EPICODE

Esercizio S6 – L3

TRACCIA

Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio. L’esercizio di oggi ha un duplice scopo:  
● Fare pratica con Hydra per craccare l’autenticazione dei servizi di rete.  
● Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

L’esercizio si svilupperà in due fasi:  
● Una prima fase dove insieme vedremo l’abilitazione di un servizio SSH e la relativa sessione di cracking dell’autenticazione con Hydra.  
● Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

SOLUZIONE

Per iniziare si è creato un nuovo utente chiamato “test\_user” con password “testpass”.  
Si è poi attivato il servizio ssh.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

segue

Si è poi testata con successo la connessione ssh dell’utente.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Successivamente si sono installate le liste “seclists”.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

segue

Utilizzando i comandi si è arrivati a poter vedere il contenuto di “seclists”.

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamente

Si è aperta la cartella delle liste “Usernames” per scegliere la lista da utilizzare.

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamente

Segue

Ci si è poi spostati nella cartella contenente le liste di passwords per scegliere una lista da utilizzare.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Giunti a questo punto si è fatto partire l’attacco a dizionario al servizio ssh utilizzando Hydra e due liste scelte (una per trovare l’username, una per la password).

Immagine che contiene testo, schermata, Carattere, informazione

Descrizione generata automaticamente

Si è in attesa di un riscontro. L’attacco è ancora in corso, ma le liste utilizzate contengono un gran numero di user e pass e sono quindi in grado di trovare combinazioni anche non particolarmente comuni.

