

Find...

portscanner.sh

```
1 #!/bin/bash
2
3 # Basic bash port scanner
4
5 host=$1
6 startport=$2
7 stopport=$3
8
9 function pingcheck
10 {
11 pingresult=$(ping -c 1 $host | grep bytes | wc -l)
12 if [ "$pingresult" -gt 1 ]; then
13     echo "$host is up"
14 else
15     echo "$host is down, quitting"
16     exit
17 fi
18 }
19
20 function portcheck
21 {
22 for ((counter=$startport; counter<=$stopport; counter++))
23 do
24     if timeout 2 bash -c "echo >/dev/tcp/$host/$counter"
25     then
26         echo "$counter open"
27     else
28         echo "$counter closed"
29     fi
30 done
31 }
32
33 # first, check that the host is alive
34 pingcheck
35 # next, loop through the ports
36 portcheck
37
38
39
```