Easy_Phis

#OSINT #nslookup

CHALLENGE DESCRIPTION

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

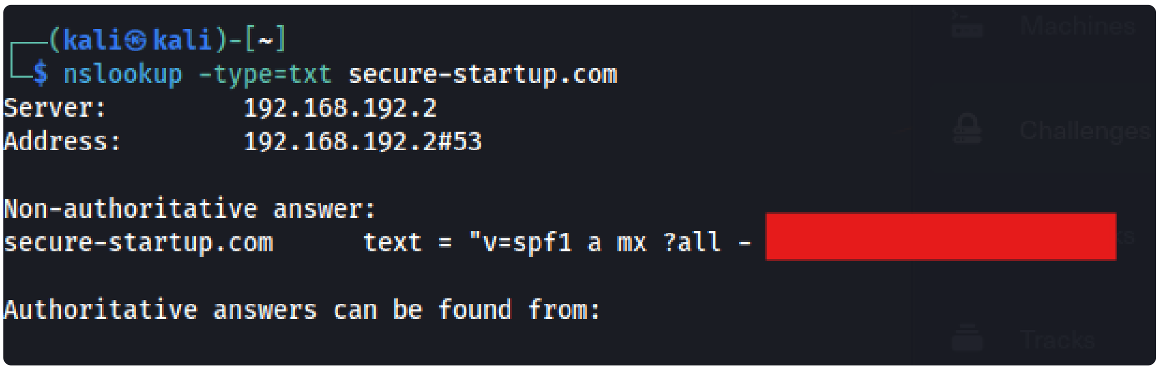
Prerequisite

- SPF (Sender Policy Framework) - it is an email authentication standard that helps sender and recipients from spam, spoofing, and phishing
- Example of the tools that use for protecting DNS
  - DMARC - is a standard that prevents spammers from using your domain to send email without your permission

Solution

`nslookup` - is a command-line network administration tool used to query Domain Name System (DNS) servers. It helps users find the IP address associated with a domain name or the domain name associated with an IP address.

1. Use `nslookup` to search for ip address
   `nslookup -type=txt secure-startup.com`
   - txt is for text record

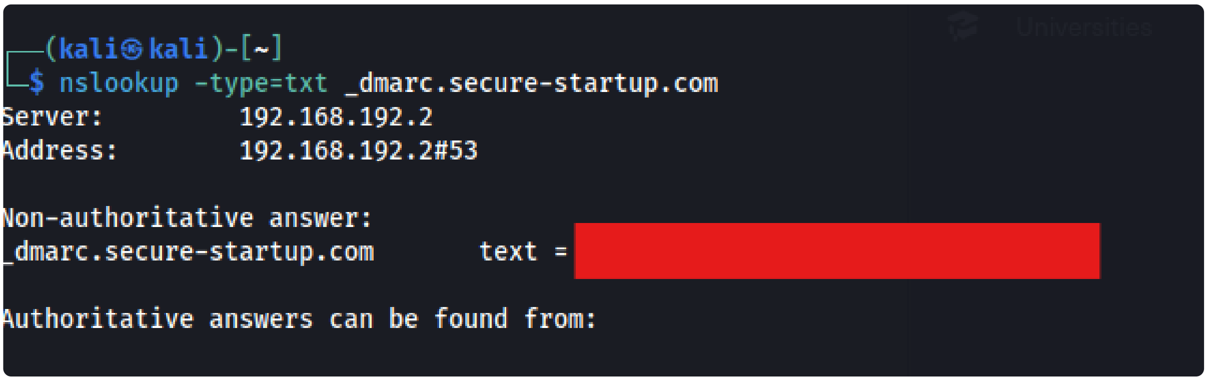


```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=txt secure-startup.com
Server:         192.168.192.2
Address:        192.168.192.2#53

Non-authoritative answer:
secure-startup.com      text = "v=spf1 a mx ?all - [redacted]

Authoritative answers can be found from:
```

2. Search for the DMARC



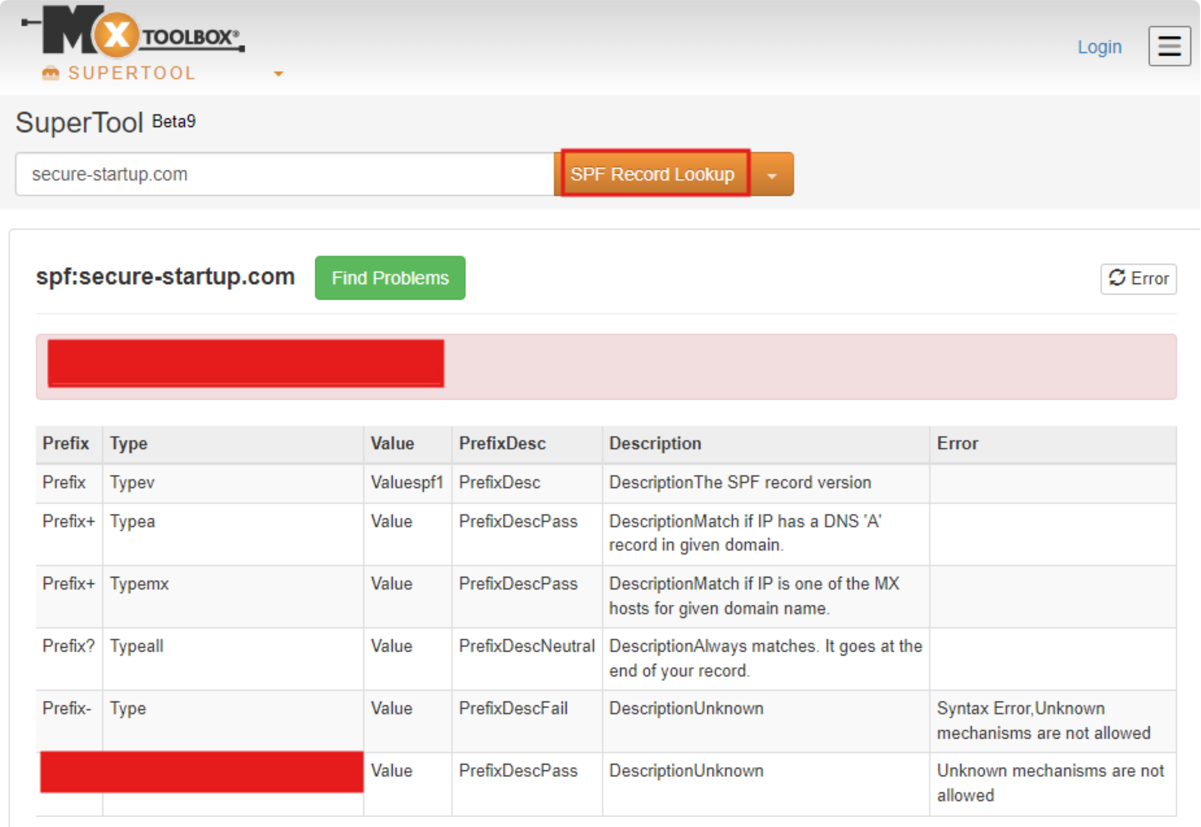
```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=txt _dmarc.secure-startup.com
Server:         192.168.192.2
Address:        192.168.192.2#53

Non-authoritative answer:
_dmarc.secure-startup.com       text = [redacted]

Authoritative answers can be found from:
```

Solution 2

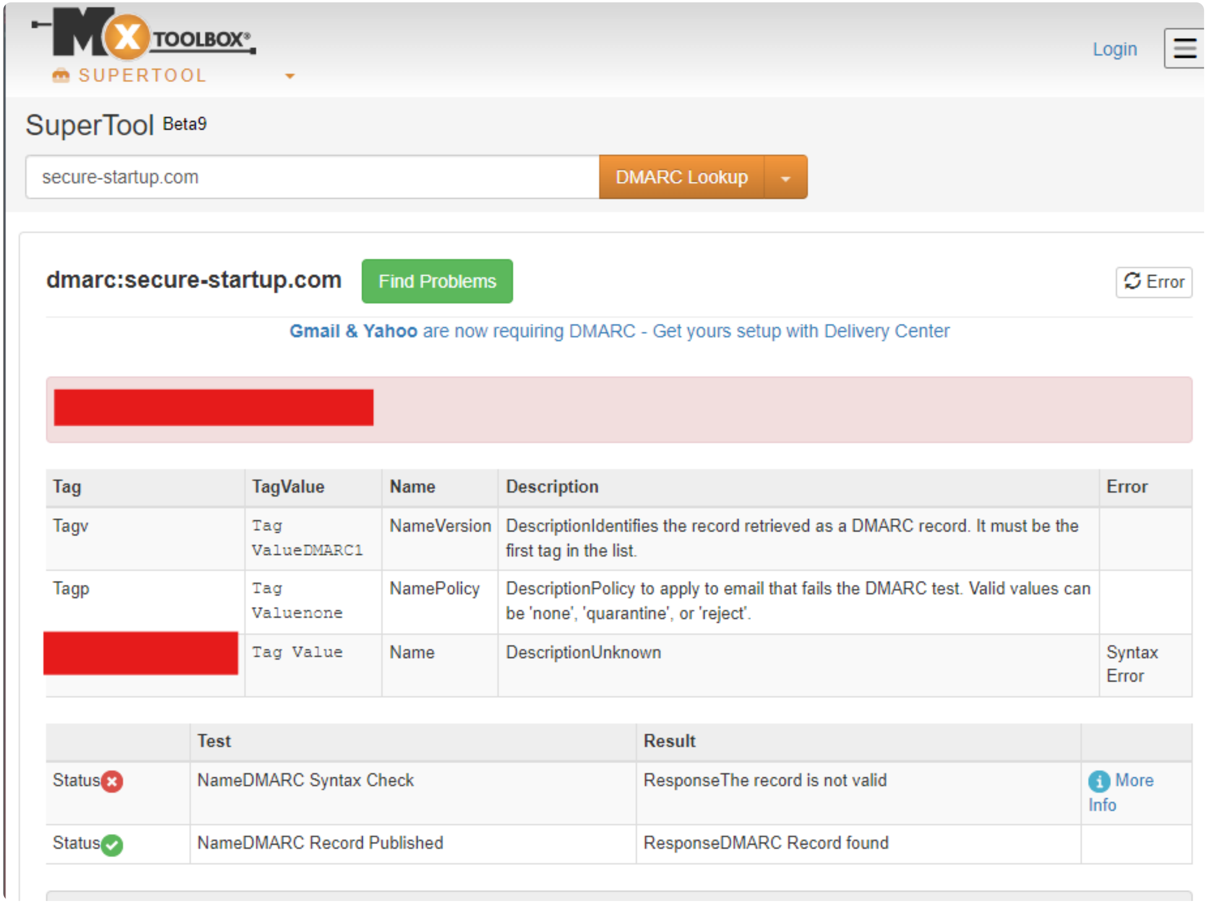
1. You can also use a tools and search for both of the flag
   https://mxtoolbox.com/supertool3?abt_id=AB-631B&abt_var=Variation



spf:secure-startup.com

[redacted]

Prefix	Type	Value	PrefixDesc	Description	Error
Prefix	Typev	Valuespf1	PrefixDesc	DescriptionThe SPF record version	
Prefix+	Typea	Value	PrefixDescPass	DescriptionMatch if IP has a DNS 'A' record in given domain.	
Prefix+	Typemx	Value	PrefixDescPass	DescriptionMatch if IP is one of the MX hosts for given domain name.	
Prefix?	Typeall	Value	PrefixDescNeutral	DescriptionAlways matches. It goes at the end of your record.	
Prefix-	Type	Value	PrefixDescFail	DescriptionUnknown	Syntax Error,Unknown mechanisms are not allowed
[redacted]	[redacted]	Value	PrefixDescPass	DescriptionUnknown	Unknown mechanisms are not allowed



dmarc:secure-startup.com

Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center

[redacted]

Tag	TagValue	Name	Description	Error
Tagv	Tag ValueDMARC1	NameVersion	DescriptionIdentifies the record retrieved as a DMARC record. It must be the first tag in the list.	
Tagp	Tag Valuenone	NamePolicy	DescriptionPolicy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.	
[redacted]	Tag Value	Name	DescriptionUnknown	Syntax Error

	Test	Result	
Status ✗	NameDMARC Syntax Check	ResponseThe record is not valid	ℹ More Info
Status ✓	NameDMARC Record Published	ResponseDMARC Record found	