Universidad del Valle de Guatemala
Administración y Mantenimiento de Sistemas

Marcos Gutiérrez
17909
29 de jul. de 21

WIRESHARK

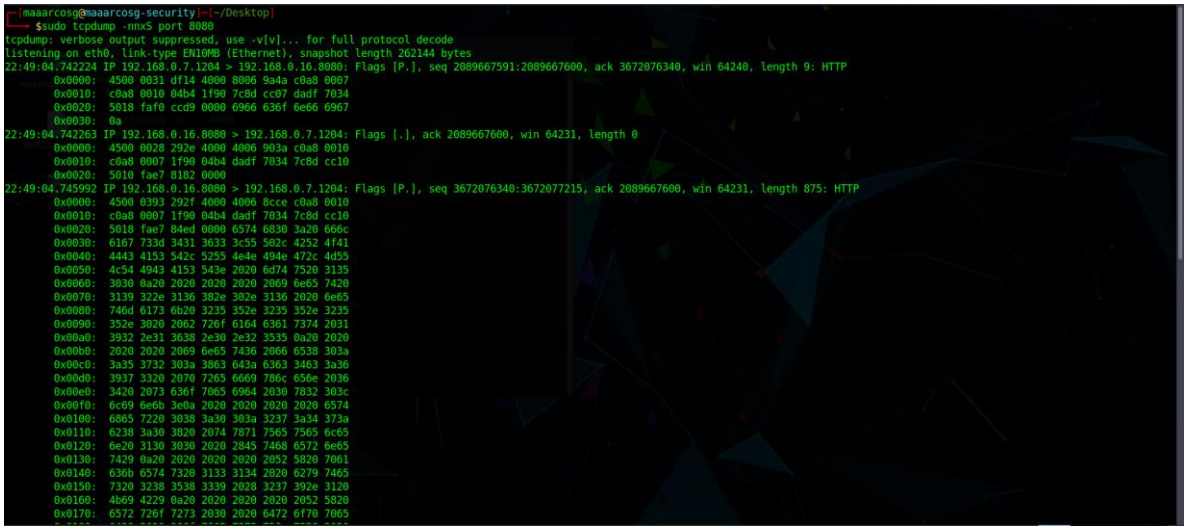
- ¿De qué se trata la captura de tráfico? (i.e. ¿qué está sucediendo?)
  Conectando un reverse Shell, con la atacante de Parrot y la victima es la maquina Windows.

- ¿Cuál es la dirección IP del equipo atacante?
  192.168.0.7

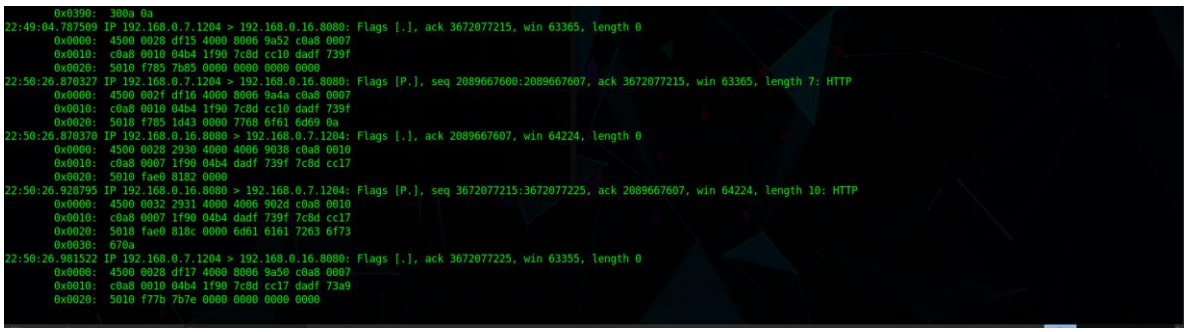
- ¿Cuál es la dirección IP de la víctima?
  192.168.0.16

- ¿Qué comandos se están ejecutando?

  Ip config



  whoaim


0x0390: 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 8006 9a52 c0a8 0007
0x0010: c0a8 0010 04b4 1f90 7c8d cc10 dadf 739f
0x0020: 5010 f785 7b85 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 8006 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
22:50:26.981522 IP 192.168.0.7.1204 > 192.168.0.16.8080: Flags [.], ack 3672077225, win 63355, length 0
0x0000: 4500 0028 df17 4000 8006 9a50 c0a8 0007
0x0010: c0a8 0010 04b4 1f90 7c8d cc17 dadf 73a9
0x0020: 5010 f77b 7b7e 0000 0000 0000