

WIRESHARK

- ¿De qué se trata la captura de tráfico? (i.e. ¿qué está sucediendo?)
Conectando un reverse Shell
- ¿Cuál es la dirección IP del equipo atacante?
192.168.245.128
- ¿Cuál es la dirección IP de la víctima?
192.168.245.1
- ¿Qué comandos se están ejecutando?

Ip config

```
> Frame 26: 63 bytes on wire (504 bits), 63 bytes captured (504 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_9d:b3:75 (00:0c:29:9d:b3:75), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
> Internet Protocol Version 4, Src: 192.168.245.128, Dst: 192.168.245.1
> Transmission Control Protocol, Src Port: 59602, Dst Port: 7070, Seq: 8, Ack: 194, Len: 9

0000  00 50 56 c0 00 08 00 0c 29 9d b3 75 08 00 45 00  -PV....-u-E-
0010  00 31 3b ea 40 00 06 93 09 c0 a8 f5 80 c0 a8    -1;@#-----
0020  f5 01 e8 d2 1b 9e 7a 40 0b 6a 9b 85 cc d1 50 18    ....2@-j...P-
0030  00 3f 6b f7 00 00 69 70 63 6f 6e 66 69 67 0a    -?k...ip config
```

whoaim

```
> Frame 15: 61 bytes on wire (488 bits), 61 bytes captured (488 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_9d:b3:75 (00:0c:29:9d:b3:75), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
> Internet Protocol Version 4, Src: 192.168.245.128, Dst: 192.168.245.1
> Transmission Control Protocol, Src Port: 59602, Dst Port: 7070, Seq: 1, Ack: 129, Len: 7

0000  00 50 56 c0 00 08 00 0c 29 9d b3 75 08 00 45 00  -PV....-u-E-
0010  00 2f 3b ea 40 00 06 93 11 c0 a8 f5 80 c0 a8    -/;@#-----
0020  f5 01 e8 d2 1b 9e 7a 40 0b 63 9b 85 cc 90 50 18    ....2@-c...P-
0030  00 3f 6b f5 00 00 7f 68 6f 61 6d 69 0a          -?k...ah.oiam!
```

```
> Frame 45: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: IPvmcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.245.1, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 64276, Dst Port: 1900

0000  01 00 5e 7f ff fa 00 50 56 c0 00 08 00 45 00  -...P V....E-
0010  00 ca ce de 00 00 01 11 44 a0 c0 a8 f5 01 ef ff    ....D.....
0020  ff fa fb 14 07 6c 00 b6 5c ab 4d 2d 53 45 41 52    ....1- \M-SEAR
0030  43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48    CH # HTT P/1.1-H
0040  4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35    OST: 239.255.255
0050  2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20    .250:190 0-MAN:
0060  22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d    "ssid:dl scover"-
0070  0a 7d 58 1a 20 31 0d 00 53 54 3a 20 75 72 6e 3a    558.192 ST: urn:
0080  64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e    dial-mul tiscreen
0090  2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61    -org:ser vice:dia
00a0  6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a    l:1-USE R-AGENT:
00b0  20 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 38    Google Chrome/8
00c0  33 2e 30 2e 34 31 30 33 2e 31 31 36 20 57 69 6e    3.0.4103 .116 Win
00d0  64 6f 77 73 0d 0a 0d 0a                          dows....
```