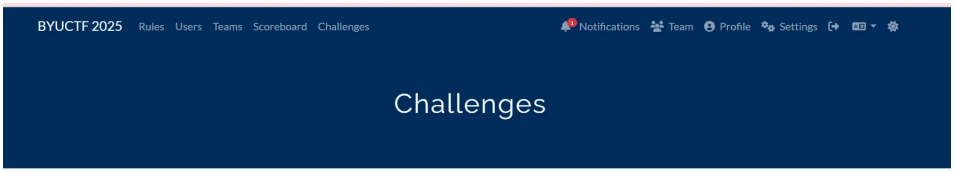
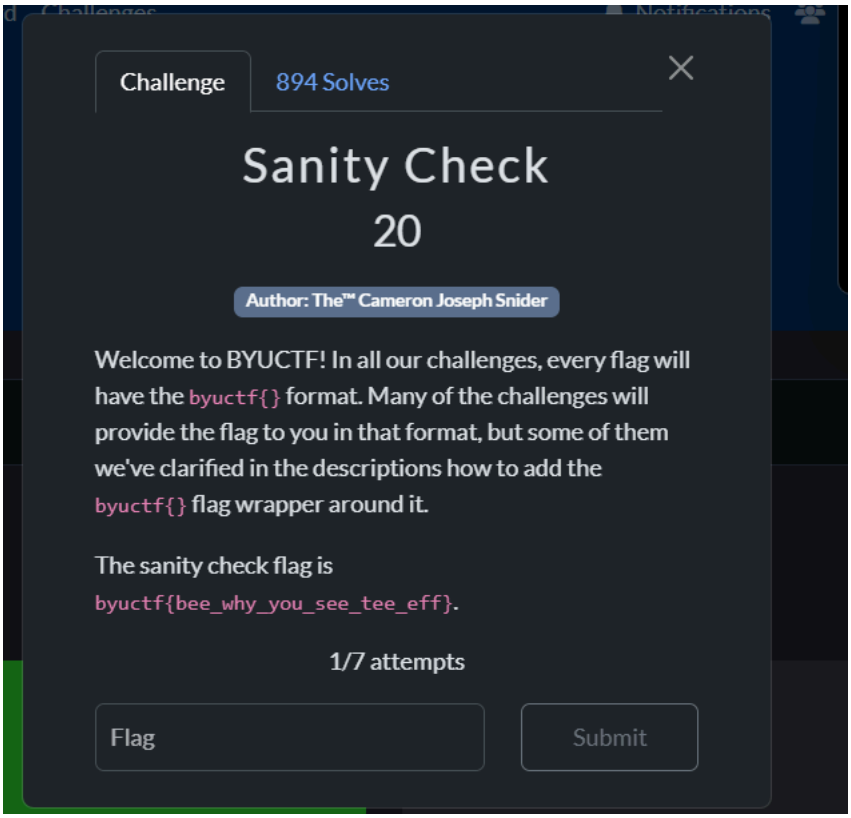
BYUCTF 2025

BYUCTF 2025 Writeup

This is a writeup of challenges from BYUCTF 2025, including solutions for various categories such as Forensics and OSINT. I completed some of all challenges .

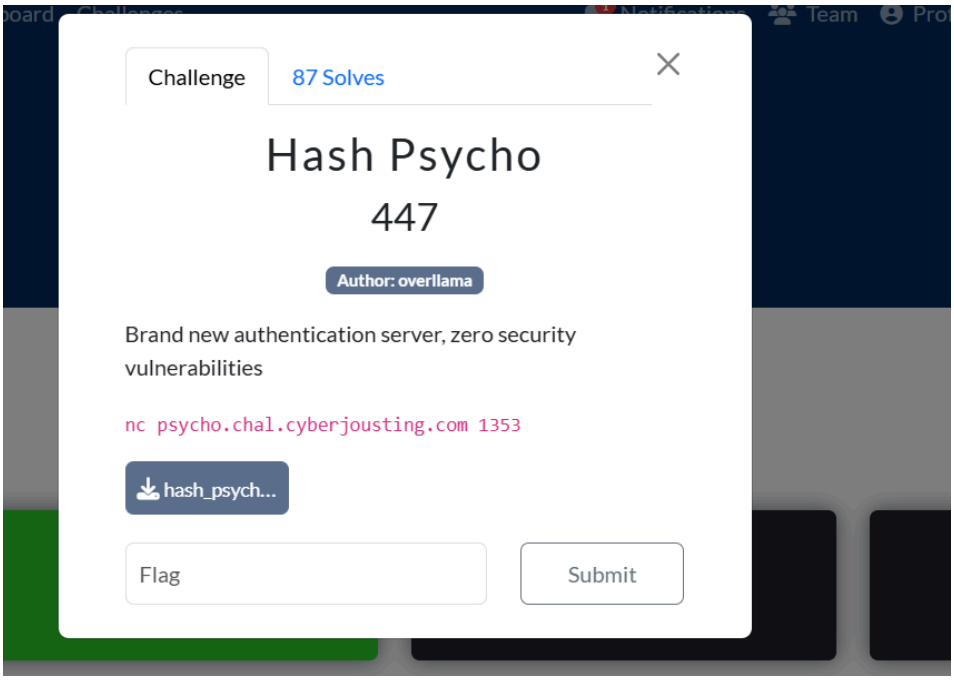
In this event, Misc included 4 challenges. The first challenge was only a test of flag format. I skipped this easy challenge.



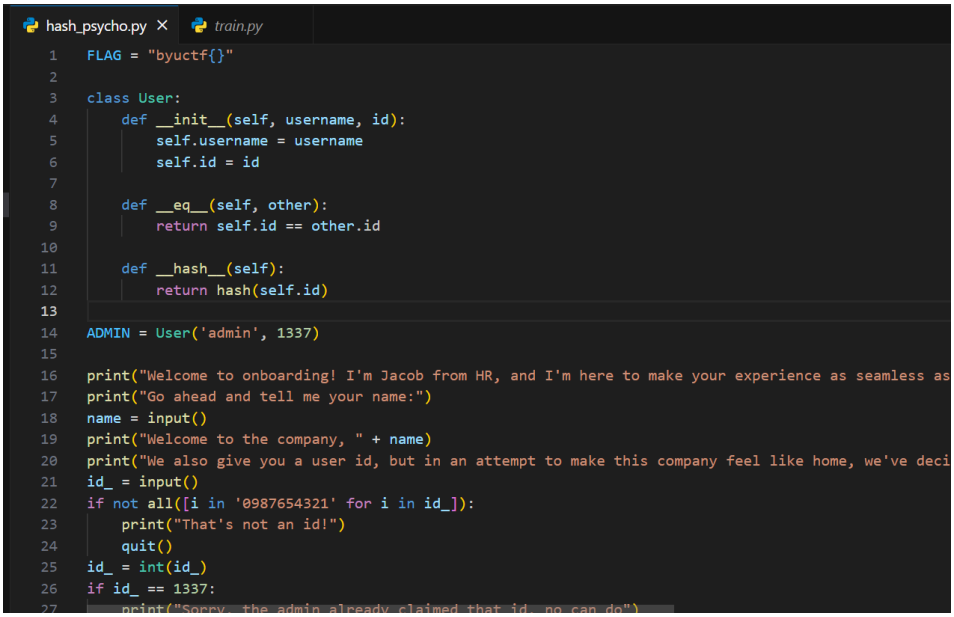


Hash Psycho

- I was provided file from challenges and command **“nc psycho.chal.cyberjousting.com 1353” .** Therefore, I am thinking to use kali for this command .
- First, I will open file by VScode to see content in it .



- In source code , I can see it conduct to create a format flag if input is valid .



- I observed condition IF-Else in end of code , so if i want get a correct flag, I have a choose==2 and YOURUSER.id != 1337

```
if hash(YOURUSER) == hash(ADMIN):
    print(FLAG)
    quit()
```

```python
id_ = int(id_)
if id_ == 1337:
    print("Sorry, the admin already claimed that id, no can do")
    quit()
YOURUSER = User(name, id_)
print("Okay, you're all set! Just head into your office. The admin's is right next door, but you can just ig
print("""*You realize you have freedom of choice. Choose a door*
      1) your office
      2) the admin's office
""")
choice = int(input())
if choice == 1:
    if hash(YOURUSER) == hash(YOURUSER):
        print("Man, this is a nice office")
        quit()
    else:
        print("Hey, HR, my key doesn't work yet!")
        quit()
elif choice == 2:
    if hash(YOURUSER) == hash(ADMIN):
        print(FLAG)
        quit()
    else:
        print("The HR guy tackles you to the ground for insolence")
        quit()
```

- Therefore, I try command given into kali .

```
That's not an id!

┌──(nkhang㉿22520617)-[~]
└─$ nc psycho.chal.cyberjousting.com 1353

Welcome to onboarding! I'm Jacob from HR, and I'm here to make your experience as seamless as possible joining the company
Go ahead and tell me your name:
18446744073709552983
Welcome to the company, 18446744073709552983
We also give you a user id, but in an attempt to make this company feel like home, we've decided to give you a choice in that, too. Go ahead and choos
e that now:
18446744073709552983
Okay, you're all set! Just head into your office. The admin's is right next door, but you can just ignore that
*You realize you have freedom of choice. Choose a door*
      1) your office
      2) the admin's office

1
Man, this is a nice office

┌──(nkhang㉿22520617)-[~]
```

With name, I can input random .

With id, I have to enter something different number 1337 .

I will select “1” ⇒ I temporary pass .

```
┌──(nkhang㉿22520617)-[~]
└─$ nc psycho.chal.cyberjousting.com 1353

Welcome to onboarding! I'm Jacob from HR, and I'm here to make your experience as seamless as possible joining the company
Go ahead and tell me your name:
nkhang
Welcome to the company, nkhang
We also give you a user id, but in an attempt to make this company feel like home, we've decided to give you a choice in that, too. Go ahead and choos
e that now:
18446744073709552983
Okay, you're all set! Just head into your office. The admin's is right next door, but you can just ignore that
*You realize you have freedom of choice. Choose a door*
      1) your office
      2) the admin's office

2
The HR guy tackles you to the ground for insolence

┌──(nkhang㉿22520617)-[~]
└─$
```

- **Hash behavior for small vs. large integers**
  - In CPython, `hash(n)` for a small integer `n` (within the platform’s native word size) simply returns `n`.
  - For “big” integers (those outside the native signed word range, e.g. ≥ 2⁶³ on a 64-bit build), Python uses a different algorithm to compute the hash.
- **Collision requirement**
  - `ADMIN.id` is `1337`, so `hash(ADMIN) == hash(1337)`.

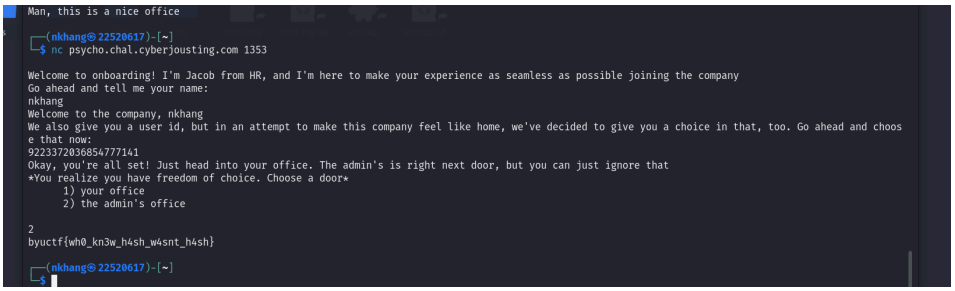
- `YOURUSER.id` is whatever number the user inputs, and `hash(YOURUSER) == hash(YOURUSER.id)`.
- To satisfy the condition `hash(YOURUSER) == hash(ADMIN)` while still having `YOURUSER.id != 1337`, we need to find an integer `x ≠ 1337` such that:

  ```
  python
  CopyEdit
  hash(x) == hash(1337)
  ```

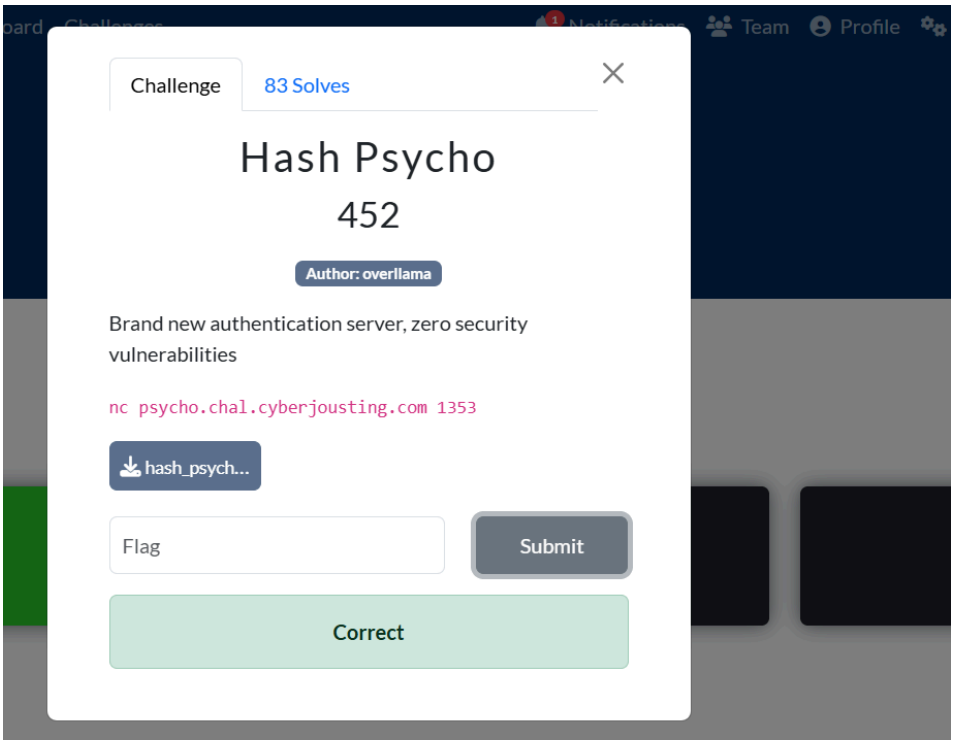
- **Leveraging Python's big-int hash algorithm**
  - By choosing `x` large enough to force Python into its "big-integer" hash path, collisions become feasible.
  - We can search starting at `2**63` (the smallest value outside the 64-bit signed range) and increment until we find `x` satisfying:

    ```
    python
    CopyEdit
    hash(x) == hash(1337)
    ```

- **Resulting exploit**
  - Once such an `x` is discovered, inputting `x` as your user ID bypasses the `id_ == 1337` check and fulfills `hash(YOURUSER) == hash(ADMIN)`.
  - Selecting the admin's office door (`choice == 2`) then prints the flag.
- **Finding the Collision Value**
- To locate a non-1337 integer `x` that satisfies `hash(x) == hash(1337)`, run this short Python script:

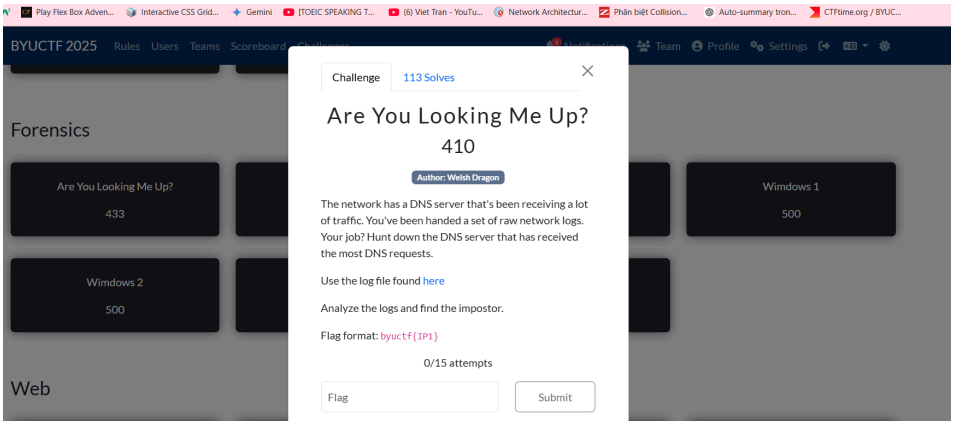


> **Flag :** byuctf{wh0_kn3w_h4sh_w4snt_h4sh}

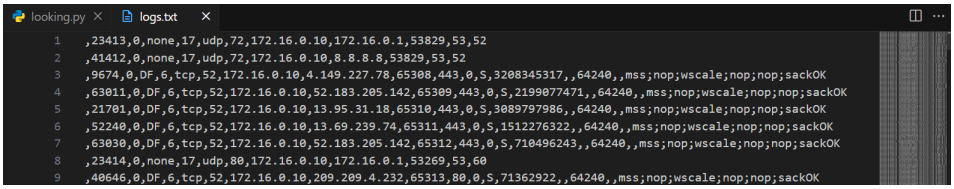

Team
Profile
Challenge
83 Solves
Hash Psycho
452
Author: overllama
Brand new authentication server, zero security vulnerabilities
nc psycho.chal.cyberjousting.com 1353
hash_psych...
Flag
Submit
Correct

Forensics


Forensics
Are You Looking Me Up?
433
Mine Over Matter
491
Wimdows 3
499
Wimdows 1
500
Wimdows 2
500
Wimdows 4
500
Wimdows 5
500


BYUCTF 2025
Rules
Users
Teams
Scoreboard
Team
Profile
Settings
Forensics
Are You Looking Me Up?
433
Wimdows 1
500
Wimdows 2
500
Web
Challenge
113 Solves
Are You Looking Me Up?
410
Author: Welsh Dragon
The network has a DNS server that's been receiving a lot of traffic. You've been handed a set of raw network logs. Your job? Hunt down the DNS server that has received the most DNS requests.
Use the log file found here
Analyze the logs and find the impostor.
Flag format: byuctf{IP1}
0/15 attempts
Flag
Submit

- Ta được cup cấp 1 file log từ chall này , mở xem nó đang theo format gì trước hoặc quăng nó vô GPT để đọc 1 vài dòng phân tích cú pháp cho nhanh .



- cóp 1 dòng trong log ra và phân tích thử

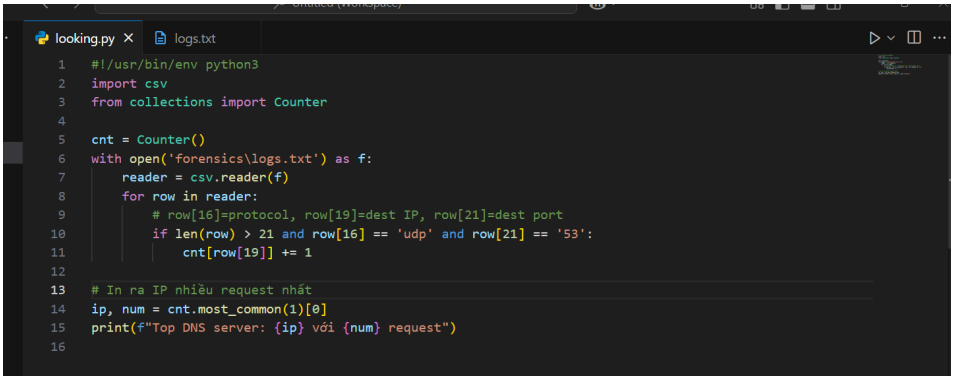
> 2025-05-06T14:49:32+00:00
> 164,,,75a2b136446ad166a85f3150b40b7d1e,vtnet0,match,pass,in,4,0x0,,128,9674,0,DF,6,tcp,52,1

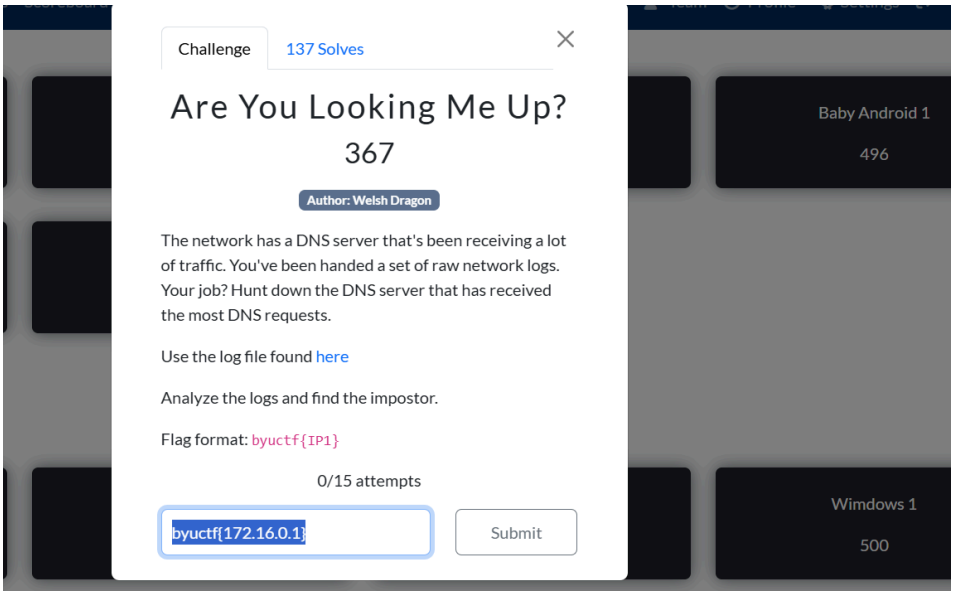
- Khúc đầu mọi thứ dường như giống nhau, ta chỉ chú trọng :

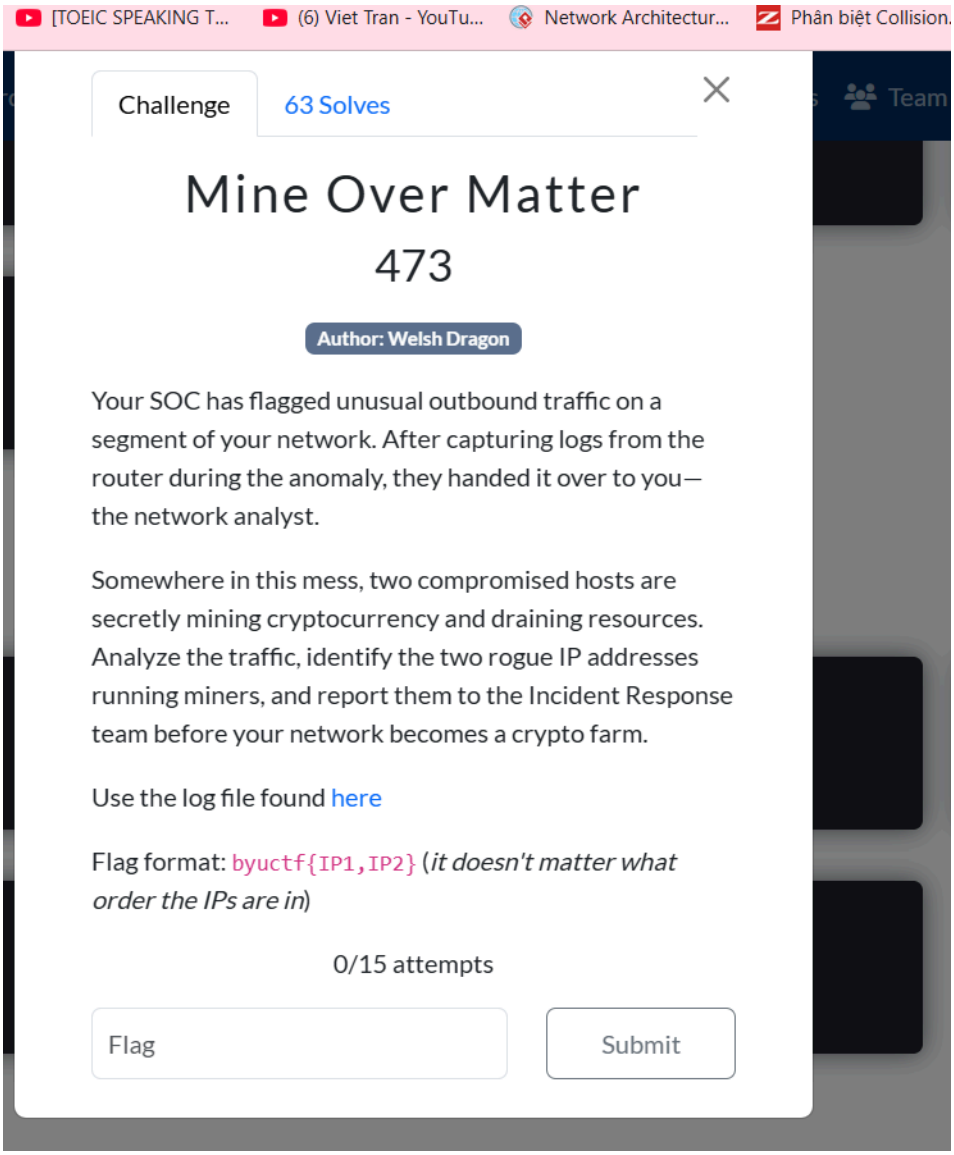
Trong mỗi dòng log, các cột quan trọng (đánh số theo `awk -F,`) là:

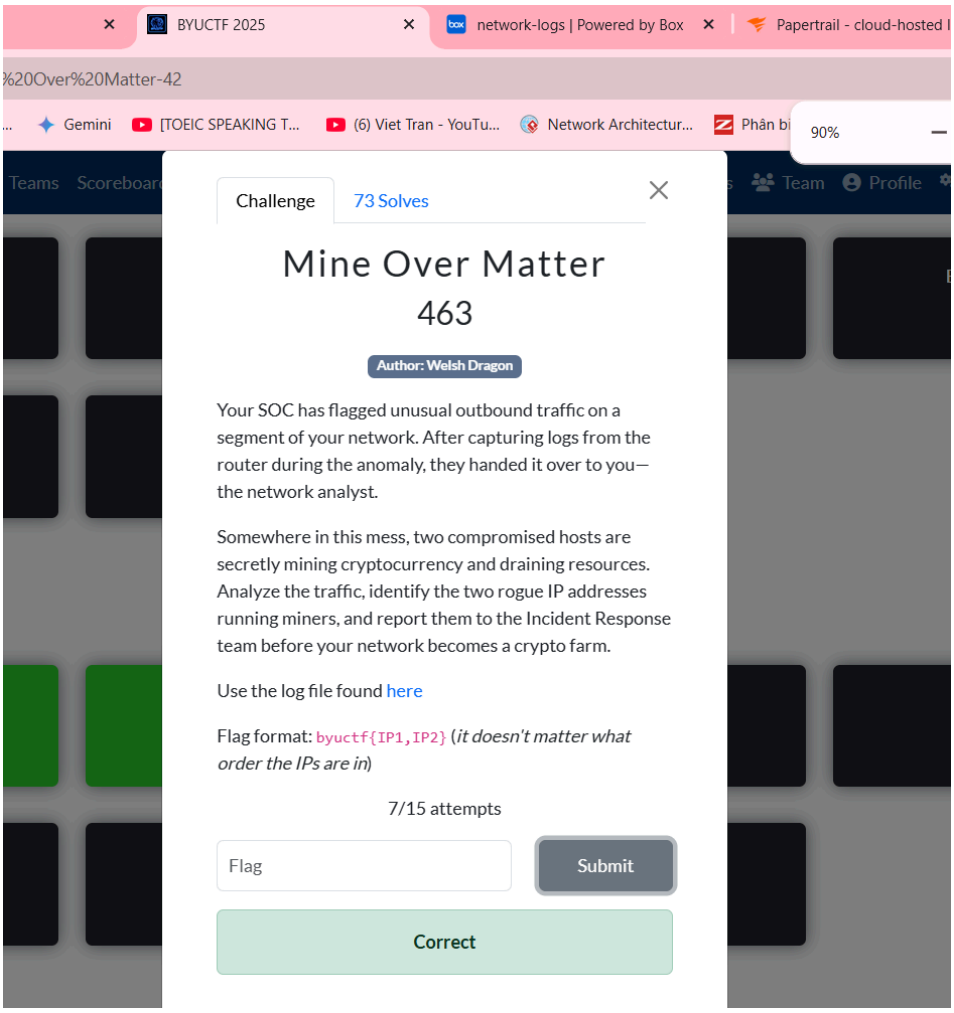
- **$17** = giao thức (`udp` hoặc `tcp`)
- **$20** = địa chỉ IP đích
- **$22** = port đích

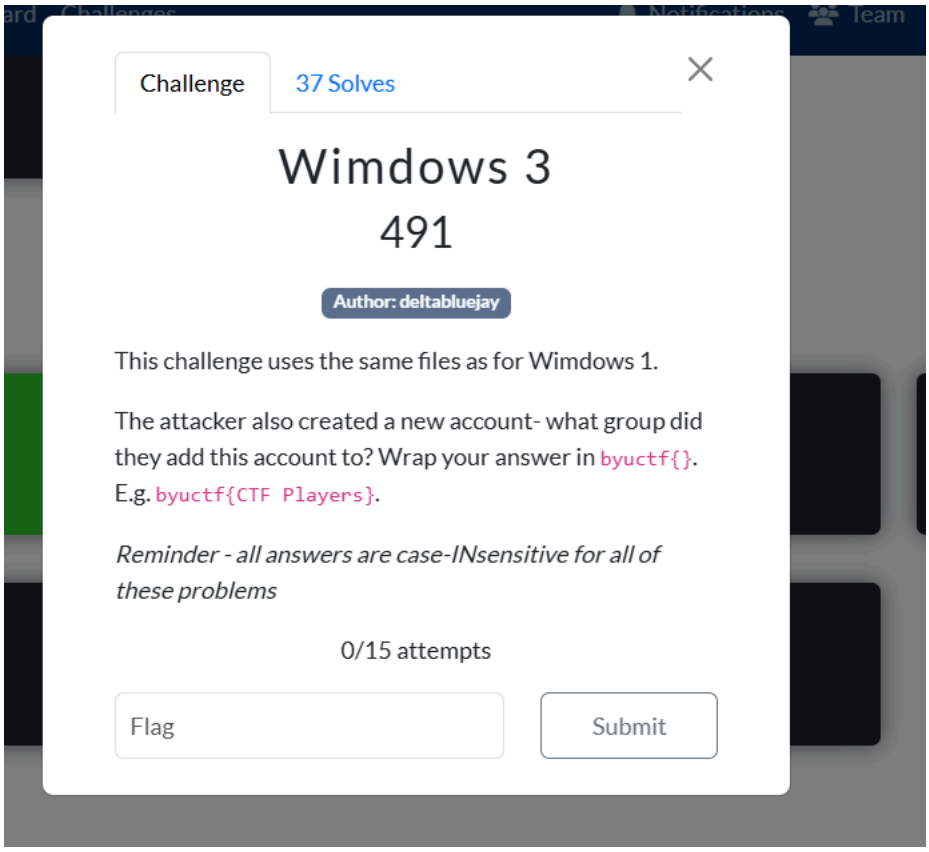
⇒ Ta có thể dùng scripts python để lọc ra ip nào có lượng traffic đổ về nhiều nhất , lọc TCP hoặc UDP và port , có thể thay đổi .




Challenge
137 Solves
Are You Looking Me Up?
367
Author: Welsh Dragon
The network has a DNS server that's been receiving a lot of traffic. You've been handed a set of raw network logs. Your job? Hunt down the DNS server that has received the most DNS requests.
Use the log file found here
Analyze the logs and find the impostor.
Flag format: byuctf{IP1}
0/15 attempts
byuctf{172.16.0.1}
Submit
Baby Android 1
496
Wimdows 1
500

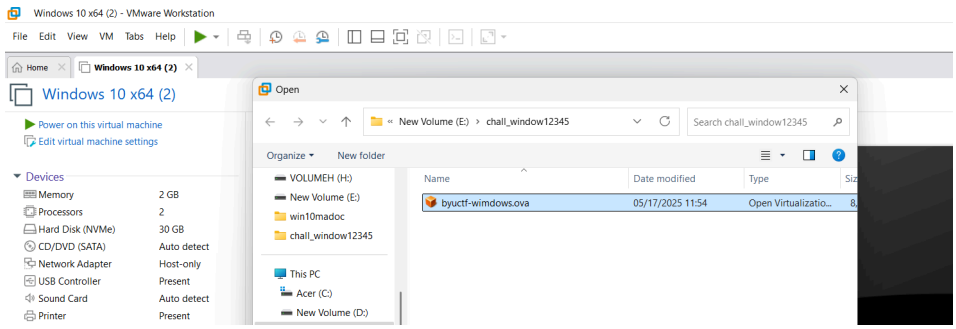

[TOEIC SPEAKING T...
(6) Viet Tran - YouTu...
Network Architectur...
Phân biệt Collision...
Team
Challenge
63 Solves
Mine Over Matter
473
Author: Welsh Dragon
Your SOC has flagged unusual outbound traffic on a segment of your network. After capturing logs from the router during the anomaly, they handed it over to you—the network analyst.
Somewhere in this mess, two compromised hosts are secretly mining cryptocurrency and draining resources. Analyze the traffic, identify the two rogue IP addresses running miners, and report them to the Incident Response team before your network becomes a crypto farm.
Use the log file found here
Flag format: byuctf{IP1,IP2} (it doesn't matter what order the IPs are in)
0/15 attempts
Flag
Submit


BYUCTF 2025
network-logs | Powered by Box
Papertrail - cloud-hosted
%20Over%20Matter-42
Gemini
[TOEIC SPEAKING T...
(6) Viet Tran - YouTu...
Network Architectur...
90%
Teams
Scoreboard
Team
Profile
Challenge
73 Solves
Mine Over Matter
463
Author: Welsh Dragon
Your SOC has flagged unusual outbound traffic on a segment of your network. After capturing logs from the router during the anomaly, they handed it over to you—the network analyst.
Somewhere in this mess, two compromised hosts are secretly mining cryptocurrency and draining resources. Analyze the traffic, identify the two rogue IP addresses running miners, and report them to the Incident Response team before your network becomes a crypto farm.
Use the log file found here
Flag format: byuctf{IP1,IP2} (it doesn't matter what order the IPs are in)
7/15 attempts
Flag
Submit
Correct

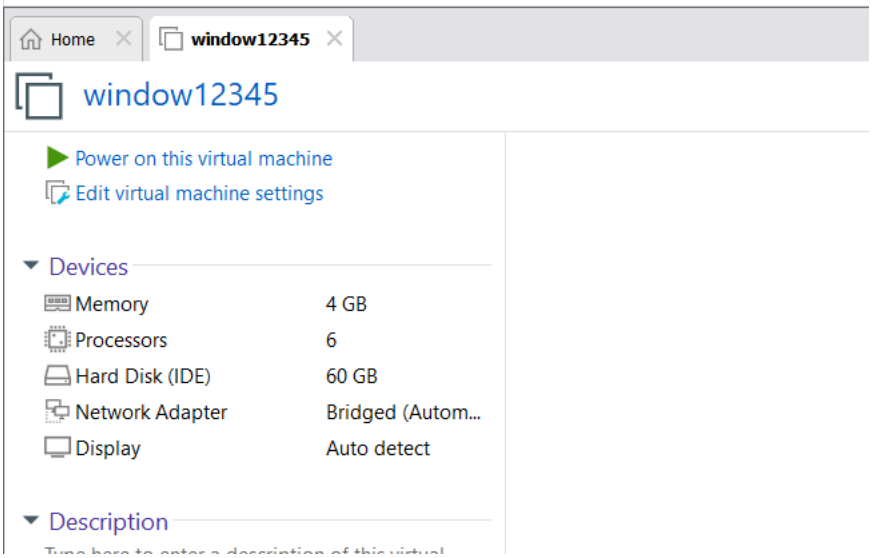


bật vmware vào file → open → chọn file đã được cấp .

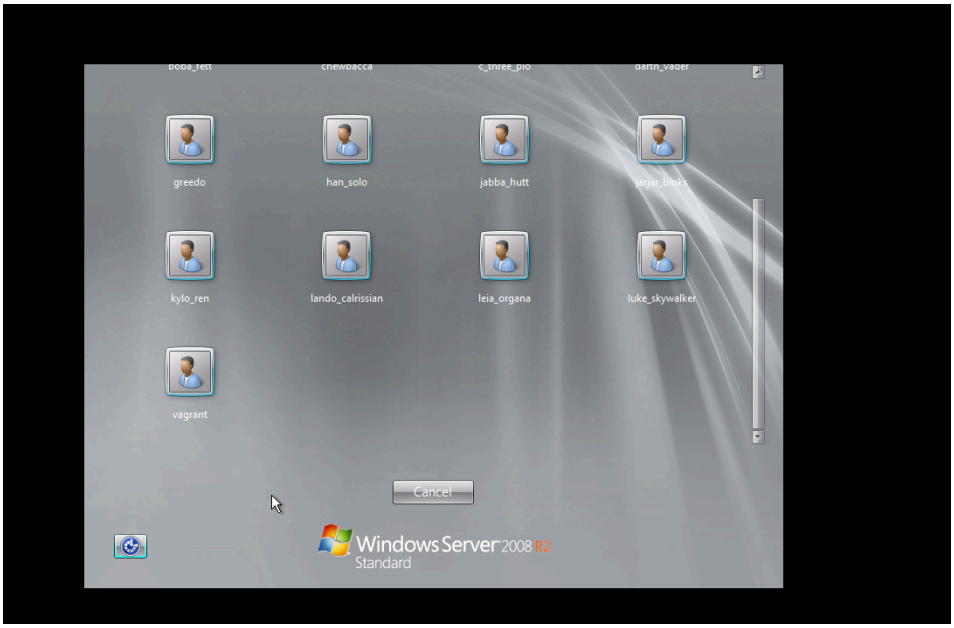
Chọn đường dẫn nơi để lưu file và đặt tên cho nó sau đó chờ nó loading thôi.



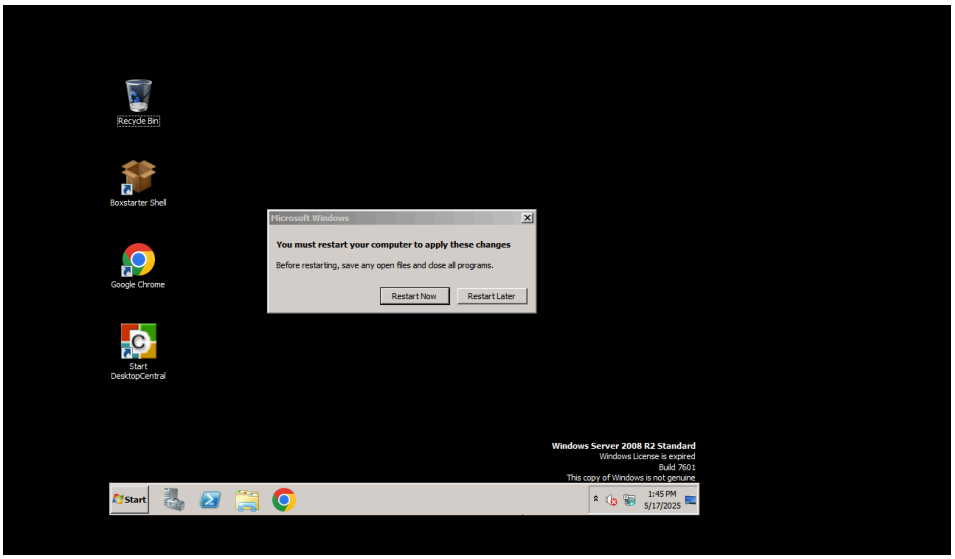
holly SH*t cấu hình này hơi cao với máy tôi rồi, nhưng vẫn có thể chơi tiếp được .

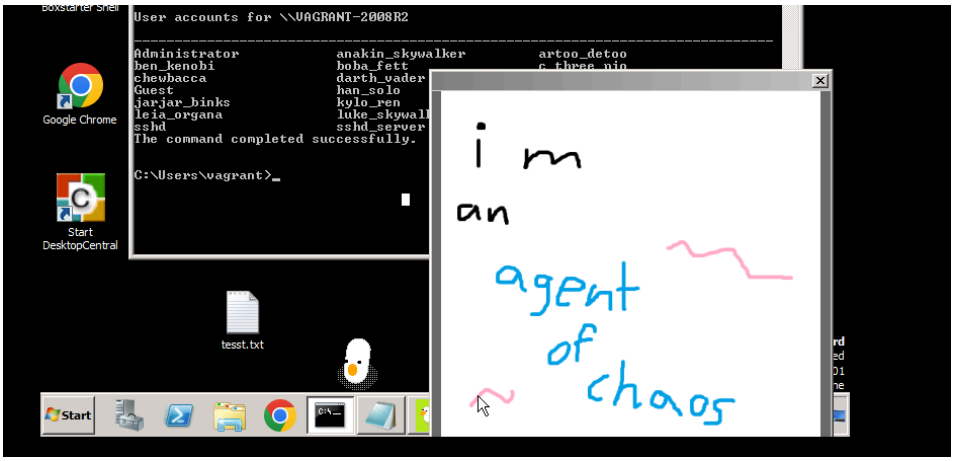


- nhấn ctrl + alt + del để vào được UI này

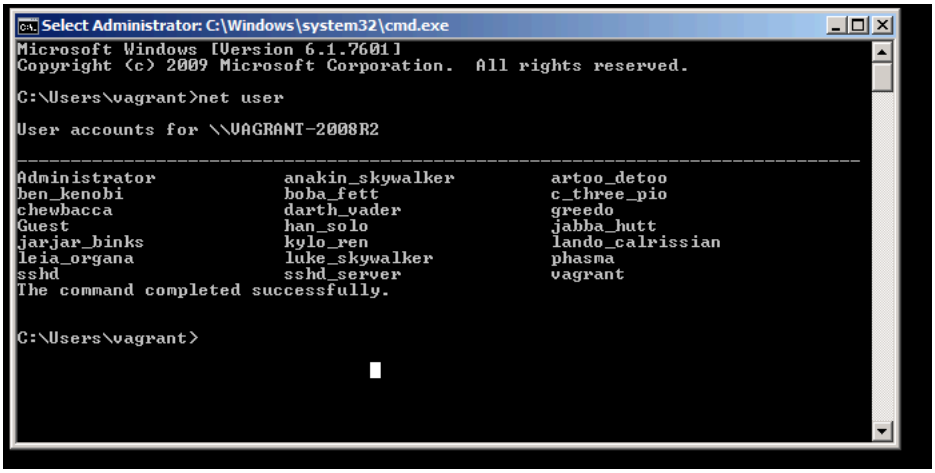


- login với user vegrant:vegrant
- Sau đó xuất hiện 1 UI thời tống hiện ra, hoài niệm quá đi :((
- Má con duck này khá khó chịu nha :)), click vào nó hoặc nó tự dí vô trỏ chuột được là nó nắm đầu đi chơi .



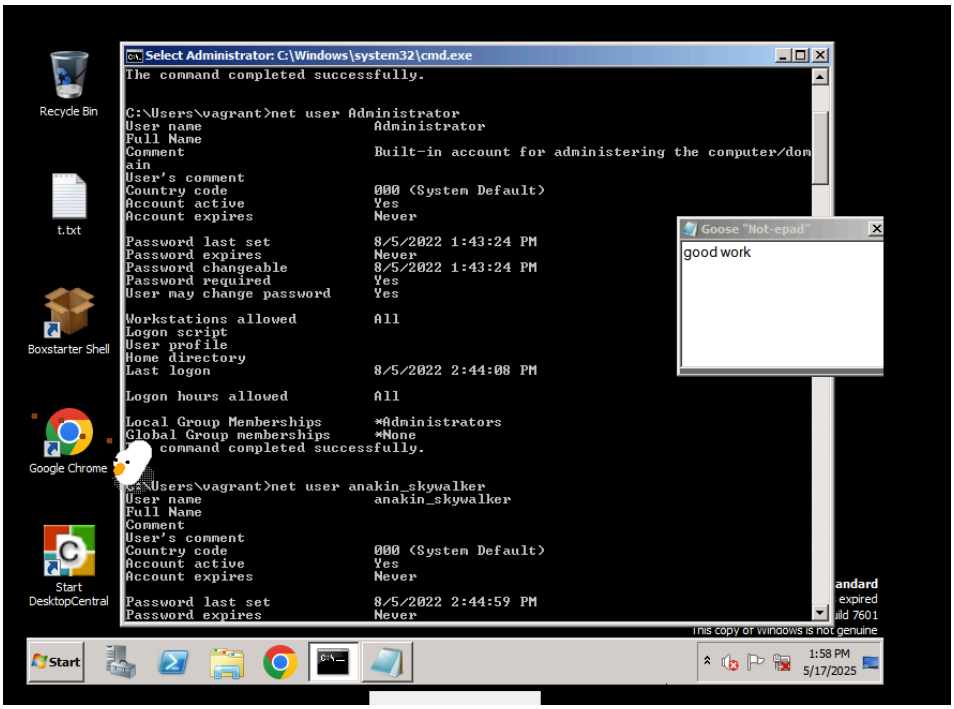


- quay lại với thử thách ta thấy rằng sau khi dùng net user để list các user hiện có ra thì thấy có rất nhiều user nhiễu

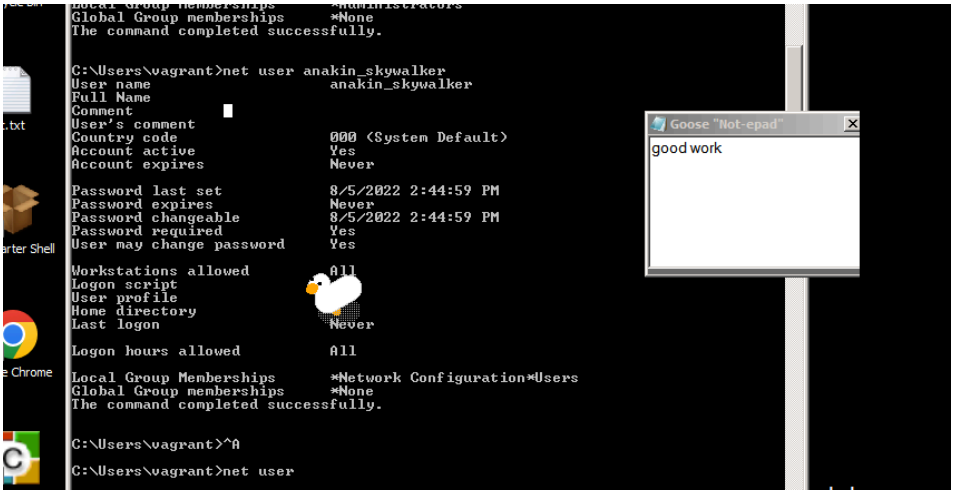


- KHông cách nào khác ngoài việc check từng user thôi .

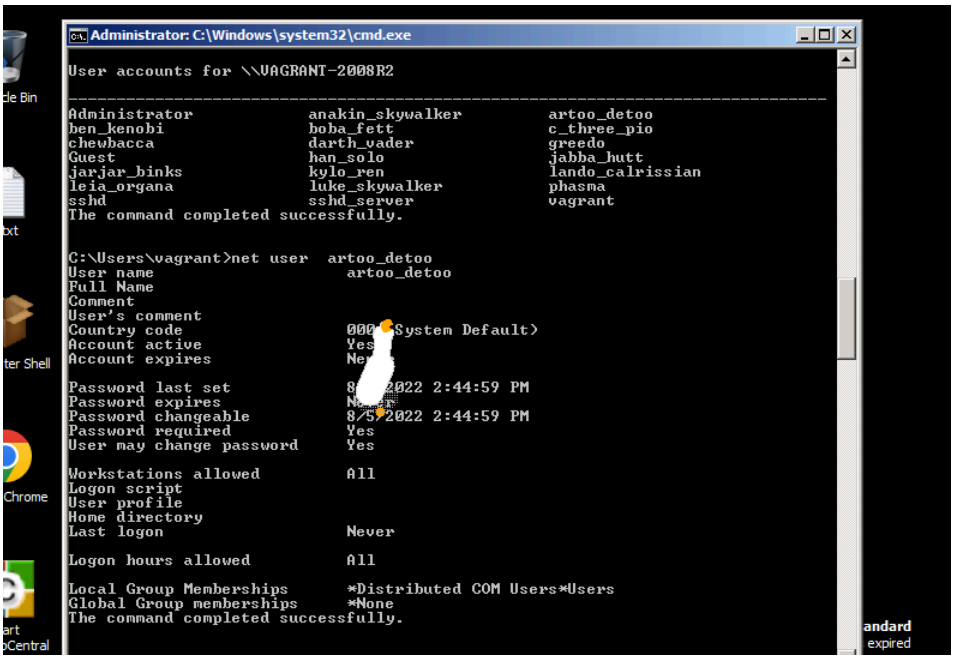
với user **administrator** trước thì quyền cao nhất là nó rồi /



- **Với anakin_skywalker**

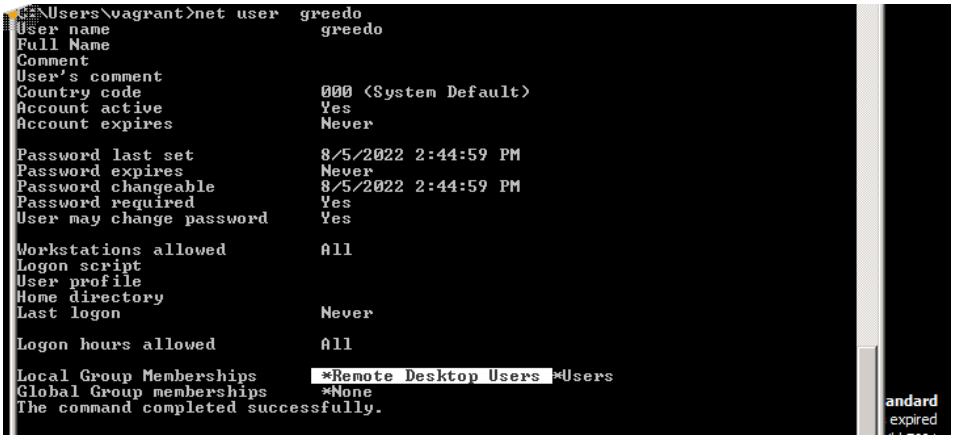


- Với a**rtoo_detoo**

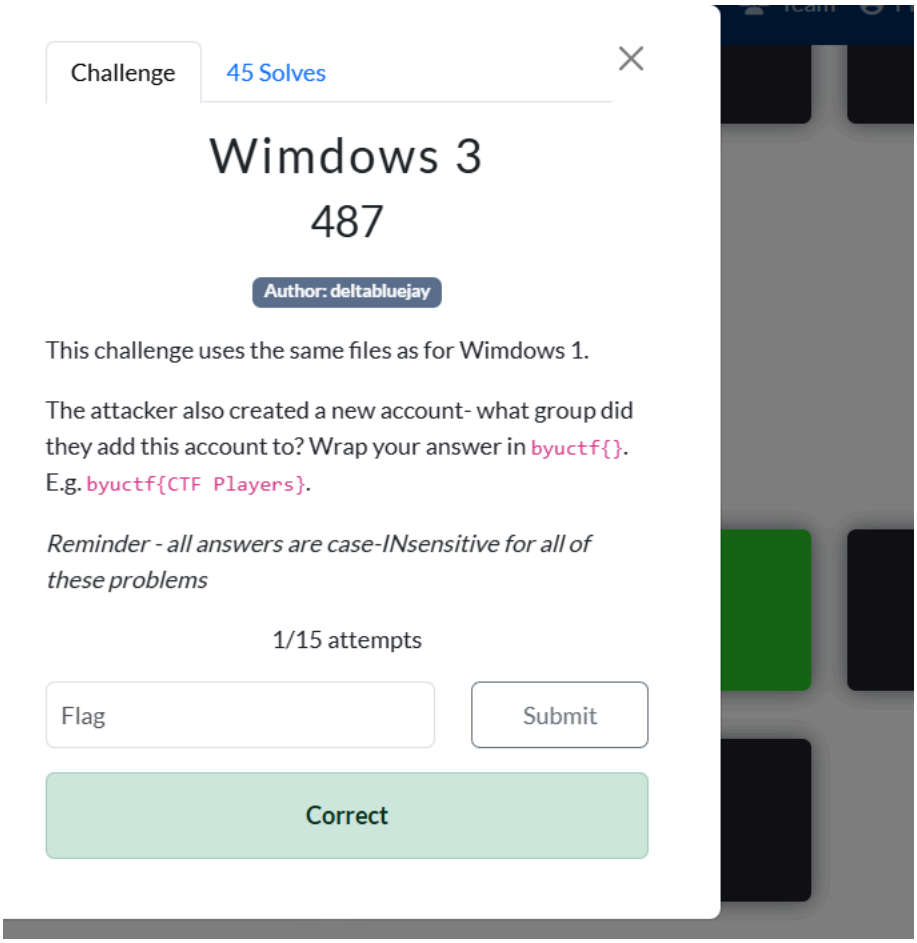


- Sau khi check từng quyền thì ta thấy user greendo có 1 quyền khá cao **Remote Desktop Users,** cho phép
  đăng nhập từ xa qua Remote Desktop (RDP), thường là mục tiêu của attacker để chiếm quyền truy cập shell trên máy.

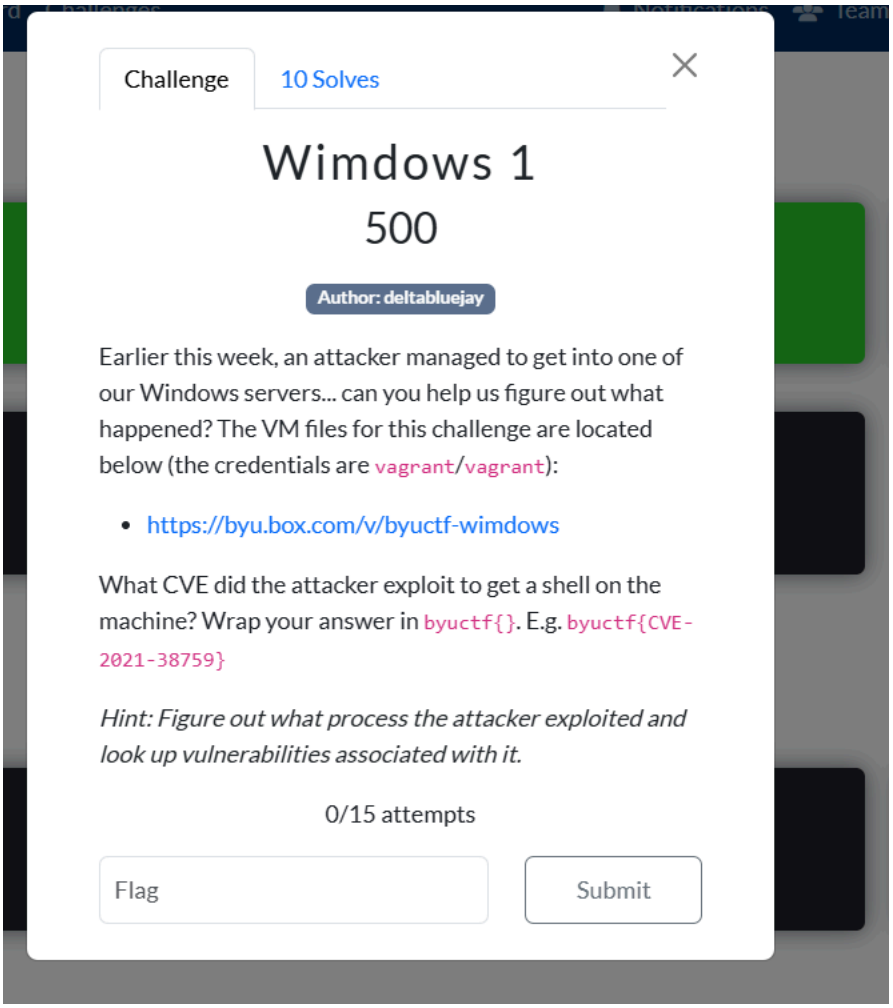
- Ta gói nó vào format flag và submit thử xem, nếu đúng thì done, holaholo :) , nếu không thì check tiếp .

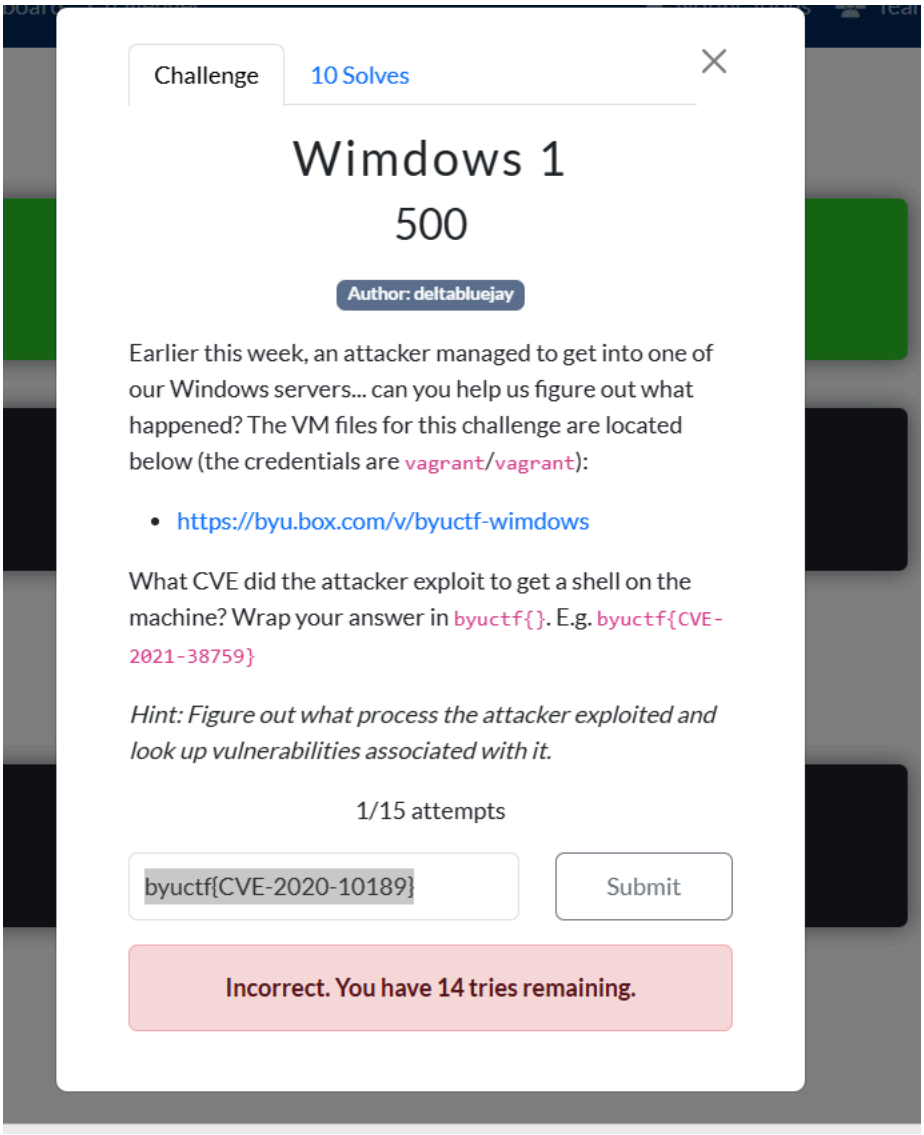


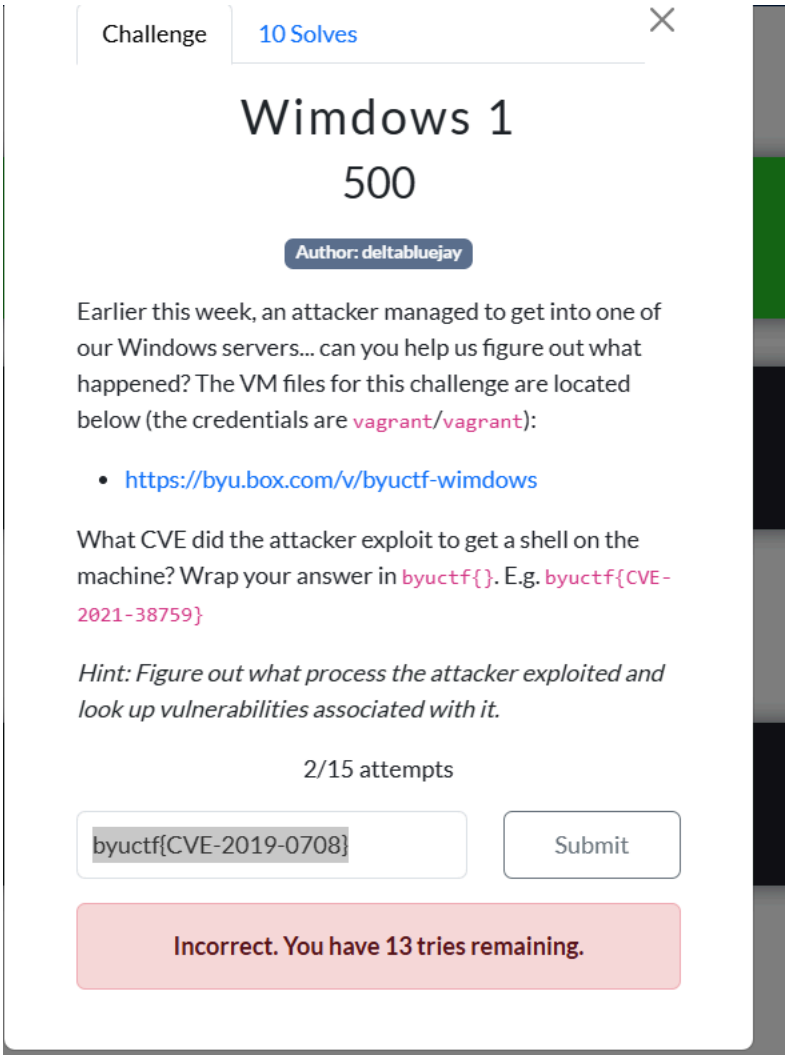
- Ôi wow, đúng rồi nè, chall này khá đơn giản nhưng tốn thời setup và tốn thời gian để né con duck :))



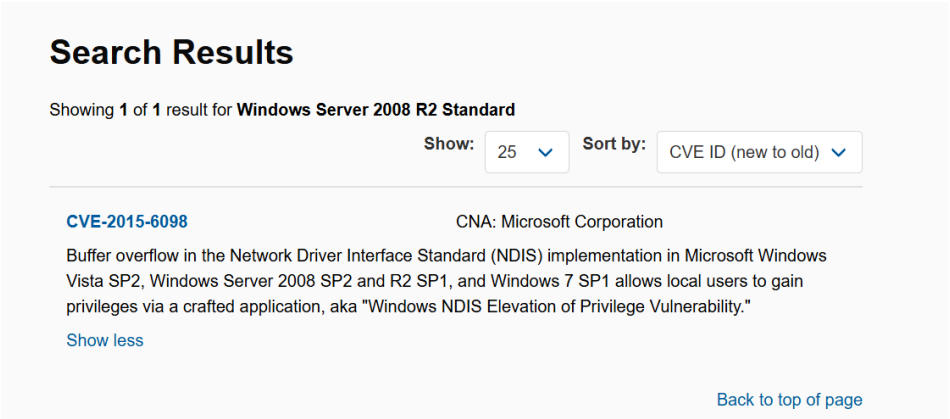
> **Flag :** byuctf{Remote Desktop Users}


Challenge
10 Solves
Wimdows 1
500
Author: deltabluejay
Earlier this week, an attacker managed to get into one of our Windows servers... can you help us figure out what happened? The VM files for this challenge are located below (the credentials are vagrant/vagrant):
https://byu.box.com/v/byuctf-wimdows
What CVE did the attacker exploit to get a shell on the machine? Wrap your answer in byuctf{}. E.g. byuctf{CVE-2021-38759}
Hint: Figure out what process the attacker exploited and look up vulnerabilities associated with it.
0/15 attempts
Flag
Submit


Challenge
10 Solves
Wimdows 1
500
Author: deltabluejay
Earlier this week, an attacker managed to get into one of our Windows servers... can you help us figure out what happened? The VM files for this challenge are located below (the credentials are vagrant/vagrant):
https://byu.box.com/v/byuctf-wimdows
What CVE did the attacker exploit to get a shell on the machine? Wrap your answer in byuctf{}. E.g. byuctf{CVE-2021-38759}
Hint: Figure out what process the attacker exploited and look up vulnerabilities associated with it.
1/15 attempts
byuctf{CVE-2020-10189}
Submit
Incorrect. You have 14 tries remaining.



bản này cũng không phải



2021-38759}

Hint: Figure out what process the attacker exploited and look up vulnerabilities associated with it.

3/15 attempts

byuctf{CVE-2015-6098}

Submit

Incorrect. You have 12 tries remaining.

Hint: Figure out what process the attacker exploited and look up vulnerabilities associated with it.

4/15 attempts

byuctf{CVE-2021-44515}

Submit

Incorrect. You have 11 tries remaining.

Hint: Figure out what process the attacker exploited and look up vulnerabilities associated with it.

5/15 attempts

byuctf{CVE-2021-44526}

Submit

Incorrect. You have 10 tries remaining.

6/15 attempts

byuctf{CVE-2018-1000861}

Submit

Incorrect. You have 9 tries remaining.