[Utility Provider] Penetration Test Phase 1: Reconnaissance

Nathan Tendido
Cybersecurity Career Track, Springboard
Penetration Test Capstone
August 13, 2023

Phase 1 Introduction

In order to conduct a thorough penetration test and at the request of the client, [Utility Provider], penetration test activities will be performed from an external perspective. Contextual information should not be provided by the client to the tester at any point. Information used for testing activities will be solely based on intelligence gathered through publicly available information. By using only publicly available information, the tester is able to build a perspective similar to a potential external threat actor.

Objective

- Build a robust external perspective profile of [Utility Provider]'s business structure, processes, employees, network, and technology stack using only publicly available information

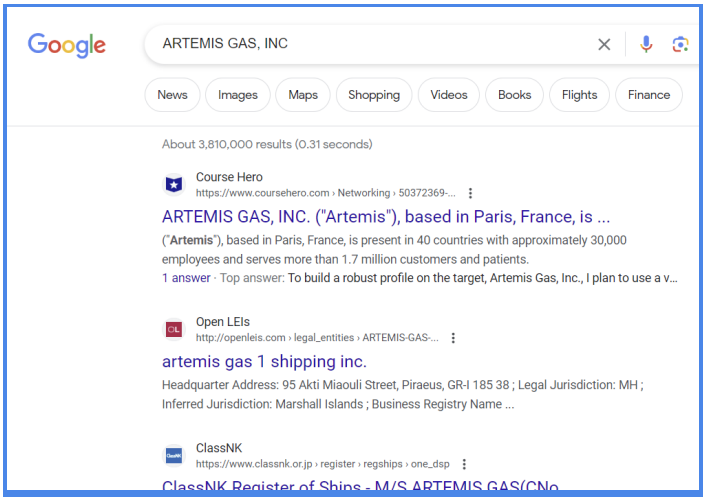
OSINT Testing tools and techniques to be used are:

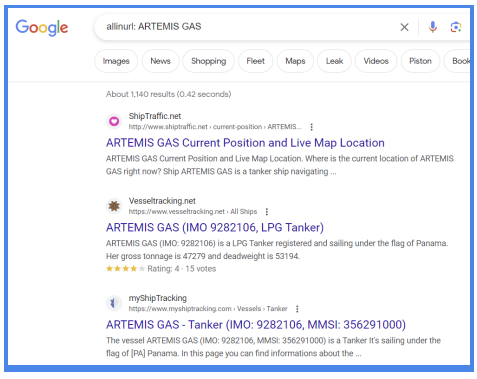
1. Google & Google Dorks *(Search Engine and Advanced Techniques)*
2. theHarvester*(Automated OSINT Frameworks)*
3. Recon-ng *(Automated OSINT Frameworks)*
4. Maltego *(Link Analysis and Data Visualization)*
5. Business Info Sources: OpenCorporates, D&B, CorporationWiki *(Domain and Web Intelligence)*
6. Social Media Sources: Facebook, Instagram *(Online Presence and Social Media)*
7. Employment Resources: LinkedIn, Glassdoor *(Online Presence and Social Media)*
8. VoilaNorbert *(Email and Contact Gathering)*
9. Shodan *(Internet Scanning and Enumeration)*
10. SecurityTrails by Recorded Future *(Internet Scanning and Enumeration)*
11. Builtwith *(Internet Scanning and Enumeration)*
12. PassiveDNS by Mnemonic *(DNS and Domain)*
13. DNSDumpster *(DNS and Domain)*
14. DNSlytics *(DNS and Domain)*

Google & Google Dorks

Search Engine and Advanced Search Techniques

Source	• https://gist.github.com/sundowndev/283efaddbcf896ab405488330d1bbc06 • https://hackr.io/blog/google-dorks-cheat-sheet • https://www.exploit-db.com/google-hacking-database
Objective	Perform basic searches as a starting point, and then use Google Dorking techniques to find additional hidden relevant information which is typically hidden in code, scripts, filenames, headers, metadata, etc. Care should be taken as to not access legally restricted or private information without explicit and documented approved permission.
Required Inputs	Company name, other related parameters. Google Dorking requires specific parameters included with search query.

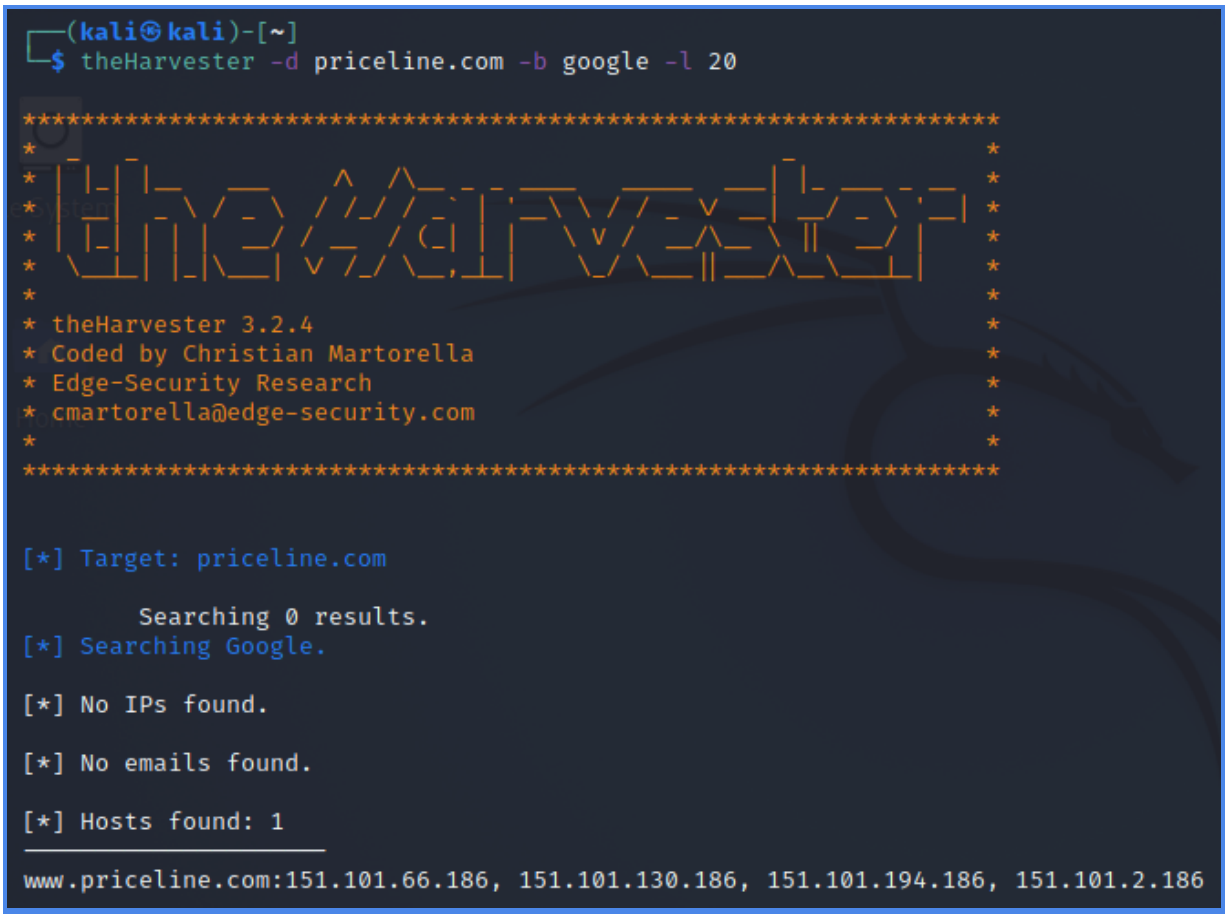




theHarvester

Automated OSINT Frameworks

Source	• https://www.kali.org/tools/theharvester/ • https://github.com/laramies/theHarvester
Objective	Perform an automated gathering of email addresses, subdomains, and virtual hosts from online sources.
Required Inputs	Domain OR Company name



Recon-ng

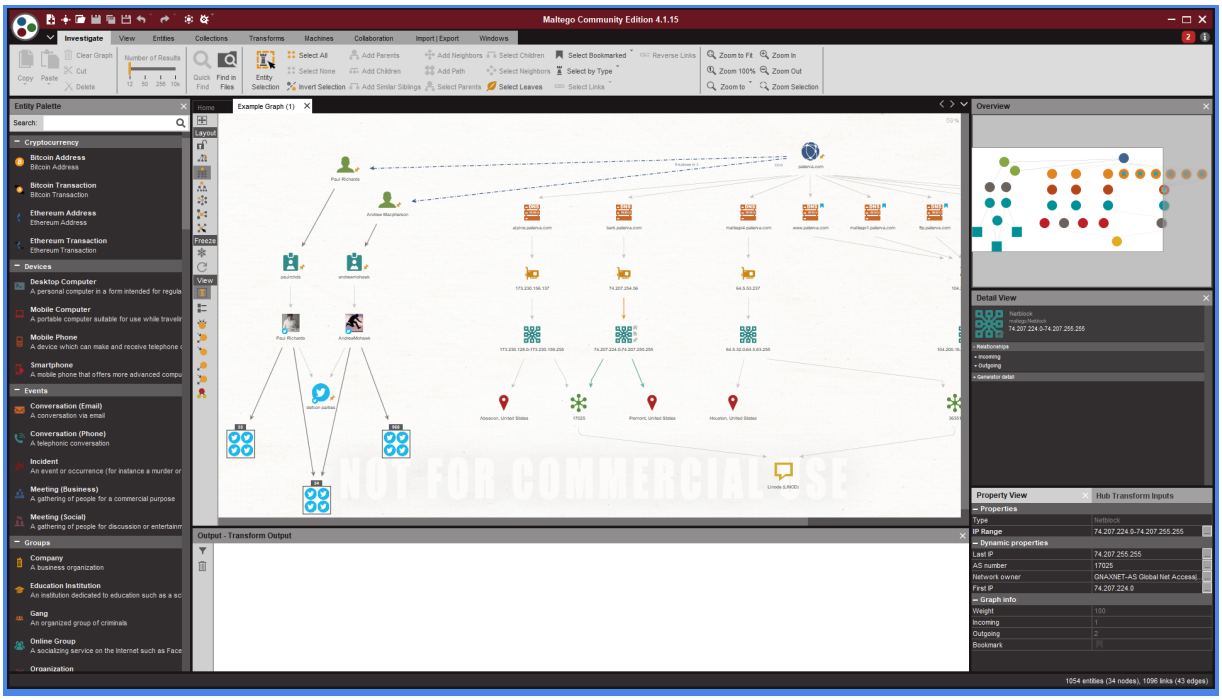
Automated OSINT Frameworks

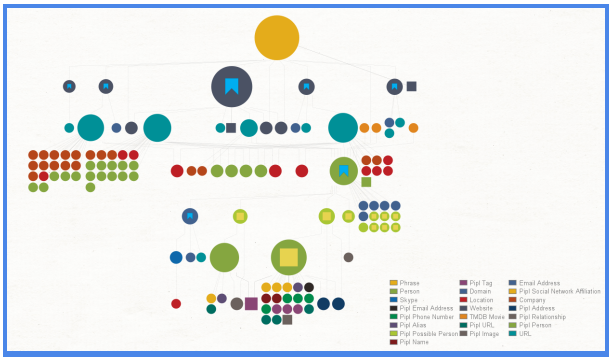
Source	• https://github.com/lanmaster53/recon-ng • https://www.kali.org/tools/recon-ng/
Objective	Perform automated intelligence gathering from various online sources.
Required Inputs	1. Create workspace 2. Select and load search module from module list 3. Set options and target 4. Run Recon-ng 5. Show results for review

Maltego

Link Analysis and Data Visualization

Source	• https://www.maltego.com/ • https://www.kali.org/tools/maltego/
Objective	Create a visualization to identify, map, and understand the target's online profile and relationship between public links.
Required Inputs	Domain name should be used for start, and additional queries can be run or manually added with other information gathered during Phase 1 (such as officer names, email addresses, subdomains, IP addresses, etc)

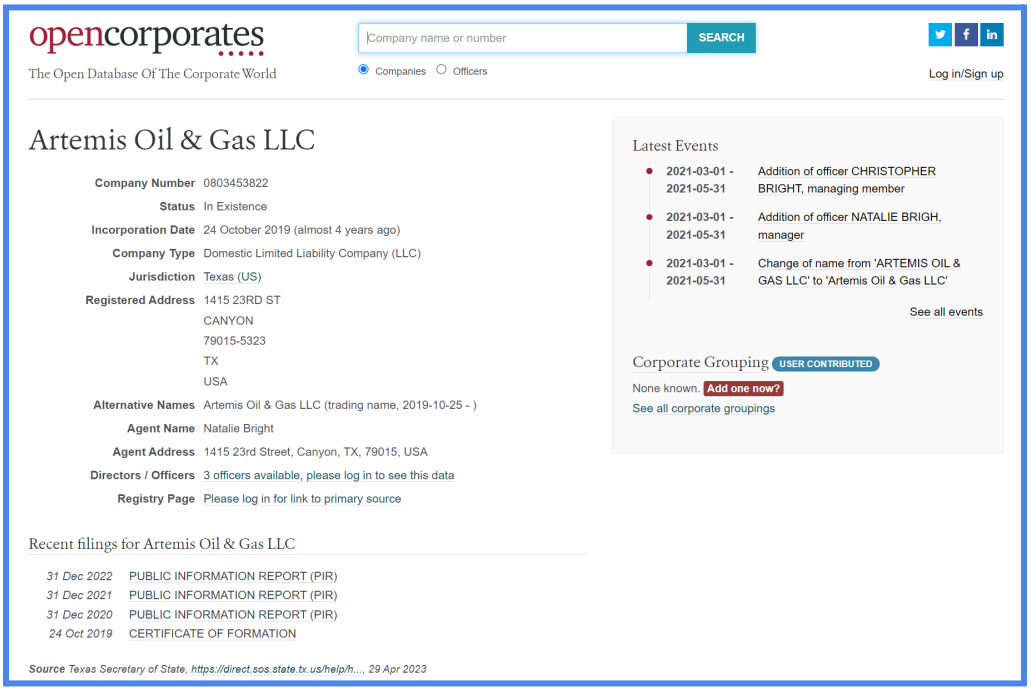


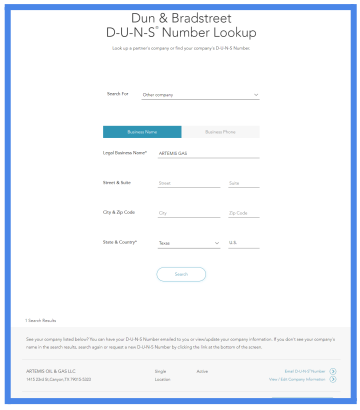


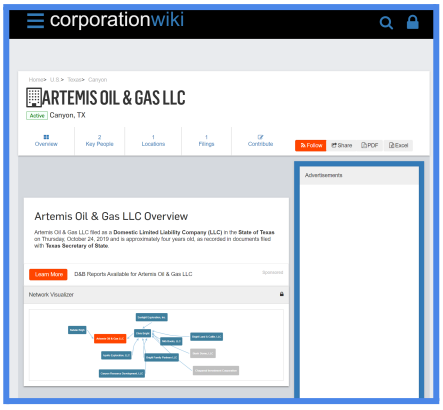
Business Info Sources (OpenCorporates, D&B, CorporationWiki)

Domain and Web Intelligence

Source	• https://opencorporates.com/ • https://www.dnb.com/duns-number/lookup.html • https://www.corporationwiki.com/
Objective	Gather domain and business information, including ownership, financial, affiliate, officer, significant events, etc. for use as input in Phase 1 tools and target gathering
Required Inputs	Business name, entity name/s, officer names



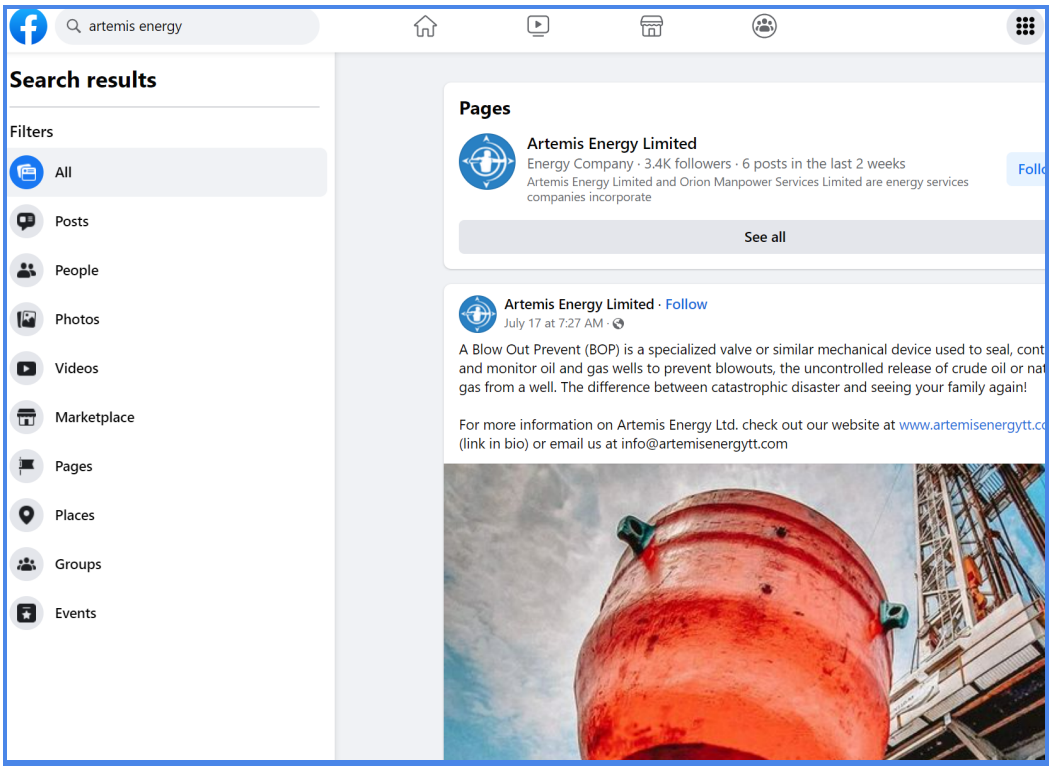


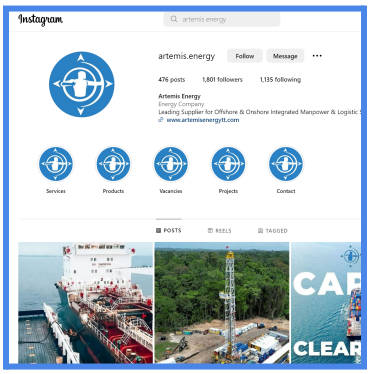


Social Media Sources (Facebook, Instagram)

Online Presence and Social Media

Source	• https://www.facebook.com/ • https://www.instagram.com/
Objective	Gather information on target's online presence on social media for use in target building and social engineering.
Required Inputs	Company name, officer name/s

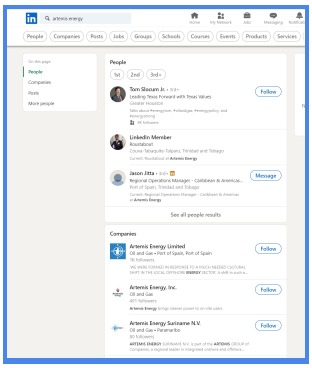


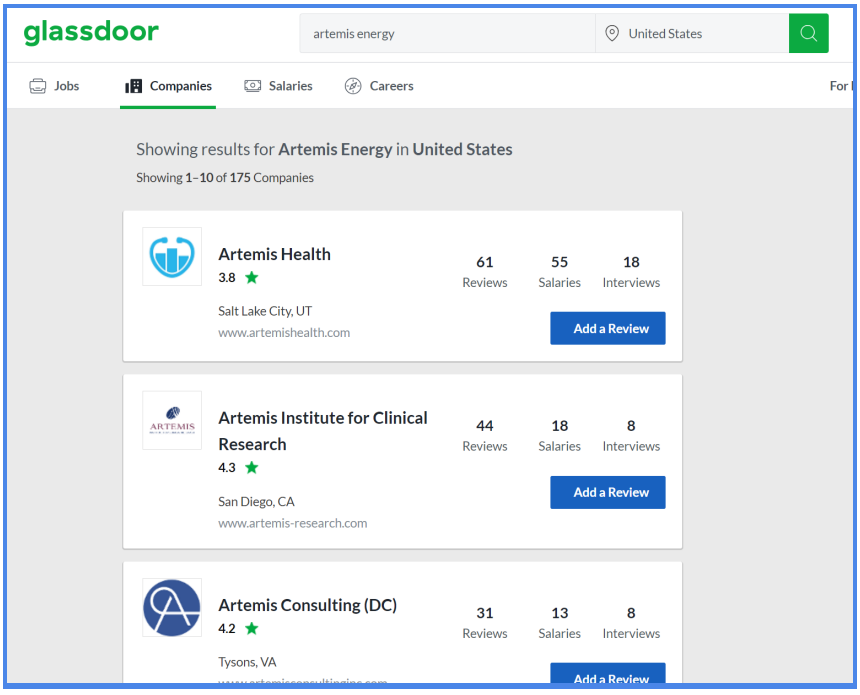


Employment Sources (LinkedIn, Glassdoor)

Online Presence and Social Media

Source	• https://www.linkedin.com/ • https://www.glassdoor.com/
Objective	Gather information on target's online presence on social media for use in target building and social engineering.
Required Inputs	Company name, officer name/s

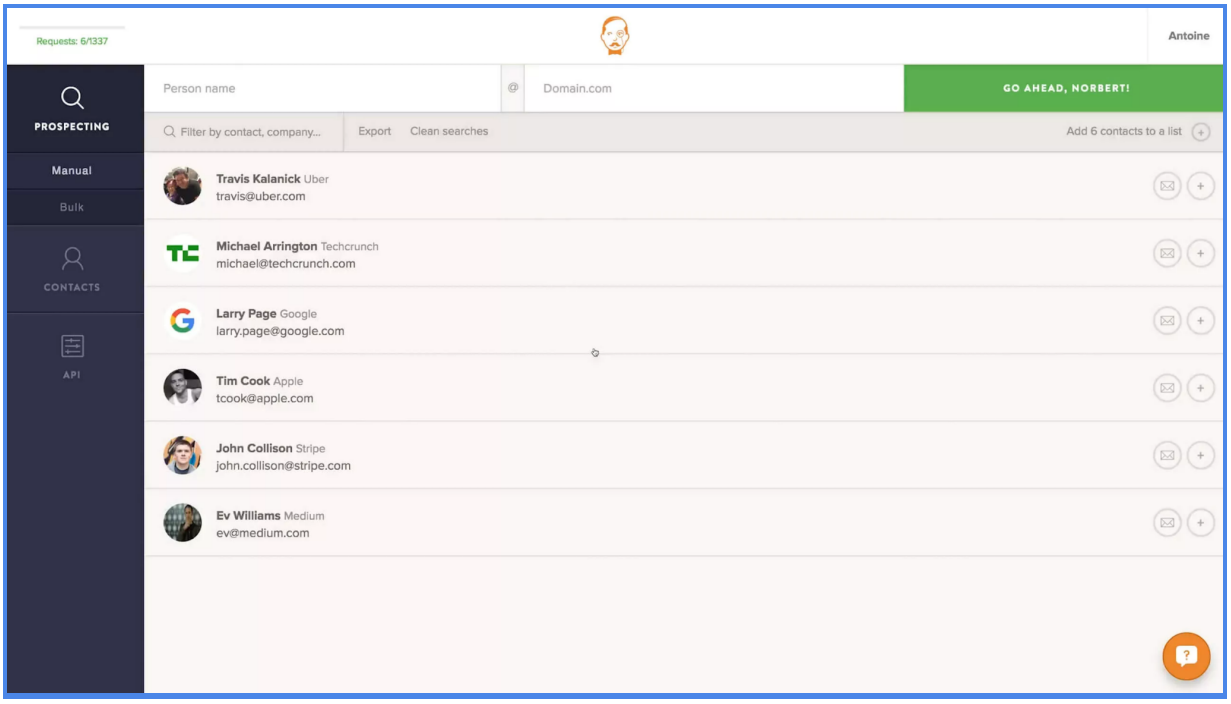




VoilaNorbert

Email and Contact Information Gathering

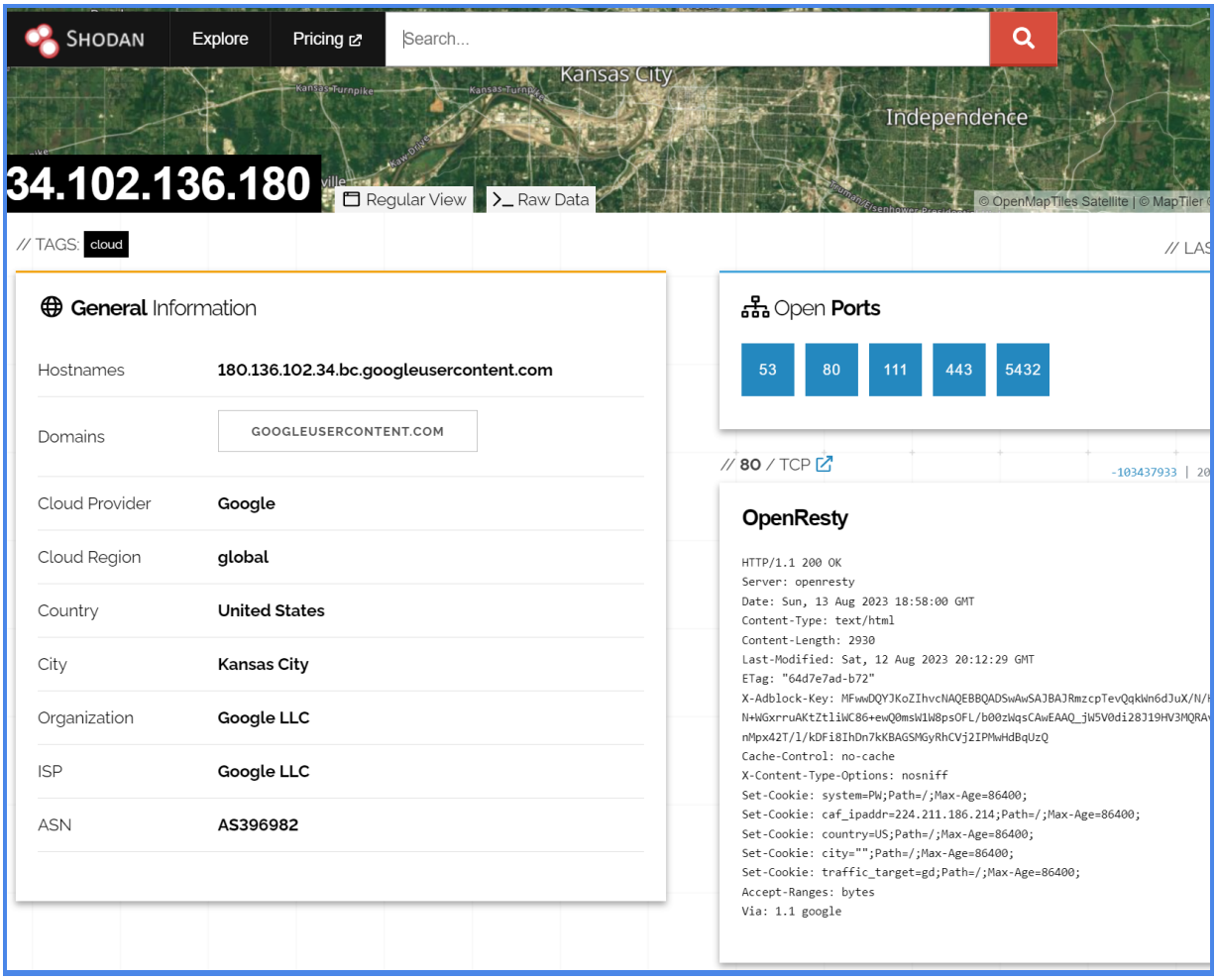
Source	• https://www.voilanorbert.com/
Objective	Gather email addresses for target building and social engineering.
Required Inputs	Target name, known email address, or domain name



Shodan

Internet Scanning and Enumeration

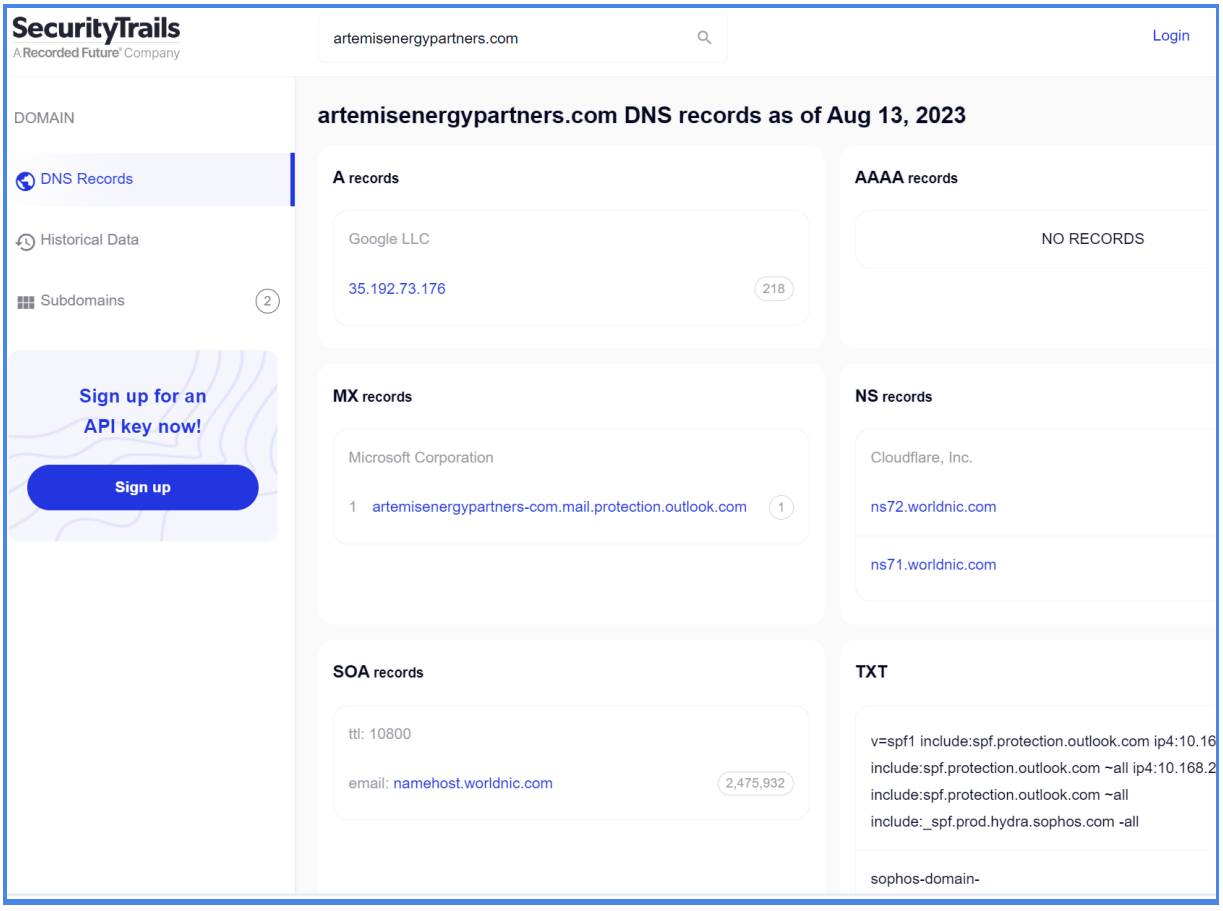
Source	• https://www.shodan.io/
Objective	Identify internet-facing devices and services.
Required Inputs	Known IP address



SecurityTrails by Recorded Future

Internet Scanning and Enumeration

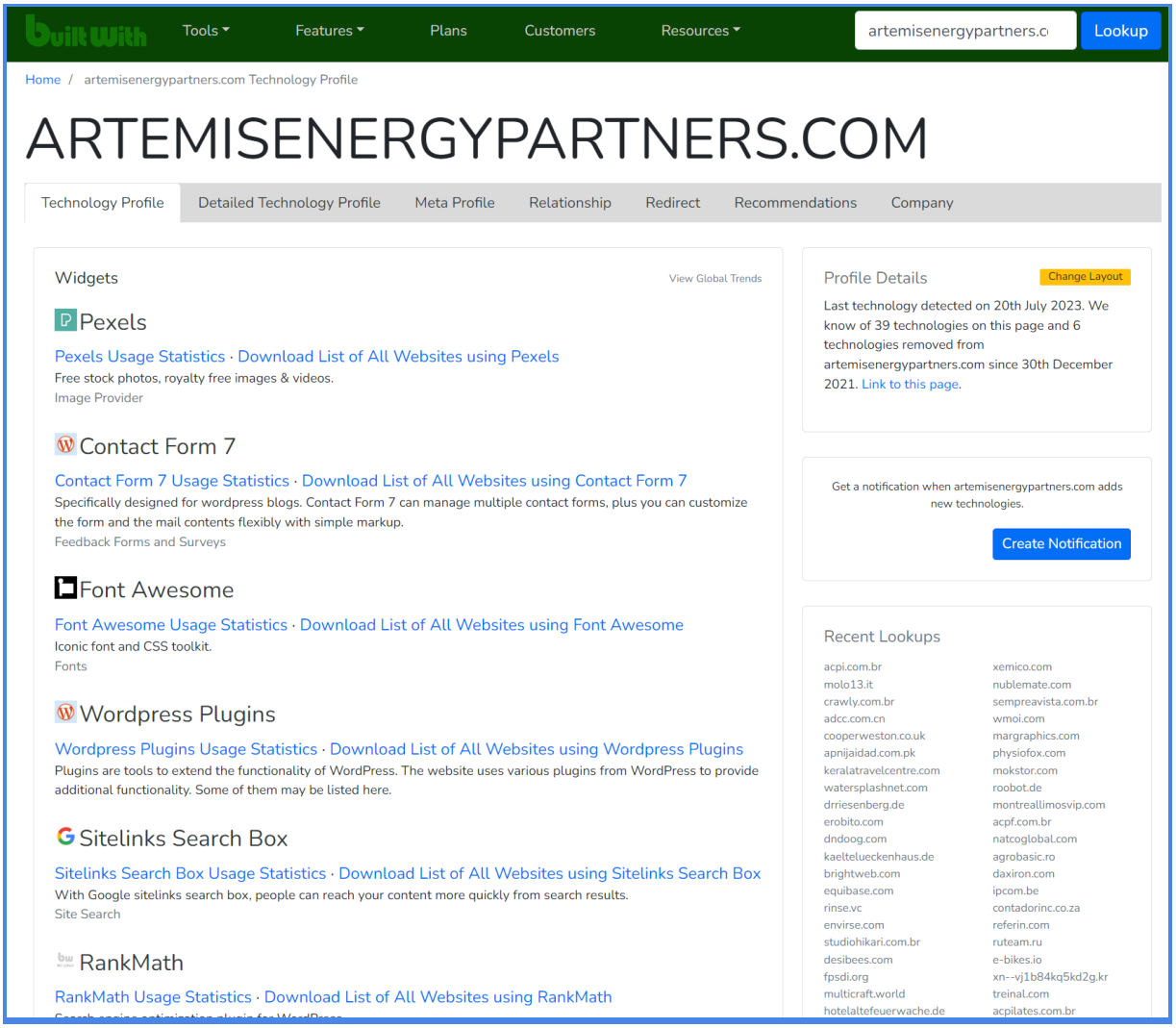
Source	• https://securitytrails.com/
Objective	Gather information on historical domain and IP information.
Required Inputs	Known domain name or IP address



Builtwith

Internet Scanning and Enumeration

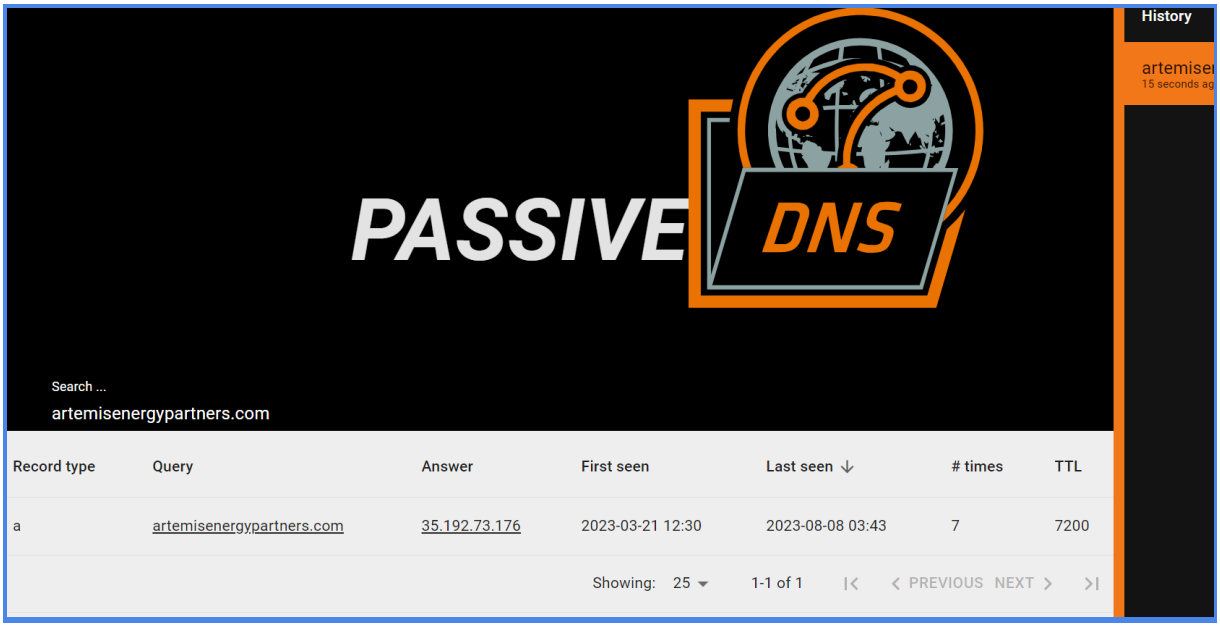
Source	• https://builtwith.com/
Objective	Analyze web technologies in use for a domain and identify technology stacks, frameworks, plugins, and tools used.
Required Inputs	Domain name or IP address



PassiveDNS by Mnemonic

DNS and Domain Information

Source	• https://passivedns.mnemonic.no/
Objective	Gather passive DNS data to build DNS history and resolution profile.
Required Inputs	Domain name or IP address



DNSDumpster

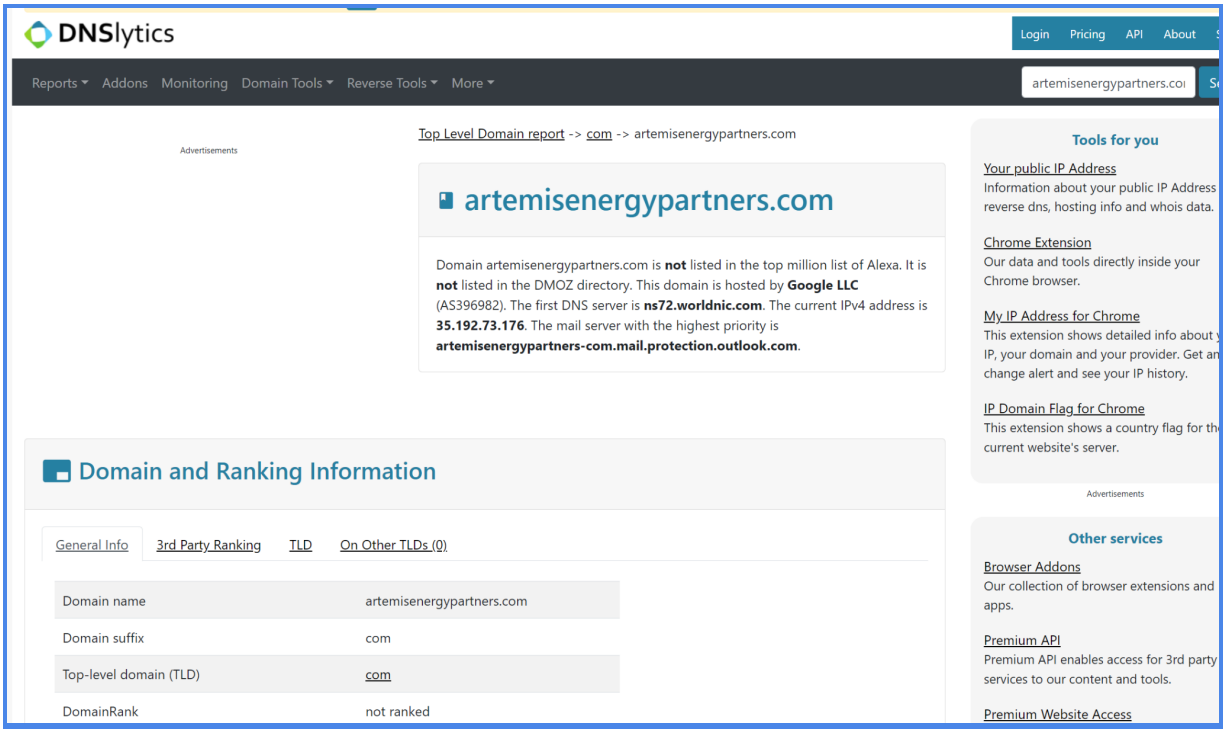
DNS and Domain Information

Source	• https://dnsdumpster.com/
Objective	Gather DNS domain and subdomain information associated with the target domain.
Required Inputs	Domain name

DNSlytics

DNS and Domain Information

Source	• https://dnslytics.com/
Objective	Gather DNS and domain information.
Required Inputs	Domain name, IPv4, or IPv6 address



Phase 1 Conclusion

Activities conducted during Phase 1 are not expected to have any major impact on client's business activities. The focus during this phase is to build a contextual profile using publicly available resources with information to be used in later testing phases.

Preparer Approval

Signature:

Name:

Date:

Client Approval

Signature:

Name:

Date: