DeAnonimize TOR Network

whit fingerprinting analisys

Paola Guarasci

July 2022

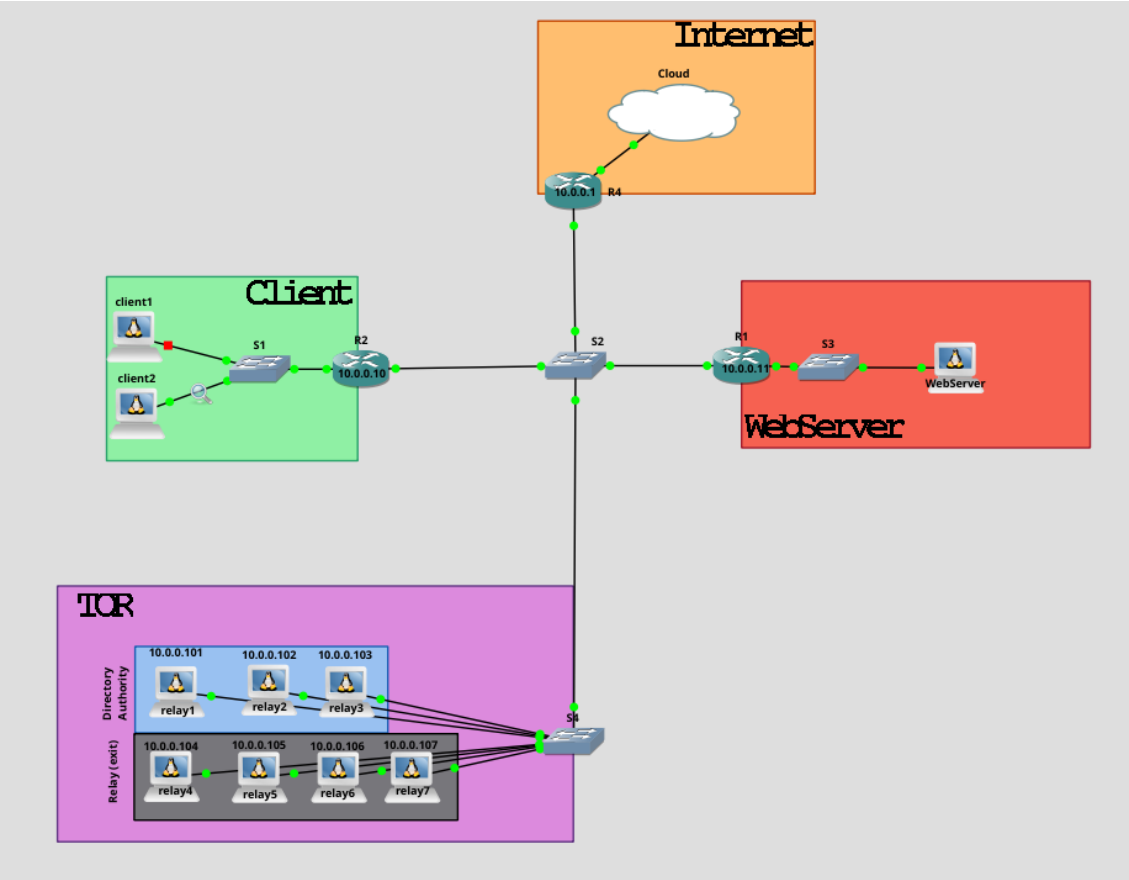
Descrizione del progetto

Il progetto prevede la deanonimizzazione di un utente TOR a partire dalle fingerprint dei siti web visitati.
In particolare e' possibile creare una correlazione tra le risorse e il traffico generato per la loro fruizione.

Aspetti tecnici

Laboratorio

Il laboratio GNS3 realizzato per questo progetto conta un totale di 10 host Debian 11 emulati con QEMU, 3 router Cisco 7200 e 4 switch Cisco 3745.



Rete Tor

La rete Tor e' stata creata partendo dalle configurazioni suggerite dal simulatore di reti Tor private (Chutney). Al suo interno la rete e' divisa in:

- 3 DA (Relay autoritativi)
- 4 Relay di uscita

Ognuno di questi host ha un accesso diretto alla rete interna del laboratorio, per simulare il piu' possibile il fatto che presumibilmente in un contesto reale questi server dispongono di un ip pubblico. La configurazione con 3 directory autority e' conseguenza di alcuni espreimenti in cui la rete non funzionava a dovere e ho poi compreso che le reti Tor necessitano di almeno 3 host auth/mid/exit per creare le rotte. In questi 3 elementi pero' ogni host non include se stesso. Questa configurazione 3+4 e' per me la configurazione minima funzionante.