PASSWORD CRACKING:

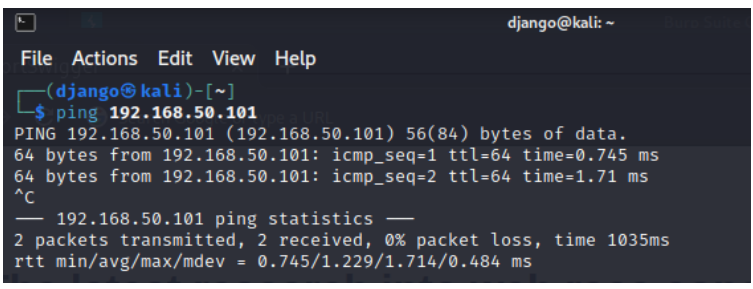
#DVWA #KALI LINUX #JOHN THE RIPPER

TRACCIA: PASSWORD CRACKING
ABBIAMO VISTO COME SFRUTTARE UN ATTACCO SQL INJECTION PER RECUPERARE LE PASSWORD DEGLI UTENTI DI UN DETERMINATO SISTEMA. SE GUARDIAMO MEGLIO ALLE PASSWORD TROVATE, NON HANNO L'ASPETTO DI PASSWORD IN CHIARO, MA SEMBRANO PIÙ **HASH DI PASSWORD MD5**.
RECUPERATE LE PASSWORD DAL DB COME VISTO, E PROVATE AD ESEGUIRE DELLE SESSIONI DI CRACKING SULLA PASSWORD PER RECUPERARE LA LORO VERSIONE IN CHIARO.
SENTITEVI LIBERI DI UTILIZZARE QUALSIASI DEI TOOL VISTI NELLA LEZIONE TEORICA.
L'OBIETTIVO DELL'ESERCIZIO DI OGGI È CRACCARE TUTTE LE PASSWORD TROVATE PRECEDENTEMENTE.

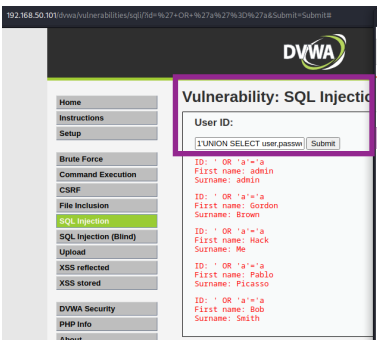
CONSEGNA:

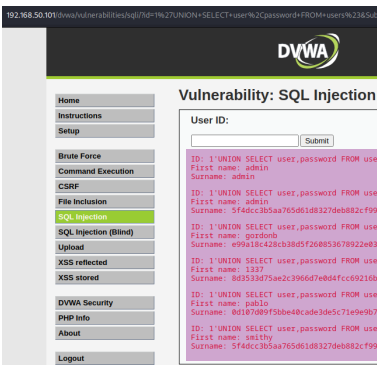
1. SCREENSHOT DELL'SQL INJECTION GIÀ EFFETTUATA
2. DUE RIGHE DI SPIEGAZIONE DI COS'È **QUESTO** CRACKING (QUALE TIPOLOGIA / QUALE MECCANISMO SFRUTTA)
3. SCREENSHOT DELL'ESECUZIONE DEL CRACKING E DEL RISULTATO

AL FINE DELL'ESERCIZIO È SUFFICIENTE CHE LE DUE MACCHINE (KALI E METASPLOITABLE) SIANO SULLA STESSA RETE, LASCIO QUINDI L'IP DI METASPLOITABLE SIA 192.168.50.101, MENTRE QUELLO DI KALI LINUX RESTERÀ 192.168.50.100. E FACCIO UN PING DI PROVA DA KALI.



IN SEGUITO MI CONNETTO DA CHROMIUM DI BURPSUITE ALL'APP VULNERABILE INSTALLATA SU METASPLOITABLE TRAMITE IL SUO INDIRIZZO IP E MANTENENDO LA SICUREZZA SU LOW RIPORTO L'ATTACCO SQL INJECTION ESEGUITO IN PRECEDENZA GRAZIE ALL'UTILIZZO DEL COMANDO UNION NELLA STRINGA 1'UNION SELECT user,password FROM users#. RECUPERATI NOME UTENTE/PASSWORD DELLE UTENZE DI DVWA IN FORMATO HASH MD5, SALVO QUESTI DATI SUL FILE .TXT AFFIANCANDOLI NEL SEGUENTE MODO: UTENTE:PASSWORD. USERÒ IL TOOL JOHN THE RIPPER PER CRACKARE GLI HASH MD5 UTILIZZANDO LA WORDLIST ROCKYOU.





#JOHN THE RIPPER: