

Primero se verifica que los Hash son de tipo md5 con la herramienta Hash Identifier:

```
Shell No.1
File Actions Edit View Help
Not Found.
HASH: 90965b0eb20e68b7d0b59accd2a3b4fd
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC(Wordpress))
[+] Haval-128
[+] Haval-128(HMAC)
[+] RipeMD-128
[+] RipeMD-128(HMAC)
[+] SNEFRU-128
[+] SNEFRU-128(HMAC)
[+] Tiger-128
[+] Tiger-128(HMAC)
[+] md5($pass.$salt)
[+] md5($salt.$pass)
[+] md5($salt.$pass.$username)
```

```
Shell No.1
File Actions Edit View Help
HASH: 0b29406e348cd5f17c2fd7b47b1012f9
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC(Wordpress))
[+] Haval-128
[+] Haval-128(HMAC)
[+] RipeMD-128
[+] RipeMD-128(HMAC)
[+] SNEFRU-128
[+] SNEFRU-128(HMAC)
[+] Tiger-128
[+] Tiger-128(HMAC)
[+] md5($pass.$salt)
[+] md5($salt.$pass)
[+] md5($salt.$pass.$username)
```

```
Shell No.1
File Actions Edit View Help
HASH: 6d5e43a73849ed75968279b6addb79ec
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC(Wordpress))
[+] Haval-128
[+] Haval-128(HMAC)
[+] RipeMD-128
[+] RipeMD-128(HMAC)
[+] SNEFRU-128
[+] SNEFRU-128(HMAC)
[+] Tiger-128
[+] Tiger-128(HMAC)
[+] md5($pass.$salt)
[+] md5($salt.$pass)
[+] md5($salt.$pass.$username)
```

```
Shell No.1
File Actions Edit View Help
HASH: 129e0c67567301df1e1088c9069b946
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC(Wordpress))
[+] Haval-128
[+] Haval-128(HMAC)
[+] RipeMD-128
[+] RipeMD-128(HMAC)
[+] SNEFRU-128
[+] SNEFRU-128(HMAC)
[+] Tiger-128
[+] Tiger-128(HMAC)
[+] md5($pass.$salt)
[+] md5($salt.$pass)
[+] md5($salt.$pass.$username)
```

```
Shell No.1
File Actions Edit View Help
HASH: 4e9878b1c28da4f305f17af5537f062a
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC(Wordpress))
[+] Haval-128
[+] Haval-128(HMAC)
[+] RipeMD-128
[+] RipeMD-128(HMAC)
[+] SNEFRU-128
[+] SNEFRU-128(HMAC)
[+] Tiger-128
[+] Tiger-128(HMAC)
[+] md5($pass.$salt)
[+] md5($salt.$pass)
[+] md5($salt.$pass.$username)
```

```
Shell No.1
File Actions Edit View Help
HASH: 66bb9ec43660194bc866bd8b4d35b151
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC(Wordpress))
[+] Haval-128
[+] Haval-128(HMAC)
[+] RipeMD-128
[+] RipeMD-128(HMAC)
[+] SNEFRU-128
[+] SNEFRU-128(HMAC)
[+] Tiger-128
[+] Tiger-128(HMAC)
[+] md5($pass.$salt)
[+] md5($salt.$pass)
[+] md5($salt.$pass.$username)
```

Luego con el comando md5sum se genera cada hash para realizar una comparación:

De acuerdo a los ultimas revisiones de las normativas y politicas de seguridad, estos son los hash md5 de los archivos

```
90965b0eb20e68b7d0b59accd2a3b4fd copia.sh
0b29406e348cd5f17c2fd7b47b1012f9 log.txt
6d5e43a730490d75968279b6adbd79ec pass.txt
129ea0c67567301df1e1088c9069b946 plan-A.txt
4e9878b1c28daf4305f17af5537f062a plan-B.txt
66bb9ec43660194bc066bd8b4d35b151 script.py
```

```
(vicherso@kali)~[~/Desktop]
$ md5sum copia.sh
90965b0eb20e68b7d0b59accd2a3b4fd copia.sh

(vicherso@kali)~[~/Desktop]
$ md5sum log.txt
f2b0428b975452afbc641e46a042231b log.txt

(vicherso@kali)~[~/Desktop]
$ md5sum pass.txt
6d5e43a730490d75968279b6adbd79ec pass.txt

(vicherso@kali)~[~/Desktop]
$ md5sum plan-A.txt
129ea0c67567301df1e1088c9069b946 plan-A.txt

(vicherso@kali)~[~/Desktop]
$ md5sum plan-B.txt
4e9878b1c28daf4305f17af5537f062a plan-B.txt

(vicherso@kali)~[~/Desktop]
$ md5sum script.py
66bb9ec43660194bc066bd8b4d35b151 script.py
```

Como se puede observar después del ataque el archivo log.txt fue modifica ya que su hash es diferente.