S6L3

Introduzione

Gli attacchi DoS (Denial of Service) sono tecniche utilizzate per sovraccaricare un sistema o una rete, rendendoli inutilizzabili per gli utenti legittimi. L'attacco UDP Flood si basa sull'invio massiccio di pacchetti UDP (User Datagram Protocol) verso un target, con l'obiettivo di saturarne le risorse di rete o di calcolo.

In questo esperimento, abbiamo scritto uno script in Python per simulare un UDP Flood contro una macchina virtuale Windows XP. L'obiettivo era osservare il comportamento della macchina durante l'attacco e documentare gli effetti sul sistema target.

Scopo dell'Esperimento

- Creare uno script Python che simuli un attacco UDP Flood.
- Lanciare l'attacco su una macchina virtuale Windows XP configurata sul PC.
- Osservare e documentare gli effetti dell'attacco, come rallentamenti o blocchi della macchina virtuale.
- Studiare i concetti base di un attacco DoS.

Materiali e Configurazione dell'Ambiente

1. **Sistema Host:**
    - Sistema operativo: kali linux
    - Software: Visual Studio Code (per eseguire lo script Python)
    - Python versione 3.x (con il modulo socket incluso).
2. **Macchina Virtuale Target:**
    - Sistema operativo: Windows XP
    - Configurazione di rete: Modalità NAT o Bridge per ricevere i pacchetti UDP.
    - Firewall disattivato per evitare il blocco dei pacchetti UDP.
3. **Script Python:**
    - Lo script è progettato per inviare pacchetti UDP di 1 KB verso un IP e una porta specificati dall'utente.

Passaggi dell'Esperimento

1. Creazione dello Script

Abbiamo scritto uno script Python con le seguenti caratteristiche:

- Richiede l'inserimento di:
    - L'indirizzo IP della macchina target.
    - La porta UDP sulla quale inviare i pacchetti.
    - Il numero di pacchetti da inviare.
- Genera pacchetti di 1 KB di dati casuali usando il modulo `random`.
- Invio dei pacchetti tramite il modulo `socket`.

Lo script è stato eseguito in Visual Studio Code e salvato come `udp_flood.py`.

2. Configurazione della Macchina Virtuale

1. Abbiamo avviato la macchina virtuale Windows XP.
2. Utilizzando il comando `ipconfig`, abbiamo identificato l'indirizzo IP della macchina virtuale.
3. Abbiamo disattivato temporaneamente il firewall per garantire che i pacchetti UDP non fossero bloccati.

3. Esecuzione dello Script

1. Abbiamo aperto il terminale integrato in Visual Studio Code.
2. Abbiamo eseguito lo script Python con il comando:
   python udp_flood.py
3. Abbiamo fornito i seguenti dati come input:
   - IP target: l'indirizzo IP della macchina Windows XP.
   - Porta UDP:(una porta scelta casualmente).

4. Osservazione dei Risultati

Durante l'esecuzione dello script, abbiamo osservato i seguenti comportamenti sulla macchina Windows XP:

- **Utilizzo della CPU:**
  - Utilizzando Task Manager, abbiamo notato un aumento significativo dell'utilizzo della CPU.
- **Stato del sistema:**
  - La macchina virtuale è diventata molto lenta e, in alcuni momenti, non rispondeva ai comandi.

Analisi dei Risultati

L'esperimento ha dimostrato che un attacco UDP Flood può facilmente saturare le risorse di una macchina con bassa capacità di rete o di calcolo, come nel caso di Windows XP. In particolare:

- L'invio massivo di pacchetti ha reso il sistema instabile.
- Il carico sulla CPU e sulla rete ha portato a un rallentamento evidente del sistema.

Questo esperimento sottolinea l'importanza di implementare misure di sicurezza come firewall configurati correttamente e sistemi di protezione contro gli attacchi DoS.

L'attacco UDP Flood è un metodo semplice ma efficace per compromettere la disponibilità di un sistema. Tuttavia, eseguire questi esperimenti in un ambiente controllato è essenziale per evitare danni a sistemi reali.

Grazie a questo esperimento, abbiamo appreso:

- Come funziona un attacco DoS basato su UDP.
- Gli effetti di un attacco su un sistema target.
- L’importanza di proteggere i sistemi da questo tipo di minaccia.