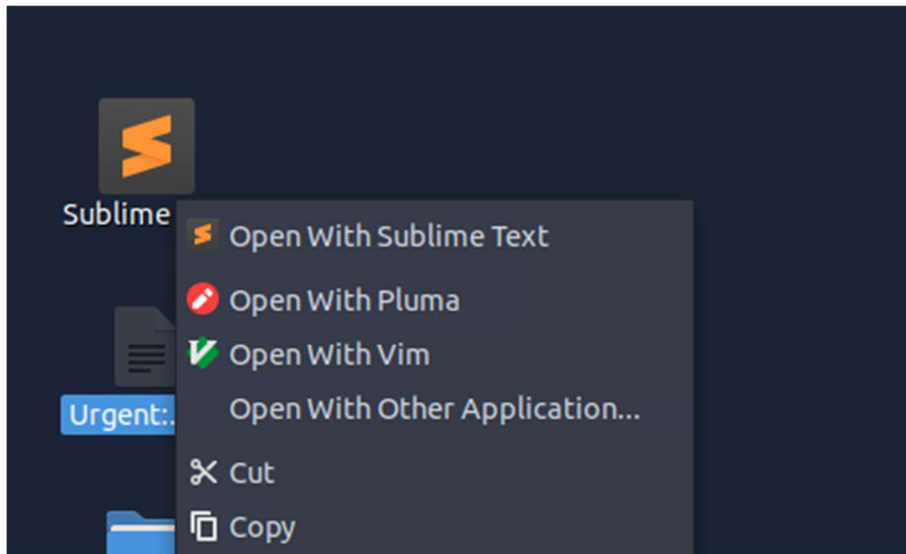


Attack Box POV



After opening

```
~/Desktop/Urgent.eml - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
Urgent.eml x
1 X-Pm-Content-Encryption: end-to-end
2 X-Pm-Origin: internal
3 Subject: Urgent: Blue section is down. Switch to the load share plan!
4 From: Chief Elf <chief.elf@santaclaus.thm>
5 Date: Tue, 6 Dec 2022 00:00:01 +0000
6 Mime-Version: 1.0
7 Content-Type: multipart/mixed;boundary=-----03edd9c682a0c8f60d54b9e4bb86659f
8 To: elves.all@santaclaus.thm <elves.all@santaclaus.thm>
9 X-Attached: Division of labour-Load share plan.doc
10 Message-Id: <QW9DMjAyML9FbWZpY3VsdGllcyBwcmVwYXJpYmNpdj48c3BhbG9e4bb86659f>
11 X-Pm-Spamscore: 3
12 Received: from mail.santaclaus.thm by mail.santaclaus.thm; Tue, 6 Dec 2022 00:00:01 +0000
13 X-Original-To: elves.all@santaclaus.thm
14 Return-Path: <murphy.evident@bandityeti.thm>
15 Delivered-To: elves.all@santaclaus.thm
16
17 -----03edd9c682a0c8f60d54b9e4bb86659f
18 Content-Type: multipart/
related;boundary=-----8f117c48beda7f1c1da0a5a894d5c4b5
19
20 -----8f117c48beda7f1c1da0a5a894d5c4b5
21 Content-Type: text/html;charset=utf-8
22 Content-Transfer-Encoding: base64
23
24 PHNwYW4+RGVhZlBhZlZlcyw8L3NwYW4+PGRpdj48YnI+PC9kaXY+PGRpdj48c3BhbG9e4bb86659f
25 dGVjaG5pY2FsIHByb2JsZW1zIGluIHRoZSBibHVLIHNLy3Rpb24gb2Ygb3VyIHRveSBmYWN0b3J5
26 LCB3ZSBhcmUgaGF2aW5nIGRpdj48YnI+PC9kaXY+PGRpdj48c3BhbG9e4bb86659f
27 PC9kaXY+PGRpdj48YnI+PC9kaXY+PGRpdj48c3BhbG9e4bb86659f
28 dCB0byB0aHJpc3RtYXMsIHVhZlZlcyw8L3NwYW4+PGRpdj48YnI+PC9kaXY+PGRpdj48c3BhbG9e4bb86659f
29 ZXBhcmUgaGF2aW5nIGRpdj48YnI+PC9kaXY+PGRpdj48c3BhbG9e4bb86659f
30 Y3Rpb24ncyAKd29ya2xvYWQgaXNpdj48YnI+PC9kaXY+PGRpdj48c3BhbG9e4bb86659f
31 eSBwcm9kdWN0aW9uIGRlbgF5Ljwvc3BhbG9e4bb86659f
32 PLRoZSBkZXRoawxlZCBkaXZpc2l2b3VzIGluIHRoZSBibHVLIHNLy3Rpb24gb2Ygb3VyIHRveSBmYWN0b3J5
33 aGVkIGRvY3VtZW50Ljwvc3BhbG9e4bb86659f
34 bHVjayB0byB5b3UgYXNpdj48YnI+PC9kaXY+PGRpdj48c3BhbG9e4bb86659f
35 PKNoaWVmIEVsZjwvc3BhbG9e4bb86659f
36 -----8f117c48beda7f1c1da0a5a894d5c4b5-----
37 -----03edd9c682a0c8f60d54b9e4bb86659f
38 Content-Type: application/msword; filename="Division of labour-Load share plan.doc";
name="Division of labour-Load share plan.doc"
39 Content-Transfer-Encoding: base64
40
```

What is the email address of the sender?

chief.elf@santaclaus.thm

✓ Correct Answer

What is the return address?

murphy.evident@bandityeti.thm

✓ Correct Answer

On whose behalf was the email sent?

Chief Elf

✓ Correct Answer

What is the X-spam score?

3

✓ Correct Answer

All this questions answers can be found on the screenshot

Message-Id.....<QW9DMjAyMl9FbWFpbF9BbmFseXNpcw==>

change that value using Base64 decoder

What is hidden in the value of the Message-ID field?

AoC2022_Email_Analysis

✓ Correct Answer

