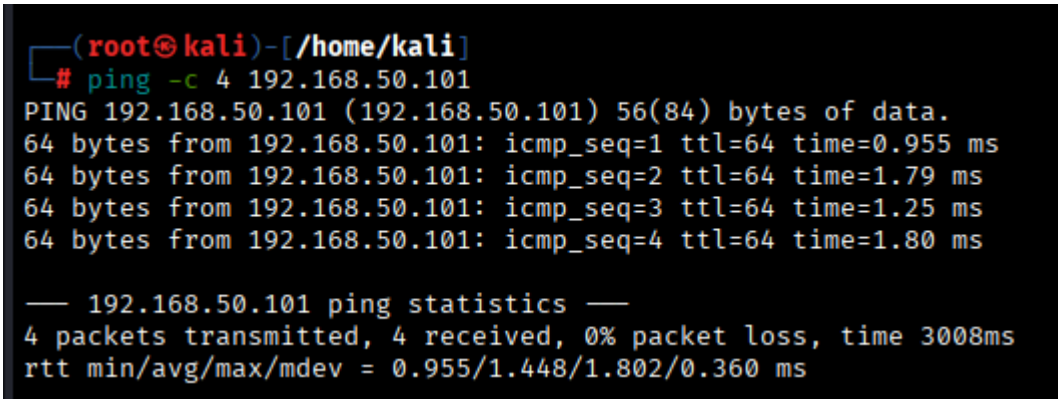
INDICE

INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: l'esercizio si concentra sull'analisi pratica di un attacco DoS a livello applicativo, simulato all'interno di un ambiente di laboratorio controllato.
L'attacco viene condotto dalla macchina Kali Linux verso un target Metasploitable utilizzando lo strumento *Slowloris*, noto per la sua capacità di rendere un servizio web non disponibile senza saturare la banda di rete.
A differenza degli attacchi DoS tradizionali basati sull'invio massivo di traffico, Slowloris opera mantenendo numerose connessioni HTTP incomplete, occupando progressivamente le risorse del web server e impedendo la gestione delle richieste legittime.
Questo tipo di attacco è particolarmente interessante dal punto di vista didattico perché evidenzia la differenza tra disponibilità del servizio applicativo e raggiungibilità del servizio a livello di rete.

OBIETTIVO è simulare un attacco DoS di tipo applicativo tramite Slowloris e osservare il suo impatto sulla disponibilità del servizio HTTP del target. In particolare, si intende dimostrare la differenza tra indisponibilità del servizio applicativo e persistenza della connettività TCP.

METODOLOGIA OPERATIVA

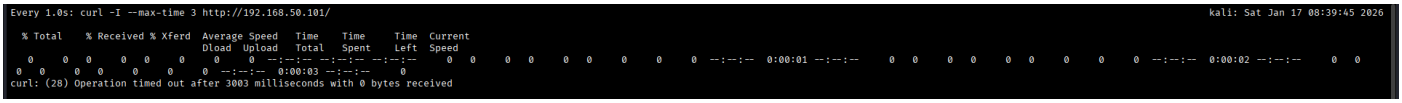


Prima di avviare l'esercizio è stata verificata la connettività tra la macchina attaccante e la macchina target, per assicurarsi che le due istanze fossero correttamente in comunicazione tra loro.
La risposta positiva del target, con tempi di risposta stabili e senza perdita di pacchetti, conferma che il collegamento di rete funziona correttamente e che entrambe le macchine sono raggiungibili.
Questa verifica iniziale permette di stabilire una condizione di partenza normale, escludendo problemi di rete che potrebbero influenzare l'interpretazione dei risultati dell'attacco.

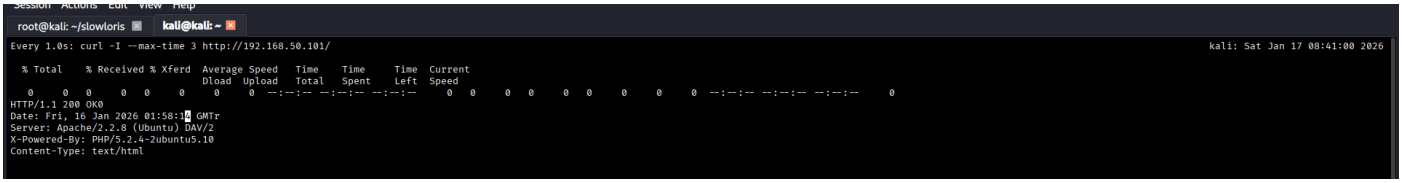
```
┌──(root㉿kali)-[/home/kali]
└─# cd ~/slowloris

┌──(root㉿kali)-[~/slowloris]
└─# ls
LICENSE  MANIFEST.in  README.md  setup.py  slowloris.py
```

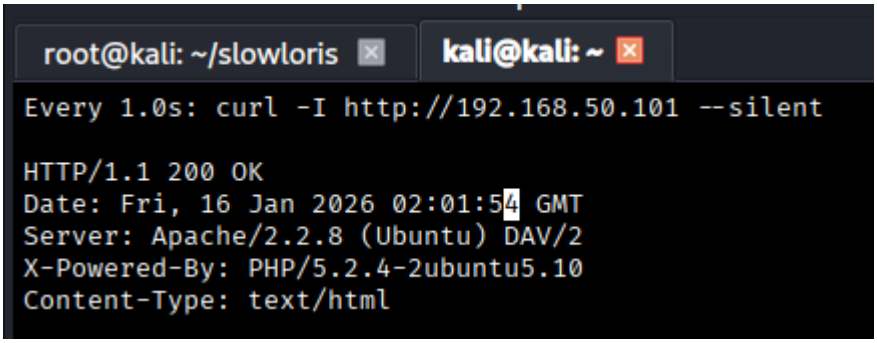
```
┌──(root㉿kali)-[~/slowloris]
└─# python3 slowloris.py 192.168.50.101
[17-01-2026 08:58:18] Attacking 192.168.50.101 with 150 sockets.
[17-01-2026 08:58:18] Creating sockets ...
[17-01-2026 08:58:22] Sending keep-alive headers ...
[17-01-2026 08:58:22] Socket count: 150
[17-01-2026 08:58:38] Sending keep-alive headers ...
[17-01-2026 08:58:38] Socket count: 150
[17-01-2026 08:58:53] Sending keep-alive headers ...
[17-01-2026 08:58:53] Socket count: 150
[17-01-2026 08:59:08] Sending keep-alive headers ...
[17-01-2026 08:59:08] Socket count: 150
[17-01-2026 08:59:23] Sending keep-alive headers ...
[17-01-2026 08:59:23] Socket count: 150
```

Dopo essersi spostati nella directory contenente lo strumento necessario al laboratorio, Slowloris viene avviato contro la macchina target.
Al momento dell'esecuzione lo script inizia a creare un numero controllato di connessioni verso il server web, mantenendole aperte tramite l'invio periodico di header incompleti. L'output mostra chiaramente l'utilizzo di **150 socket**, valore iniziale impiegato per la simulazione dell'attacco, confermando che le connessioni vengono create e mantenute attive nel tempo. Questa fase rappresenta l'inizio effettivo dell'attacco DoS a livello applicativo.

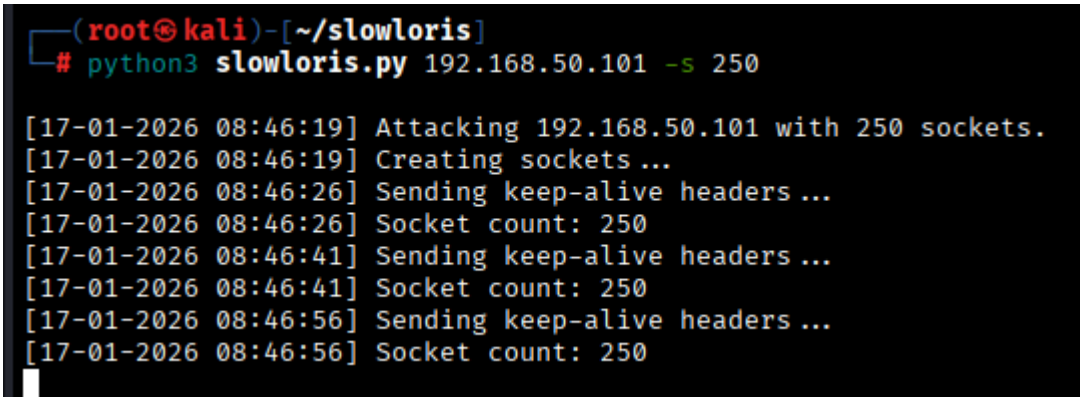


Contestualmente all'avvio di Slowloris, viene avviato un monitor per verificare lo stato del servizio HTTP del target.
Il controllo viene effettuato tramite richieste periodiche che interrogano esclusivamente gli header della risposta, consentendo di osservare in tempo reale il comportamento del web server; con l'attacco attivo, il servizio smette progressivamente di rispondere: le richieste non ricevono più alcun header e il comando va in timeout, indicando che il server non è più in grado di gestire nuove connessioni HTTP.
Questo comportamento evidenzia come le risorse applicative risultino saturate dalle connessioni mantenute aperte da Slowloris, rendendo il servizio web non disponibile pur senza interrompere la connettività di rete tra le due macchine.

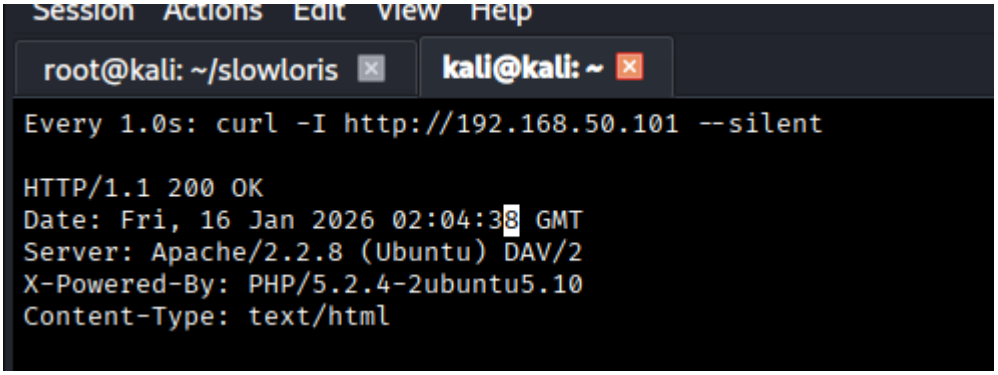




Subito dopo l'interruzione di Slowloris, il comportamento del servizio HTTP cambia immediatamente.
Il monitor mostra nuovamente una risposta valida da parte del server, con il ritorno dello stato e l'aggiornamento regolare dell'intestazione temporale.
Questo passaggio conferma che l'indisponibilità osservata in precedenza non era dovuta a problemi di rete o a un malfunzionamento permanente del servizio, ma era direttamente causata dall'attacco in corso.
La ripresa immediata delle risposte HTTP dimostra quindi il rapporto di causa/effetto tra l'esecuzione di Slowloris e il blocco del servizio web, evidenziando come la saturazione delle risorse applicative venga meno non appena le connessioni mantenute aperte dallo strumento vengono rilasciate.



Successivamente, l'attacco viene ripetuto aumentando il numero di socket utilizzati da Slowloris.
Lo strumento viene quindi riavviato specificando un valore più elevato rispetto alla configurazione iniziale, portando il numero di connessioni mantenute aperte a **250 socket**.
L'output conferma la creazione e il mantenimento continuo di queste connessioni, indicando che il web server viene sottoposto a una pressione maggiore a livello applicativo.
Questa fase consente di osservare come l'incremento del numero di socket renda il blocco del servizio HTTP più rapido o più stabile nel tempo, rafforzando l'effetto già evidenziato nella fase precedente e mostrando come la disponibilità del servizio sia direttamente influenzata dalla quantità di connessioni incomplete mantenute attive dall'attacco.



Durante la fase di attacco con un numero maggiore di socket, il monitor del servizio HTTP viene mantenuto attivo per osservare il comportamento del server. In questa configurazione, il servizio continua inizialmente a rispondere con stato 200 OK, mostrando che l'aumento del numero di connessioni non produce necessariamente un blocco immediato.
Questo comportamento evidenzia come l'impatto di Slowloris non sia istantaneo ma dipenda dalla progressiva saturazione delle risorse applicative del web server.
L'osservazione conferma quindi che l'incremento dei socket aumenta la pressione sul servizio, rendendo il blocco potenzialmente più rapido o più stabile, ma senza modificare il funzionamento di base del meccanismo di attacco, che rimane legato al mantenimento di connessioni HTTP incomplete nel tempo.

CONCLUSIONE

L’esercizio ha permesso di osservare in modo pratico il funzionamento di un attacco DoS a livello applicativo tramite Slowloris, evidenziando come la disponibilità del servizio HTTP possa essere compromessa anche in assenza di problemi di connettività tra le macchine coinvolte.
Durante l’attacco, il servizio web del target è risultato non responsivo a causa della saturazione delle risorse applicative, mentre la comunicazione di rete rimaneva invariata.
L’interruzione di Slowloris ha portato al ripristino immediato delle risposte HTTP, dimostrando chiaramente il rapporto di causa/effetto tra l’attacco e l’indisponibilità del servizio.
La ripetizione dell’attacco con un numero maggiore di socket ha inoltre mostrato come l’intensità dell’attacco influisca sulla stabilità e sulla rapidità del blocco del servizio, confermando l’efficacia di Slowloris come tecnica di DoS applicativo e l’importanza di adeguate misure di mitigazione a livello di web server.

Dos: un attacco Denial of Service (DoS) ha come obiettivo rendere un servizio non disponibile agli utenti legittimi attraverso l'esaurimento delle risorse necessarie al suo funzionamento.
Nel caso di un DoS, l'attacco proviene da una singola sorgente e colpisce direttamente il servizio target, senza la necessità di un traffico particolarmente elevato.
Nell'esercizio svolto, l'attacco simulato rientra in questa categoria: una sola macchina attaccante è stata sufficiente per rendere il servizio HTTP del target non responsivo, dimostrando come anche un attacco DoS semplice possa avere un impatto significativo sulla disponibilità di un servizio esposto.

DDos: distributed Denial of Service (DDoS) estende il concetto di DoS distribuendo l'attacco su più macchine sorgenti, spesso coordinate tramite botnet.
Questa modalità aumenta la potenza dell'attacco e rende più complessa l'individuazione e la mitigazione del traffico malevolo, poiché le richieste provengono da numerosi indirizzi differenti.
A differenza dell'esercizio svolto, che utilizza una singola sorgente, un attacco DDoS applicherebbe lo stesso principio osservato durante la simulazione, ma amplificato su larga scala, con un impatto potenzialmente più rapido e difficile da contenere.

Slowloris: slowloris è una tecnica di DoS a livello applicativo progettata per colpire specificamente i web server. Il suo funzionamento si basa sul mantenimento di numerose connessioni HTTP incomplete, che vengono tenute aperte inviando periodicamente porzioni di header, impedendo al server di liberare le risorse allocate.
Durante l'esercizio, Slowloris ha dimostrato in modo evidente questo comportamento: pur mantenendo la connettività tra le due macchine, il servizio HTTP del target è diventato non responsivo a causa della saturazione delle risorse applicative.
L'interruzione dello strumento ha portato al ripristino immediato delle risposte HTTP, confermando il meccanismo di attacco e il suo impatto diretto sulla disponibilità del servizio.