

♥ these comics?
buy a collection!

→ wizardzines.com ←

nmap

JULIA EVANS
@b0rk

nmap lets you explore
a network

which ports
are open?

what hosts
are up?

security people use it a lot!

find which hosts are up

```
$ nmap -sn 192.168.1.0/24
           ↑
       my home network
```

just finds hosts, doesn't
port scan

aggressive scan

```
nmap -v -A scanme.nmap.org
```

real host!
try it!

it can often detect the OS
the server is running. Ports,
webserver version, etc.

fast port scan

```
$ nmap -ss -F 192.168.1.0/24
```

just sends a SYN packet to
check if each port is open.
I found out which ports my
printer has open!

-F

scan less ports: just the
most common ones

-T4 or -T5

scan faster by timing
out more quickly

♥ check TLS version ♥
and ciphers

check if your server still supports
old TLS versions

```
$ nmap
--script ssl-enum-ciphers
-p 443 wizardzines.com
```

nmap comes with HUNDREDS
of useful scripts like this ♥

page 15 of upcoming "bite size networking" zine!

