

Joe Grassl

## Easy Phish

1. This challenge is about determining the email security measures a domain has in place. SPF can be confirmed by using dig to get the domain's TXT record.

```
delta@host:~$ dig secure-startup.com txt [0/159]
; <<>> DiG 9.16.27-Debian <<>> secure-startup.com txt
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27646
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: leebaaa6ce588bb2c802ecb662c5eabcf8159b098f8e39dc (good)
; QUESTION SECTION:
;secure-startup.com.          IN      TXT
;
; ANSWER SECTION:
secure-startup.com.  1651   IN      TXT     "v=spf1 a mx ?all - HTB{RIP_SPF_Always_2nd}"
;
; Query time: 86 msec
; SERVER: 192.168.94.69#53(192.168.94.69)
; WHEN: Wed Jul 06 13:04:12 PDT 2022
; MSG SIZE rcvd: 129
delta@host:~$
```

2. DMARC can be found on the domain by using dig against the \_dmarc subdomain. Easy indeed!

```
delta@host:~$ dig _dmarc.secure-startup.com txt [0/216]
; <<>> DiG 9.16.27-Debian <<>> _dmarc.secure-startup.com txt
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15275
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 678c55f73dbd532cb18dc3b262c5eafaa744dde09a279b10 (good)
; QUESTION SECTION:
;_dmarc.secure-startup.com.  IN      TXT
;
; ANSWER SECTION:
_dmarc.secure-startup.com. 1800   IN      TXT     "v=DMARC1;p=none; F1dd13_2_DMARC}"
;
; Query time: 183 msec
; SERVER: 192.168.94.69#53(192.168.94.69)
; WHEN: Wed Jul 06 13:05:14 PDT 2022
; MSG SIZE rcvd: 127
delta@host:~$
```