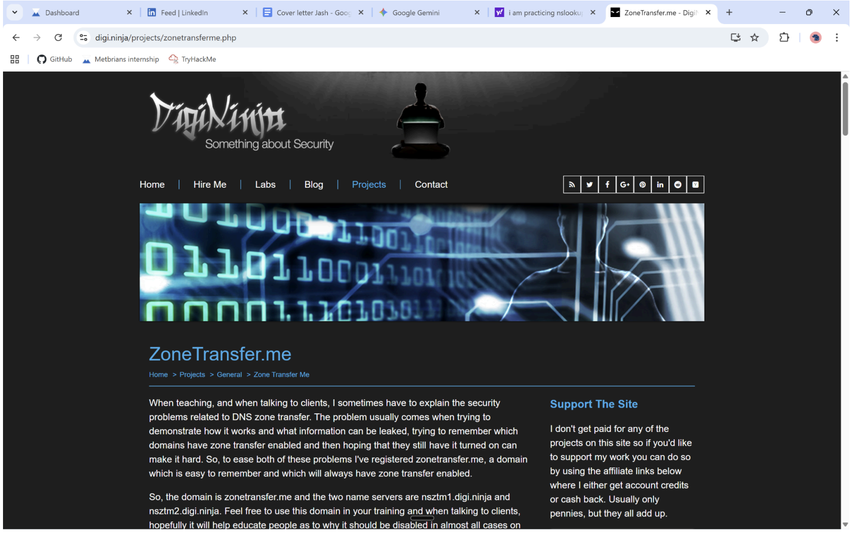
1. For this practice, I chose to use **zonetransfer.me**. It is a domain specifically set up by security professionals to allow students and researchers to practice DNS reconnaissance techniques safely and legally.



ZoneTransfer.me

Home > Projects > General > Zone Transfer Me

When teaching, and when talking to clients, I sometimes have to explain the security problems related to DNS zone transfer. The problem usually comes when trying to demonstrate how it works and what information can be leaked, trying to remember which domains have zone transfer enabled and then hoping that they still have it turned on can make it hard. So, to ease both of these problems I've registered zonetransfer.me, a domain which is easy to remember and which will always have zone transfer enabled.

So, the domain is zonetransfer.me and the two name servers are nsztm1.digi.ninja and nsztm2.digi.ninja. Feel free to use this domain in your training and when talking to clients, hopefully it will help educate people as to why it should be disabled in almost all cases on

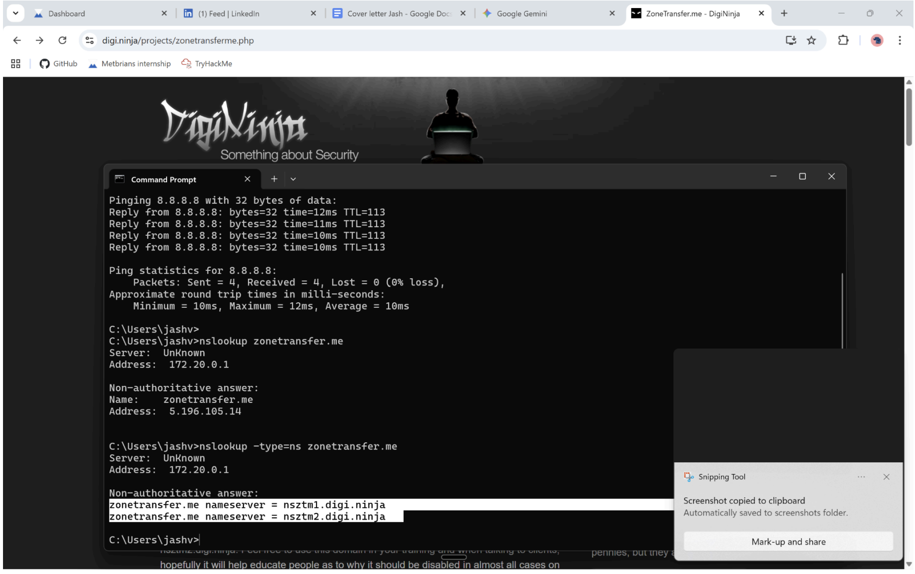
Support The Site

I don't get paid for any of the projects on this site so if you'd like to support my work you can do so by using the affiliate links below where I either get account credits or cash back. Usually only pennies, but they all add up.

1

2. I started by running a basic **nslookup** on **zonetransfer.me**. Honestly, I just wanted to make sure the domain was reachable from my Windows host since my Kali VM was having network trouble. This gave me the basic A record, which is the IP address where the website lives. It's like checking the front door of a building before trying to find the blueprints.

Next, I needed to figure out which specific servers actually hold the records for this domain. I used **nslookup -type=ns zonetransfer.me** to pull the nameserver records. This is where things got interesting. I got a non-authoritative answer pointing to servers like **nsztm1.digi.ninja**. Even though the answer was "non-authoritative," which just means my computer pulled it from a cache instead of the source, it gave me the exact targets I needed for the deeper dive



```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=12ms TTL=113
Reply from 8.8.8.8: bytes=32 time=11ms TTL=113
Reply from 8.8.8.8: bytes=32 time=10ms TTL=113
Reply from 8.8.8.8: bytes=32 time=10ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 12ms, Average = 10ms

C:\Users\jashv>
C:\Users\jashv>nslookup zonetransfer.me
Server:  UnKnown
Address:  172.20.0.1

Non-authoritative answer:
Name:    zonetransfer.me
Address:  5.196.105.14


C:\Users\jashv>nslookup -type=ns zonetransfer.me
Server:  UnKnown
Address:  172.20.0.1

Non-authoritative answer:
zonetransfer.me nameserver = nsztm1.digi.ninja
zonetransfer.me nameserver = nsztm2.digi.ninja

C:\Users\jashv>
```

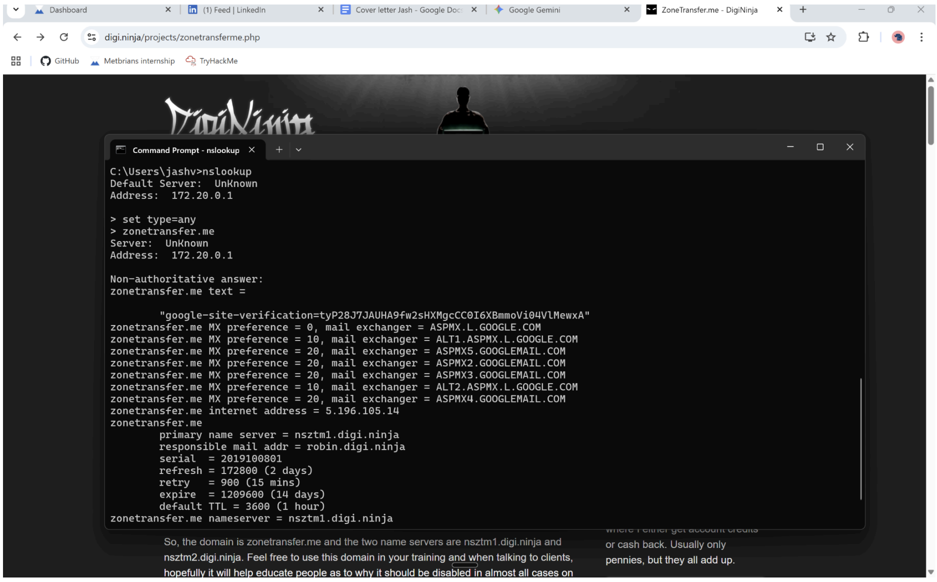
Snipping Tool

Screenshot copied to clipboard
Automatically saved to screenshots folder.

Mark-up and share

2

3. Once I had the nameservers, I wanted to see how much data I could grab without even trying a zone transfer. I jumped into the interactive mode of nslookup and used **set type=any**. This is a classic move to see if a server is over-sharing. By then typing the domain name, I was able to see a mix of MX records for mail and TXT records.


Dashboard
(1) Feed | LinkedIn
Cover letter Jash - Google Doc
Google Gemini
ZoneTransfer.me - DigiNinja
digi.ninja/projects/zonetransferme.php
GitHub
Metbrians internship
TryHackMe
DigiNinja
Command Prompt - nslookup

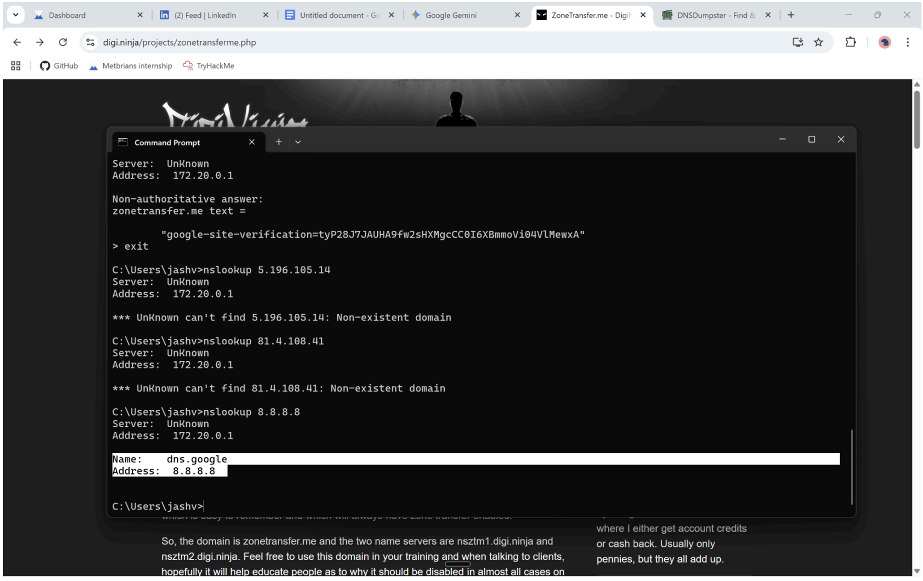
```
C:\Users\jashv>nslookup
Default Server:  UnKnown
Address:  172.20.0.1

> set type=any
> zonetransfer.me
Server:  UnKnown
Address:  172.20.0.1

Non-authoritative answer:
zonetransfer.me text =

        "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
zonetransfer.me MX preference = 0, mail exchanger = ASPMX.L.GOOGLE.COM
zonetransfer.me MX preference = 10, mail exchanger = ALT1.ASPMX.L.GOOGLE.COM
zonetransfer.me MX preference = 20, mail exchanger = ASPMX5.GOOGLEMAIL.COM
zonetransfer.me MX preference = 20, mail exchanger = ASPMX2.GOOGLEMAIL.COM
zonetransfer.me MX preference = 20, mail exchanger = ASPMX3.GOOGLEMAIL.COM
zonetransfer.me MX preference = 10, mail exchanger = ALT2.ASPMX.L.GOOGLE.COM
zonetransfer.me MX preference = 20, mail exchanger = ASPMX4.GOOGLEMAIL.COM
zonetransfer.me internet address = 5.196.105.14
zonetransfer.me
        primary name server = nsztm1.digi.ninja
        responsible mail addr = robin.digi.ninja
        serial  = 2019100801
        refresh = 172800 (2 days)
        retry   = 900 (15 mins)
        expire  = 1209600 (14 days)
        default TTL = 3600 (1 hour)
zonetransfer.me nameserver = nsztm1.digi.ninja
```

So, the domain is zonetransfer.me and the two name servers are nsztm1.digi.ninja and nsztm2.digi.ninja. Feel free to use this domain in your training and when talking to clients, hopefully it will help educate people as to why it should be disabled in almost all cases on

or cash back. Usually only pennies, but they all add up.

3

4. After gathering the IPs **5.196.105.14** and **81.4.108.41**, I wanted to see if I could tie them back to the domain using a reverse DNS lookup. This is basically a way to double check if an IP actually belongs to the domain you are investigating. However, when I ran the command, it came back with a "Non-existent domain" error for both addresses.Instead of just assuming my command was failing or that my network was broken, I wanted to verify my methodology. I decided to try a reverse lookup on **8.8.8.8**, which is the well-known Google Public DNS. As you can see in the screenshot, it immediately gave me the answer **dns.google**.



```
Server:  UnKnown
Address:  172.20.0.1

Non-authoritative answer:
zonetransfer.me text =

        "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
> exit

C:\Users\jashv>nslookup 5.196.105.14
Server:  UnKnown
Address:  172.20.0.1

*** UnKnown can't find 5.196.105.14: Non-existent domain

C:\Users\jashv>nslookup 81.4.108.41
Server:  UnKnown
Address:  172.20.0.1

*** UnKnown can't find 81.4.108.41: Non-existent domain

C:\Users\jashv>nslookup 8.8.8.8
Server:  UnKnown
Address:  172.20.0.1

Name:    dns.google
Address:  8.8.8.8


C:\Users\jashv>
```

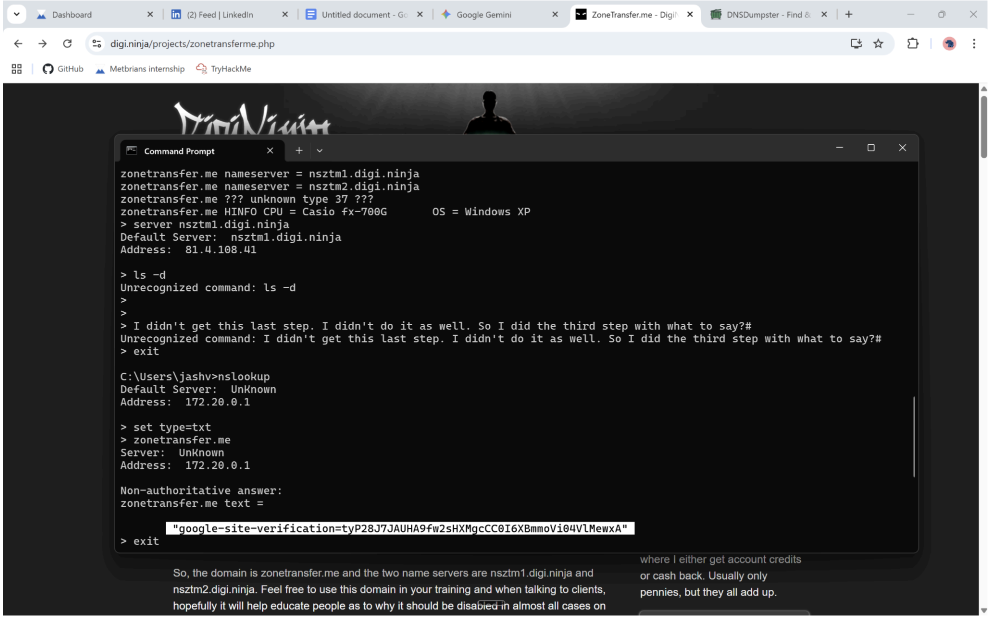
So, the domain is zonetransfer.me and the two name servers are nsztm1.digi.ninja and nsztm2.digi.ninja. Feel free to use this domain in your training and when talking to clients, hopefully it will help educate people as to why it should be disabled in almost all cases on

where I either get account credits or cash back. Usually only pennies, but they all add up.

4

After that, I decided to dig into the TXT records by using the **set type=txt** command. I was specifically hunting for an SPF record to see how they handle email security, but the result came back with a Google site verification string instead.

The Analysis: Actually, the reason the SPF record didn't show up is simply that the domain hasn't configured one. While the Google string proves the domain is active, the missing SPF is a real security gap. Without it, there is no policy to stop someone from spoofing their email address. In a real audit, I'd mark this as a finding because what is "missing" from a DNS setup often tells you more about a target's vulnerabilities than what is actually there.



```
zonetransfer.me nameserver = nsztm1.digi.ninja
zonetransfer.me nameserver = nsztm2.digi.ninja
zonetransfer.me ??? unknown type 37 ???
zonetransfer.me HINFO CPU = Casio fx-700G       OS = Windows XP
> server nsztm1.digi.ninja
Default Server:  nsztm1.digi.ninja
Address:  81.4.108.41

> ls -d
Unrecognized command: ls -d
>
>
> I didn't get this last step. I didn't do it as well. So I did the third step with what to say?#
Unrecognized command: I didn't get this last step. I didn't do it as well. So I did the third step with what to say?#
> exit

C:\Users\jashv>nslookup
Default Server:  UnKnown
Address:  172.20.0.1

> set type=txt
> zonetransfer.me
Server:  UnKnown
Address:  172.20.0.1

Non-authoritative answer:
zonetransfer.me text =

        "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
> exit
```

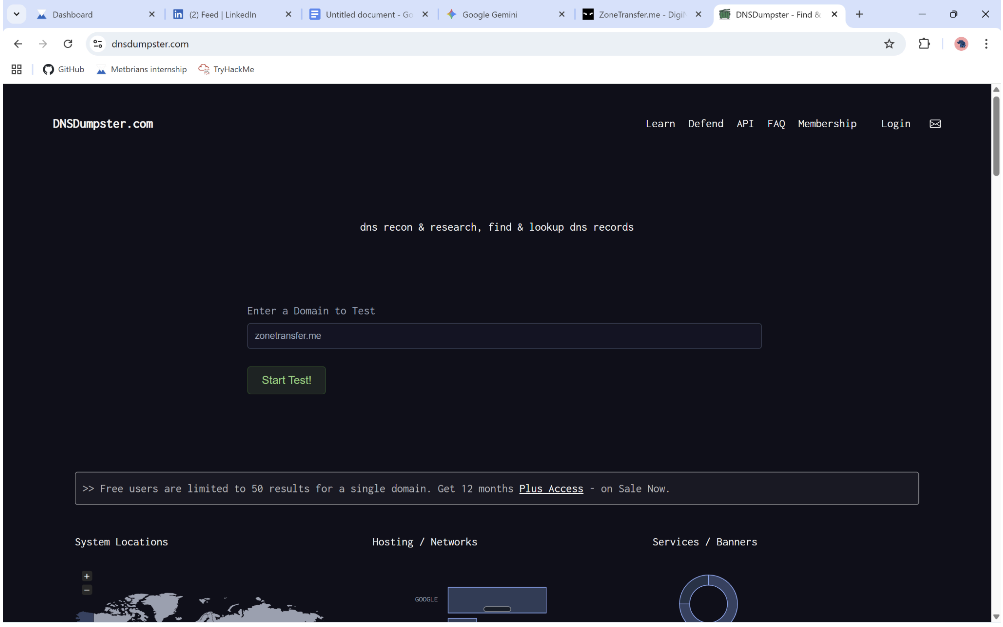
So, the domain is zonetransfer.me and the two name servers are nsztm1.digi.ninja and nsztm2.digi.ninja. Feel free to use this domain in your training and when talking to clients, hopefully it will help educate people as to why it should be disabled in almost all cases on

where I either get account credits or cash back. Usually only pennies, but they all add up.

5

6,7. After getting the manual results, I wanted to see the "big picture" of the domain's infrastructure without sending any more packets directly to their servers. I used a passive **OSINT** method by putting the domain into DNSDumpster, which is an excellent tool for mapping out an entire digital footprint.

The Analysis: Actually, this visual mapping is vital because it reveals how different servers, like mail (MX) and web hosts, interact with each other. By looking at the graphic map and the record list, I could quickly spot the entire layout of the domain in a way that manual commands don't always show. It's a much stealthier way to work because you're gathering intelligence from a database rather than the target itself. For an analyst, this is about finding "orphaned" subdomains or forgotten assets that might have been overlooked by the IT team, giving me a complete view of the attack surface before deciding where to look closer.



DNSDumpster.com

Learn Defend API FAQ Membership Login

dns recon & research, find & lookup dns records

Enter a Domain to Test

zonetransfer.me

Start Test!

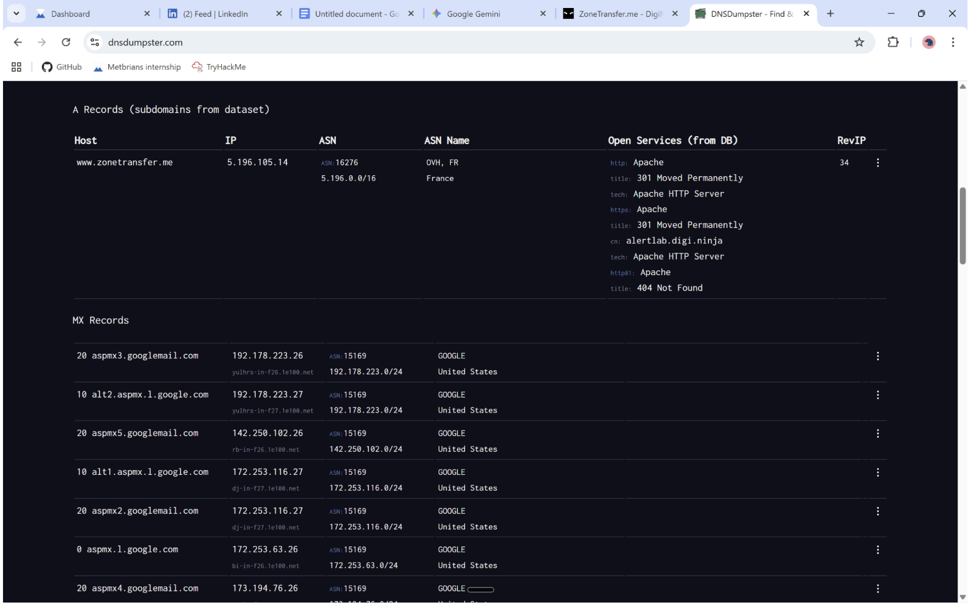
>> Free users are limited to 50 results for a single domain. Get 12 months Plus Access - on Sale Now.

System Locations

Hosting / Networks

Services / Banners

6



A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
www.zonetransfer.me	5.196.105.14	ASN: 16276 5.196.0.0/16	OVH, FR France	http: Apache title: 301 Moved Permanently tech: Apache HTTP Server https: Apache title: 301 Moved Permanently cn: alertlab.digi.ninja tech: Apache HTTP Server http81: Apache title: 404 Not Found	34

MX Records

20 aspmx3.googlemail.com	192.178.223.26 yulhrs-in-f26.1e100.net	ASN: 15169 192.178.223.0/24	GOOGLE United States
10 alt2.aspmx.l.google.com	192.178.223.27 yulhrs-in-f27.1e100.net	ASN: 15169 192.178.223.0/24	GOOGLE United States
20 aspmx5.googlemail.com	142.250.102.26 rb-in-f26.1e100.net	ASN: 15169 142.250.102.0/24	GOOGLE United States
10 alt1.aspmx.l.google.com	172.253.116.27 dj-in-f27.1e100.net	ASN: 15169 172.253.116.0/24	GOOGLE United States
20 aspmx2.googlemail.com	172.253.116.27 dj-in-f27.1e100.net	ASN: 15169 172.253.116.0/24	GOOGLE United States
0 aspmx.l.google.com	172.253.63.26 bi-in-f26.1e100.net	ASN: 15169 172.253.63.0/24	GOOGLE United States
20 aspmx4.googlemail.com	173.194.76.26	ASN: 15169	GOOGLE

7

A Recommendations Section:

Implement an SPF Record: To prevent email spoofing, the domain should define a clear policy in its TXT records.

Restrict "ANY" Queries: The server should be configured to limit the amount of information it provides to generic queries to reduce the metadata leaked to attackers.

Configure PTR Records: Setting up reverse DNS for all active IP addresses would help in verifying the legitimacy of the infrastructure