S3/L5 - Esercizio programmazione per Hacker NetRaiders, 08 marzo 2024

Consegna:

L'esercizio di oggi è 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.

Requisiti:

- Il programma deve richiedere l'inserimento dell'IP target.
- Il programma deve richiedere l'inserimento della porta target.
- La grandezza dei pacchetti da inviare è di 1 KB per pacchetto
- Suggerimento: per costruire il pacchetto da 1KB potete utilizzare il modulo «random» per la generazione di byte casuali.
- Il programma deve chiedere all'utente quanti pacchetti da 1 KB inviare.

A scopo dimostrativo del programma, abbiamo utilizzato il programma creato su una macchina con Windows che hosta il bersaglio, su una macchina virtuale con Kali Linux. Seguono le impostazioni utilizzate.

Windows 11:

```
Scheda LAN wireless Wi-Fi:

Suffisso DNS specifico per connessione: homenet.telecomitalia.it
Indirizzo IPv6 locale rispetto al collegamento . : fe80::a669:7195:3773:4481%18
Indirizzo IPv4. . . . . . . . . . : 192.168.1.18
Subnet mask . . . . . . . . . . . : 255.255.255.0
Gateway predefinito . . . . . . . . : 192.168.1.1
```

Kali Linux:

```
-(kali® kali)-[~]
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group d
efault glen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
    inet6 :: 1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
   link/ether 08:00:27:21:b1:d0 brd ff:ff:ff:ff:ff
    inet 192.168.1.70/24 brd 192.168.1.255 scope global dynamic noprefixrou
te eth0
       valid_lft 67836sec preferred_lft 67836sec
    inet6 fe80::17f9:985c:3781:1b80/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Il codice sorgente può essere consultato nel file presente su GitHub, con tanto di relativi commenti.

Avvio del programma su macchina Windows:

```
Benvenuto nel miglior programma di UDP Flood del mondo creato dai NetRaiders @
      /$$ /$$$$$$$ /$$$$$$$ /$$$$$$
                                        /$$$$$$
                                              $$|_
 $$$ | $$ | $$
                        $$_
                           /| $$
                                    $$ /$$_
                                                   $$ /|
                                                         $$
                                                               $$ $$
                                                                                   $$ /$$
 $$$$| $$| $$
                        $$
                              $$ \ $$ | $$
                                           \ $$
                                                  | $$
                                                         $$
                                                              \ $$| $$
                                                                             $$
                                                                                 \ $$| $$
 $$ $$ $$| $$$$$
                       $$
                              $$$$$$$/|
                                        $$$$$$$$
                                                   $$
                                                         $$
                                                               $$|
                                                                   $$$$$
                                                                             $$$$$$$/|
                                                                                        $$$$$$
                                              $$
                                                    $$
                                                         $$
                                                                                   $$
           $$
                        $$
                                    $$|
                                        $$
                                                               $$|
                                                                   $$
                                                                             $$
 $$
     $$$$
                              $$
 $$\
      $$$|
                        $$
                              $$
                                   \ $$|
                                        $$
                                              $$
                                                  | $$
                                                         $$
                                                               $$|
                                                                   $$
                                                                             $$
                                                                                  $$
                                                                                           \$$
           $$
                                                                                     /$$
 $$
    \ $$|
           $$$$$$$$
                        $$
                              $$
                                    $$| $$
                                              $$
                                                 /$$$$$$
                                                         $$$$$$$/
                                                                   $$$$$$$$$ $$
                                                                                   $$|
                                                                                       $$$$$$/
Inserisci indirizzo IP/Host bersaglio: 192.168.1.70
Inserisci porta bersaglio (Da 0 a 65535): 1234
Inserisci numero di pacchetti da 1KB da inviare: 20
     Sono stati spediti 20 pacchetti da 1KB all'indirizzo IP 192.168.1.70 sulla porta 1234
```

L'indirizzo bersaglio è, come specificato prima, quello della macchina virtuale Kali. Una volta terminato l'invio dei pacchetti, se non riscontra errori, il programma può essere eseguito nuovamente.

Arrivo dei pacchetti analizzati tramite WireShark, che verifica il traffico di tipo UDP in entrata.

