Usando "strings tag":
.encriptador - um executável?
chmod u+x .encriptador && ./.encriptador - roda o .encriptador
mkdir -p $USER && cp ~/* $USER 2> /dev/null - linha de comando
http://ix.io/2c6V - link que baixa se entrar
encripta_arquivos - nome de função ou diretório não sei
write_data - traduzindo deve ser o nome de uma função
Rodando com GDB:
Printa string: "Olá"
Faz syscall: "mkdir -p $USER && cp ~/* $USER 2> /dev/null"
(Ele faz um diretório copia com o cp e joga fora em null)
"Procure por uma forma de decodificá-los
OBS: Não desligue sua máquina, se não não será mais possível recuperar os dados!!!

(VOCÊ FOI OWNADO AQUI)

brincadeira, fiz uma cópia da sua home no diretório atual e encriptar seus arquivos lá, rs"

Agora tem no diretório que eu estou um executável .encriptador um diretório com meu nome de usuário que não tinha NADA

Usando o gdb vejo que "encripta_arquivos" e "write_data" são funções , mas não consegui fazer nada com isso. O gdb falou que usa 'libthread_db', catei na internet e achei algo sobre pthreads.

Ai eu usei "strings .encriptador":
u3UH - estranho
[]A\A]A^A_ - estranho
usage: ./%s <argument> - deve funcionar assim?
Error : Failed to open input directory - %s - saida de erro %s/%s - erro
Error : Failed to open %s - %s - erro
%s.leo - coloca os arquivos em .leo(AHHHHHHHHH)
find $USER -type f ! -name '*.leo' -delete - bash script ;*3$" - estranho (muito)

Não existia nada na pasta "thvelos" (PQ NAO TINHA NADA E ISSO ME TRAVOU PQ NAO TINHA NADA NA MINHA HOME MEUS DEUS) e deu erro e eu fiquei mais perdido que criança no carrefour.

Ai eu inocente baixei um txt um no lugar errado e de novo fui fazer a tag e voilà agora tem algo na pasta thvelos que criou

fui tentar ler o arquivo .leo e nossa tava tudo estranho e eu pensei bom encriptou vamo começar a lista:
-base64
-cifra de césar
-md5(?????? não mas eu to listando)
(Não tinha nenhum caracter especial então pensei em algo simples)

Bom base64 não era pois a palavra “corno” do meu txt nao estava “Y29ybm8=” (também não tinha nenhum = no txt logo exclui a possibilidade de ser base64)

Agora vamos pra cifra de cesar a palavra “corno” do meu txt estava “htwst” e voilà de novo, eu usei o site https://www.dcode.fr/caesar-cipher que faz um brute force e a primeira que apareceu lá com +5 foi “corno”(print cifra.png)

Então agora eu sei que ele encripta com cifra de cesár e sei que é +5 então é só eu passar ./encriptador -5 que ele defaz tudo (será)

E FINALMENTE VOILÀ desfez

Agora a gente precisa renomear os arquivos(podia fazer na mão mas um bash script ajuda aqui se existirem muitos arquivos,eu não me dei muito o trabalho pois só tinha 1)
Mas podemos usar o Rename(sudo pacman -Su rename)
rename ‘s/.leo/.txt/’ *.leo
OBS:Usar o rename é mais seguro que usar o mv(eu já perdi uma tag usando mv então nunca mais)

E remove o .leo com
rm $USER/*.leo