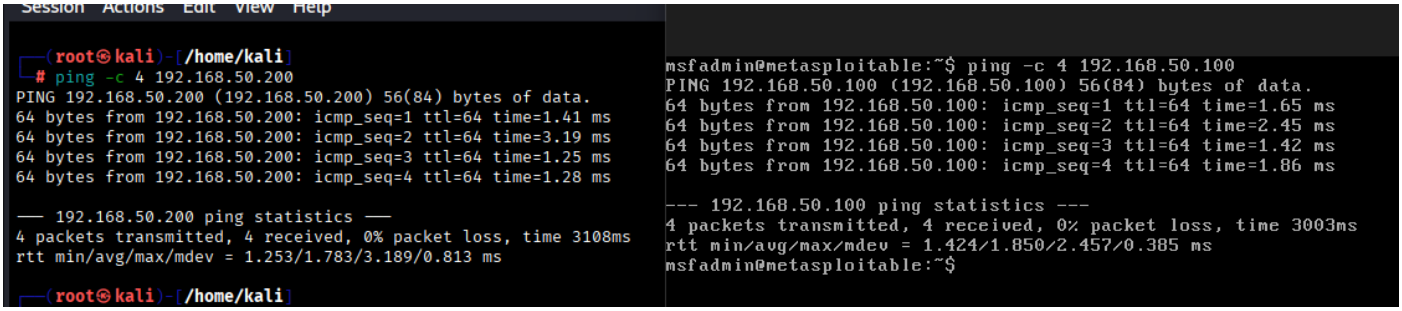
INDICE

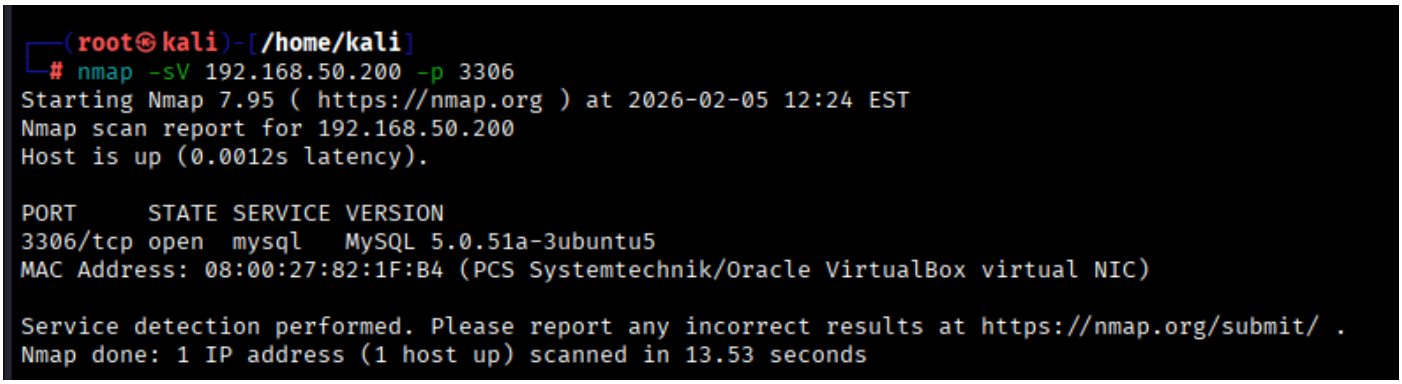
INTRODUZIONE ED OBIETTVO

INTRODUZIONE: il laboratorio consiste nell'analisi del servizio MySQL esposto su un sistema target Metasploitable, con l'obiettivo di verificare se una configurazione non sicura consenta l'accesso non autorizzato al database.
L'attività prevede una fase iniziale di individuazione del servizio in ascolto sulla porta 3306, seguita da un'attività di enumerazione delle credenziali e dall'accesso diretto al database tramite strumenti standard di analisi di sicurezza.
Attraverso questo esercizio viene simulato uno scenario realistico in cui un attaccante, partendo da un servizio di database esposto in rete, tenta di ottenere informazioni sugli account configurati, sfruttando credenziali deboli o assenti. L'analisi mette in evidenza come una configurazione MySQL non adeguatamente protetta possa consentire l'accesso agli account di sistema del database e rappresentare un punto di partenza per compromissioni più gravi.

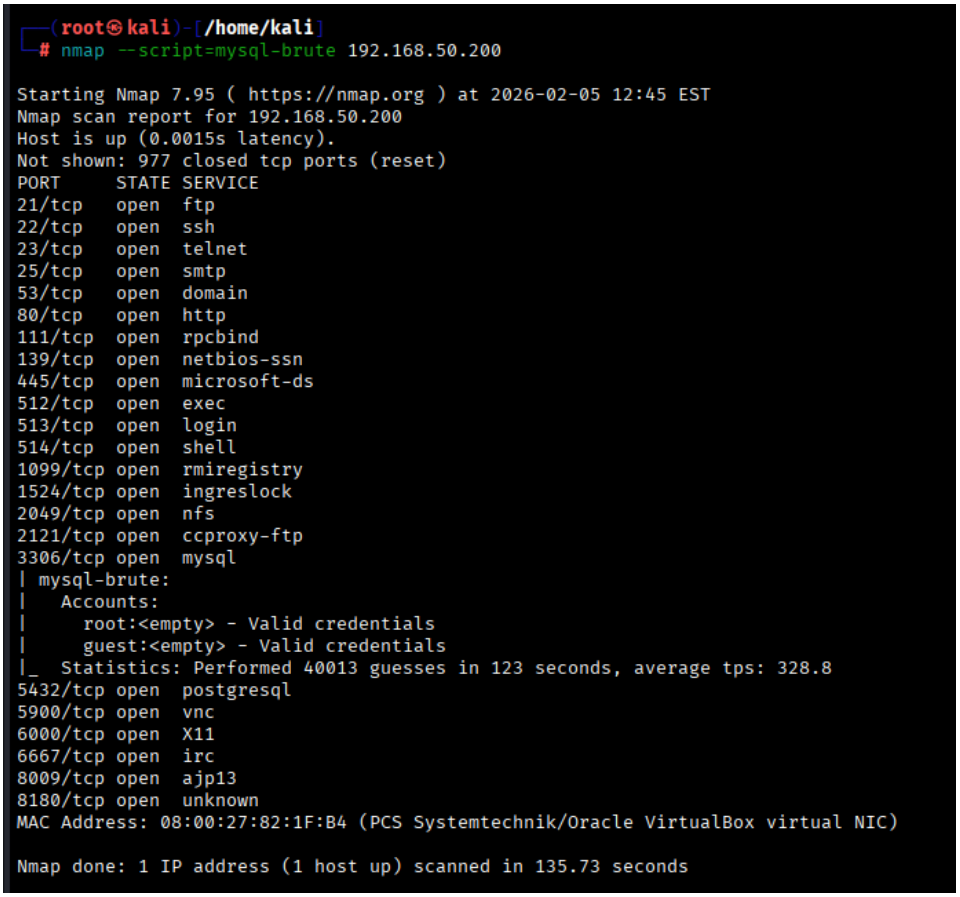
OBIETTIVO: ottenere la lista degli utenti MySQL presenti sul sistema Metasploitable, utilizzando tecniche di enumerazione basate su scansioni di rete e sull'accesso diretto al servizio di database.



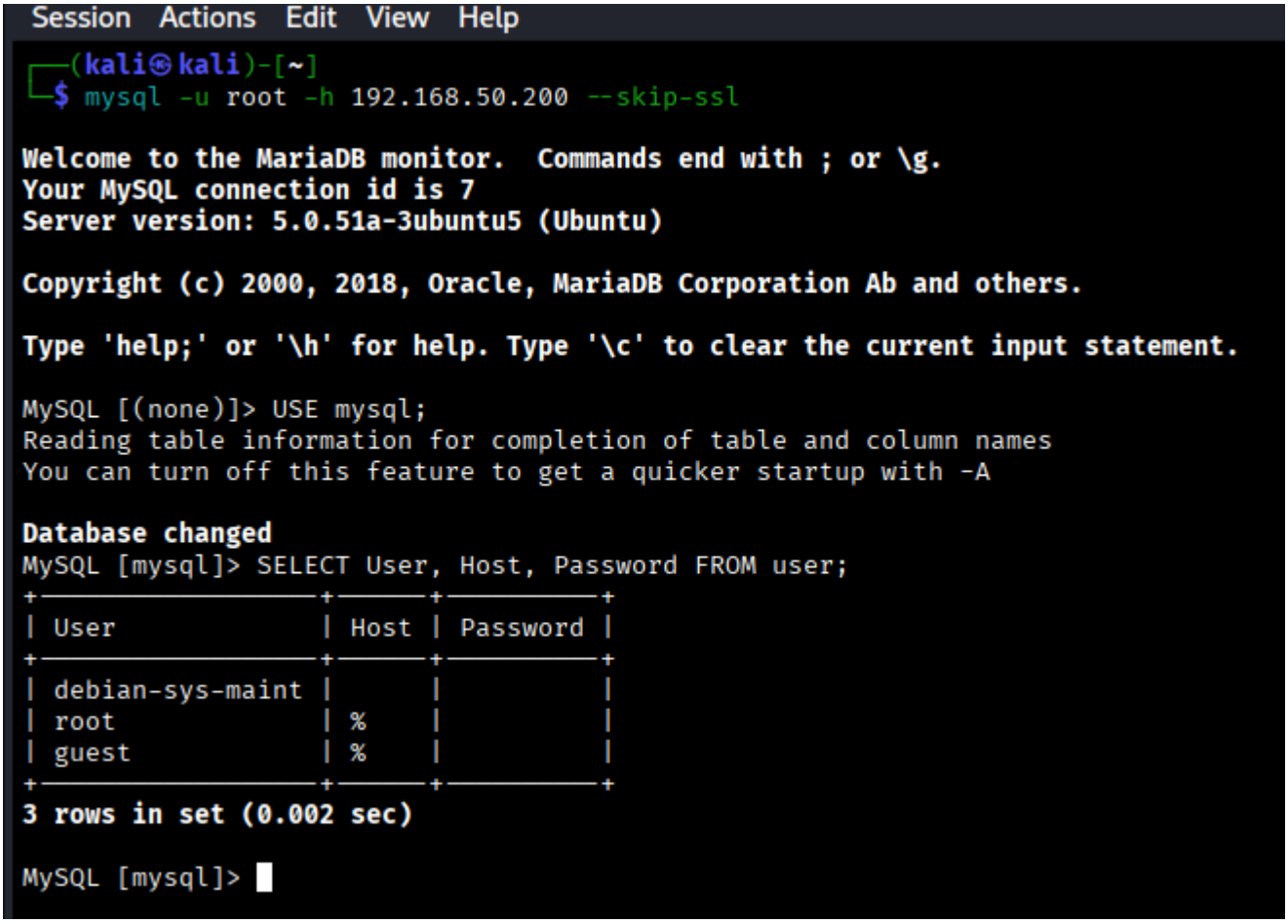
Prima di procedere con le attività di analisi del servizio MySQL, è stata verificata la connettività di rete tra la macchina di attacco Kali Linux e il sistema target Metasploitable. Mediante ping è stato confermato che le due macchine erano correttamente raggiungibili e in grado di comunicare tra loro senza perdite di pacchetti; questa verifica ha consentito di escludere problematiche di rete e di proseguire con le successive fasi dell'esercizio in un ambiente correttamente funzionante.



A seguire è stata effettuata un'analisi del servizio MySQL esposto sul sistema target Metasploitable, al fine di verificare la presenza di configurazioni non sicure.
L'attività ha consentito di individuare il servizio di database in esecuzione e di confermarne l'accessibilità; successivamente è stata svolta un'attività di enumerazione delle credenziali associate al servizio MySQL, che ha permesso di identificare account autenticabili senza password.
Sfruttando le credenziali individuate, è stato possibile accedere direttamente al database e procedere con l'analisi delle informazioni di sistema; in particolare, è stato interrogato il database di sistema per ottenere l'elenco degli utenti configurati sul server MySQL.
I risultati hanno evidenziato la presenza degli account debian-sys-maint, root e guest, confermando una configurazione del servizio non adeguatamente protetta e potenzialmente esposta ad accessi non autorizzati.



A seguire è stata effettuata un'attività di analisi del sistema target finalizzata alla verifica della configurazione del servizio MySQL esposto.
L'analisi ha permesso di individuare il servizio di database attivo e di procedere con un'attività di enumerazione delle credenziali associate; i risultati hanno evidenziato la presenza di account MySQL autenticabili senza password, in particolare gli utenti root e guest.
Sfruttando le credenziali individuate, è stato possibile accedere al database e interrogare il database di sistema, ottenendo l'elenco degli utenti configurati sul server, l'analisi ha confermato la presenza degli account debian-sys-maint, root e guest, evidenziando una configurazione del servizio MySQL non adeguatamente protetta e suscettibile ad accessi non autorizzati.



A seguito dell'individuazione di credenziali MySQL valide, è stato effettuato l'accesso diretto al servizio di database utilizzando l'account root.

Una volta stabilita la connessione, è stato selezionato il database di sistema ed è stata eseguita un'operazione di interrogazione finalizzata all'ottenimento dell'elenco degli utenti configurati sul server MySQL.

L'output ha restituito la presenza degli account debian-sys-maint, root e guest, confermando che il servizio di database era configurato in modo non sicuro e consentiva la visualizzazione di informazioni sensibili relative agli utenti senza l'applicazione di adeguati meccanismi di protezione.

CONCLUSIONE

L’esercizio ha dimostrato come l’esposizione di un servizio MySQL configurato in modo non sicuro possa consentire a un attaccante di ottenere accesso non autorizzato al database e di enumerare gli account di sistema.

La presenza di utenti autenticabili senza password e l’assenza di adeguate misure di hardening evidenziano un rischio significativo per la sicurezza del sistema, in quanto tali condizioni possono rappresentare un punto di ingresso per ulteriori compromissioni.

L’attività svolta ha quindi evidenziato l’importanza di una corretta configurazione dei servizi di database e dell’adozione di meccanismi di autenticazione e controllo degli accessi adeguati.