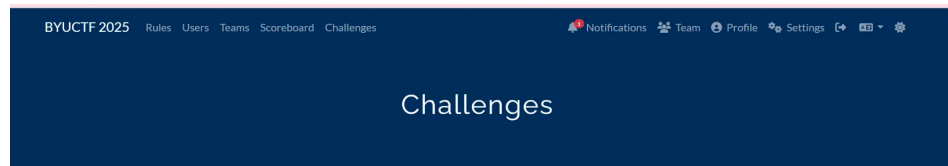


BYUCTF 2025

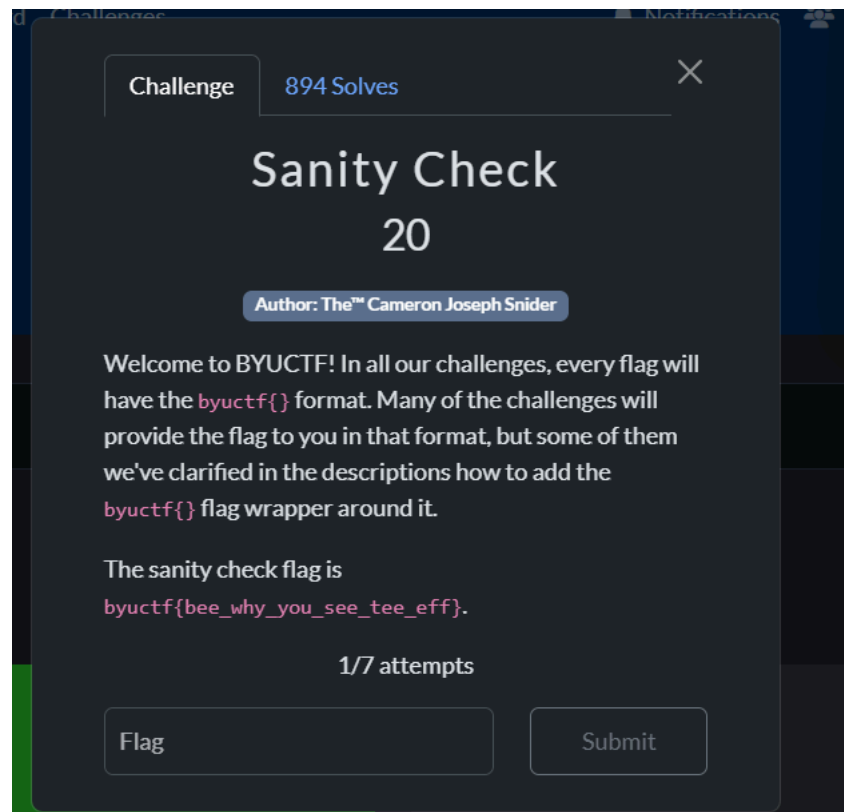
BYUCTF 2025 Writeup

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.

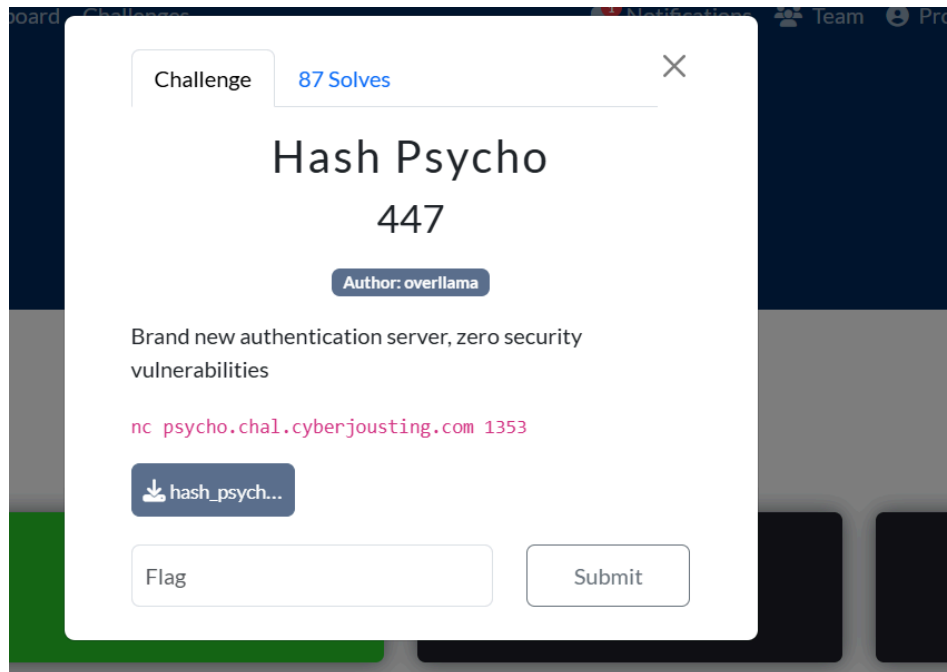


Misc



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 .

```

hash_psych.py x train.py
1 FLAG = "byctf{}"
2
3 class User:
4     def __init__(self, username, id):
5         self.username = username
6         self.id = id
7
8     def __eq__(self, other):
9         return self.id == other.id
10
11     def __hash__(self):
12         return hash(self.id)
13
14 ADMIN = User('admin', 1337)
15
16 print("Welcome to onboarding! I'm Jacob from HR, and I'm here to make your experience as seamless as
17 print("Go ahead and tell me your name:")
18 name = input()
19 print("Welcome to the company, " + name)
20 print("We also give you a user id, but in an attempt to make this company feel like home, we've deci
21 id_ = input()
22 if not all([i in '0987654321' for i in id_]):
23     print("That's not an id!")
24     quit()
25 id_ = int(id_)
26 if id_ == 1337:
27     print("Sorry, the admin already claimed that id, no can do")

```

- 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()

```

```

hash_psycho.py X train.py
25 id_ = int(id_)
26 if id_ == 1337:
27     print("Sorry, the admin already claimed that id, no can do")
28     quit()
29 YOURUSER = User(name, id_)
30 print("Okay, you're all set! Just head into your office. The admin's is right next door, but you can just ignore that")
31 print("""*You realize you have freedom of choice. Choose a door*
32     1) your office
33     2) the admin's office
34 """)
35 choice = int(input())
36 if choice == 1:
37     if hash(YOURUSER) == hash(YOURUSER):
38         print("Man, this is a nice office")
39         quit()
40     else:
41         print("Hey, HR, my key doesn't work yet!")
42         quit()
43 elif choice == 2:
44     if hash(YOURUSER) == hash(ADMIN):
45         print(FLAGS)
46         quit()
47     else:
48         print("The HR guy tackles you to the ground for insolence")
49         quit()
50
51

```

- Therefore, I try command given into kali .

```

That's not an id!
[nkhng@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 choose 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
[nkhng@22520617]-[~]

```

With name, I can input random .

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

I will select "1" ⇒ I temporary pass .

```

[nkhng@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:
nkhng
Welcome to the company, nkhng
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 choose 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
[nkhng@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. $\geq 2^{63}$ 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

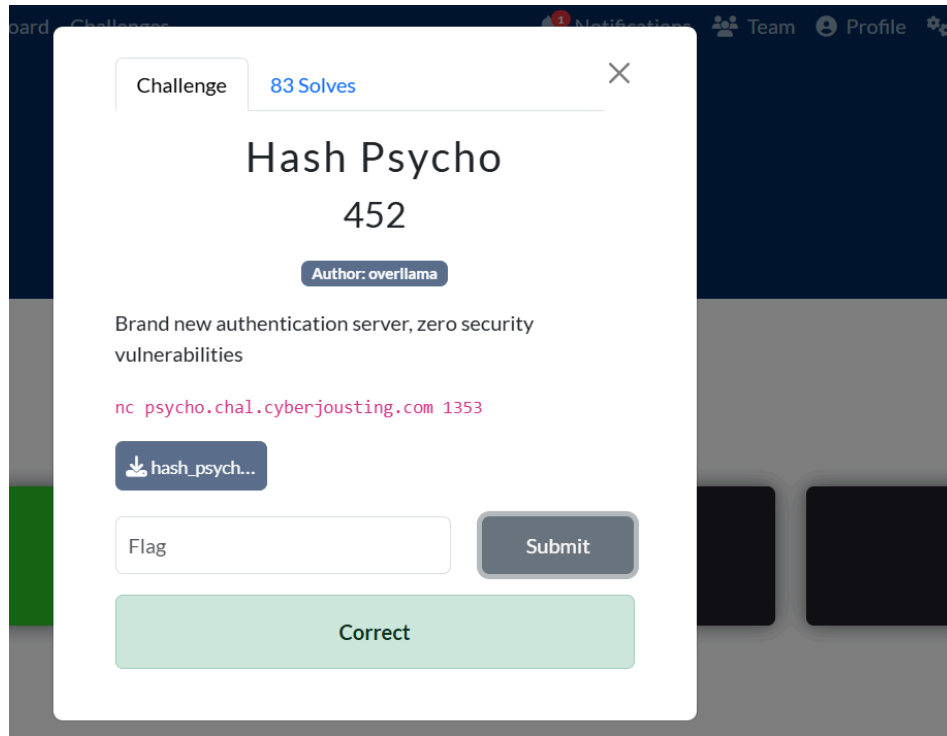
- To locate a non-1337 integer `x` that satisfies `hash(x) == hash(1337)`, run this short Python script:

```
hash_psycho.py  X  code.py  X
1  target = hash(1337)
2  i = 2**63      # bắt đầu từ số lớn để CPython vào thuật toán hash khác
3  while True:
4      if hash(i) == target:
5          print("Collision found:", i)
6          break
7      i += 1
8  # Collision found: 9223372036854777141s
```

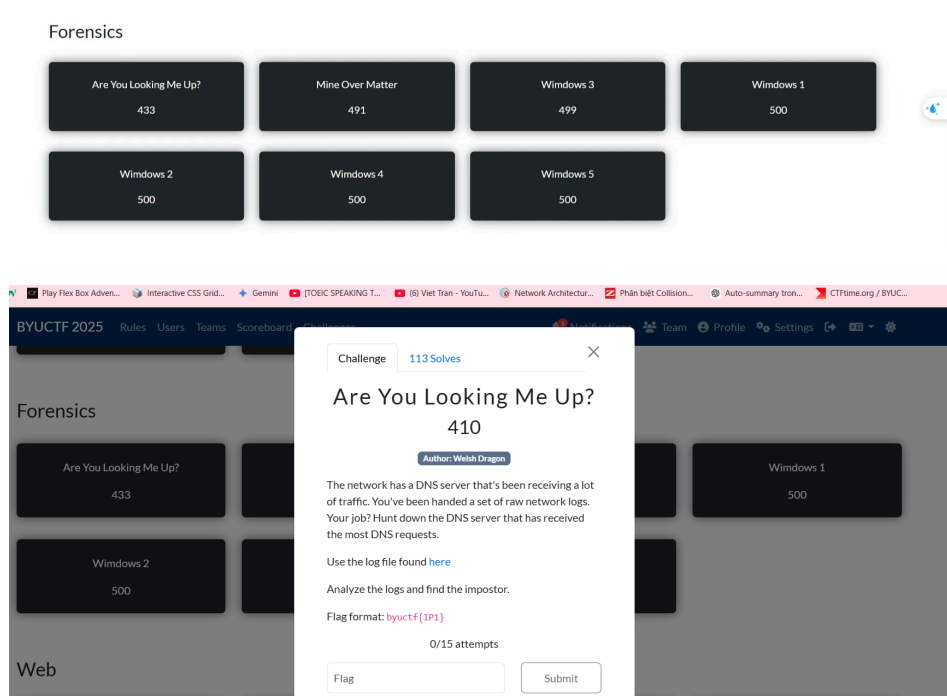
```
Man, this is a nice office
(nkhang@22520617)-[~]
$ nc psycho.chal.cyberjousting.com 1353
Welcome to onboarding! I'm Jacob from HR, and I'm here to make your experience as seamless as possible joining the company
Go ahead and tell me your name:
nkhang
Welcome to the company, nkhang
We also give you 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 choose that now:
9223372036854777141
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
byuctf{wh0_kn3w_h4sh_w4snt_h4sh}
(nkhang@22520617)-[~]
```

Flag : byuctf{wh0_kn3w_h4sh_w4snt_h4sh}



Forensics



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

```

1 23413,0,none,17,udp,72,172.16.0.10,172.16.0.1,53829,53,52
2 41412,0,none,17,udp,72,172.16.0.10,8.8.8.8,53829,53,52
3 9674,0,DF,6,tcp,52,172.16.0.10,4.149.227.78,65308,443,0,S,3208345317,,64240,,mss;nop;wscale;nop;nop;sackOK
4 63011,0,DF,6,tcp,52,172.16.0.10,52.183.205.142,65309,443,0,S,2199077471,,64240,,mss;nop;wscale;nop;nop;sackOK
5 21701,0,DF,6,tcp,52,172.16.0.10,13.95.31.18,65310,443,0,S,3089797986,,64240,,mss;nop;wscale;nop;nop;sackOK
6 52240,0,DF,6,tcp,52,172.16.0.10,13.69.239.74,65311,443,0,S,1512276322,,64240,,mss;nop;wscale;nop;nop;sackOK
7 63030,0,DF,6,tcp,52,172.16.0.10,52.183.205.142,65312,443,0,S,710496243,,64240,,mss;nop;wscale;nop;nop;sackOK
8 23414,0,none,17,udp,80,172.16.0.10,172.16.0.1,53269,53,60
9 40646,0,DF,6,tcp,52,172.16.0.10,209.209.4.232,65313,80,0,S,71362922,,64240,,mss;nop;wscale;nop;nop;sackOK

```

- copy 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 .

```

1 #!/usr/bin/env python3
2 import csv
3 from collections import Counter
4
5 cnt = Counter()
6 with open('forensics/logs.txt') as f:
7     reader = csv.reader(f)
8     for row in reader:
9         # row[16]=protocol, row[19]=dest IP, row[21]=dest port
10        if len(row) > 21 and row[16] == 'udp' and row[21] == '53':
11            cnt[row[19]] += 1
12
13 # In ra IP nhiều request nhất
14 ip, num = cnt.most_common(1)[0]
15 print(f"Top DNS server: {ip} với {num} request")
16

```

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

Submit

Baby Android 1

496

Windows 1

500

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 I

%20Over%20Matter-42

Gemini

[TOEIC SPEAKING T...

(6) Viet Tran - YouTu...

Network Architectur...

Phản b

90%

Teams

Scoreboard

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](#)

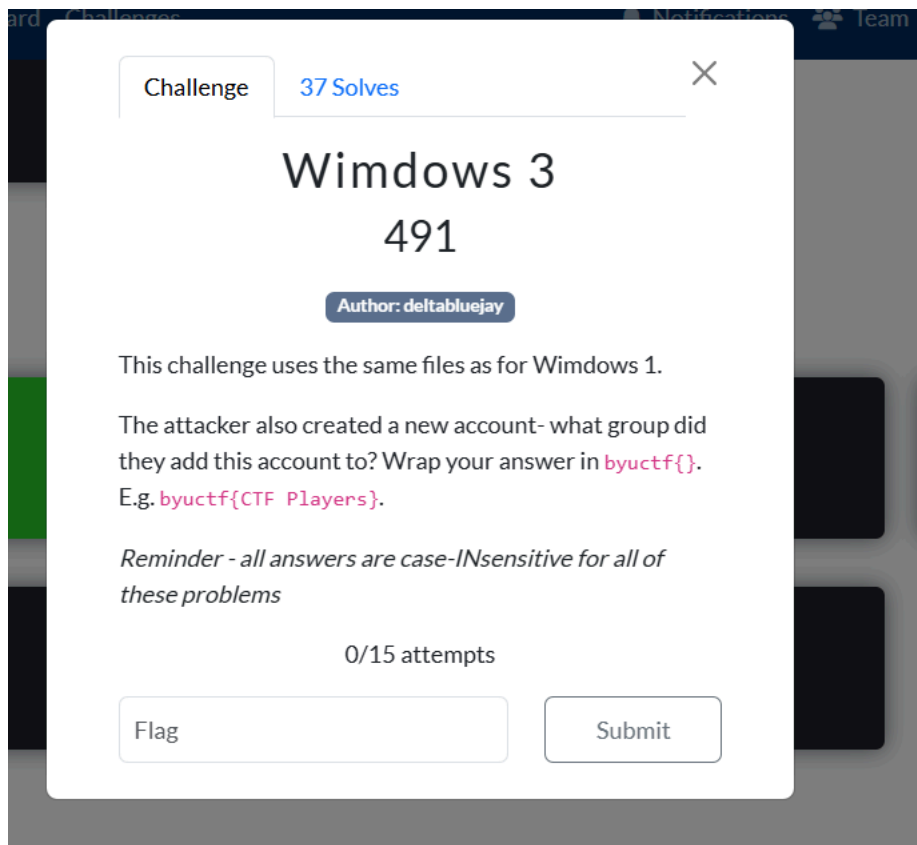
Flag format: `byuctf{IP1,IP2}` (it doesn't matter what order the IPs are in)

7/15 attempts

Flag

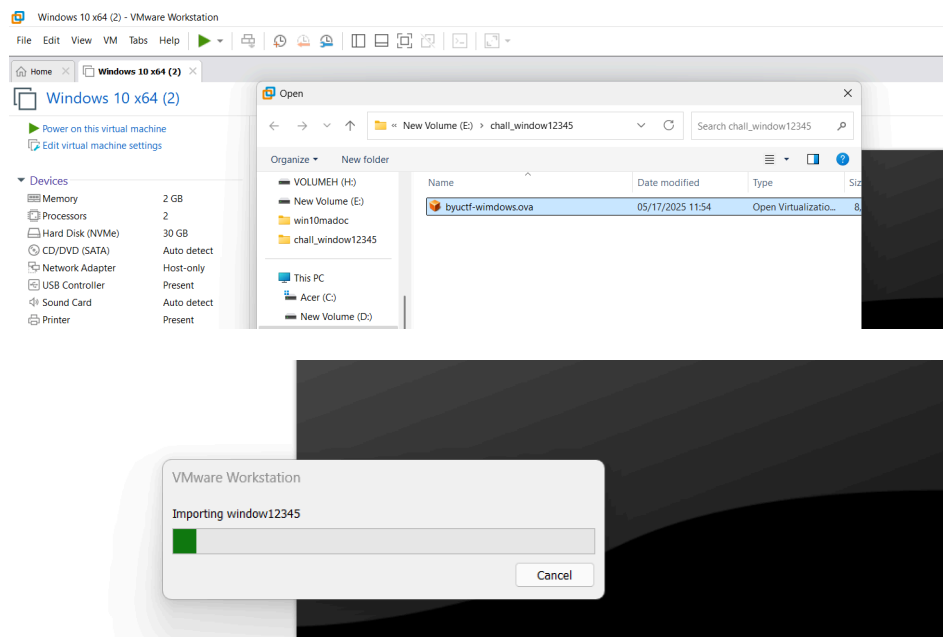
Submit

Correct

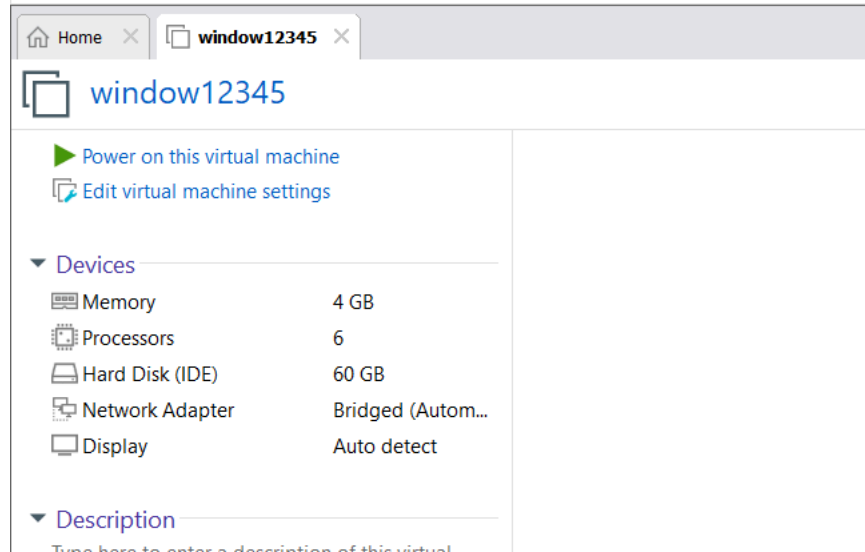


bật vmware vào file → open → chọn file đã được cấp .

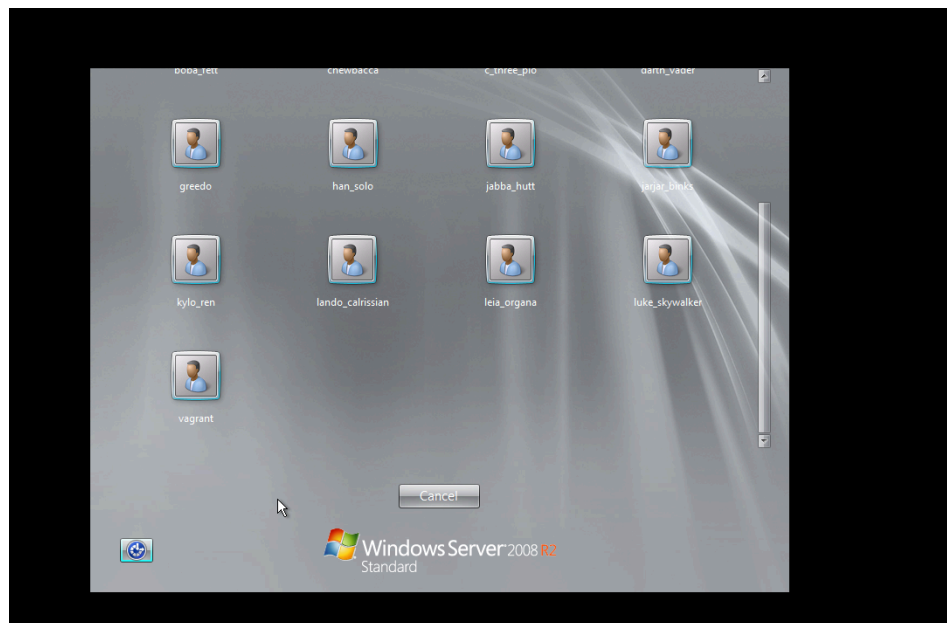
Chọn đường dẫn nơi để lưu file và đặt tên cho nó sau đó chờ nó loading thôi.



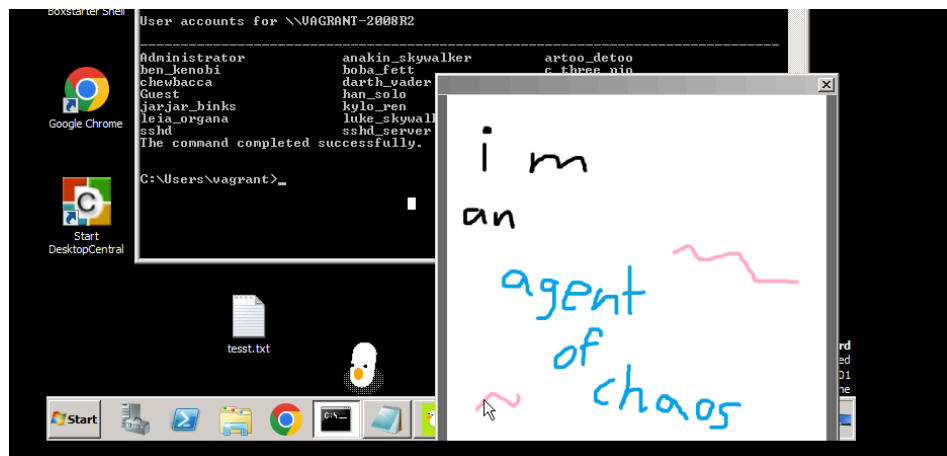
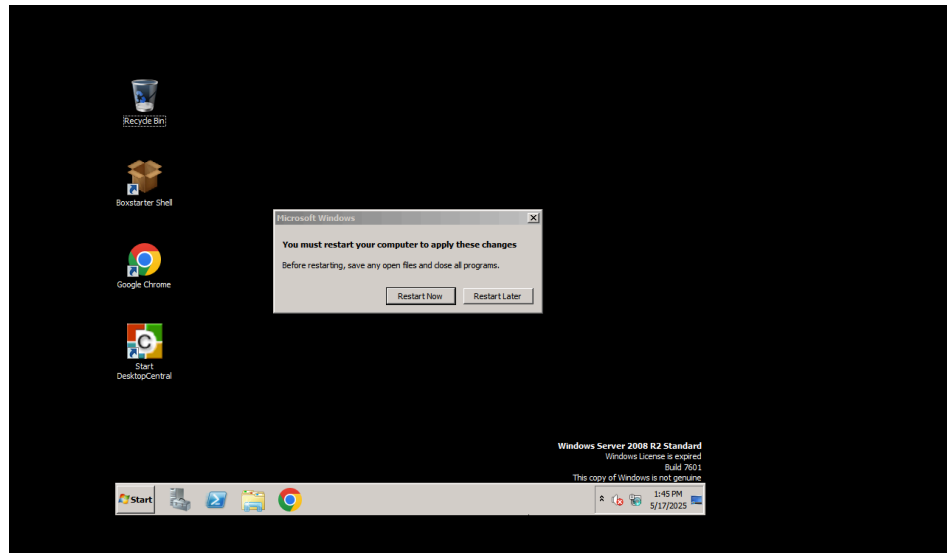
holly SH*t cấu hình này hơi cao với máy tôi rồi, nhưng vẫn có thể chơi tiếp được .



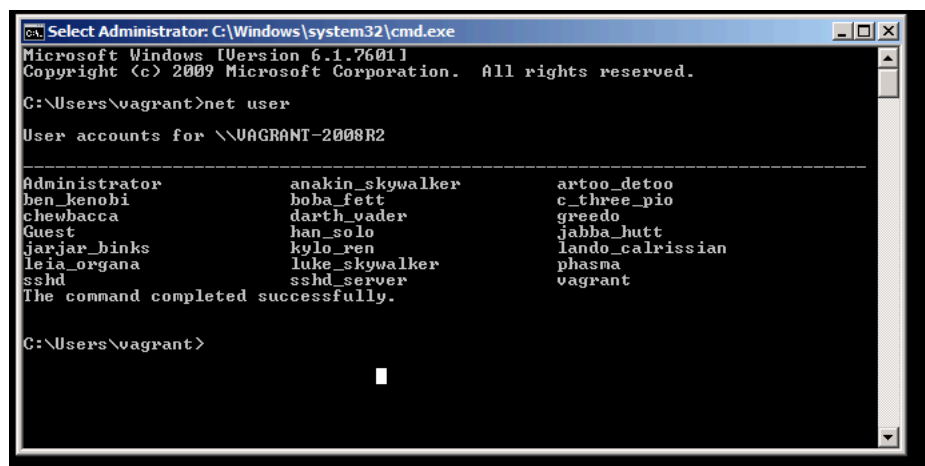
- nhấn ctrl + alt + del để vào được UI này



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

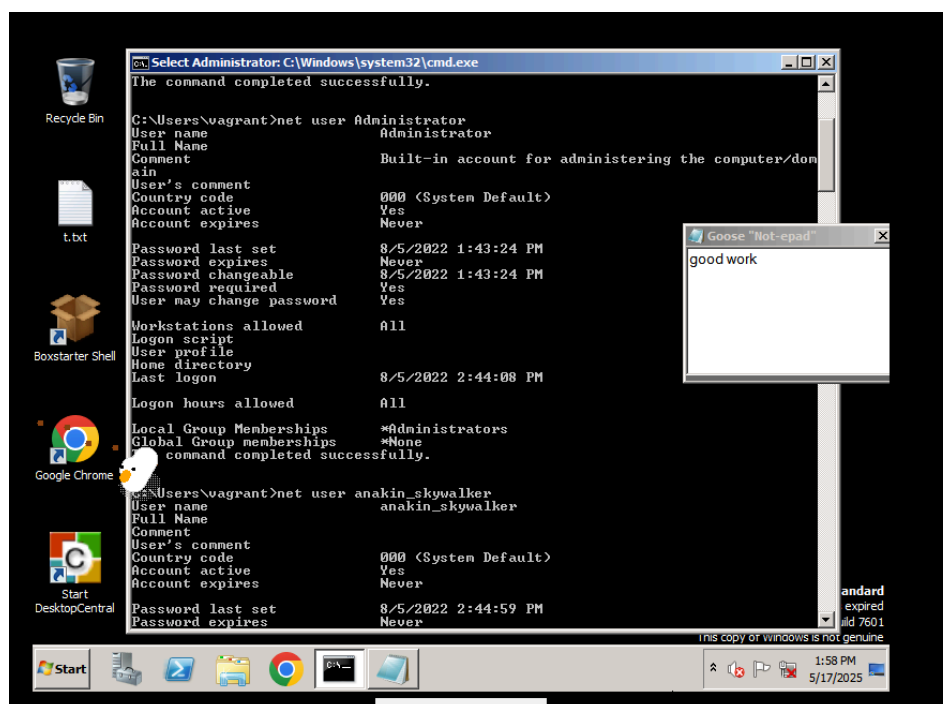


- quay lại với thử thách ta thấy rằng sau khi dùng net user để list các user hiện có ra thì thấy có rất nhiều user nhiều

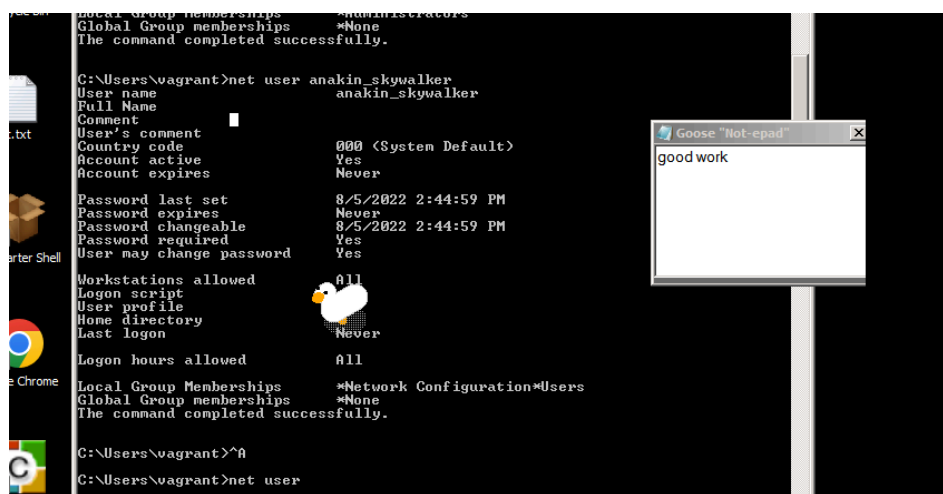


- Không cách nào khác ngoài việc check từng user thôi .

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



- Với anakin_skywalker



- Với artoo_detoo

```

Administrator: C:\Windows\system32\cmd.exe
User accounts for \VAGRANT-2008R2
-----
Administrator      anakin_skywalker    artoo_detoo
ben_kenobi          boba_fett           c_three_pio
chewbacca           darth_vader         greedo
Guest              han_solo            jabba_hutt
jarjar_binks        kylo_ren            lando_calrissian
leia_organa         luke_skywalker       phasma
sshd                sshd_server         vagrant
The command completed successfully.

C:\Users\vagrant>net user artoo_detoo
User name          artoo_detoo
Full Name
Comment
User's comment
Country code       000 (System Default)
Account active      Yes
Account expires    Never
Password last set   8/5/2022 2:44:59 PM
Password expires    Never
Password changeable 8/5/2022 2:44:59 PM
Password required   Yes
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon          Never
Logon hours allowed All
Local Group Memberships *Distributed COM Users*Users
Global Group memberships *None
The command completed successfully.

```

- 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 .

```

C:\Users\vagrant>net user greedo
User name          greedo
Full Name
Comment
User's comment
Country code       000 (System Default)
Account active      Yes
Account expires    Never
Password last set   8/5/2022 2:44:59 PM
Password expires    Never
Password changeable 8/5/2022 2:44:59 PM
Password required   Yes
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon          Never
Logon hours allowed All
Local Group Memberships *Remote Desktop Users*Users
Global Group memberships *None
The command completed successfully.

```

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

Challenge

45 Solves

×

Wimdows 3 487

Author: deltabluejay

This challenge uses the same files as for Wimdows 1.

The attacker also created a new account- what group did they add this account to? Wrap your answer in `byuctf{}`.
E.g. `byuctf{CTF Players}`.

Reminder - all answers are case-INsensitive for all of these problems

1/15 attempts

Flag

Submit

Correct

| **Flag** : `byuctf{Remote Desktop Users}`

Challenge

10 Solves

×

Windows 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-windows>

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

×

Windows 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-windows>

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.

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.

2/15 attempts

Submit

Incorrect. You have 13 tries remaining.

bản này cũng không phải

Search Results

Showing 1 of 1 result for **Windows Server 2008 R2 Standard**

Show: 25 Sort by: CVE ID (new to old)

CVE-2015-6098

CNA: Microsoft Corporation

Buffer overflow in the Network Driver Interface Standard (NDIS) implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to gain privileges via a crafted application, aka "Windows NDIS Elevation of Privilege Vulnerability."

Show less

[Back to top of page](#)

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.

look up vulnerabilities associated with it.

6/15 attempts

byuctf{CVE-2018-1000861}

Submit

Incorrect. You have 9 tries remaining.

