VishwaCTF

CHALLENGE NAME : [Bounty Email]

DEV : [Samarth Ghante]

CATEGORY : [Forensics]

LEVEL : [MEDIUM]

2024

Description :-

We've received a tip from an alert netizen about a suspicious email related to a bounty. Your mission is to analyze the contents of this email and uncover any hidden information or clues that might help us identify the sender!

Interpretation:-

The question says about the spam email, and a ".eml" file has been provided! The challenge is of type, Forensics; Which means we have to analyze the email headers and find the sender of the mail!

Step1:

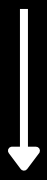
Open the file content in the email analyzer or any email header analyzer! (Optional) You can use a simple notepad too!
This will give you all the headers!

Headers Found

Header Name	Header Value
Delivered-To	samarthghante@vishwactf.com
X-Received	by 2002:a17:907:a08:b0:a27:48c6:28b3 with SMTP id bb8-20020a1709070a0800b00a2748c628b3mr4788154ejc.6.1704758579058; Mon, 08 Jan 2024 16:02:59 -0800 (PST)
ARC-Seal	i=2; a=rsa-sha256; t=1704758579; cv=pass; d=redhost.com; s=arc-20160816; b=h+bigwroSG/O2rqL0YDTx1QKNoNy0D5LAyBJnZXEOORZzWeB0DEYNYIWsNjtXHWU2h yrNGmM+X3TXrNz92+R6NyW7qtL LwfhZh/2xPkXLceMlVlsCPbUpCbhCjlmUMzA7M1l5t lqP9M0KrQlsJ9JA0caYE+8qDea4kT8mX20L1aRUzfvGt4NlnS975BW7B4yn7WL1xdB8W sgvk8bgvKXSPbA5fZOGS3P8Kax/bFklyLZNk5eEfOt4fM9Dg5E DPJHADWR/pByNfC7ER hcl4B5t52zQm88Lnhw2SWhVYMY2Fg6pNaZSrXk+Nw1hoVcCfXSQESpz5Esh5CI2mcHGR nwqQ==
ARC-Message-Signature	i=2; a=rsa-sha256; c=relaxed/relaxed; d=redhost.com; s=arc-20160816; h=mime-version:feedback-id:list-unsubscribe-post:list-unsubscribe :message-id:date:to:from:subject:cfbl-address:dkim-signature :dkim-signature:delivered-to; bh=YtPs2TqmFwBY88pmpe2LhPuDT6uW8Ap0aYJbnoKdfGc=; fh=XXghk4IevaA7G0+IpTbPBVecpYS65FPeYJPbpsHNP1A=; b=WhXQwcQaw/3hx0j7hVil0ecUjOOopE5XNYrjhupPdW GCBxW4zGILtlDHpxVYGhC6j4 PKPdQ5Wn/BkBJRSJ5kKkevr5jqfFTyAo0SeuQx9fma2rm5D1KsgxlycpQ3km1d+Pl2II cEEcqvp3nr0pY1VGFTmrVsni/HXqbvLe0ZQNj+hCVjkxBQlf0Zge+Pm94n1yuDNBhQE4 5saTBWPGheVXdSYVP2wZ8XTBL2wPmkiOtkyk5U5l8KtzGFpaDrllO97BpHJa2BnH7IWJ l4P+d5JBxCQxe6SsH5uhtAq3S8LZmxgDo6R+O7KFCyitreg6ZN+JyilvPkIOxrZtUpgl q07Q==
ARC-Authentication-Results	i=2; mx.365-micro-outlook.com; dkim=pass header.i=@inbound.redhost-7a-relay.com header.s=systemeio1 header.b=JAlYRLw5; dkim=pass header.i=@thecompleteonlinebusiness.com header.s=systemeio1 header.b="X/HTdDi/"; arc=pass (i=1 spf=pass spfdomain=si3273694.thecompleteonlinebusiness.com dkim=pass dkdomain=inbound.redhost-7a-relay.com dkim=pass dkdomain=thecompleteonlinebusiness.com); spf=pass (redhost.com: domain of vishwactf+caf_=samarthghante@vishwactf.com=vishwactf.com@vishwactf.com designates 209.85.220.41 as permitted sender) smtp.mailfrom="vishwactf+caf_=samarthghante@vishwactf.com=vishwactf.com@vishwactf.com"
Return-Path	<vishwactf+caf_=samarthghante@vishwactf.com=vishwactf.com@vishwactf.com>
Received-SPF	pass (redhost.com: domain of vishwactf+caf_=samarthghante@vishwactf.com=vishwactf.com@vishwactf.com designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results	relay.outlook.com; dkim=pass header.i=@inbound.redhost-7a-relay.com header.s=systemeio1 header.b=JAlYRLw5; dkim=pass header.i=@thecompleteonlinebusiness.com header.s=systemeio1 header.b="X/HTdDi/"; arc=pass (i=1 spf=pass spfdomain=si3273694.thecompleteonlinebusiness.com dkim=pass dkdomain=inbound.redhost-7a-relay.com dkim=pass dkdomain=thecompleteonlinebusiness.com); spf=pass

From	Moo Toba <moo@thecompleteonlinebusiness.com>

You may think the “from” header is a lead in this challenge but its not, cause as it is a spam email; The From section can be spoofed.

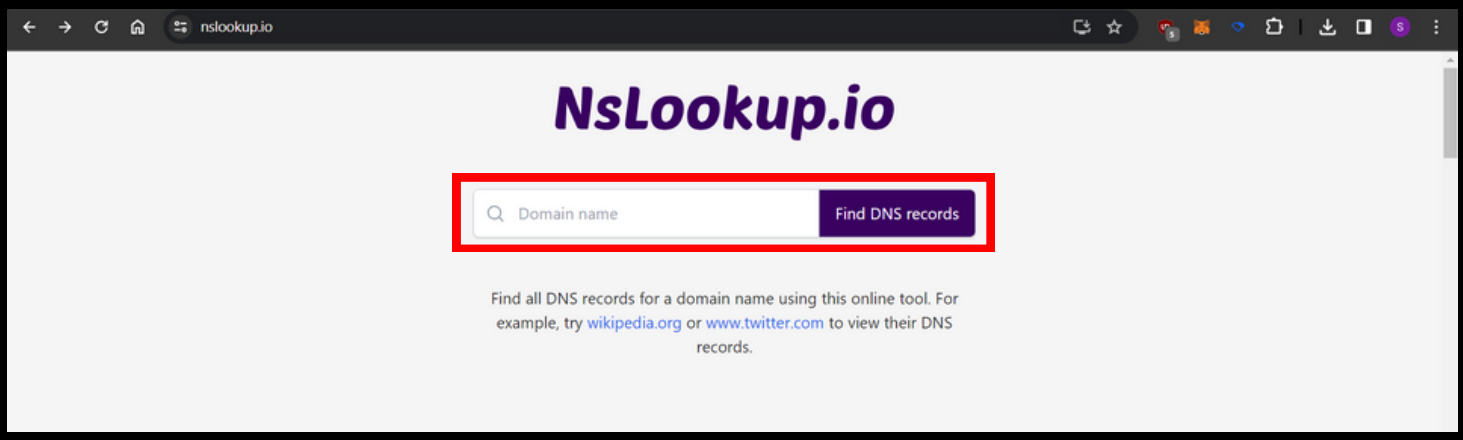


There is a “X-mailer” tag which is having a domain name as a value. “Mailer” signifies the sender or the mailer, which is asked in the challenge!

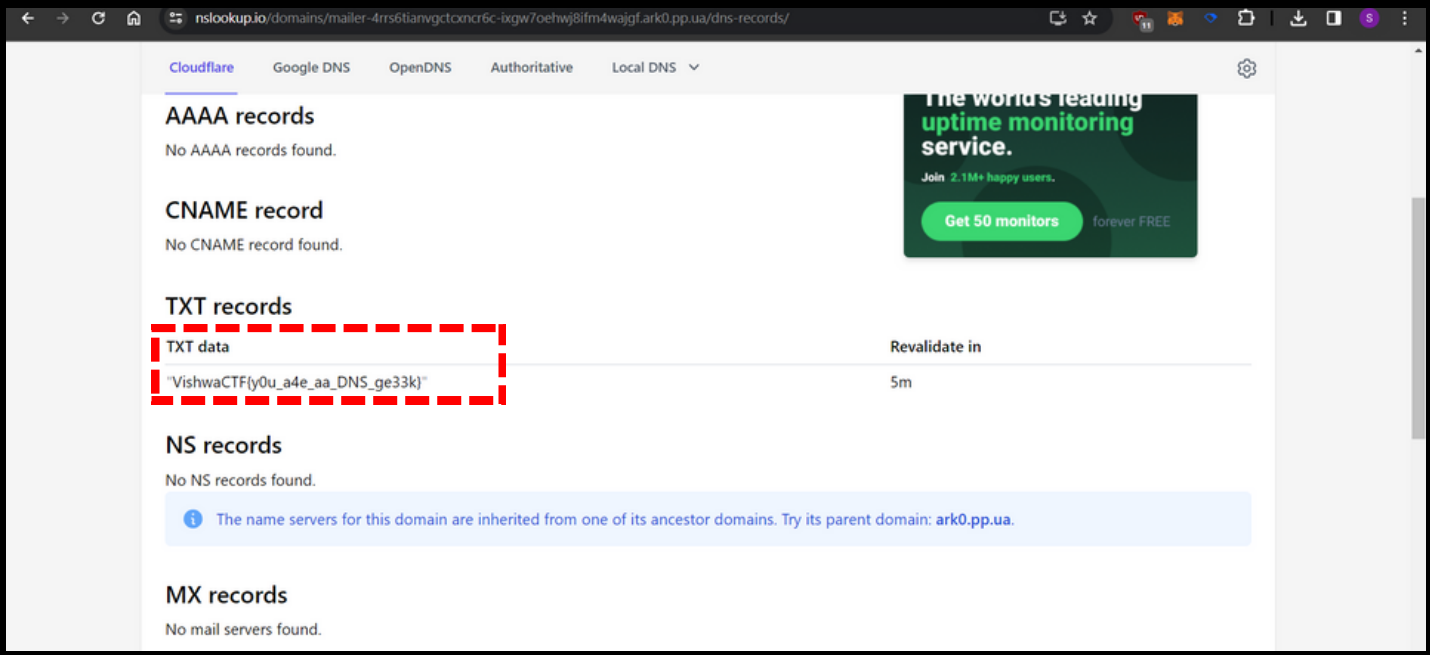
X-mailer	mailer-4rrs6tianvgctcxncr6c-ixgw7oehwj8ifm4wajgf.ark0.pp.ua

Step 2:

Run the DNS Lookup
for the domain to find the DNS Records!



You will get the flag as TXT Record for that domain!



You can also get the DNS Records using Dig Command or NMAP Scan in Linux!

```
root@main-backend:/home/azure# dig mailer-4rrsótianvgctcxncr6c-ixgw7oehwj8ifm4wajgf.ark0.pp.ua txt

; <<>> DiG 9.16.44-Debian <<>> mailer-4rrsótianvgctcxncr6c-ixgw7oehwj8ifm4wajgf.ark0.pp.ua txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25804
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1224
;; QUESTION SECTION:
;mailer-4rrsótianvgctcxncr6c-ixgw7oehwj8ifm4wajgf.ark0.pp.ua. IN        TXT

;; ANSWER SECTION:
mailer-4rrsótianvgctcxncr6c-ixgw7oehwj8ifm4wajgf.ark0.pp.ua. 299 IN TXT "VishwaCTF{y0u_a4e_aa_DNS_ge33k}"

;; Query time: 424 msec
;; SERVER: 168.63.129.16#53(168.63.129.16)
;; WHEN: Thu Feb 08 09:08:26 UTC 2024
;; MSG SIZE  rcvd: 132
```

Thank You!

Samarth Ghante