STREAM SERIES

devnator

Comparação de Segurança

Protocolos SSH Versus Telnet

SERGIO CABRAL

sergiocabral.com

Índice

Objetivo prático desta demonstração

Verificar com um analisador de pacotes de redes (um sniffer) a criptografia presente via SSH e ausente via Telnet. Justificar o uso do protocolo SSH sempre que possível ao invés do protocolo Telnet.

1. Analisando pacotes Telnet

Porque todo mundo usa SSH ao invés de Telnet? — SSH e Telnet são dois protocolos que se destinam ao mesmo objetivo, isto é, acessar um servidor para executar operações nesse sistema remoto. Mas a principal diferença entre ambos é a criptografia.

Uma definição simples para criptografia é a capacidade de tornar uma mensagem ilegível e apenas alguém com a chave de reversão poderia ler o conteúdo original.

Se uma mensagem não criptografada trafega por uma rede, qualquer um que a intercepte consegue ler seu conteúdo. Usando um analisador de pacotes de rede, que também é conhecido como Sniffer, podemos demonstrar isso. Como exemplo podemos usar o Wireshark, na *Figura 1*, e ver os pacotes de rede trafegando tanto numa conexão SSH como também numa conexão Telnet.

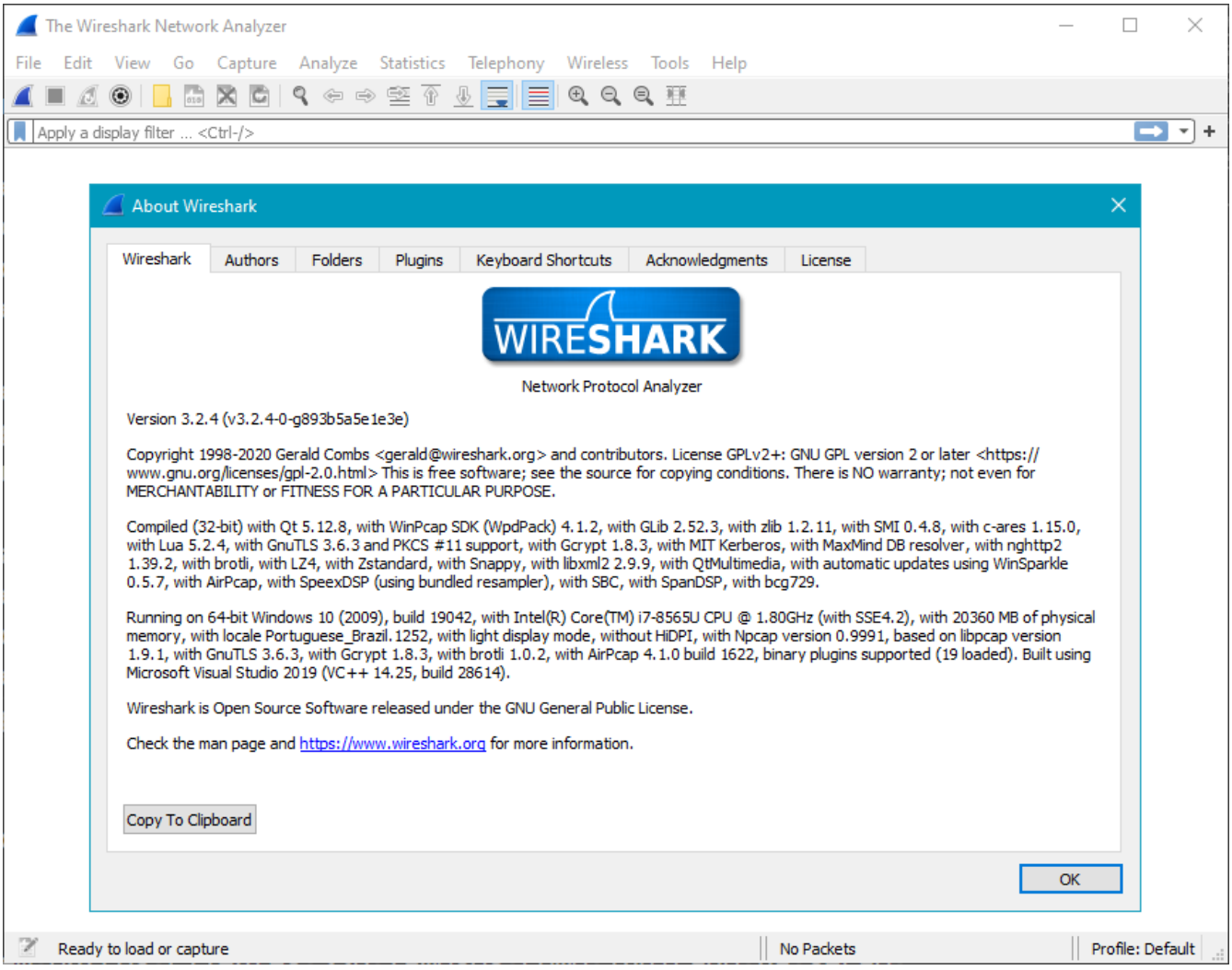


Figura 1. Aplicativo Wireshark

Veja outras alternativas ao Wireshark na seção Opções de sniffers de rede.

Precisamos conferir qual é o IP do servidor e pedir para o Wireshark filtrar os pacotes endereçados a esse IP usando a sintaxe `ip.dst == 191.235.98.138`. Agora só vão ser exibidos pacotes de rede dessa conexão Telnet.

Para o teste podemos informar o usuário na conexão telnet e pressionar `Enter`. Então limpamos o

histórico do Wireshark e poderemos ver a partir daqui que para cada tecla digitada é enviado um pacote de rede expondo o que você digita.

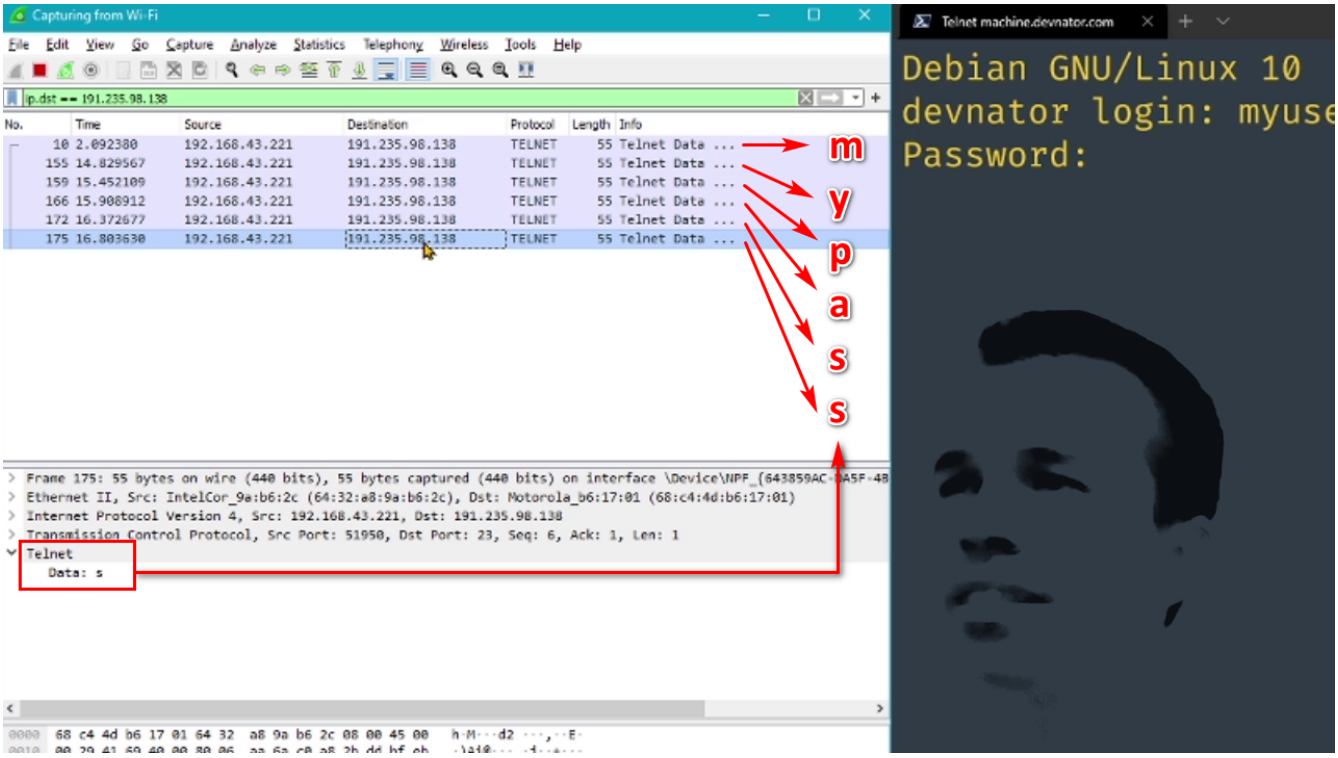


Figura 2. Pacotes Telnet com exposição dos dados digitados

Como mostra a *Figura 2*, sendo a minha senha é “mypass” e eu consigo ver cada letra sendo enviada pelos pacotes de rede: “m”, ”y”, ”p”, ”a”, ”s”, ”s”.

Ao prosseguir com a conexão e enviar comandos vemos os pacotes de rede trafegando com os dados abertos para leitura, sem usar criptografia.

2. Analisando pacotes SSH

Fazemos agora a conexão usando o protocolo SSH. Diferente do Telnet, que após estabelecer a conexão precisa receber via teclado o nome do usuário, o SSH já envia essa informação junto com o endereço do computador remoto no momento da conexão. Então você informa via teclado apenas a senha.

Sendo o mesmo computador remoto, vamos continuar usando o filtro por IP aplicado no Wireshark mas limpamos o histórico antes de digitar a senha. Você vai reparar que para cada tecla digitada não é enviado um pacote de rede. Ele só será enviado quando terminar de digitar a senha e pressionar `Enter`. E mesmo assim o pacote será enviado de forma criptografada.

Após o login o protocolo SSH também envia um pacote de rede para cada tecla digitada, assim como faz o Telnet. Mas esses pacotes ficam criptografados, não são legíveis, como indicado em amarelo na *Figura 3*.

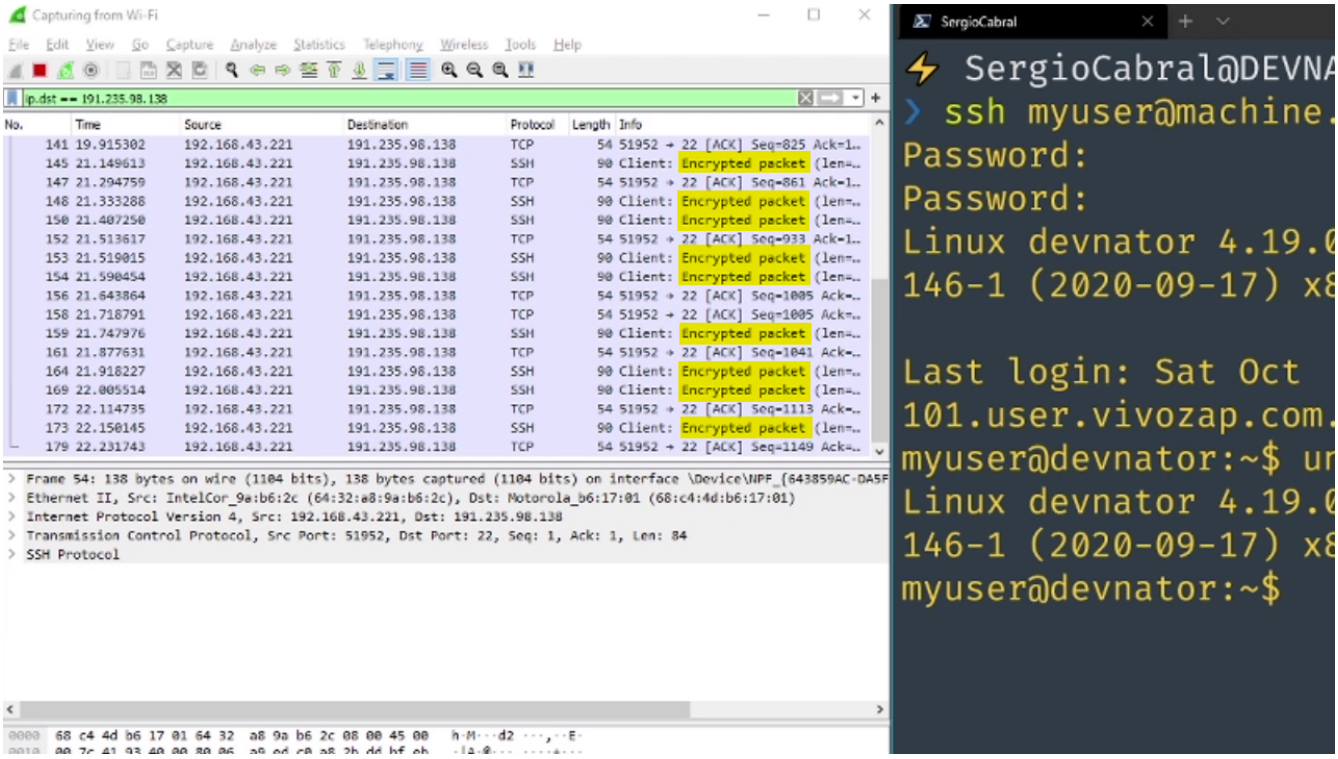


Figura 3. Pacotes SSH criptografados

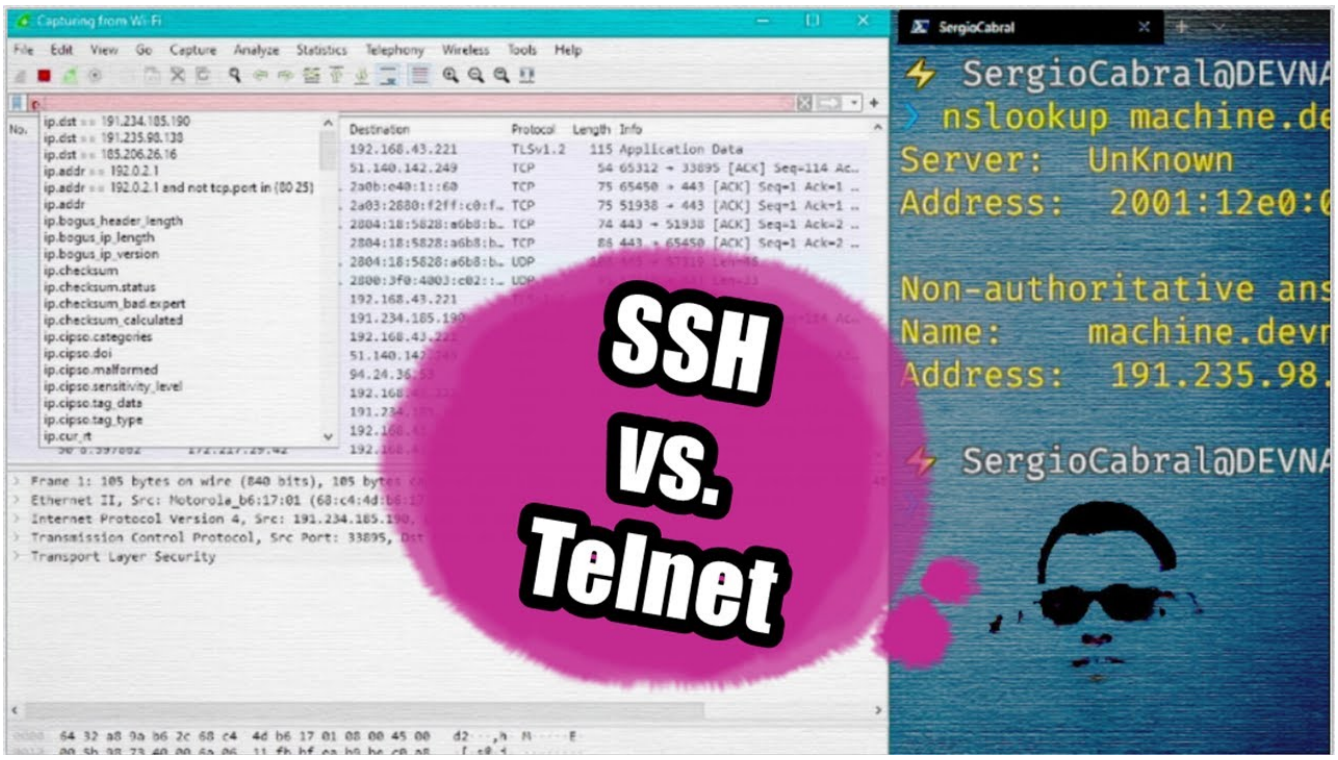
3. Conclusão

Por isso que SSH é uma sigla para Secure Shell, ou terminal seguro. Ou seja, não use Telnet em redes inseguras e sempre prefira SSH.

4. Opções de sniffers de rede

Nome	Licença	Download
Tcpdump	free; open-source	https://www.tcpdump.org/
Cloudshark	trial	https://www.cloudshark.org/
Sysdig	free; open-source	https://sysdig.com/opensource/inspect/
Ettercap	free; open-source	https://www.ettercap-project.org/downloads.html
SmartSniff	free	https://www.nirsoft.net/utils/smsniff.html

5. Demonstração em vídeo



https://youtu.be/qracA6LUctA

I'll be back.