REPORT
OSINT Email Enumeration & Validation

v1.0.0

Author:

Eldon Gabriel

October 17, 2025

TABLE OF CONTENTS

Disclaimer: This report documents my personal work in completing a lab exercise. It reflects my independent understanding and application of publicly available tools and techniques. No proprietary instructional videos, lab guides, or specific content from the original exercise have been posted, shared, or distributed, ensuring full compliance with academic and professional policies.

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	10/17/2025	Eldon G.	Initial draft.

1.0 EMAIL RECONNAISSANCE AND VALIDATION

1.1 Project Description

An **Open-Source Intelligence (OSINT**) exercise was performed to find and check potential email addresses linked to a target domain and person using public data sources.

1.2 Scope

The work focused on:

1. Locating email addresses within publicly accessible **PDF files** using targeted search queries.
2. Generate educated email guesses based on the identified **naming conventions**.
3. Testing mailbox validity using online email **verification tools**.

1.3 Tools and Environment

- **Kali Linux** virtual machine, running within a **Virtual Private Network** (**VPN**)
- `Google Search` (using advanced operators/dorks)
- Email verification tools: **Hunter.io**, **CentralOps.net**
- Local text editor for documentation

2.0 EXECUTION

2.1 Reconnaissance

I used **Google dorks** to locate exposed PDF documents containing contact information. This involved leveraging the `filetype:pdf` operator in conjunction with organization-specific keywords. Example of a successful query pattern:

```
"example company name" filetype:pdf "contact" OR "email"
```

The PDFs provided both a reference **organization email** and a **personal email**, which served as baselines for the pattern analysis.

2.2 Pattern Analysis

From the organization email (e.g., *jsmith@example.org*), I identified the corporate **naming convention**: `[first initial][lastname]`. This format was verified against other staff members within the same document to ensure accuracy.

2.3 Email Guess Generation

Organization Guesses: Using the established `[firstinitial][lastname]` pattern, I generated organizational email guesses for two other employees mentioned in the file:

- *ajones@example.org*
- *rbrown@example.org*

Personal Guesses: For the email *john.doe1@gmail.com*, I created expanded guesses across three other providers. I maintained the username *john.doe1*:

- *john.doe1@yahoo.com*
- *john.doe1@protonmail.com*
- *john.doe1@cloud.com*

2.4 Verification

Each guessed address was tested using online verification tools. This process checks for the existence of the mailbox by querying the domain's **MX records** and/or attempting an **SMTP connection** (depending on the tool).

Key Observation: Results varied from a definitive **“valid”** to **“unknown”** or **“risky,”** highlighting the importance of using multiple tools and acknowledging the limitations of free-tier services. At least one of the guessed email addresses returned a definitive 'valid' response, which was cross-validated by one of the verification tools.

3.0 FINDINGS

3.1 Summary Findings

- The naming convention of the target organization was confirmed to be **predictable and uniform**, allowing for successful enumeration.
- At least one of the guessed email addresses returned a definitive **“valid”** response across all verification tools.
- Verification tools exhibit varying levels of accuracy and are subject to rate limitations under their free-service tiers, which can impact the certainty of the final results.

4.0 CONCLUSION

4.1 Key Takeaways

- **Publicly exposed PDFs** and other documents are primary sources for quickly identifying internal organizational naming conventions.
- Email enumeration remains a **practical and low-cost** initial step in OSINT investigations.
- Verification accuracy depends heavily on the **tool's methodology** (e.g., simple MX check vs. full SMTP validation).

4.2 Security Implications & Recommendations

Audit and Redaction: Organizations should implement strict policies to audit and redact sensitive employee contact information from all publicly accessible documents, including PDFs.

Use Aliases: Replace direct staff emails with **generic contact aliases** (e.g., *info@, support@*) in public materials to prevent automated data harvesting from these sources.

Ethical Boundary: Investigators must strictly adhere to the legal and moral limits of OSINT; verified addresses must **never** be used for contact, intrusion, or social engineering attempts.
