

Pentest com Kali Linux





Instrutor: Vitor Mazuco

<http://facebook.com/vitormazuco>

Email: vitor.mazuco@gmail.com

WebSite: <http://vmzsolutions.com.br>



Visualização de controle

Agora vamos aprender como aplicar filtros no Wireshark para olhar para gerenciamento, controle e quadros de dados. Para visualizar todos os quadros de gestão em que os pacotes de ser capturado, digite o filtro: *wlan.fc.type == 0*, para os *Control Frames* coloque assim *wlan.fc.type == 1*, para os *data frames*, *wlan.fc.type == 2*



Visualização de controle

Capturing from mon0 [Wireshark 1.8.5]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.fc.type==0

Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1452	147.804849000	D-Link_62:6d:08	Broadcast	802.11	142	Beacon
1453	147.907929000	D-Link_62:6d:08	Broadcast	802.11	142	Beacon
1454	148.009835000	D-Link_62:6d:08	Broadcast	802.11	142	Beacon
1455	148.112300000	D-Link_62:6d:08	Broadcast	802.11	142	Beacon

Frame 1452: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0

Radiotap Header v0, Length 18

IEEE 802.11 Beacon frame, Flags:

IEEE 802.11 wireless LAN management frame

- Fixed parameters (12 bytes)
- Tagged parameters (88 bytes)
 - Tag: SSID parameter set: Upstairs
 - Tag Number: SSID parameter set (0)

0000	00 00 12 00 2e 48 00 00	00 02 6c 09 a0 00 aa 01H.. ..l.....
0010	00 00 80 00 00 00 ff ff	ff ff ff ff 00 22 b0 62".b
0020	6d 08 00 22 b0 62 6d 08	70 f1 1c 47 74 83 4c 00	m..".bm. p..Gt.L.
0030	00 00 64 00 11 04 00 08	55 70 73 74 61 69 72 73	..d..... Upstairs
0040	01 04 82 84 8b 96 03 01	01 dd 16 00 50 f2 01 01P...
0050	00 00 50 f2 02 01 00 00	50 f2 02 01 00 00 50 f2	..P..... P.....P.
0060	02 05 04 00 01 00 30 dd	18 00 50 f2 02 01 01 000. ..P.....



Visualização de controle

Para selecionar, um subtipo, use o filtro `wlan.fc.subtype`
`filter` Por exemplo, para visualizar todos os *Beacon frames*
entre todos os quadros de gerenciamento, use o seguinte
filtro: `(wlan.fc.type == 0) && (wlan.fc.subtype == 8)`



Visualização de controle

Capturing from mon0 [Wireshark 1.8.5]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `(wlan.fc.type==0) && (wlan.fc.subtype==8)` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
533	48.550416000	D-Link_62:6d:08	Broadcast	802.11	142	Beacon
537	48.652957000	D-Link_62:6d:08	Broadcast	802.11	142	Beacon
538	48.755640000	D-Link_62:6d:08	Broadcast	802.11	142	Beacon
541	48.857660000	D-Link_62:6d:08	Broadcast	802.11	142	Beacon

Frame 533: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0

- Radiotap Header v0, Length 18
- IEEE 802.11 Beacon frame, Flags:
- IEEE 802.11 wireless LAN management frame
 - Fixed parameters (12 bytes)
 - Tagged parameters (88 bytes)
 - Tag: SSID parameter set: Upstairs
 - Tag Number: SSID parameter set (0)

0000 00 00 12 00 2e 48 00 00 00 02 6c 09 a0 00 ac 01H.. ..l.....
0010 00 00 80 00 00 00 ff ff ff ff ff ff 00 22 b0 62".b
0020 6d 08 00 22 b0 62 6d 08 f0 b3 fc bd 89 7d 4c 00 m..".bm.}L.
0030 00 00 64 00 11 04 00 08 55 70 73 74 61 69 72 73 ..d..... Upstairs
0040 01 04 82 84 8b 96 03 01 01 dd 16 00 50 f2 01 01P...
0050 00 00 50 f2 02 01 00 00 50 f2 02 01 00 00 50 f2 ..P..... P....P.
0060 02 05 04 00 01 00 30 dd 18 00 50 f2 02 01 01 000. ..P.....