Welcome to Wireshark MeetUp #3

27-2-2024

Sshdump & Ciscodump

By Eduard Kooijmans

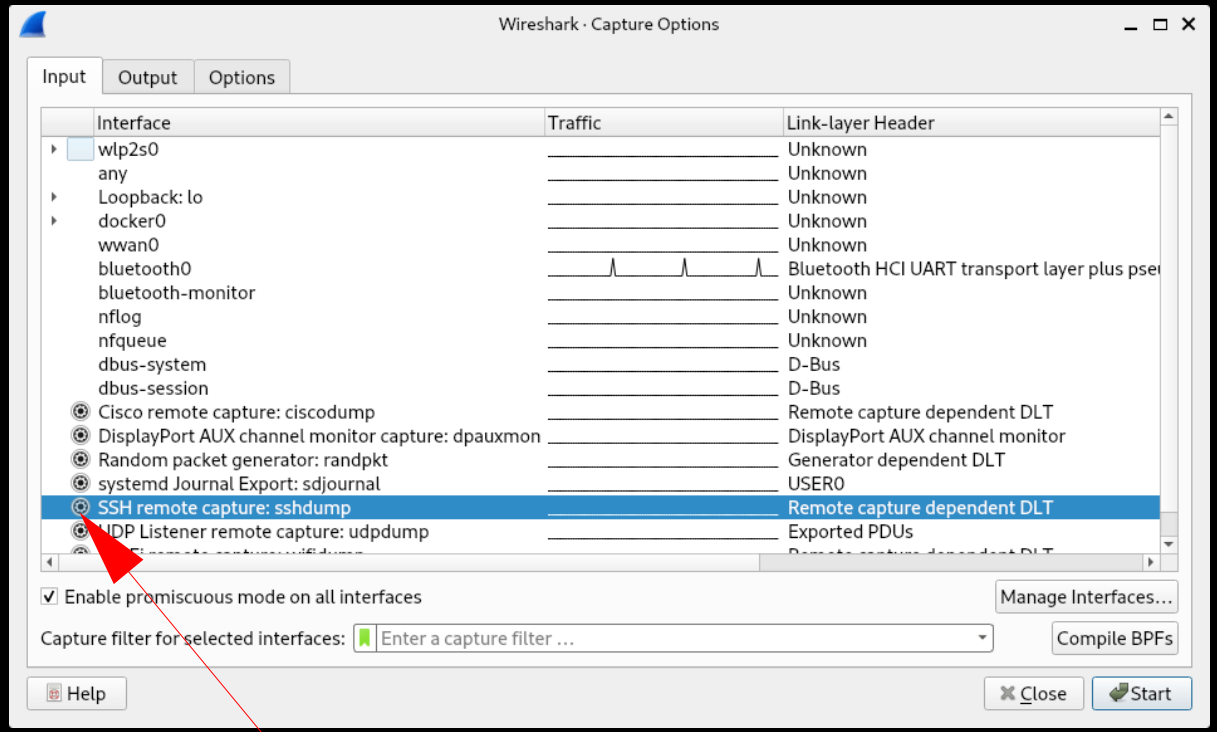
Sshdump

User needs sudo rights!

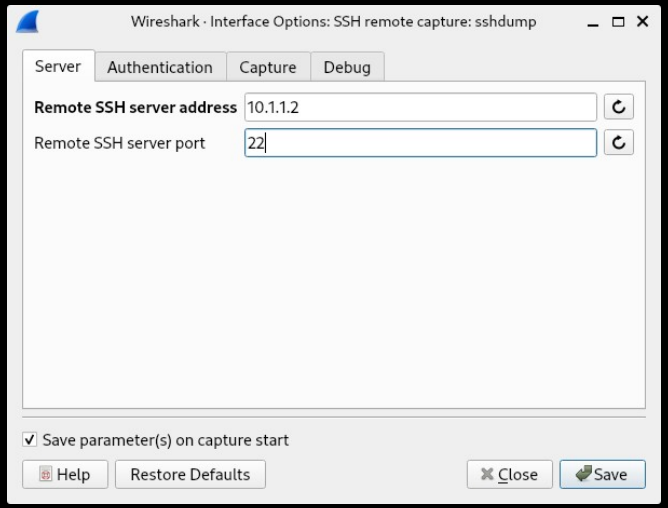
The following command gives the user sudo right to sudo without enter a password:

echo "$USER ALL=(ALL:ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/$USER

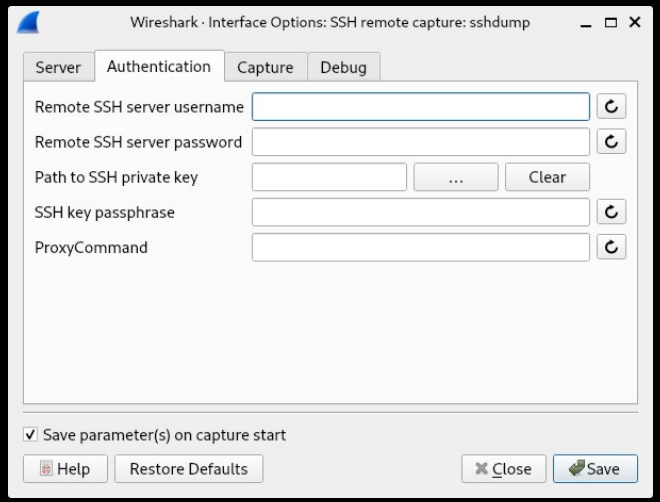
Use at your own risk!!!!


Wireshark · Capture Options
Input
Output
Options
Interface
Traffic
Link-layer Header
wlp2s0 Unknown
any Unknown
Loopback: lo Unknown
docker0 Unknown
wwan0 Unknown
bluetooth0 Bluetooth HCI UART transport layer plus pse
bluetooth-monitor Unknown
nflog Unknown
nfqueue Unknown
dbus-system D-Bus
dbus-session D-Bus
Cisco remote capture: ciscodump Remote capture dependent DLT
DisplayPort AUX channel monitor capture: dpauxmon DisplayPort AUX channel monitor
Random packet generator: randpkt Generator dependent DLT
systemd Journal Export: sdjournal USER0
SSH remote capture: sshdump Remote capture dependent DLT
UDP Listener remote capture: udpdump Exported PDUs
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces:
Enter a capture filter ...
Compile BPFs
Help
Close
Start

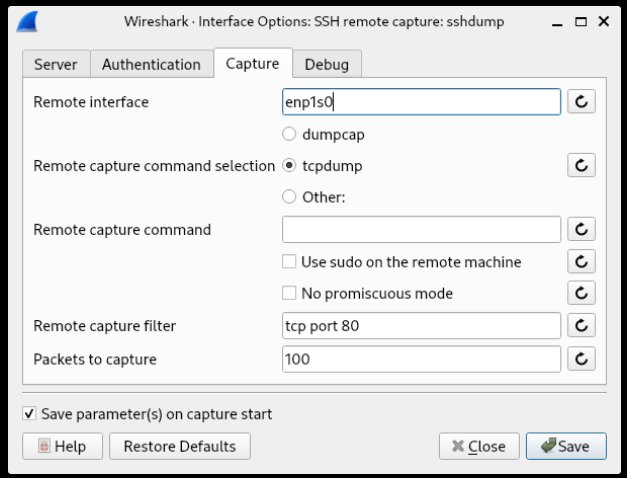
Click on



Enter IP address



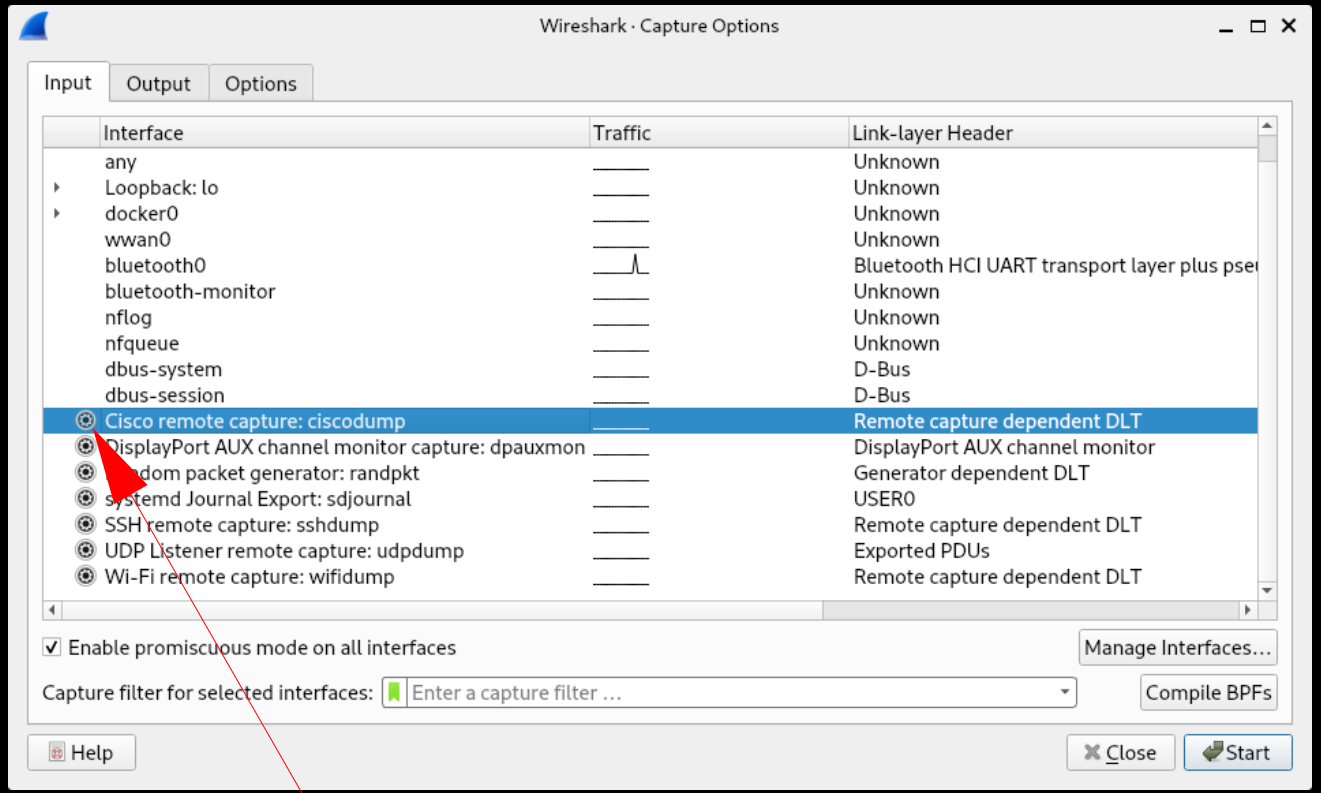
Enter Credentials



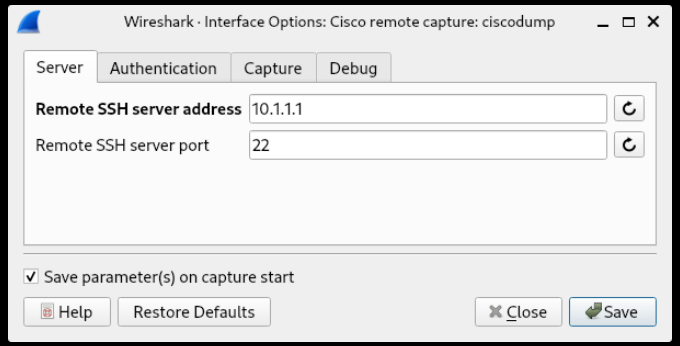
Enter interface remote ssh server, capture filter

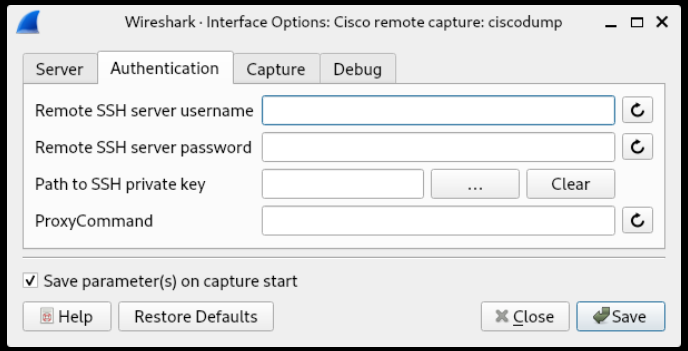
Ciscodump

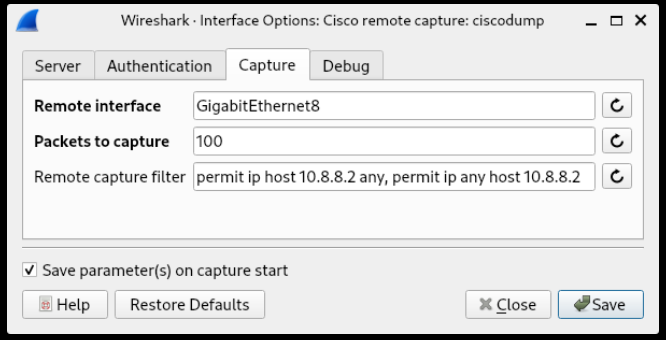
User needs privelege rights


Wireshark · Capture Options
Input
Output
Options
Interface
Traffic
Link-layer Header
any
Unknown
Loopback: lo
Unknown
docker0
Unknown
wwan0
Unknown
bluetooth0
Bluetooth HCI UART transport layer plus pse
bluetooth-monitor
Unknown
nflog
Unknown
nfqueue
Unknown
dbus-system
D-Bus
dbus-session
D-Bus
Cisco remote capture: ciscodump
Remote capture dependent DLT
DisplayPort AUX channel monitor capture: dpauxmon
DisplayPort AUX channel monitor
dom packet generator: randpkt
Generator dependent DLT
systemd Journal Export: sdjournal
USER0
SSH remote capture: sshdump
Remote capture dependent DLT
UDP Listener remote capture: udpdump
Exported PDUs
Wi-Fi remote capture: wifidump
Remote capture dependent DLT
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces:
Enter a capture filter ...
Compile BPFs
Help
Close
Start

Click on


Wireshark · Interface Options: Cisco remote capture: ciscodump
Server
Authentication
Capture
Debug
Remote SSH server address
10.1.1.1
Remote SSH server port
22
Save parameter(s) on capture start
Help
Restore Defaults
Close
Save


Wireshark · Interface Options: Cisco remote capture: ciscodump
Server
Authentication
Capture
Debug
Remote SSH server username
Remote SSH server password
Path to SSH private key
...
Clear
ProxyCommand
Save parameter(s) on capture start
Help
Restore Defaults
Close
Save


Wireshark · Interface Options: Cisco remote capture: ciscodump
Server
Authentication
Capture
Debug
Remote interface
GigabitEthernet8
Packets to capture
100
Remote capture filter
permit ip host 10.8.8.2 any, permit ip any host 10.8.8.2
Save parameter(s) on capture start
Help
Restore Defaults
Close
Save

Cli sshdump

3 ways to do the same (start tcpdump remote on a ssh server and write output local to a fifo pipe):

1.
./sshdump --extcap-interface=sshdump --remote-host 10.1.1.2 --remote-port 22 --remote-username jack --remote-password welkom --remote-capture-command 'sudo tcpdump -U -i enp1s0 -w - -c 100 tcp port 80' --fifo=/home/jack/MeetUP-Wireshark/host1 --capture

2.
./sshdump --extcap-interface=sshdump --remote-host 10.1.1.2 --remote-port 22 --remote-username jack --remote-password welkom --remote-interface enp1s0 --remote-capture-command-select tcpdump --remote-priv sudo --remote-filter 'tcp port 80' --remote-count 100 --fifo=/home/jack/MeetUP-Wireshark/host1 --capture

3.
ssh jack@10.1.1.2 -p 22 'sudo tcpdump -U -i enp1s0 -w - -c 100 tcp port 80' > /home/jack/MeetUP-Wireshark/host1

Use wireshark to read from the fifo pipes

Cli sshdump

Script to start sshdump concurrent locally and use tcpdump remotely on two different ssh servers and write output to a fifo pipe

----
./sshdump --extcap-interface=sshdump --remote-host 10.1.1.2 --remote-port 22 --remote-username jack --remote-password welkom --remote-capture-command 'sudo tcpdump -U -i enp1s0 -w - -c 100 tcp port 80' --fifo=/home/jack/MeetUP-Wireshark/host1 --capture &

./sshdump --extcap-interface=sshdump --remote-host 10.8.8.2 --remote-port 22 --remote-username jack --remote-password welkom --remote-capture-command 'sudo tcpdump -U -i enp1s0 -w - -c 100 tcp port 80' --fifo=/home/jack/MeetUP-Wireshark/host2 --capture &

Use wireshark to read from the fifo pipe

Cli Ciscodump

./ciscodump --extcap-interface=ciscodump --remote-host 10.1.1.1 --remote-port 22 --remote-username ciscodump --remote-password ciscodump --remote-interface gigabitethernet8 --remote-count 100 --remote-filter 'permit ip host 10.8.8.2 any, permit ip any host 10.8.8.2' --fifo=/home/jack/MeetUP-Wireshark/cisco –capture

Use wireshark to read from the fifo pipes

More info:

https://www.wireshark.org/docs/man-pages/ciscodump.html

https://www.wireshark.org/docs/man-pages/sshdump.html

https://wiki.wireshark.org/CaptureSetup/Pipes