Analisi Wireshark:

Dopo un analisi dei pacchetti catturati tramite Wireshark, posso dedurre che si tratta con buona probabilità di un attacco DoS poichè è stato inviato un numero considerevole di richieste RST, ACK di tipo TCP che possono causare un sovraccarico del server e conseguenti problemi di operatività nel server.

Una possibile soluzione potrebbe essere quella di disattivare *SAMBA* poiché è stata utilizzata nella fase iniziale dell'attacco o di aggiornala alla versione stable più recente e verificare che le vulnerabilità si siano risolte.

Un altra soluzione può essere quella di bloccare permanentemente o temporaneamente (es. 24h, 7g, 30g ...) gli indirizzi IP che stanno effettuando l'attacco ed di impostare un firewall che filtri le connessioni in entrata.

Altre misure posso essere quelle di usufruire di sistemi che mitighino gli attacchi di questo tipo es: DDos Guard, Cloudflare DDoS Mitigation e verifiche anti baot/spam.

CVE:

La versione Samba 3.0.20-Debian risulta non protetta alle seguenti vulnerabilità:

- CVE-2020-14883: Può causare il crash del servizio Samba con un Denial-of-Service.
- CVE-2021-20234: Un buffer overflow nella funzione net_getdcname() può causare un DoS.