Øvelse 11 – Brugerkontoer med svage passwords

Information

Formålet med denne øvelse er at gøre dig bevidst om, hvorfor det er vigtigt at anvende stærke passwords. Selv når der anvendes en stærk hash-algoritme, yder hashen kun begrænset beskyttelse for svage kodeord. Dette skal der eksperimenteres med i denne øvelse.

Øvelsen viser også meget tydeligt, hvorfor kontroller som *CIS 18* eller *ISO 27002* har et stærkt fokus på password-politikker, både på systemniveau og i den generelle organisation.

I øvelsen skal der oprettes en bruger med et svagt kodeord. Herefter skal du trække kodeordshashet ud fra shadow-filen og forsøge at genskabe passwordet ud fra hash-værdien.

Bogen *Mastering Ubuntu server* giver en fin vejledning til hvordan man kan implementer password politik på *Ubuntu server* med F.eks. *Pluggable Authentication Module(PAM)*

Instruktioner

Alle kommandoer skal eksekveres mens du er i dit hjemme directory

---

1 Opsætning af værktøjer og testbruger

1. installer værktøjer `john-the-ripper` med kommandoen `sudo apt install john`
2. Her efter skal du downloade en *wordlist* kaldet rockyou med følgende kommando `wget https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt`.
3. Opret nu en bruger ved navn `misternaiv` og giv ham passwordet `password`

---

2 Udtræk og analyse af password-hash

1. Hent nu det hashet kodeord for misternaiv med følgende kommando `sudo cat /etc/shadow | grep misternaiv > passwordhash.txt`
2. udskriv indholdet af filen `passwordhash.txt`, og bemærk hvilken krypterings algoritme der er brugt.

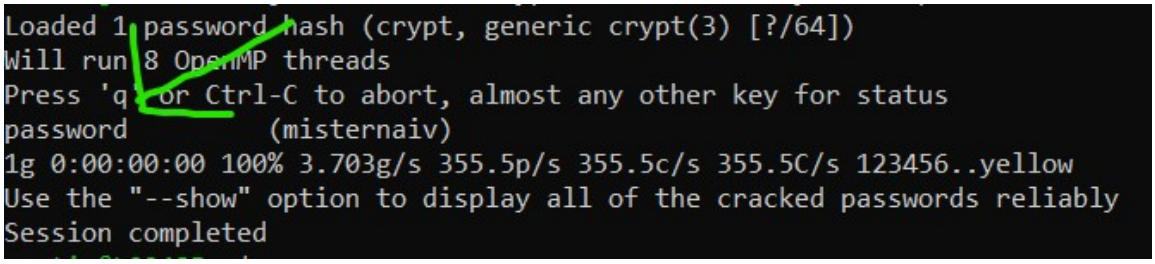
---

3 Knækning af svagt password

1. Eksekver nu kommandoen `john -wordlist=rockyou.txt passwordhash.txt`.
2. Kommandoen resulter i `No password loaded`.
   Dette er fordi john the ripper værktøjet ikke selv har kunne detekter hvilken algoritme det drejer sig om.
3. Eksekver nu kommandoen: `john --format=crypt -wordlist=rockyou.txt passwordhash.txt`.

format fortæller john the ripper hvilken type algoritme det drejer sig om

1. Resultat skulle gerne være at du nu kan se kodeordet, som vist på billede nedenunder.



---

4 Sammenligning med stærkt password

1. gentag processen fra trin 1 af.
   Men med et stærkt password.
   (minnimum 16 karakterer, både store og små bogstaver, samt special tegn)
2. Reflekter over hvorfor komplekse kodeord er vigtige og de fleste sikkerheds standarder har meget fokus på dem.

Last update: 2026-03-20 13:58:28