Usando "strings tag":
.encriptador - Provavelmente um executavel
chmod u+x .encriptador && ./.encriptador - linha de comando para rodar o.encriptador
mkdir -p $USER && cp ~/* $USER 2> /dev/null - linha de comando
http://ix.io/2c6V - link que baixa algo se entrar
encripta_arquivos - nome de função ou diretório não sei
write_data - traduzindo deve ser o nome de uma função ou um diretório
Rodando com GDB:
Printa : "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(mas não me aprofundei muito).

Usando "strings .encriptador":
u3UH - indefinido
[]A\A]A^A_ - indefinido
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??
find $USER -type f ! -name '*.leo' -delete - bash script ;*3$" - indefinido

Não existia nada na pasta "thvelos"
Então depois de baixar um txt no lugar errado e mais um dia tentar fazer a tag,agora tinha algo na pasta thvelos

Fui tentar ler o arquivo .leo e nossa tava tudo encriptador e eu pensei bom encriptou vamos começar a listar possíveis formas:
-base64
-cifra de césar
-md5
(Devia ser algo pois não haviam sinais só letras diferentes)

Então base64 não era pois a palavra “corno”(não me pergunte o por que do corno no txt só aceite) do meu txt nao estava “Y29ybm8=” (também não tinha nenhum = no txt logo exclui a possibilidade de ser base64)

Agora vamos pra cifra de césar a palavra “corno” do meu txt estava “htwst” e usando 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 césar e sei que é +5 então talvez seja só eu passar ./encriptador -5 que ele defaz tudo

E finalmente conseguimos decriptar tudo(o arquivo txt)

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

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