Challenge: Easy Phish

Challenge Description:

Customers of secure-startup.com have been recieving some very convincing phishing emails, can you figure out why?

Context:

- Domain to lookup / Recon would be Secure-startup.com
 - We use a tool to scan / search up the DNS records on the Domain

Notes:

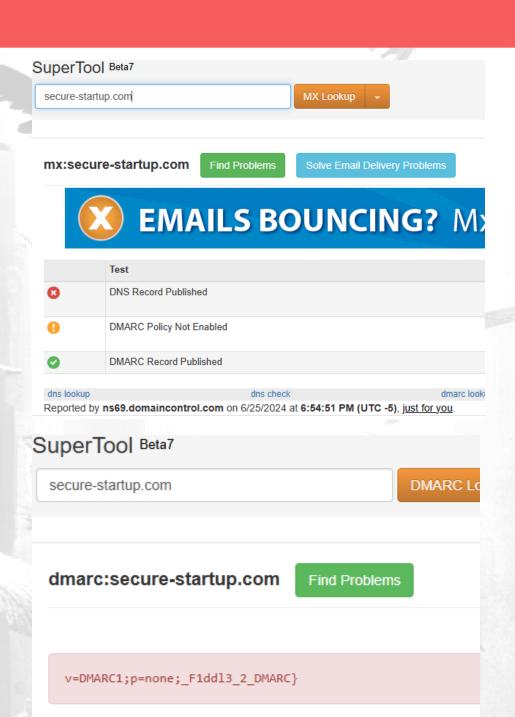
- I'm just gonna use a web-tool for this,
 - https://mxtoolbox.com/

Challenge:

Just scan the domain for anything Phishy / Flaggy

Flag:

- First we go to Mxtoolbox.com and enter the domain we want to search the records for.
- The first scan wasn't a success for anything interesting, lets try looking up the DMARC record
- The Second Scan gave us half the flag, we need to find the other half.
- After we keep scanning for different dns records like SPF / MX, we Get a hit on the SPF records, for the other part of the flag, meaning we have it all.



| Tag | TagValue | Name |
|------------------|----------|---------|
| V | DMARC1 | Version |
| p | none | Policy |
| _F1ddl3_2_DMARC} | | |

SuperTool Beta7

secure-startup.com

SPF Record Lookup

spf:secure-startup.com

Find Problems

Gr

v=spf1 a mx ?all - HTB{RIP_SPF_Always_2nd

| Prefix | Туре | Value | PrefixDesc |
|--------|------------------------|-------|------------|
| | V | spf1 | |
| + | a | | Pass |
| + | mx | | Pass |
| ? | all | | Neutral |
| - | | | Fail |
| + | HTB{RIP_SPF_Always_2nd | | Pass |

We get the flag: HTB{RIP_SPF_Always_2nd_F1ddl3_2_DMARC}

From Birdo