

Some useful tips about /dev/tcp

Mar 6, 2021

Just some simple tips that I found very useful.

Bash supports read/write operations on a pseudo-device file `/dev/tcp/[host]/[port]` ^[1].

Writing to this special file makes bash open a tcp connection to `host:port`, and this feature may be used for some useful purposes, for example:

Query an NTP server

this command:

```
cat </dev/tcp/time.nist.gov/13
```

reads the time in **Daytime Protocol** from the NIST Internet Time Service server.

Fetch a web page

this script

```
exec 3<>/dev/tcp/www.google.com/80
echo -e "GET / HTTP/1.1\r\nhost: http://www.google.com\r\nConnection: close\r\n\r\n" >&3
cat <&3
```

fetches the front page from Google.com.

Perform a port scan

In case you are not enabled to install any software on your linux box, using the same special file, you can check if a tcp port is open: if writing to the port succeeds, the port is open, else the port is closed.

So, you can perform a basic port scan, for example of an entire subnet, using a simple script like

```
for ip in {1..254};
do for port in {22,80,443,3306,3389};
do (echo >/dev/tcp/192.168.1.|$ip/$port) >& /dev/null && echo "192.168.1.$ip:$port is c
done;
done
```

You can customize the script changing the involved subnet.

Download a file

```
wget ()
{
IFS=/ read proto z host query <<< "$1"
exec 3< /dev/tcp/$host/80
{
echo GET /$query HTTP/1.1
echo connection: close
echo host: $host
echo
} >&3
sed '1,/^\$/d' <&3 > $(basename $1)
}




_wget http://www.andreafortuna.org/robots.txt
```

References

1. <https://tldp.org/LDP/abs/html/devref1.html>

Andrea Fortuna

Andrea Fortuna
andrea@andreafortuna.org

-  [andreafortuna](#)
-  [andrea-fortuna](#)
-  [andrea](#)

Cybersecurity expert, software developer,
experienced digital forensic analyst, musician