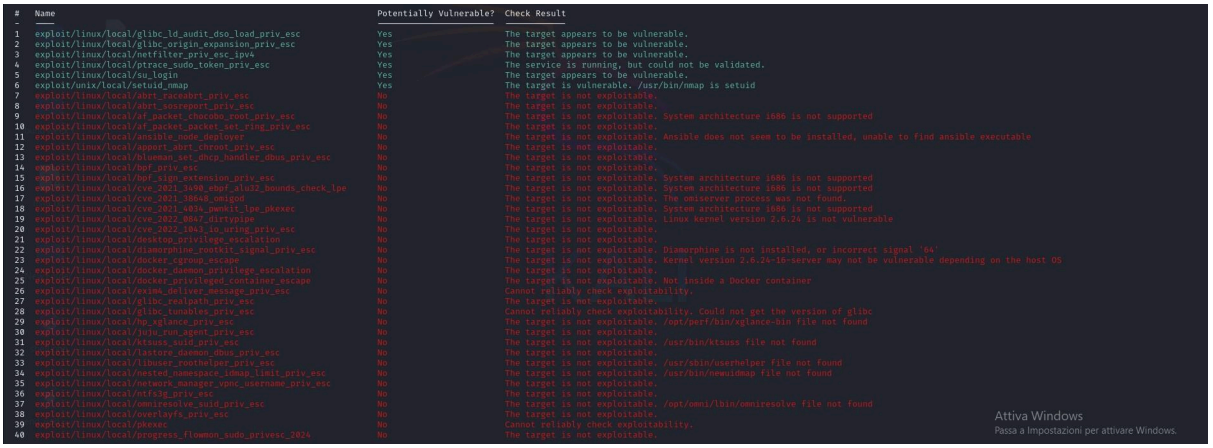
l’esercizio consisteva nell’eseguire tramite un exploit una escalation di privilegi e ottenere il root.
Ho usato il modulo exploit/linux/postgres/postgres_payload per sfruttare una vulnerabilità nel servizio PostgreSQL di Metasploitable 2.
successivamente ho eseguito l'exploit per ottenere una sessione Meterpreter sul sistema target, in questo caso metasploitable2.
Con il comando search suggester è apparso tutto un elenco di exploit per ottenere i privilegi root.
In questo caso dopo diverse prove quello funzionante era il primo.



Ho incontrato una piccola problematica con l’esecuzione dell’exploit perche in automatico il target era settato su linux x64 mentre quello che dovevamo utilizzare era x86 sul quale si basa metasploitable2.
Una volta cambiato il target l’unica cosa che mancava fare era lanciare l’exploit, aprire la sessione e ottenere i privilegi.

Con il comando getuid possiamo vedere che abbiamo ottenuto i privilegi root e di conseguenza l’attacco è stato eseguito con successo.