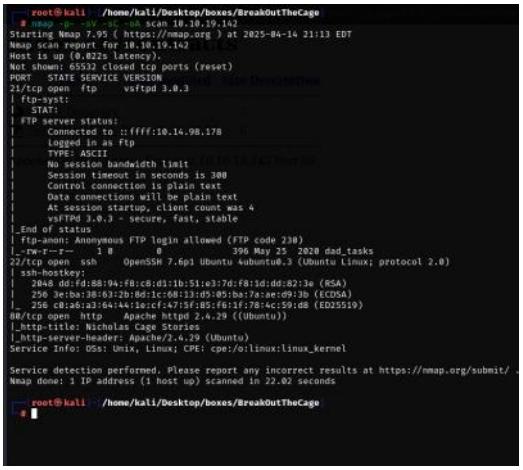
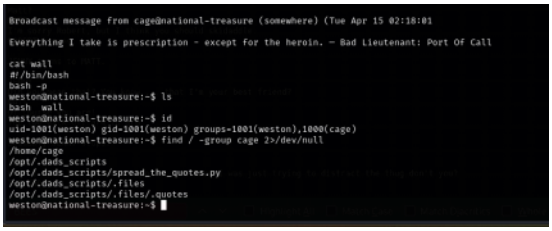
We began by running an nmap scan and discovered that ports **21 (FTP)**, **22 (SSH)**, and **80 (HTTP)** were open.



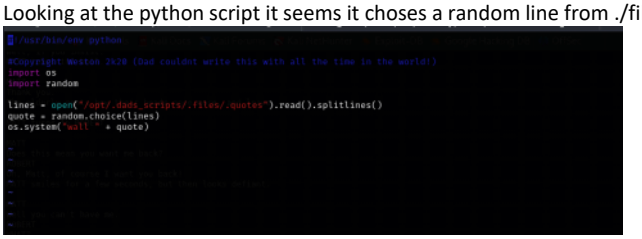
FTP allowed **anonymous login**. Inside was a file called dad_tasks containing **base64-encoded text**. After decoding, the output was a **ciphered message**. I tried **Caesar cipher** without success, but **Vigenère cipher** worked and gave me **Weston's password**.

Logged in as **weston**. Found that /usr/bin/bees could be run as **root**, but it just sent broadcast messages — a **rabbit hole**.

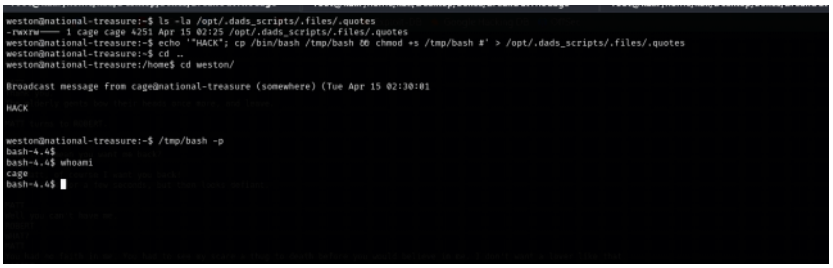
I noticed **broadcast messages** appearing every few minutes. After some digging, I found that **cage** was the user sending them. I searched for files writable by the **cage** group and found /opt/.dads_scripts/spread_the_quotes.py, which sends random lines from .quotes using wall.



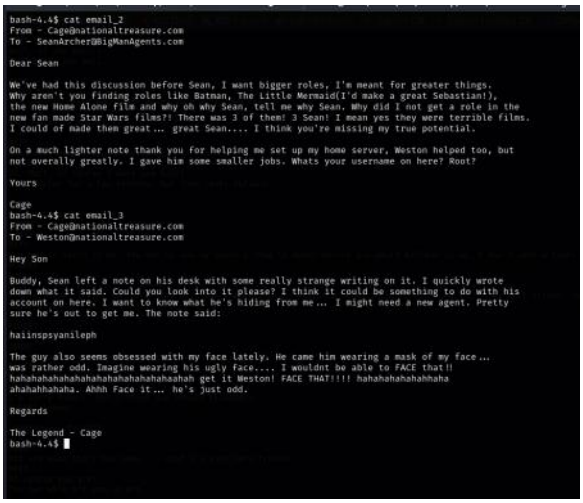
Looking at the python script it seems it choses a random line from ./file./quates and broadcast it



The .quotes file was **group-writable**, and Weston was in the **cage** group. I modified the file to include a payload that creates a **SUID shell**. After a short wait, I used /tmp/bash -p to become **cage**.



In **cage's home directory**, I found emails. One mentioned Sean left a strange note: haiinspsyanileph. Another hinted Sean's username might be **root**.
I tried many ways to decrypt the note. Eventually, after checking a write-up, I learned it was a **Vigenère cipher** with the key **"face"** — hinted by the joke "FACE THAT!!!". Decrypting gave the **root password**, and I used it to get the **final flag**.




VIGENERE CIPHER
Cryptography · Poly-Alphabetic Cipher · Vigenere Cipher
VIGENERE DECODER
VIGENERE CIPHERTEXT
PARAMETERS
PLAINTEXT LANGUAGE: English
ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ
AUTOMATIC DECRYPTION
DECRYPTION METHOD
KNOWING THE KEY/PASSWORD: FACE
KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3
KNOWING ONLY A PARTIAL KEY: KE?
KNOWING A PLAINTEXT WORD: CODE
VIGENERE CRYPTANALYSIS (KASISKI'S TEST)
DECRYPT
See also: Beaufort Cipher – Caesar Cipher
VIGENERE ENCODER
VIGENERE PLAIN TEXT
stheonessintedli
CIPHER KEY: KEY
ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ
PRESERVE PUNCTUATION
ENCRYPT
See also: Beaufort Cipher – Autoclave Cipher – Caesar Cipher
Summary
Vigenere Decoder
Vigenere Encoder
What is the Vigenere cipher? (Definition)
How to encrypt using Vigenere cipher?
How to decrypt Vigenere cipher?
How to recognize Vigenere ciphertext?
How to break Vigenere without knowing the key?
How to find the key when having both cipher and plaintext?
What are the variants of the Vigenere cipher?
How to choose the encryption key?
What is the running key vigenere cipher?
What is the keyed vigenere cipher?
What are the advantages of the Vigenere cipher versus Caesar Cipher?
What is a Saint-Cyr slide?
Why the name Vigenere?
When Vigenere was invented?
Similar pages
Beaufort Cipher
Search for a tool
SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'boolean'
BROWSE THE FULL DCODE TOOLS' LIST
Results
FACE
Vigenere Cipher - dCode
Tag(s) : Poly-Alphabetic Cipher
Share
dCode and more
dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? Write to dCode!
Feedback


root@national-treasure: ~/email_backup
root@kali: /home/kali/Desktop/boxes/BreakOutTheCage
root@kali: /home/kali/Desktop/boxes/BreakOutTheCage
bash-4.4$ su root
Password:
root@national-treasure:/home/cage/email_backup# cat /root/
.bash_history .bashrc .cache/ email_backup/ .gnupg/ .local/ .profile .ssh/ .vim/ .viminfo
root@national-treasure:/home/cage/email_backup# cd /root/email_backup/
root@national-treasure:~/email_backup# ls
email_1 email_2
root@national-treasure:~/email_backup# cat email_2
From - master@ActorsGuild.com
To - SeanArcher@BigManAgents.com
Dear Sean
I'm very pleased to here that Sean, you are a good disciple. Your power over him has become
strong... so strong that I feel the power to promote you from disciple to crony. I hope you
don't abuse your new found strength. To ascend yourself to this level please use this code:
Thank you
Sean Archer
root@national-treasure:~/email_backup#