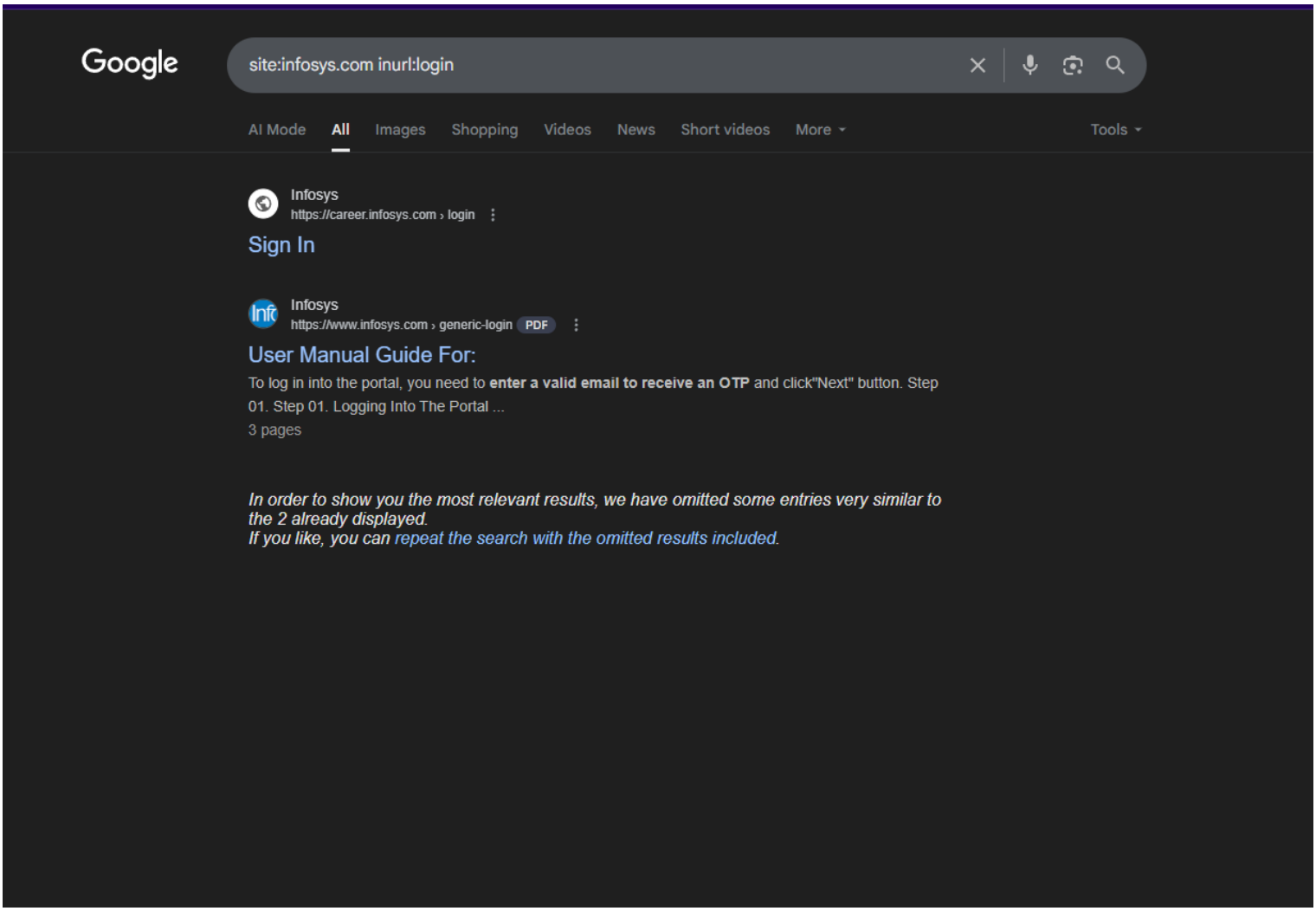


- **EVD-03: Recon-ng Scan Results**
  - **Description:** Console output from Recon-ng's `hackertarget` module, listing resolved hosts and their corresponding IP addresses (e.g., `jamfadcs.infosys.com`).

- **EVD-04: Google Dorking for Confidential Documents**
  - **Description:** Google search results for `site:infosys.com filetype:pdf "confidential"`, showing multiple PDF documents indexed by the search engine.



- **EVD-05: Google Dorking for Login Pages**
  - **Description:** Google search results for `site:infosys.com inurl:login`, identifying a "Sign in" portal and a "User Manual Guide" in PDF format.



- **EVD-06: Amass Scan Results**
  - **Description:** Console output from Amass showing detailed passive DNS enumeration, including CNAME records, A records, and associated netblocks/ASNs.

- **EVD-07: theHarvester XML Output**
  - **Description:** The raw XML output file saved from theHarvester, confirming the emails and hosts discovered during the scan.