

DNS Record

Challenge

235 Solves



DNS Record Hunting

5

DNS

The flag for this challenge is easy - You just need to read the DNS records for securityblue.team, and look for a TXT record. Once you've found it, select the answer that matches the flag value.

- ☐ 9210314KLALDM
- ☐ SDFL2342OOOP
- ☐ 8432Y45M65SMF
- ☐ KDisTHEbest1337

You only have two attempts to select the right answer.

Submit

Answer: Using <https://toolbox.googleapps.com/apps/dig/> you can look up ANY record for securityblue.team. Below is the output. Flag:9210314KLALDM

The same thing can be done using the dig command in kali > dig -t any securityblue.team

```

id 53255
opcode QUERY
rcode NOERROR
flags QR RD RA
;QUESTION
securityblue.team. IN ANY
;ANSWER
securityblue.team. 59 IN A 3.9.68.12
securityblue.team. 21599 IN NS ns-1044.awsdns-02.org.
securityblue.team. 21599 IN NS ns-1768.awsdns-29.co.uk.
securityblue.team. 21599 IN NS ns-378.awsdns-47.com.
securityblue.team. 21599 IN NS ns-901.awsdns-48.net.
securityblue.team. 899 IN SOA ns-1044.awsdns-02.org. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
securityblue.team. 59 IN MX 0 securityblue-team.mail.protection.outlook.com.
securityblue.team. 59 IN TXT "MS=ms76074950"
securityblue.team. 59 IN TXT "sbt-vip-ctf flag:9210314KLALDM"
securityblue.team. 59 IN TXT "v=spf1 a: include:mailgun.org protection.outlook.com ~all"
securityblue.team. 59 IN SRV 10 1 443 sipdir.online.lync.com.
securityblue.team. 59 IN SRV 10 1 5061 sipfed.online.lync.com.
;AUTHORITY
;ADDITIONAL

```

```

kali@kali:~$ dig -t any securityblue.team

;<<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> -t any securityblue.team
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 48657
;; flags: qr rd ra; QUERY: 1, ANSWER: 12, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 47c79986a7e5307f794a8b355e6b76e1f3ea529bb2b5b9c5 (good)
;; QUESTION SECTION:
;securityblue.team.      IN      ANY

;; ANSWER SECTION:
securityblue.team.      60      IN      SRV     10 1 5061 sipfed.online.lync.com.
securityblue.team.      60      IN      SRV     10 1 443 sipdir.online.lync.com.
securityblue.team.      60      IN      TXT     "sbt-vip-ctf flag:9210314KLALDM"
securityblue.team.      60      IN      TXT     "MS=ms76074950"
securityblue.team.      60      IN      TXT     "v=spf1 a: include:mailgun.org protection.outlook.com ~all"
securityblue.team.      60      IN      MX      0 securityblue-team.mail.protection.outlook.com.
securityblue.team.      900     IN      SOA     ns-1044.awsdns-02.org. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
securityblue.team.      11      IN      A       3.9.68.12
securityblue.team.      86351   IN      NS      ns-1044.awsdns-02.org.
securityblue.team.      86351   IN      NS      ns-1768.awsdns-29.co.uk.
securityblue.team.      86351   IN      NS      ns-901.awsdns-48.net.
securityblue.team.      86351   IN      NS      ns-378.awsdns-47.com.

;; ADDITIONAL SECTION:
ns-378.awsdns-47.com.   51868   IN      A       205.251.193.122
ns-901.awsdns-48.net.   32352   IN      A       205.251.195.133

;; Query time: 20 msec
;; SERVER: 192.168.23.2#53(192.168.23.2)
;; WHEN: Fri Mar 13 08:04:48 EDT 2020
;; MSG SIZE rcvd: 601

```