NAME

sshdump − Provide interfaces to capture from a remote host through SSH using a remote capture binary.

SYNOPSIS

sshdump [**−−help**] [**−−version**] [**−−extcap−interfaces**] [**−−extcap−dlts**]
[**−−extcap−interface**=<interface>] [**−−extcap−config**] [**−−extcap−capture−filter**=<capture filter>]
[**−−capture**] [**−−fifo**=<path to file or pipe>] [**−−remote−host**=<IP address>]
[**−−remote−port**=<TCP port>] [**−−remote−username**=<username>]
[**−−remote−password**=<password>] [**−−sshkey**=<public key path>]
[**−−remote−interface**=<interface>] [**−−remote−capture−command**=<capture command>]
[**−−remote−sudo**]

sshdump −−extcap−interfaces

sshdump −−extcap−interface=<interface> **−−extcap−dlts**

sshdump −−extcap−interface=<interface> **−−extcap−config**

sshdump −−extcap−interface=<interface> **−−fifo**=<path to file or pipe> **−−capture**
−−remote−host=myremotehost −−remote−port=22 −−remote−username=user
−−remote−interface=eth2 −−remote−capture−command='tcpdump −U −i eth0 −w−'

DESCRIPTION

Sshdump is an extcap tool that allows one to run a remote capture tool over a SSH connection. The requirement is that the capture executable must have the capabilities to capture from the wanted interface.

The feature is functionally equivalent to run commands like

```
$ ssh remoteuser@remotehost −p 22222 'tcpdump −U −i IFACE −w −' > FILE &
$ wireshark FILE

$ ssh remoteuser@remotehost '/sbin/dumpcap −i IFACE −P −w − −f "not port 22"' > F
$ wireshark FILE

$ ssh somehost dumpcap −P −w − −f udp | tshark −i −
```

Typically sshdump is not invoked directly. Instead it can be configured through the Wireshark graphical user interface or its command line. The following will start Wireshark and start capturing from host **remotehost**:

```
$ wireshark '−oextcap.sshdump.remotehost:"remotehost"' −i sshdump −k
```

To explicitly control the remote capture command:

```
$ wireshark '−oextcap.sshdump.remotehost:"remotehost"' \
            '−oextcap.sshdump.remotecapturecommand:"tcpdump −i eth0 −Uw− not port
            −i sshdump −k
```

Supported interfaces:

1. ssh

OPTIONS

−−help

Print program arguments.

−−version

Print program version.

−−extcap−interfaces

List available interfaces.

−−extcap−interface=<interface>

Use specified interfaces.

−−extcap−dlts

List DLTs of specified interface.

−−extcap−config

List configuration options of specified interface.

−−capture

Start capturing from specified interface and write raw packet data to the location specified by −−fifo.

−−fifo=<path to file or pipe>

Save captured packet to file or send it through pipe.

−−remote−host=<remote host>

The address of the remote host for capture.

−−remote−port=<remote port>

The SSH port of the remote host.

−−remote−username=<username>

The username for ssh authentication.

−−remote−password=<password>

The password to use (if not ssh−agent and pubkey are used). WARNING: the passwords are stored in plaintext and visible to all users on this system. It is recommended to use keyfiles with a SSH agent.

−−sshkey=<SSH private key path>

The path to a private key for authentication.

−−remote−interface=<remote interface>

The remote network interface to capture from.

−−remote−capture−command=<capture command>

A custom remote capture command that produces the remote stream that is shown in Wireshark. The command must be able to produce a PCAP stream written to STDOUT. See below for more examples.

If using tcpdump, use the **−w−** option to ensure that packets are written to standard output (stdout). Include the **−U** option to write packets as soon as they are received.

When specified, this command will be used as is, options such as the capture filter (**−−extcap−capture−filter**) will not be appended.

−−extcap−capture−filter=<capture filter>

The capture filter. It corresponds to the value provided via the **tshark −f** option, and the Capture Filter field next to the interfaces list in the Wireshark interface.

EXAMPLES

To see program arguments:

```
sshdump --help
```

To see program version:

```
sshdump --version
```

To see interfaces:

```
sshdump --extcap-interfaces
```

Only one interface (sshdump) is supported.

Example output

```
interface {value=sshdump}{display=SSH remote capture}
```

To see interface DLTs:

```
sshdump --extcap-interface=sshdump --extcap-dlts
```

Example output

```
dlt {number=147}{name=sshdump}{display=Remote capture dependent DLT}
```

To see interface configuration options:

```
sshdump --extcap-interface=sshdump --extcap-config
```

Example output

```
arg {number=0}{call=--remote-host}{display=Remote SSH server address}{type=string
    {tooltip=The remote SSH host. It can be both an IP address or a hostname}{req
arg {number=1}{call=--remote-port}{display=Remote SSH server port}{type=unsigned}
    {tooltip=The remote SSH host port (1-65535)}{range=1,65535}{group=Server}
arg {number=2}{call=--remote-username}{display=Remote SSH server username}{type=s
    {tooltip=The remote SSH username. If not provided, the current user will be u
arg {number=3}{call=--remote-password}{display=Remote SSH server password}{type=p
    {tooltip=The SSH password, used when other methods (SSH agent or key files) a
```

```
arg {number=4}{call=--sshkey}{display=Path to SSH private key}{type=fileselect}
    {tooltip=The path on the local filesystem of the private ssh key}{group=Authe
arg {number=5}{call=--sshkey-passphrase}{display=SSH key passphrase}{type=passwor
    {tooltip=Passphrase to unlock the SSH private key}{group=Authentication}
arg {number=6}{call=--proxycommand}{display=ProxyCommand}{type=string}
    {tooltip=The command to use as proxy for the SSH connection}{group=Authentica
arg {number=7}{call=--remote-interface}{display=Remote interface}{type=string}
    {tooltip=The remote network interface used for capture}{group=Capture}
arg {number=8}{call=--remote-capture-command}{display=Remote capture command}{typ
    {tooltip=The remote command used to capture}{group=Capture}
arg {number=9}{call=--remote-sudo}{display=Use sudo on the remote machine}{type=b
    {tooltip=Prepend the capture command with sudo on the remote machine}{group=C
arg {number=10}{call=--remote-noprom}{display=No promiscuous mode}{type=boolflag}
    {tooltip=Don't use promiscuous mode on the remote machine}{group=Capture}
arg {number=11}{call=--remote-filter}{display=Remote capture filter}{type=string}
    {tooltip=The remote capture filter}{default=not ((host myhost) and port 22)}{
arg {number=12}{call=--remote-count}{display=Packets to capture}{type=unsigned}{d
    {tooltip=The number of remote packets to capture. (Default: inf)}{group=Captu
arg {number=13}{call=--debug}{display=Run in debug mode}{type=boolflag}{default=f
    {tooltip=Print debug messages}{required=false}{group=Debug}
arg {number=14}{call=--debug-file}{display=Use a file for debug}{type=string}
    {tooltip=Set a file where the debug messages are written}{required=false}{gro
```

To capture:

```
sshdump --extcap-interface=sshdump --fifo=/tmp/ssh.pcap --capture --remote-host 1
--remote-username user --remote-filter "not port 22"
```

To use different capture binaries:

```
sshdump --extcap-interface=sshdump --fifo=/tmp/ssh.pcap --capture --remote-host 1
--remote-capture-command='dumpcap -i eth0 -P -w -'

sshdump --extcap-interface=sshdump --fifo=/tmp/ssh.pcap --capture --remote-host 1
--remote-capture-command='sudo tcpdump -i eth0 -U -w -'
```

Note

To stop capturing CTRL+C/kill/terminate application.

The sshdump binary can be renamed to support multiple instances. For instance if we want sshdump to show up twice in wireshark (for instance to handle multiple profiles), we can copy sshdump to sshdump−host1 and sshdump−host2. Each binary will show up an interface name same as the executable name. Those executables not being "sshdump" will show up as "custom version" in the interface description.

SEE ALSO

wireshark(1), tshark(1), dumpcap(1), extcap(4), tcpdump(1)

NOTES

Sshdump is part of the **Wireshark** distribution. The latest version of **Wireshark** can be found at https://www.wireshark.org.

HTML versions of the Wireshark project man pages are available at https://www.wireshark.org/docs/man−pages.

AUTHORS

Original Author

Dario Lombardo <lomato[AT]gmail.com>