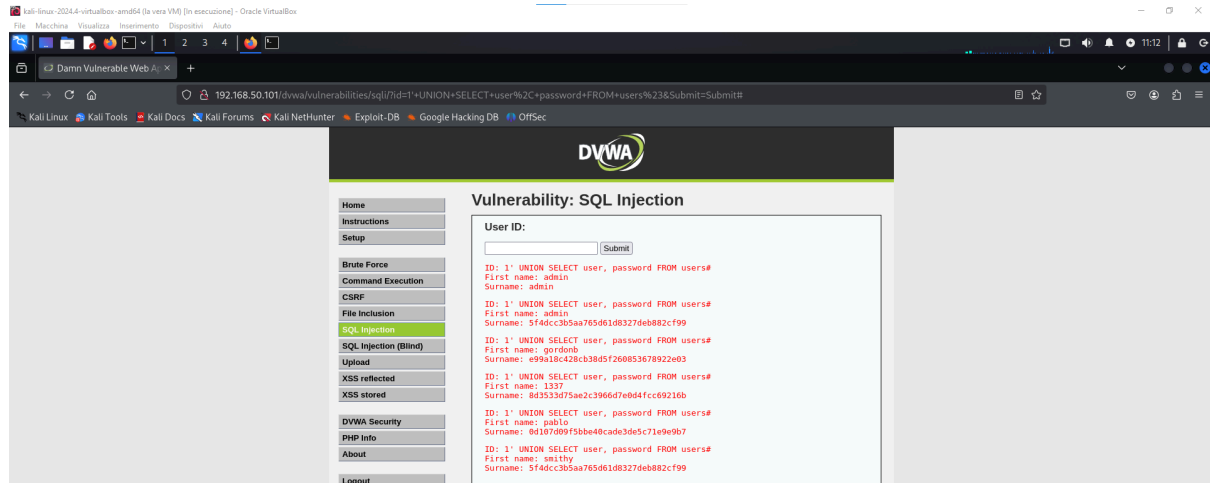
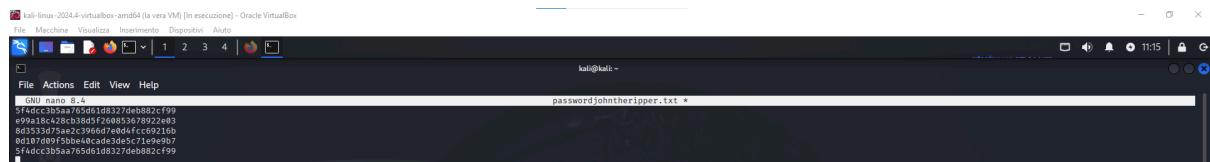


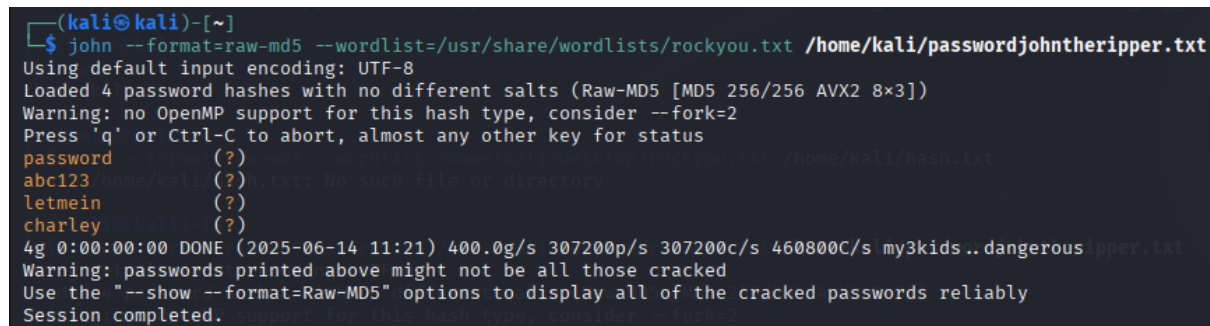
Nello scorso esercizio abbiamo trovato le password degli utenti sfruttando le query e database con SQL injection ma le password trovate non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5. Adesso proveremo ad eseguire delle sessioni di cracking sulla password con John the Ripper per recuperare la loro versione in chiaro.



facciamo un file di testo con le password



e poi eseguiamo:



Format, specifica il tipo di hash da craccare.

--wordlist, specifica il dizionario da utilizzare per craccare le password.

/home/kali/passwordjohntheripper.txt specifica il file con gli hash delle password da craccare.

Hai appena scoperto che l'azienda che segui come consulente di sicurezza ha un computer con Windows infettato dal malware WannaCry. Cosa fai per mettere in sicurezza il tuo sistema?

**Intervento immediato sul sistema infetto:**

- Disconnettere immediatamente il computer infetto dalla rete per evitare ulteriore diffusione
- Isolare fisicamente la macchina infetta
- Avviare un backup offline dei dati critici, se possibile
- Notificare il team IT e il management dell'incidente di sicurezza

**Elenco delle possibilità di messa in sicurezza:**

- Formattazione e reinstallazione pulita
- Ripristino da un backup precedente all'infezione
- Utilizzo di strumenti di rimozione malware specializzati
- Aggiornamento a un sistema operativo più recente e supportato