Programação para Redes de Computadores

EP 4 – Socket L2TP

CVE-2014-4943

Alunos: Evandro Fernandes Giovanini

Leonardo Pereira Macedo

Professor: Daniel Macêdo Batista

Vulnerabilidade

CVE-2014-4943

- *The PPPoL2TP feature in net/l2tp/l2tp_ppp.c in the Linux kernel through 3.15.6 allows local users to gain privileges by leveraging data-structure differences between an l2tp socket and an inet socket*
- *CVSS v2 Base Score: 6.9 (MEDIUM)*
- Reportado por Sasha Levin, da Oracle

Sockets

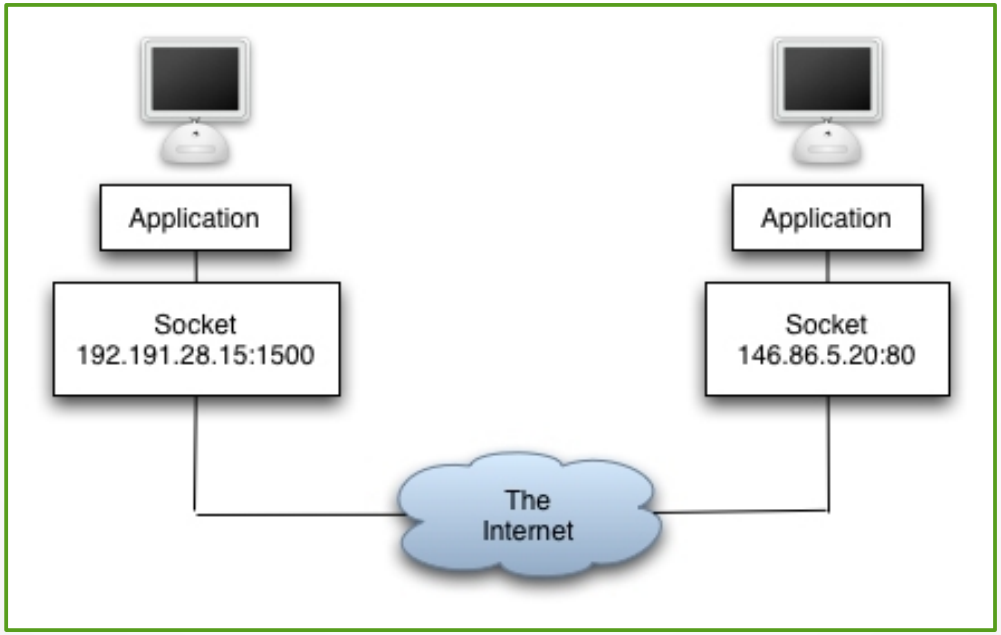
Conceito

- “Porta” para comunicação entre dois programas
- Processo de envio “empurra” a mensagem para fora da “porta”

Sockets

Sockets de Rede

- Comunicação entre sockets é feita através de uma rede
- Tipo mais comum são sockets de Internet, que possuem:
  - Endereço local: endereço IP local + porta
  - Protocolo da camada de transporte (TCP, UDP, etc.)

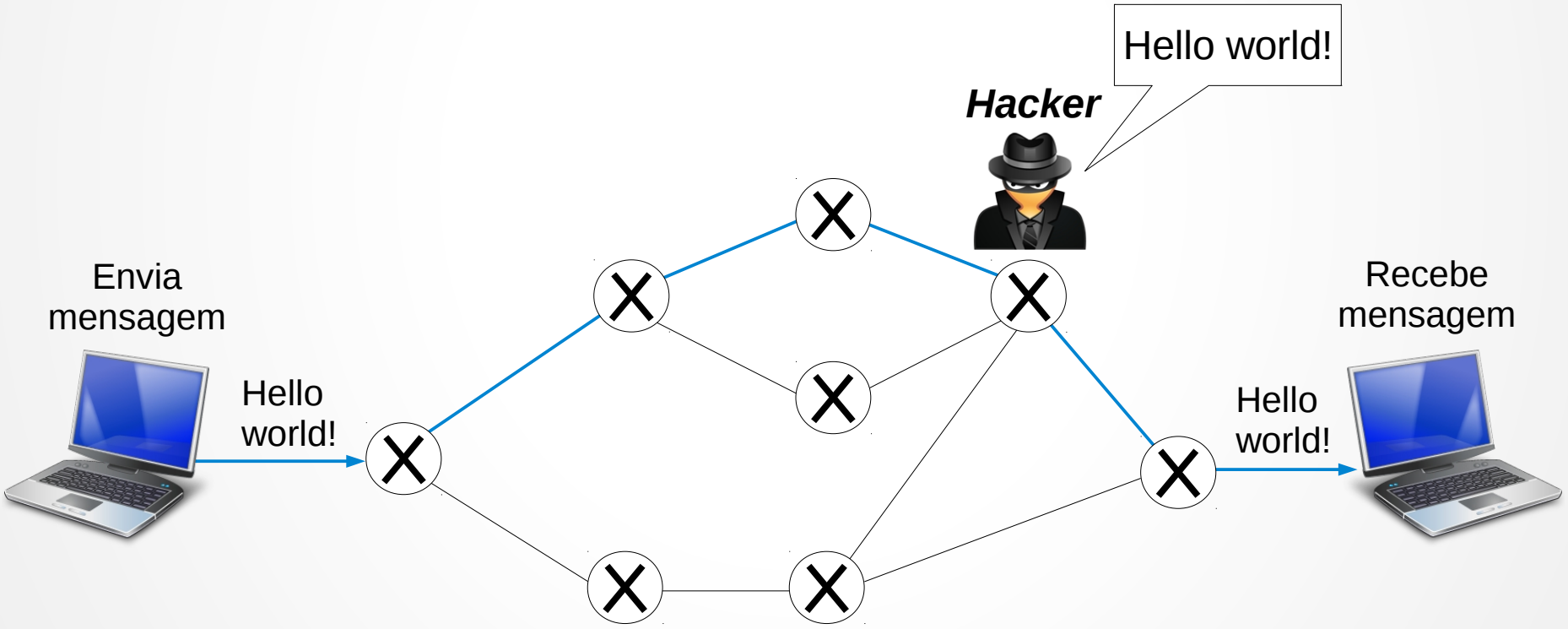


Fonte:
http://www.vertexinfosolution.com

Sockets

Transmissão Normal

- Dados podem ser interceptados



Fontes: https://cert.eccouncil.org
http://www.fordesigner.com

VPN

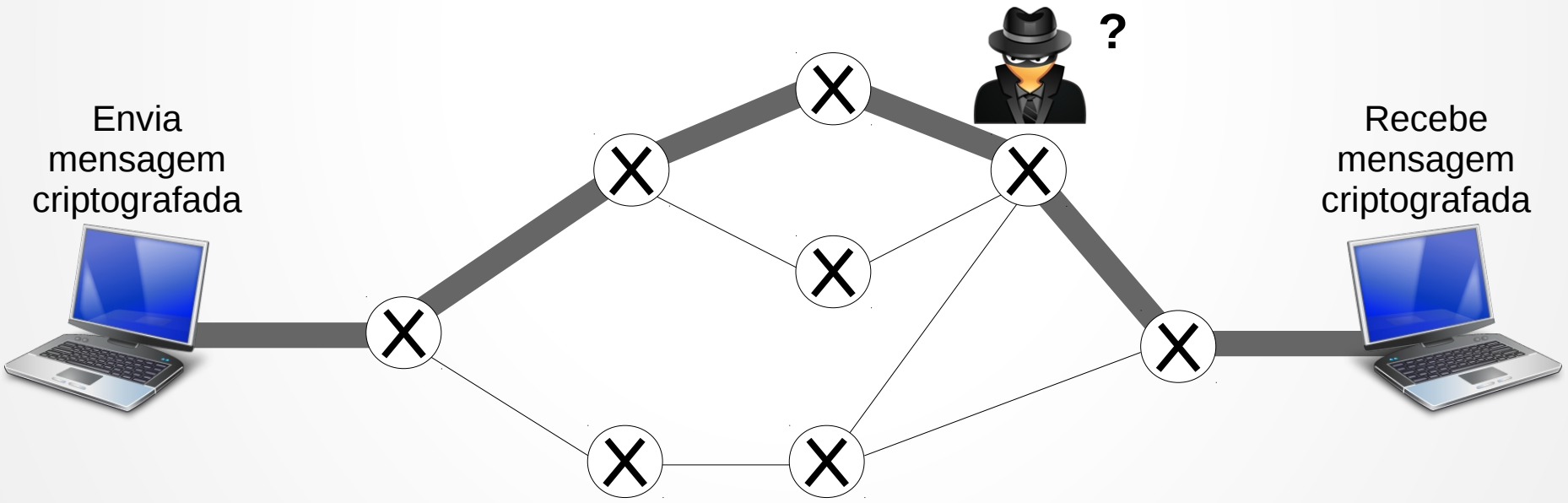
Informações Gerais

- Sigla para *Virtual Private Network*
- Compartilhamento de dados remotamente por rede públicas
- Emula conexão ponto a ponto em uma rede privada
- Protocolos de encapsulamento (PPTP, L2TP)
- Protocolos para criptografia (SSL, TLS)

VPN

Transmissão em uma VPN

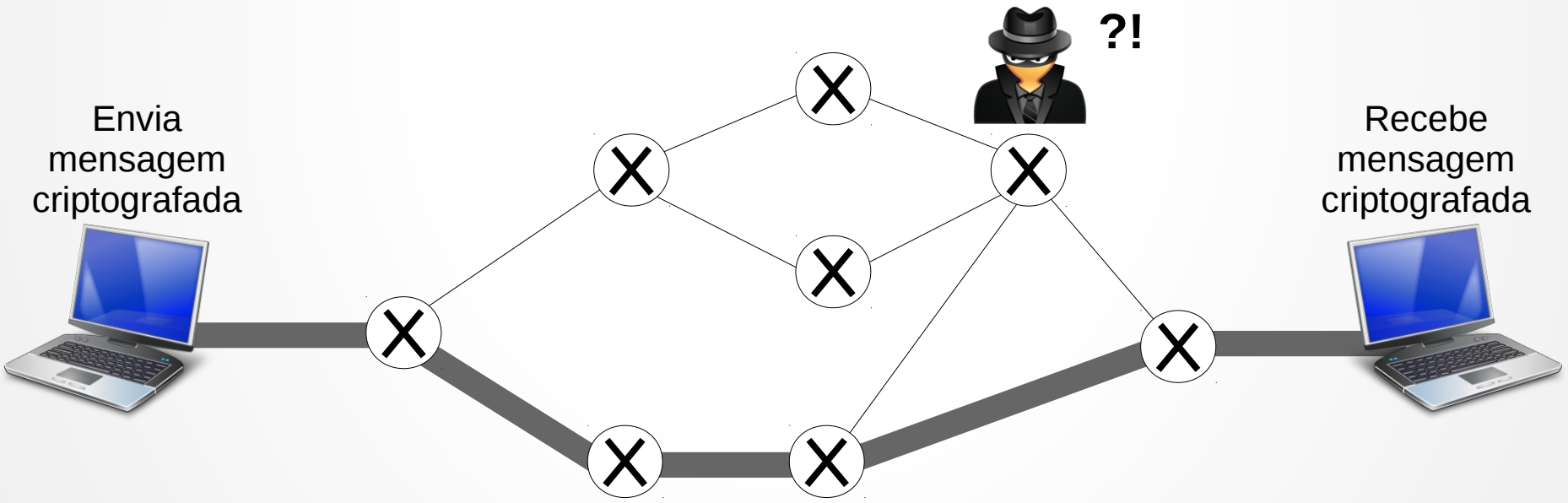
- Dados criptografados
- Criação de um túnel (camada para proteger os dados)



VPN

Transmissão em uma VPN

- Túnel é recriado numa rota diferente se um dos lados perceber uma demora na recepção dos dados



PPP

Informações Gerais

- Sigla para *Point-to-Point Protocol*
- Protocolo da camada de enlace, mas também age em outras camadas, como a de rede
- Estabelece conexão direta entre dois nós
- É o padrão principal para acesso remoto
- Possui suporte para métodos de autenticação

L2TP

Informações Gerais

- Sigla para *Layer Two Tunneling Protocol*
- Protocolo da camada de enlace
- Responsável por encapsular dados do PPP
- Enviado em um datagrama UDP

Estrutura de Sockets

socket( )

```
int socket(int domain, int type, int protocol)
```

AF_INET

```
tcp_socket = socket(AF_INET, SOCK_STREAM, 0);

udp_socket = socket(AF_INET, SOCK_DGRAM, 0);
```

AF_PPPOX

```
l2tp_socket = socket(AF_PPPOX, SOCK_DGRAM,
                     PX_PROTO_OL2TP);
```

Estrutura de Sockets

setsockopt( )

```
int setsockopt(int sockfd, int level, int optname,
               const void * optval, socklen_t optlen)
```

Explorando a Vulnerabilidade

Etapas

- Código vulnerável do kernel
- Exploit (código e execução)
- Patch (código e aplicação)
- Falha no exploit