Authentication cracking con Hydra

Introduzione

L'esercizio di oggi ha l'obiettivo di approfondire le tecniche di attacco e configurazione dei servizi di rete, con un focus particolare sull'utilizzo dello strumento **Hydra** per il cracking delle credenziali di autenticazione. In un contesto di penetration testing, è fondamentale sia saper configurare correttamente i servizi di rete sia comprendere le potenzialità di strumenti come Hydra per individuare vulnerabilità legate all'autenticazione.

Il lavoro si sviluppa in due fasi principali. La prima fase prevede l'abilitazione di un servizio **SSH** (Secure Shell), seguito dalla dimostrazione pratica del cracking della sua autenticazione tramite Hydra. La seconda fase, invece, offre una maggiore libertà di scelta, permettendo di configurare e attaccare un servizio di rete a scelta tra quelli disponibili, come **FTP**, **RDP**, **Telnet** o l'autenticazione **HTTP**.

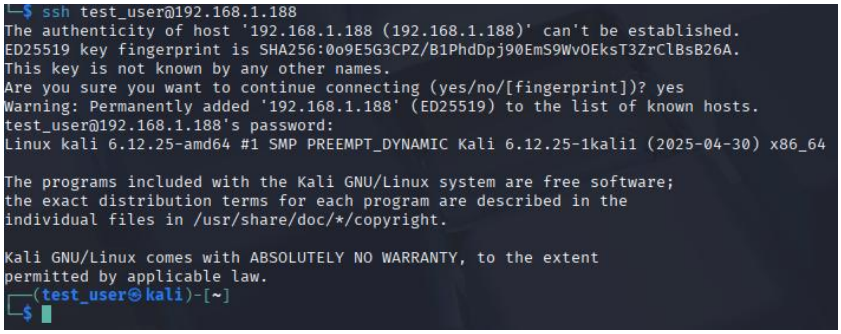
L'esercizio si propone di migliorare le competenze pratiche relative alla configurazione dei servizi di rete e al testing delle loro vulnerabilità, consolidando al contempo la conoscenza delle modalità di autenticazione e delle tecniche di cracking per garantire una comprensione completa della sicurezza dei sistemi.

1. Creazione dell'utente di test

Per avviare l'attacco di cracking dell'autenticazione SSH, il primo passo consiste nella creazione di un utente di test con credenziali conosciute, che saranno poi utilizzate durante l'esercizio. In questa fase, è stato creato un utente denominato **test_user**, con una password di facile individuazione, che fungerà da target per l'attacco di cracking.

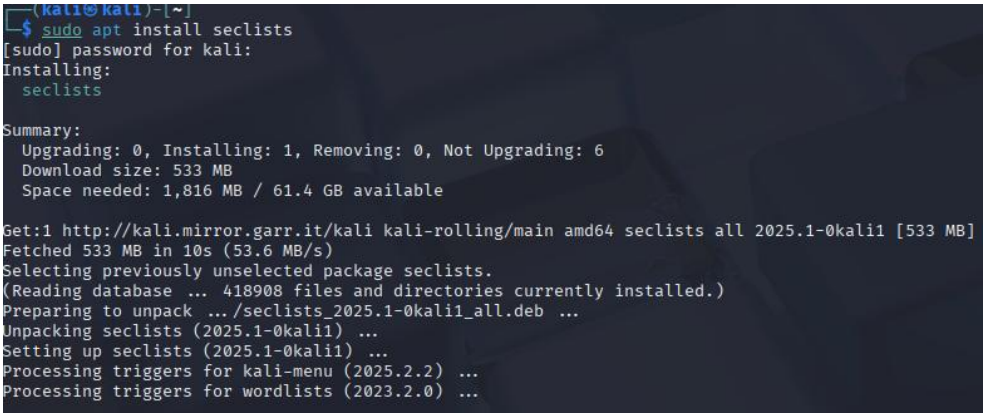
2. Verifica dell'accesso SSH per l'utente di test

Una volta creato l'utente test_user e assegnata la relativa password, è stata effettuata una verifica preliminare per accertarsi che il servizio SSH fosse attivo e correttamente configurato, e che l'utente creato potesse accedervi.



Comando utilizzato: ssh test_user@192.168.1.188
Lo scopo di è quello di avviare una connessione SSH. L'accesso è avvenuto con successo, confermando che: il servizio SSH era correttamente attivo e in ascolto sulla porta 22, l'utente test_user è abilitato all'accesso remoto e credenziali inserite erano valide. Questa verifica è fondamentale per garantire la riuscita dell'esercizio successivo, in quanto consente di procedere con l'attacco di forza bruta tramite Hydra in un ambiente controllato e funzionante.

3. Installazione del pacchetto SecLists:



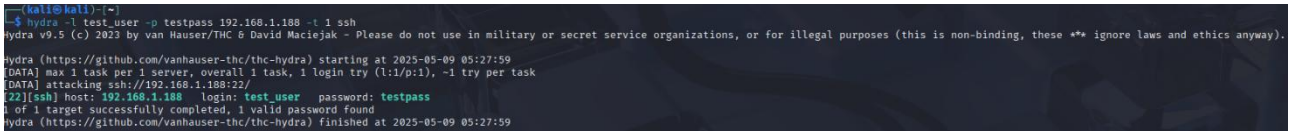
Per eseguire un attacco di forza bruta efficace con Hydra, è necessario disporre di una wordlist contenente una serie di nomi utente e password comunemente utilizzati o potenzialmente deboli.

A tal fine, abbiamo installato il pacchetto **SecLists,** al suo interno si trovano diverse directory tematiche, tra cui:

- Passwords/
- Usernames/
- Fuzzing/
- Discovery/

Per questo esercizio, verranno utilizzate in particolare le wordlist contenute nella cartella Passwords per effettuare il cracking delle credenziali SSH con Hydra.

4. Comando Hydra per il Brute Force su SSH



Il comando Hydra viene utilizzato per eseguire un attacco di forza bruta contro un servizio SSH al fine di testare la sicurezza delle credenziali di accesso, utilizzando un nome utente e una password specifici.

Esecuzione del Comando:
L'attacco di forza bruta cercherà di autenticarsi sulla macchina target (192.168.1.188) utilizzando il nome utente test_user e la password testpass. Ogni tentativo di accesso verrà effettuato uno alla volta, utilizzando un singolo thread per minimizzare il rischio di errori o di blocchi da parte del sistema di protezione dell'host.

Considerazioni sulla Sicurezza:
Gli attacchi di forza bruta sono metodi potenzialmente dannosi e devono essere condotti solo con il consenso del proprietario del sistema target. Gli amministratori di sistema dovrebbero implementare politiche di sicurezza come il blocco degli account dopo un numero definito di tentativi di accesso falliti, l'uso di chiavi SSH anziché password e la protezione con firewall per prevenire attacchi simili.

---

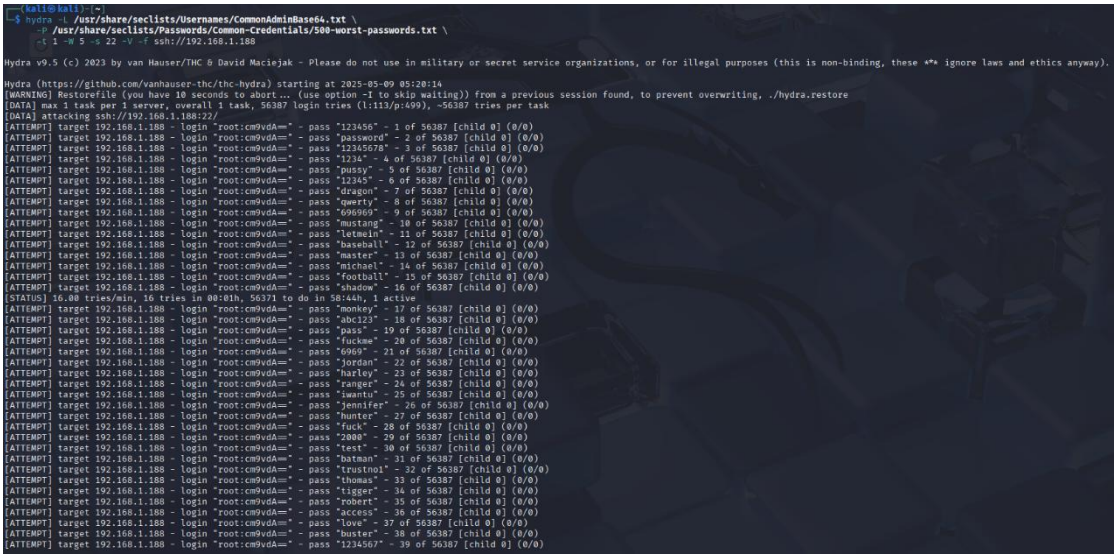
5. Cracking SSH

Spieghiamo la funzione di ciascun parametro:

**hydra -L /usr/share/seclists/Usernames/CommonAdminBase64.txt **

**-P /usr/share/seclists/Passwords/Common-Credentials/500-worst-passwords.txt **

-t 1 -w 5 -s 22 -V -f ssh://192.168.1.188



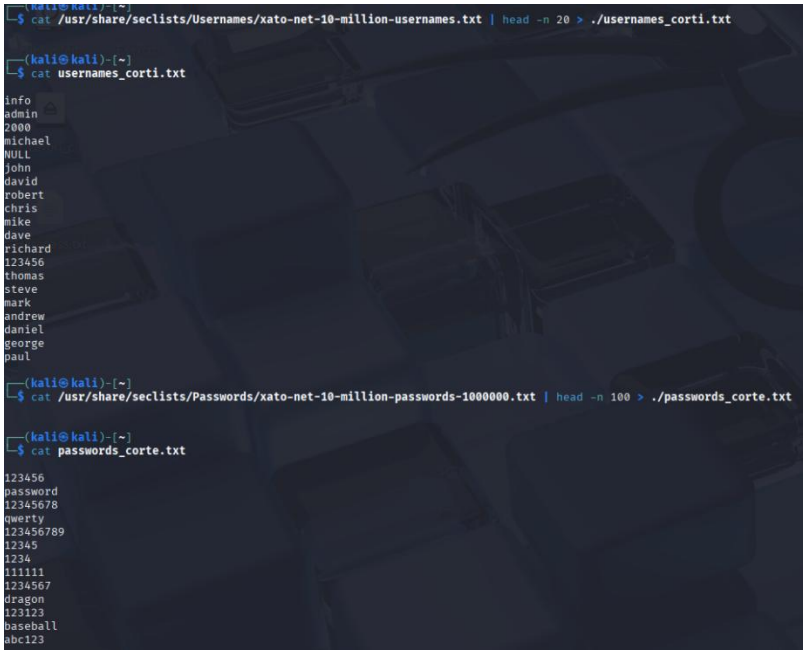
Spiegazione di ciascun parametro:

- -L /usr/share/seclists/Usernames/CommonAdminBase64.txt: specifica il file contenente la lista di nomi utente da testare. In questo caso, si utilizza un file chiamato CommonAdminBase64.txt, che potrebbe contenere username comuni o codificati in Base64.
- -P /usr/share/seclists/Passwords/Common-Credentials/500-worst-passwords.txt: specifica il file contenente la lista di password da provare per ogni nome utente. In questo caso, viene utilizzato un file che contiene una lista di 500 password più comuni.
- -t 1: imposta il numero di thread simultanei per i tentativi di login. In questo caso, è impostato su 1, quindi i tentativi verranno fatti uno alla volta.
- -w 5: imposta un timeout di attesa di 5 secondi per ciascun tentativo di login. Se non arriva una risposta dal server entro 5 secondi, Hydra passa al tentativo successivo.
- -s 22: indica la porta a cui Hydra deve connettersi. La porta 22 è quella standard per SSH.
- -V: abilita la modalità verbosa (verbose), che fornisce una panoramica dettagliata dei tentativi effettuati, mostrando ogni combinazione di username e password che Hydra sta testando.
- -f: interrompe l'attacco non appena viene trovata una combinazione valida di username e password.
- ssh://192.168.1.188: è l'indirizzo IP e il protocollo del servizio a cui Hydra sta cercando di connettersi. In questo caso, si tratta di un servizio SSH in esecuzione su 192.168.1.188.

Sommario del comando:

Il comando esegue un attacco di brute force su un server SSH all'indirizzo IP 192.168.1.188.
Hydra tenterà tutte le combinazioni di username (dal file CommonAdminBase64.txt) e password (dal file 500-worst-passwords.txt). Il test avviene uno alla volta (-t 1), con una pausa di 5 secondi tra un tentativo e l'altro (-w 5). Se viene trovata una combinazione valida di username e password, l'attacco si interrompe (-f). La modalità verbosa (-V) mostrerà i dettagli di ogni tentativo effettuato.

Possiamo anche creare noi delle liste, per velocizzare tutti i processi in modo da non sprecare tempo:

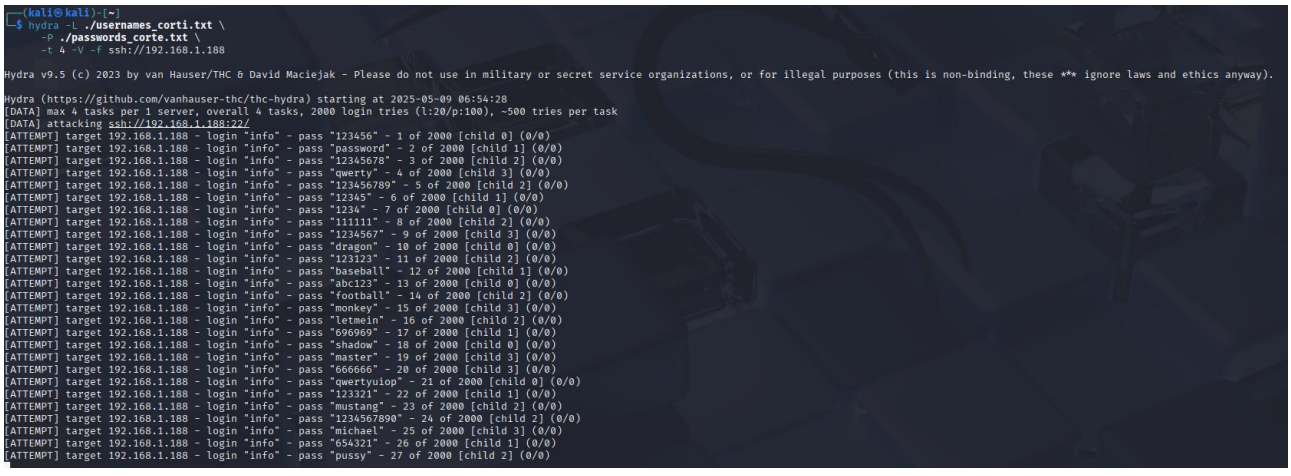


con il comando cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt | head -n 20 > ./usernames_corti.txt – estraiamo le prime 20 righe degli users, avviandolo vediamo il suo funzionamento con cat usernames_corti.txt.
Facciamo lo stesso per le password: cat /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt | head -n 100 > ./passwords_corte.txt - Avviamo anche questo e osserviamo il risultato elencato correttamente (cat passwords_corte.txt)

A questo punto avviamo Hydra con :
hydra -L ./usernames_corti.txt -P ./passwords_corte.txt -t 4 -V -f ssh://192.168.1.188
Spiegazione del comando:

- **-L ./usernames_corti.txt**: indica il percorso del file con gli username (in questo caso, usernames_corti.txt).
- **-P ./passwords_corte.txt**: indica il percorso del file con le password (in questo caso, passwords_corte.txt).
- **-t 4**: definisce il numero di **thread** (processi simultanei) che Hydra userà per i tentativi. Puoi aumentarlo per velocizzare il processo (ad esempio -t 4 è buono per non sovraccaricare il sistema).
- **-V**: fa sì che Hydra mostri ogni tentativo che fa (utile per vedere i tentativi e per il debug).
- **-f**: indica che Hydra si fermerà **non appena trova una combinazione valida**.
- **ssh://192.168.1.188**: è il protocollo e l'indirizzo del target (in questo caso un server SSH locale).

Ed ecco il risultato finale



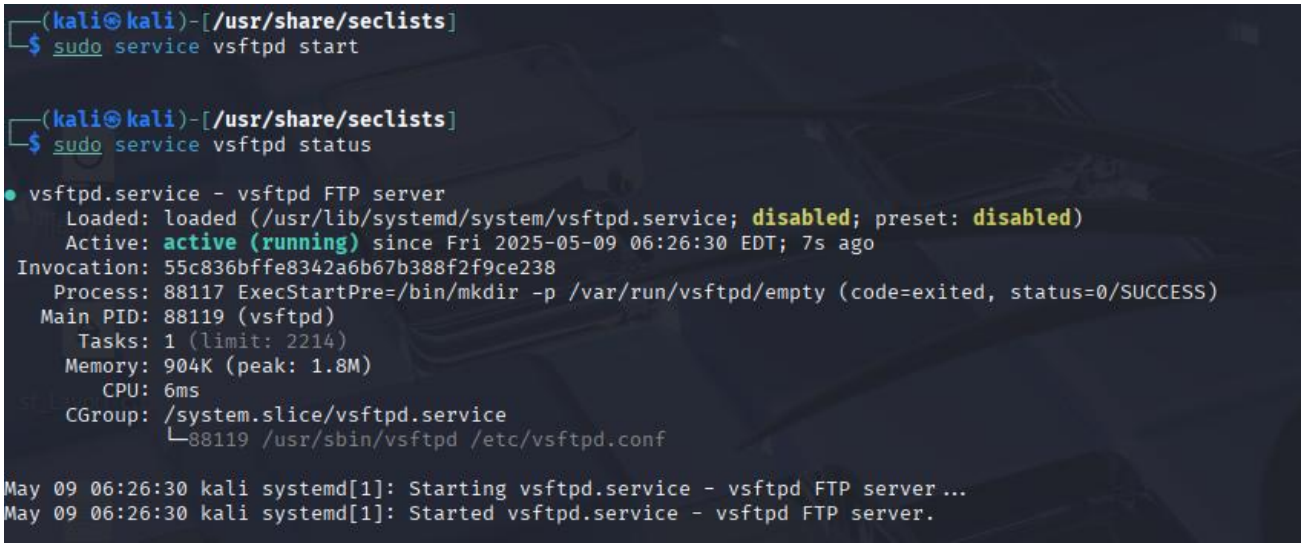
Esercizio Fase 2

Configurazione e Cracking del Servizio FTP
Obiettivo

L'obiettivo della seconda fase è configurare un servizio di rete, nello specifico un server FTP, e successivamente tentare di craccare l'autenticazione utilizzando Hydra. Questo esercizio aiuterà a comprendere la configurazione di un servizio di rete comune e le vulnerabilità legate all'autenticazione tramite attacchi di forza bruta.

Procedura

Una volta seguita l'operazione suggerita nelle slide, dopo l'istallazione procediamo all'avvio del processo e alla verifica del suo status.

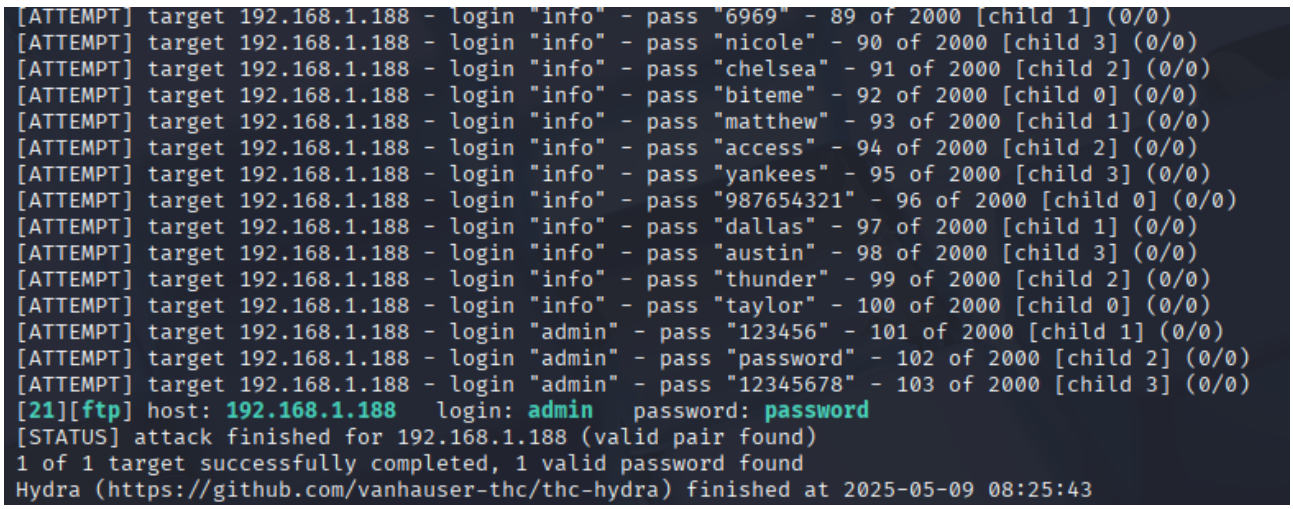


ATTACCO FTP

Passiamo ora all'attacco del server FTP tramite il comando:
hydra -L ./usernames_corti.txt -P ./passwords_corte.txt -t 4 -V -f ftp://192.168.1.188.

Risultato dell'attacco:

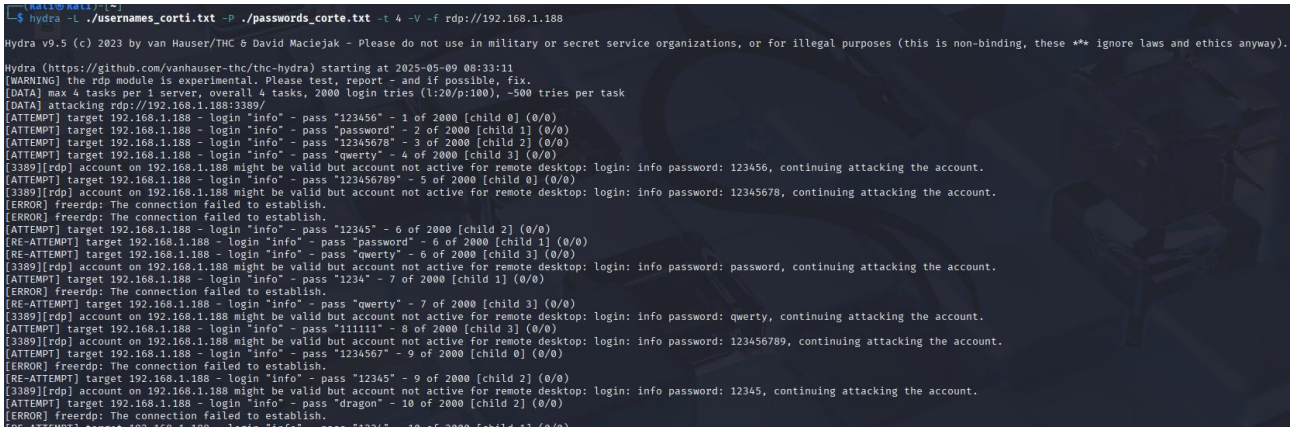
Una volta completato l'attacco, Hydra ha trovato la combinazione corretta di credenziali per il login al server FTP. Il risultato è stato il seguente:



Questo indica che l'account **admin** con la password **password** è stato identificato come valido per l'accesso al server FTP all'indirizzo IP **192.168.1.188**.

RDP (Remote Desktop Protocol)

Abbiamo anche provato a farlo per RDP.
Il comando è simile a quello per FTP, ma il protocollo cambia in rdp://.
Comando usato: hydra -L ./usernames_corti.txt -P ./passwords_corte.txt -t 4 -V -f rdp://192.168.1.188



Conclusione

L'esercitazione svolto ha permesso di acquisire una solida comprensione pratica delle tecniche di attacco brute force contro diversi servizi di rete, attraverso l'utilizzo dello strumento Hydra.
Dopo aver configurato correttamente un ambiente controllato, sono stati simulati attacchi verso servizi SSH, FTP, RDP dimostrando l'efficacia di semplici combinazioni username/password deboli nel compromettere l'accesso ai sistemi.

Questo tipo di simulazioni evidenzia quanto sia fondamentale, in un'ottica difensiva, adottare contromisure appropriate: implementare policy di password robuste, abilitare sistemi di blocco automatico dopo ripetuti tentativi falliti, utilizzare meccanismi di autenticazione più sicuri (come le chiavi SSH), e mantenere monitorati costantemente i servizi esposti in rete.

In definitiva, l'attività ha rafforzato le competenze relative sia alla configurazione dei servizi di rete che alla loro valutazione dal punto di vista della sicurezza, fornendo uno scenario realistico per applicare i concetti teorici del penetration testing.

Anais Fabriani
09/05/2025