STREAM SERIES

devnator

Security Comparison
SSH and Telnet Protocols

SERGIO CABRAL

sergiocabral.com

Topics

Practical purpose of this demonstration

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. Analyzing Telnet packets

Why does everyone use SSH instead of Telnet? - SSH and Telnet are two protocols that have the same objective, that is, access a server to perform operations on that remote system. But the main difference between the two is encryption.

A simple definition for encryption is the ability to make a message unreadable and only someone with the rollback key could read the original content.

If an unencrypted message travels over a network, anyone who intercepts it can read its contents. Using a network packet analyzer, which is also known as a Sniffer, we can demonstrate this. As an example, we can use Wireshark, in *Figure 1*, and see network packets traveling both on an SSH connection and on a Telnet connection.

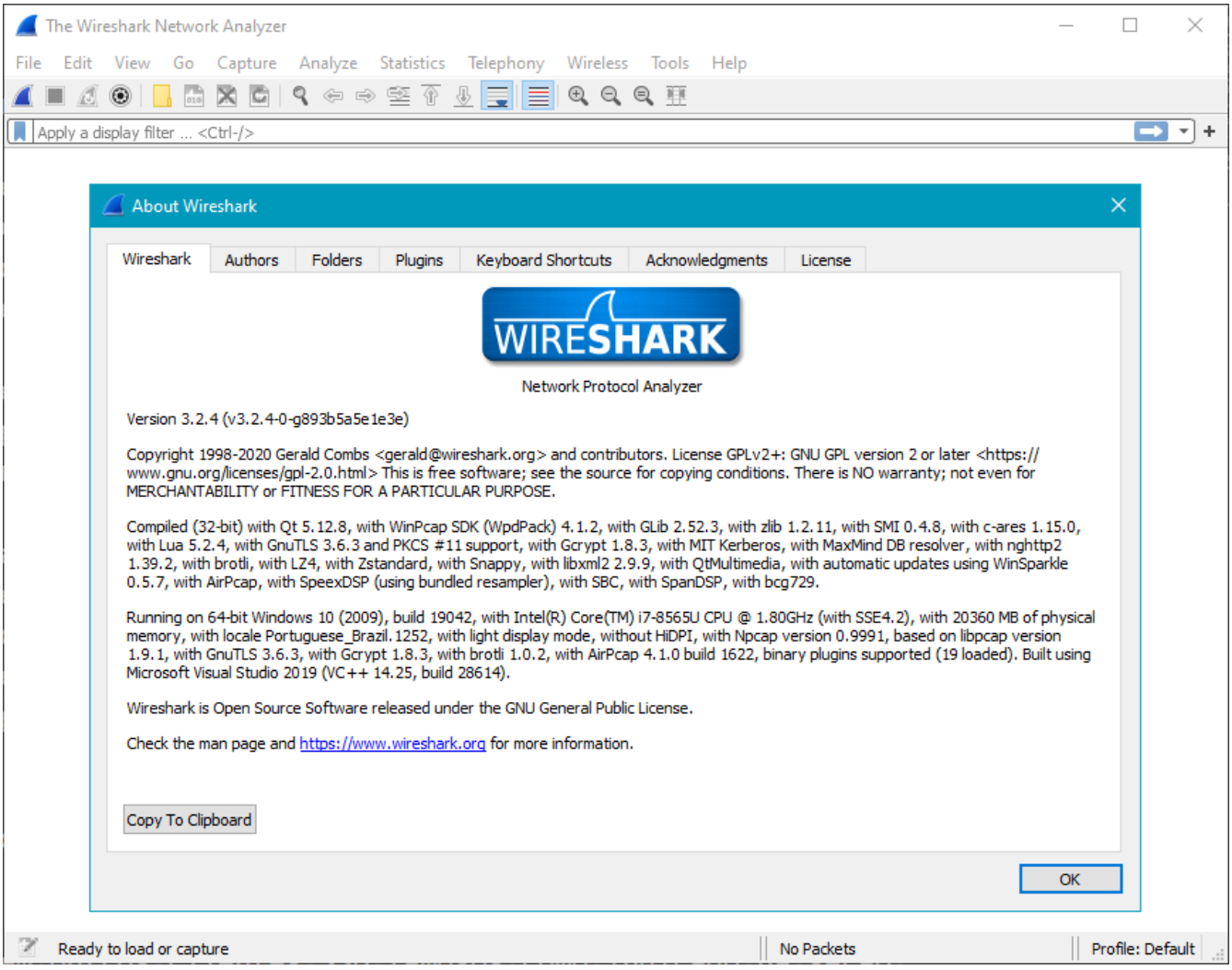


Figure 1. Wireshark app

See other alternatives to Wireshark in section Network sniffers options.

We need to check which is the server IP and make Wireshark filter IP packets addressed to this using the syntax `ip.dst == 191.235.98.138`. Now only network packets from that Telnet connection will be displayed.

For the test we can inform the user on the telnet connection and press `Enter`. Then we clear the

Wireshark history and we can see from here that for each key typed a network packet is sent exposing what you type.

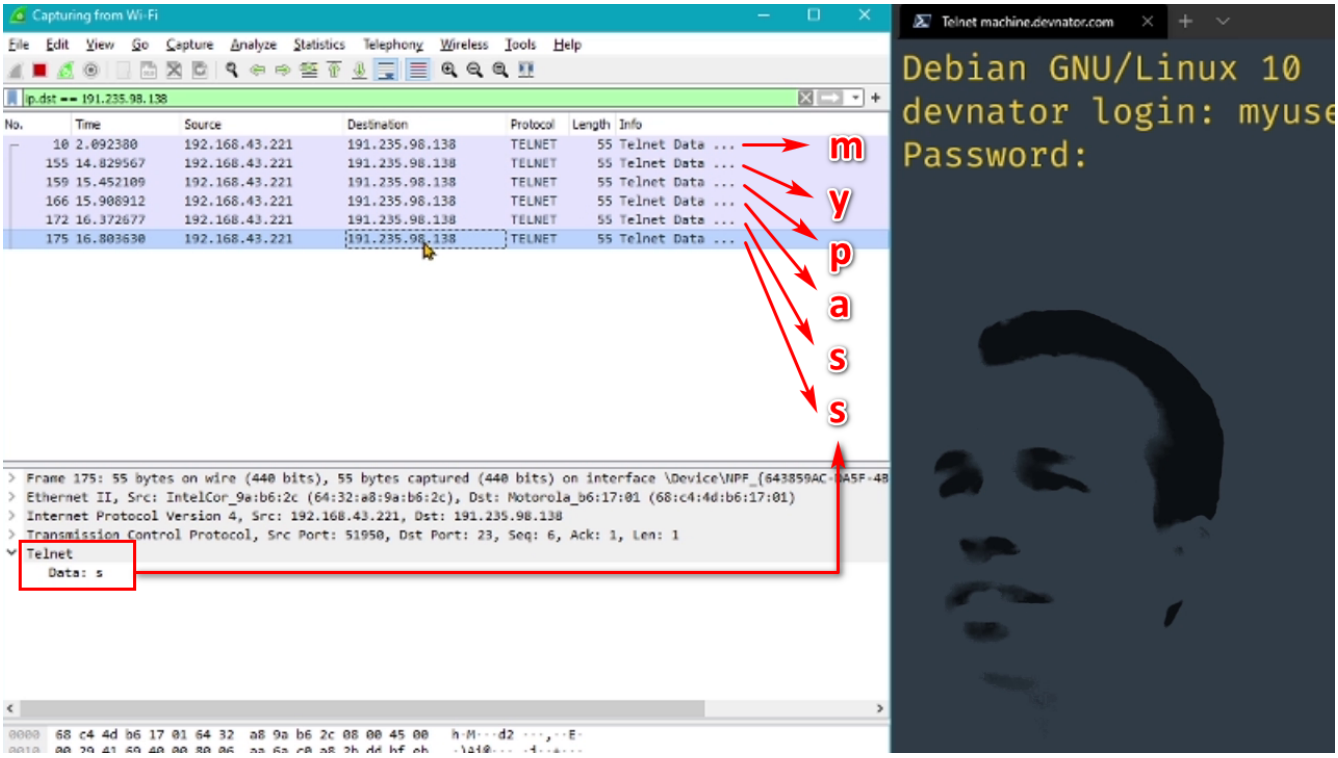


Figure 2. Telnet packets with leaked keystrokes

As shown in *Figure 2*, my password being “mypass” and I can see each letter being sent by the network packets: “m”, “y”, “p”, “a”, “s”, “s”.

When proceeding with the connection and sending commands we see the network packets traveling with the data open for reading, without using encryption.

2. Analyzing SSH packets

We now connect using the SSH protocol. Unlike Telnet, which after establishing the connection needs to receive the user's name via keyboard, SSH already sends this information together with the address of the remote computer at the time of connection. Then you only enter the password via the keyboard.

Since it is the same remote computer, we will continue to use the IP filter applied in Wireshark but we clear the history before entering the password. You will notice that a network packet is not sent for each keystroke. It will only be sent when you are finished entering the password and pressing `Enter`. And the package will be sent in encrypted form.

After login, the SSH protocol also sends a network packet for each key typed, just like Telnet does. But these packages are encrypted, they are not readable, as indicated in yellow in *Figure 3*.

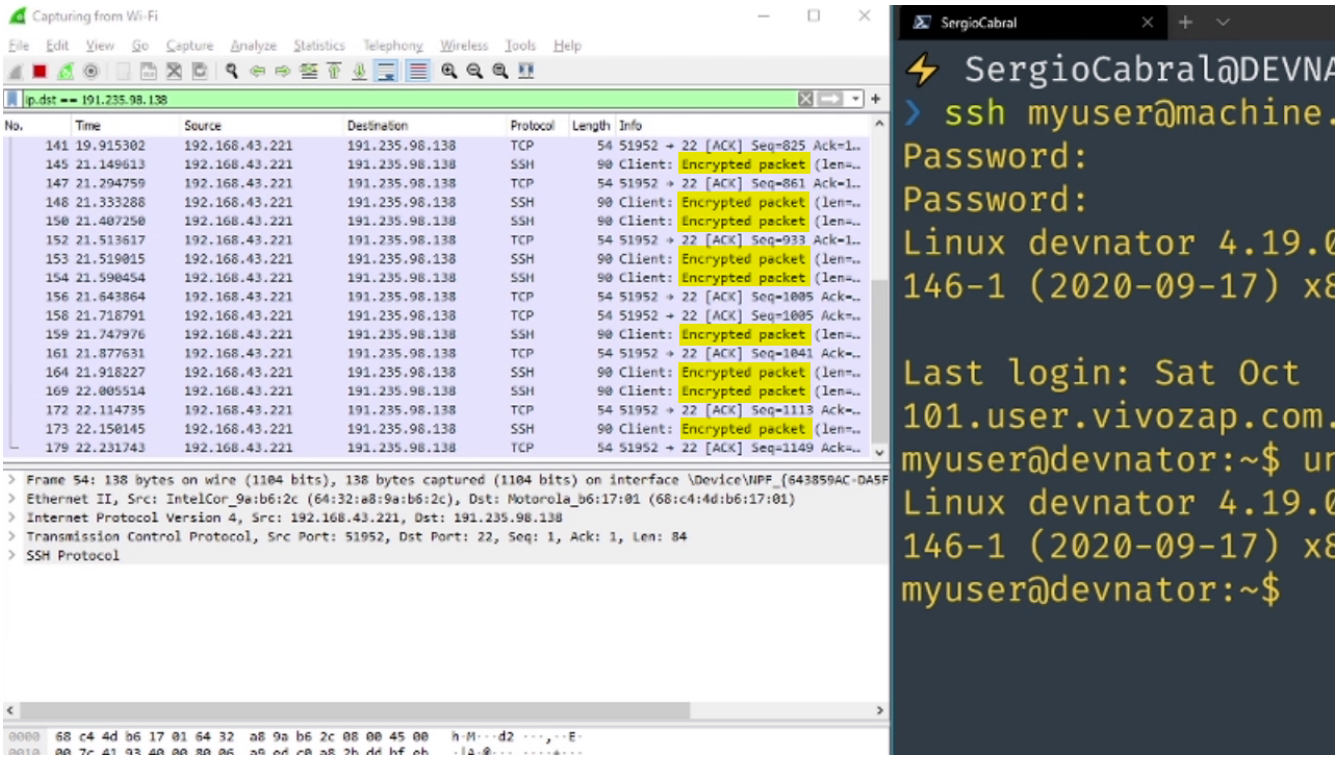


Figure 3. Encrypted SSH packets

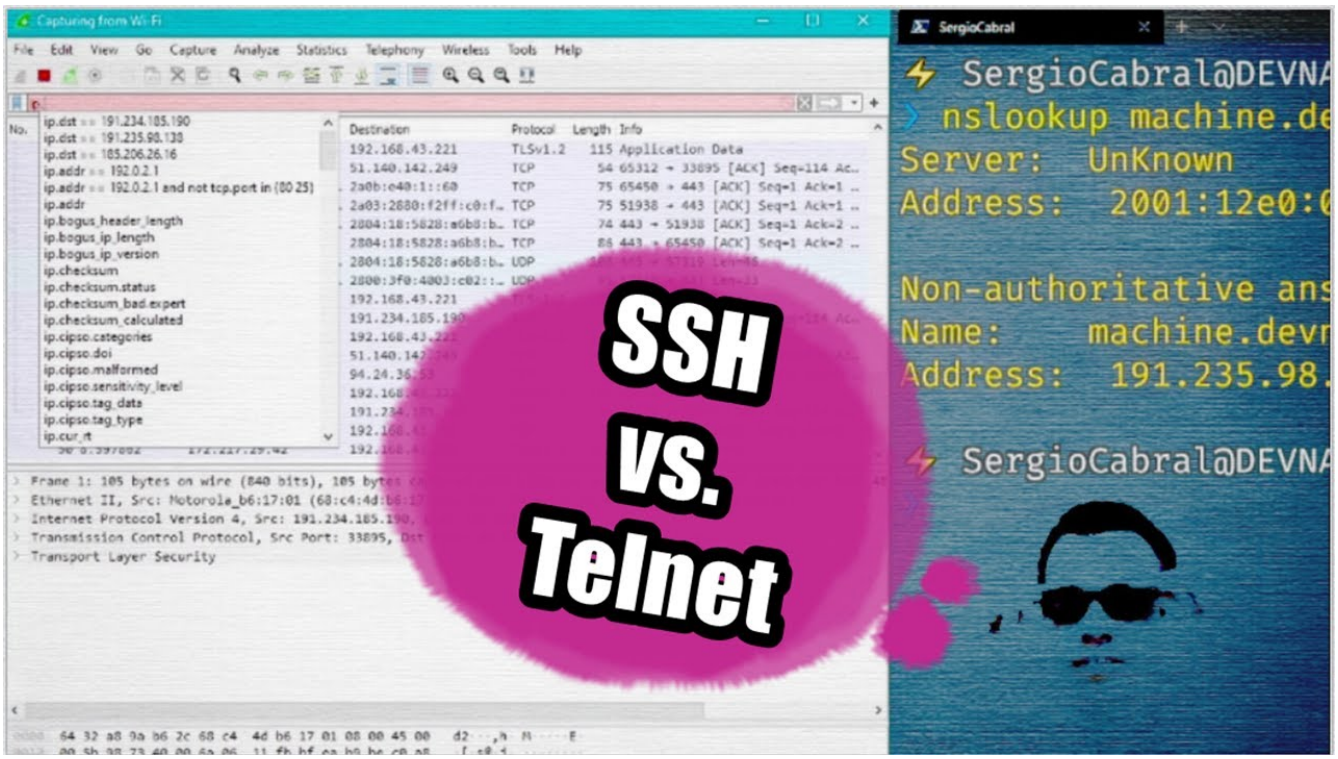
3. Conclusion

That is why SSH is an acronym for Secure Shell. That is, do not use Telnet on insecure networks and always prefer SSH.

4. Network sniffers options

Name	License	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. Video demonstration



https://youtu.be/f3FdwUO4v6M

I'll be back.