Cracking SSH

Il primo passaggio da fare è creare un utente da attaccare con il comando "adduser" e il nome da dare al nuovo utente insieme alla password.Una volta creato l'utente dobbiamo verificare la connessione dall'utente appena creato sul sistema e quindi utilizziamo il comando " ssh test_user@indirizzo IP della macchina". Nel caso in cui tutto è andato bene dovremmo adesso ricevere la prompt di comandi dell'utente appena creato. Dopo aver verificato la connessione bisogna configurare hydra, quindi dopo aver scaricato una lista di nome utente e password, avvio hydra alla ricerca del nome utente e password dell'account appena creato utilizzando questo comando: "Hydra -L home/kali/Documents/SecLists/Usernames/xato-net-10-million-usernames.txt -P /home/kali/Documents/SecLists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.10 -t4 ssh". Il comando è diverso in base a come avete installato la lista, io ho utilizzato questo comando avendola scaricata direttamente dal link di GitHub. Quindi ho ricreato il percorso per raggiungere il file sia per i nomi utenti che per le password. cambiamo l'indirizzo IP mettendo quello della nostra macchina e avviamo. Come possiamo notare ha avviato un attacco con metodo BruteForce contro l'utente per trovare i suoi dati, il problema è che così ci metterebbe troppo, quindi ho modificato li comando in modo tale da essere più veloce utilizzando "-t16" al posto di "-t4". Così facendo velocizzi la ricerca. Per ultimo ho scelto un servizio da configurare, in questo caso ftp e ne ho craccato l'autenticazione con hydra. Ho installato il servizio con il comando "sudo apt-get install vsftpd" e poi l'ho configurato utilizzando il comando "ftp localhost". Dopodichè ho avviato hydra modificando il comando e aggiungendo prima dell'indirizzo IP "ftp://".