

Footprinting and Reconnaissance

NSLookup is a network administration tool for querying the Domain Name System (DNS) to obtain the mapping between domain name and IP address, or other DNS records.

Now I shall use NSLookup to get DNS records of Smartinternz.com.

DNS records for smartinternz.com

CloudflareGoogle DNSOpenDNSAuthoritativeLocal DNS

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
> 3.111.252.14	1m
> 35.154.227.143	1m

AAAA records

No AAAA records found.

CNAME record

No CNAME record found.

TXT records

SPF record

This record is valid for 1h.

Pass if the email sender's IP is in the A or AAAA records of smartinternz.com.	a
Or else, pass if the email sender's IP is in the MX records of smartinternz.com.	mx
Or else, pass if a reverse lookup of the email sender's IP resolves to smartinternz.com.	ptr
Or else, include the SPF record at secureserver.net and pass if it matches the sender's IP.	include:secureserver.net
Or else, mark the email as softfail.	~all

NS records

Name server	Revalidate in
ns-1493.awsdns-58.org.	48h
ns-1745.awsdns-26.co.uk.	48h
ns-401.awsdns-50.com.	48h
ns-914.awsdns-50.net.	48h

MX records

Mail server	Priority	Revalidate in
mail.smartinternz.com.	0 Primary	5m

Other records

SOA

SOA data

		Revalidate in
Start of authority	ns-1745.awsdns-26.co.uk.	15m
Email	awsdns-hostmaster@amazon.com	
Serial	1	
Refresh	2h	
Retry	15m	
Expire	336h	
Negative cache TTL	24h	

By Nslookup.io
DNS for Developers
Never be confused
about DNS again.

RAW Output

A records

QUESTION

dig @ smartinternz.com. A

ANSWER

smartinternz.com.	60	A	3.111.252.14
smartinternz.com.	60	A	35.154.227.143

AUTHORITY

ADDITIONAL

. 0 OPT ; payload 1232, xrcode 0, version 0, flags 0

AAAA records

QUESTION

dig @ smartinternz.com. AAAA

ANSWER

AUTHORITY

smartinternz.com.	900	SOA	ns-1745.awsdns-26.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
-------------------	-----	-----	---

ADDITIONAL

. 0 OPT ; payload 1232, xrcode 0, version 0, flags 0

CNAME record

QUESTION

dig @ smartinternz.com. CNAME

ANSWER

AUTHORITY

smartinternz.com. 900 SOA ns-1745.awsdns-26.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

ADDITIONAL

. 0 OPT ; payload 1232, xrcode 0, version 0, flags 0

TXT records

QUESTION

dig @ smartinternz.com. TXT

ANSWER

smartinternz.com. 3600 TXT "v=spf1 a mx ptr include:secureserver.net ~all"

AUTHORITY

ADDITIONAL

. 0 OPT ; payload 1232, xrcode 0, version 0, flags 0

NS records

QUESTION

dig @ smartinternz.com. NS

ANSWER

smartinternz.com. 172800 NS ns-1493.awsdns-58.org.
smartinternz.com. 172800 NS ns-1745.awsdns-26.co.uk.

```
smartinternz.com.      172800  NS      ns-401.awsdns-
50.com.
smartinternz.com.      172800  NS      ns-914.awsdns-
50.net.
```

AUTHORITY

ADDITIONAL

```
.      0      OPT      ; payload 1232, xrcode 0, version
0, flags 0
```

MX records

QUESTION

```
dig @ smartinternz.com. MX
```

ANSWER

```
smartinternz.com.      300      MX      0
mail.smartinternz.com.
```

AUTHORITY

ADDITIONAL

```
.      0      OPT      ; payload 1232, xrcode 0, version
0, flags 0
```

Other records

QUESTION

```
dig @ smartinternz.com. SOA
```

ANSWER

```
smartinternz.com.      900      SOA      ns-1745.awsdns-
26.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
```

AUTHORITY

```
      ADDITIONAL
      .          0      OPT      ; payload 1232, xrcode 0, version
0, flags 0
```

From the output of nslookup, we can find out

- The IP addresses of the website
- The Mail servers
- Website is running on AWS
- SOA Data

Analyzing this data will allow us to find vulnerabilities in the website. Then we can use exploit-db to find exploits for the website.