

S3/L5 - Esercizio programmazione per Hacker

NetRaiders, 15 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)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 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:ff
    inet 192.168.1.70/24 brd 192.168.1.255 scope global dynamic noprefixroute 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.

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.

Wireshark packet capture showing UDP traffic. The filter is `_ws.col.protocol == "UDP"`. The packet list shows 28 packets, with 25 highlighted in blue. The packet details pane shows the structure of a UDP packet with fields for Number of ports, Length, and Info.

No.	Time	Source	Destination	Protocol	Length	Info
2413	613.997739125	192.168.1.2	239.255.255.250	UDP	77	46577 → 15600 Len=35
2422	616.557012334	192.168.1.81	255.255.255.255	UDP	78	56700 → 56700 Len=36
2424	616.971179434	192.168.1.2	192.168.1.255	UDP	77	46294 → 15600 Len=35
2433	619.937507107	192.168.1.2	239.255.255.250	UDP	77	53424 → 15600 Len=35
2447	625.978769235	192.168.1.2	239.255.255.250	UDP	77	38691 → 15600 Len=35
2478	628.950359271	192.168.1.2	192.168.1.255	UDP	77	53562 → 15600 Len=35
2498	632.021615088	192.168.1.2	239.255.255.250	UDP	77	56384 → 15600 Len=35
2503	633.603148020	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2504	633.603148158	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2507	633.603226019	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2508	633.603226079	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2509	633.603226102	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2510	633.603226125	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2511	633.603226147	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2512	633.603226170	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2516	633.603329055	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2517	633.603329159	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2518	633.603329192	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2519	633.603329218	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2520	633.603372725	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2521	633.603372782	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2522	633.603372808	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2523	633.603372831	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2525	633.603459542	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2526	633.603459615	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2527	633.603459641	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2528	633.603495008	192.168.1.18	192.168.1.70	UDP	1066	64887 → 1234 Len=1024
2533	634.684048794	192.168.1.24	255.255.255.255	UDP	82	49154 → 1947 Len=40
2534	634.994202984	192.168.1.2	192.168.1.255	UDP	77	53480 → 15600 Len=35
2535	635.404076679	192.168.1.24	239.255.255.250	UDP	698	60959 → 3702 Len=656
2536	635.410699735	192.168.1.24	239.255.255.250	UDP	698	60959 → 3702 Len=656