

[🏠 \(https://dnsdumpster.com/\)](https://dnsdumpster.com/) [🛡 \(/osint-network-defenders/\)](/osint-network-defenders/)

[🎓 \(/footprinting-reconnaissance/\)](/footprinting-reconnaissance/) [🎯 \(https://hackertarget.com/\)](https://hackertarget.com/)

dns recon & research, find & lookup dns records

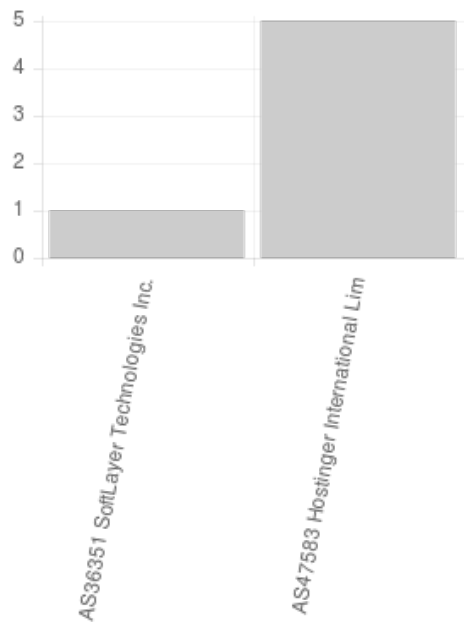
exampledomain.com

Search ➤

Showing results for **pengowin.com.ar**

[DNS Servers](#) [MX Records](#) [TXT Records](#) [Host \(A\) Records](#) [Domain Map](#)

Hosting (IP block owners)



GeoIP of Host Locations

[🏠 \(https://dnsdumpster.com/\)](https://dnsdumpster.com/) [🛡 \(/osint-network-defenders/\)](/osint-network-defenders/)

[🎓 \(/footprinting-reconnaissance/\)](/footprinting-reconnaissance/) [© \(https://hackertarget.com/\)](https://hackertarget.com/)



## DNS Servers

ns3.hostinger-ar.com. 📊 <a href="https://api.hackertarget.com/reverseiplookup/?q=173.192.183.247"> (https://api.hackertarget.com/reverseiplookup/?q=173.192.183.247)</a> <a href="https://api.hackertarget.com/httpheaders/?q=ns3.hostinger-ar.com.">🌐 (https://api.hackertarget.com/httpheaders/?q=ns3.hostinger-ar.com.)</a> ➡ <a href="https://api.hackertarget.com/zonetransfer/?q=ns3.hostinger-ar.com."> (https://api.hackertarget.com/zonetransfer/?q=ns3.hostinger-ar.com.)</a> ⚡ <a href="https://api.hackertarget.com/mtr/?q=173.192.183.247"> (https://api.hackertarget.com/mtr/?q=173.192.183.247)</a> 📌 <a href="https://api.hackertarget.com/findshareddns/?q=ns3.hostinger-ar.com."> (https://api.hackertarget.com/findshareddns/?q=ns3.hostinger-ar.com.)</a> 👁️ ⚡	173.192.183.247 f7.b7.c0ad.ip4.static.sl-reverse.com	AS36351 SoftLayer Technologies Inc. United States
ns2.hostinger-ar.com. 📊 <a href="https://api.hackertarget.com/reverseiplookup/?q=31.220.23.1"> (https://api.hackertarget.com/reverseiplookup/?q=31.220.23.1)</a> <a href="https://api.hackertarget.com/httpheaders/?q=ns2.hostinger-ar.com.">🌐 (https://api.hackertarget.com/httpheaders/?q=ns2.hostinger-ar.com.)</a> ➡ <a href="https://api.hackertarget.com/zonetransfer/?q=ns2.hostinger-ar.com."> (https://api.hackertarget.com/zonetransfer/?q=ns2.hostinger-ar.com.)</a> ⚡ <a href="https://api.hackertarget.com/mtr/?q=31.220.23.1"> (https://api.hackertarget.com/mtr/?q=31.220.23.1)</a> 📌 <a href="https://api.hackertarget.com/findshareddns/?q=ns2.hostinger-ar.com."> (https://api.hackertarget.com/findshareddns/?q=ns2.hostinger-ar.com.)</a> 👁️ ⚡	31.220.23.1 ns2.hostinger.com	AS47583 Hostinger International Limited United States
ns4.hostinger-ar.com. 📊 <a href="https://api.hackertarget.com/reverseiplookup/?q=31.170.164.249"> (https://api.hackertarget.com/reverseiplookup/?q=31.170.164.249)</a> <a href="https://api.hackertarget.com/httpheaders/?q=ns4.hostinger-ar.com.">🌐 (https://api.hackertarget.com/httpheaders/?q=ns4.hostinger-ar.com.)</a> ➡ <a href="https://api.hackertarget.com/zonetransfer/?q=ns4.hostinger-ar.com."> (https://api.hackertarget.com/zonetransfer/?q=ns4.hostinger-ar.com.)</a> ⚡ <a href="https://api.hackertarget.com/mtr/?q=31.170.164.249"> (https://api.hackertarget.com/mtr/?q=31.170.164.249)</a> 📌 <a href="https://api.hackertarget.com/findshareddns/?q=ns4.hostinger-ar.com."> (https://api.hackertarget.com/findshareddns/?q=ns4.hostinger-ar.com.)</a> 👁️ ⚡	31.170.164.249 ns4.hostinger.com	AS47583 Hostinger International Limited United Kingdom
ns1.hostinger-ar.com. 📊 <a href="https://api.hackertarget.com/reverseiplookup/?q=31.170.163.241"> (https://api.hackertarget.com/reverseiplookup/?q=31.170.163.241)</a> <a href="https://api.hackertarget.com/httpheaders/?q=ns1.hostinger-ar.com.">🌐 (https://api.hackertarget.com/httpheaders/?q=ns1.hostinger-ar.com.)</a> ➡ <a href="https://api.hackertarget.com/zonetransfer/?q=ns1.hostinger-ar.com."> (https://api.hackertarget.com/zonetransfer/?q=ns1.hostinger-ar.com.)</a> ⚡ <a href="https://api.hackertarget.com/mtr/?q=31.170.163.241"> (https://api.hackertarget.com/mtr/?q=31.170.163.241)</a> 📌 <a href="https://api.hackertarget.com/findshareddns/?q=ns1.hostinger-ar.com."> (https://api.hackertarget.com/findshareddns/?q=ns1.hostinger-ar.com.)</a> 👁️ ⚡	31.170.163.241 ns1.hostinger.com	AS47583 Hostinger International Limited United States


MX Records \*\* This is where email for the domain goes...

10 mx1.hostinger.com.ar (https://dnsdumpster.com/) (/osint-network-defenders/) 21.220.106.26 AS47583 Hostinger International Limited United Kingdom  
 (https://api.hackertarget.com/reverseiplookup/?q=31.220.106.26) (https://api.hackertarget.com/mtr/?q=31.220.106.26) (https://footprinting-reconnaissance/) (https://hackertarget.com/)

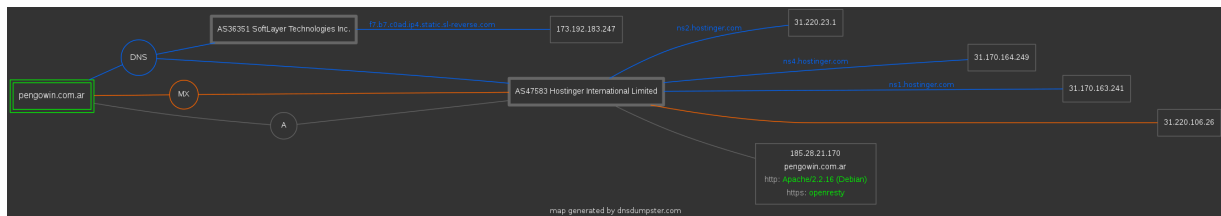
TXT Records \*\* Find more hosts in Sender Policy Framework (SPF) configurations

Host Records (A) \*\* this data may not be current as it uses a static database (updated monthly)

pengowin.com.ar 185.28.21.170 AS47583 Hostinger International Limited United States  
 (https://api.hackertarget.com/reverseiplookup/?q=185.28.21.170) (https://api.hackertarget.com/httpheaders/?q=http://pengowin.com.ar) (https://api.hackertarget.com/mtr/?q=185.28.21.170)    
 HTTP: Apache/2.2.16 (Debian)  
 HTTPS: openresty

 Download .xlsx of Hosts (https://dnsdumpster.com/static/xls/pengowin.com.ar-201806150325.xlsx)

Mapping the domain \*\* click for full size image





(/static/map/pengowin.com.ar.png)

DNSdumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process.

this is a HackerTarget.com (https://hackertarget.com/) project

Open Source Intelligence for Networks

 (<https://dnsdumpster.com/>)  (</osint-network-defenders/>)

 (</footprinting-reconnaissance/>)  (<https://hackertarget.com/>)

### Attack

The ability to quickly identify the attack surface is essential. Whether you are penetration testing or chasing bug bounties.



### Defend

Network defenders benefit from passive reconnaissance in a number of ways. With analysis informing information security strategy.



### Learn



Understanding network based OSINT helps information technologists to better operate, assess and manage the network.



Map an organizations attack surface with a virtual *dumpster dive*\* of the DNS records associated with the target

organization.

 (<https://dnsdumpster.com/>)  (</osint-network-defenders/>)

 (</footprinting-reconnaissance/>)  (<https://hackertarget.com/>)

\*DUMPSTER DIVING: The practice of sifting refuse from an office or technical installation to extract confidential data, especially security-compromising information.

## Frequently Asked Questions

How can I take my security assessments to the next level?

The company behind DNSDumpster is [hackertarget.com](https://hackertarget.com/) (<https://hackertarget.com/>) where we provide online hosted access to trusted open source security testing tools. Save time and headaches by incorporating hosted scanners into your vulnerability assessment process.

What data does DNSDumpster use?

No brute force subdomain enumeration is used as is common in dns recon tools that enumerate subdomains. We use open source intelligence resources to query for related domain data. It is then compiled into an actionable resource for both attackers and defenders of Internet facing systems.

More than a simple [DNS lookup](https://hackertarget.com/dns-lookup/) (<https://hackertarget.com/dns-lookup/>) this tool will discover those hard to find sub-domains and web hosts. The search relies on data from our crawls of the Alexa Top 1 Million sites, Search Engines, Common Crawl, Certificate Transparency, Max Mind, Team Cymru, Shodan and [scans.io](https://scans.io/) (<https://scans.io/>).



I have hit the host limit, do you have a PRO option?



Over at [hackertarget.com](https://hackertarget.com/) (<https://hackertarget.com/>) there's a tool we call [domain profiler](https://hackertarget.com/domain-profiler/) (<https://hackertarget.com/domain-profiler/>). This compiles data similar to DNSDumpster with up to 40K results. With a STARTER membership you have access to the domain profiler tool for 12 months. Once the years membership expires you will revert to BASIC member status, however access to Domain Profiler and Basic Nmap scans continue. The BASIC access does not expire.

What are some other resources and tools for learning more?

There are some great open source recon frameworks that have been developed over the past couple of years. In addition tools such as **Metasploit** and **Nmap** include

various modules for enumerating DNS. Check our [Getting Started with Footprinting](https://dnsdumpster.com/footprinting-reconnaissance/) (<https://dnsdumpster.com/footprinting-reconnaissance/>) for more information.


 (<https://dnsdumpster.com/>)  ([/osint-network-defenders/](https://osint-network-defenders.com/))

 ([/footprinting-reconnaissance/](https://dnsdumpster.com/footprinting-reconnaissance/))  (<https://hackertarget.com/>)

## About

At [hackertarget.com](https://hackertarget.com/) (<https://hackertarget.com/>), we have been scanning the Internet since 2007. Our vulnerability scanners now reach millions of IP addresses every year. We work to raise awareness of the value in open source security solutions.

## Stay in Touch

 [dnsdumpster@gmail.com](mailto:dnsdumpster@gmail.com)

 [@hackertarget](https://twitter.com/hackertarget/) (<https://twitter.com/hackertarget/>)

☐ Subscribe to our List ☐ Low volume Updates and News

Copyright © 2017 Hacker Target Pty Ltd

Russia