Description

'Suspicious' is written all over this disk image. Download suspicious.dd.sda1

Hints

- It may help to analyze this image in multiple ways: as a blob, and as an actual mounted disk.
- Have you heard of slack space? There is a certain set of tools that now come with Ubuntu that I'd recommend for examining that disk space phenomenon...

Solución

```
kali@kali: ~/shared/notas-seguridad-redes2024/picoCTF/parciales/parcial_02/parte_04_forensic_02/pitter_patter_platters
File Actions Edit View Help
 GNU nano 8.1
                                                      suspicious.dd.sda1
                                                `AA^@
                                                     ^a^BA^a
                                        ^aA^a
                        `a∙a^a
                               `മ•മ′
Blost+found
                                                                                `Asuspicious-file.txt
                                                        ^Btce′
 `[+(t^X:^NM++Ht(*++Q4*+dr^B)"++2)+^D]J+S&E+hL&V+rx*+^B+#+++^X+F++Tg+q++V^]+F^P+@^@+k+T+?+t3^D+='
X^A****l^G**^E*<M**^*+xM****k*5*^Zx^M*^F^^S**;^*[^U*^C**^U**W**^HU**^S*S*^O**^zzU**^U**W**^zes*^z**W**lm^
eGQ*:=*w*D^XQ_******fh**>*X*0M^W***x08;**^S^\*^W[*^V*D^PEKu*3j*(^A#***J*X****F*^SA**(*C****T**Z*U*)%**^S^[
|5*$*n*z*M****SD*L*u!**04^V*~Y*^\K9^Q*öd**~Y*f__*,^D**^*r*(^H&(****^\*^\?*J*J*_"*n***&OP**^W*V*R#Y***S*
****t0'*@5^?-%*{*^^*r*XvZ*^A*A**^Cy^D******4U*q^@^_Z^H^E*g***X***8*R"C*
*a*^T^R**R***^L**bF*^Q^Z%*^P^YE=^T=**^^z*(^H*C***H**N**,#*W**y~ww***E*6.****~=***"^\v*J*o<*!**f
•0)•J^GHB•••p^_|~•
                  ^***$S$$^N$[*D${^E$|3^$$$^Y$^G$$^T$$^P$$R*$$$$}$$$k$$rbC$$$+z^F$$$$¬籛<^$$$^$\n^]$^Y=$$Yf$S$$\>
 **2T~2^_<***9.^
 ����<mark>Br</mark>ɗ��An�^D��5 �^S�hM*�9�@�N�^D�}�$�����H�1�^@�SW^B�y^Sێ��+^U�¼4 wI^E9���� �Y^F�^S
   :R+c!+!+*^[R++
e,U+^@X)X+U +D>++^K^R+^B+^S++=+0:^H`+^@^K^N^@(:+++f+v+++^[^L+j+^@(;X++k+|+^_+k^C+m+>++[3++]+U@v+m+ ^D
                                                                                       `_◆k^C�m�>��[3��]�Ц@v�m� ^D R^E>
`L�e"D�3�dso�$^Z.;�4��p^S�o��^RGV>
             L! + +> ++^E++^\{?++$^
                                        Y • • • • • • • • • • ^ M ^ X 7 • Nbtc? • • • • • ; ^ G • • • e • ^ Z
•(r•P^^/•:]^N |^?PA`ź^K•J••t•-•L;^T••4••^K• •FYI•JTY•••
 ^◆#◆◆l^U◆<Hb~[Jh◆(Q◆◆◆◆◆~◆◆T"R◆◆j◆b^Q^+p◆^R%:^V◆啕 ◆Z9 y◆f<◆G□@>◆
                                                                                   ♦|♦i♦♦r♦^TV♦♦6♦^G♦]♦^Xi^Kj[:WRK♦^]♦>

        **_k**j***Eca<*t***a(^N@k***WK^DS**$**K^UT***B*****E*Qe****Y**L****X*TJ***_'***5*s*[</td>

        3M**k**F4***}A****X[*S**>*1*Y*L,***Cl*

   `Z���7��^C��^B^N�2S��h9B^Fj��y�A���æB��GP�;<Ku,"��^_��^�zw^M��w�/�y3ę^^L@=v.���?=�v�h����^Z�^L��}fV^O�s��
«۴۰(«dko~««!«********/۵۰۵» و اهمونو کړ=۶۰۰!۳۵ کې ۱۹۰۵ ک
[ Read 55930 lines
                  O Write Out
                                     Where Is
                                                                         Execute
                                                                                                         M-U Undo
G Help
                                                                                          Location
                    Read File
   Exit
                                      Replace
                                                       Paste
                                                                         Justify
                                                                                           Go To Line
```

Al utilizar NANO se observa que no será fácilmente así que procedemos a:

```
r—(kali⊕kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/pitter_patter_platters]
└─$ strings -e b suspicious.dd.sdal
6b7d549b_3<_|Lm_111t5_3b{FTCocip
```

```
qQWTYUiI0Pb
FGjJKLs
ZXvc
#+3; CScs
!1Aa
qQWTYUiI0Pb
FGjJKLs
ZXvc
#+3; CScs
!1Aa
#+3; CScs
! 1Aa
777777777
┌──(kali⊕kali)-
[~/.../parciales/parcial_02/parte_04_forensic_02/pitter_patter_platters]
└$ strings -e b suspicious.dd.sdal | rev
picoCTF{b3_5t111_mL|_<3_b945d7b6
bP0IiUYTWQq
sLKJjGF
cvXZ
scSC; 3+#
aA1!
bP0IiUYTWQq
sLKJjGF
cvXZ
scSC;3+#
aA1!
scSC;3+#
aA1!
777777777
```

Bandera

```
flag: picoCTF{b3_5t111_mL|_<3_b945d7b6}
```

Notas Adicionales

El comando strings -e b suspicious.dd.sda1 | rev busca y extrae todas las cadenas de texto legibles en el archivo suspicious.dd.sda1, interpretando los bytes en formato bigendian (-e b), y luego invierte cada una de esas cadenas usando el comando rev. Esto puede ser útil para buscar texto legible que esté en un formato específico (como un archivo binario o un volcado de memoria) y detectar patrones o datos invertidos, como contraseñas o información codificada.

Referencias

.