ADVANCED OSINT

Techniques to reveal hidden data

Unveiling Organization's Infrastructure

Author

Nekelash Prabhu

Advanced OSINT Techniques: Unveiling Organization’s Infrastructure.

Author : Nekelash IL

OSINT involves the gathering, examination, and distribution of intelligence sourced from publicly accessible materials. These can encompass resources like news pieces, social media updates, governmental publications, and internet discussion boards. For deep osint method, we can perform the following step to **uncover the details of the organization**

Techniques:

1. Certificate Transparency Hunting
2. Passive DNS & Subdomain Enumeration
3. Employee Footprint Mapping (Human OSINT)
4. Metadata Extraction
5. Public Breach Data Correlation
6. Job Post & Vendor Enumeration, Code Repository Analysis
7. Shodan & Censys Scanning (Passive Recon)
8. Code Leak OSINT
9. Email Header & Tracking Pixel Analysis
10. Behavioral Time Pattern OSINT

1. Certificate Transparency Hunting

Certificate Transparency (CT) Hunting can be used for advanced exploitation by identifying vulnerabilities in a target's digital infrastructure.This approach allows for the manipulation of trust systems, undermining security defenses and gaining unauthorized access to sensitive information.

Tools: crt.sh, Censys, Google CT logs, Let’s Encrypt

Steps to perform:

- ✓ Scans for wildcard certs like `*.corp.hiddenorg.com`
- ✓ Discovers dev, staging, and internal domains
- ✓ Example: `api.dev.hiddenorg.internal` exposed via Let’s Encrypt cert

Reference :

- https://www.youtube.com/watch?v=cvGFTuZ2TRo
- https://www.youtube.com/watch?v=siELBLVW5cU

Use: Maps internal infra names without DNS brute-forcing

2. Passive DNS & Subdomain Enumeration

This method involves collecting DNS records to gather information about domains, subdomains, and their associated IP addresses without directly interacting with the target.It can unintentionally reveal sensitive internal network information, aiding attackers in gaining insights into an organization’ s structure or identifying weak points for further exploitation.

Tools: DNSDumpster, PassiveTotal, SecurityTrails

Steps to perform:

✓ Maps external footprint: `vpn.hiddenorg.com`, `ci.hiddenorg.com`

✓ Uses CDN and SSL cert clues to link assets across providers

Use: Identify hidden assets & pivot points

3. Employee Footprint Mapping (Human OSINT)

This technique to automate the process of mining vast amounts of personal data about employees, correlating information across platforms to target specific individuals with high precision, potentially leading to **identity theft**, data breaches, or even physical security risks.

Tools: LinkedIn, GitHub, Reddit, Twitter, OSINT Framework

Steps to perform:

✓ Scrapes LinkedIn job titles, certs, endorsements

✓ Correlates GitHub commits to internal devs

✓ Finds usernames reused across forums

Use: Build organized chart + target social engineering campaigns

4. Metadata Extraction

Metadata Extraction is often more immediately useful for uncovering hidden, sensitive details that are directly tied to an individual, location, or organization. Metadata can expose sensitive information that might be unintentionally included in a file, such as internal version numbers, usernames, or even geolocation coordinates.

Tools: ExifTool, Metagoofil,FOCA (Fingerprinting Organizations with Collected Archives)

Steps to perform:

- ✓ Use tools like **ExifTool**, **Metagoofil**, and **FOCA** to automatically extract metadata from large volumes of publicly available files
- ✓ Correlates extracted metadata across multiple sources
- ✓ Search for critical, often-overlooked details such as version numbers of outdated software, internal file directories, or references to unprotected systems.
- ✓ Map the sensitive details (e.g., knowing an employee's role and the software they use), it can craft highly personalized spear-phishing messages or targeted social engineering schemes.

Use: Reveal internal usernames and file structures.

5. Public Breach Data Correlation

When a data breach occurs, attackers or researchers can gain access to sensitive data such as usernames, email addresses, passwords, and other personal or organizational details. This data often becomes publicly available through breach databases, forums, or dark web marketplaces.

Tools: HaveIBeenPwned, Dehashed, Intelligence X, BreachCompilation

Steps to perform:

- ✓ Searches for email leaks
- ✓ Identifies internal naming conventions and login patterns

- ✓ look for patterns in the breached data that indicate other weaknesses within the target organization
- ✓ Using **credential stuffing**, attackers test breached login data on multiple platforms

Use: Extract valid user accounts and passwords for later phishing

6. Job Post & Vendor Enumeration

Identifying an organization ' s **job postings** and **vendor relationships** to gather valuable information about its structure, technology stack, and operational vulnerabilities.

Tools : Google Dorks, Indeed, Glassdoor

Steps to perform:

- ✓ Scans for job posts with tech stack leaks: "SIEM, EDR, AWS, Terraform"
- ✓ Scrapes Glassdoor for interview process or tool mentions.
- ✓ Maps supply chain vendors from employee reviews.

Use: Reverse-engineer internal architecture

7. Shodan & Censys Scanning (Passive Recon)

Shodan & Censys Scanning (Passive Recon) is a method used in OSINT to gather information about an organization's exposed infrastructure.

Tools: Shodan.io, Censys.io

Steps to perform:

- ✓ Searches for exposed assets with matching TLS certs or unique ports
- ✓ Finds misconfigured dev tools, forgotten admin panels
- ✓ Shodan and Censys also provide detailed geolocation information for devices and services, as well as associated domain names and

IP ranges. This helps to understand how the organization’s infrastructure is distributed

Use: Build attack surface without touching target

8. Code Leak OSINT

Code Leak OSINT is a technique used to gather valuable insights from leaked source code, repositories, or development environments. Use advanced Google or GitHub dorking queries to infiltrate an organization, you can take inspiration from real-world techniques, but make them more powerful or unique.

Tools: GitHub Dorks, Google Dorks

Steps to perform:

✓ Dorks for secrets: `filename:.env password`, `AWS_SECRET=`
✓ Finds internal docs, .git folders, config files

Examples of Google Dork queries:

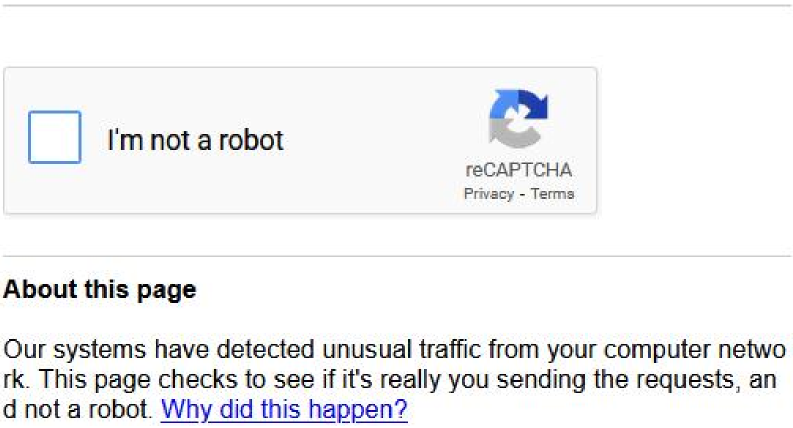
✧ site:<companyname.com> filetype:pdf inurl:confidential
✧ intitle:″admin login″ inurl:admin
✧ “aws_secret_access_key″ in:file extension:yaml
✧ site:s3.amazonaws.com inurl:″/public/″ -github.com
✧ filetype:env ″DB_PASSWORD″ -github.com
✧ ″DB_LOG″ ″ERROR″ in:file extension:log

Examples of Github Dork queries:

✧ filetype:yaml ″cloud_config″ site:github.com
✧ filetype:yml ″secrets″ site:github.com
✧ filetype:py ″os.system″ site:github.com

Try these also:

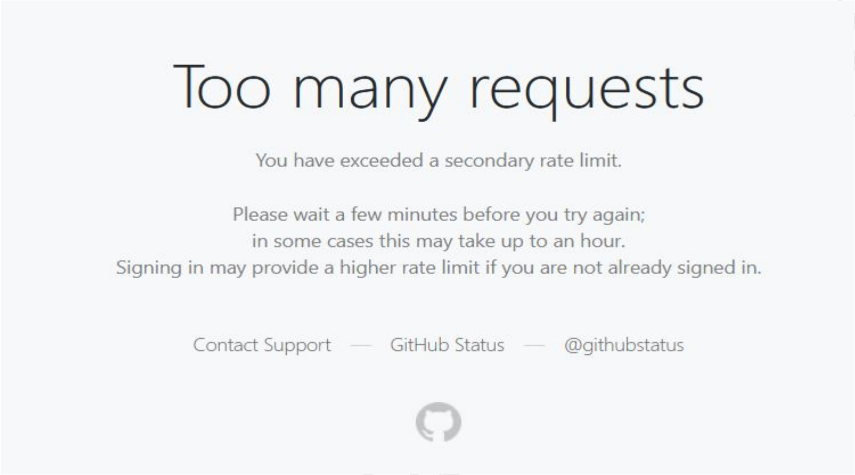
✧ https://gist.github.com/win3zz/0a1c70589fcbea64dba4588b93095855
✧ https://buckets.grayhatwarfare.com/
(must try, just type **“aadhar”** in search !!MAGIC!!)



□ I'm not a robot

About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. Why did this happen?



Too many requests

You have exceeded a secondary rate limit.

Please wait a few minutes before you try again;
in some cases this may take up to an hour.
Signing in may provide a higher rate limit if you are not already signed in.

You will get this often in dorking (Just a normal thing)

Use: Capture credentials, internal URLs, debug logs

9. Email Header & Tracking Pixel Analysis

Use **email header analysis** not just for basic information, but to **aggregate, cross-reference, and map out complex networks** of communication. **Tracking pixel analysis** can be used to monitor if the recipient clicks on a link, downloads an attachment, or even forwards the email to others. It could then use this data to predict future behaviors.

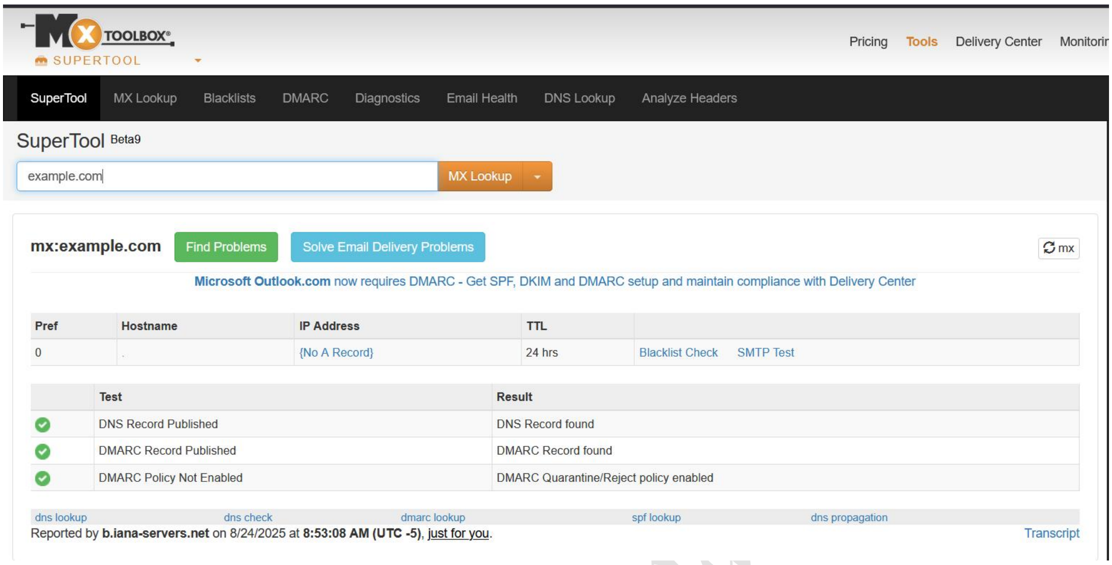
Tools:

Email header analysis [Custom parser, mxtoolbox.com, email-parser,…]

Tracking pixel analysis [pastepixel.com, collinsmc23/spy-pixel,…]

Steps to perform:

- ✓ Parses headers from any leaked or intercepted email
- ✓ Extracts internal relay IPs, mail server names, time zones



mx:example.com

Microsoft Outlook.com now requires DMARC - Get SPF, DKIM and DMARC setup and maintain compliance with Delivery Center

Pref	Hostname	IP Address	TTL	
0	.	{No A Record}	24 hrs	Blacklist Check SMTP Test

	Test	Result
✓	DNS Record Published	DNS Record found
✓	DMARC Record Published	DMARC Record found
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled

dns lookup dns check dmarc lookup spf lookup dns propagation

Reported by **b.iana-servers.net** on 8/24/2025 at **8:53:08 AM (UTC -5)**, just for you. Transcript

Above img. show how mxtoolbox is used to trace the route of email from orgn. to rev.

Use: Trace back infra and identify internal routing logic

10. **Behavioral Time Pattern OSINT**

Behavioral Time Pattern OSINT includes **email interactions, digital calendar activities, social media behavior**, and even subtle actions like the times they **access certain files** or **log into specific systems.**

Tools: Web activity logs, social posts, push timing, shodan, maltego

Steps to perform:

- ✓ Analyzes when users post, commit, or comment
- ✓ Maps org working hours, shift overlap, devops cycle

Use: Predict internal behavior and schedule phishing/social engineering

By using **OSINT**, we can **infiltrate, manipulate**, and **ultimately take over** an organization by exploiting human weaknesses and predicting behaviors with high precision.

OSINT is a stealthy but incredibly powerful tool that turns the organization’s own information against it. OSINT becomes the **first phase** in a **multi-layered hacking strategy**—leading to widespread **chaos**, **paralysis**, and **eventual collapse** of the organization’s resilience piece by piece.