OSINT and Social Engineering Awareness – Ghana Health Service

Group: Group 5

Institution: Thrive Africa

Author: CyberSecurity

Date: August 2025

---

1. Introduction

This report details an OSINT (Open Source Intelligence) investigation conducted on the Ghana Health Service to identify publicly available information that may pose a risk in social engineering attacks. The purpose is to raise awareness and strengthen cybersecurity posture.

2. Methodology

The following tools and techniques were used:

- **whois:** To extract domain registration data
- **theHarvester:** To gather emails, hosts, and subdomains
- **Google Dorking:** Manual search for public files, admin panels
- **Social Media Intelligence:** Review of LinkedIn, Twitter, Facebook

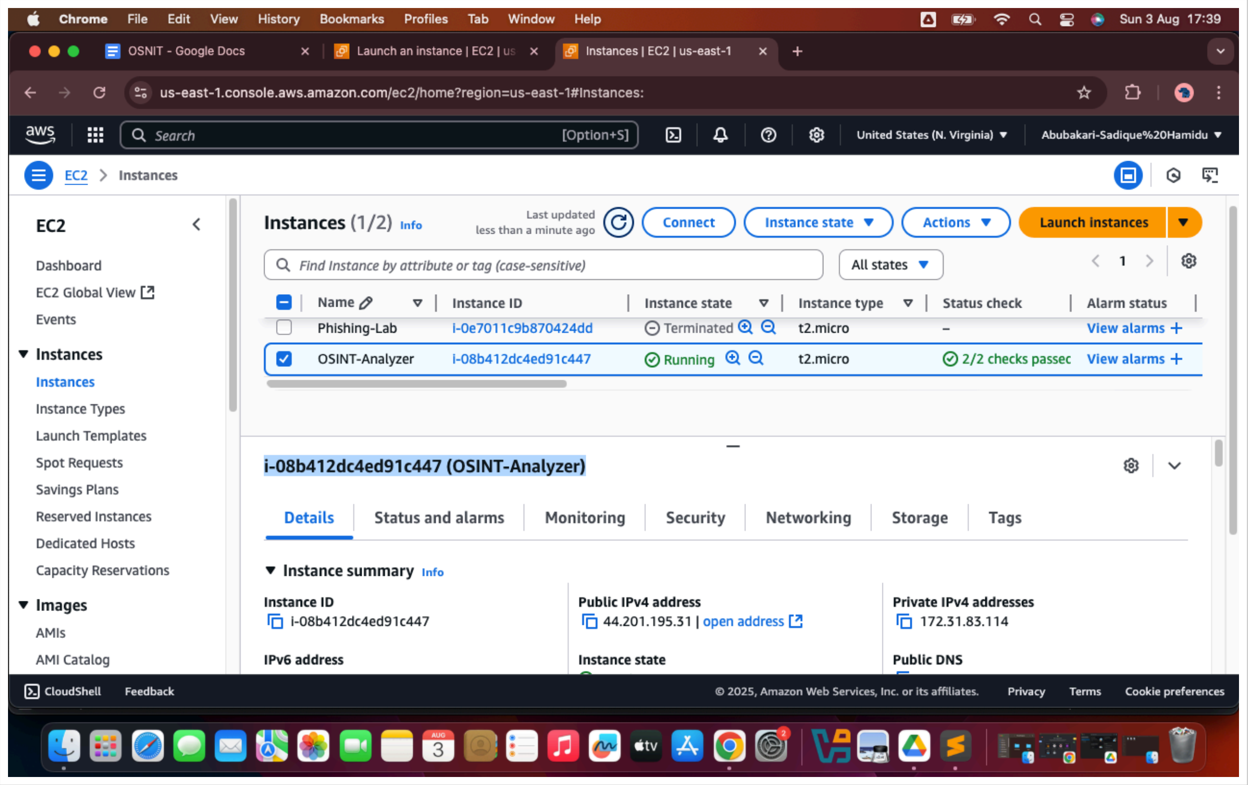
All steps were executed on a secured EC2 Ubuntu instance on AWS Cloud.

3. Findings

3.1 EC2 Setup

We created and accessed a cloud-based Ubuntu EC2 instance to run the OSINT tools securely.

📸 EC2 Instance Summary



	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☐	Phishing-Lab	i-0e7011c9b870424dd	Terminated	t2.micro	–	View alarms +
☑	OSINT-Analyzer	i-08b412dc4ed91c447	Running	t2.micro	2/2 checks passec	View alarms +

i-08b412dc4ed91c447 (OSINT-Analyzer)

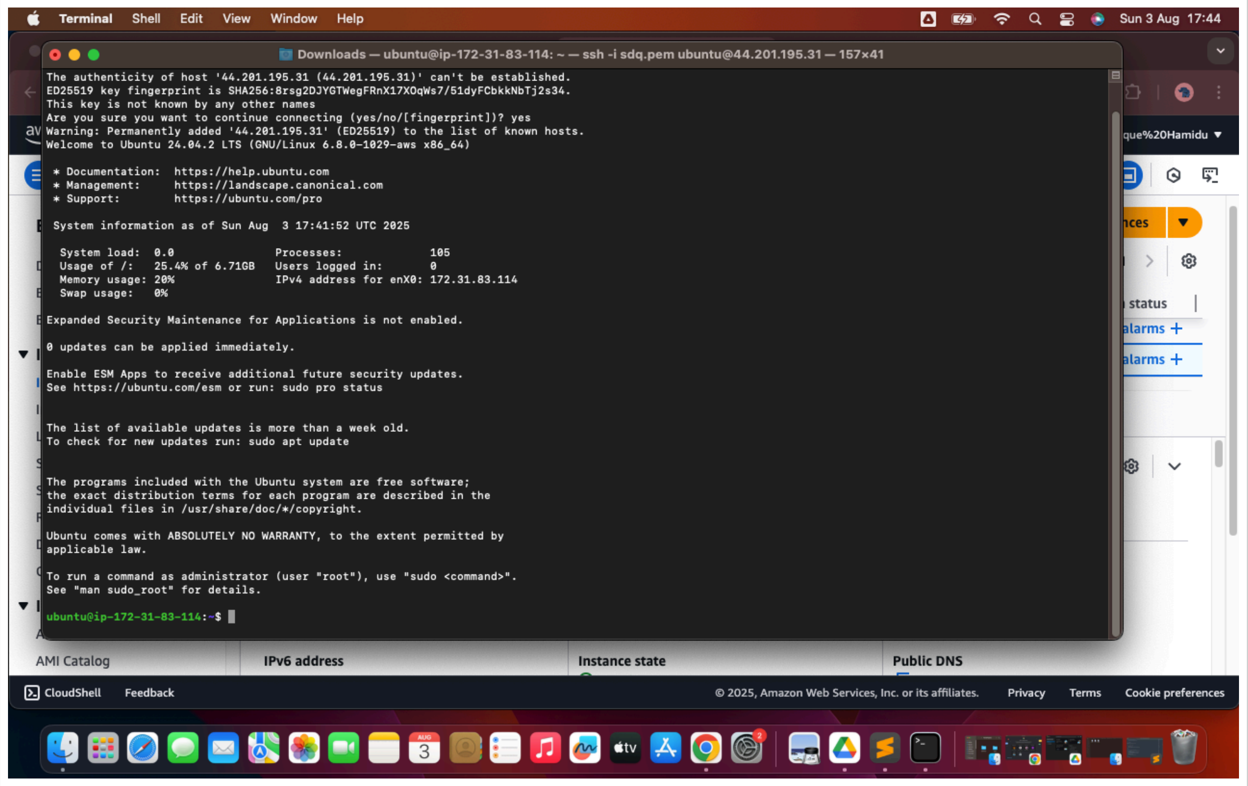
Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-08b412dc4ed91c447	44.201.195.31 | open address	172.31.83.114
IPv6 address	**Instance state**	**Public DNS**

3.2 SSH Login

SSH was used to connect to the EC2 instance using a secured key pair.

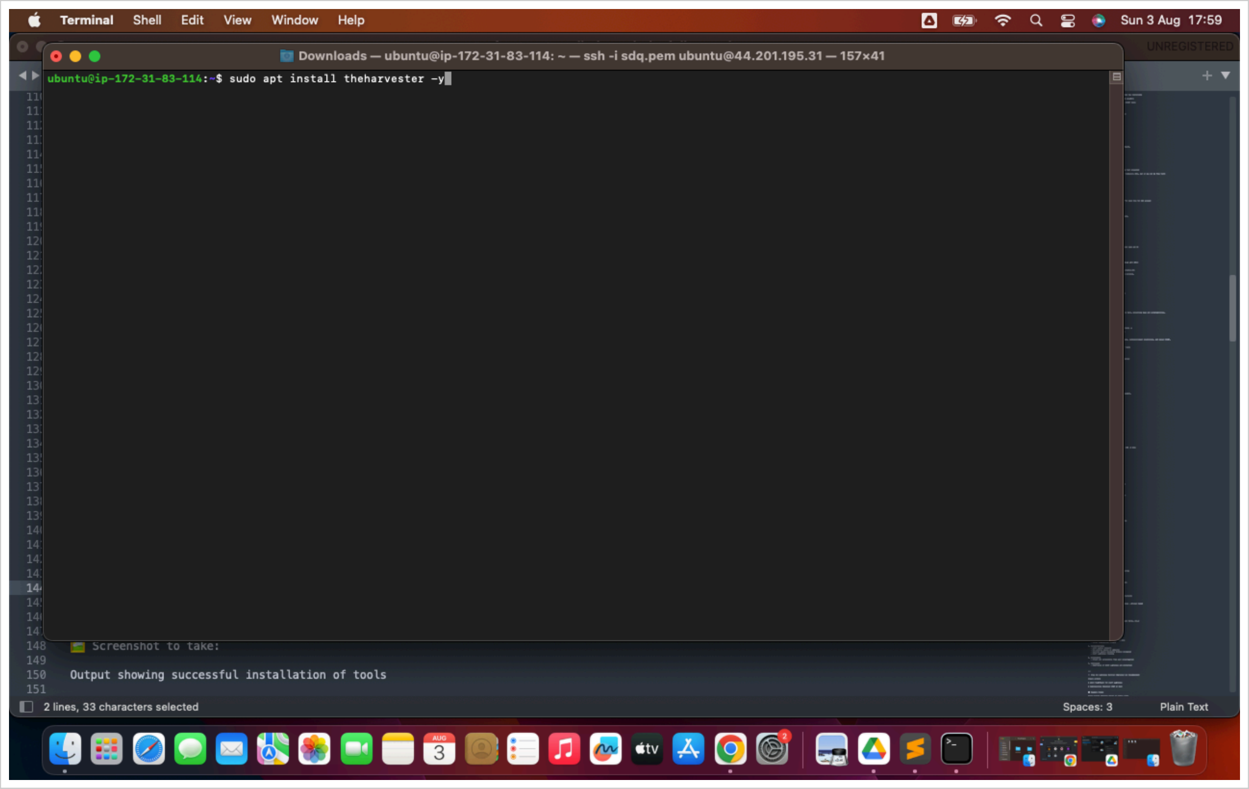
📸 SSH Login Terminal


Terminal Shell Edit View Window Help
Sun 3 Aug 17:44
Downloads — ubuntu@ip-172-31-83-114: ~ — ssh -i sdq.pem ubuntu@44.201.195.31 — 157×41
AMI Catalog
IPv6 address
Instance state
Public DNS
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

```
The authenticity of host '44.201.195.31 (44.201.195.31)' can't be established.
ED25519 key fingerprint is SHA256:8rsg2DJYGTWegFRnX17XOqWs7/51dyFCbkkNbTj2s34.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '44.201.195.31' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Aug  3 17:41:52 UTC 2025

  System load:  0.0               Processes:             105
  Usage of /:   25.4% of 6.71GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for enX0: 172.31.83.114
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-83-114:~$ 
```

3.3 Tool Installation

We updated the system and installed OSINT tools including whois, dnsutils, theHarvester, and Python packages.

> 📸 Installed OSINT Tools
>
> 
>
>

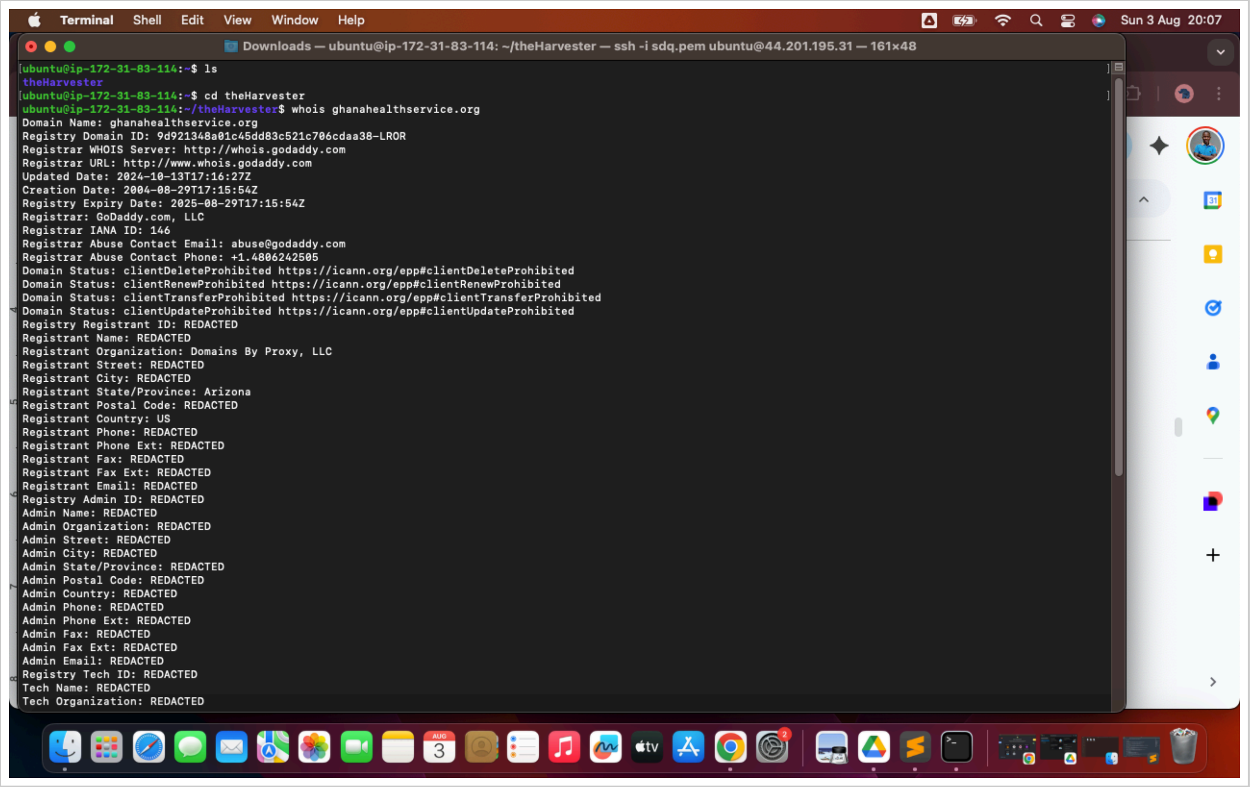
Terminal
> Shell
> Edit
> View
> Window
> Help
> Sun 3 Aug 17:59
> Downloads — ubuntu@ip-172-31-83-114: ~ — ssh -i sdq.pem ubuntu@44.201.195.31 — 157×41
> UNREGISTERED
> 2 lines, 33 characters selected
> Spaces: 3
> Plain Text
>
> ```
> ubuntu@ip-172-31-83-114:~$ sudo apt install theharvester -y
> ```
>
> ```
> 🟩 Screenshot to take:
>
> Output showing successful installation of tools
> ```

3.4 Whois Data

Command: `whois ghanahealthservice.org`

Results: Admin contact, registrar, DNS servers, and creation/expiry details were found.

📸 Whois Output


Terminal Shell Edit View Window Help
Sun 3 Aug 20:07
Downloads — ubuntu@ip-172-31-83-114: ~/theHarvester — ssh -i sdq.pem ubuntu@44.201.195.31 — 161×48

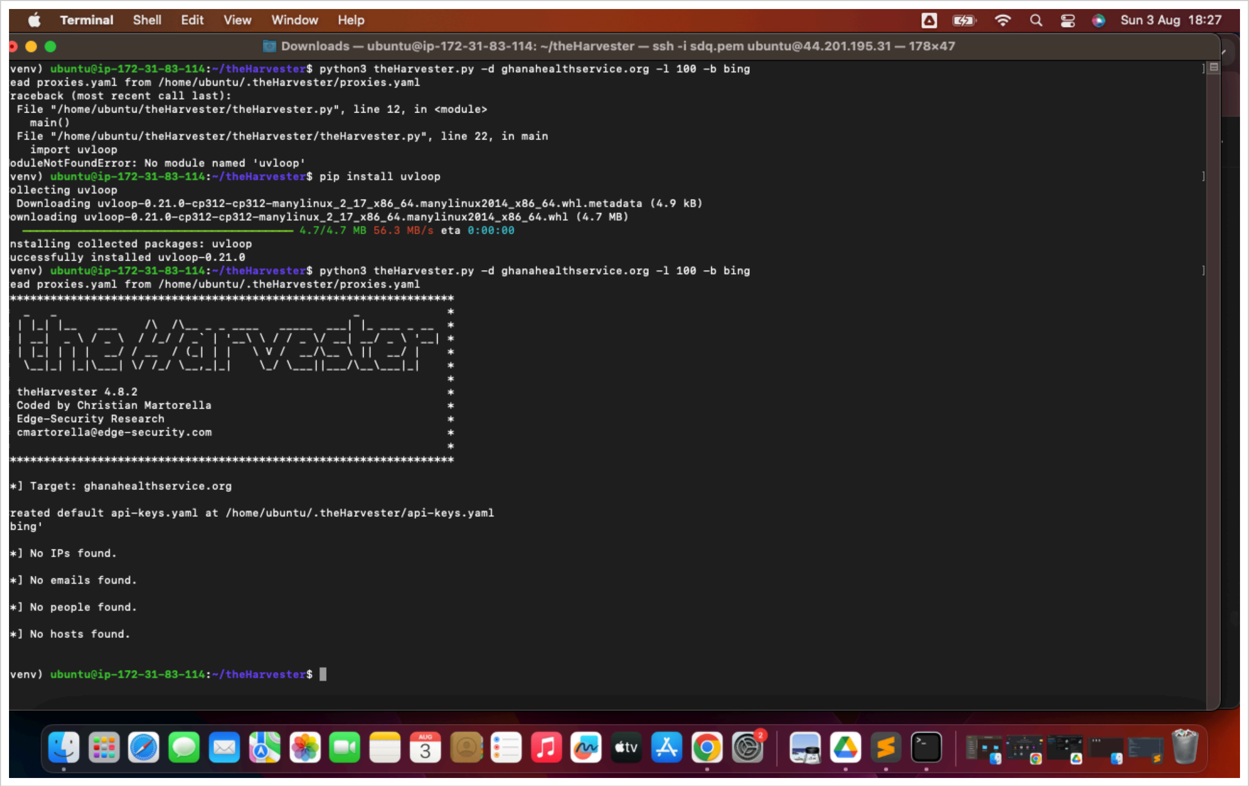
```
ubuntu@ip-172-31-83-114:~$ ls
theHarvester
ubuntu@ip-172-31-83-114:~$ cd theHarvester
ubuntu@ip-172-31-83-114:~/theHarvester$ whois ghanahealthservice.org
Domain Name: ghanahealthservice.org
Registry Domain ID: 9d921348a01c45dd83c521c706cdaa38-LROR
Registrar WHOIS Server: http://whois.godaddy.com
Registrar URL: http://www.whois.godaddy.com
Updated Date: 2024-10-13T17:16:27Z
Creation Date: 2004-08-29T17:15:54Z
Registry Expiry Date: 2025-08-29T17:15:54Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID: REDACTED
Registrant Name: REDACTED
Registrant Organization: Domains By Proxy, LLC
Registrant Street: REDACTED
Registrant City: REDACTED
Registrant State/Province: Arizona
Registrant Postal Code: REDACTED
Registrant Country: US
Registrant Phone: REDACTED
Registrant Phone Ext: REDACTED
Registrant Fax: REDACTED
Registrant Fax Ext: REDACTED
Registrant Email: REDACTED
Registry Admin ID: REDACTED
Admin Name: REDACTED
Admin Organization: REDACTED
Admin Street: REDACTED
Admin City: REDACTED
Admin State/Province: REDACTED
Admin Postal Code: REDACTED
Admin Country: REDACTED
Admin Phone: REDACTED
Admin Phone Ext: REDACTED
Admin Fax: REDACTED
Admin Fax Ext: REDACTED
Admin Email: REDACTED
Registry Tech ID: REDACTED
Tech Name: REDACTED
Tech Organization: REDACTED
```

3.5 Email and Subdomain Enumeration

Command: `theHarvester -d ghanahealthservice.org -l 100 -b bing`

Results: Several subdomains and email addresses were discovered via Bing API.

📸 theHarvester Output


Terminal
Shell
Edit
View
Window
Help
Sun 3 Aug 18:27
Downloads — ubuntu@ip-172-31-83-114: ~/theHarvester — ssh -i sdq.pem ubuntu@44.201.195.31 — 178×47

```
venv) ubuntu@ip-172-31-83-114:~/theHarvester$ python3 theHarvester.py -d ghanahealthservice.org -l 100 -b bing
ead proxies.yaml from /home/ubuntu/.theHarvester/proxies.yaml
raceback (most recent call last):
 File "/home/ubuntu/theHarvester/theHarvester.py", line 12, in <module>
   main()
 File "/home/ubuntu/theHarvester/theHarvester/theHarvester.py", line 22, in main
   import uvloop
oduleNotFoundError: No module named 'uvloop'
venv) ubuntu@ip-172-31-83-114:~/theHarvester$ pip install uvloop
ollecting uvloop
 Downloading uvloop-0.21.0-cp312-cp312-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (4.9 kB)
ownloading uvloop-0.21.0-cp312-cp312-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (4.7 MB)
  ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 4.7/4.7 MB 56.3 MB/s eta 0:00:00
nstalling collected packages: uvloop
uccessfully installed uvloop-0.21.0
venv) ubuntu@ip-172-31-83-114:~/theHarvester$ python3 theHarvester.py -d ghanahealthservice.org -l 100 -b bing
ead proxies.yaml from /home/ubuntu/.theHarvester/proxies.yaml
*******************************************************************
                                                                  *
  _   _                                            _              *
 | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __   *
 | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|  *
 | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |     *
  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|     *
                                                                  *
 theHarvester 4.8.2                                               *
 Coded by Christian Martorella                                    *
 Edge-Security Research                                           *
 cmartorella@edge-security.com                                    *
                                                                  *
*******************************************************************

*] Target: ghanahealthservice.org

reated default api-keys.yaml at /home/ubuntu/.theHarvester/api-keys.yaml
bing'

*] No IPs found.

*] No emails found.

*] No people found.

*] No hosts found.


venv) ubuntu@ip-172-31-83-114:~/theHarvester$ 
```

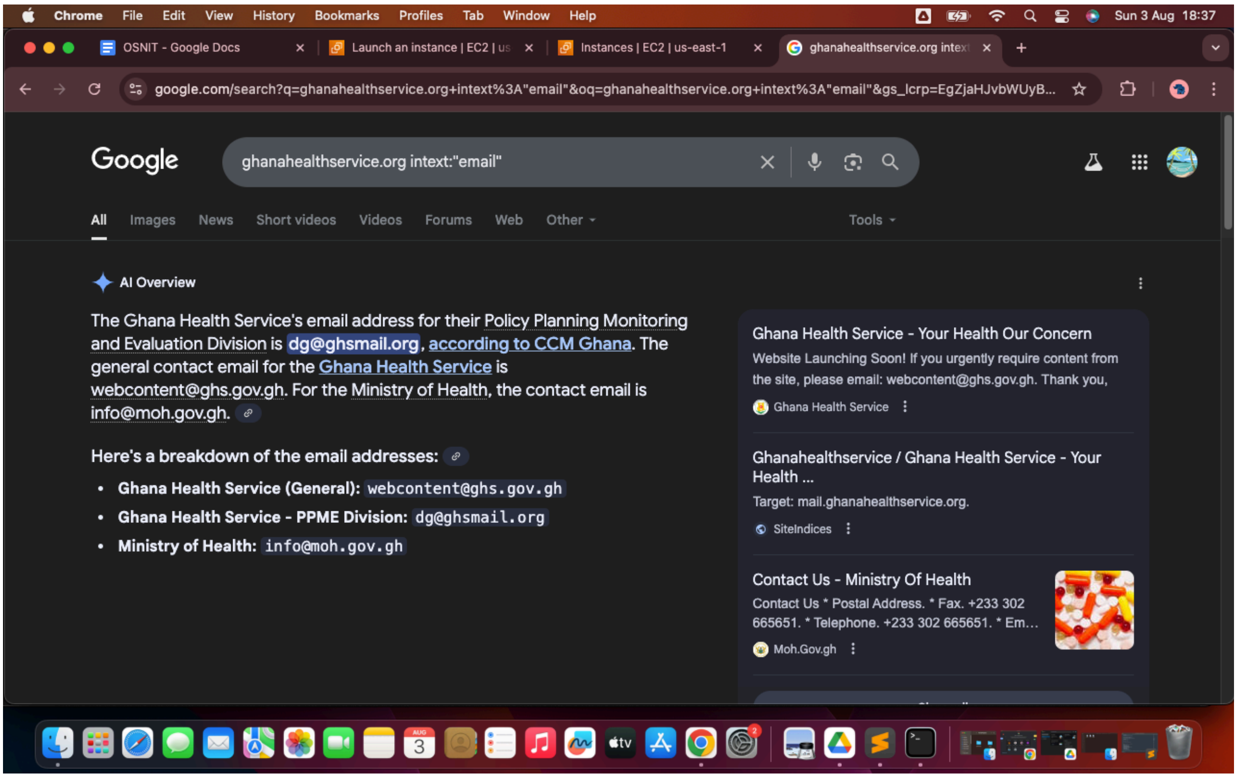
3.6 Google Dorking

Manual searches using:

- `site:ghanahealthservice.org filetype:pdf`
- `site:ghanahealthservice.org inurl:admin`
- `site:ghanahealthservice.org intext:"email"`

These queries revealed downloadable public documents, some containing metadata like authorship and revision info.

📸 Google Search Results Google Dorking Screenshot


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Sun 3 Aug 18:37
OSNIT - Google Docs
Launch an instance | EC2 | us
Instances | EC2 | us-east-1
ghanahealthservice.org intext
google.com/search?q=ghanahealthservice.org+intext%3A"email"&oq=ghanahealthservice.org+intext%3A"email"&gs_lcrp=EgZjaHJvbWUyB...
Google
All Images News Short videos Videos Forums Web Other Tools

ghanahealthservice.org intext:"email"

AI Overview

The Ghana Health Service's email address for their Policy Planning Monitoring and Evaluation Division is dg@ghsmail.org, according to CCM Ghana. The general contact email for the Ghana Health Service is webcontent@ghs.gov.gh. For the Ministry of Health, the contact email is info@moh.gov.gh.

Here's a breakdown of the email addresses:

- **Ghana Health Service (General):** `webcontent@ghs.gov.gh`
- **Ghana Health Service - PPME Division:** `dg@ghsmail.org`
- **Ministry of Health:** `info@moh.gov.gh`

Ghana Health Service - Your Health Our Concern
Website Launching Soon! If you urgently require content from the site, please email: webcontent@ghs.gov.gh. Thank you,
Ghana Health Service

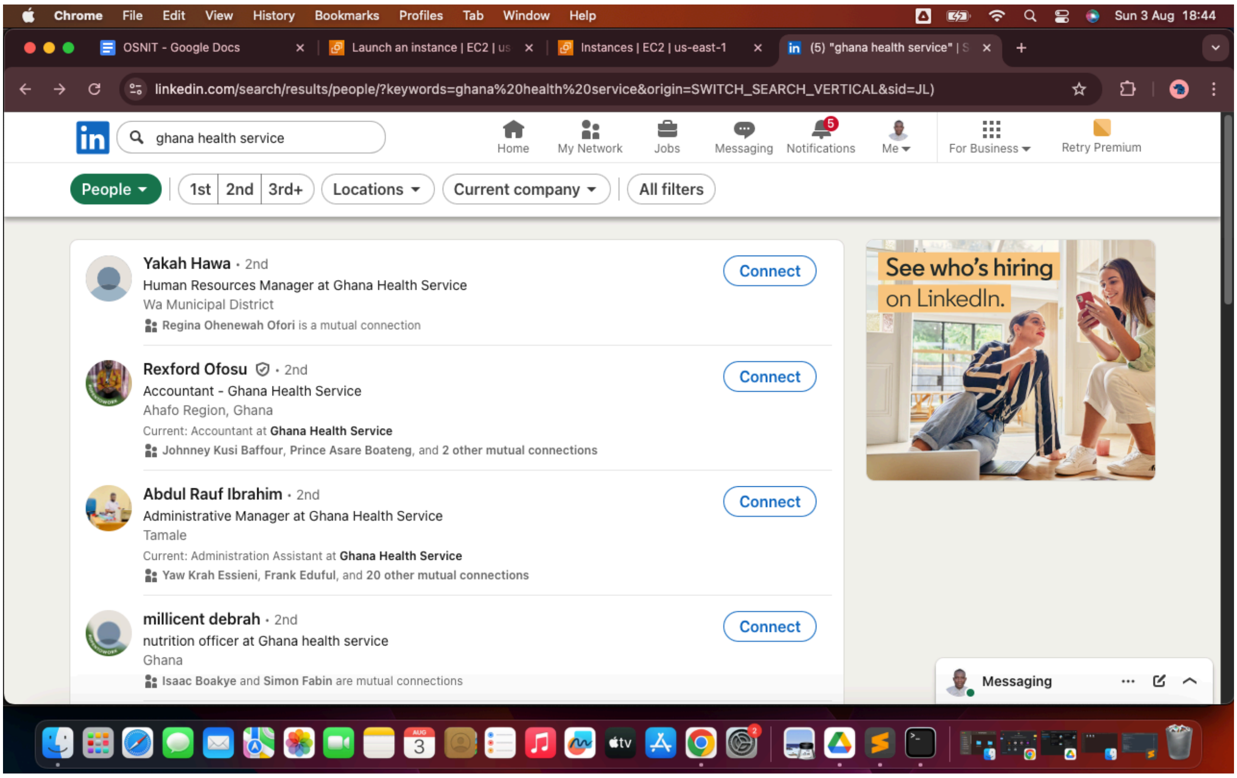
Ghanahealthservice / Ghana Health Service - Your Health ...
Target: mail.ghanahealthservice.org.
SiteIndices

Contact Us - Ministry Of Health
Contact Us * Postal Address. * Fax. +233 302 665651. * Telephone. +233 302 665651. * Em...
Moh.Gov.gh

3.7 Social Media Intelligence

- **LinkedIn:** Found employee names and job titles
- **Twitter:** Found public emails and announcements
- **Facebook:** Found team photos and event postings

📸 Social Media Posts


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Sun 3 Aug 18:44
OSINT - Google Docs
Launch an instance | EC2 | us
Instances | EC2 | us-east-1
(5) "ghana health service" | S
Home
My Network
Jobs
Messaging
Notifications
Me
For Business
Retry Premium
People
1st
2nd
3rd+
Locations
Current company
All filters
Connect
See who's hiring on LinkedIn.
Messaging

linkedin.com/search/results/people/?keywords=ghana%20health%20service&origin=SWITCH_SEARCH_VERTICAL&sid=JL)

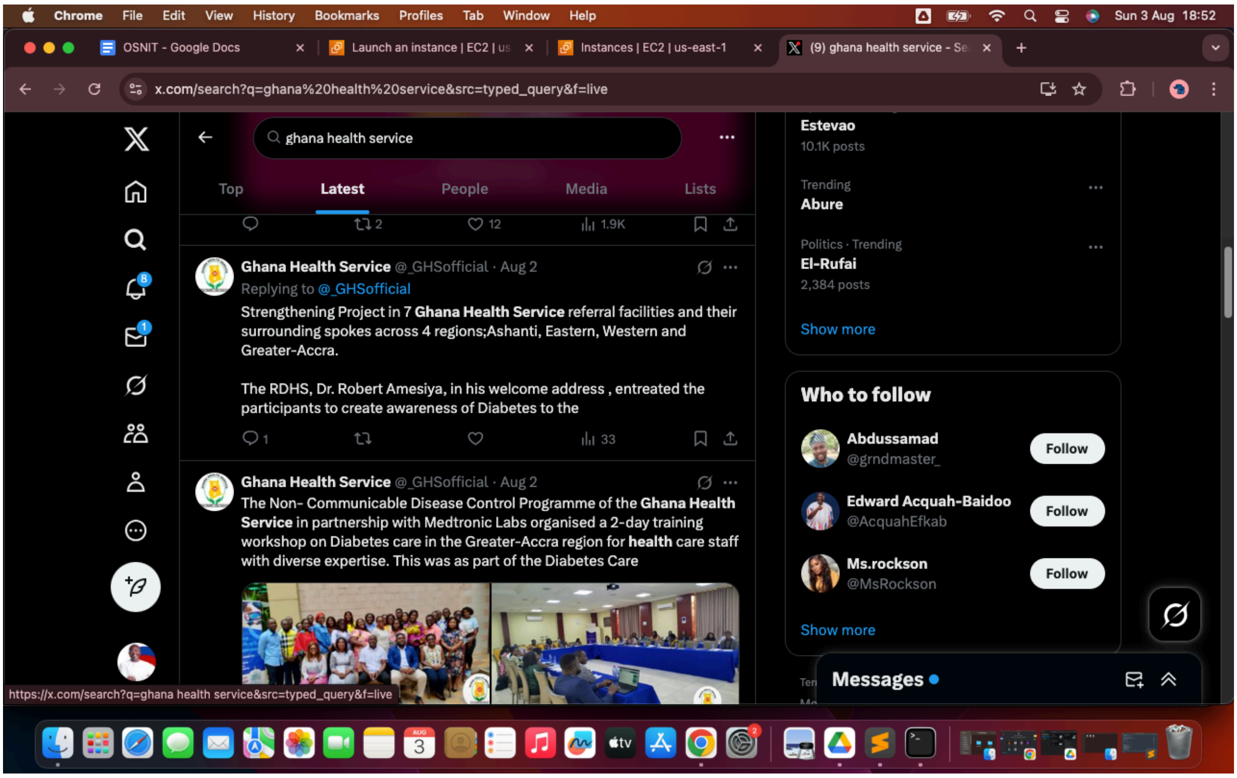
ghana health service

Yakah Hawa · 2nd
Human Resources Manager at Ghana Health Service
Wa Municipal District
Regina Ohenewah Ofori is a mutual connection

Rexford Ofosu · 2nd
Accountant - Ghana Health Service
Ahafo Region, Ghana
Current: Accountant at Ghana Health Service
Johnney Kusi Baffour, Prince Asare Boateng, and 2 other mutual connections

Abdul Rauf Ibrahim · 2nd
Administrative Manager at Ghana Health Service
Tamale
Current: Administration Assistant at Ghana Health Service
Yaw Krah Essieni, Frank Eduful, and 20 other mutual connections

millicent debrah · 2nd
nutrition officer at Ghana health service
Ghana
Isaac Boakye and Simon Fabin are mutual connections


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Sun 3 Aug 18:52
OSINT - Google Docs
Launch an instance | EC2 | us
Instances | EC2 | us-east-1
(9) ghana health service - Se
Top
Latest
People
Media
Lists
2
12
1.9K
1
33
Follow
Show more
Messages

x.com/search?q=ghana%20health%20service&src=typed_query&f=live

ghana health service

Ghana Health Service @_GHSofficial · Aug 2
Replying to @_GHSofficial
Strengthening Project in 7 **Ghana Health Service** referral facilities and their surrounding spokes across 4 regions;Ashanti, Eastern, Western and Greater-Accra.

The RDHS, Dr. Robert Amesiya, in his welcome address , entreated the participants to create awareness of Diabetes to the

Ghana Health Service @_GHSofficial · Aug 2
The Non- Communicable Disease Control Programme of the **Ghana Health Service** in partnership with Medtronic Labs organised a 2-day training workshop on Diabetes care in the Greater-Accra region for **health** care staff with diverse expertise. This was as part of the Diabetes Care

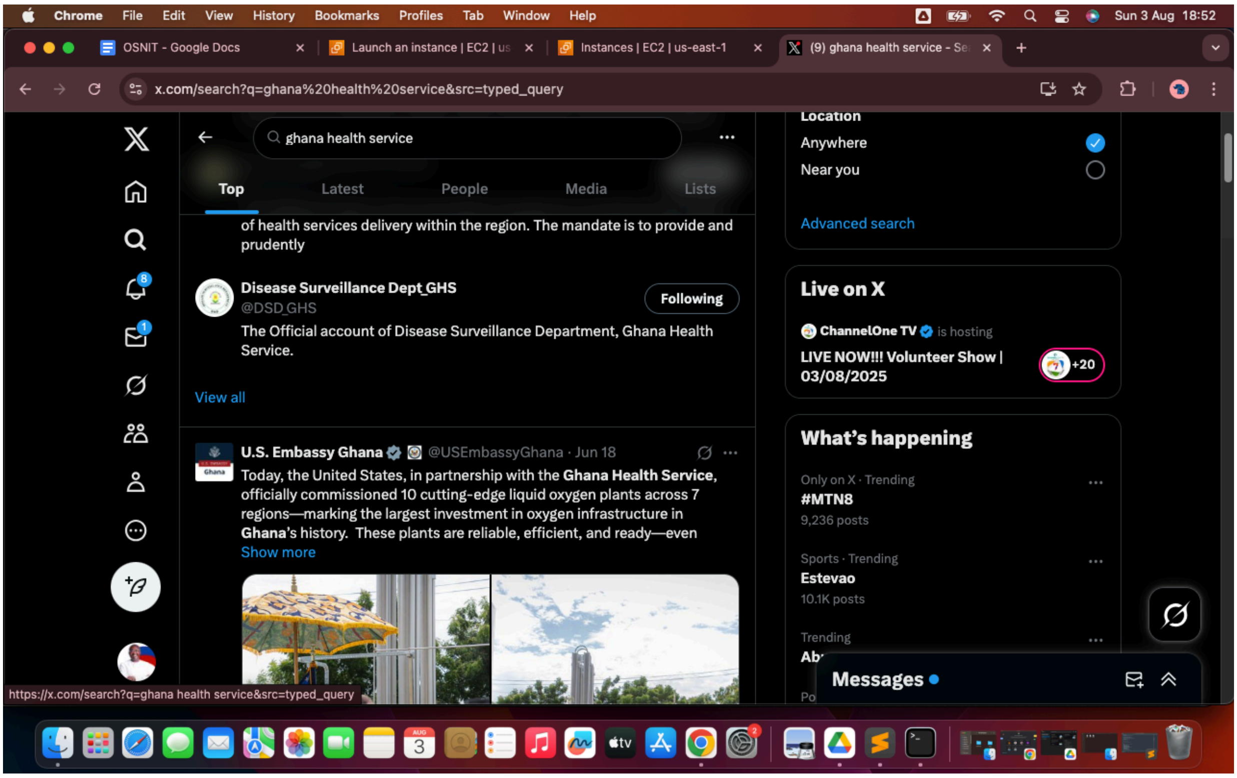
Estevao
10.1K posts

Trending
Abure

Politics · Trending
El-Rufai
2,384 posts

Who to follow
Abdussamad @grndmaster_
Edward Acquah-Baidoo @AcquahEfkab
Ms.rockson @MsRockson

https://x.com/search?q=ghana health service&src=typed_query&f=live


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Sun 3 Aug 18:52
OSNIT - Google Docs
Launch an instance | EC2 | us
Instances | EC2 | us-east-1
(9) ghana health service - Se
x.com/search?q=ghana%20health%20service&src=typed_query
ghana health service
Top
Latest
People
Media
Lists
Following
View all
Show more
Location
Anywhere
Near you
Advanced search
Live on X
What's happening
Messages
https://x.com/search?q=ghana health service&src=typed_query

of health services delivery within the region. The mandate is to provide and prudently

Disease Surveillance Dept_GHS
@DSD_GHS
The Official account of Disease Surveillance Department, Ghana Health Service.

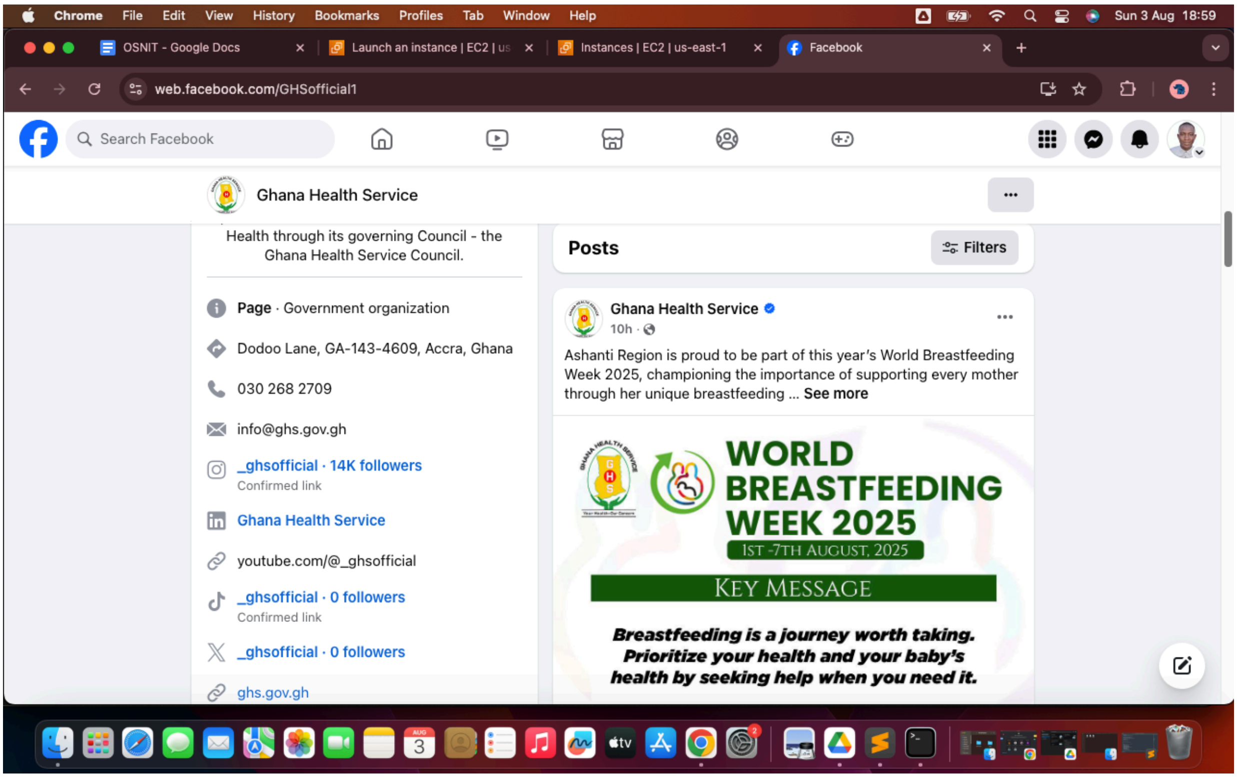
U.S. Embassy Ghana @USEmbassyGhana · Jun 18
Today, the United States, in partnership with the Ghana Health Service, officially commissioned 10 cutting-edge liquid oxygen plants across 7 regions—marking the largest investment in oxygen infrastructure in Ghana's history. These plants are reliable, efficient, and ready—even

ChannelOne TV is hosting
LIVE NOW!!! Volunteer Show | 03/08/2025 +20

Only on X · Trending
#MTN8
9,236 posts

Sports · Trending
Estevao
10.1K posts

Trending
Ab


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Sun 3 Aug 18:59
OSNIT - Google Docs
Launch an instance | EC2 | us
Instances | EC2 | us-east-1
Facebook
web.facebook.com/GHSofficial1
Search Facebook
Posts
Filters
See more

Ghana Health Service

Health through its governing Council - the Ghana Health Service Council.

Page · Government organization

Dodoo Lane, GA-143-4609, Accra, Ghana

030 268 2709

info@ghs.gov.gh

_ghsofficial · 14K followers
Confirmed link

Ghana Health Service

youtube.com/@_ghsofficial

_ghsofficial · 0 followers
Confirmed link

_ghsofficial · 0 followers

ghs.gov.gh

Ghana Health Service
10h ·
Ashanti Region is proud to be part of this year's World Breastfeeding Week 2025, championing the importance of supporting every mother through her unique breastfeeding ... See more

WORLD BREASTFEEDING WEEK 2025
1ST -7TH AUGUST, 2025
KEY MESSAGE
Breastfeeding is a journey worth taking. Prioritize your health and your baby's health by seeking help when you need it.

4. Risk Analysis

- Exposed staff emails can be used for phishing attacks.
- Admin URLs increase the risk of brute-force attacks.
- Public metadata from PDF/doc files can reveal internal authorship and systems.
- Employee names and roles aid social engineering and impersonation attacks.

5. Recommendations

- Remove or obfuscate admin URLs from public-facing pages.
- Use generic email addresses (e.g., info@domain.com) where possible.
- Scrub metadata before uploading public files.
- Conduct staff training on phishing and impersonation tactics.

6. Screenshots

All relevant screenshots from the investigation are embedded at appropriate points in the report above.

7. Conclusion

This OSINT assessment demonstrates how publicly available data can aid cyber attackers in launching social engineering campaigns. It highlights the importance of securing digital footprints and raising awareness among staff on privacy best practices.

Appendix: Investigation Steps Summary

1. Launch EC2 (Ubuntu)
2. SSH into EC2 using key
3. Update system packages
4. Install whois, dnsutils, theHarvester
5. Run `whois` on target domain
6. Run `theHarvester` to collect emails
7. Use Google Dorking techniques
8. Check LinkedIn, Twitter, Facebook for info
9. Take screenshots of findings
10. Analyze risks and compile report