BHASKARACHARYA NATIONAL INSTITUTE FOR SPACE APPLICATIONS AND GEO-INFORMATICS

WEEKLY PROGRESS REPORT (08/01/2026 – 15/01/2026)

WEEK 2	
PROJECT NAME	Monitoring and change detection system using OSINT

PROJECT DESCRIPTION :	CREATING OSINT TOOL FOR MONITORING AND CHANGE DETECTION SYSTEM BY MONITORING PUBLICLY AVAILABLE INFORMATION.
GROUP MEMBER :	Harshil Vaniya, Shalomo Agarwarkar, Vrushank Thakkar
GROUP ID :	2026G195
GROUP GUIDE :	CHASIYA KRUTIKA
GROUP COORDINATOR :	SIDHDHARTH PATEL
COLLEGE GUIDE NAME :	BHUMIKA DOSHI
COLLEGE GUIDE No. :	9016888925
COLLEGE GUIDE EMAIL. :	BHUMIKASDOSHI@GMAIL.COM
COLLEGE NAME :	DEPT. OF BIOCHEMISTRY AND FORENSICS SCIENCE, GUJARAT UNIVERSITY

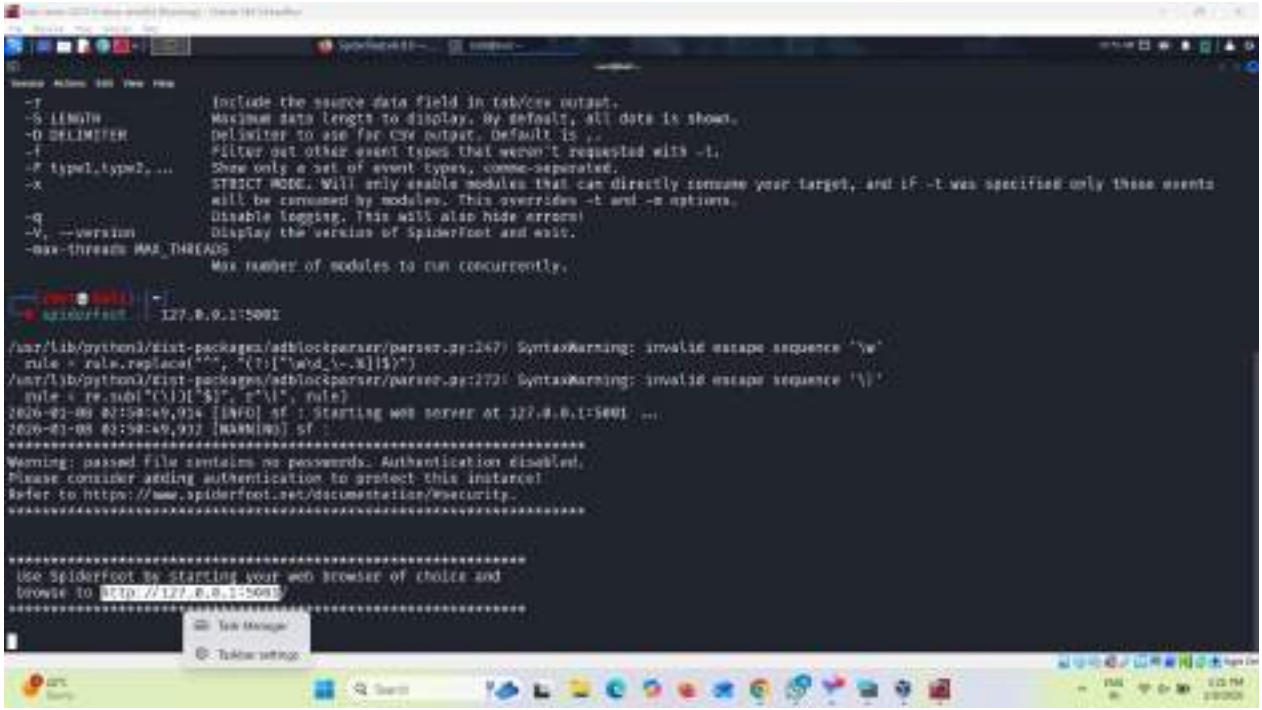
08/01/2026	• **Testing web domain enumeration using tools like spider foot and sub finder(Vaniya Harshil, Vrushank Thakkar)** • **Kali Linux VirtualBox setup & basics of change detection engine for OSINT (Vaniya Harshil)** • **Public repos research(Shalomo Agarwarkar)**
09/01/2026	• **Form filling and amass usage and implementation (Vaniya Harshil)** • **Reconnicence tool creation (Vrushank Thakkar)** • **Researched HIBP and alternatives& test page creation (Shalomo Agarwarkar)**
10/01/2026	**Holiday (2nd Saturday)**
11/01/2026	**Holiday (Sunday)**
12/01/2026	• **Reconnicence tool error solving (Vrushank Thakkar)** • **Wapiti testing and researching alternatives (Vaniya Harshil)** • **Researching behaviour analysis and change detection techniques (Shalomo Agarwarkar)** • **Half day leave (Vaniya Harshil, Shalomo Agarwarkar, Vrushank Thakkar)**
13/01/2026	• **Researching new technologies to integrate in the tool(Vrushank Thakkar, Harshil Vaniya)** • **Researching cryptocurrency forensics (Shalomo Agarwarkar)**
14/01/2026	**Holiday (Uttarayan)**

Next Week Plan	**Organising everything we've learned and starting the basics of tool creation.**

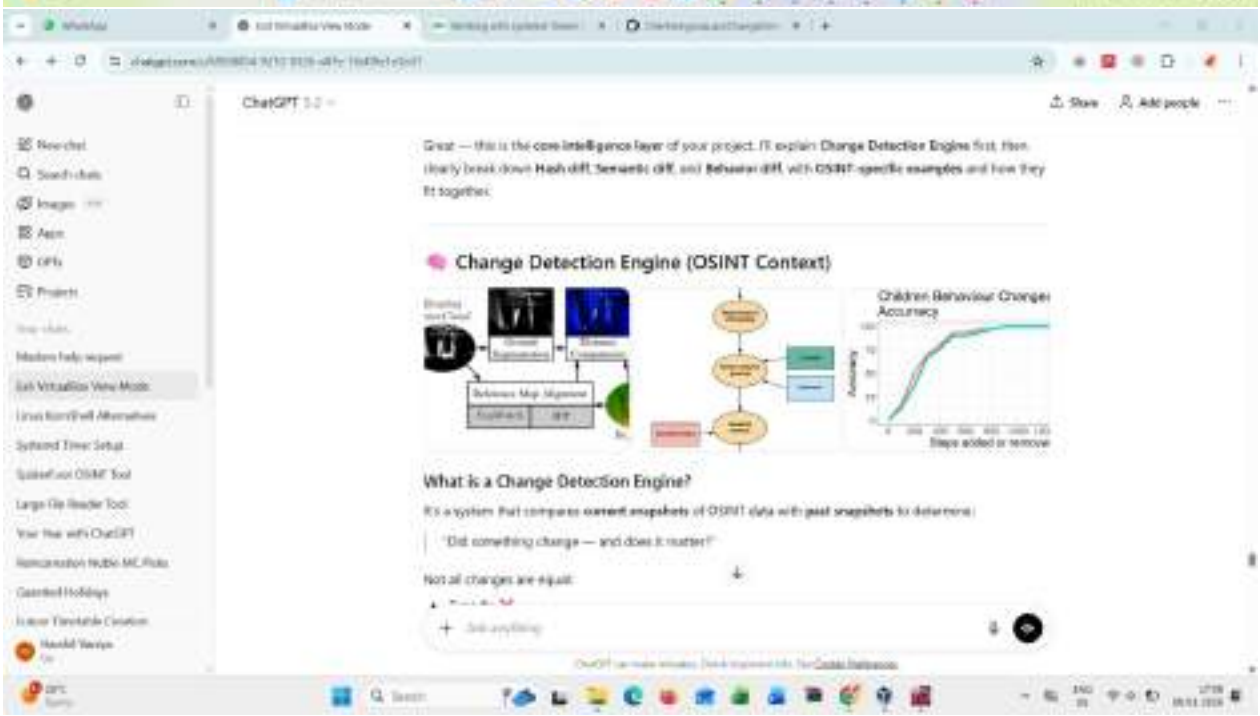
REFERENCE:

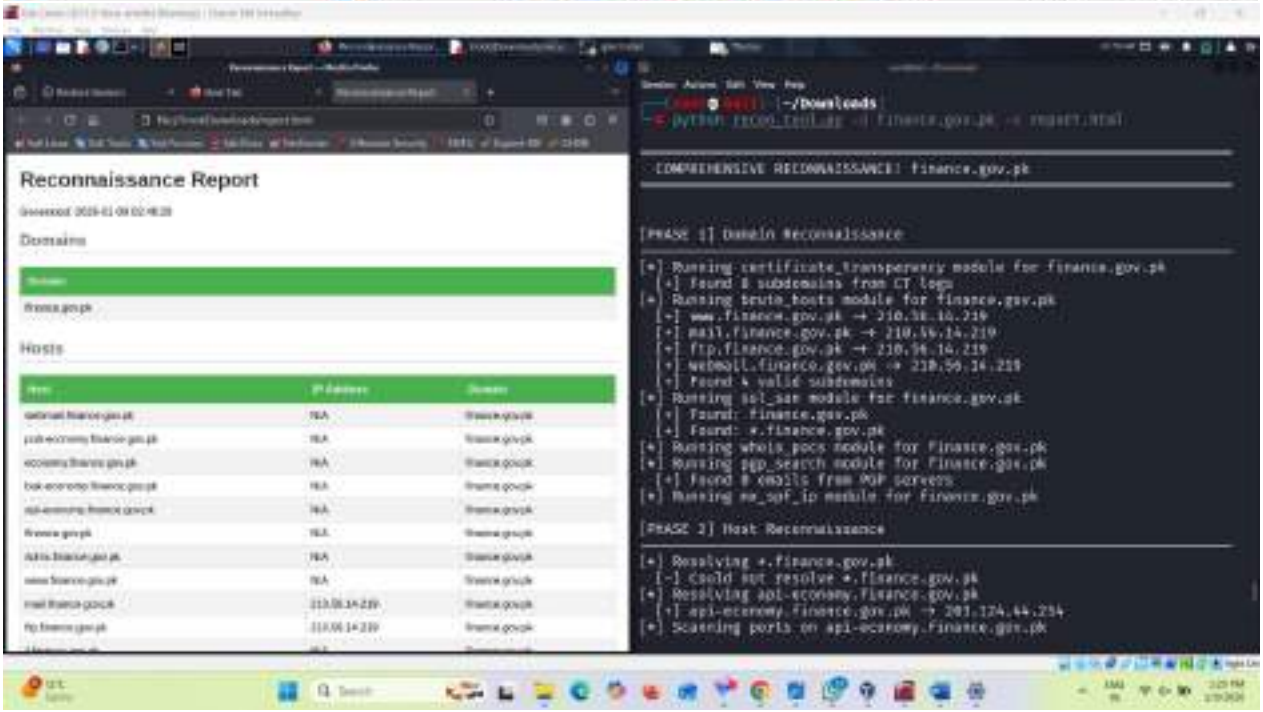
- https://www.atlassystems.com/blog/open-source-intelligence-osint
- https://www.getsignal.info/blog/the-missing-link-in-threat-detection-from-identification-to-action
- https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/
- https://www.geeksforgeeks.org/linux-unix/subfinder-tool-in-linux/
-

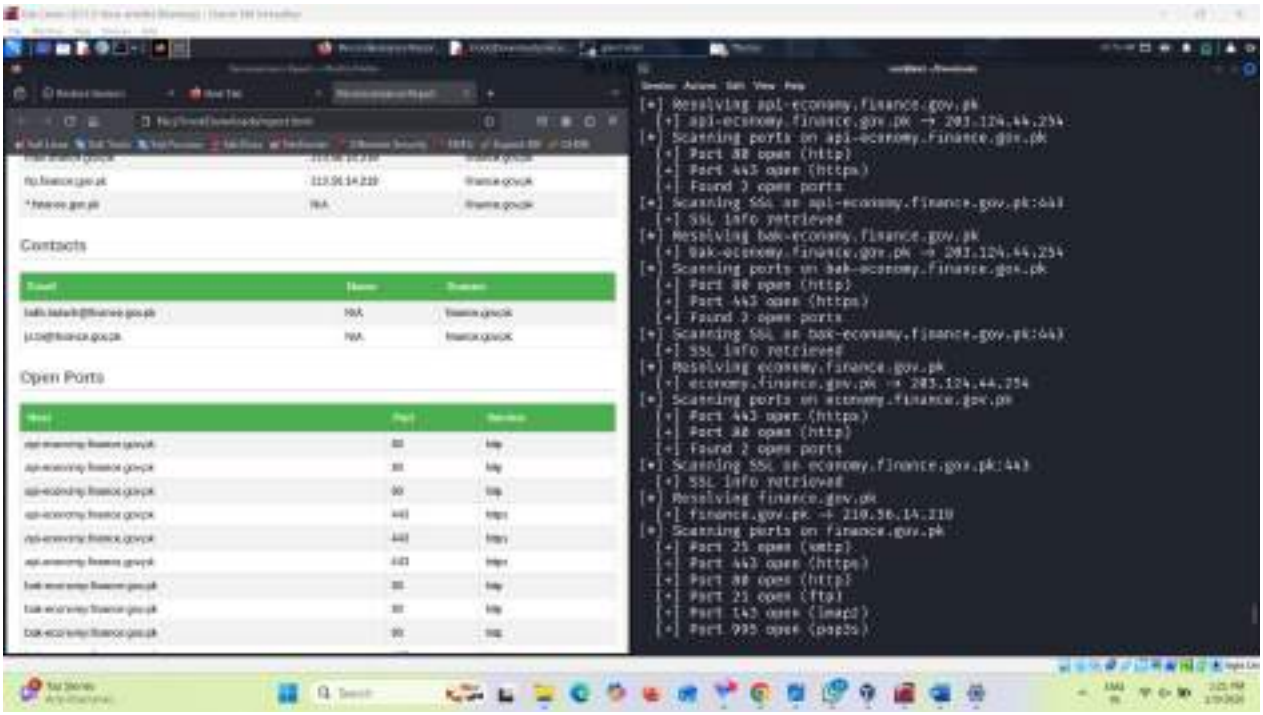
SCREEN SHOTS:

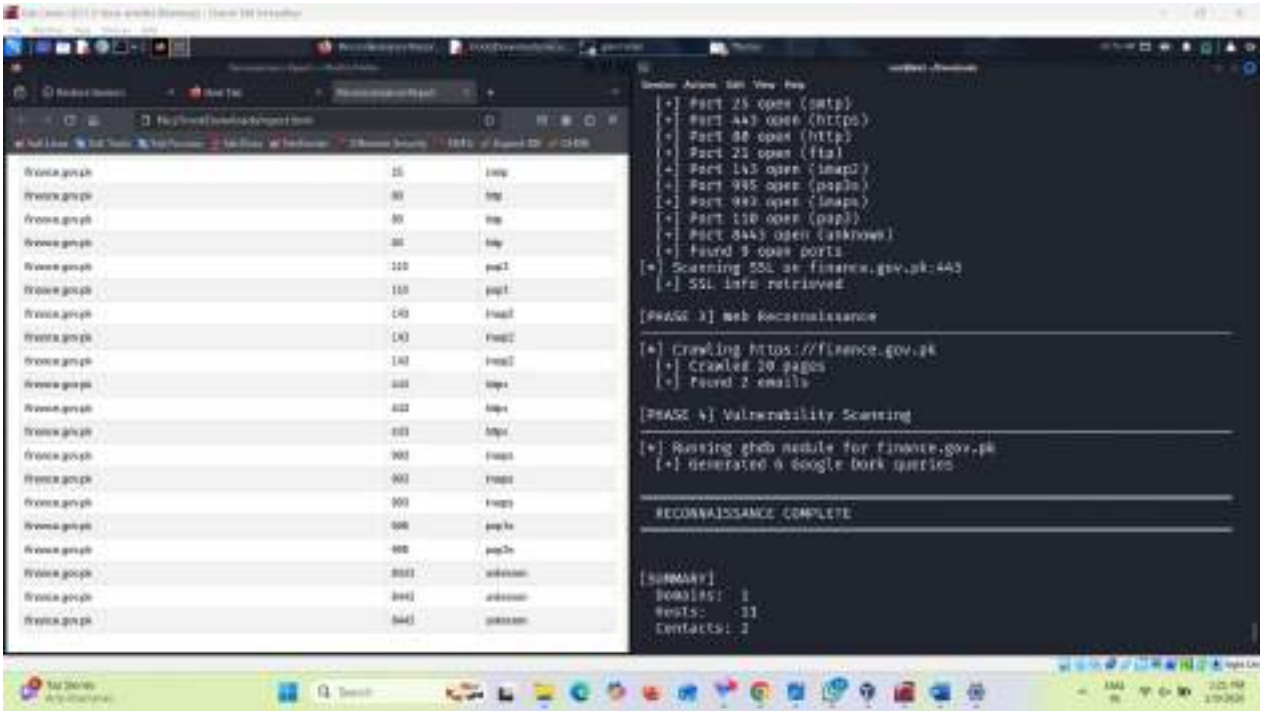


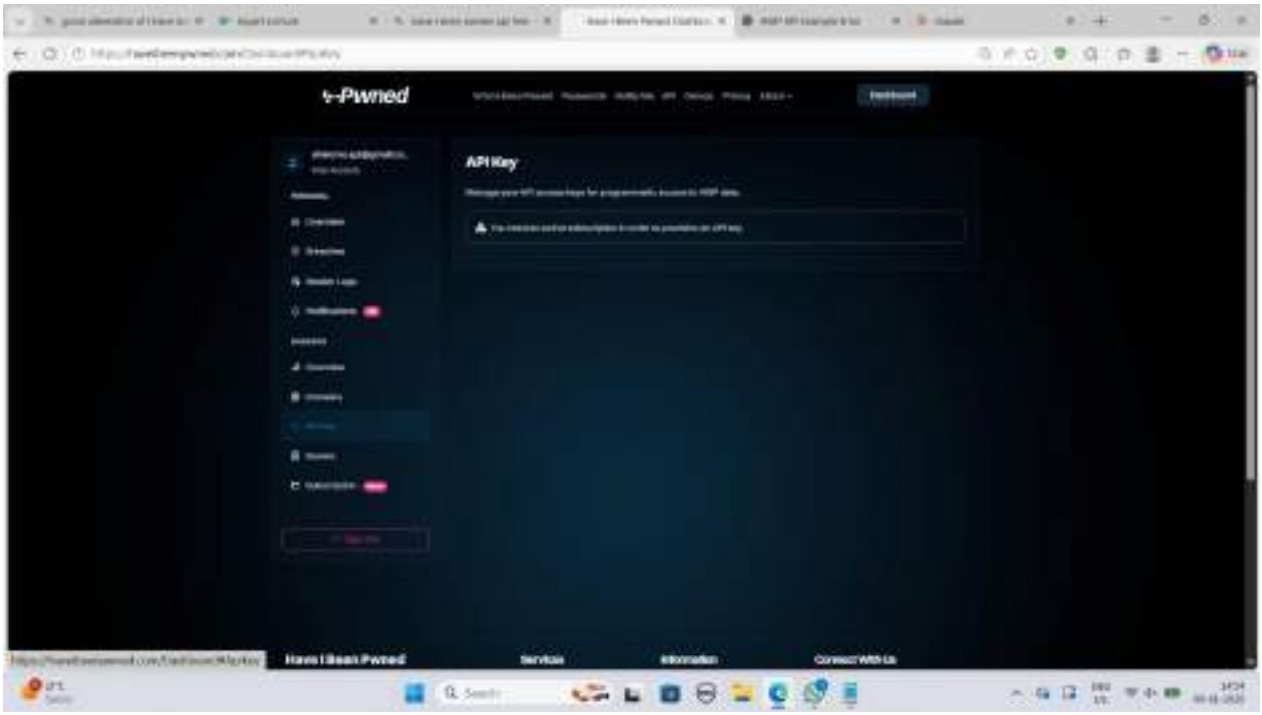
```
[INF] Migration successful from /root/.config/subfinder/config.yaml to /root/.config/subfinder/provider-config.yaml.

┌──(root㉿kali)-[~/Downloads]
└─# python3 subfinder_python.py
[+] Subfinder OSINT Module

Enter domain name (example.com): pakistan.gov.pk
[+] Running subfinder for: pakistan.gov.pk

[+] Subfinder exit code: 0

[+] Subdomains found:

email.pakistan.gov.pk
mail.pakistan.gov.pk
pmc.pakistan.gov.pk
mail.heritage.pakistan.gov.pk
www.heritage.pakistan.gov.pk
mail.pmc.pakistan.gov.pk
www.pakistan.gov.pk
eiweek.pakistan.gov.pk
fccp.pakistan.gov.pk
heritage.pakistan.gov.pk
email.heritage.pakistan.gov.pk
www.mail.pakistan.gov.pk
```

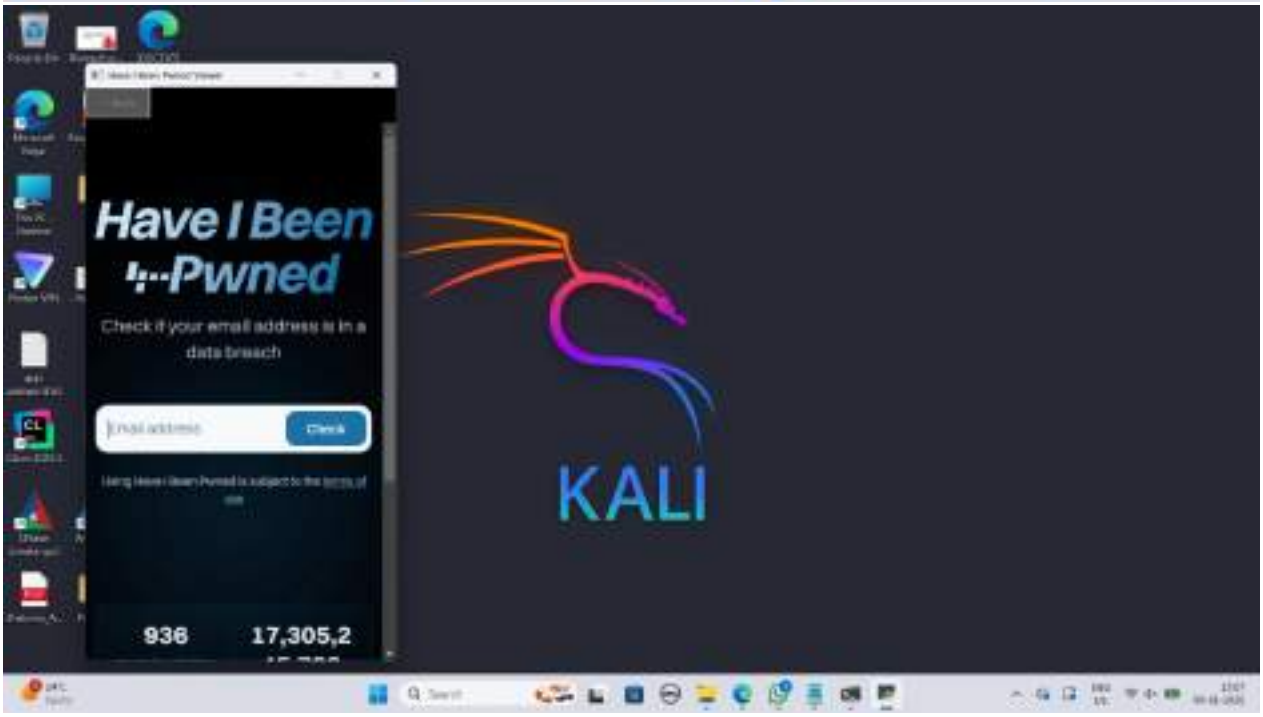



Reconnaissance Report
Domains
Hosts
COMPREHENSIVE RECONNAISSANCE: finance.gov.pk
[PHASE 1] Domain Reconnaissance
[PHASE 2] Host Reconnaissance


Contacts
Open Ports
[*] Resolving api-economy.finance.gov.pk
[+] api-economy.finance.gov.pk → 203.124.44.254
[*] Scanning ports on api-economy.finance.gov.pk
[+] Port 80 open (http)
[+] Port 443 open (https)
[+] Found 2 open ports
[*] Scanning SSL on api-economy.finance.gov.pk:443
[+] SSL info retrieved
[*] Resolving bak-economy.finance.gov.pk
[+] bak-economy.finance.gov.pk → 203.124.44.254
[*] Scanning ports on bak-economy.finance.gov.pk
[+] Port 80 open (http)
[+] Port 443 open (https)
[+] Found 2 open ports
[*] Scanning SSL on bak-economy.finance.gov.pk:443
[+] SSL info retrieved
[*] Resolving economy.finance.gov.pk
[+] economy.finance.gov.pk → 203.124.44.254
[*] Scanning ports on economy.finance.gov.pk
[+] Port 443 open (https)
[+] Port 80 open (http)
[+] Found 2 open ports
[*] Scanning SSL on economy.finance.gov.pk:443
[+] SSL info retrieved
[*] Resolving finance.gov.pk
[+] finance.gov.pk → 210.56.14.210
[*] Scanning ports on finance.gov.pk
[+] Port 25 open (smtp)
[+] Port 443 open (https)
[+] Port 80 open (http)
[+] Port 21 open (ftp)
[+] Port 143 open (imap2)
[+] Port 995 open (pop3s)


[+] Port 25 open (smtp)
[+] Port 443 open (https)
[+] Port 80 open (http)
[+] Port 21 open (ftp)
[+] Port 143 open (imap2)
[+] Port 995 open (pop3s)
[+] Port 993 open (imaps)
[+] Port 110 open (pop3)
[+] Port 8443 open (unknown)
[+] Found 9 open ports
[*] Scanning SSL on finance.gov.pk:443
[+] SSL info retrieved
[PHASE 3] Web Reconnaissance
[*] Crawling https://finance.gov.pk
[+] Crawled 20 pages
[+] Found 2 emails
[PHASE 4] Vulnerability Scanning
[*] Running ghdb module for finance.gov.pk
[+] Generated 6 Google Dork queries
RECONNAISSANCE COMPLETE
[SUMMARY]
Domains: 1
Hosts: 11
Contacts: 2


API Key
Have I Been Pwned
Services
Information
Connect With Us


Have I Been Pwned
Check if your email address is in a data breach
Email address
Check
936
17,305,2
KALI

README

WhatBreach

WhatBreach is an OSINT tool that simplifies the task of discovering what breaches an email address has been discovered in. WhatBreach provides a simple and effective way to search either multiple, or a single email address and discover all known breaches that this email has been seen in. From there WhatBreach is capable of downloading the database (if it is publicly available), downloading the pastes the email was seen in, or searching the domain of the email for further investigation. To perform this task successfully WhatBreach takes advantage of the following websites and/or APIs:

- WhatBreach takes advantage of haveibeenpwned.com's API. HIBP's API is no longer free and costs 3.50 USD per month. To get an API key please see here
- WhatBreach takes advantage of dehashed.com in order to discover if the database has been seen in a breach before. WhatBreach provides a link to a dehashed search for effective downloading
- WhatBreach takes advantage of hunter.io's API (requires free API token) this allows simple and effective domain searching and will provide further information on the domain being searched along with store the discovered results in a file for later processing
- WhatBreach takes advantage of pastes from pastebin.com that have been found from HIBP. It will also provide a link to the paste that the breach was seen in and is capable of downloading the raw paste if requested
- WhatBreach takes advantage of databases.today to download the databases off the website. This allows a simple and effective way of downloading databases without having to search manually
- WhatBreach takes advantage of weleakinfo.com's API (requires free API token) this provides an extra search for the email in order to discover even more public breaches
- WhatBreach takes advantage of emailrep.io's simple open API to search for possible profiles associated with an email. It also dumps all information discovered into a file for further processing

Some interesting features of WhatBreach include the following:

- Ability to detect if the email is a ten minute email or not and prompt to process it or not

Packages

No packages published

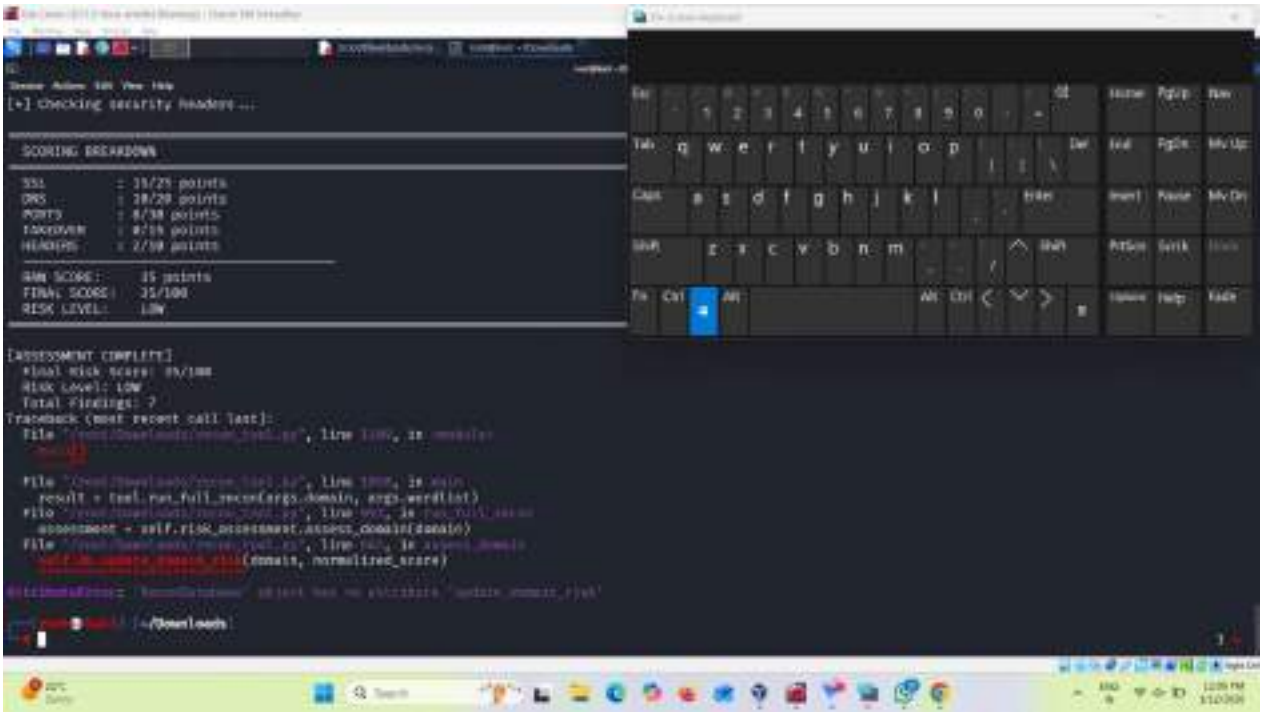
Contributors 4

Gaylin

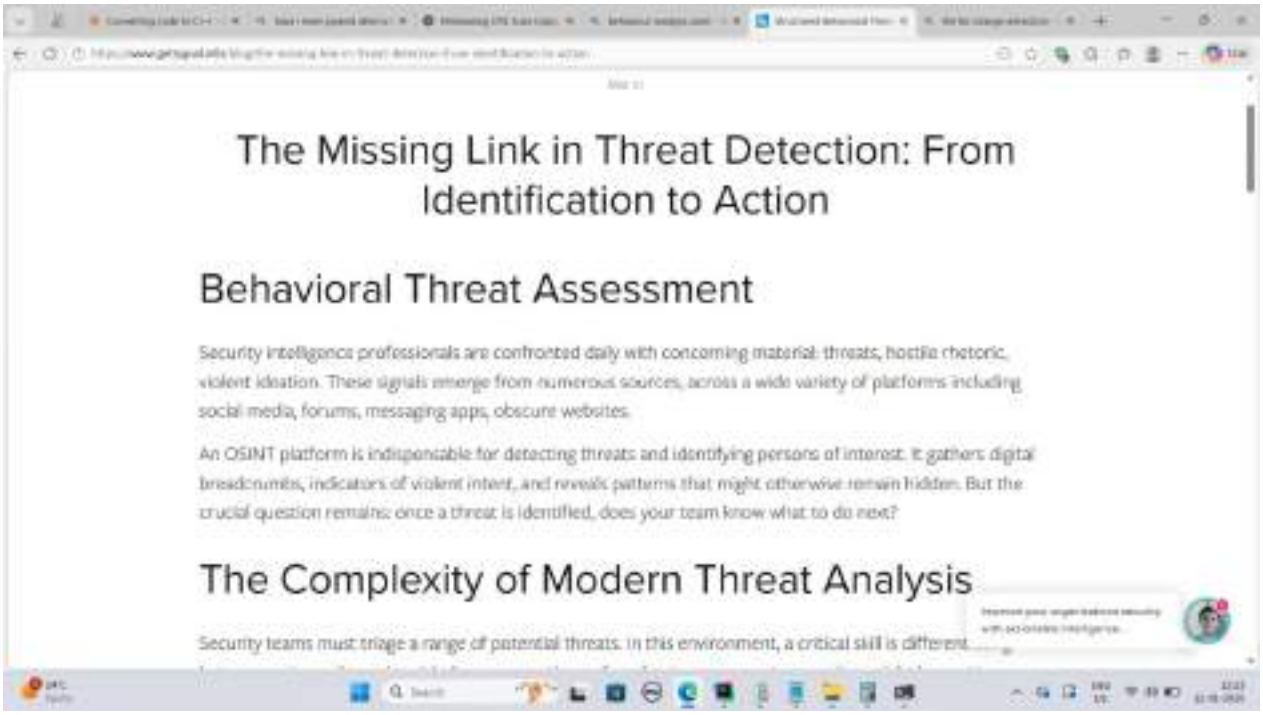
Languages

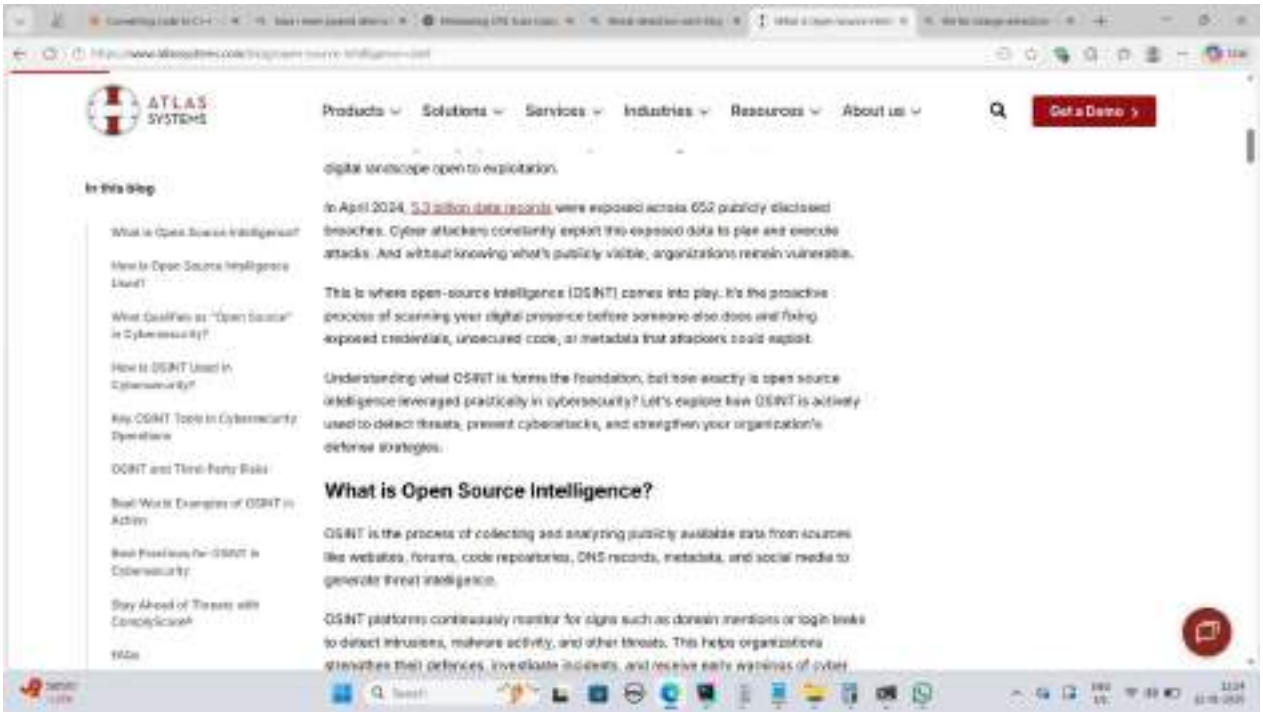
- Python 100.0%

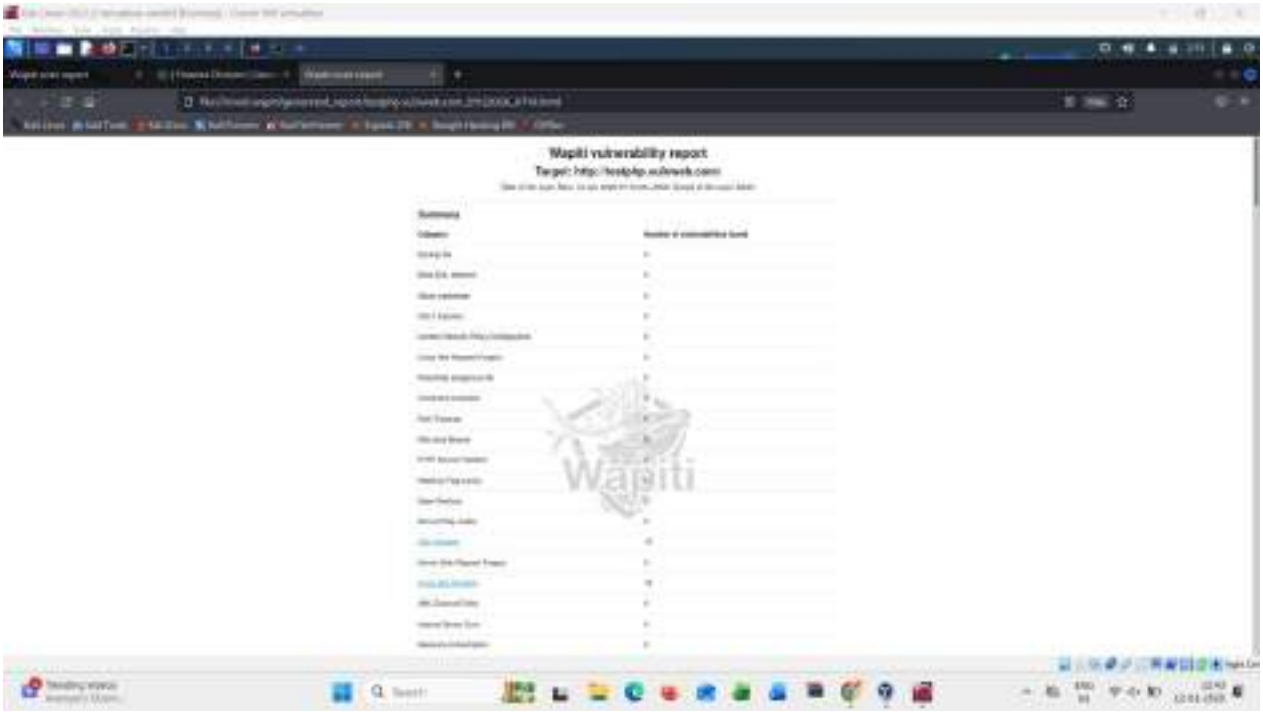
```
  PORTS        : 10/30 points
  TAKEOVER     : 0/15 points
  HEADERS      : 2/10 points
  ----------------------------------------
  RAW SCORE:     57 points
  FINAL SCORE:   57/100
  RISK LEVEL:    MEDIUM
------------------------------------------------------------

[ASSESSMENT COMPLETE]
  Final Risk Score: 57/100
  Risk Level: MEDIUM
  Total Findings: 17
  Recommendations: 5

Traceback (most recent call last):
  File "/home/[redacted]", line [redacted], in [redacted]
    [redacted]

  File "/home/[redacted]", line [redacted], in [redacted]
    result = tool.run_full_recon(args.domain, args.wordlist)
  File "/home/[redacted]", line [redacted], in run_full_recon
    assessment = self.risk_assessment.assess_domain(domain)
  File "/home/[redacted]", line [redacted], in assess_domain
    [redacted]

    [redacted]

    ... (2 lines) ...
    [redacted]

    [redacted]

[redacted]: [redacted] risk_assessment.[redacted] has no attribute 'calculate_risk_score'
```

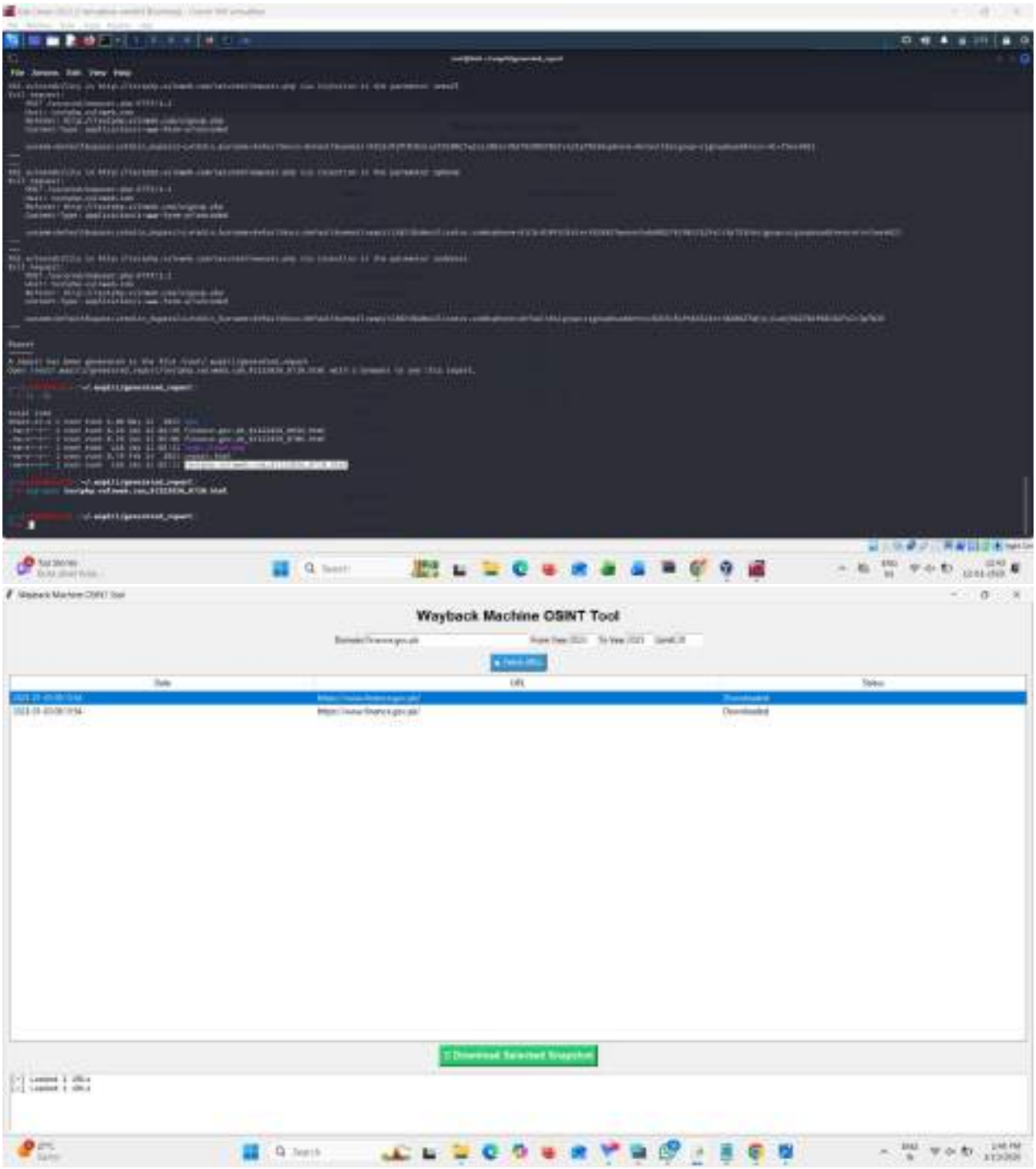

[+] Checking security headers ...
SCORING BREAKDOWN
SSL : 15/25 points
DNS : 20/20 points
PORTS : 8/30 points
TAKEOVER : 0/15 points
HEADERS : 2/10 points
RAW SCORE: 35 points
FINAL SCORE: 35/100
RISK LEVEL: LOW
[ASSESSMENT COMPLETE]
Final Risk Score: 35/100
Risk Level: LOW
Total Findings: 7
Traceback (most recent call last):

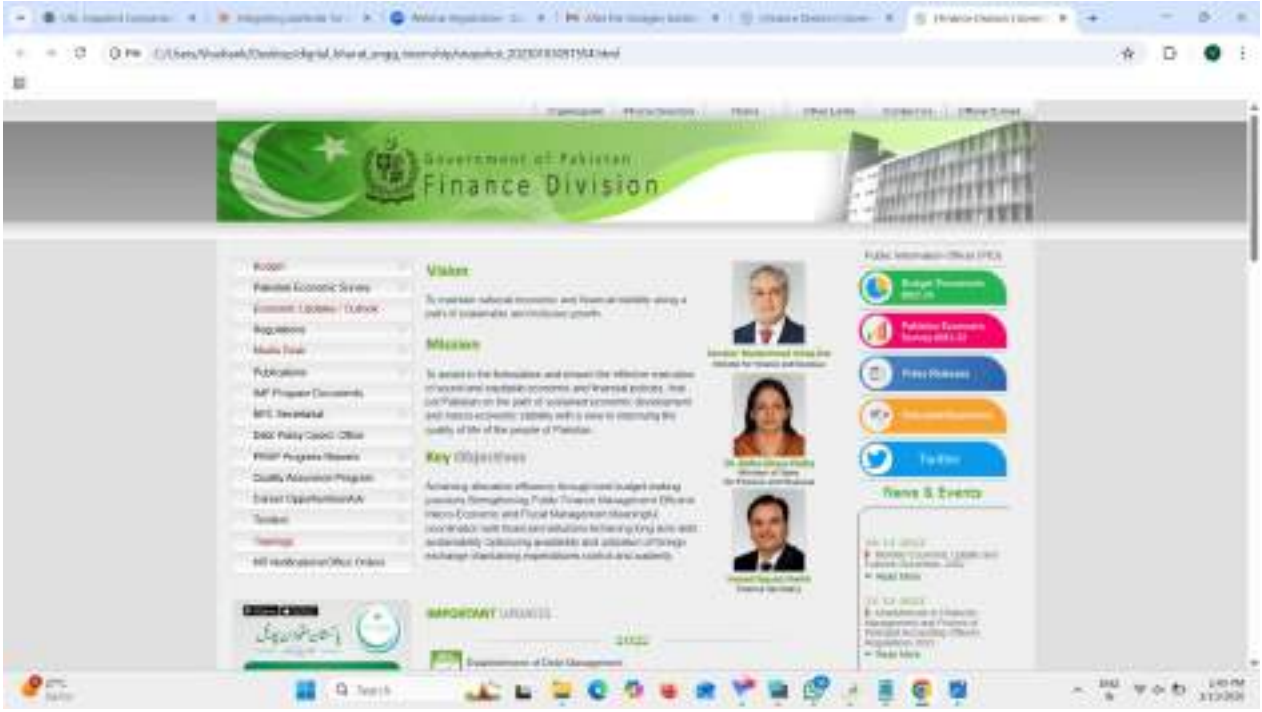
\

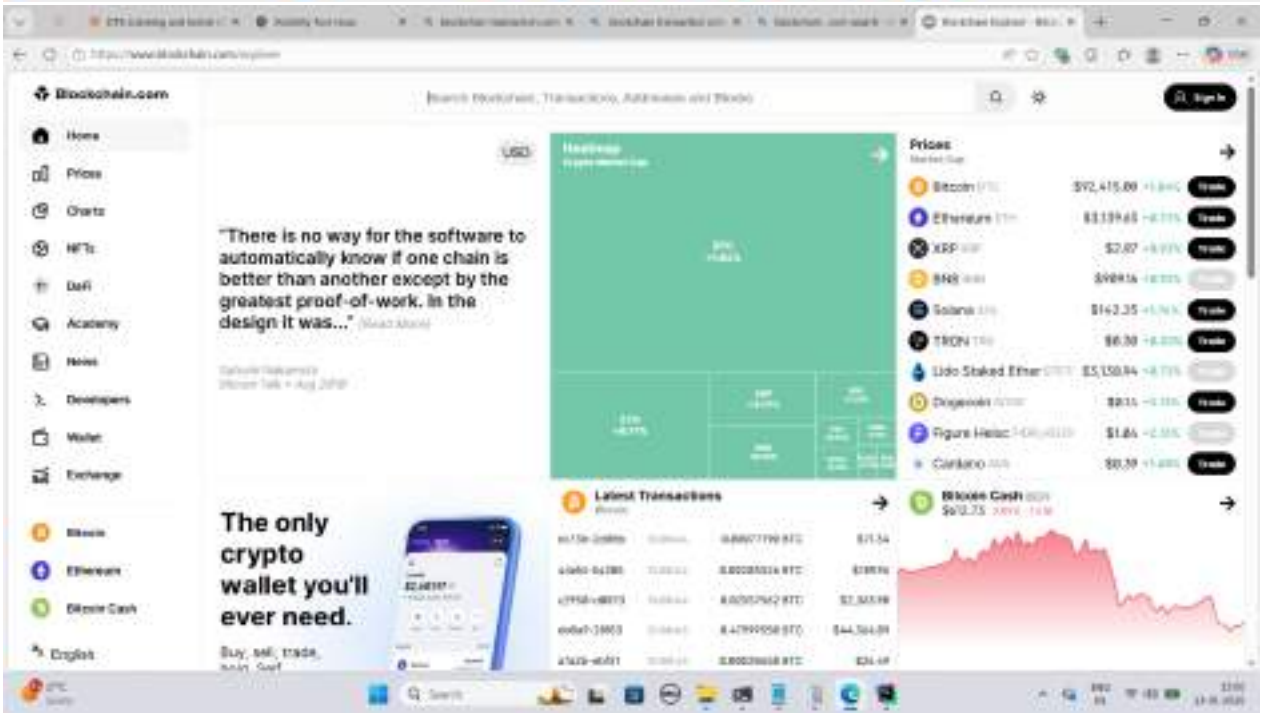

The Missing Link in Threat Detection: From Identification to Action
Behavioral Threat Assessment
Security intelligence professionals are confronted daily with concerning material: threats, hostile rhetoric, violent ideation. These signals emerge from numerous sources, across a wide variety of platforms including social media, forums, messaging apps, obscure websites.
An OSINT platform is indispensable for detecting threats and identifying persons of interest. It gathers digital breadcrumbs, indicators of violent intent, and reveals patterns that might otherwise remain hidden. But the crucial question remains: once a threat is identified, does your team know what to do next?
The Complexity of Modern Threat Analysis
Security teams must triage a range of potential threats. In this environment, a critical skill is different

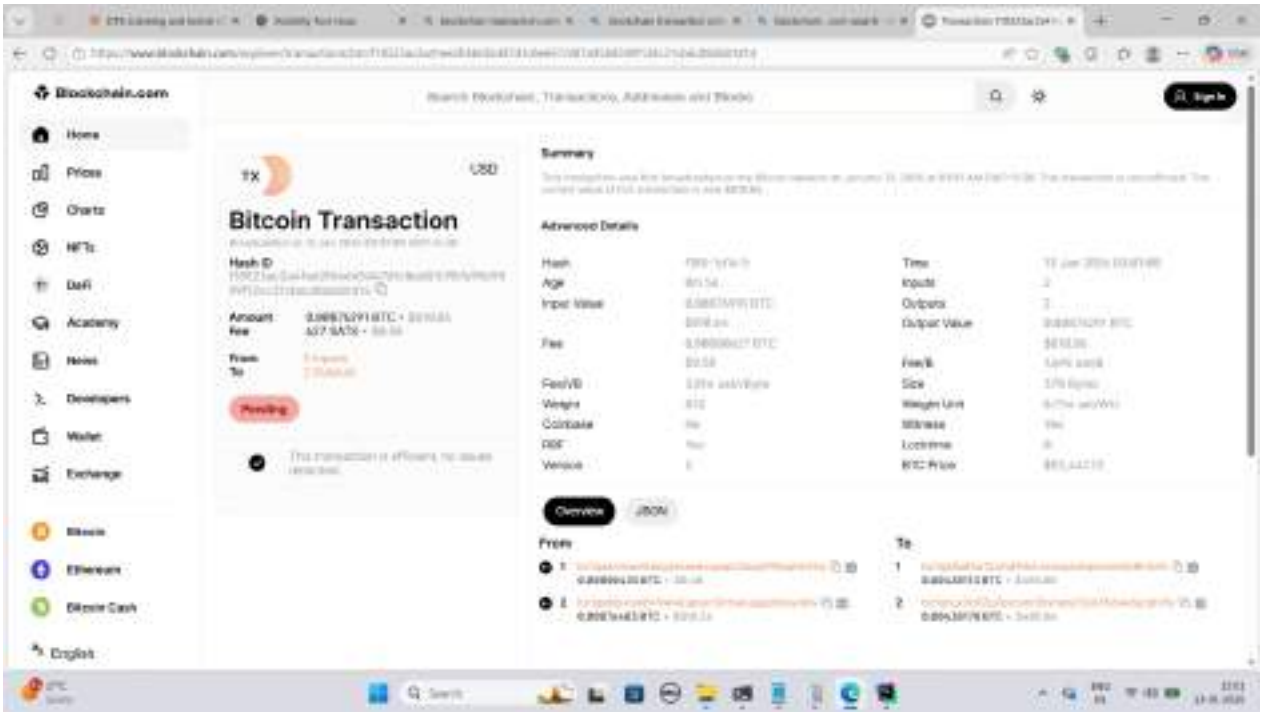

ATLAS SYSTEMS
Products
Solutions
Services
Industries
Resources
About us
Get a Demo
In this blog
What is Open Source Intelligence?
How to Open Source Intelligence Used?
What Qualifies as "Open Source" in Cybersecurity?
How to OSINT Used in Cybersecurity?
Key OSINT Tools in Cybersecurity Operations
OSINT and Third-Party Risks
Real-World Examples of OSINT in Action
Best Practices for OSINT in Cybersecurity
Stay Ahead of Threats with Concepticsoft
FAQs
digital landscape open to exploitation.
In April 2024, 5.3 billion data records were exposed across 652 publicly disclosed breaches. Cyber attackers constantly exploit this exposed data to plan and execute attacks. And without knowing what's publicly visible, organizations remain vulnerable.
This is where open-source intelligence (OSINT) comes into play. It's the proactive process of scanning your digital presence before someone else does and fixing exposed credentials, unsecured code, or metadata that attackers could exploit.
Understanding what OSINT is forms the foundation, but how exactly is open source intelligence leveraged practically in cybersecurity? Let's explore how OSINT is actively used to detect threats, prevent cyberattacks, and strengthen your organization's defense strategies.
What is Open Source Intelligence?
OSINT is the process of collecting and analyzing publicly available data from sources like websites, forums, code repositories, DNS records, metadata, and social media to generate threat intelligence.
OSINT platforms continuously monitor for signs such as domain mentions or login leaks to detect intrusions, malware activity, and other threats. This helps organizations strengthen their defences, investigate incidents, and receive early warnings of cyber


Wapiti vulnerability report
Target: http://testphp.vulnweb.com
Wapiti


Wayback Machine OSINT Tool


Government of Pakistan
Finance Division
Vision
Mission
Key Objectives
News & Events


Blockchain.com
Home
Prices
Charts
NFTs
DeFi
Academy
News
Developers
Wallet
Exchange
Bitcoin
Ethereum
Bitcoin Cash
English
"There is no way for the software to automatically know if one chain is better than another except by the greatest proof-of-work. In the design it was..."
The only crypto wallet you'll ever need.
Buy, sell, trade,
Prices
Bitcoin
Ethereum
XRP
BNB
Solana
TRON
Lido Staked Ether
Dogecoin
Figure Heloc
Cardano
Latest Transactions
Bitcoin Cash


Blockchain.com
Home
Prices
Charts
NFTs
DeFi
Academy
News
Developers
Wallet
Exchange
Bitcoin
Ethereum
Bitcoin Cash
English
Sign In
USD
Bitcoin Transaction
Hash ID
Amount
Fee
From
To
Pending
Summary
Advanced Details
Hash
Age
Input Value
Fee
Fee/VB
Weight
Coinbase
RBF
Version
Time
Inputs
Outputs
Output Value
Fee/B
Size
Weight Unit
Witness
Locktime
BTC Price
Overview
JSON
From
To