Laborator 6

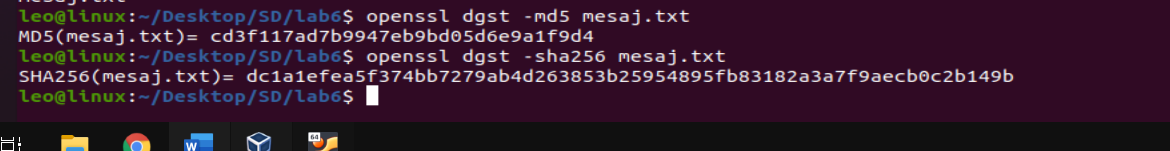
Parvan Andrei Leonard

Comenzi pregatitoare:

1. Adaugati userul curent in grupul *sudoers: usermod -aG sudo <username>*, unde *username* este userul cu care sunteti logat. Reporniti masina virtuala
2. Instalati utiltarul *john: sudo apt install john*. *John* este un utilitar care va permite sa faceti bruteforcing sau dictionary attacks asupra parolelor.

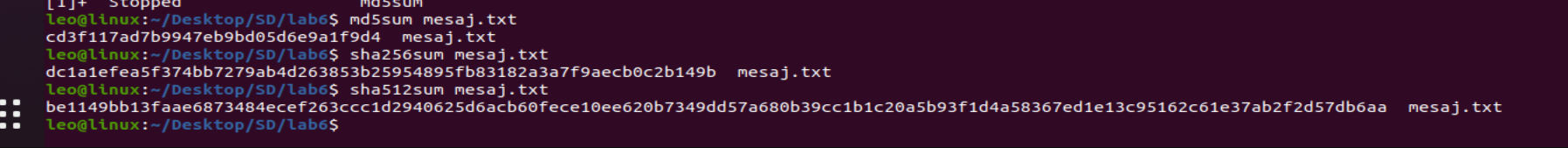
Cerinte laborator:

1. (2p) Utilizati următoarea comandă *openssl dgst dgsttype filename* pentru a genera hash-ul unui fişier. Pentru a consulta manualele tastaţi *man openssl* şi *man dgst* în linia de comandă. Înlocuiţi *dgsttype* cu un algoritm de dispersie specific cum ar fi -md5, -sha256, etc. La această activitate trebuie să testaţi minim doi algoritmi diferiţi şi să descrieţi observaţiile



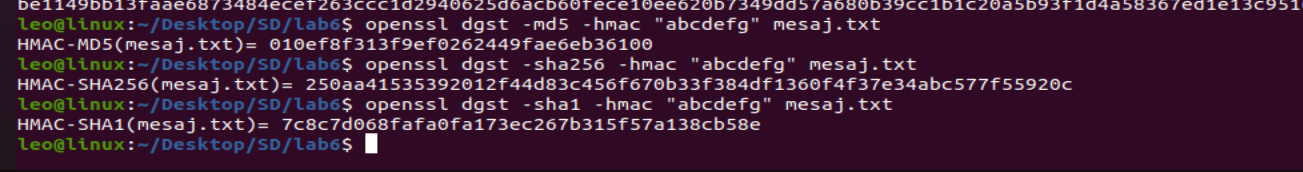
Fiecare algoritm genereaza propriul sau hash. Daca schimbam algoritmul sau modificam mesajul avem alt hash.

1. (2p) Aceleaşi rezultate pot fi obţinute şi prin folosirea directă a comenzilor *md5sum, sha1sum, sha224sum, sha256sum, sha384sum, sha512sum*.  Testati minim 2 algoritmi si comparati rezultatele.



Hash-urile sunt la fel ca cele obtinute cu comanda openssl dgst atata timp cat respectam conditiile si anume fisierul ramane la fel si folosim acelasi algoritm.

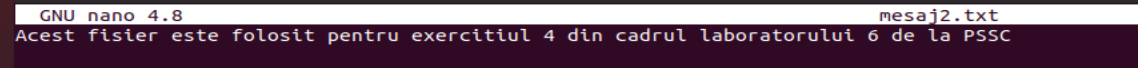
1. (2p) La această activitate trebuie generat un hash cu cheie (MAC) pentru un fişier. Puteţi folosi opţiunea *-hmac: openssl dgst -md5 -hmac "abcdefg" filename.*Generaţi minim 2 rezumate cu cheie folosind HMAC-MD5, HMAC-SHA256 şi HMAC-SHA1 pentru fişiere la alegere.



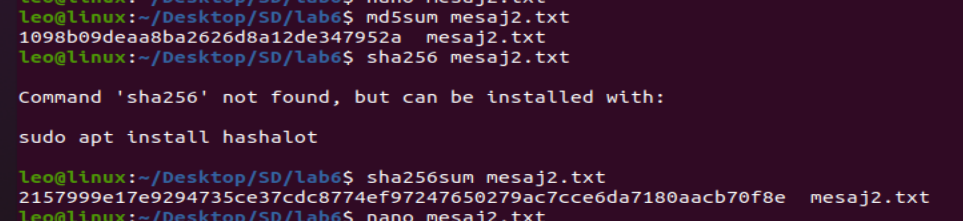
1. (3p) Efectuati următorul exerciţiu pentru MD5 şi SHA256:

             a. Creaţi un fişier de orice lungime

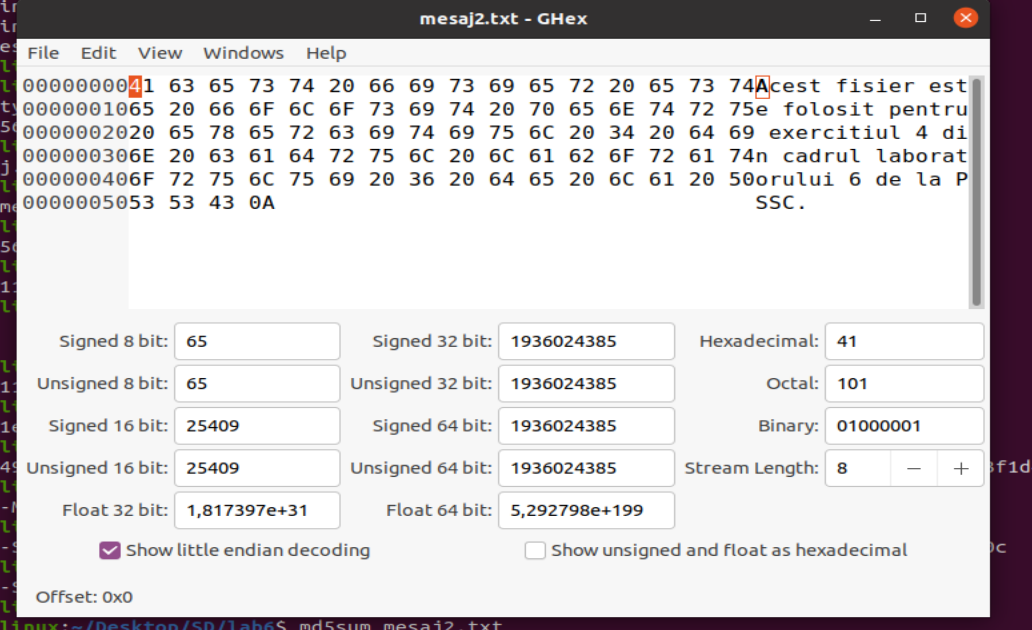


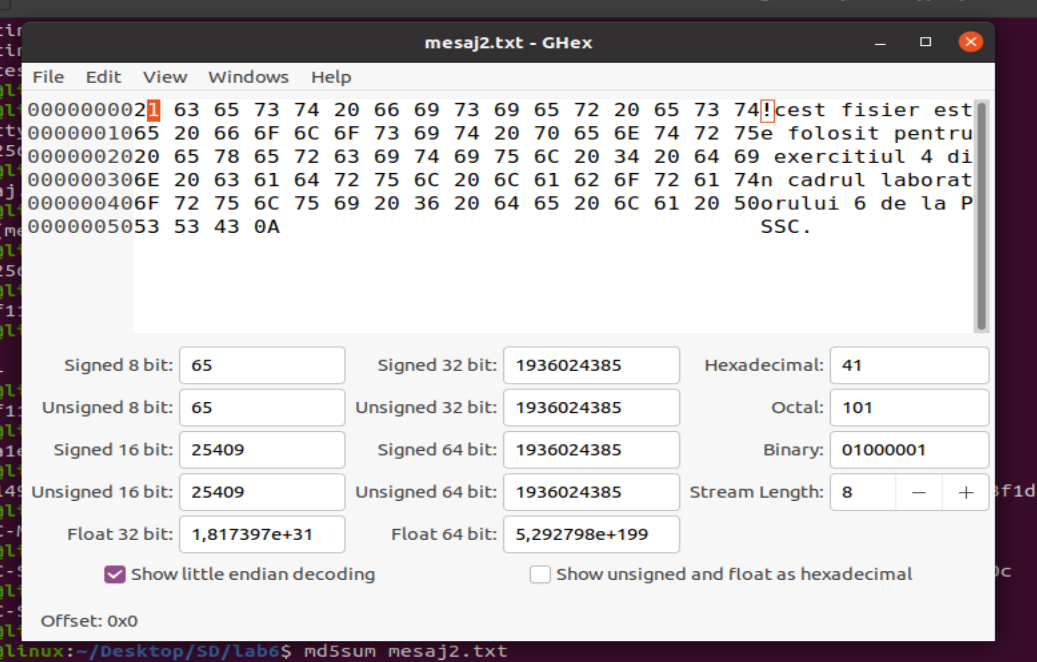


             b.  Generaţi hash-ul H1 pentru acest fişier folosind ambii algoritmi de dispersie

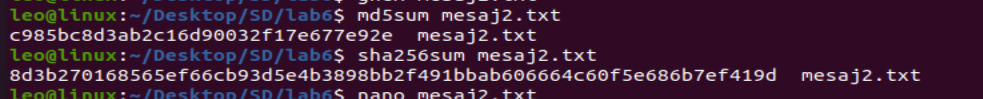


             c. Inversaţi un bit din fişierul de intrare. Puteţi efectua modificarea utilizând ghex.





             d. Generaţi hash-ul H2 pentru fişierul modificat.



             e. Observaţi dacă H1 şi H2 sunt sau nu similare. Descrieţi observaţiile.

Atat H1 cat si H2 nu sunt similare. Din cauza ca s-a modificat un bit din fisier acesta a produs un cu totul alt hash indiferent algoritmul folosit.

      5. (1p) Folositi utilitarul *unshadow* pentru a genera un fisier cu userii si parolele din Linux: sudo *unshadow /etc/passwd /etc/shadow > credentials.txt.*Folositi *john* pentru a gasi parolele aferente userilor Linux.

