

WIRESHARK

- ¿De qué se trata la captura de tráfico? (i.e. ¿qué está sucediendo?)
Conectando un reverse Shell, con la atacante de Parrot y la víctima es la maquina Windows.
- ¿Cuál es la dirección IP del equipo atacante?
192.168.0.7
- ¿Cuál es la dirección IP de la víctima?
192.168.0.16
- ¿Qué comandos se están ejecutando?

Ip config

```
maaacosg@maaacosg-security:~/Desktop
$ sudo tcpdump -nnXS port 8888
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:49:04.742224 IP 192.168.0.7.1204 > 192.168.0.16.8888: Flags [P.], seq 2089667591:2089667600, ack 3672076340, win 64240, length 9: HTTP
  0x0000: 4500 0031 df14 4000 8006 9a4a c0a8 0007
  0x0010: c0a8 0010 04b4 1f90 7c8d cc07 dadf 7034
  0x0020: 5018 faf0 ccd9 0000 6966 636f 6e66 6967
  0x0030: 0a
22:49:04.742263 IP 192.168.0.16.8888 > 192.168.0.7.1204: Flags [.] , ack 2089667600, win 64231, length 0
  0x0000: 4500 0020 202e 4000 4006 9a3a c0a8 0010
  0x0010: c0a8 0007 1f90 04b4 dadf 7034 7c8d cc10
  0x0020: 5010 fae7 8182 0000
22:49:04.745992 IP 192.168.0.16.8888 > 192.168.0.7.1204: Flags [P.], seq 3672076340:3672077215, ack 2089667600, win 64231, length 875: HTTP
  0x0000: 4500 0393 292f 4000 4006 8cce c0a8 0010
  0x0010: c0a8 0007 1f90 04b4 dadf 7034 7c8d cc10
  0x0020: 5010 fae7 84e4 0000 6574 6830 3a20 666c
  0x0030: 6167 733d 3431 3633 3c55 502c 4252 4f41
  0x0040: 4443 4153 542c 5255 4e4e 494e 472c 4d55
  0x0050: 4c54 4943 4153 543e 2020 6d74 7520 3135
  0x0060: 3030 0a20 2020 2020 2020 2069 6e65 7420
  0x0070: 3139 322e 3136 382e 302e 3136 2020 6e65
  0x0080: 746d 6173 6620 3225 352e 3235 352e 3235
  0x0090: 352e 3020 2062 7261 6164 6361 7374 2031
  0x00a0: 3932 2e31 3638 2e30 2e32 3535 0a20 2020
  0x00b0: 2020 2020 2069 6e65 7436 2066 6538 303a
  0x00c0: 3a35 3732 303a 3863 643a 6363 3463 3a36
  0x00d0: 3937 3320 2070 7265 6669 706c 656e 2036
  0x00e0: 3420 2073 636f 7065 6964 2030 7832 303c
  0x00f0: 6c69 6e6e 3a0e 2020 2020 2020 2020 6574
  0x0100: 6865 7220 3038 3a30 303a 3237 3a34 373a
  0x0110: 6238 3a30 3020 2074 7071 7565 7565 6c65
  0x0120: 6e20 3130 3030 2020 2845 7468 6572 6e65
  0x0130: 7429 0a20 2020 2020 2020 2052 5820 7061
  0x0140: 636b 6574 7320 3133 3134 2020 6279 7465
  0x0150: 7320 3238 3538 3339 2028 3237 3924 3120
  0x0160: 4b69 4229 0a20 2020 2020 2020 2052 5030
  0x0170: 6572 726f 7273 2030 2020 6472 6170 7065
  .....
```

whoaim

```
0x0300: 300a 0a
22:49:04.787509 IP 192.168.0.7.1204 > 192.168.0.16.8080: Flags [.], ack 3672077215, win 63365, length 0
0x0000: 4500 0028 df15 4000 0006 9a52 c0a8 0007
0x0010: c0a8 0010 04b4 1f90 7c8d cc10 dadf 739f
0x0020: 5010 f785 7b85 0000 0000 0000 0000 0000
22:50:26.870327 IP 192.168.0.7.1204 > 192.168.0.16.8080: Flags [P.], seq 2089667600:2089667607, ack 3672077215, win 63365, length 7: HTTP
0x0000: 4500 002f df16 4000 0006 9a4a c0a8 0007
0x0010: c0a8 0010 04b4 1f90 7c8d cc10 dadf 739f
0x0020: 5018 f785 1d43 0000 7768 6f61 6d69 0a
22:50:26.870370 IP 192.168.0.16.8080 > 192.168.0.7.1204: Flags [.], ack 2089667607, win 64224, length 0
0x0000: 4500 0028 2930 4000 4006 9038 c0a8 0010
0x0010: c0a8 0007 1f90 04b4 dadf 739f 7c8d cc17
0x0020: 5010 fae0 8182 0000
22:50:26.928795 IP 192.168.0.16.8080 > 192.168.0.7.1204: Flags [P.], seq 3672077215:3672077225, ack 2089667607, win 64224, length 10: HTTP
0x0000: 4500 0032 2931 4000 4006 902d c0a8 0010
0x0010: c0a8 0007 1f90 04b4 dadf 739f 7c8d cc17
0x0020: 5018 fae0 818c 0000 6d61 6161 7263 6f73
0x0030: 670a
22:50:26.901522 IP 192.168.0.7.1204 > 192.168.0.16.8080: Flags [.], ack 3672077225, win 63355, length 0
0x0000: 4500 0028 df17 4000 0006 9a50 c0a8 0007
0x0010: c0a8 0010 04b4 1f90 7c8d cc17 dadf 73a9
0x0020: 5010 f77b 7b7e 0000 0000 0000 0000 0000
```