

[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	<ul style="list-style-type: none"> • https://gist.github.com/sundowndev/283efaddbcf896ab405488330d1bbc06 • https://hackr.io/blog/google-dorks-cheat-sheet • https://www.exploit-db.com/google-hacking-database
Objective	<p>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.</p> <p>Care should be taken as to not access legally restricted or private information without explicit and documented approved permission.</p>
Required Inputs	<p>Company name, other related parameters.</p> <p>Google Dorking requires specific parameters included with search query.</p>

theHarvester

Automated OSINT Frameworks

Source	<ul style="list-style-type: none">• 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

```
(kali㉿kali)-[~]
$ theHarvester -d priceline.com -b google -l 20

*****
* [H][I][T][R][E][A][S][H][O][W][D][A][C][K][I][N][G][P][A][C][H][E][A][R][V][E][S][T][E][R][E][M][A][R][T][O][R][E][L][L][A][@][E][D][G][E][S][E][C][U][R][I][T][Y][.][C][O][M]
*
* theHarvester 3.2.4
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
[*] Target: priceline.com
      Searching 0 results.
[*] Searching Google.
[*] No IPs found.
[*] No emails found.
[*] Hosts found: 1
-----
www.priceline.com:151.101.66.186, 151.101.130.186, 151.101.194.186, 151.101.2.186
```

Recon-ng

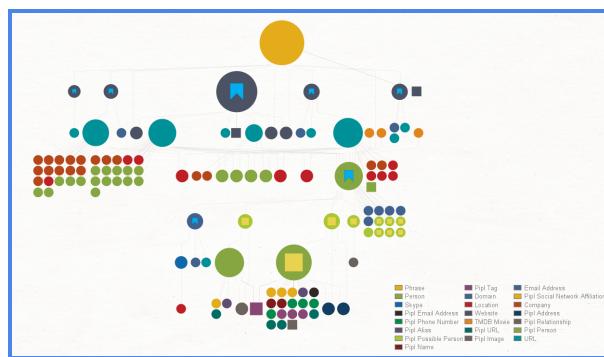
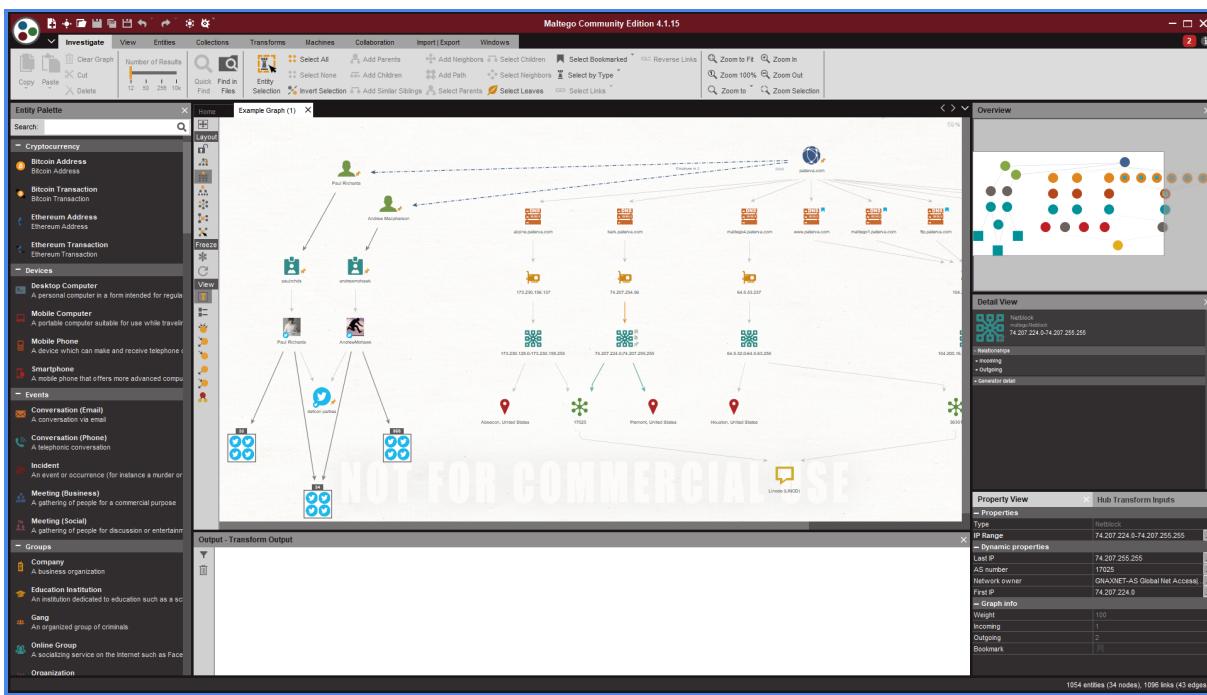
Automated OSINT Frameworks

Source	<ul style="list-style-type: none">• https://github.com/lanmaster53/recon-ng• https://www.kali.org/tools/recon-ng/
Objective	Perform automated intelligence gathering from various online sources.
Required Inputs	<ol style="list-style-type: none">1. Create workspace2. Select and load search module from module list3. Set options and target4. Run Recon-ng5. Show results for review

Maltego

Link Analysis and Data Visualization

Source	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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

The screenshot shows the OpenCorporates website interface. At the top, there's a search bar with placeholder text "Company name or number" and a "SEARCH" button. Below the search bar are buttons for "Companies" and "Officers". To the right, there are social media links for Twitter, Facebook, and LinkedIn, and a "Log in/Sign up" link.

The main content area displays the company profile for "Artemis Oil & Gas LLC". Key details include:

- Company Number:** 0803453822
- Status:** In Existence
- Incorporation Date:** 24 October 2019 (almost 4 years ago)
- Company Type:** Domestic Limited Liability Company (LLC)
- Jurisdiction:** Texas (US)
- Registered Address:** 1415 23RD ST
CANYON
79015-5323
TX
USA
- Alternative Names:** Artemis Oil & Gas LLC (trading name, 2019-10-25 -)
- Agent Name:** Natalie Bright
- Agent Address:** 1415 23rd Street, Canyon, TX, 79015, USA
- Directors / Officers:** 3 officers available, please log in to see this data
- Registry Page:** Please log in for link to primary source

On the right side, there's a "Latest Events" section listing three recent changes:

- 2021-03-01 - 2021-05-31 Addition of officer CHRISTOPHER BRIGHT, managing member
- 2021-03-01 - 2021-05-31 Addition of officer NATALIE BRIGHT, manager
- 2021-03-01 - 2021-05-31 Change of name from 'ARTEMIS OIL & GAS LLC' to 'Artemis Oil & Gas LLC'

Below the events, there are links to "See all events" and "Corporate Grouping" (USER CONTRIBUTED). It also says "None known" and "Add one now?" with a "See all corporate groupings" link.

At the bottom left, it says "Recent filings for Artemis Oil & Gas LLC" with a list of documents filed:

- 31 Dec 2022 PUBLIC INFORMATION REPORT (PIR)
- 31 Dec 2021 PUBLIC INFORMATION REPORT (PIR)
- 31 Dec 2020 PUBLIC INFORMATION REPORT (PIR)
- 24 Oct 2019 CERTIFICATE OF FORMATION

Source: Texas Secretary of State, <https://direct.sos.state.tx.us/help/#...>, 29 Apr 2023

The screenshot shows the CorporationWiki website interface. At the top, there's a search bar and a navigation menu with options like "Overview", "Key People", "Locations", "Filings", "Contributors", "Edit", "Share", "PDF", and "Excel".

The main content area displays the company profile for "ARTEMIS OIL & GAS LLC". Key details include:

- Overview:** Artemis Oil & Gas LLC filed as a Domestic Limited Liability Company (LLC) in the State of Texas on Thursday, October 24, 2019 and is approximately 3 years old, as recorded in documents filed with Texas Secretary of State.
- Key People:** 2 people listed.
- Locations:** 1 location listed.
- Filings:** 1 filing listed.
- Contributors:** 0 contributors listed.

On the right side, there's a "Network Visualizer" diagram showing the relationships between various entities. At the bottom, there's a sidebar with an "Advertisements" section.

Social Media Sources (Facebook, Instagram)

Online Presence and Social Media

Source	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none">• https://www.voilanorbert.com/
Objective	Gather email addresses for target building and social engineering.
Required Inputs	Target name, known email address, or domain name

The screenshot shows the VoilaNorbert web application interface. On the left, there's a sidebar with navigation options: PROSPECTING (selected), Manual, Bulk, CONTACTS (selected), and API. The main area has a search bar at the top with fields for 'Person name' and 'Domain.com'. Below the search bar, there's a green button labeled 'GO AHEAD, NORBERT!' and a link to 'Add 6 contacts to a list'. The main content area displays a list of contacts with their names, companies, and email addresses:

- Travis Kalanick Uber travis@uber.com
- Michael Arrington Techcrunch michael@techcrunch.com
- Larry Page Google larry.page@google.com
- Tim Cook Apple tcook@apple.com
- John Collison Stripe john.collison@stripe.com
- Ev Williams Medium ev@medium.com

Each contact entry includes small icons for email and adding to a list, and a question mark icon in the bottom right corner of the main area.

Shodan

Internet Scanning and Enumeration

Source	<ul style="list-style-type: none"> https://www.shodan.io/
Objective	Identify internet-facing devices and services.
Required Inputs	Known IP address

The screenshot shows the Shodan search results for the IP address 34.102.136.180. The top navigation bar includes links for SHODAN, Explore, Pricing, and a search bar. Below the search bar is a map of the Kansas City area with the IP address highlighted. The main content area displays the following information:

General Information

Hostnames	180.136.102.34.bc.googleusercontent.com
Domains	GOOGLEUSERCONTENT.COM
Cloud Provider	Google
Cloud Region	global
Country	United States
City	Kansas City
Organization	Google LLC
ISP	Google LLC
ASN	AS396982

Open Ports

Open ports: 53, 80, 111, 443, 5432

OpenResty

```

HTTP/1.1 200 OK
Server: openresty
Date: Sun, 13 Aug 2023 18:58:00 GMT
Content-Type: text/html
Content-Length: 2930
Last-Modified: Sat, 12 Aug 2023 20:12:29 GMT
ETag: "64d7e7ad-b72"
X-AdBlock-Key: MFwwDQYJKoZIhvNAQEBBQADSwAwSAJBARDmzcpTevQqklnh6dJuX/N/HN+GxrruAKztliiC86+ewQ0msW1W8psOFL/000zklqsCaewAAQ_1w5V0di28J19HV3MQRA/nMpx427/1/kDFi8IhDn7KBAGSMgYRhCVj2IPMwHdBqUzQ
Cache-Control: no-cache
X-Content-Type-Options: nosniff
Set-Cookie: system=PW;Path=/;Max-Age=86400;
Set-Cookie: cof_ipaddr=224.211.186.214;Path=/;Max-Age=86400;
Set-Cookie: country=US;Path=/;Max-Age=86400;
Set-Cookie: city="";Path=/;Max-Age=86400;
Set-Cookie: traffic_target=gd;Path=/;Max-Age=86400;
Accept-Ranges: bytes
Via: 1.1 google

```

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

The screenshot shows the SecurityTrails interface for the domain `artemisenergypartners.com`. The left sidebar has tabs for DOMAIN, DNS Records (selected), Historical Data, and Subdomains (with 2 results). A blue button says "Sign up for an API key now!" and "Sign up". The main content area displays DNS records as of Aug 13, 2023:

- A records:** Google LLC (35.192.73.176, 218 entries)
- AAAA records:** NO RECORDS
- MX records:** Microsoft Corporation (1 record: artemisenergypartners-com.mail.protection.outlook.com)
- NS records:** Cloudflare, Inc., ns72.worldnic.com, ns71.worldnic.com
- SOA records:** ttl: 10800, email: namehost.worldnic.com (2,475,932 entries)
- TXT:** v=spf1 include:spf.protection.outlook.com ip4:10.16 include:spf.protection.outlook.com ~all ip4:10.168.2 include:spf.protection.outlook.com ~all include:_spf.prod.hydra.sophos.com -all sophos-domain-

Builtwith

Internet Scanning and Enumeration

Source	<ul style="list-style-type: none"> 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

The screenshot shows the Builtwith interface for the domain `artemisenergypartners.com`. The top navigation bar includes links for Tools, Features, Plans, Customers, Resources, and a search bar with the query `artemisenergypartners.com` and a **Lookup** button. Below the navigation is a breadcrumb trail: Home / artemisenergypartners.com Technology Profile.

ARTEMISENERGYPARTNERS.COM

The main content area has tabs for Technology Profile (selected), Detailed Technology Profile, Meta Profile, Relationship, Redirect, Recommendations, and Company.

Widgets:

- Pexels**: Pexels Usage Statistics · Download List of All Websites using Pexels. Free stock photos, royalty free images & videos. Image Provider.
- Contact Form 7**: Contact Form 7 Usage Statistics · Download List of All Websites using Contact Form 7. Specifically designed for wordpress blogs. Contact Form 7 can manage multiple contact forms, plus you can customize the form and the mail contents flexibly with simple markup. Feedback Forms and Surveys.
- Font Awesome**: Font Awesome Usage Statistics · Download List of All Websites using Font Awesome. Iconic font and CSS toolkit. Fonts.
- Wordpress Plugins**: Wordpress Plugins Usage Statistics · Download List of All Websites using Wordpress Plugins. Plugins are tools to extend the functionality of WordPress. The website uses various plugins from WordPress to provide additional functionality. Some of them may be listed here.
- Sitelinks Search Box**: Sitelinks Search Box Usage Statistics · Download List of All Websites using Sitelinks Search Box. With Google sitelinks search box, people can reach your content more quickly from search results. Site Search.
- RankMath**: RankMath Usage Statistics · Download List of All Websites using RankMath. Search engine optimization plugin for WordPress.

Profile Details (Change Layout): Last technology detected on 20th July 2023. We know of 39 technologies on this page and 6 technologies removed from `artemisenergypartners.com` since 30th December 2021. [Link to this page.](#)

Get a notification when `artemisenergypartners.com` adds new technologies. **Create Notification**.

Recent Lookups:

acpi.com.br	xemico.com
molo13.it	nublemate.com
crawly.com.br	sempraeavista.com.br
adcc.com.cn	wmoi.com
cooperweston.co.uk	margraphics.com
apnijaidad.com.pk	physifox.com
keralatravelcentre.com	mokstor.com
watersplashnet.com	roobot.de
dirriesenberg.de	montrealimmosvip.com
erobito.com	acpf.com.br
dndoog.com	natcglobal.com
kaetteluueckenhaus.de	agrobasic.ro
brightweb.com	daxiron.com
equibase.com	ipcom.be
rinse.vc	contadorinc.co.za
envrise.com	referin.com
studiodhikari.com.br	ruteam.ru
desibees.com	e-bikes.io
fpsdi.org	xn--vj1b84kq5kd2g.kr
multicraft.world	treinal.com
hotelaltefeuerwache.de	acpilates.com.br

PassiveDNS by Mnemonic

DNS and Domain Information

Source	<ul style="list-style-type: none">• https://passivedns.mnemonic.no/
Objective	Gather passive DNS data to build DNS history and resolution profile.
Required Inputs	Domain name or IP address

The screenshot shows the PassiveDNS by Mnemonic web application. At the top, there is a large logo with the words "PASSIVE" and "DNS" in white and orange. Below the logo is a search bar containing the query "artemisenergypartners.com". The main area displays a table of DNS records:

Record type	Query	Answer	First seen	Last seen	# times	TTL
a	artemisenergypartners.com	35.192.73.176	2023-03-21 12:30	2023-08-08 03:43	7	7200

At the bottom of the table, there are pagination controls: "Showing: 25 ▾", "1-1 of 1", and arrows for navigating through the results. To the right of the table, a vertical sidebar titled "History" shows a single entry for "artemisenergypartners.com" with a timestamp of "15 seconds ago".

DNSDumpster

DNS and Domain Information

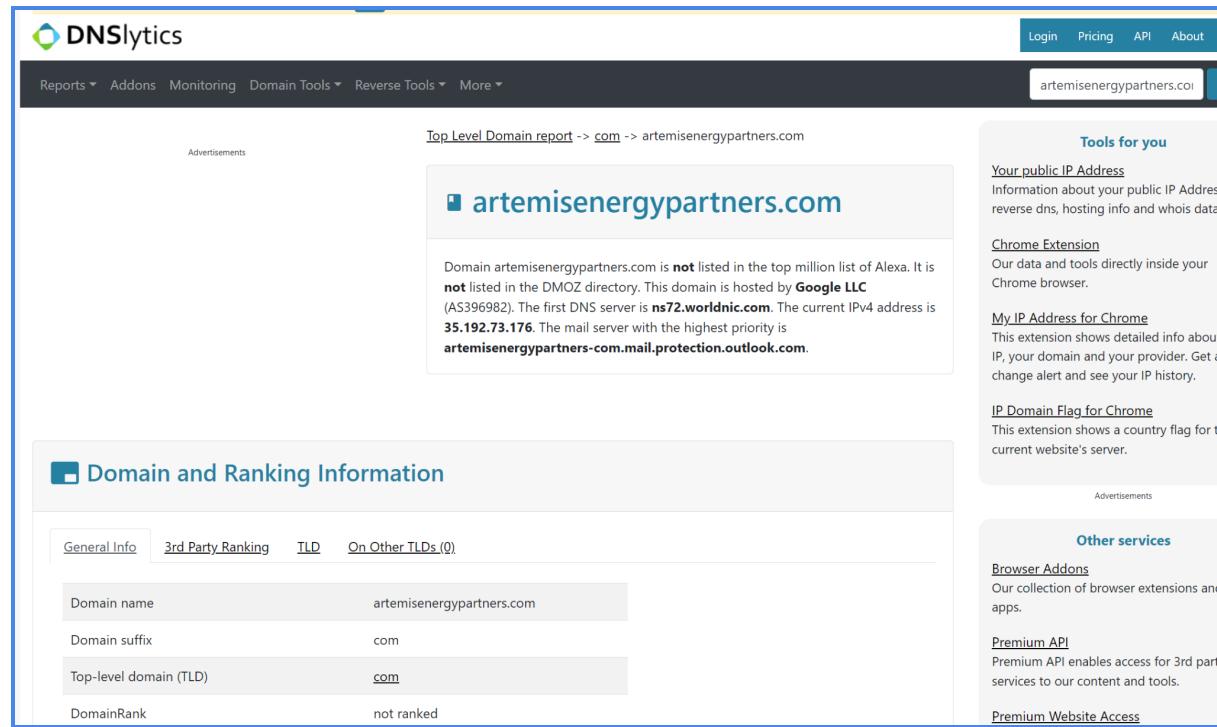
Source	<ul style="list-style-type: none"> https://dnsdumpster.com/
Objective	Gather DNS domain and subdomain information associated with the target domain.
Required Inputs	Domain name



DNSlytics

DNS and Domain Information

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



The screenshot shows the DNSlytics interface. At the top, there's a navigation bar with links for Reports, Addons, Monitoring, Domain Tools, Reverse Tools, More, Login, Pricing, API, and About. A search bar contains the domain 'artemisenergypartners.com'. The main content area displays a summary for the domain:

Top Level Domain report -> com -> artemisenergypartners.com

artemisenergypartners.com

Domain artemisenergypartners.com is **not** listed in the top million list of Alexa. It is **not** listed in the DMOZ directory. This domain is hosted by **Google LLC** (AS396982). The first DNS server is **ns72.worldnic.com**. The current IPv4 address is **35.192.73.176**. The mail server with the highest priority is **artemisenergypartners-com.mail.protection.outlook.com**.

Domain and Ranking Information

General Info	3rd Party Ranking	TLD	On Other TLDs (0)
Domain name	artemisenergypartners.com		
Domain suffix	com		
Top-level domain (TLD)	com		
DomainRank	not ranked		

Tools for you

- Your public IP Address**: Information about your public IP Address reverse dns, hosting info and whois data.
- Chrome Extension**: Our data and tools directly inside your Chrome browser.
- My IP Address for Chrome**: This extension shows detailed info about your IP, your domain and your provider. Get an change alert and see your IP history.
- IP Domain Flag for Chrome**: This extension shows a country flag for the current website's server.

Other services

- Browser Addons**: Our collection of browser extensions and apps.
- Premium API**: Premium API enables access for 3rd party services to our content and tools.
- Premium Website Access**

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: