# Attacco DoS e Analisi dei Pacchetti con Wireshark

## Attacco DoS (Denial of Service)

### 1. Identificazione della Minaccia

Cos'è un attacco DoS: Un attacco Denial of Service (DoS) è una tipologia di attacco informatico in cui un aggressore tenta di sovraccaricare un server, sistema o rete con un traffico non valido, rendendolo non disponibile agli utenti legittimi. L'attacco può essere realizzato con un elevato numero di richieste false che esauriscono le risorse del sistema, rendendo il servizio non disponibile.

Funzionamento: Durante un attacco DoS, il server della vittima riceve un'enorme quantità di traffico artificiale, con l'intento di impedire agli utenti legittimi di accedere ai servizi. Questo può compromettere la disponibilità delle risorse critiche, portando a gravi interruzioni dei servizi.

### 2. Analisi del Rischio

Impatto potenziale: Un attacco DoS può causare danni significativi all'azienda, compromettendo la disponibilità di servizi web e applicazioni aziendali. Le perdite finanziarie possono essere notevoli se i sistemi critici rimangono offline per lungo tempo, oltre a possibili danni reputazionali.

Servizi critici compromessi:

- - Server web aziendali.
- - Applicazioni interne ed esterne.
- - Sistemi di pagamento online o database.

### 3. Pianificazione della Remediation

Identificazione delle fonti dell'attacco: Utilizzare strumenti di monitoraggio del traffico di rete, come Wireshark, per identificare l'origine del traffico anomalo e individuare gli indirizzi IP sospetti.

Mitigazione del traffico malevolo: Implementare soluzioni di filtraggio del traffico, come firewall e bilanciatori di carico, per gestire il traffico e prevenire il sovraccarico dei sistemi.

### 4. Implementazione della Remediation

Passaggi pratici:

- - Bilanciamento del carico: Implementare soluzioni di bilanciamento del carico per distribuire il traffico in modo efficiente, evitando che un singolo server venga sovraccaricato.

- - Servizi di mitigazione DoS: Utilizzare soluzioni offerte da terze parti, come Cloudflare o AWS Shield, per assorbire e filtrare il traffico malevolo prima che raggiunga i server aziendali.
- - Configurazione firewall: Configurare regole avanzate sui firewall per bloccare richieste sospette provenienti da indirizzi IP noti per comportamenti malevoli.

### 5. Mitigazione dei Rischi Residuali

Misure di mitigazione:

- - Monitoraggio continuo: Implementare un sistema di monitoraggio continuo del traffico di rete per rilevare tempestivamente nuovi tentativi di attacco.
- - Collaborazione con il team di sicurezza: Assicurarsi che le contromisure contro DoS siano sempre aggiornate e che il team di sicurezza migliori costantemente le difese.
- - Test di resilienza: Eseguire periodicamente simulazioni di attacchi DoS per valutare la capacità del sistema di resistere a tali attacchi e adattare le strategie di difesa.

## Wireshark e l'attacco DoS

L' imagine in basso mostra una cattura di pacchetti DoS con Wireshark. Questi pacchetti sono tipicamente caratterizzati da una grande quantità di richieste provenienti da IP sorgenti che inviano traffico verso la destinazione bersaglio. Utilizzando Wireshark è possibile identificare la natura di questo traffico analizzando i pacchetti TCP.

**Wireshark che cattura un attacco Dos:**

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 2024-07-19 06:51:17.946205 | 192.168.1.1 | 10.0.0.1 | TCP | 60 | DoS attack packet |
| 2 | 2024-07-19 06:51:18.946205 | 192.168.1.2 | 10.0.0.1 | TCP | 60 | DoS attack packet |
| 3 | 2024-07-19 06:51:19.946205 | 192.168.1.1 | 10.0.0.1 | TCP | 60 | DoS attack packet |
| 4 | 2024-07-19 06:51:20.946205 | 192.168.1.2 | 10.0.0.1 | TCP | 60 | DoS attack packet |
| 5 | 2024-07-19 06:51:21.946205 | 192.168.1.1 | 10.0.0.1 | TCP | 60 | DoS attack packet |
| 6 | 2024-07-19 06:51:22.946205 | 192.168.1.2 | 10.0.0.1 | TCP | 60 | DoS attack packet |
| 7 | 2024-07-19 06:51:23.946205 | 192.168.1.1 | 10.0.0.1 | TCP | 60 | DoS attack packet |
| 8 | 2024-07-19 06:51:24.946205 | 192.168.1.2 | 10.0.0.1 | TCP | 60 | DoS attack packet |
| 9 | 2024-07-19 06:51:25.946205 | 192.168.1.1 | 10.0.0.1 | TCP | 60 | DoS attack packet |
| 10 | 2024-07-19 06:51:26.946205 | 192.168.1.2 | 10.0.0.1 | TCP | 60 | DoS attack packet |

## Rispondere a un Attacco DoS

Per rispondere efficacemente a un attacco Denial of Service (DoS), è importante adottare una serie di misure tecniche e operative che possono mitigare l'impatto dell'attacco.

## Rispondere a un Attacco DoS

Per rispondere efficacemente a un attacco Denial of Service (DoS), è importante adottare una serie di misure tecniche e operative che possono mitigare l'impatto dell'attacco.

### 1. Identificare l'attacco

Monitoraggio del traffico di rete: Usare strumenti di monitoraggio del traffico (come Wireshark, NetFlow o sistemi di gestione SIEM) per rilevare un traffico anomalo.

Segnali di un attacco: Elevato volume di traffico in entrata proveniente da fonti sconosciute, aumento del numero di connessioni non completate (richieste SYN incomplete), eccessiva latenza del server o indisponibilità del servizio.

### 2. Isolare il traffico malevolo

Bloccare gli IP sospetti: Configurare il firewall o il router per bloccare il traffico proveniente da indirizzi IP identificati come sospetti.

Filtraggio del traffico: Imposta regole per filtrare il traffico sospetto, come il blocco di pacchetti TCP SYN se si sospetta un attacco SYN Flood o il blocco di richieste HTTP in eccesso.

### 3. Utilizzare soluzioni di mitigazione DoS

Bilanciamento del carico: Se i server sono sovraccaricati, implementare un bilanciamento del carico per distribuire il traffico su più server, riducendo il rischio di sovraccarico di un singolo nodo.

Servizi di protezione DoS: Puoi rivolgerti a servizi esterni di mitigazione DoS (come Cloudflare, Akamai, AWS Shield), che possono filtrare e assorbire il traffico malevolo prima che raggiunga la tua rete.

Limiti di connessione: Configura il server per limitare il numero di connessioni simultanee da un singolo indirizzo IP, riducendo così l'impatto dell'attacco.

### 4. Configurare difese di rete avanzate

Intrusion Detection System (IDS) / Intrusion Prevention System (IPS): Implementare sistemi IDS/IPS per rilevare e prevenire attacchi. Questi sistemi possono essere configurati per identificare traffico malevolo e bloccarlo in tempo reale.

Firewall avanzato: Configura regole di firewall per filtrare il traffico in base a criteri specifici, come la quantità di traffico in entrata, l'origine del traffico, o il tipo di pacchetti.

### 5. Monitoraggio continuo e risposta automatica

Monitoraggio continuo: Implementare un sistema di monitoraggio in tempo reale per rilevare nuovi attacchi. Le piattaforme SIEM possono fornire avvisi in tempo reale quando rilevano anomalie nel traffico di rete.

Automatizzare la risposta: Utilizza regole di mitigazione automatizzate nei firewall, nei router o nei dispositivi di sicurezza per reagire velocemente senza la necessità di un intervento umano.

## 6. Collaborazione con ISP

Chiedere assistenza al provider di servizi internet (ISP): In caso di un attacco di larga scala, collaborare con l' ISP per filtrare il traffico a monte prima che raggiunga la rete. Molti ISP offrono servizi di mitigazione per attacchi DoS.

## 7. Post-attacco: Rafforzare le difese

Analisi dell'attacco: Una volta fermato l'attacco, analizzare i log di rete per comprendere meglio l'origine e la natura dell'attacco. Questo ti aiuterà a identificare i punti deboli.

Patching e aggiornamenti: Assicurasi che tutti i sistemi siano aggiornati e che le vulnerabilità scoperte siano corrette con le patch appropriate.

Simulazione e test: Eseguire simulazioni di attacco DoS e test di resilienza per verificare se le contromisure adottate sono efficaci e aggiornate.

## 8. Comunicazione interna ed esterna

Notificare il team di sicurezza: Mantenere il team IT e il team di sicurezza informato sugli sviluppi dell'attacco e sulle contromisure adottate.

Comunicare con i clienti: Se l'attacco ha causato interruzioni significative, informare i clienti in modo trasparente su ciò che è successo e su come stai lavorando per risolvere il problema.

## Conclusione

L'implementazione di misure preventive e di remediation contro un attacco DoS è fondamentale per garantire la continuità dei servizi aziendali e minimizzare i danni economici e reputazionali.