Andrea Fortuna

About   Rss

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
```

reads the time in

Fetch a we

this script

```
exec 3<>/dev/                                              \n\r\n" >&3
echo -e "GET
cat <&3
```

fetches the front

Perform a

In case you are r   l file, you can check if a tcp po   osed.

So, you can perf   t 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

andreafortuna.org asks for your consent to use your personal data to:

Personalised advertising and content, advertising and content measurement, audience research and services development

Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with 134 TCF vendor(s) and 63 ad partner(s), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.