**Pratica S6L4**

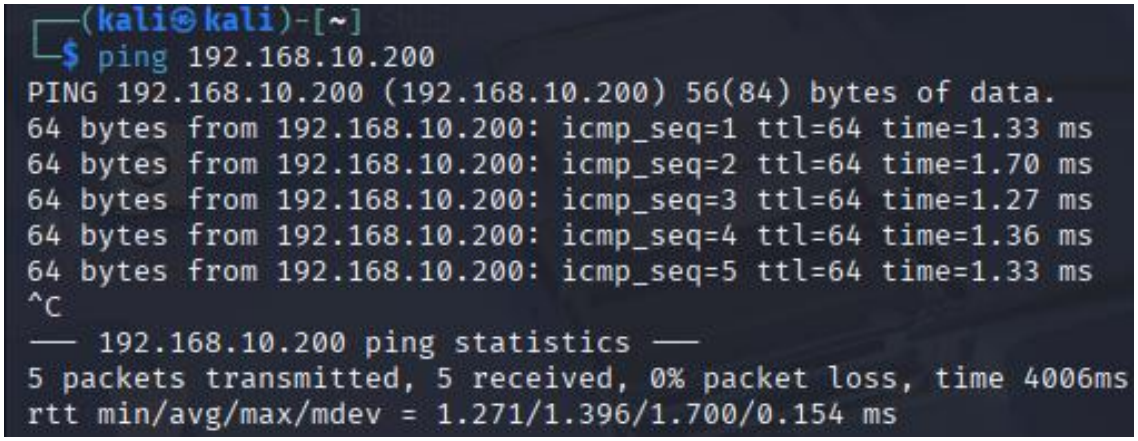
**Introduzione**: l'obiettivo di questo esercizio è recuperare le password hashate presenti nel database dell'applicazione web DVWA e successivamente eseguire un password cracking utilizzano lo strumento John the Ripper (JTR).

1. **Configurazione del laboratorio**

Il laboratorio è stato configurato usando due macchine virtuali Kali Linux (attaccante) e Metasploitable2 (bersaglio)

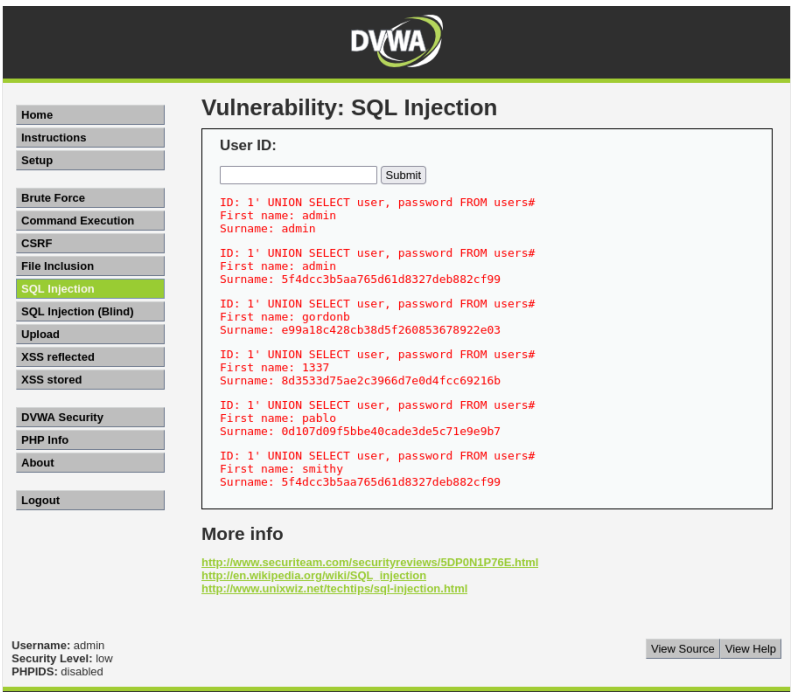
- Kali Linux IP: 192.168.10.100
- Metasploitable2 IP: 192.168.10.200

La comunicazione tra le due macchine è stata verificata tramite un comando di ping da Kali a Metasploitable2.




2. **SQL Injection**

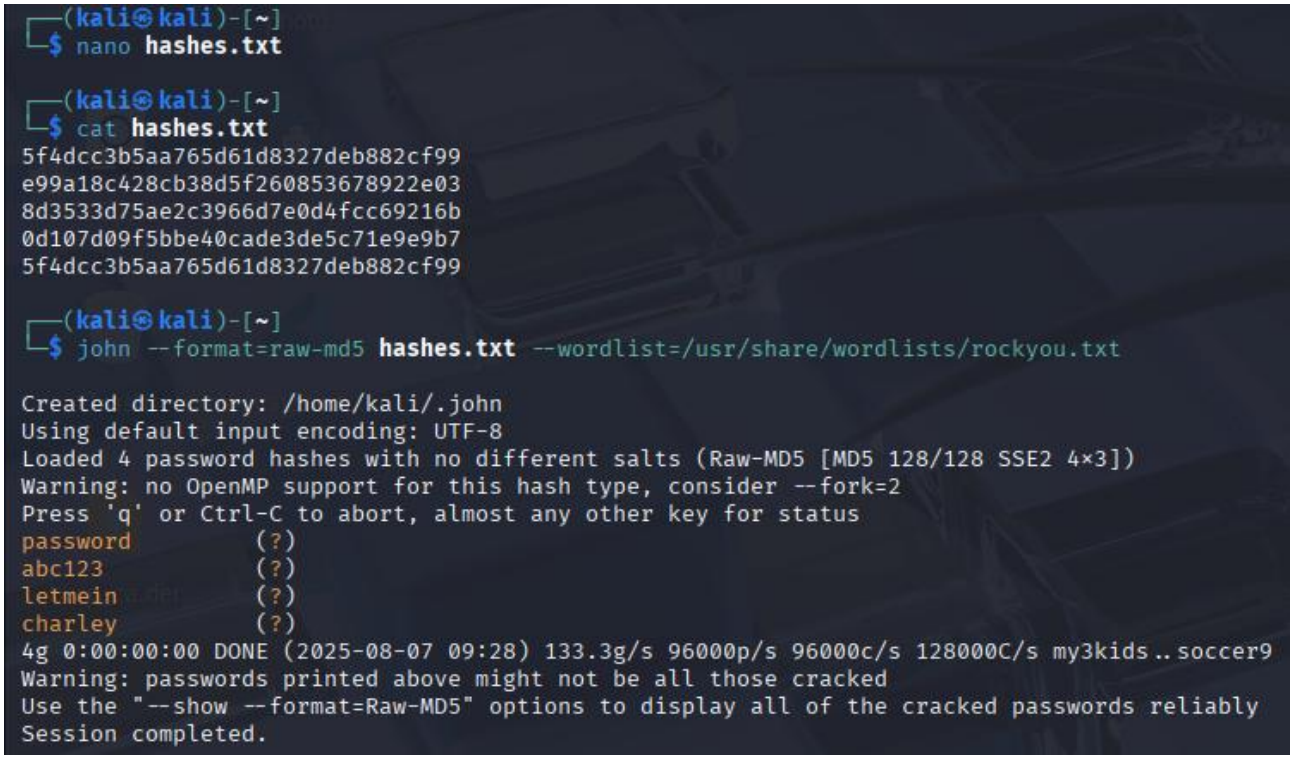
Una volta effettuato l'accesso a DVWA e aver impostato il livello di sicurezza su low, è stato utilizzato l'SQL Injection per estrarre i dati del database. Per eseguire ciò è stato usato il payload "1' UNION SELECT user, password FROM users#".



Questo payload ha permesso di estrarre le credenziali hashate direttamente dal database. Gli hash recuperati sono risultati di tipo MD5.

3. **Creazione del file hashes.txt e utilizzo di JTR**

Gli hash ottenuti sono stati copiati e salvati in un file di testo chiamato “hashes.txt”. Dopo la creazione del file è stato usato il tool John the Ripper per il cracking delle password.




**Conclusioni e osservazioni**

L'esercizio ha evidenziato l'efficacia delle tecniche di SQL Injection combinate con il cracking degli hash. L'utilizzo di hash MD5, ormai considerato insicuro, ha permesso il recupero delle password in chiaro in pochi secondi. Questo dimostra l'importanza di implementare controlli di input robusti e utilizzare algoritmi di hashing più sicuri, come bcrypt o Argon2. Inoltre, la disponibilità di dizionari come rockyou.txt facilita ulteriormente il lavoro degli attaccanti.