

**Universidad Nacional Autónoma de México**

**Facultad de Estudios Superiores Aragón**

**Alumno:** Bermeo Espino Juan Daniel

**Reporte de practica:** Ataque de fuerza bruta y diccionario

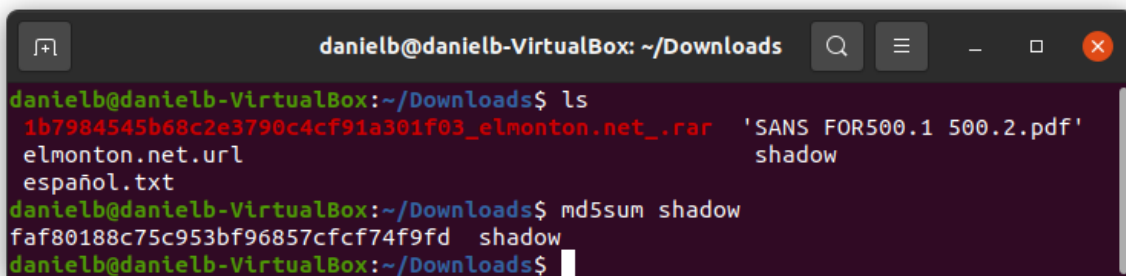
**Temas especiales de seguridad informática**

Grupo: 2060

**Profesor:** Jose Francisco Aguilar Hernandez

Semestre 2024-II

**1. Verificar la integridad del archivo Shadow (md 2, 4 ,5 SHA 1, 256, 384, 512, de todos). MD5 y SHA512 esperados:**

A screenshot of a terminal window titled 'danielb@danielb-VirtualBox: ~/Downloads'. The terminal shows the following commands and output:

```
danielb@danielb-VirtualBox:~/Downloads$ ls
1b7984545b68c2e3790c4cf91a301f03_elmonton.net_.rar  'SANS FOR500.1 500.2.pdf'
elmonton.net.url                                     shadow
español.txt
danielb@danielb-VirtualBox:~/Downloads$ md5sum shadow
faf80188c75c953bf96857cfcf74f9fd shadow
danielb@danielb-VirtualBox:~/Downloads$
```

En la captura se muestra como en nuestro sistema se identifica la ubicación donde descargamos el archivo shadow y procedemos a hacer la llamada al comando md5sum y comprobamos que es exactamente el que se esperaba.

**2. Romper las contraseñas en el archivo Shadow, Por Fuerza Bruta (tardado) o por ataque Diccionario (Rápido si la palabra está en el diccionario)**

### **Fuerza Bruta**

En la siguiente captura muestra un ataque al archivo shadow con el programa John The Ripper, en este primer caso es un ataque por fuerza bruta, y el funcionamiento del programa fue de 42 minutos aproximadamente.

```
danielb@danielb-VirtualBox: ~/Downloads
danielb@danielb-VirtualBox:~/Downloads$ john shadow
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
forense01      (forense)
a              (firewall)
2g 0:00:13:21 74% 2/3 0.002496g/s 163.6p/s 462.3c/s 462.3C/s Avatar?...Corvette?
2g 0:00:13:24 74% 2/3 0.002487g/s 163.6p/s 462.4c/s 462.4C/s Sapphire?...Trish?
2g 0:00:13:26 74% 2/3 0.002481g/s 163.5p/s 462.4c/s 462.4C/s Cristina?...Katrina?
2g 0:00:13:30 75% 2/3 0.002468g/s 163.5p/s 462.5c/s 462.5C/s Cirque?...Huang?
2g 0:00:20:29 3/3 0.001627g/s 160.9p/s 464.3c/s 464.3C/s bibee...bunit
2g 0:00:20:33 3/3 0.001622g/s 160.9p/s 464.3c/s 464.3C/s 104113...104231
2g 0:00:23:45 3/3 0.001403g/s 159.6p/s 462.9c/s 462.9C/s annolo...anapid
2g 0:00:40:52 3/3 0.000815g/s 155.4p/s 456.9c/s 456.9C/s cise...clad1
2g 0:00:42:00 3/3 0.000793g/s 155.2p/s 456.7c/s 456.7C/s soppy06...sopcary
2g 0:00:42:20 3/3 0.000787g/s 155.2p/s 456.8c/s 456.8C/s bonety7...bonaley
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

Siendo un ataque de fuerza bruta no se obtuvieron muchos resultados (solo 2), los resultados los obtenemos con el comando show aunque también son lanzados conforme se van encontrando.

```
danielb@danielb-VirtualBox: ~/Downloads
danielb@danielb-VirtualBox:~/Downloads$ john --show shadow
forense:forense01:16898:0:99999:7:::
firewall:a:17052:0:99999:7:::

2 password hashes cracked, 3 left
danielb@danielb-VirtualBox:~/Downloads$
```

## Diccionario

Para el ataque de diccionario se usó un documento de diccionario en español proporcionado por el profesor, este ataque fue considerablemente menos tardado y se concluyó en tan solo 1'24"

```
danielb@danielb-VirtualBox: ~/Downloads
danielb@danielb-VirtualBox:~/Downloads$ john --wordlist=español.txt shadow
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/64])
Remaining 3 password hashes with 3 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
c              (marzo)
b              (dmz)
camara         (captacion)
3g 0:00:01:24 100% 0.03557g/s 446.2p/s 448.5c/s 448.5C/s calzaras...camarist
Use the "--show" option to display all of the cracked passwords reliably
Session completed
danielb@danielb-VirtualBox:~/Downloads$
```

Después de realizar este segundo ataque john obtiene 3 contraseñas mas

```
danielb@danielb-VirtualBox: ~/Downloads
danielb@danielb-VirtualBox:~/Downloads$ john --show shadow
forense:forense01:16898:0:99999:7:::
firewall:a:17052:0:99999:7:::
dmz:b:17052:0:99999:7:::
marzo:c:17052:0:99999:7:::
captacion:camara:17052:0:99999:7:::

5 password hashes cracked, 0 left
danielb@danielb-VirtualBox:~/Downloads$
```

### 3. Resultado que arroje el comando mkpasswd con la contraseña FESAragonUNAMsi y la salt OKXE6xme utilizar SHA de 256 y 512 bits

Finalmente con el último ejercicio me acabo de agenciar el conocimiento de cómo hacer contraseñas seguras para mis redes, además de eso podemos ver la diferencia entre la encriptación SHA en 256 y 512, ya que se está ingresando la misma contraseña, sin embargo, podemos ver como en la versión 512 se incluyen caracteres especiales (. /) además de la obvia mayor extensión

```
danielb@danielb-VirtualBox: ~/Downloads
danielb@danielb-VirtualBox:~/Downloads$ mkpasswd -m sha-256 FESAragonUNAMsi -s OKXE6xme
$5$OKXE6xme$8wVN71g LX2fRNQqJ50Muxod0nFMLodfZNck2Adbtu25
danielb@danielb-VirtualBox:~/Downloads$ mkpasswd -m sha-512 FESAragonUNAMsi -s OKXE6xme
$6$OKXE6xme$9nh45hM9Mg7Jf6c2AxGLM3QL4t2qnUZw2nmn.qRv/QLxs8tw9oFcn2P12stCTngIEkFGX63g3T4
vZJhPkye56.
danielb@danielb-VirtualBox:~/Downloads$
```