

UNIVERSIDADE CATÓLICA DE PELOTAS  
ENGENHARIA DE COMPUTAÇÃO  
REDES DE COMPUTADORES

# Ataques Cibernéticos

Manipulação de URLs, DoS, DDoS e Eavesdropping

MATHEUS GONÇALVES STIGGER

# Introdução

---

- Em um intervalo de apenas 3 meses, entre março e junho de 2019, o Brasil sofreu 15 bilhões de tentativas de ataques cibernéticos.



# Manipulação de URL

---

- O ataque por manipulação de URL é usado por alguns hackers para fazer o servidor transmitir páginas às quais ele não teria autorização de acesso.
- Se o usuário alterar manualmente a URL, ele pode testar diversas combinações para chegar a um endereço que esconde uma área restrita.

# Manipulação de URL

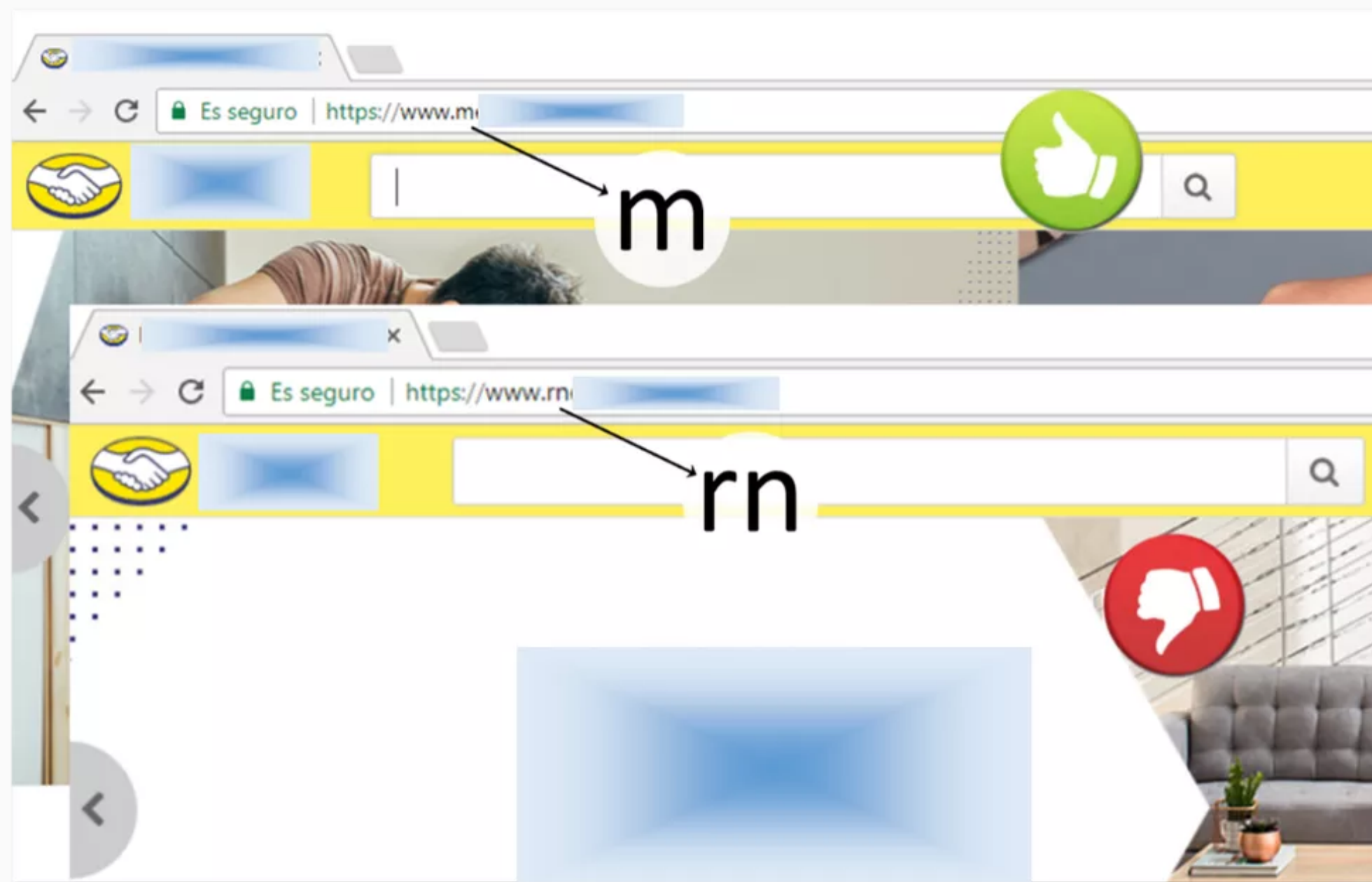
---

- O ataque por manipulação de URL é bem comum. Ele faz com que o servidor local consiga transmitir páginas às quais ele não poderia ter acesso, devido a restrições de segurança.
- Há casos mais simples em que registram um domínio o mais similar possível como "twiitter.com" — com dois "i" — em vez de "twitter.com".

# Manipulação de URL

---

5



Versão falsa do site MercadoLivre com letras trocadas – Foto: Reprodução/ESET



# Ataque DoS e DDoS

---

6

- Os tipos DoS e DDoS, têm o objetivo apenas de sobrecarregar os servidores ou “derrubá-los”, deixando-os inativos temporariamente.



# Ataque DoS

---

7

- O ataque do tipo DoS (Denial Of Service, em inglês), também conhecido como ataque de negação de serviço, é uma tentativa de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores.



# Ataque DoS

---

8

- O primeiro caso documentado de Ataque de Negação de Serviço foi em fevereiro do ano 2000 quando um hacker Canadense de 15 anos de idade atacou de forma eficaz os servidores da Amazon e eBay.
- Alguns ataques de Negação de Serviço buscam atrapalhar o acesso de pessoas específicas às suas redes ou banco de dados, enquanto outros tentam tornar esses recursos totalmente inacessíveis.

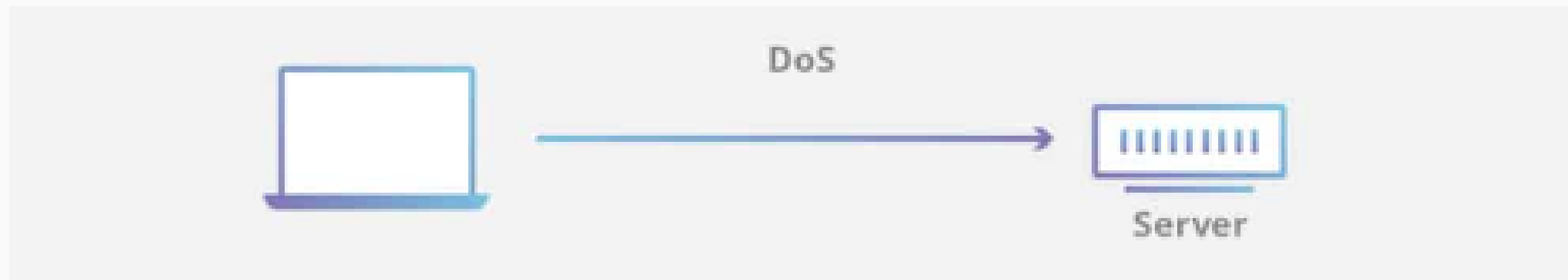




# Ataque DoS

---

- Para isso, o invasor utiliza meios para enviar diversos pedidos de pacotes para o alvo, com a finalidade de que este fique tão sobrecarregado que não consiga mais responder a nenhuma requisição.



# Ataque DDoS

---

IO

- Já no ataque distribuído de negação de serviço, conhecido como DDoS (Distributed Denial of Service, em inglês), o ataque acontece de forma similar ao DoS, porém, ele ganha algumas camadas extras. Nele, um computador mestre pode gerenciar uma série de outros computadores, que são chamados de zumbis.



# Ataque DDoS

---

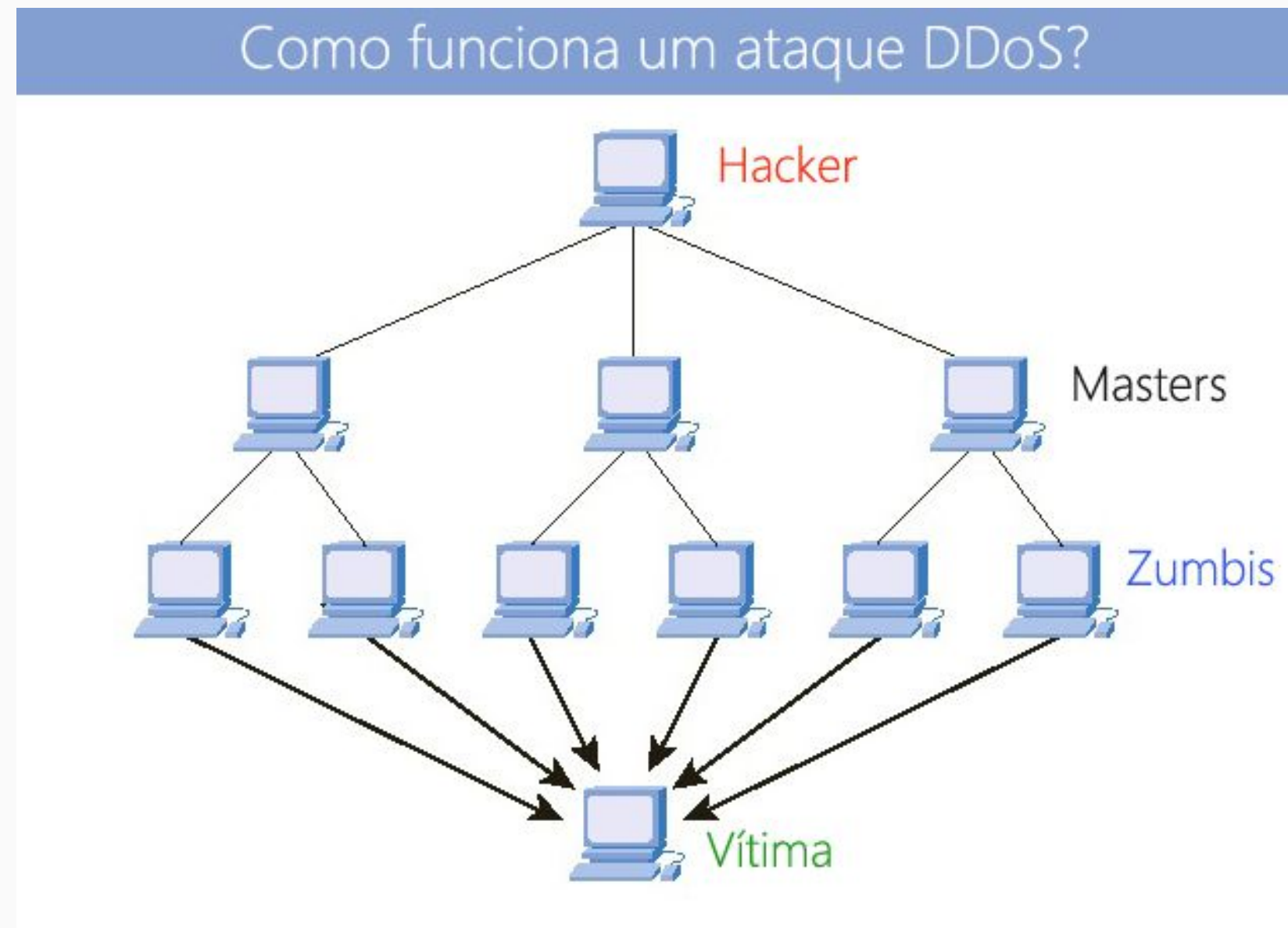
II

- Por meio do DDoS, o hacker ou cracker invade um computador mestre e este, por sua vez, escraviza várias máquinas, fazendo com que elas passem a acessar um determinado recurso em um servidor todos ao mesmo tempo. Assim, todos os zumbis acessam juntamente e de maneira ininterrupta o mesmo recurso de um servidor, tentando sobrecarregá-lo.



# Ataque DDoS

I2



Estrutura de um ataque de DDoS – Imagem: Canaltech



# Eavesdropping

---

I3

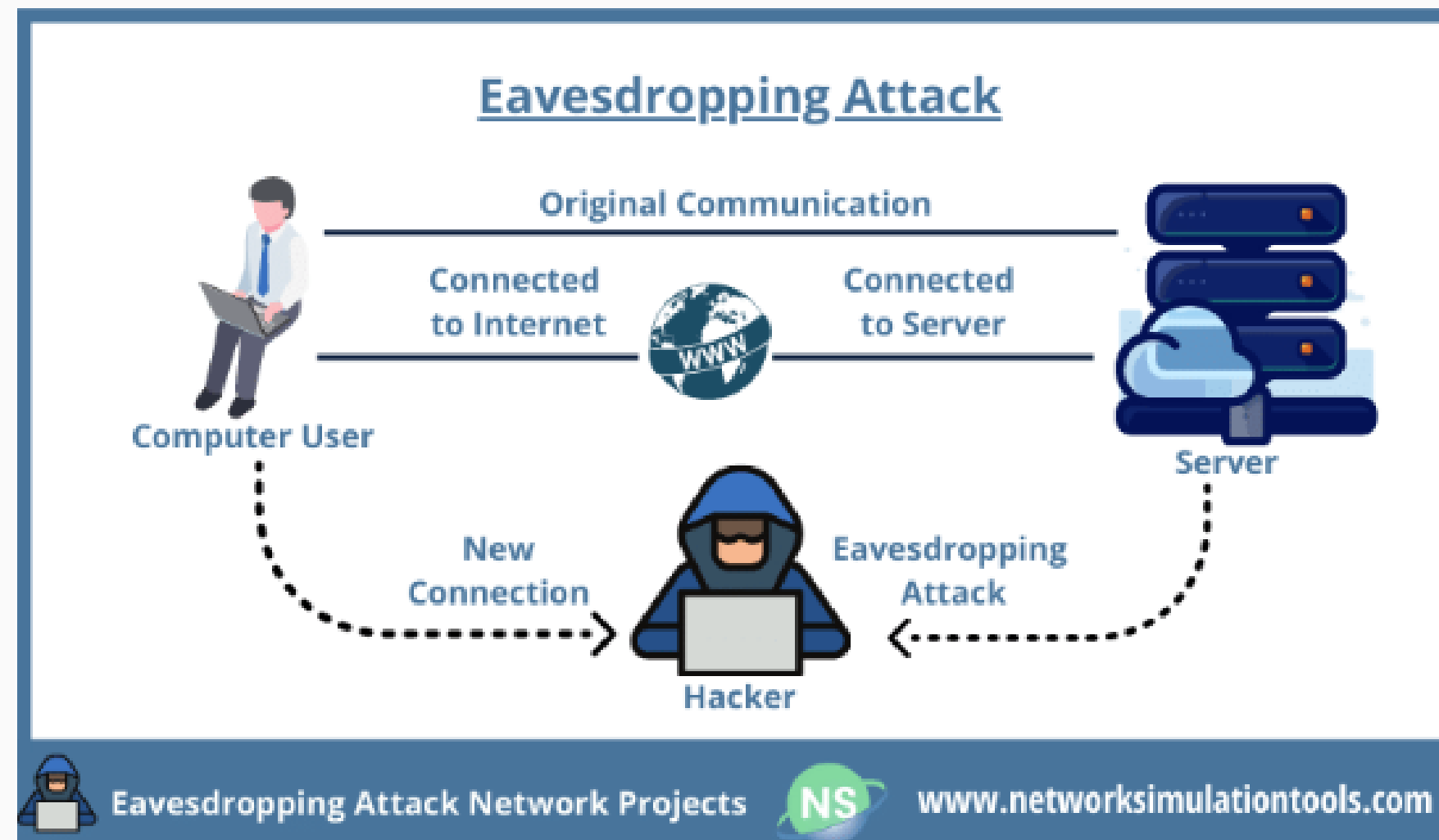
- No ataque Eavesdropping, o hacker utiliza diferentes sistemas de e-mail, mensagens instantâneas e telefonia, além de serviços de internet, para violar a confidencialidade da vítima, roubando seus dados para usá-los de forma indevida posteriormente.



# Eavesdropping

I4

- Em conexões não encriptadas, ou encriptadas usando algoritmos fracos, é possível que um atacante consiga capturar os dados transmitidos através da rede caso tenha acesso à mídia de transmissão.



# Obrigado!

---



UNIVERSIDADE CATÓLICA DE PELOTAS  
ENGENHARIA DE COMPUTAÇÃO  
REDES DE COMPUTADORES

# Ataques Cibernéticos

Manipulação de URLs, DoS, DDoS e Eavesdropping

MATHEUS GONÇALVES STIGGER