Consegna w14d1

ATTACCO DoS sulla macchina ataccante Kali verso Metaspoitable

SVOLGIMENTO

In questo report si documenta la simulazione di un attacco Denial of Service (DoS) dalla macchina attaccante Kali Linux (IP: 192.168.51.99) verso il target Metasploitable (IP: 192.168.51.100), utilizzando il tool Slowloris. Lo scopo è comprendere il funzionamento di un attacco DoS e monitorare l’effetto sull’accessibilità del servizio HTTP esposto sulla porta 80 del target.

SPIEGAZIONE DELL’ATTACCO E TOOL UTILIZZATO

**DoS (Denial of Service):**

Un attacco DoS mira a rendere un servizio o una rete indisponibile per gli utenti legittimi, sovraccaricandolo con traffico o risorse in modo da saturarne la capacità.

**DDoS (Distributed Denial of Service):**

È una variante del DoS in cui l’attacco viene lanciato da molteplici macchine distribuite (botnet o più host), rendendo più difficile bloccare il traffico malevolo.

**Slowloris:**

Slowloris è un tool che sfrutta una tecnica di attacco DoS “a bassa e lenta velocità”. Mantiene aperte molte connessioni HTTP verso il server target, inviando richieste incomplete e lente, occupando risorse del server fino a esaurirle e impedendogli di rispondere a richieste legittime.

SVOLGIMENTO

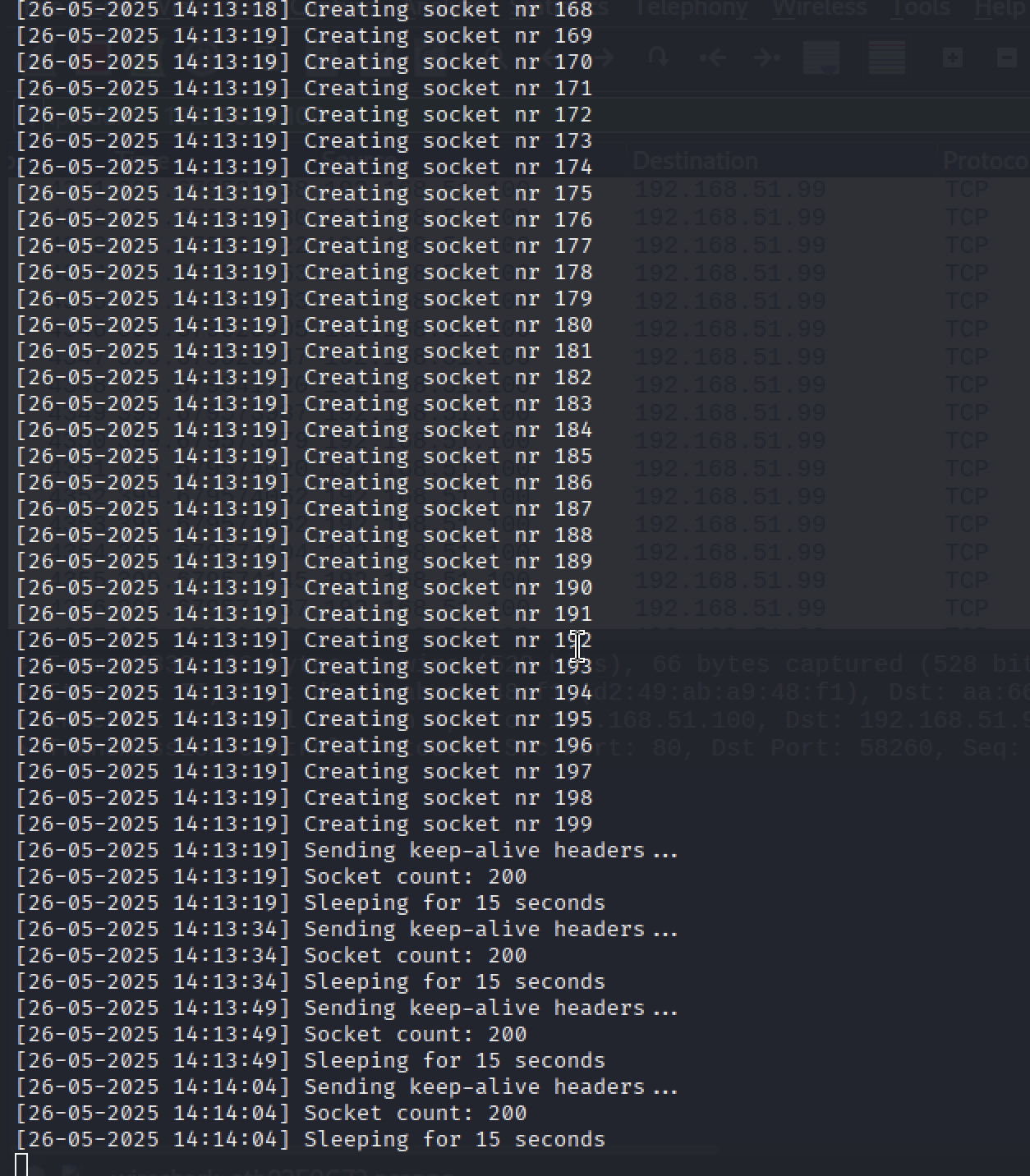
* Macchina attaccante Kali Linux: IP 192.168.51.99
* Macchina target Metasploitable: IP 192.168.51.100
* Servizio HTTP in ascolto sulla porta 80

Il tool Slowloris è stato avviato da Kali con il comando:

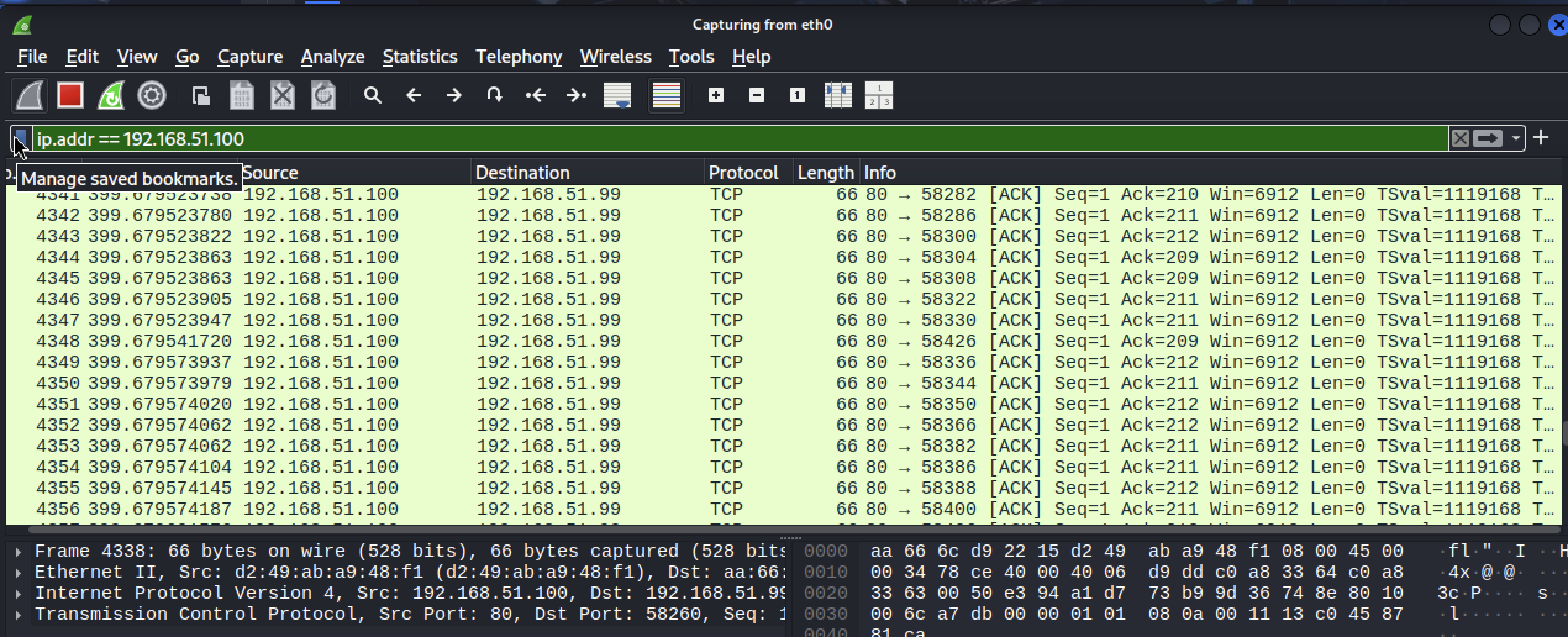
python3 slowloris.py 192.168.51.100 -p 80 -s 200 -v

* -p 80 indica la porta HTTP
* -s 200 imposta il numero di socket aperti (connessioni simultanee)
* -v abilita la modalità verbose per il d ebug

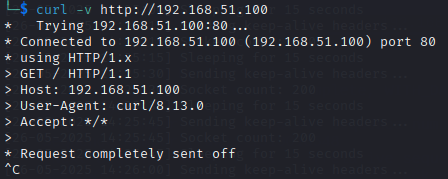
Andando a creare 200 connessioni, come richiesto dal comando.



Verificato il fatto che siano connessioni lasciate in sospeso, chiarito dall’acronimo ACK, singolo, sinonimo del non completamento della connessione TCP per protocollo ACK-SYN-ACK.



Mentre è in esecuzione il tool, il servizio web server sarà temporaneamente inaccessibile causa l’eccessivo traffico.



**Differenze tra connettività HTTP e TCP**

* **HTTP (cURL):** misura la capacità del server di rispondere correttamente a richieste HTTP, quindi valuta sia la raggiungibilità della porta che la funzionalità del servizio web.
* **TCP (tcptraceroute):** verifica semplicemente se la porta TCP 80 è aperta e raggiungibile, indipendentemente dal servizio HTTP che risponde o meno.

Questa differenza è evidente durante un attacco Slowloris, in quanto la porta TCP può risultare aperta, ma il server HTTP può essere comunque incapace di gestire nuove connessioni o richieste.