Pentest com Kali Linux

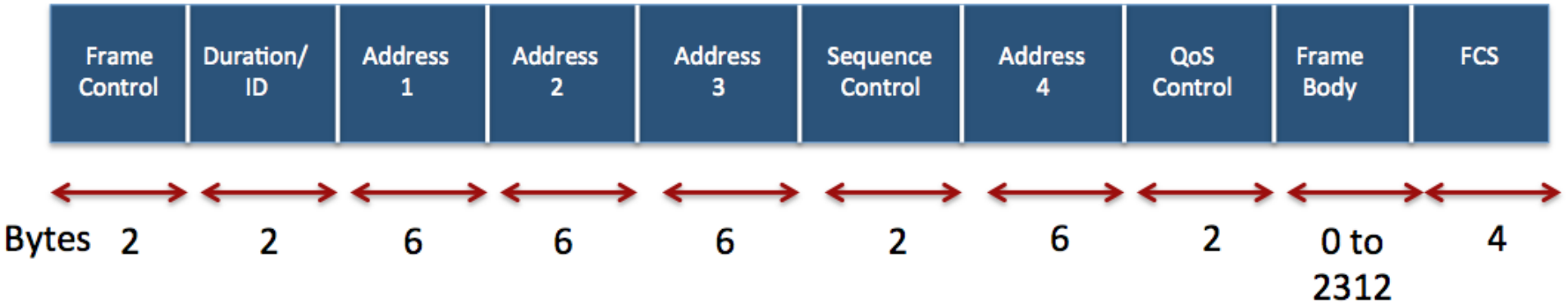
Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

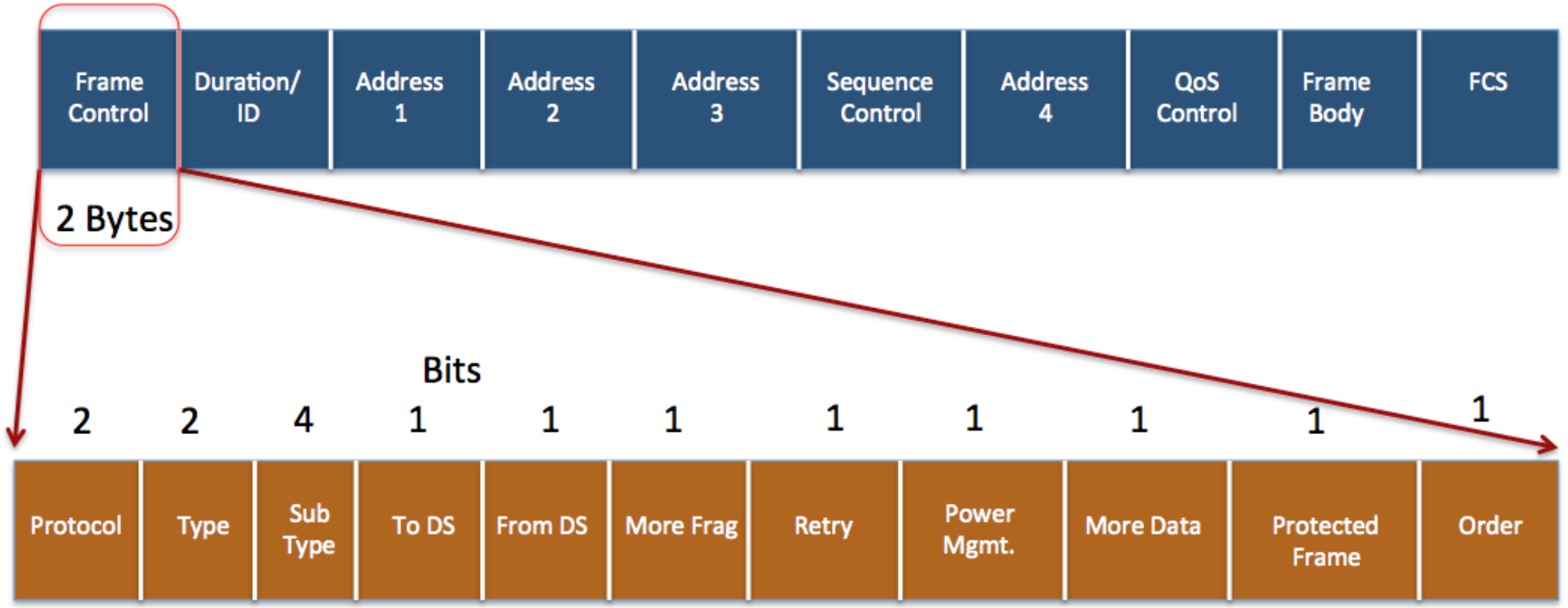
Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Vamos agora revisar alguns conceitos básicos de WLANs que a maioria de vocês podem já estar ciente. Em WLANs, a comunicação acontece ao longo de *frames*. Um *frame(quadro)* teria a seguinte estrutura de cabeçalho:



O próprio campo de *Frame Control* tem uma estrutura mais complexa:



O campo Type define três tipos de estrutura WLAN:

- **Frames de gerenciamento**
- **Frames de controle**
- **Os Frames de dados**

Os Frames de gerenciamento são responsáveis pela manutenção comunicação entre pontos de acesso e clientes sem fio. Eles podem ter os seguintes subtipos:

- Autenticação
- Desautenticação
- Pedido de associação
- Associação de resposta
- Pedido de reassociação
- Resposta de reassociação

WLAN e suas inseguranças inerentes

- Dissociação
- Aviso
- Pedido de sondagem
- Pesposta da sondagem

Os frames de controle são responsáveis por garantir um correcto intercâmbio de dados entre os pontos de acesso e clientes sem fio. Eles podem ter os seguintes subtipos:

- Solicitação de envio (RTS)
- Clear to Send (CTS)
- Confirmação (ACK)

Os quadros de dados carregam os dados reais que são enviados na rede sem fio. Não existem subtipos para ele.

Em nossas aulas vamos farejar esses quadros através de uma rede sem fio usando o Wireshark. Existem outras ferramentas, tais como Airodump-NG, Tcpdump ou Tshark, que você pode usar também. O primeiro passo de fazer isso é para criar uma interface de modo monitor. Isto irá criar uma interface para o nosso adaptador, o que nos permite ler todos os frames no ar, independentemente de se é destinado a nós ou não. No mundo conectado, este é popularmente chamado de ***modo promíscuo***.