Writeup - OffSec

Crack the hash - TryHackMe

Nicolas Sanson Giaboeski.

Para a sala Crack the hash, utilizamos algumas ferramentas básicas para decriptar as chaves dadas, dentre elas, estão o hashid e hash-identifier que analisam a chave e retornam um palpite da criptografia que foi utilizada na hash. Em seguida, foi utilizado a ferramenta hashcat e o site cyberchef para descriptografar.

Identificação das hashs no Level 1

```
 HASH: 48bb6e862e54f2a795ffc4e541caed4d

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

```
 HASH: CBFDAC6008F9CAB4083784CBD1874F76618D2A97

Possible Hashs:
[+] SHA-1
[+] MySQL5 - SHA-1(SHA-1($pass))
```

```
 HASH: 1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7B336B63032

Possible Hashs:
[+] SHA-256
[+] Haval-256
```

```
$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom
```

A chave mostrada acima não é identificada pelas ferramentas, porém, o início da chave $2y$ é um identificador de hash no formato bcrypt, que demoram bastante para descriptografar.

```
 HASH: 279412f945939ba78ce0758d3fd83daa

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

Identificação das hashs no Level 2

```
 HASH: F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85

Possible Hashs:
[+] SHA-256
[+] Haval-256
```

```
 HASH: 1DFECA0C002AE40B8619ECF94819CC1B

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

```
Hash: $6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.

Salt: aReallyHardSalt
```

Essa hash também é um tipo de bcrypt (sha512crypt) que não é identificada pelas ferramentas citadas.

```
 HASH: e5d8870e5bdd26602cab8dbe07a942c8669e56d6

Possible Hashs:
[+] SHA-1
[+] MySQL5 - SHA-1(SHA-1($pass))
```

Decrypt

O exemplo de uso do hashcat para encontrar as respostas é o seguinte:

```
┌──(kali㉿kali)-[~]
└─$ hashcat hash.txt -m 0 -a 0 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

Onde, chamamos a ferramenta com “hashcat”, passamos o arquivo em formato texto que contém a hash, a flag “-m 0” para indicar que é criptografia MD5, a flag “-a 0” para indicar que o modo de ataque vai ser Straight, e por fim passamos a wordlist que a ferramenta irá percorrer.

A flag m deve ser mudada de acordo com o tipo de criptografia que a chave utiliza.