Il CISO ha esplicitamente richiesto di non effettuare nessun test invasivo in ambiente di produzione, e quindi abbiamo riprodotto le componenti nei nostri laboratori di test, così da poter effettuare i test in sicurezza, separati dagli ambienti di lavoro. In particolare il web server verrà simulato dalla macchina **Metasploitable** che espone di default un servizio web sulla porta **80**, come si può verificare digitando l'indirizzo IP di Metasploitable nella barra del browser da Kali Linux.

Il codice python per il **port scanner** richiede in input un IP ed un range di porte da scansionare (in formato standard, esempio 1-1024). Ricaviamo il range dalla stringa inserita, e inseriamo gli estremi nelle variabili lowport e highport; viene utilizzato il metodo **split** e utilizzato il simbolo - come separatore.

Il ciclo **for** successivo ci serve per tentare la connessione TCP ad ogni porta nell'intervallo specificato; utilizziamo il metodo **socket.socket** che restituisce un socket che chiamiamo s, specificando i parametri del socket per IPv4 e TCP.

La funzione **s.connect_ex** tenta la connessione alla coppia IP:PORTA specificata, e ci restituisce uno stato che può essere 0 o diverso da 0; nel primo caso la connessione è andata a buon fine, dunque possiamo dedurre che la porta sia aperta. Nel caso il valore sia 113 vuol dire che la rete non è raggiungibile e terminiamo pertanto l'esecuzione del codice, altrimenti possiamo dedurre che la porta è chiusa (valore 111).

In output viene restituito un dizionario con le coppie porta (**chiave**) e relativo stato (aperta o chiusa, **valore**), che può essere utilizzato per eventuali successive elaborazioni; vengono infine stampate tali coppie con una formattazione colorata per una maggiore visibilità.