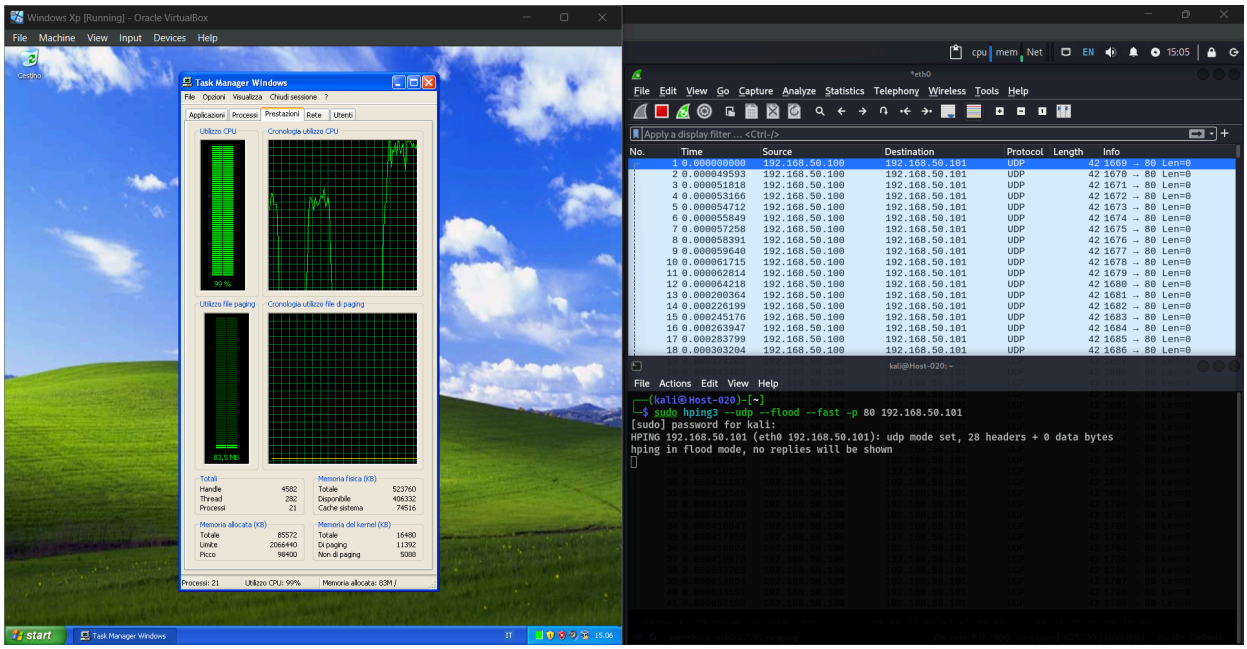
Consegna Ottobre 21

Relazione Completa: Remediation e Mitigazione di Attacchi DoS

Scenario:

In qualità di amministratore di sistema per una media azienda, è stato simulato un attacco **DoS (Denial of Service)** con l'obiettivo di sovraccaricare i server aziendali, rendendo i servizi web inaccessibili agli utenti legittimi. Questo tipo di attacco può paralizzare le attività aziendali, compromettendo la disponibilità dei servizi.



---

1. Identificazione della Minaccia

Un attacco **DoS** si verifica quando un malintenzionato sovraccarica un server con un'enorme quantità di richieste o traffico di rete, impedendo l'accesso agli utenti legittimi. In particolare, un **attacco UDP flood** sfrutta il protocollo UDP per inviare pacchetti senza stato, rendendo il sistema target incapace di elaborare o rispondere adeguatamente. Questo tipo di attacco si

basa sull'invio continuo di pacchetti UDP a una specifica porta del server bersaglio, causando un uso eccessivo delle risorse del sistema (CPU e memoria).

2. Analisi del Rischio

L'impatto di un attacco DoS sull'azienda può essere devastante, specialmente se colpisce servizi critici. Nel nostro scenario, i seguenti servizi potrebbero essere compromessi:

- **Server web aziendali**: essendo il principale punto di accesso per i clienti, la loro indisponibilità può causare una perdita significativa di vendite e fiducia.
- **Applicazioni aziendali**: la disponibilità di software o applicazioni interne è cruciale per il funzionamento quotidiano dell'azienda. La loro indisponibilità potrebbe compromettere l'efficienza del team.

Impatto potenziale:

- **Perdita di produttività**: il personale non potrebbe utilizzare i sistemi aziendali.
- **Perdita economica**: ogni minuto di inattività comporta potenziali perdite di entrate.
- **Impatto sulla reputazione**: clienti e partner potrebbero perdere fiducia nell'azienda.

3. Pianificazione della Remediation

Il piano per contrastare un attacco DoS include i seguenti passaggi:

- **Identificazione della fonte dell'attacco**: Utilizzare strumenti come Wireshark per monitorare e catturare il traffico anomalo. Questo può aiutare a identificare gli indirizzi IP di origine dell'attacco.
- **Mitigazione del traffico malevolo**: Implementare regole di firewall per filtrare il traffico in entrata, limitando il numero di pacchetti provenienti da IP sospetti o volumi eccessivi di traffico UDP.

4. Implementazione della Remediation

Per simulare un attacco DoS, è stato utilizzato il comando **hping3** da una macchina Kali Linux per inviare pacchetti UDP flood al server Windows XP target. Ecco i dettagli della dimostrazione:

Attacco DoS simulato: Il comando usato è stato:

```
sudo hping3 --udp --flood --fast -p 80 192.168.50.101
```

1. Questo comando ha inviato pacchetti **UDP** in modalità flood alla porta **80** del sistema target (Windows XP), saturando il server.
2. **Monitoraggio del Target**: Sul target (Windows XP), il **Task Manager** ha mostrato che l'utilizzo della **CPU** ha raggiunto il **99%**, segnalando che il sistema era quasi completamente sovraccaricato dal traffico in entrata.
3. **Analisi del traffico con Wireshark**: Utilizzando **Wireshark**, è stato catturato e analizzato il traffico UDP in entrata, confermando l'inondazione di pacchetti provenienti dall'indirizzo IP dell'attaccante. Il traffico UDP veniva inviato in modo rapido e continuo, senza risposte dal target, poiché era troppo sovraccaricato per gestire le richieste.

Lo **screenshot** allegato è stato realizzato da me durante un **penetration test** come dimostrazione pratica di un attacco DoS, evidenziando come l'uso di strumenti come **hping3** su Kali e **Wireshark** per la cattura del traffico possano confermare e monitorare l'efficacia dell'attacco.

5. Mitigazione dei Rischi Residuali

Dopo aver identificato l'attacco, si potrebbe valutare l'implementazione di diversi metodi di mitigazione per proteggere il server da attacchi futuri:

Soluzioni di mitigazione:

1. **Bilanciamento del carico**:
    - Implementare un **load balancer** per distribuire uniformemente il traffico tra più server, prevenendo il sovraccarico di un singolo sistema. Questo riduce il rischio che un singolo punto di accesso venga saturato.
2. **Servizi di mitigazione DoS**:
    - Utilizzare servizi di terze parti come **Cloudflare** o **AWS Shield** per filtrare e mitigare il traffico malevolo. Questi servizi offrono protezione avanzata contro attacchi DoS e DDoS.
3. **Configurazione di firewall e filtri**:
    - Configurare il **firewall** aziendale per bloccare o limitare il traffico proveniente da indirizzi IP sospetti, soprattutto per protocolli come UDP che non richiedono una connessione stabile. Regole di **rate limiting** possono essere utili per prevenire inondazioni di pacchetti.
4. **Monitoraggio continuo**:
    - Implementare sistemi di **monitoraggio continuo del traffico di rete**, come intrusion detection systems (IDS), per identificare tempestivamente nuove minacce e rispondere rapidamente. Questo può includere l'uso di log e alert per avvisare l'amministratore di rete quando il traffico raggiunge livelli anomali.
5. **Collaborazione interna**:

- Collaborare con il team di sicurezza per migliorare le difese contro attacchi DoS e altre minacce simili. Pianificare esercitazioni periodiche di resilienza per testare l’efficacia delle misure adottate.

6. Conclusione

L'attacco DoS simulato ha dimostrato l'efficacia di una semplice inondazione UDP nel sovraccaricare un sistema Windows XP. Il target ha raggiunto quasi il **100%** di utilizzo della CPU, rendendolo incapace di rispondere a richieste legittime. Questo tipo di attacco può avere conseguenze gravi su un'azienda, ma con un’adeguata pianificazione di mitigazione, monitoraggio continuo e l'uso di strumenti avanzati, è possibile ridurre il rischio di interruzioni prolungate e proteggere i servizi aziendali.