Experiment No. 2a

Title: Passive Reconnaissance with OSINT tools

Batch: SY-IT(B3) **Roll No.:16010423076** **Experiment No.: 2a**

Aim: To understand and perform Passive Reconnaissance with OSINT tools

Resources needed: Internet access

Theory:

What is Reconnaissance?

Reconnaissance is gathering information on the target to perform a sophisticated attack later. Without recon, the attacker/pen tester will have no idea where to begin and randomly brute-force their way through multiple tools (like how a script kiddie would), which will most likely get them thrown out of the network.

What is Passive Recon?

The term passive means one does not take action. But in this context, Passive Reconnaissance means collecting information on the target without the target knowing anything about it.

Example: include searching on Google or using various tools that gather publicly available information about the target and to know about it.

What information could be gathered?

Different tools will provide different kinds of information. But broadly, passive recon will allow you to gather the following information.

- Domain Names
- IP Addresses
- Technologies
- DNS Records
- Subdomains
- Unlisted Files

Procedure:

1. Write a case study describing which information to be gathered. Refer the following example:

Target Organization : Perplexity AI

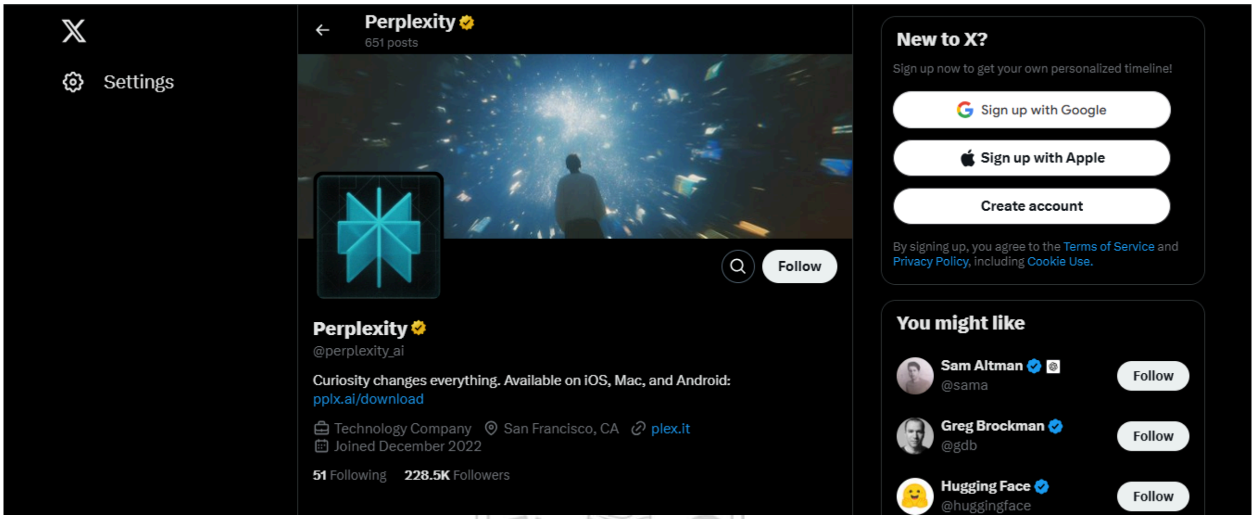
Twitter / X

Content posted - Updates, Game schedules, latest news related to the development of perplexity, Posts of founder

Frequency & timings of posts - 1 post per week

Tone and Language - Informative, casual

Common hashtags & Keywords - #perplexitysports #liveupdates



Perplexity
@perplexity_ai

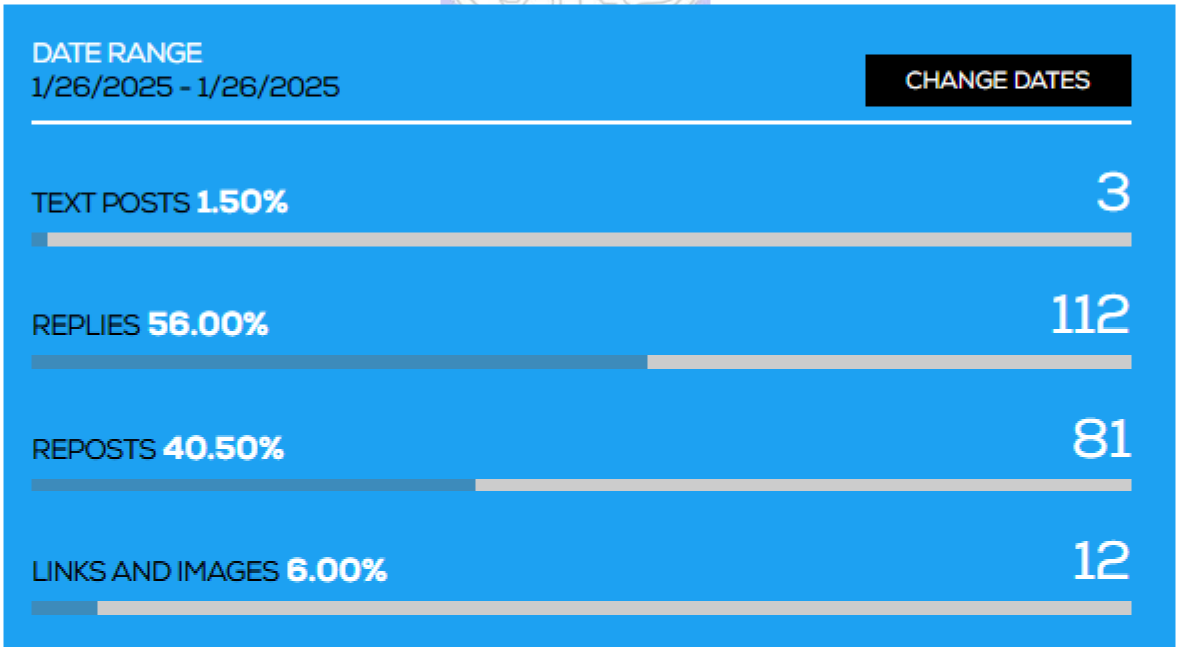
Curiosity changes everything. Available on iOS, Mac, and Android: pplx.ai/download

Technology Company San Francisco, CA plex.it
Joined December 2022

51 Following 228.5K Followers

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use.

Twitter Stats



DATE RANGE
1/26/2025 - 1/26/2025

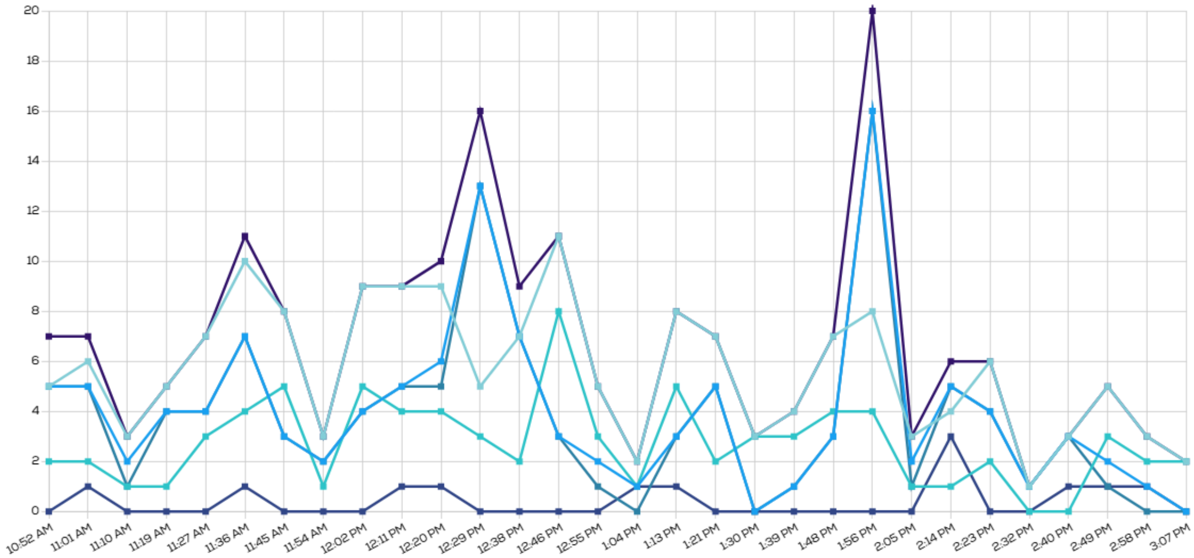
TEXT POSTS 1.50% 3

REPLIES 56.00% 112

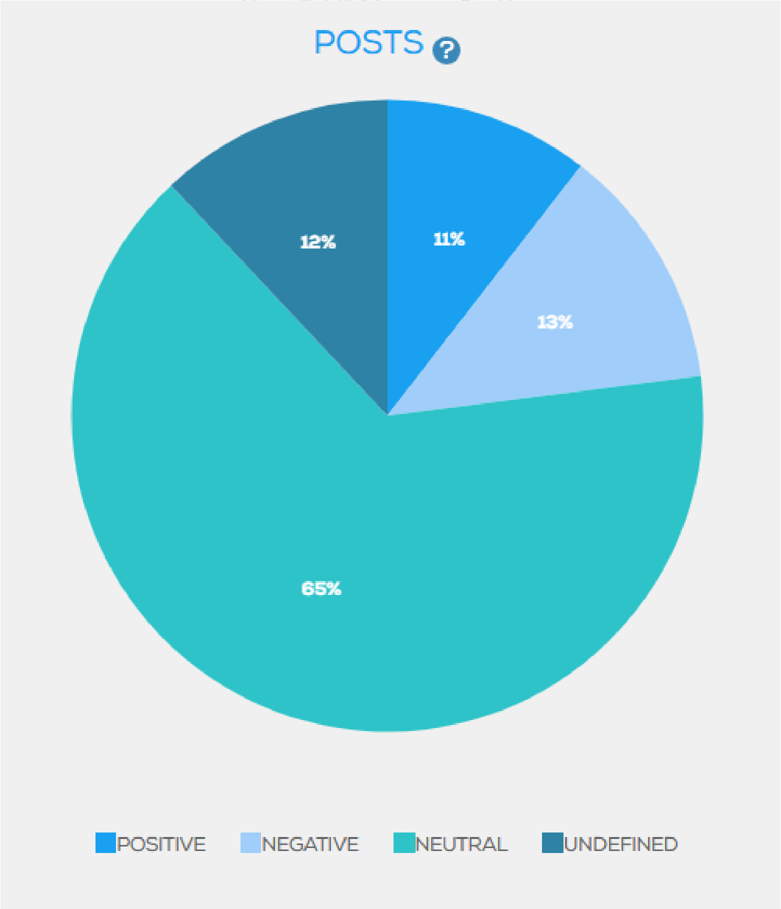
REPOSTS 40.50% 81

LINKS AND IMAGES 6.00% 12

Tweet timings

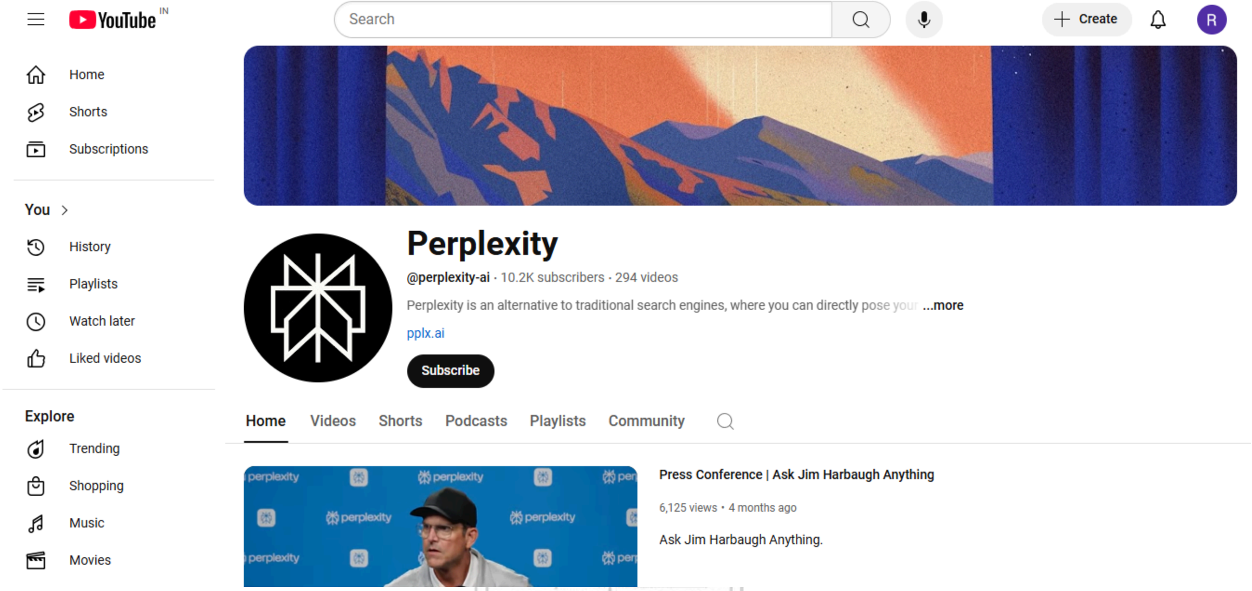


Sentiment Analysis of Tweets :



Youtube

Content posted - Discover daily, Tutorials and guides on using AI
Frequency & timings of posts - Atleast 1 video everyday
Tone and Language - Educational
Common hashtags & Keywords - discover daily, AI, search

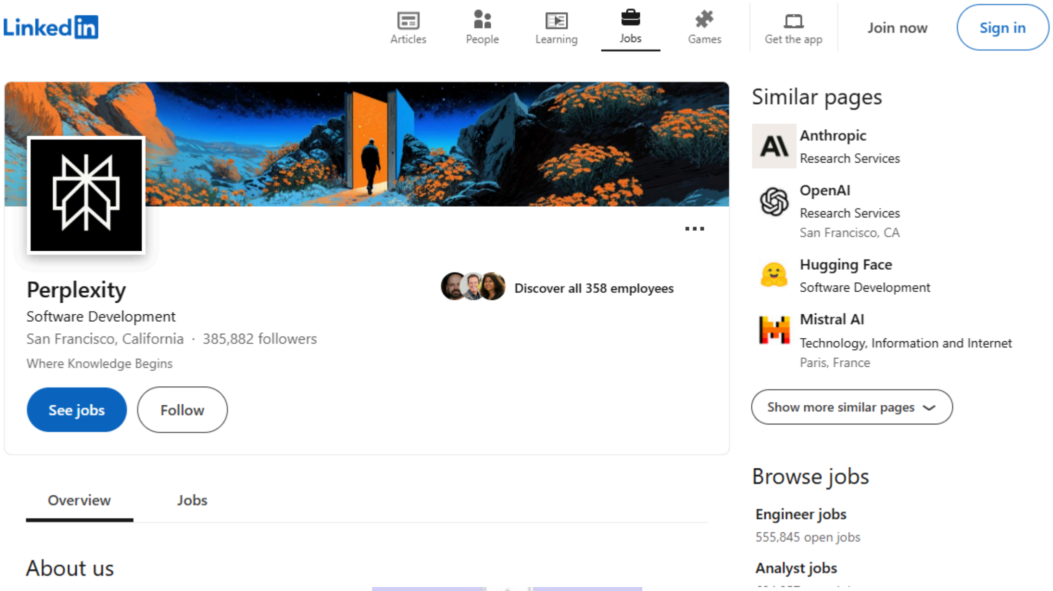


Perplexity
@perplexity-ai · 10.2K subscribers · 294 videos
Perplexity is an alternative to traditional search engines, where you can directly pose your ...more
pplx.ai

Press Conference | Ask Jim Harbaugh Anything
6,125 views • 4 months ago
Ask Jim Harbaugh Anything.

Linkedin

Content posted - Company updates, product updates, announcements
Frequency & timings of posts - 2 posts per month
Tone and Language - Professional, aspirational
Common hashtags & Keywords - #TechInnovation, #PerplexityAI



Perplexity
Software Development
San Francisco, California · 385,882 followers
Where Knowledge Begins

Discover all 358 employees

About us

Similar pages

Anthropic
Research Services

OpenAI
Research Services
San Francisco, CA

Hugging Face
Software Development

Mistral AI
Technology, Information and Internet
Paris, France

Browse jobs

Engineer jobs
555,845 open jobs

Analyst jobs

Based on the content, tone, hashtags, and frequency, what marketing strategies can you infer?

- Leveraging real-time engagement to connect with users during live events.
- Providing educational content to enhance user understanding and adoption.
- Highlighting product developments to attract potential clients and partners.

Who is the company targeting (age group, interests, demographic)?

- Individuals interested in AI tools and looking for guidance on usage
- Industry professionals, potential business partners, and clients interested in AI innovations
- Sports enthusiasts seeking real-time updates.

Based on your analysis, identify potential cybersecurity risks and attacks the company may face from its social media presence.

- Impersonation attacks through fake profiles.
- Phishing attempts via malicious links in comments or posts.
- Data scraping from public posts leading to information leakage.
- Corporate espionage through fake profiles attempting to connect with employees.

Referring to identified potential cybersecurity risks and attacks, discuss one scenario about how attackers could exploit the company's public interactions.

1) An attacker could create a counterfeit LinkedIn profile mimicking a high-ranking Perplexity AI executive. By sending connection requests to employees they might solicit sensitive company information or distribute malicious links leading to data breaches or network compromises.

2) Attackers could create a fake Perplexity AI support profile on Twitter, responding to user inquiries with malicious links. Unsuspecting users might click on these links leading to credential theft or malware installation.

Passive Reconnaissance to find crucial information :

Domain Name

https://www.perplexity.ai/

WHOIS Data

```
Domain Name: perplexity.ai
Registry Domain ID: 312544b477a245559d0aa243e1fe27f7-DONUTS
Registrar WHOIS Server: whois.1api.net
Registrar URL: http://www.1api.net
Updated Date: 2025-01-22T00:54:17Z
Creation Date: 2022-07-08T20:44:58Z
Registry Expiry Date: 2034-07-08T20:44:58Z
Registrar: 1API GmbH
Registrar IANA ID: 1387
Registrar Abuse Contact Email: abuse@1api.net
Registrar Abuse Contact Phone: +49.68949396850
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: 64e95453d34644ec9cfa461a6733bcda-DONUTS
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com, 100 S. Mill Ave, Suite 1600
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85281
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax:
```

```
Registrant Fax Ext:
Registrant Email: perplexity.ai@domainsbyproxy.com
Registry Admin ID: 2bd22c71f22e4d6486d47cd496a17a87-DONUTS
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com, 100 S. Mill Ave, Suite 1600
Admin City: Tempe
Admin State/Province: Arizona
Admin Postal Code: 85281
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: perplexity.ai@domainsbyproxy.com
Registry Tech ID: 3b9de2b6e5be49a7a7d9b60f01314414-DONUTS
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com, 100 S. Mill Ave, Suite 1600
Tech City: Tempe
Tech State/Province: Arizona
Tech Postal Code: 85281
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: perplexity.ai@domainsbyproxy.com
Name Server: jessica.ns.cloudflare.com
Name Server: emerson.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

DNS Records :

Type	Domain Name	TTL	Address	Owner	ASN
A	www.perplexity.ai	300	104.18.26.48	CloudFlare Inc., United States	AS13335
A	www.perplexity.ai	300	104.18.27.48	CloudFlare Inc., United States	AS13335

AAAA	www.perplexity.ai	300	2606:4700::6812:1b30	CloudFlare Inc., United States	-
AAAA	www.perplexity.ai	300	2606:4700::6812:1a30	CloudFlare Inc., United States	-

Source code of their PC app :
https://github.com/inulute/perplexity-ai-app

Additional information :
Support Email: support@perplexity.ai
Employee Emails: firstname@perplexity.ai (49%), firstnameL@perplexity.ai (1%)
HQ Address: 341 Moultrie St, San Francisco, California 94110, US
Decision Makers: Aravind Srinivas, Denis Yarats, Emily Jorgens

Outcomes:

CO1: Realize that premise of vulnerability analysis and penetration testing (VAPT).

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

From this experiment, I learned how to perform passive reconnaissance using OSINT tools to gather crucial information about a target organization like Perplexity AI. By analyzing domain details, DNS records, social media presence, and publicly available data, I understood how attackers or security professionals can collect valuable insights without alerting the target. This exercise highlighted the importance of understanding cybersecurity risks such as phishing, impersonation, and data leakage that can arise from publicly shared information

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

References:

https://osintframework.com/

▶ **What is Passive Reconnaissance?**