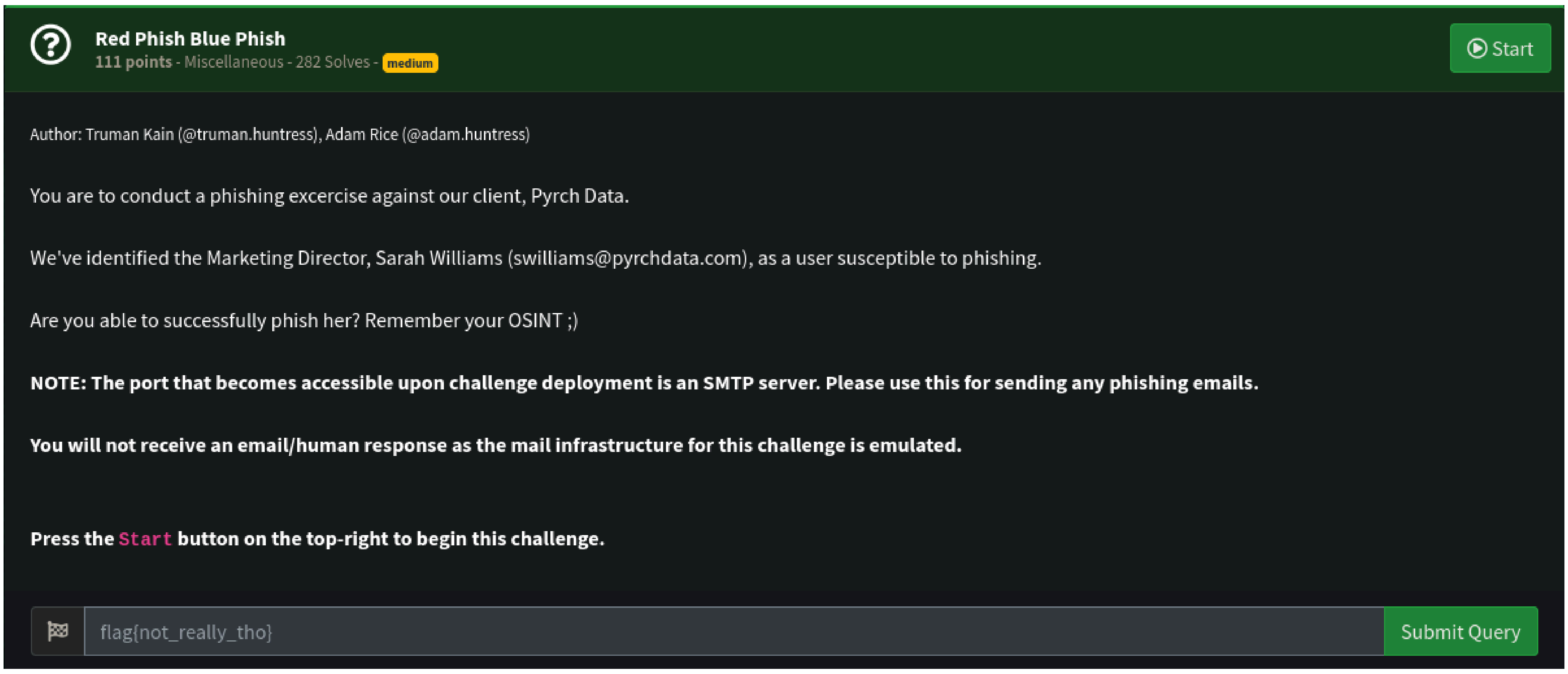
# Red Phish Blue Phish Challenge



**Red Phish Blue Phish**
111 points - Miscellaneous - 282 Solves - medium

Author: Truman Kain (@truman.huntress), Adam Rice (@adam.huntress)

You are to conduct a phishing excercise against our client, Pyrch Data.

We've identified the Marketing Director, Sarah Williams (swilliams@pyrchdata.com), as a user susceptible to phishing.

Are you able to successfully phish her? Remember your OSINT ;)

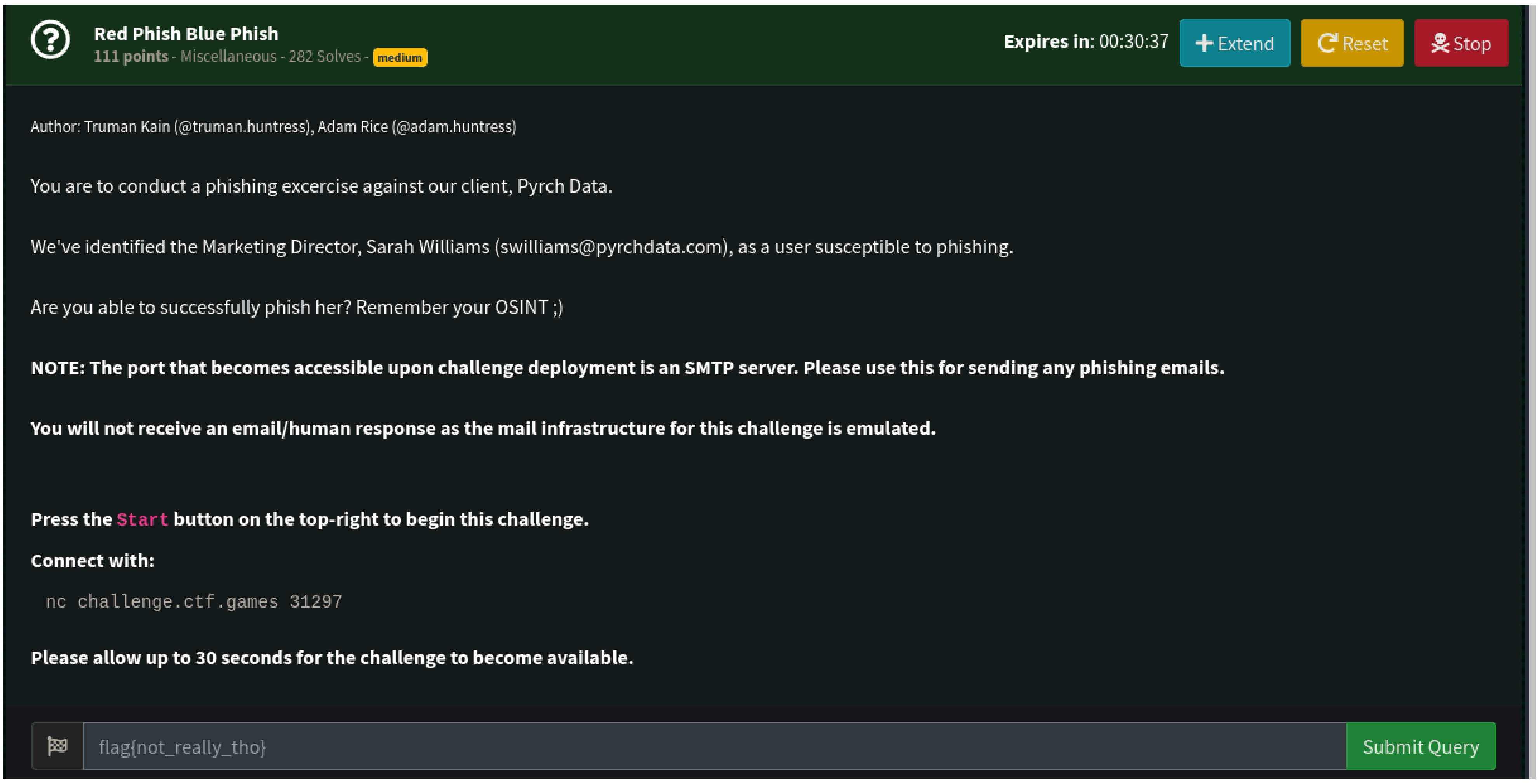
**NOTE: The port that becomes accessible upon challenge deployment is an SMTP server. Please use this for sending any phishing emails.**

**You will not receive an email/human response as the mail infrastructure for this challenge is emulated.**

**Press the `Start` button on the top-right to begin this challenge.**

flag{not_really_tho}

Reading the instructions and hints of the challenge, we can see that this will be an SMTP server we are working with. We are given the netcat command to utilize when we start the machine. This will connect us to the the SMTP server.



**Red Phish Blue Phish**
111 points - Miscellaneous - 282 Solves - medium

**Expires in:** 00:30:37

Author: Truman Kain (@truman.huntress), Adam Rice (@adam.huntress)

You are to conduct a phishing excercise against our client, Pyrch Data.

We've identified the Marketing Director, Sarah Williams (swilliams@pyrchdata.com), as a user susceptible to phishing.

Are you able to successfully phish her? Remember your OSINT ;)

**NOTE: The port that becomes accessible upon challenge deployment is an SMTP server. Please use this for sending any phishing emails.**

**You will not receive an email/human response as the mail infrastructure for this challenge is emulated.**

**Press the `Start` button on the top-right to begin this challenge.**

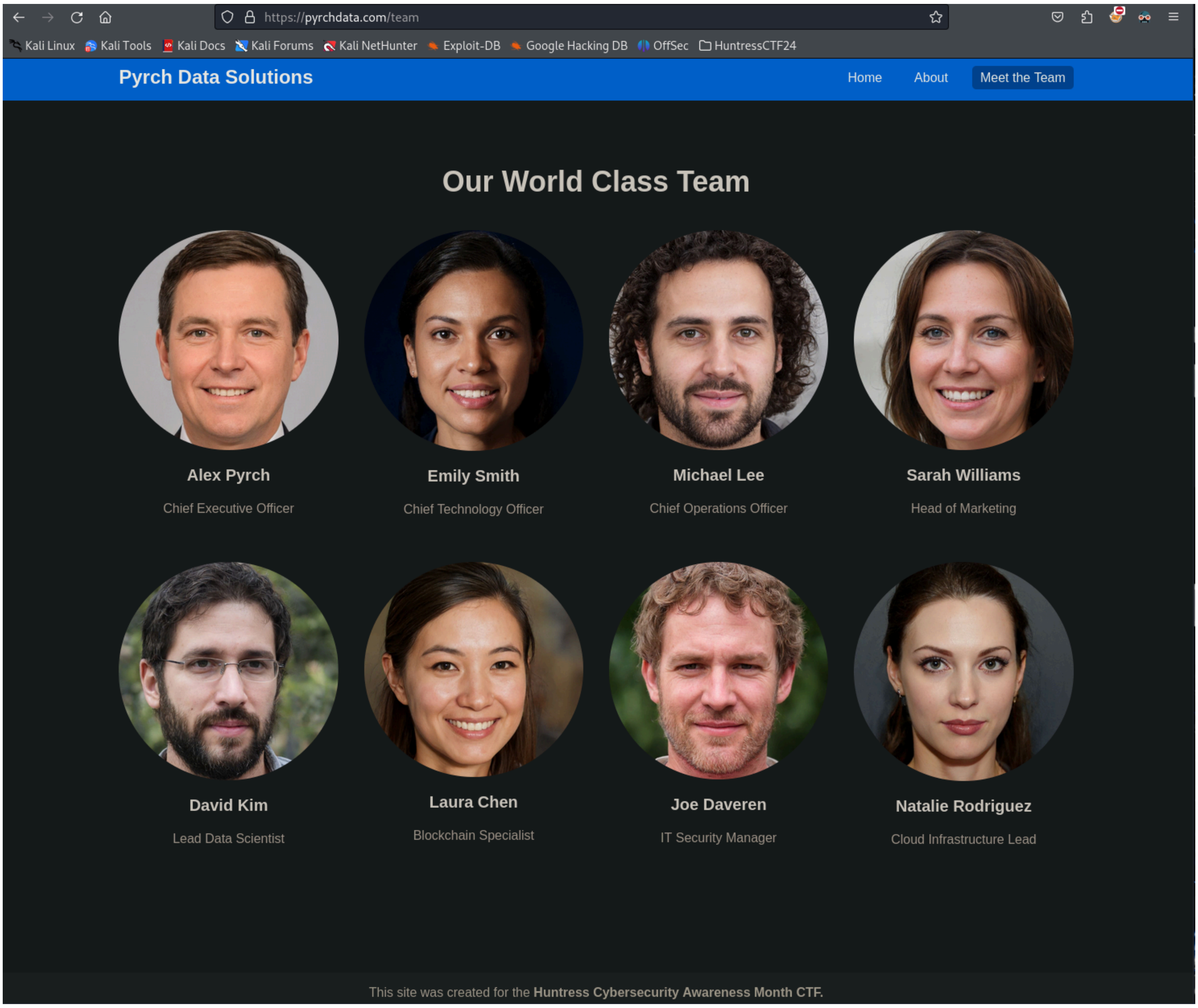
**Connect with:**

```
nc challenge.ctf.games 31297
```

**Please allow up to 30 seconds for the challenge to become available.**

flag{not_really_tho}

We receive the syntax "nc challenge.ctf.games 31297" for this instance created. The challenge also mentions "Remember your OSINT ;)" So we should use OSINT techniques to research the company the phishing attempt is targeting. Searching the name given of the target company and employee we find a web page for the target.



Pyrch Data Solutions

Our World Class Team

Alex Pyrch
Chief Executive Officer

Emily Smith
Chief Technology Officer

Michael Lee
Chief Operations Officer

Sarah Williams
Head of Marketing

David Kim
Lead Data Scientist

Laura Chen
Blockchain Specialist

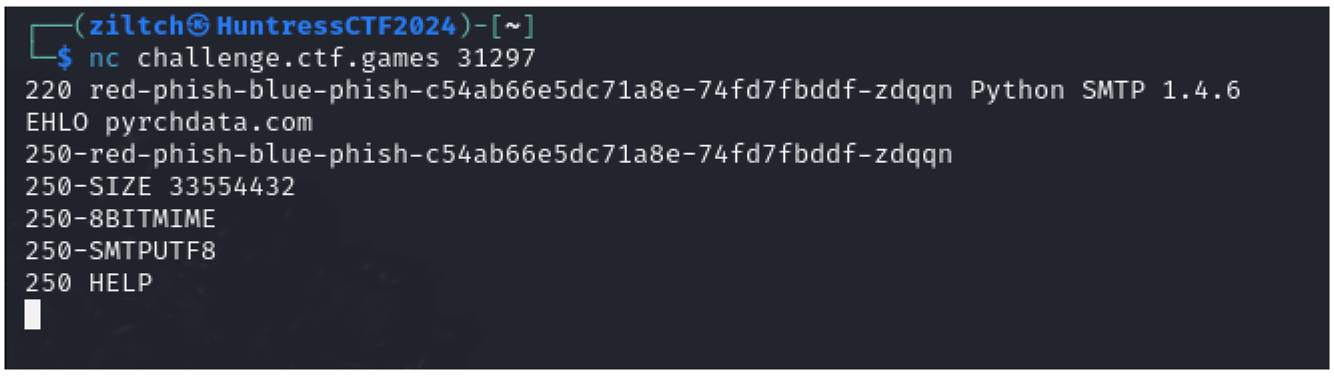
Joe Daveren
IT Security Manager

Natalie Rodriguez
Cloud Infrastructure Lead

This site was created for the **Huntress Cybersecurity Awareness Month CTF.**

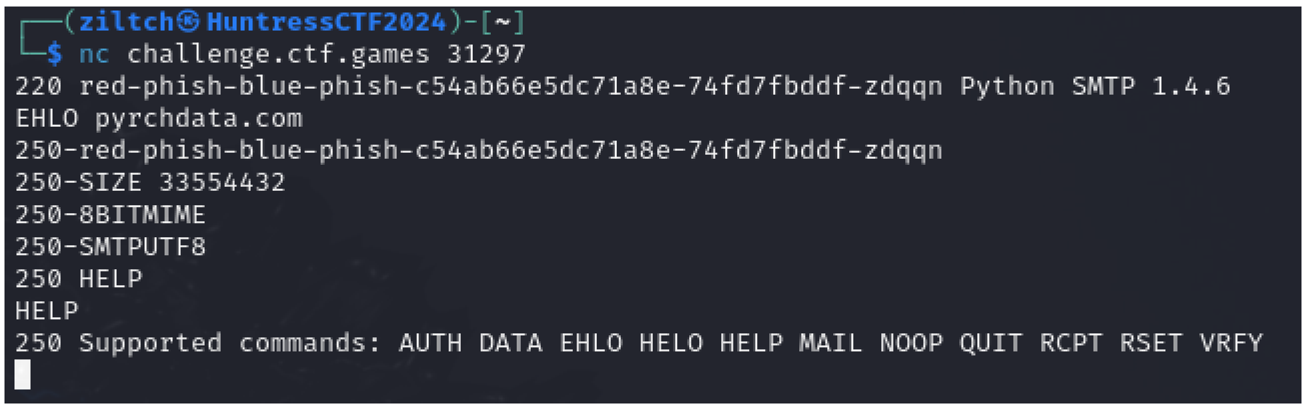
Note: seems that the person that would be most trusted for anything related to IT within the company would be, Joe Daveren.

We will attempt to use the given info and the OSINT obtained info in order to send a phishing email. Using the EHLO command we get a reach back from the server.



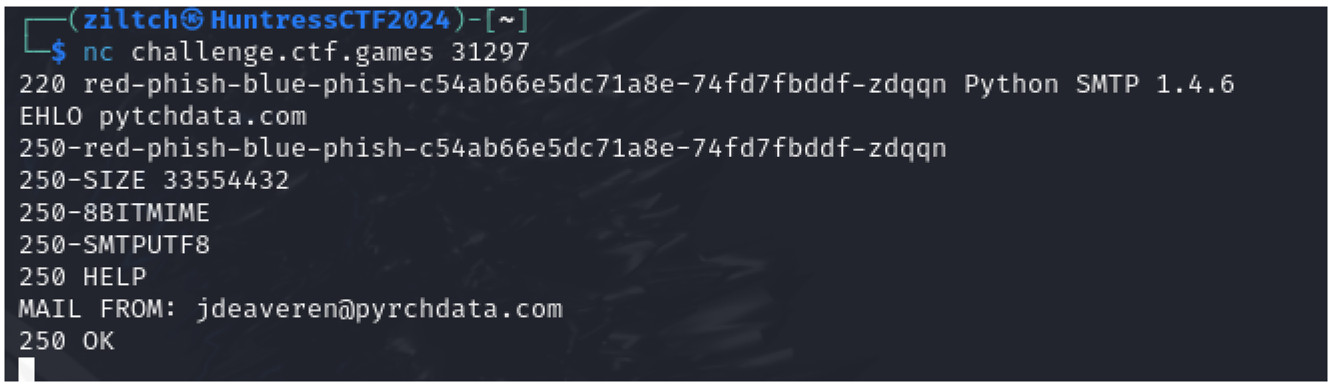
```
┌──(ziltch㉿HuntressCTF2024)-[~]
└─$ nc challenge.ctf.games 31297
220 red-phish-blue-phish-c54ab66e5dc71a8e-74fd7fbddf-zdqqn Python SMTP 1.4.6
EHLO pyrchdata.com
250-red-phish-blue-phish-c54ab66e5dc71a8e-74fd7fbddf-zdqqn
250-SIZE 33554432
250-8BITMIME
250-SMTPUTF8
250 HELP
```

Typing the command HELP gives us what commands are accepted in this server.



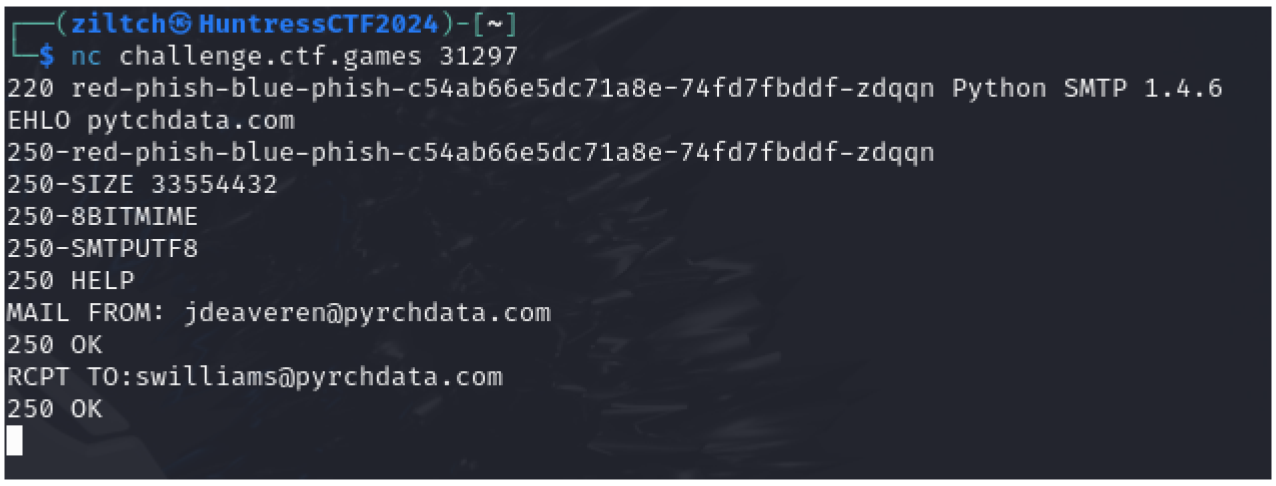
```
┌──(ziltch㉿HuntressCTF2024)-[~]
└─$ nc challenge.ctf.games 31297
220 red-phish-blue-phish-c54ab66e5dc71a8e-74fd7fbddf-zdqqn Python SMTP 1.4.6
EHLO pyrchdata.com
250-red-phish-blue-phish-c54ab66e5dc71a8e-74fd7fbddf-zdqqn
250-SIZE 33554432
250-8BITMIME
250-SMTPUTF8
250 HELP
HELP
250 Supported commands: AUTH DATA EHLO HELO HELP MAIL NOOP QUIT RCPT RSET VRFY
```

Now we will use the IT security managers name and use the same format of the username that is susceptible to phishing, we can start to construct our email. Using the command "MAIL TO:"



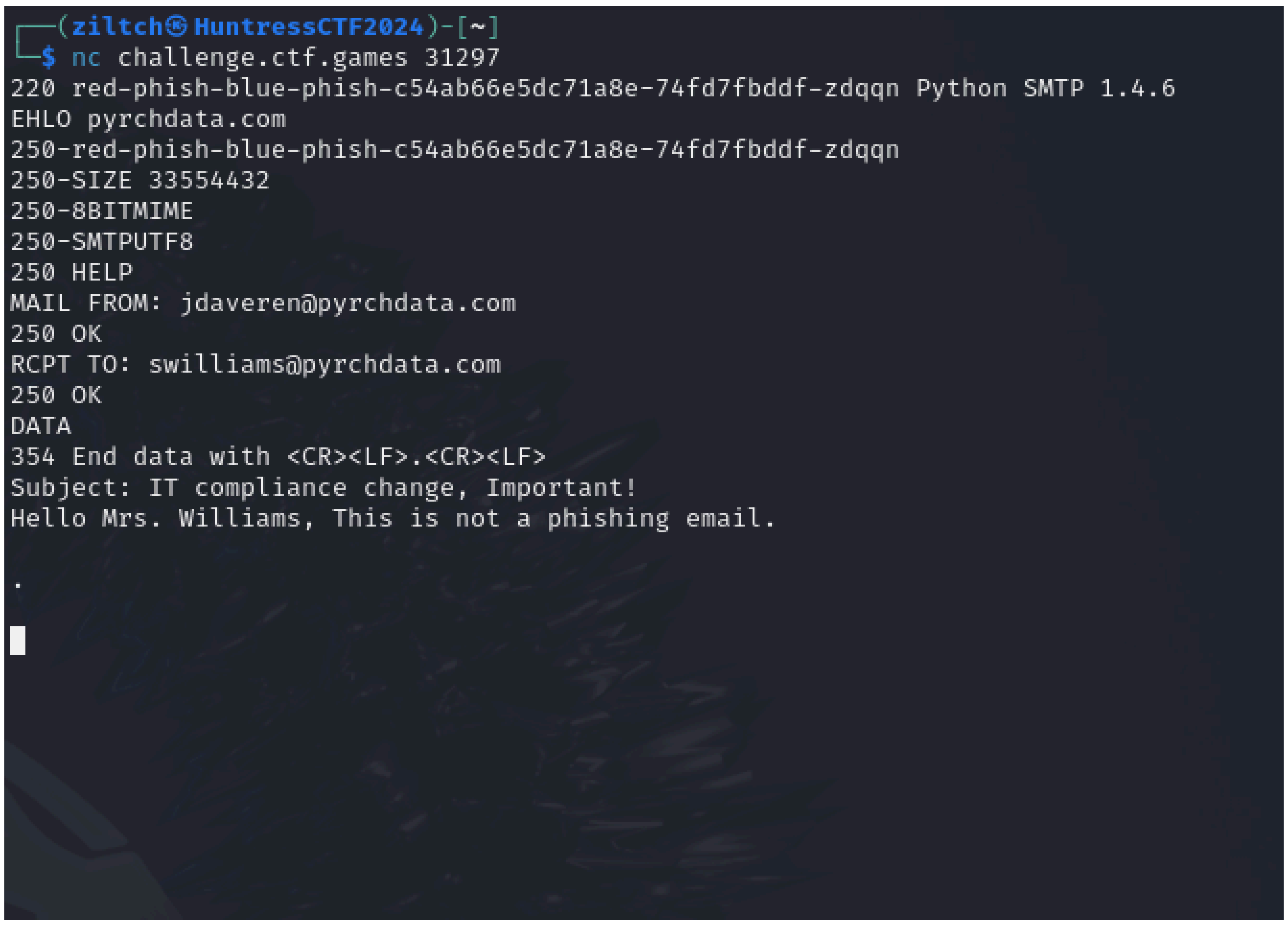
```
┌──(ziltch㉿HuntressCTF2024)-[~]
└─$ nc challenge.ctf.games 31297
220 red-phish-blue-phish-c54ab66e5dc71a8e-74fd7fbddf-zdqqn Python SMTP 1.4.6
EHLO pytchdata.com
250-red-phish-blue-phish-c54ab66e5dc71a8e-74fd7fbddf-zdqqn
250-SIZE 33554432
250-8BITMIME
250-SMTPUTF8
250 HELP
MAIL FROM: jdeaveren@pyrchdata.com
250 OK
```

We can now us the "RCPT TO" command to add the recipient.



```
┌──(ziltch㉿HuntressCTF2024)-[~]
└─$ nc challenge.ctf.games 31297
220 red-phish-blue-phish-c54ab66e5dc71a8e-74fd7fbddf-zdqqn Python SMTP 1.4.6
EHLO pytchdata.com
250-red-phish-blue-phish-c54ab66e5dc71a8e-74fd7fbddf-zdqqn
250-SIZE 33554432
250-8BITMIME
250-SMTPUTF8
250 HELP
MAIL FROM: jdeaveren@pyrchdata.com
250 OK
RCPT TO:swilliams@pyrchdata.com
250 OK
```

Finishing up with the subject and body of the email. Using the given username susceptible to phishing and the given Netcat syntax, we are unable to send the SMTP mail due to the shell capability. The mail should send using a "." one a separate line at the bottom of the mail to be sent. This should exit the mail editing format of the DATA section and send the mail to the recipient.

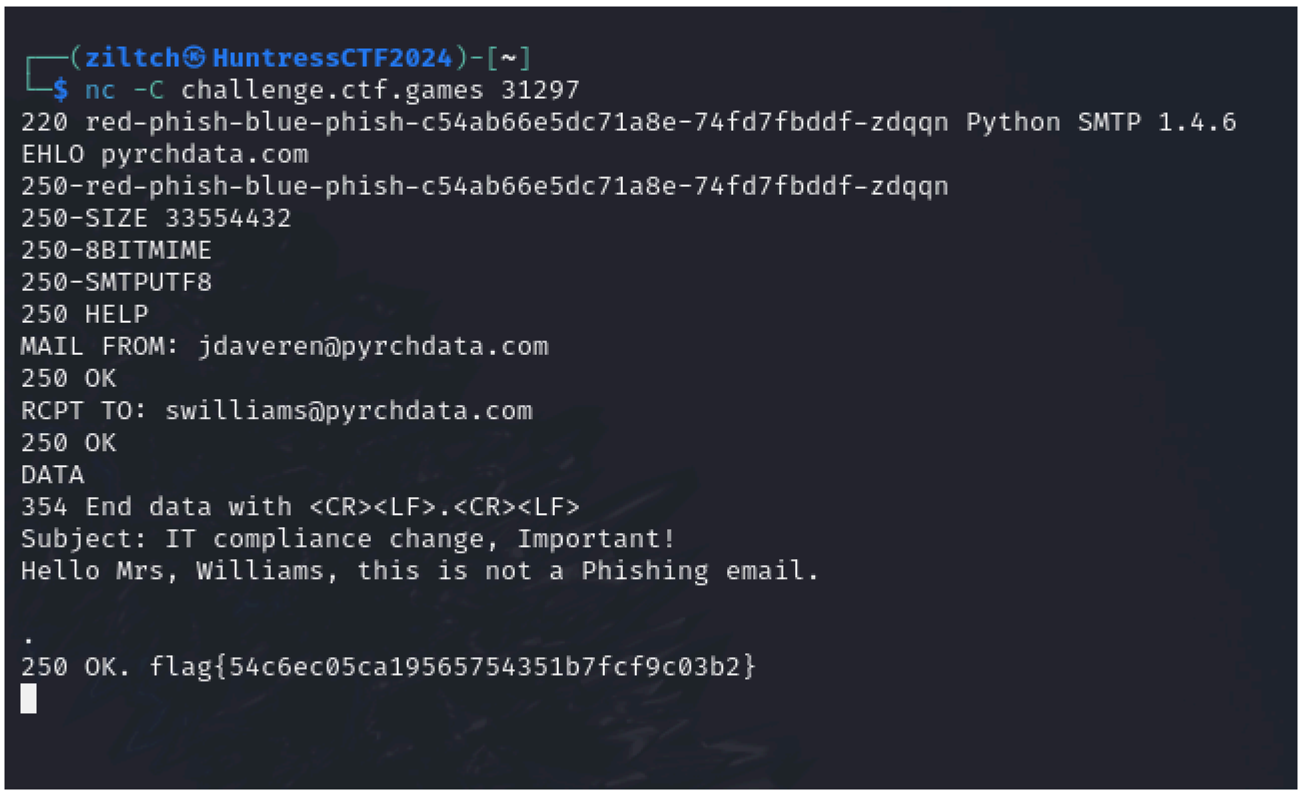


```
┌──(ziltch㉿HuntressCTF2024)-[~]
└─$ nc challenge.ctf.games 31297
220 red-phish-blue-phish-c54ab66e5dc71a8e-74fd7fbddf-zdqqn Python SMTP 1.4.6
EHLO pyrchdata.com
250-red-phish-blue-phish-c54ab66e5dc71a8e-74fd7fbddf-zdqqn
250-SIZE 33554432
250-8BITMIME
250-SMTPUTF8
250 HELP
MAIL FROM: jdaveren@pyrchdata.com
250 OK
RCPT TO: swilliams@pyrchdata.com
250 OK
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: IT compliance change, Important!
Hello Mrs. Williams, This is not a phishing email.

.
```

NOTE: Unfortunately this does not work as intended due to the weak shell.

Upon further research I am informed that you can use the "-C" tack in the Netcat command. This triggers the "." and return as the way of completing the mail data entry. So repeating the same steps but using "-C" we are able to send the mail and get a return with the flag.



```
┌──(ziltch㉿HuntressCTF2024)-[~]
└─$ nc -C challenge.ctf.games 31297
220 red-phish-blue-phish-c54ab66e5dc71a8e-74fd7fbddf-zdqqn Python SMTP 1.4.6
EHLO pyrchdata.com
250-red-phish-blue-phish-c54ab66e5dc71a8e-74fd7fbddf-zdqqn
250-SIZE 33554432
250-8BITMIME
250-SMTPUTF8
250 HELP
MAIL FROM: jdaveren@pyrchdata.com
250 OK
RCPT TO: swilliams@pyrchdata.com
250 OK
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: IT compliance change, Important!
Hello Mrs, Williams, this is not a Phishing email.

.
250 OK. flag{54c6ec05ca19565754351b7fcf9c03b2}
```

flag{54c6ec05ca19565754351b7fcf9c03b2}