Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 7

# La disciplina „Tehnici de Inginerie Inversa”

A efectuat: st. gr. SI-211 S. Chirita

A verificat: C. Maxim

Chișinău – 2024

Introducere

Binwalk este un instrument gratuit și open-source folosit pentru analizarea imaginilor de firmware. Acesta poate identifica diferite tipuri de fișiere încorporate într-o imagine de firmware, inclusiv arhive comprimate, cod executabil și fișiere imagine.

Binwalk folosește o varietate de tehnici pentru a identifica aceste tipuri de fișiere, inclusiv scanarea de semnături și dezasamblarea. Scanarea de semnături implică căutarea în imaginea de firmware a unor modele cunoscute de octeți care sunt asociate cu tipuri specifice de fișiere. Dezasamblarea implică descompunerea codului mașină al imaginii de firmware într-un format mai ușor de citit de oameni. Acest lucru poate ajuta la identificarea codului sau a datelor încorporate care ar putea să nu fie ușor de recunoscut folosind scanarea de semnături.

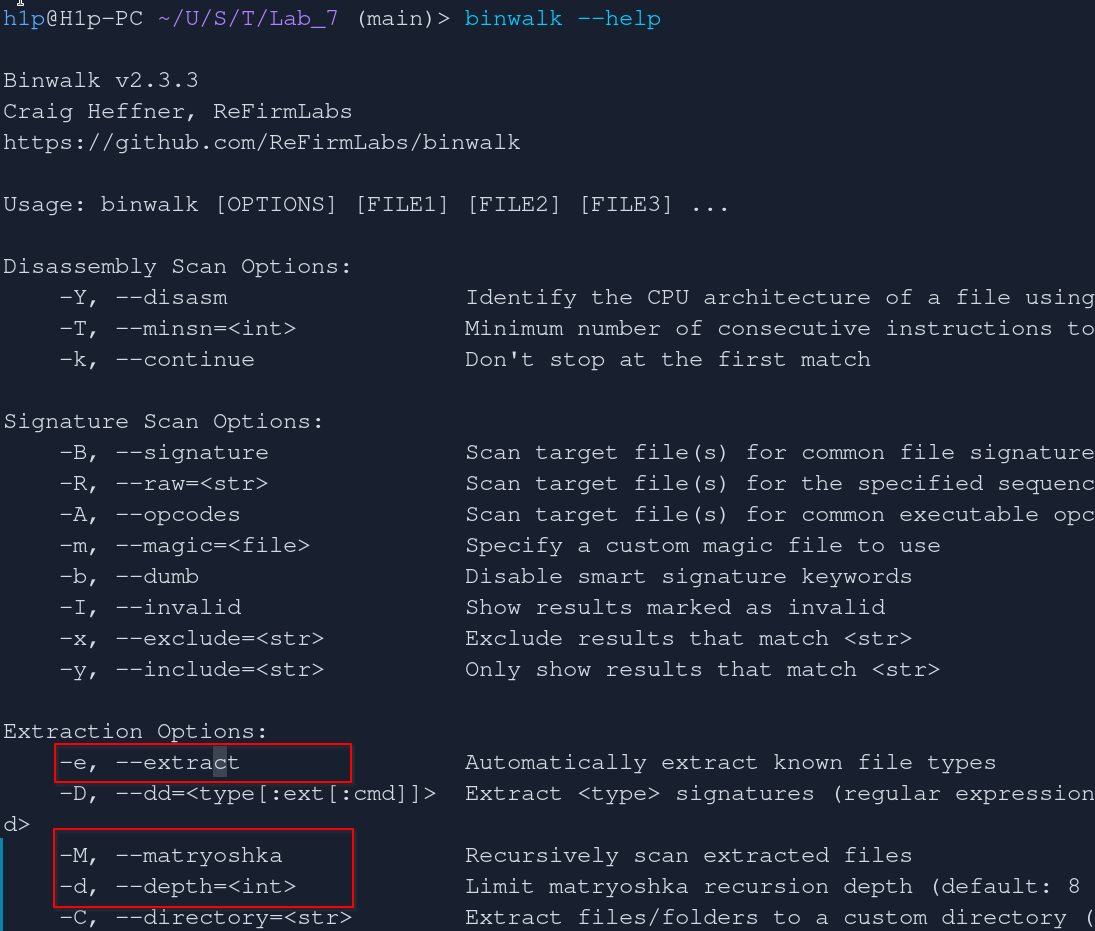
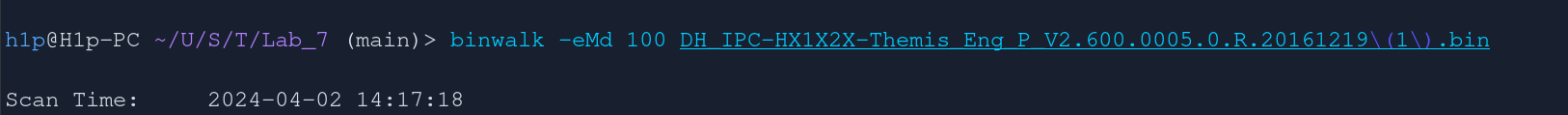


Figura 1 – Meniul help pentru binwalk

Comanda binwalk -eMd 100 DH\_IPC-HX1X2X-Themis\_Eng\_P\_V2.600.0005.0.R.20161219\(1\).bin este folosită pentru a analiza și extrage informații dintr-un fișier binar specificat. Iată o explicație fără enumerare:

* binwalk: Este instrumentul utilizat pentru analizarea fișierelor binare și extragerea conținutului înglobat din acestea.
* -e: Opțiunea care indică Binwalk să extragă conținutul înglobat găsit în fișierul binar specificat.
* -M: Această opțiune indică Binwalk să efectueze analiza pe mai multe nivele de înglobare, dacă este necesar.
* -d 100: Specifică adâncimea maximă de înglobare pe care Binwalk o va urmări în căutarea conținutului înglobat.
* DH\_IPC-HX1X2X-Themis\_Eng\_P\_V2.600.0005.0.R.20161219\(1\).bin: Este numele fișierului binar de intrare, din care Binwalk va extrage și analiza conținutul.

Această comandă este utilă pentru analiza și extragerea conținutului înglobat din fișiere binare, oferind o imagine detaliată a structurii și conținutului acestora.

Figura 2 – Extragerea fișierilor ascunse

**Conținutul directorului:**

* Fișier sign.img:
  + Tip: imagine raw.
  + Potențiale tipuri de fișiere identificate de binwalk:
    - Squashfs file systems.
    - Kernel images.
    - Compressed archive files.

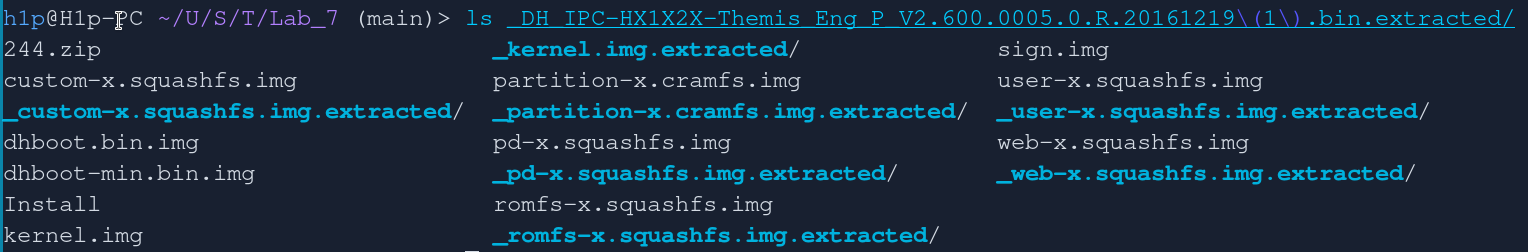
****

Figura 3 – Fișierile extrase

Comanda grep -r "admin" \_DH\_IPC-HX1X2X-Themis\_Eng\_P\_V2.600.0005.0.R.20161219\(1\).bin.extracted este utilizată pentru a căuta recursiv în directorul \_DH\_IPC-HX1X2X-Themis\_Eng\_P\_V2.600.0005.0.R.20161219\(1\).bin.extracted după orice apariții ale șirului "admin".

* grep: Este un utilitar de linie de comandă care caută șabloane de text în fișiere.
* -r: Această opțiune indică grep să căute recursiv în toate subdirectoarele din directorul specificat.
* "admin": Este șirul de text căutat, în acest caz, cuvântul cheie "admin".
* \_DH\_IPC-HX1X2X-Themis\_Eng\_P\_V2.600.0005.0.R.20161219\(1\).bin.extracted: Este directorul în care se va efectua căutarea. Acesta este directorul în care Binwalk a extrag filele din fișierul binar specificat.

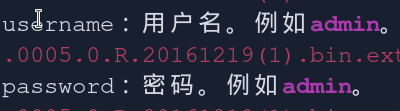


Figura 4 – Credințialile by default

**Concluzie:**

După ce Binwalk a fost folosit pentru a extrage conținutul înglobat, este important să inspectați conținutul fișierelor extrase, să căutați fișiere de configurare, fișiere de setări sau alte fișiere care ar putea conține credențiale implicite. Este important să menționăm că găsirea credențialelor implicite în fișierele binare poate ridica întrebări de securitate și sănătatea informațiilor. Utilizatorii și administratorii de sisteme trebuie să fie conștienți de acest lucru și să ia măsuri corespunzătoare pentru a asigura securitatea și integritatea datelor.

**Bibliografie:**

* **https://manpages.org/binwalk**
* **https://manpages.org/grep**