2018-09-01-TokyoWesterners-CTF - Mondai	
Sistema Operativo:	**Linux**
Dificultad:	**Medium**

Técnicas utilizadas

- Packet Analysis / ICMP Traffic Filtering
- Data Extraction
- Python Scripting
- Password Cracking
- Hash Identification
- MD5 Decryption
- File Decompression

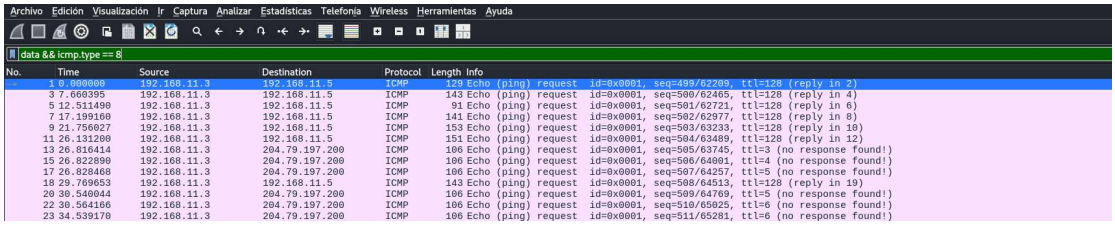
En el presente reto de criptografía, se proporcionó un archivo comprimido que contenía a su vez otro archivo comprimido, el cual requería una contraseña para ser accedido.

```
┌──(isolated)─(administrador㉿kali)-[~/Descargas]
└─$ zipinfo mondai.zip
Archive:  mondai.zip
Zip file size: 10041 bytes, number of entries: 1
-rw-a--     2.0 fat     9923 b- stor 18-Sep-01 03:29 y0k0s0.zip
1 file, 9923 bytes uncompressed, 9923 bytes compressed:  0.0%

┌──(isolated)─(administrador㉿kali)-[~/Descargas]
└─$ unzip mondai.zip
Archive:  mondai.zip
 extracting: y0k0s0.zip

┌──(isolated)─(administrador㉿kali)-[~/Descargas]
└─$ zipinfo y0k0s0.zip
Archive:  y0k0s0.zip
Zip file size: 9923 bytes, number of entries: 2
-rw-a--     6.3 fat     3948 Bx defN 18-Aug-31 22:26 capture.pcapng
-rw-a--     6.3 fat     8677 Bx defN 18-Sep-01 03:29 mondai.zip
2 files, 12625 bytes uncompressed, 9605 bytes compressed:  23.9%

┌──(isolated)─(administrador㉿kali)-[~/Descargas]
└─$ unzip y0k0s0.zip
Archive:  y0k0s0.zip
[y0k0s0.zip] capture.pcapng password:
```

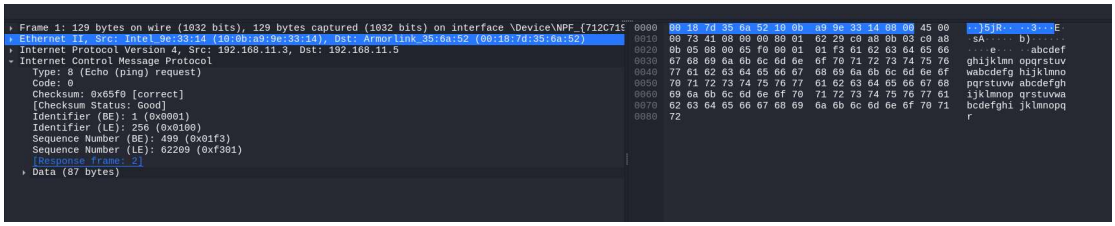
Ante la ausencia de credenciales válidas, opté por utilizar el mismo nombre del archivo como contraseña, lo cual resultó ser correcto. Dentro de este segundo archivo comprimido, se encontraba un tercer archivo comprimido y un archivo adicional destinado a ser analizado con Wireshark.

```
┌──(isolated)─(administrador㉿kali)-[~/Descargas]
└─$ unzip y0k0s0.zip -d challenge
Archive:  y0k0s0.zip
[y0k0s0.zip] capture.pcapng password:
  inflating: challenge/capture.pcapng
  inflating: challenge/mondai.zip

┌──(isolated)─(administrador㉿kali)-[~/Descargas]
└─$ ls -l
total 28
drwxrwxr-x 2 administrador administrador  4096 oct 18 10:14 challenge
-rw-rw-r-- 1 administrador administrador 10041 oct 18 10:11 mondai.zip
-rw-rw-r-- 1 administrador administrador  9923 sep  1  2018 y0k0s0.zip

┌──(isolated)─(administrador㉿kali)-[~/Descargas]
└─$
```

Al analizar el archivo con Wireshark, descubrí que se había capturado tráfico ICMP. Procedí a filtrar los datos utilizando la expresión data && icmp.type==8. En este contexto, data se refiere a los paquetes que contienen información útil, es decir, aquellos que llevan la carga de datos que se está transmitiendo a través de la red. Por otro lado, icmp.type==8 filtra específicamente las trazas ICMP de tipo 8, conocidas como Echo Request. Este tipo de traza es comúnmente utilizado para enviar solicitudes de eco en el protocolo ICMP.



Investigando más a fondo los datos obtenidos, observé que si al valor de la longitud del paquete (length), que era 129, se le restaban 42 bytes, el resultado era 87, un valor que corresponde a un carácter en el código ASCII.



Para desencriptar el contenido, desarrollé un script en Python 3 que realizaba la conversión de los valores obtenidos a caracteres ASCII:

```python
#!/usr/bin/python3
def decrypt():
    print(''.join(map(lambda n: chr(n - 42), [129, 143, 91, 141, 153, 151, 106, 106, 106, 143, 106, 106, 106])))
if __name__ == '__main__':
    decrypt()
```

Finalmente, logré desencriptar el mensaje, aunque en ese momento no estaba seguro de su utilidad.

```
┌──(administrador㉿kali)-[~/Descargas/challenge]
└─$ python3 decrypt_wireshark.py
We1com@@@e@@@

┌──(administrador㉿kali)-[~/Descargas/challenge]
└─$
```

Posteriormente, al acceder al archivo comprimido mondai.zip, encontré una lista con una combinación de letras y caracteres especiales, junto con otro archivo comprimido. Posiblemente, esta lista contenía las credenciales necesarias para descomprimir el archivo adicional.

```
┌──(administrador㉿kali)-[~/Descargas/challenge]
└─$ zipinfo mondai.zip
Archive:  mondai.zip
Zip file size: 8677 bytes, number of entries: 2
-rw-a--     6.3 fat    10999 Bx defN 18-Aug-31 22:40 list.txt
-rw-a--     6.3 fat      758 Bx defN 18-Sep-01 03:13 mondai.zip
2 files, 11757 bytes uncompressed, 8371 bytes compressed:  28.8%

┌──(administrador㉿kali)-[~/Descargas/challenge]
└─$ unzip mondai.zip -d mondai
Archive:  mondai.zip
[mondai.zip] list.txt password:
  inflating: mondai/list.txt
  inflating: mondai/mondai.zip

┌──(administrador㉿kali)-[~/Descargas/challenge]
└─$ cd mondai

┌──(administrador㉿kali)-[~/Descargas/challenge/mondai]
└─$ ls
list.txt  mondai.zip
```

Por tanto, utilicé el comando zip2john para obtener el hash necesario y proceder a crackearlo con John the Ripper. Finalmente, obtuve la contraseña que me permitió acceder a los archivos contenidos en el archivo comprimido.

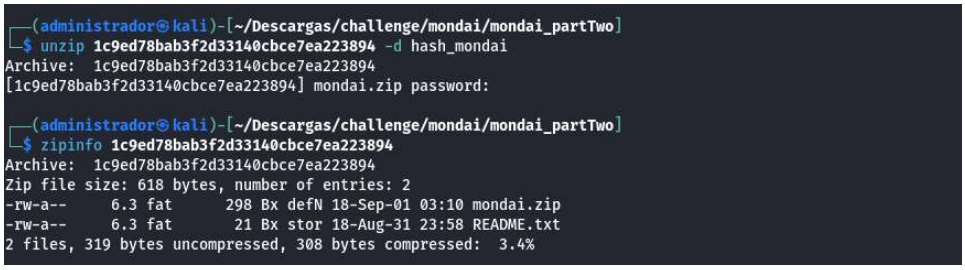
```
┌──(administrador㉿kali)-[~/Descargas/challenge/mondai]
└─$ zip2john mondai.zip
ver 2.0 mondai.zip/1c9ed78bab3f2d33140cbce7ea223894 PKZIP Encr: cmplen=560, decmplen=618, crc=5361F7E2 ts=196A cs=5361 type=8
mondai.zip/1c9ed78bab3f2d33140cbce7ea223894:$pkzip$1*1*2*0*230*26a*5361f7e2*0*3e*8*230*5361*eafc9406758d89f12eeff0ca6ccafc22e9cea12f6c915a5f3a679ffd
4079fddcdb3e355329c6bdc4832e77c92064bd1e95f614c34502c256e4a5d5b4ce63463403f90e03058c455e954fcb1b11847e1e2c0593a687096be3cd6eae3e5171bdc1a3e88f97583c
b585a946d2f1ce625930e65eca1f11097292f2c3c71dee03a9839510025b09c956e0beea5f14029ba75b393f88463efbb4df42eebe2b180567ee4df1894fcc96dc0e92b0f579c0848de1
8d6aca192ddfab7be5d05388b81a48ff5da30f59d0713a5c4f6465ecd74314b75a25d886f1fec31184a0926ead96bf39d3148e102a50f152d2c7bfa0985081ae16bcef24cc174ba731b6
bf1e01a382d7bbae3580d92f8d8a1a6482232ced5fa61501c54730330f97ab63c1fdad63b519e31b2a81dceb19ae9c194959ff136b747902051d0445c916addde99a5031419acca325ec
1eacad00a62813a6b44023*$/pkzip$:1c9ed78bab3f2d33140cbce7ea223894:mondai.zip::mondai.zip

┌──(administrador㉿kali)-[~/Descargas/challenge/mondai]
└─$ zip2john mondai.zip > mondai_hash
ver 2.0 mondai.zip/1c9ed78bab3f2d33140cbce7ea223894 PKZIP Encr: cmplen=560, decmplen=618, crc=5361F7E2 ts=196A cs=5361 type=8

┌──(administrador㉿kali)-[~/Descargas/challenge/mondai]
└─$ john -w=list.txt mondai.zip
Warning: invalid UTF-8 seen reading mondai.zip
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

┌──(administrador㉿kali)-[~/Descargas/challenge/mondai]
└─$ john -w=list.txt mondai_hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
eVjbtTpvkU       (mondai.zip/1c9ed78bab3f2d33140cbce7ea223894)
1g 0:00:00:00 DONE (2024-10-18 11:05) 100.0g/s 100000p/s 100000c/s 100000C/s nb`_hlPYgZ..WsYYhSUXP]
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

El archivo mondai.zip contenía otro archivo comprimido con una larga cadena de números y letras, posiblemente un hash MD5. Lo curioso de este archivo es que, a pesar de estar comprimido, no tenía extensión.

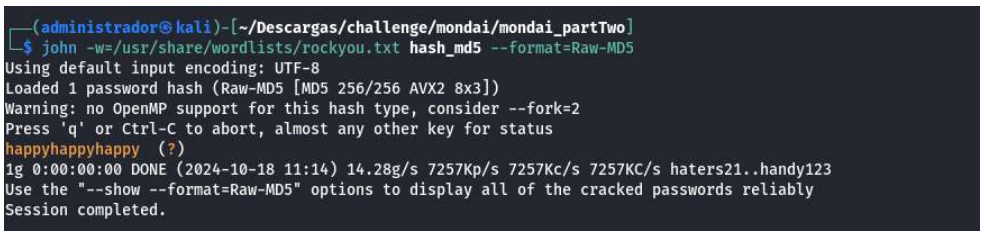
```
┌──(administrador㉿kali)-[~/Descargas/challenge/mondai]
└─$ unzip mondai.zip -d mondai_partTwo
Archive:  mondai.zip
[mondai.zip] 1c9ed78bab3f2d33140cbce7ea223894 password:
  inflating: mondai_partTwo/1c9ed78bab3f2d33140cbce7ea223894

┌──(administrador㉿kali)-[~/Descargas/challenge/mondai]
└─$ cd mondai_partTwo

┌──(administrador㉿kali)-[~/Descargas/challenge/mondai/mondai_partTwo]
└─$ file 1c9ed78bab3f2d33140cbce7ea223894
1c9ed78bab3f2d33140cbce7ea223894: Zip archive data, at least v2.0 to extract, compression method=deflate

┌──(administrador㉿kali)-[~/Descargas/challenge/mondai/mondai_partTwo]
└─$ xxd 1c9ed78bab3f2d33140cbce7ea223894
00000000: 504b 0304 1400 0800 0800 4d19 214d acc3  PK........M.!M..
00000010: 5247 2b01 0000 2a01 0000 0a00 0000 6d6f  RG+...*.......mo
00000020: 6e64 6169 2e7a 6970 30fc c34b ee61 96e5  ndai.zip0..K.a..
00000030: b013 69de c1c0 694e 6bc7 cc63 596a 1ff1  ..i...iNk..cYj..
00000040: f09b d8b0 f487 4c14 3596 955f 7833 1ea5  ......L.5.._x3..
00000050: 3f8a 1b5f 00de 1c8b ef27 4c99 41c3 4749  ?.._.....'L.A.GI
00000060: 4607 7029 eee6 ef66 d80a a7f1 84f4 7df7  F.p)...f......}.
00000070: 9605 6674 3306 0856 9ff0 6fce 871a 0ae2  ..ft3..V..o.....
00000080: 5a34 a219 4db0 f276 91cd 80de 3626 ca17  Z4..M..v....6&..
00000090: 4f7f f920 e695 eca1 e8e2 6a09 b37c 7709  O.. ......j..|w.
000000a0: 4fb6 c675 7738 eaa9 e119 4cb1 2884 975d  O..uw8....L.(...]
000000b0: c371 e4d1 286b 5938 3529 ddbf b18b 6b9d  .q..(kY85)....k.
000000c0: c2a7 3934 d850 f9ad b249 2a3e 7768 669e  ..94.P...I*>whf.
000000d0: c388 de66 8211 bbe1 6b3b b874 a724 f67f  ...f....k;.t.$..
000000e0: a7c7 96da f93f 0bd6 9b9e 53b3 98db 0d30  .....?....S....0
000000f0: 9a38 7bf5 6f2f 4efe 745b 6724 b54a 8255  .8{.o/N.t[g$.J.U
00000100: 773b 7a01 ef4a ff07 faf1 b2bd 8ee2 b63e  w;z..J.........>
00000110: c06f 3adf 836d 1ae1 eadf 8bb7 4296 8e58  .o:..m......B..X
00000120: ca3f 3fd4 5102 e0ed 3fd4 1a1e a03c 077f  .??.Q...?....<..
00000130: 0775 30ad 4a1e f834 8e11 5ce1 0394 ee51  .u0.J..4..\....Q
00000140: 8dc0 6759 bf6b e5e2 0f8a 87c5 9d7f dab0  ..gY.k..........
00000150: 88e4 4b50 4b03 0414 0001 0000 0058 bf1f  ..KPK........X..
00000160: 4d2f 7d3e ae21 0000 0015 0000 000a 0000  M/}>.!..........
00000170: 0052 4541 444d 452e 7478 745c df5c 4b2a  .README.txt\.\K*
00000180: 7332 4193 effc c466 2db9 6124 1153 b6e6  s2A....f-.a$.S..
00000190: 1c56 cf4b 1080 7467 e86f 321e 504b 0102  .V.K..tg.o2.PK..
000001a0: 3f00 1400 0800 0800 4d19 214d acc3 5247  ?.......M.!M..RG
000001b0: 2b01 0000 2a01 0000 0a00 2400 0000 0000  +...*.....$.....
000001c0: 0000 2000 0000 0000 0000 6d6f 6e64 6169  .. .......mondai
000001d0: 2e7a 6970 0a00 2000 0000 0000 0100 1800  .zip.. ..... . .
000001e0: a095 41e4 5541 d401 0aa4 41e4 5541 d401  ..A.UA....A.UA..
000001f0: 9fa7 b5bf 5541 4d01 504b 0102 3f00 1400  ....UA..PK..?...
00000200: 0800 0800 58bf 1f4d 2f7d 3eae 2100 0000  ....X..M/}>.!...
00000210: 1500 0000 0a00 2400 0000 0000 0000 2000  ......$....... .
00000220: 0000 5301 0000 5245 4144 4d45 2e74 7874  ..S...README.txt
00000230: 0a00 2000 0000 0000 0100 1800 b371 cc1e  .. ..........q..
00000240: 3b41 d401 085c c9f9 5541 d401 085c c9f9  ;A...\..UA...\..
00000250: 5541 d401 504b 0506 0000 0000 0200 0200  UA..PK..........
00000260: b800 0000 9c01 0000 0000                 ..........
```

Para confirmar el tipo de hash encontrado, utilicé la herramienta hash-identifier, la cual verificó que efectivamente se trataba de un hash MD5.

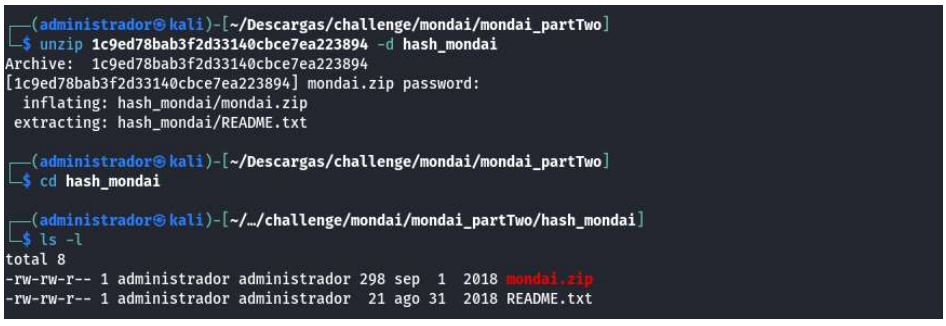
Sin embargo, al intentar descomprimir el archivo, se me solicitó una contraseña que no poseía.



Dado que no tenía credenciales disponibles, intenté desencriptar el hash MD5 y utilizarlo como contraseña.



Sorprendentemente, esto funcionó, permitiéndome acceder al contenido del archivo, donde encontré otro archivo comprimido y un archivo de texto.



Finalmente, el archivo readme indicaba que la contraseña era muy corta, por lo que probé con ‘to’, resultando ser correcta. De esta manera, obtuve la flag.