HACKING ÉTICO: COMO ATACAR/DEFENDER AS VLANS DE UM SWITCH?

INSTITUTO FEDERAL
Goiás
Câmpus Formosa

SECITEC
SEMANA DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Prof. Mario Lemes

07/12/2021 (19:00 às 21:00)

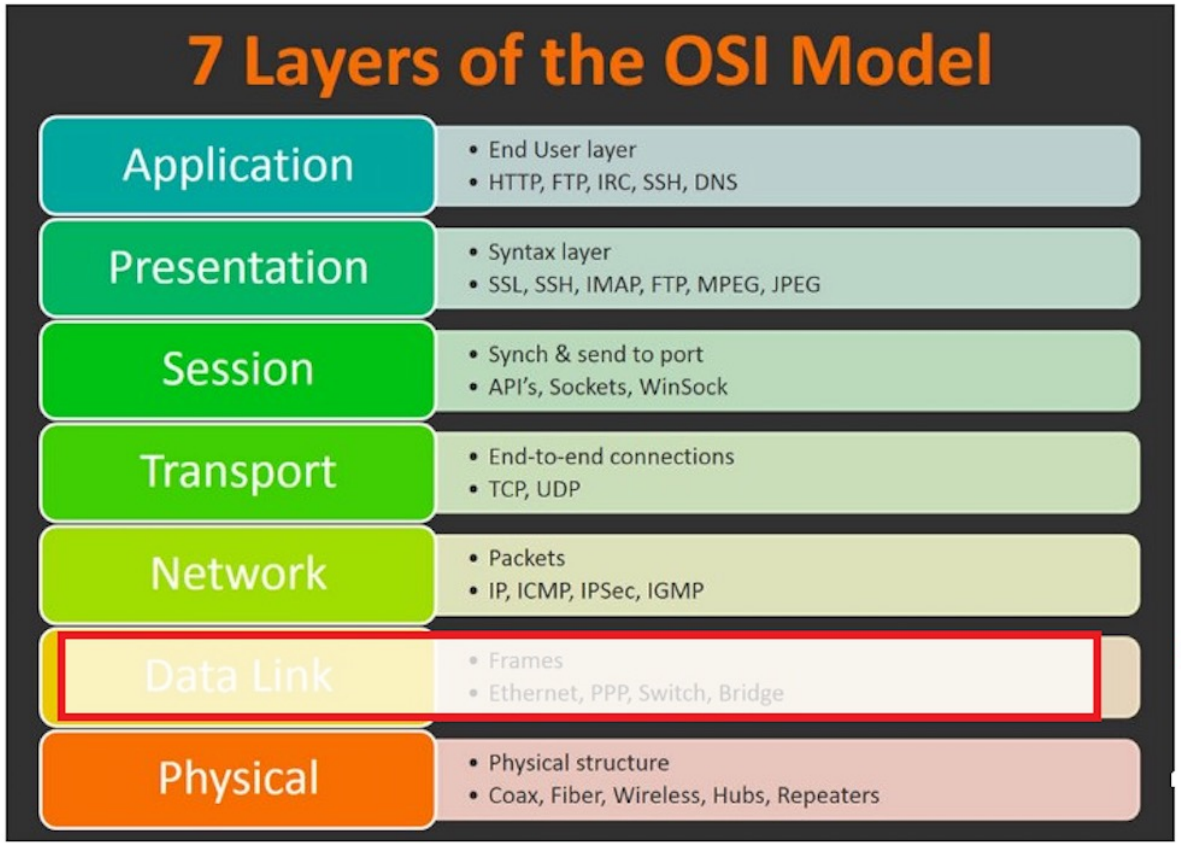
AVISO DE ISENÇÃO

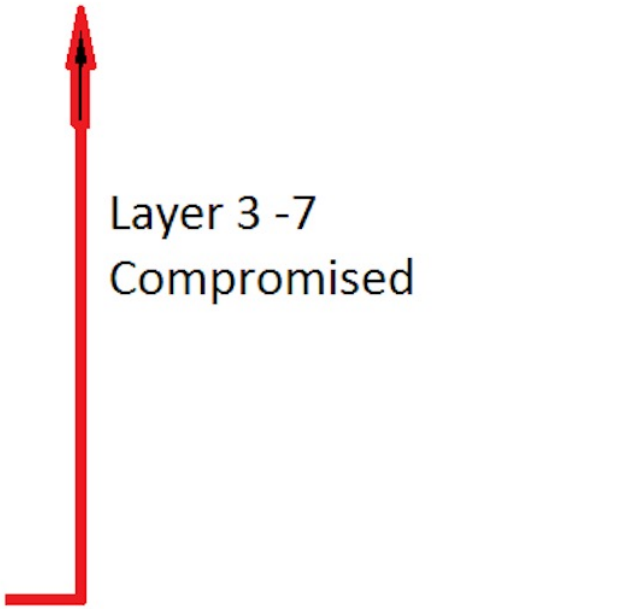
- Todos os conteúdos, atividades e aplicações (softwares) mostrados nesta conferência possuem objetivos 100% educativos, no qual o palestrante e o IFG não possuem qualquer responsabilidade em relação ao mal uso que os participantes possam fazer com as informações adquiridas.

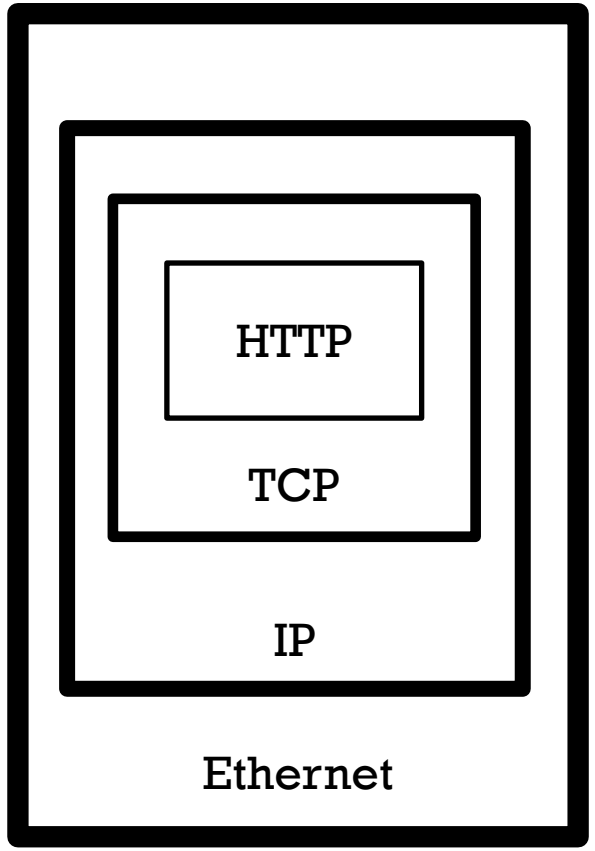
- O hacking ético é feito pelo "hacker do bem". Este é um profissional de TI com alta especialização em invasão de sistemas e detecção de vulnerabilidades, que se passa por um invasor e faz ataques programados para tentar achar brechas de invasão de uma rede/sistema.

- Não use as informações deste seminário para hackear redes/sistemas que você não tem permissão.

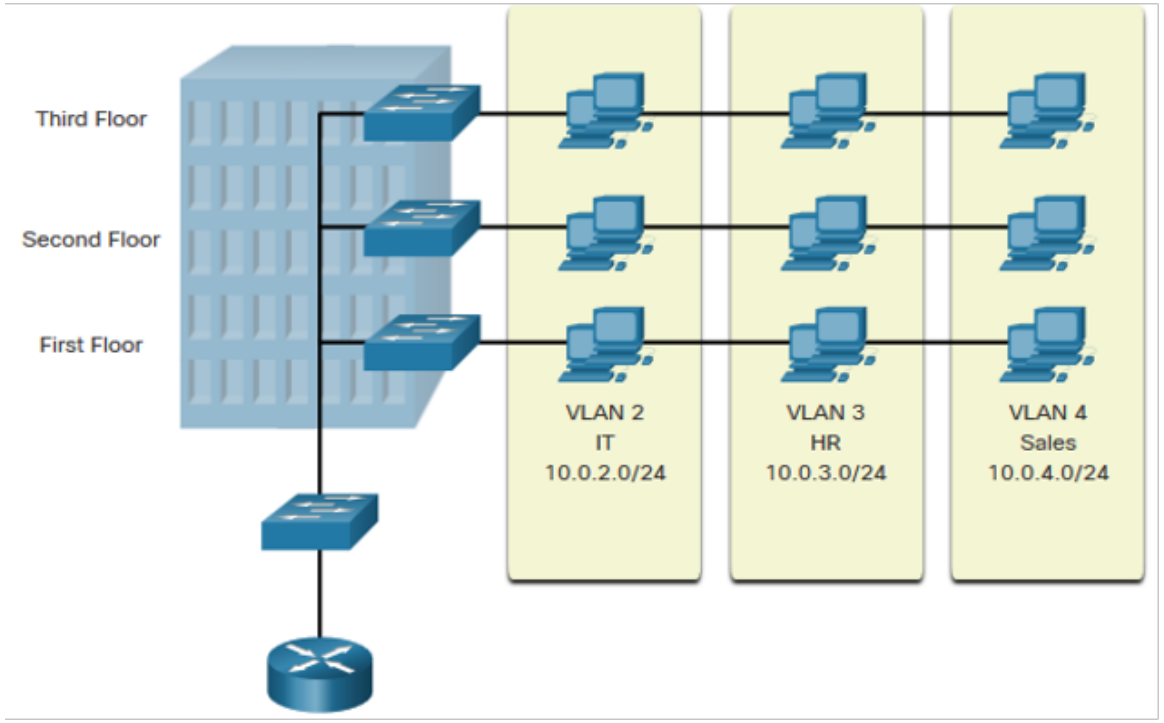
POR QUE SEGURANÇA DA CAMADA L2?





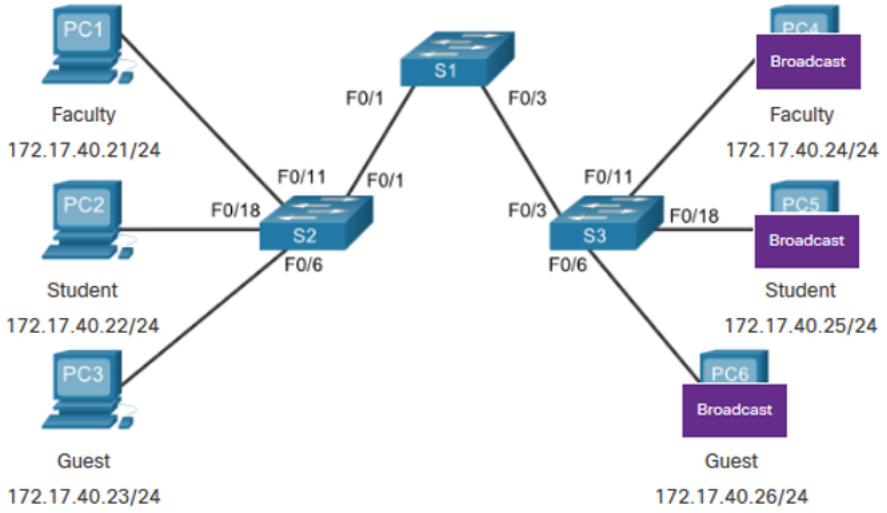


O QUE SÃO VLANS?

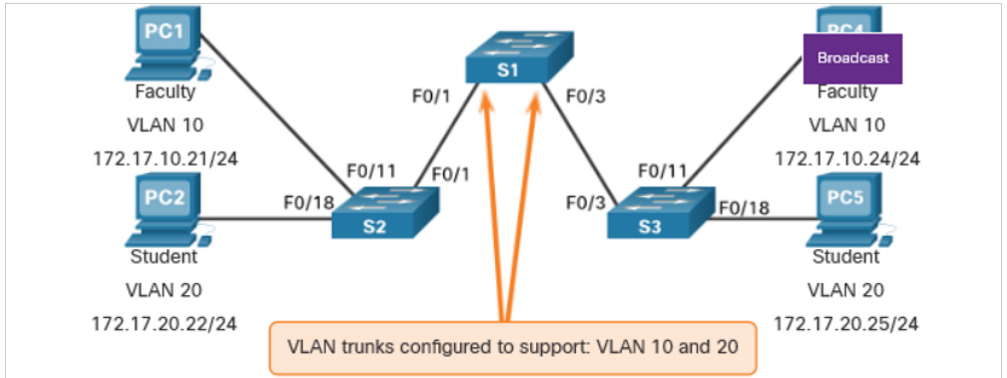


- VLANs (redes locais virtuais) são conexões lógicas entre dispositivos semelhantes.
- Segmentação de diferentes grupos de dispositivos em um mesmo switch.
- Fornece uma organização mais gerenciável.
- Transmissões unicast, multicast e broadcast são isoladas dentro da VLAN.

VLANS EM UM AMBIENTE COM MÚLTIPLOS SWITCHES



PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame out all available ports.



PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame only out ports configured for VLAN10.

TIPOS DE VLANS

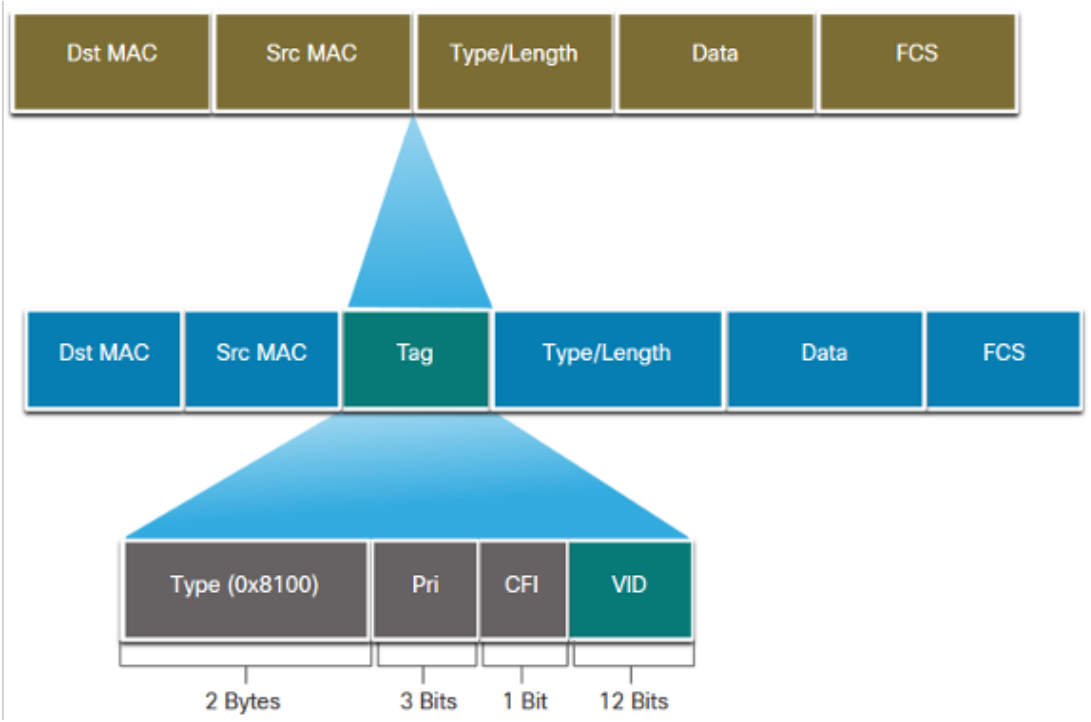
- VLAN de dados (padrão)
- VLAN nativa.
- VLAN de gerenciamento.
- VLAN de voz.
- Por padrão, a VLAN 1 é a padrão, nativa e de gerenciamento (e isso é péssimo).

```
Switch# show vlan brief
VLAN Name                Status    Ports
---- ------------------- --------  -------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                   Gi0/1, Gi0/2
1002 fddi-default                       act/unsup
1003 token-ring-default                 act/unsup
1004 fddinet-default                    act/unsup
1005 trnet-default                      act/unsup
```

COMO IDENTIFICAR UMA VLAN?

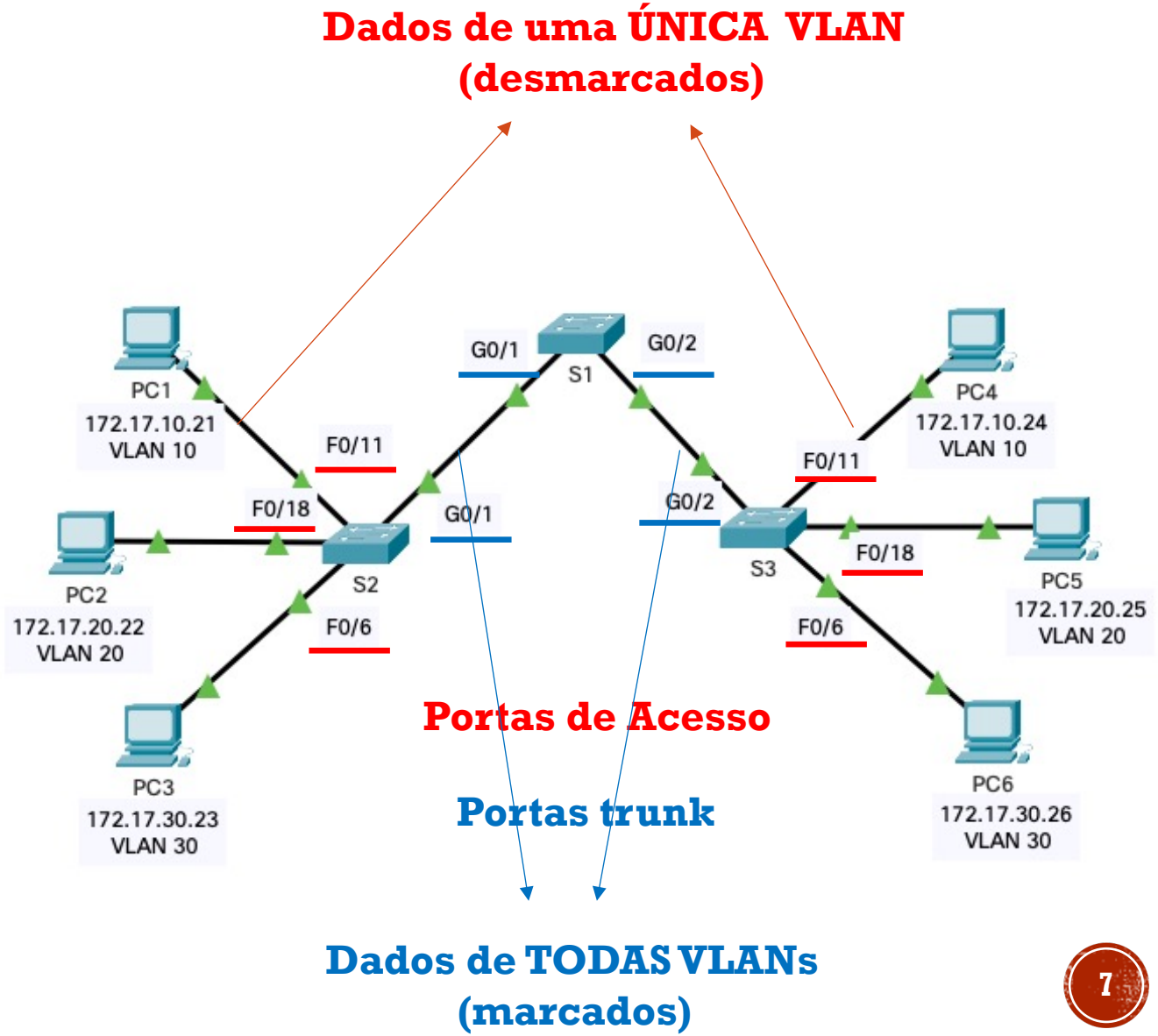
- Identificação: Tag ~ marcação.

- IEEE 802.1Q* (4 Bytes) é um protocolo de marcação (taggeamento).



PORTAS DE ACESSO E TRUNK

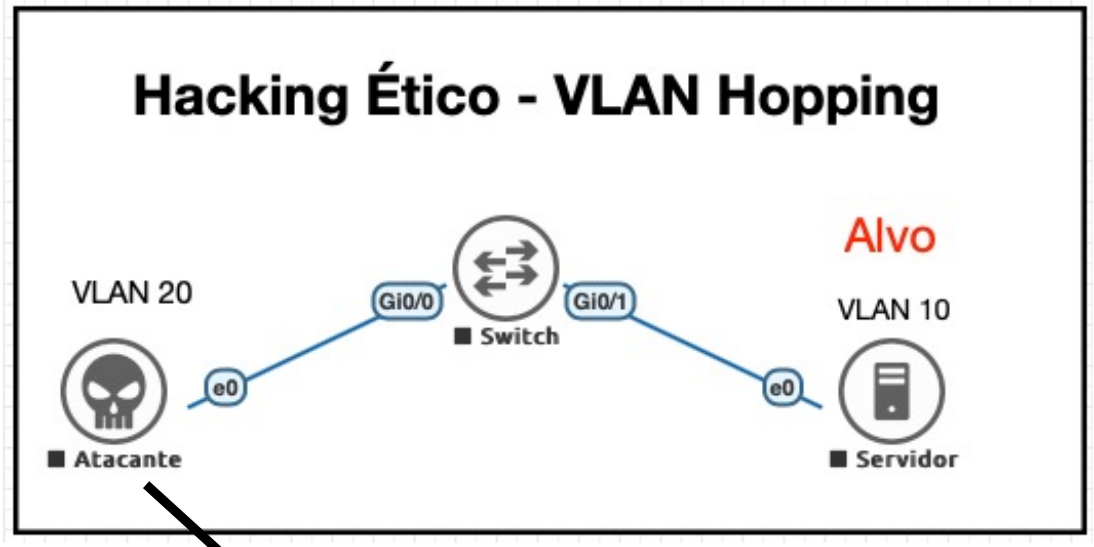
- **Portas de acesso** conectam dispositivos finais (exemplo: PCS) aos switches.
- **Portas de acesso** pertencem a uma **única** VLAN.
- **Portas trunk** (tronco) conectam dispositivos de rede (switches) entre si.
- **Portas trunk** pertencem a **todas** VLANs.



RESUMINDO...

ATAQUE: SALTO DE VLAN (VLAN HOPPING)

- Objetivo deste ataque é gerar links trunk entre dispositivos finais e dispositivos intermediários.
- Uma vez gerado o link trunk indevido, o atacante tem acesso a dados de todas as VLANs.
- Por padrão, as portas de um switch vem com a negociação de links trunk configurados no modo dinâmico (protocolo DTP* habilitado).

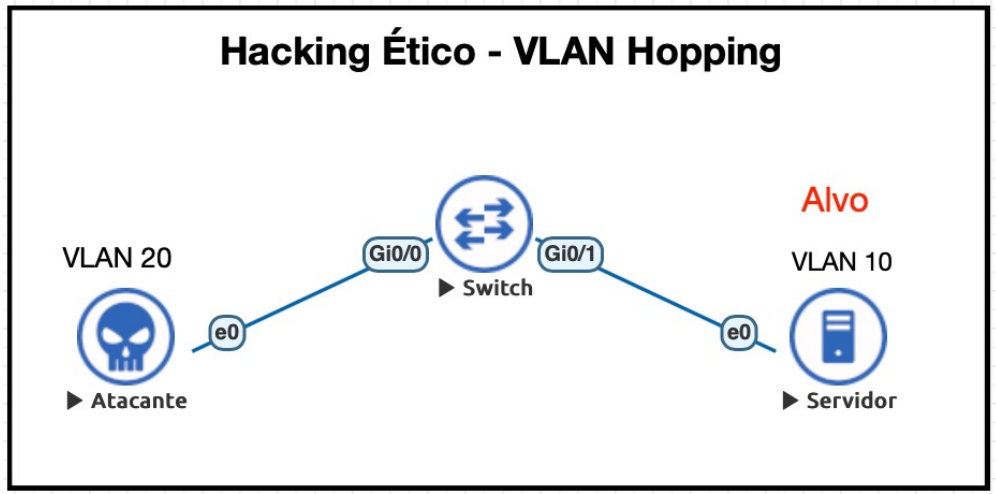


"Se o DTP estiver habilitado na porta Gi0/0, vou tentar gerar um trunk e acessar dados da vlan do servidor"

*Dynamic Trunk Protocol

VAMOS PARA PRÁTICA?

Emulated Virtual Environment
Next Generation



Prof. Mario Lemes (IFG Campus Formosa)

CONTRA-MEDIDAS AO ATAQUE DE SALTO DE VLAN

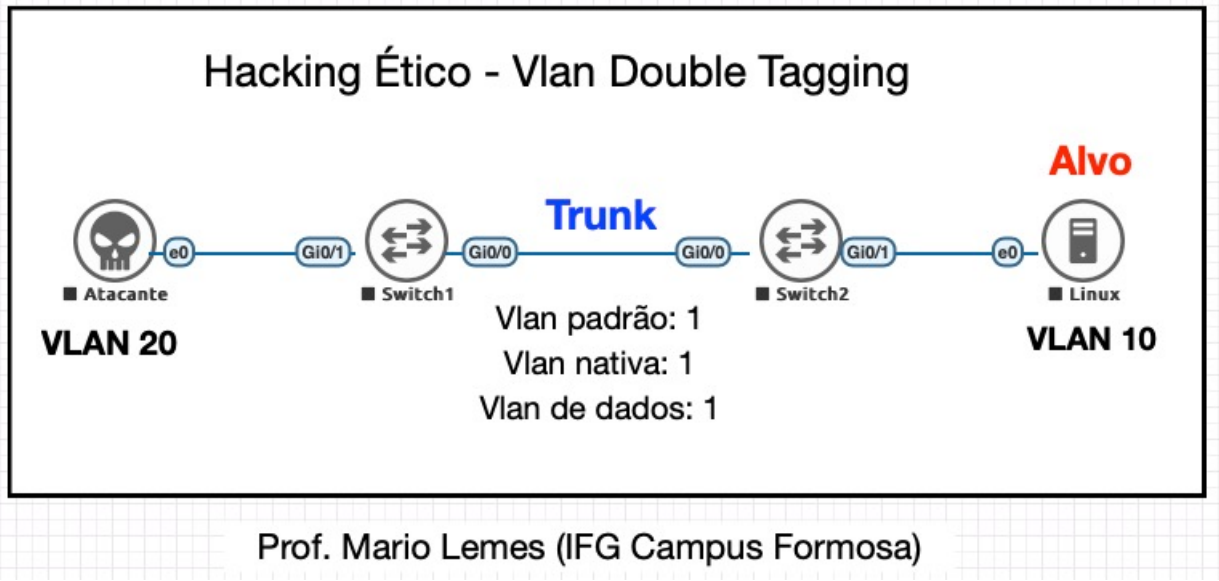
- Configurar TODAS portas de acesso manualmente.
- Desabilitar o DTP.
- Portas não usadas devem ser desligadas (administrativamente) e retiradas da VLAN padrão para uma outra VLAN qualquer (VLAN inutilizada)

ATAQUE: MARCAÇÃO DUPLA DE VLAN (VLAN DOUBLE TAGGING)

- Este ataque consiste na marcação dupla de VLAN no qual um atacante forja quadros Ethernet (duplamente marcados) e os insere na rede.

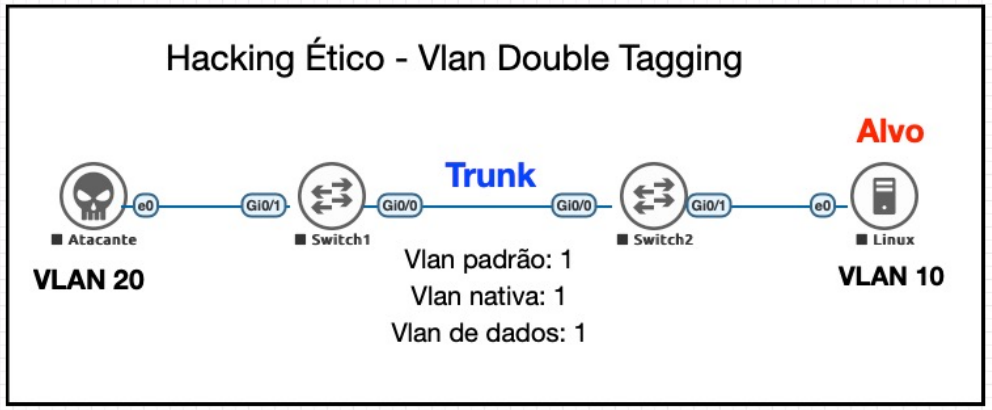
- O atacante marca o quadro mais externo usando a VLAN nativa 1 (explorando a vulnerabilidade de a VLAN nativa ser igual a VLAN padrão). Na parte interna, o atacante marca novamente o quadro Ethernet com a identificação da VLAN alvo.

- O quadro duplamente marcado chega no Switch que retira a marcação mais externa (VLAN nativa), mantendo a marcação mais interna destinada ao alvo.



VAMOS PARA PRÁTICA?

Emulated Virtual Environment
Next Generation



Prof. Mario Lemes (IFG Campus Formosa)

CONTRA-MEDIDAS AO ATAQUE DE DUPLA MARCAÇÃO DE VLAN

- Criar uma VLAN inutilizada e jogar todas as portas do Switch para essa vlan, colocar que são portas de acesso e desliga-las.
- Criar uma vlan nativa DIFERENTE da 1 para que o tráfego no tronco não utilize a VLAN padrão 1.
- Criar VLANs para as portas de acesso e associa-las o acesso a VLAN criada.
- Configurar as portas trunk: i) modo trunk, ii) não negociando trunk, iii) mudando o tráfego da vlan nativa, iv) dizendo que o trunk usa o método de encapsulamento dot1q. Lembrar de ligar as portas (pois anteriormente a desligamos).

DÚVIDAS?

QUESTIONAMENTOS?

COMENTÁRIOS?

OBRIGADO PELA PARTICIPAÇÃO!

- Prof. Mario Lemes (IFG – Campus Formosa)

- Contato: mario.lemes@ifg.edu.br
- Youtube: http://www.youtube.com/c/MarioTeixeiraLemes?sub_confirmation=1
- Currículo lattes: http://lattes.cnpq.br/4918126641251231
- Site pessoal: https://mariotlemes.github.io
- Slides: https://url.gratis/jknS9T