HACKING ÉTICO: COMO ATACAR/DEFENDER UM SERVIDOR DHCP?

INSTITUTO FEDERAL
Goiás
Câmpus Formosa

SECITEC
SEMANA DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Prof. Mario Lemes

10/12/2021 (09:00 às 10:00)

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 um sistema.

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

SOBRE O PROFESSOR

- Mestre em Ciência da Computação.
- Especialista em Sistemas de Informação.
- Bacharel em Engenharia de Computação.
- Instrutor CCNA (Cisco Certified Network Associate) pela academia Cisco IFG – Campus Formosa.
- Certificado pela Huawei Certified ICT Associate 5G e fundador da Academia Huawei no IFG – Campus Formosa.
- Professor DE do IFG Campus Formosa com atuação nas seguintes áreas: Redes de Computadores, Sistemas Distribuídos, Segurança da Informação, Telecomunicações, Software/Hardware livre e Internet das Coisas.

ENDEREÇO IP: COMO CONSEGUIR UM?

Atualmente existem duas questões relacionadas a obtenção de endereçamento IP:

1. Q: Como um host (dispositivo final) consegue um endereço IP dentro da sua propria rede?
2. Q: Como uma rede consegue um endereço IP para si mesma?

Como um host consegue um endereço IP?

- configuração manual do adminstrador da rede (e.g., /etc/rc.config in UNIX)
- DHCP: Dynamic Host Configuration Protocol: dinamicamente recebe um endereço IP do servidor.
  - “plug-and-play”

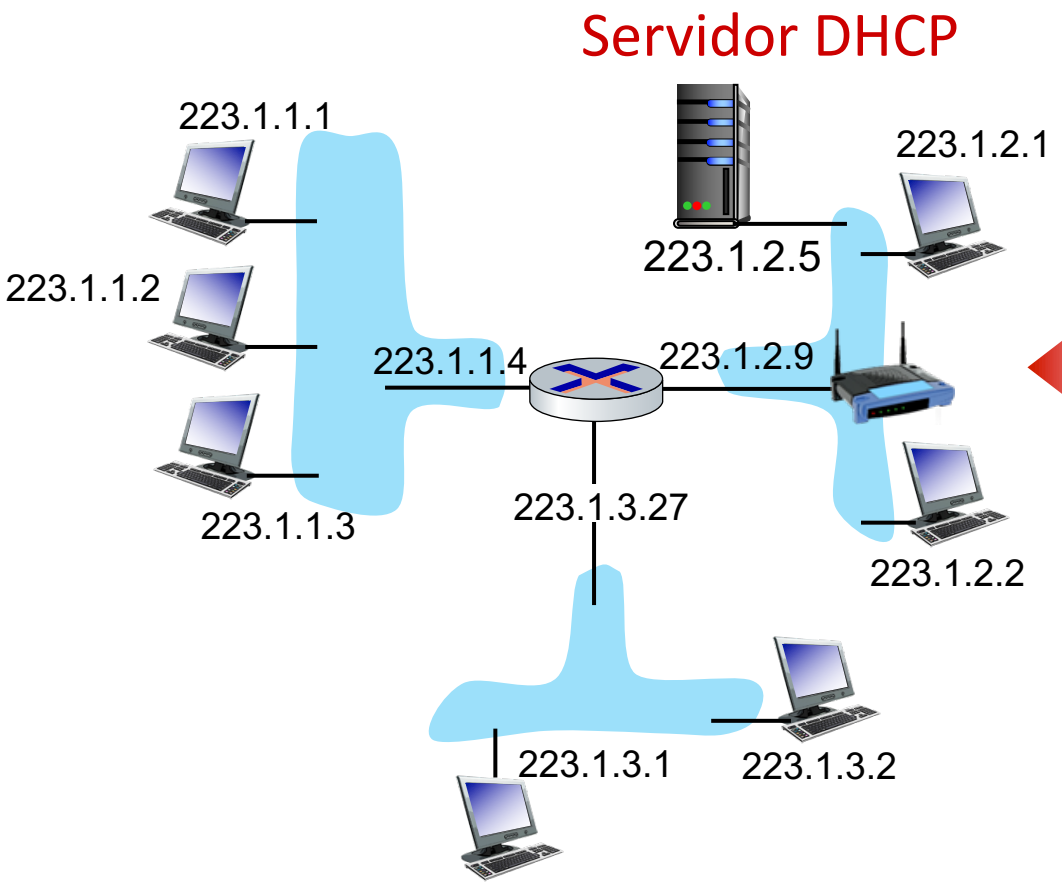
DHCP: DYNAMIC HOST CONFIGURATION PROTOCOL

objetivo: computador (*host*) dinamicamente obtém um endereço IP a partir do servidor DHCP quando ele ingressa na rede.

Visão geral do DHCP:

- Computador envia uma mensagem *DHCP discover*, em broadcast.
- Servidor DHCP responde com *DHCP offer*.
- Computador faz uma requisição: mensagem *DHCP request*.
- DHCP envia endereços IP com a mensagem: *DHCP ack*.

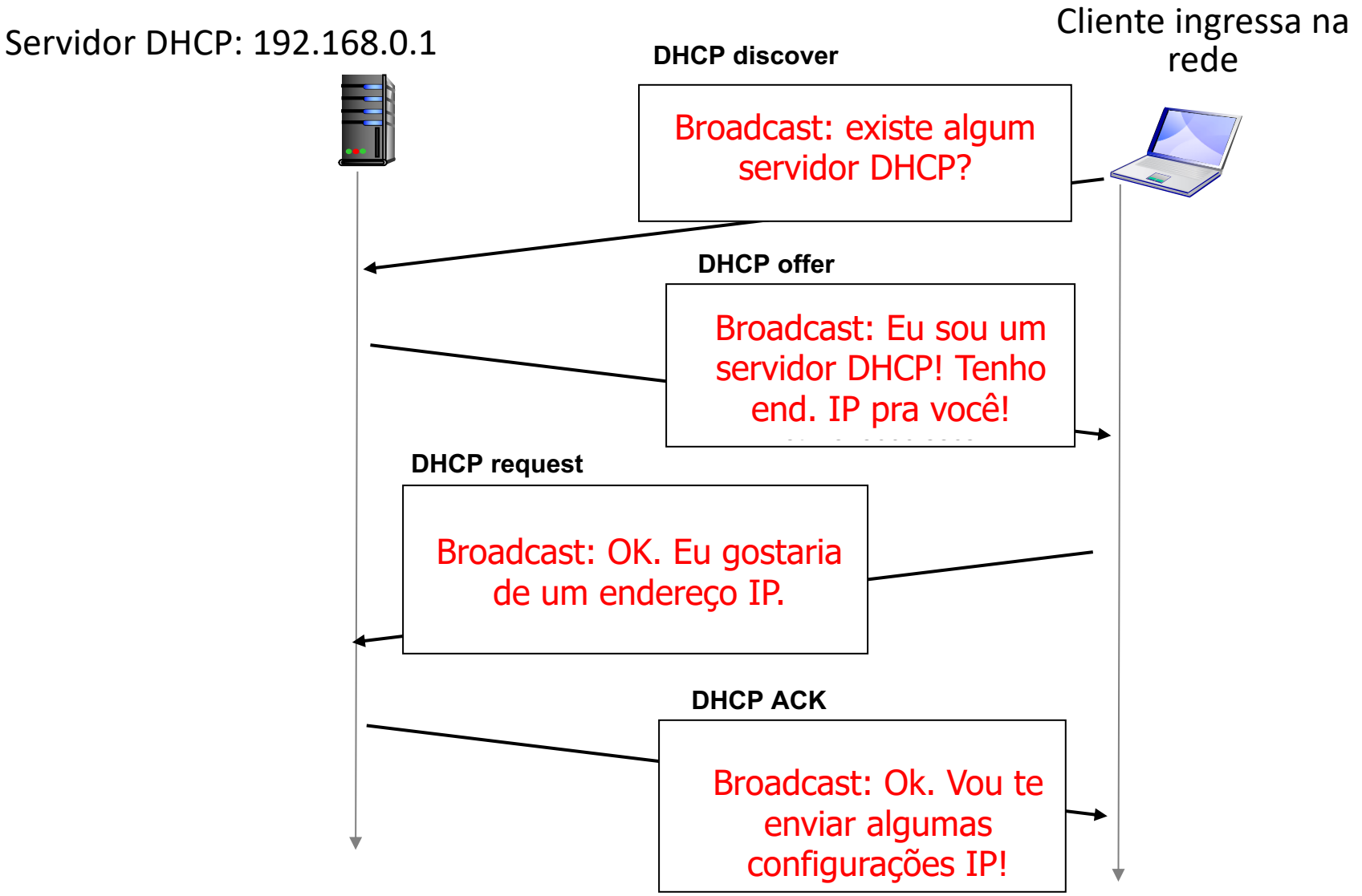
SERVIDOR DHCP: ARQUITETURA CLIENTE-SERVIDOR



Tipicamente, um servidor DHCP é co-localizado dentro de um roteador, servindo as sub-redes a ele conectadas.

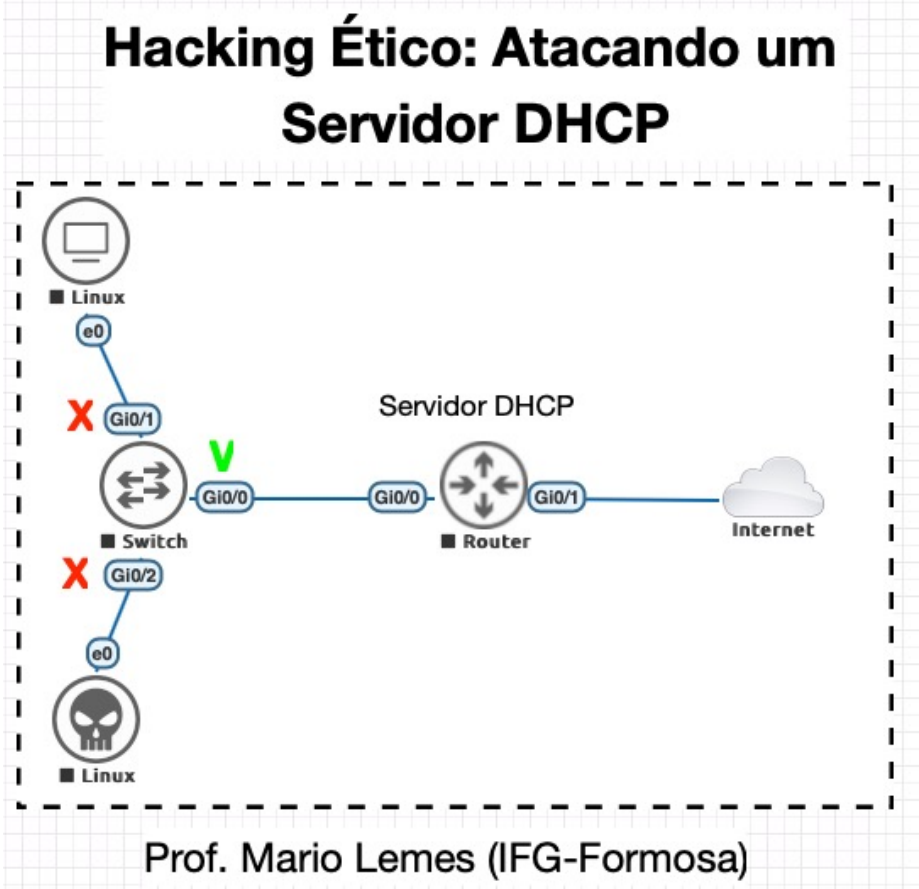
Host ingressa na rede e necessita de um endereçamento IP

SERVIDOR DHCP – ARQUITETURA CLIENTE-SERVIDOR



VAMOS PARA PRÁTICA?

Emulated Virtual Environment
Next Generation



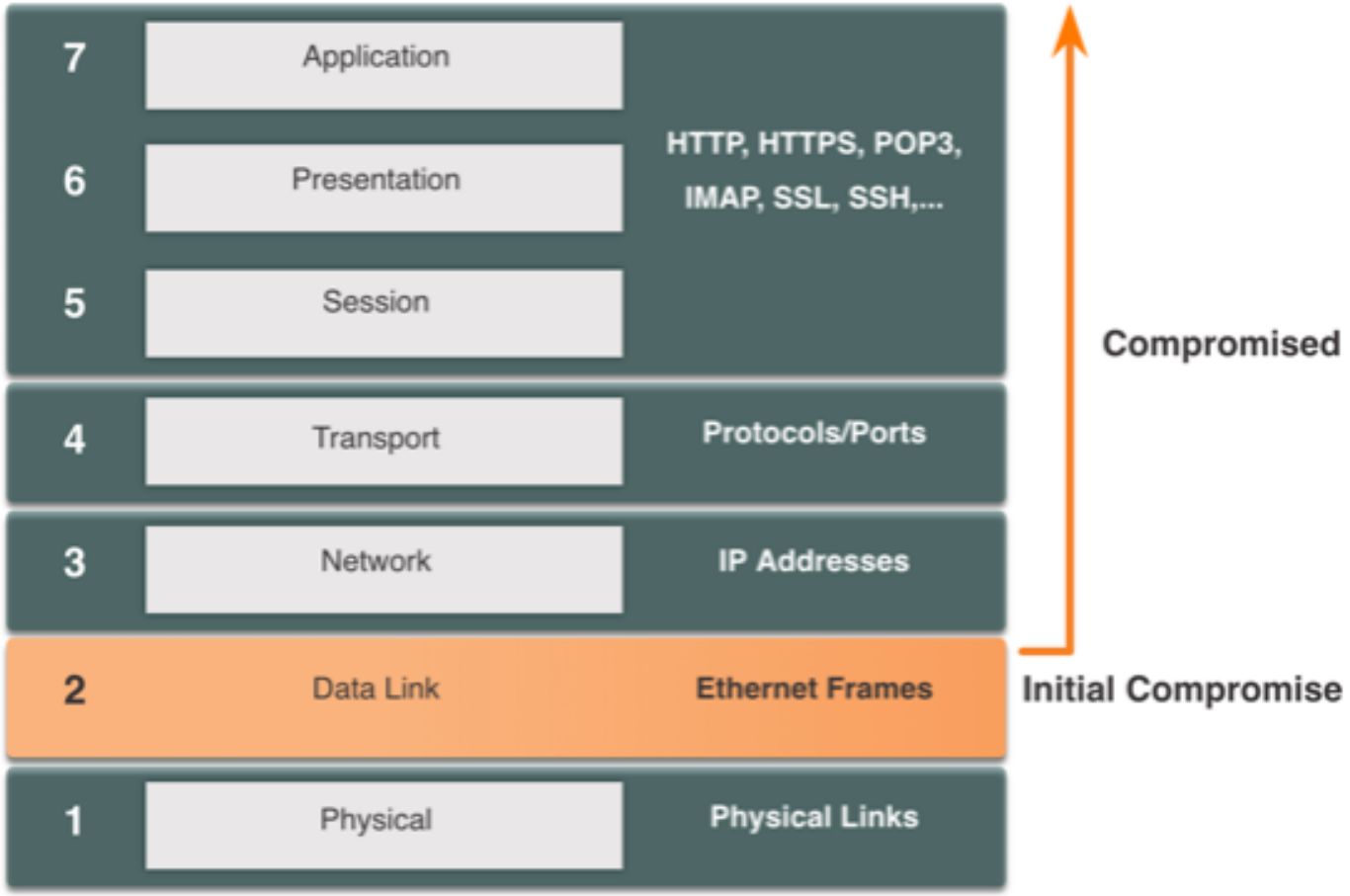
CONTRA-MEDIDAS AO ATAQUE DE NEGAÇÃO DE SERVIÇO (DOS) NO SERVIDOR DHCP

- No dispositivo de camada 2 (Switch) devemos ativar o **DHCP Snooping**.

- Dizer explicitamente qual porta do Switch é confiável (ip dhcp snooping trust). Somente a porta do Switch que se conecta ao Roteador é confiável.

- Dizer explicitamente qual(is) porta(s) do Switch não é(são) confiável(is). Todas portas de acesso devem ser colocadas como não confiáveis.

POR QUE SEGURANÇA DA CAMADA L2?



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://drive.google.com/file/d/10coGHWtv1BNXDBxDQmhlQno8ZAE2NTPr/view?usp=sharing