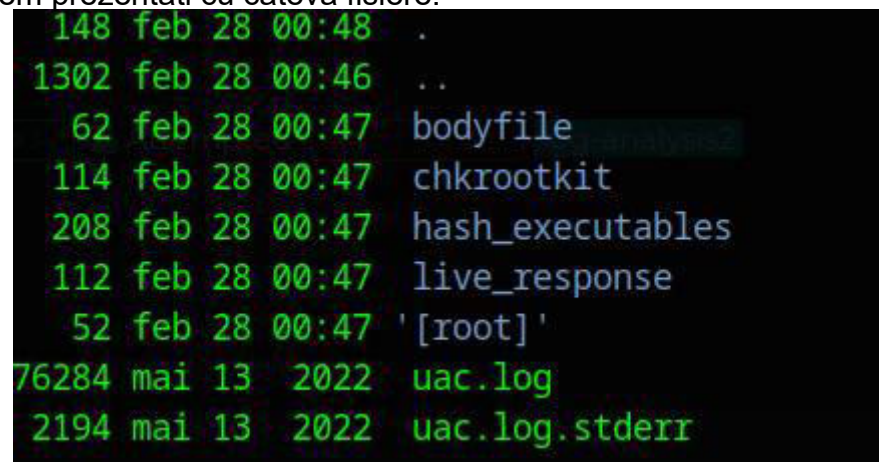
log-analysis2

Similar cu primul (pentru mine a fost mai usor decat primul) dupa ce extragem fisierele prezente suntem prezentati cu cateva fisiere:



Q1. Which is the machine id of the compromised host? (Points: 100) Acessez folderul de root si in el intru in /etc (contine majoritatea fisierelor de configurare ale sistemului) si dupa citesc ce se afla in machine id

Raspuns:8d200bff9e81….905ed77e21306

Q2. What is the name of the scheduled task created by the attacker on the compromised machine? (Points: 100)

Pentru a gasi asta ar trebui sa intru in crontab si sa vad ce task este scheduled la un interval de timp .În directorul **`/var/spool/cron/crontabs/`**, se află fișiere care conțin job-urile cron programate pentru diferiți utilizatori ai sistemului.Singurul lucru de facut aici este de citit acel fisier si de a vedea ce are programat userul bitsentinel la un interval de timp.

Raspuns:
qSCYAp….ko

Q3. Which antivirus is used by the compromised computer? (Points: 100)

uac.log este de obicei un fișier jurnal (log file) asociat cu activitatea User Account Control (UAC) în Windows. Acesta înregistrează evenimente legate de controlul contului de utilizator, cum ar fi:

- **Cereri de escaladare a privilegiilor** (când o aplicație cere drepturi de administrator)
- **Aprobări sau refuzuri** ale prompturilor UAC
- **Erori** apărute în timpul acestor procese

Am deschis acel fisier si am dat grep la av (antivirus) si primim raspunsul la intrebare deoarece antivirusul a fost instalat in /var/lib/ :

Raspuns: cl..av

Q4. Which is the latest command executed on the compromised machine? (Points: 100)

Pentru a raspunde la aceasta intrebare trebuie sa ne uitam la bash history specific la userul bitsentinel si o sa vedem in fisierul [root]/home/bitsentinel/.bash_history raspunsul:

Raspuns:sudo….

Trolled by masquerade8077