Attacco dos

Un **attacco DoS** (Denial of Service) è un tipo di attacco informatico volto a rendere un sistema, un servizio o una rete indisponibile per gli utenti legittimi. In pratica, l'obiettivo di un attacco DoS è sovraccaricare un server, una rete o una risorsa di sistema con una quantità eccessiva di richieste, in modo che il sistema non riesca più a gestire correttamente il traffico e quindi non sia più in grado di rispondere agli utenti legittimi.

Esistono diverse varianti di attacchi DoS:

- **Attacco DoS tradizionale**: L'attaccante invia un numero estremamente elevato di richieste al sistema, causando un sovraccarico e un'interruzione del servizio.

- **Attacco DDoS (Distributed Denial of Service)**: In questo caso, l'attacco è effettuato da una rete di dispositivi compromessi, chiamata botnet, che invia richieste simultanee al sistema bersaglio. Poiché provengono da molte fonti diverse, gli attacchi DDoS sono più difficili da difendere rispetto a un attacco DoS tradizionale.

Le tecniche comuni per realizzare un attacco DoS includono:

- **Flooding**: invio massivo di traffico di rete (ad esempio, pacchetti ICMP o HTTP) per esaurire le risorse del sistema.

- **Exploitation of vulnerabilities**: sfruttamento di vulnerabilità nel software o nel protocollo per bloccare o rallentare il sistema.

L'obiettivo di un attacco DoS è generalmente quello di causare un'interruzione temporanea del servizio, ma in alcuni casi, può anche essere utilizzato come distrazione per altri tipi di attacchi più mirati.

Esercizio del Giorno

Input dell'IP Target:

- Il programma deve richiedere all'utente di inserire l'IP della macchina target.

Input della Porta Target:

- Il programma deve richiedere all'utente di inserire la porta UDP della macchina target.

Costruzione del Pacchetto:

- La grandezza dei pacchetti da inviare deve essere di 1 KB per pacchetto.

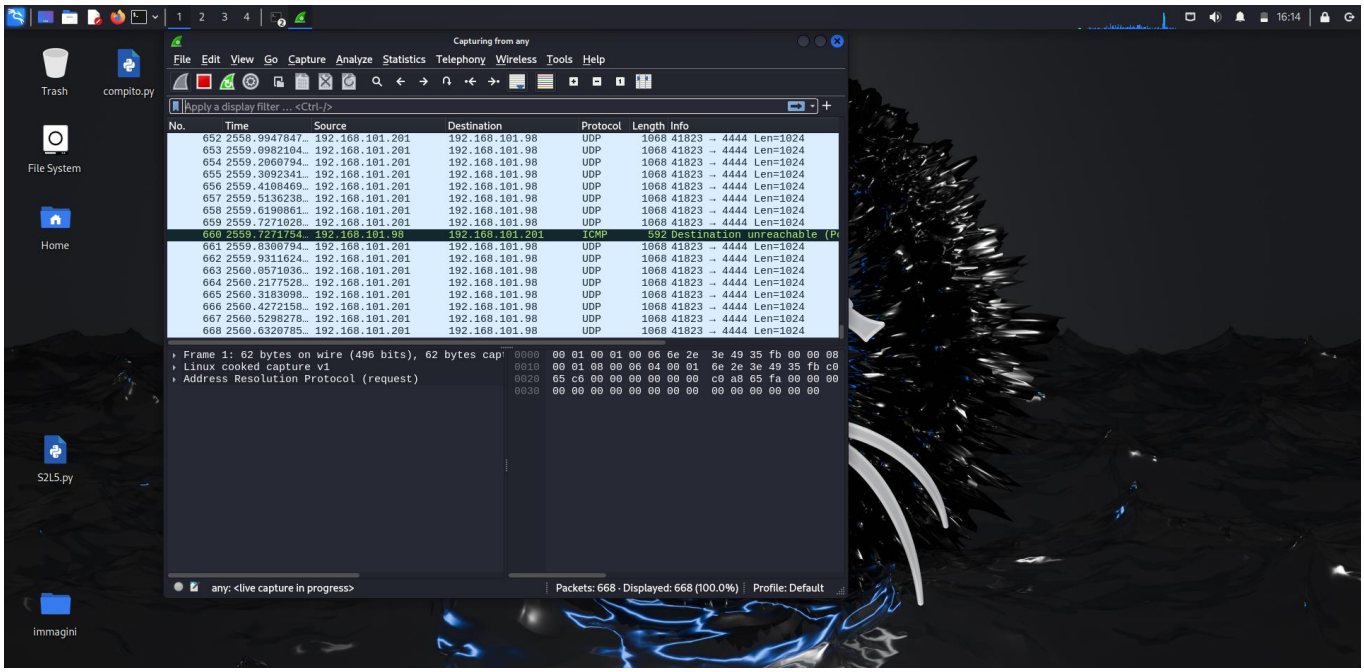
Numero di Pacchetti da Inviare:

- Il programma deve chiedere all'utente quanti pacchetti da 1 KB inviare.

Immagine 1:

Nella prima immagine vediamo lo script che abbiamo usato per inviare i pacchetti. Lo script ci permette di inserire l'IP della macchina interessata, la porta e la quantità di pacchetti da inviare.

Immagine 2:



Nella seconda immagine vediamo la macchina attaccata e tramite Wireshark vediamo i 1000 pacchetti che ho scelto di inviare.

Wireshark

Wireshark è uno degli strumenti più potenti e versatili per l'analisi di rete. La sua capacità di catturare e analizzare il traffico di rete in dettaglio lo rende uno strumento indispensabile per amministratori di rete, esperti di sicurezza informatica, e per chiunque abbia bisogno di risolvere problemi di rete o studiare il comportamento delle comunicazioni di rete. Nonostante la sua complessità iniziale, la potenza e la flessibilità di Wireshark sono difficili da eguagliare, e le sue applicazioni sono molteplici, dall'analisi della sicurezza alla diagnosi di problemi di rete fino alla formazione tecnica. Lo abbiamo usato nell'esercizio per vedere i pacchetti in arrivo sulla macchina dossata.