Estudo Técnico: Atacando Hashes

+ O objetivo aqui é entender o princípio da quebra de hashes

+ Como não há fórmulas para o hash reverso, o que fazemos é aplicar o operador de hash em milhares de possíveis senhas mais comuns até que se chegue a encontrar um hash igual ao que estamos tentando quebrar

+ Há sites que já guardam milhares dessas possíveis senhas como
https://hashes.com
https://md5decrypt.net

+ Mas aprenderemos a fazer isso de maneira manual (ataque de Rainbow Tables)

+ Primeiro devemos ter uma lista.txt com as possíveis senhas a serem quebradas

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali/semana08]
└─# cat senhas.txt
catulo
catulo2402
senha123
admin
root
mrcat123
```

+ Agora devemos pequisar pelo tipo de hash que estamos trabalhando

```
hashid 732646b4e740669986f108f41e36b71f
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali/semana08]
└─# hashid 732646b4e740669986f108f41e36b71f
Analyzing '732646b4e740669986f108f41e36b71f'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

→ testaremos esse md5

+ Para converter essas palavras da lista para o hash md5, fazemos

```
for palavra in $(cat senhas.txt); do echo -n "$palavra" " "; echo -n "$palavra" | md5sum; done
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali/semana08]
└─# for palavra in $(cat senhas.txt); do echo -n "$palavra" " "; echo -n "$palavra" | md5sum; done
catulo  e901abac19529ec85c460674ace16dd2  -
catulo2402  732646b4e740669986f108f41e36b71f  -
senha123  e7d80ffeefa212b7c5c55700e4f7193e  -
admin  21232f297a57a5a743894a0e4a801fc3  -
root  63a9f0ea7bb98050796b649e85481845  -
mrcat123  81abdf41b956c1b1277943474d735e91  -
```

+ Podemos salvar essa saída para um arquivo qualquer como resultadomd5

```
for palavra in $(cat senhas.txt); do echo -n "$palavra" " "; echo -n "$palavra" | md5sum; done > resultadomd5
```

+ Para pesquisar nessa nova lista o hash procurado, fazemos

```
grep "732646b4e740669986f108f41e36b71f" resultadomd5
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali/semana08]
└─# grep "732646b4e740669986f108f41e36b71f" resultadomd5
catulo2402  732646b4e740669986f108f41e36b71f  -
```

toma!!!