LAB - SEM 08 - Hashes e Senhas

LAB01: CleanZoomHost38.exe
Quando baixamos o arquivo caso.zip e unzipamos ele, encontramos todos os arquivos no diretório integridade. Dentro dele, executamos

```
for palavra in $(ls); do echo "$palavra"; cat "$palavra" | md5sum; done
```

```
CleanZoomHost36.exe
37ecb62f912e85ac16faf220a3d09292  -
CleanZoomHost37.exe
37ecb62f912e85ac16faf220a3d09292  -
CleanZoomHost38.exe
6bc664de142144d81576fe4788d60327  -
CleanZoomHost39.exe
37ecb62f912e85ac16faf220a3d09292  -
CleanZoomHost4.exe
37ecb62f912e85ac16faf220a3d09292  -
CleanZoomHost40.exe
```

De onde ficou evidente qual o único arquivo com assinatura de hash diferente

LAB02: 37ecb62f912e85ac16faf220a3d09292
Resposta já do lab anterior

LAB03: 6bc664de142144d81576fe4788d60327
Resposta já do lab01

LAB04: 1d2da0cc838de8996cc71dc72bdbbe03d347b573cb3a4ab46c9e68987832f6bfe192579ab7604cdea76347828b3a0382602401e3417cc8a53e87da7565da4766

```
echo -n keeplearning | sha512sum
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali/Downloads/semana08/integridade]
└─# echo -n keeplearning | sha512sum
1d2da0cc838de8996cc71dc72bdbbe03d347b573cb3a4ab46c9e68987832f6bfe192579ab7604
cdea76347828b3a0382602401e3417cc8a53e87da7565da4766  -
```

LAB05: JDUkZGVzZWMkS2NhRGsxeEt6b05zZUtIclVEQ01CLjNqcHc4MHNzVFFydzFMdG56Rml5MA==
+ Aqui usamos a estrutura do openssl

```
openssl passwd -5 -salt desec 1337
```

Como o id da sha256 é 5 [pode ser visto nas anotações da aula de Senhas em Sistemas Linux], setamos ele depois do passwd e o salt usado foi desec, junto da senha 1337

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali/semana08]
└─# openssl passwd -5 -salt desec 1337
$5$desec$KcaDk1xKzoNseKHrUDCMB.3jpw80ssTQrw1LtnzFiy0
```

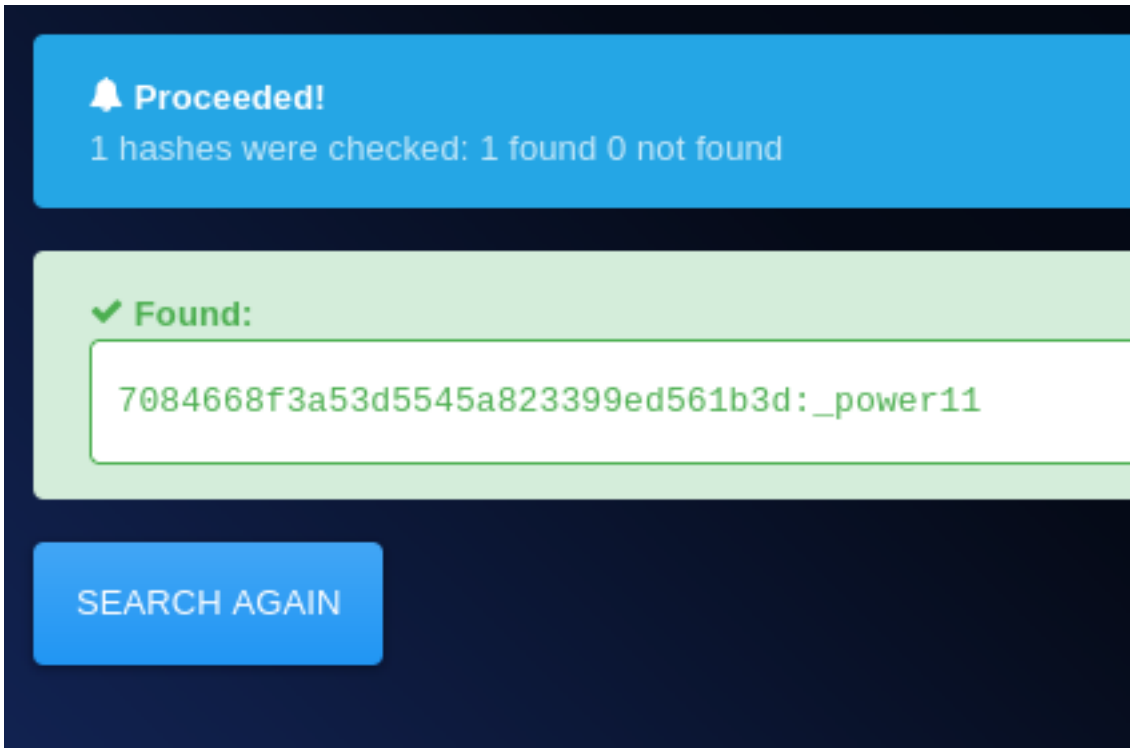
+ E aí, para que conseguíssemos fazer a conversão de base64, demos um contrabarra (\) antes dos "$" para que eles fossem reconhecidos como caracteres.

```
echo -n "\$5\$desec\$KcaDk1xKzoNseKHrUDCMB.3jpw80ssTQrw1LtnzFiy0" | base64
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali/semana08]
└─# echo -n "\$5\$desec\$KcaDk1xKzoNseKHrUDCMB.3jpw80ssTQrw1LtnzFiy0" | base64
JDUkZGVzZWMkS2NhRGsxeEt6b05zZUtIclVEQ01CLjNqcHc4MHNzVFFydzFMdG56Rml5MA==
```

LAB06: _power11

+ Usamos o site do https://hashes.com



LAB07: help123

+ Aqui eu saí fazendo testes com uma só palavra até que acertasse a combinação correta da aplicação das etapas descritas no enunciado. Quando encontrei, apliquei no mesmo script de antes:

```
for palavra in $(cat hsenhas.txt); do
echo -n "$palavra" " ";
echo -n "$(echo -n "$(echo -n "$palavra" | md5sum | cut -d " " -f 1)" |
base64)"| sha1sum;
done > saida
```

→ em que hsenhas.txt foi uma cópia da wordlist retirada e editada (apaguei o cabeçalho) do john

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali/semana08]
└─# for palavra in $(cat hsenhas.txt); do echo -n "$palavra" " "; echo -n "$(echo -n "$(echo -n
"$palavra" | md5sum | cut -d " " -f 1)" | base64)"| sha1sum; done > saida

┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali/semana08]
└─# grep "806825f0827b628e81620f0d83922fb2c52c7136" saida
help123  806825f0827b628e81620f0d83922fb2c52c7136  -
```