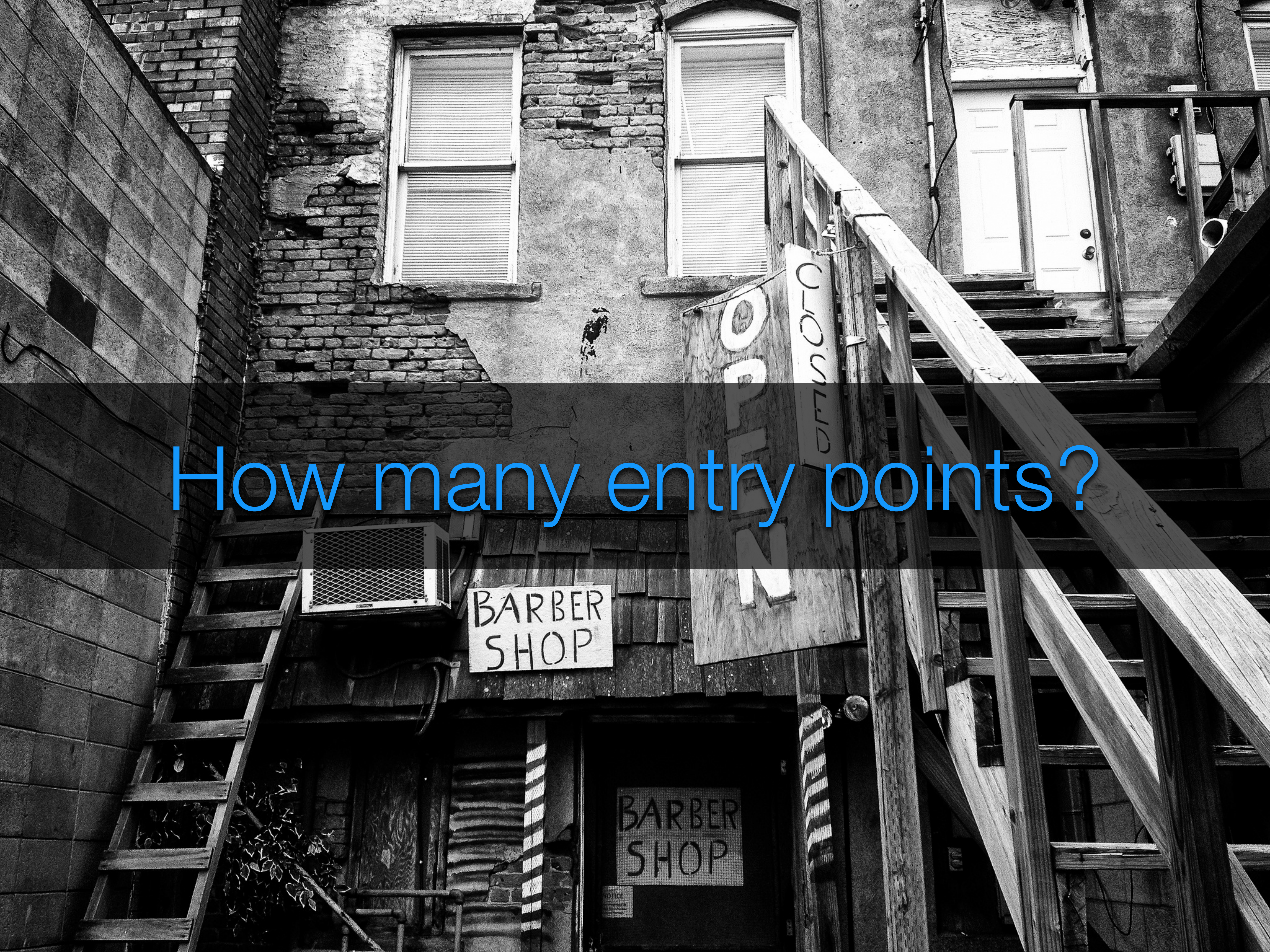
Names and virtual host discovery

Can you spot all names?

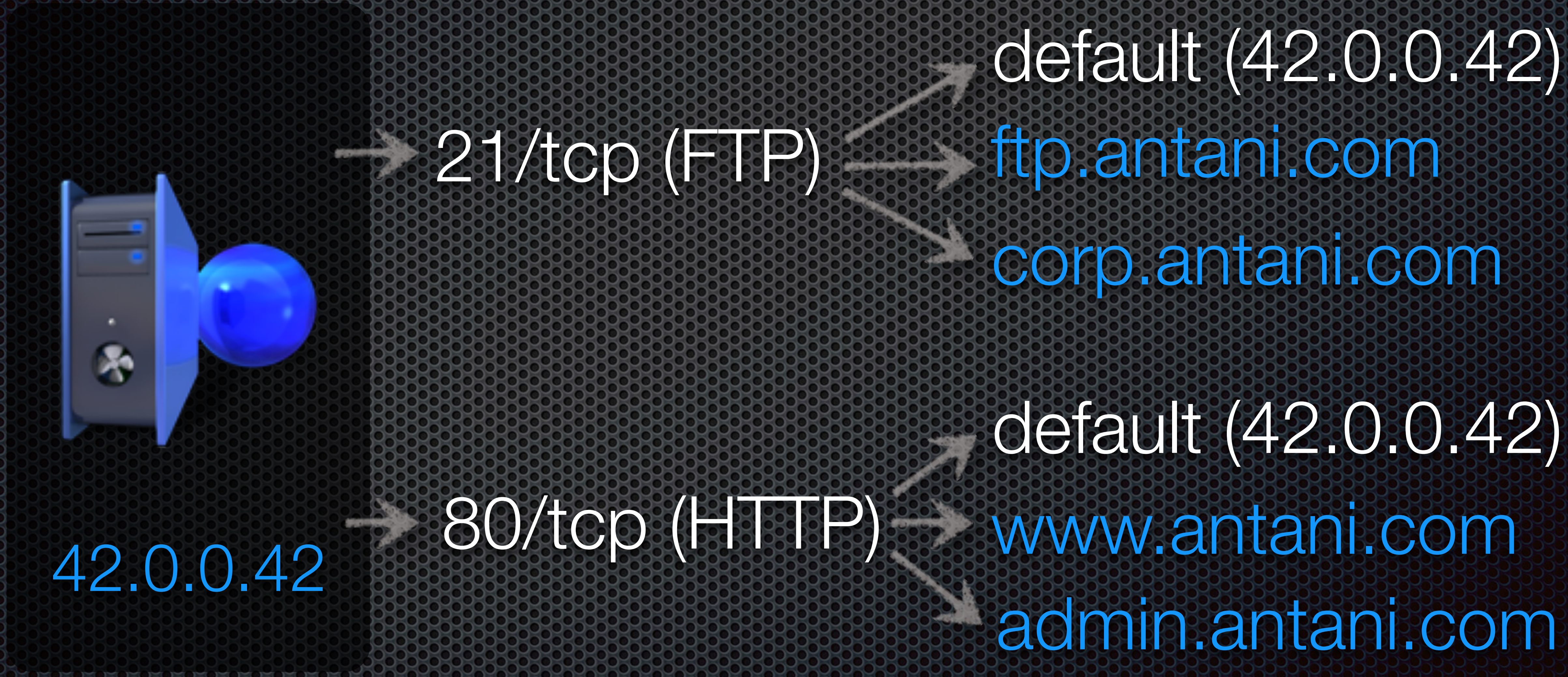
@jekil

- Cuckoo Sandbox (cuckoosandbox.org)
- Malwr (malwr.com)
- Secdocs (secdocs.org)
- Ghiro (getghiro.org)
- Hostmap



How many entry points?

Virtual hosting



42.0.0.42

21/tcp (FTP)

default (42.0.0.42)

ftp.antani.com

corp.antani.com

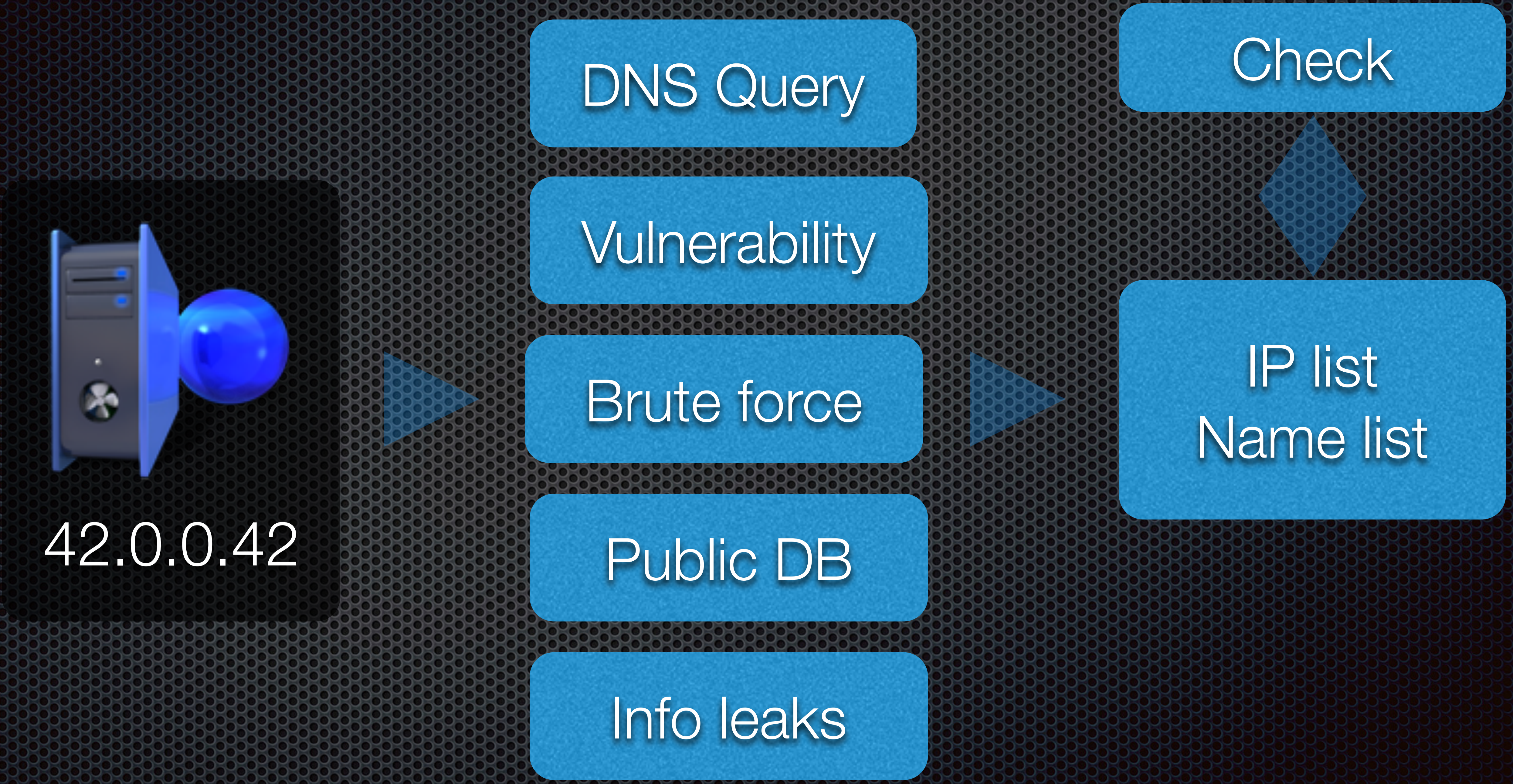
80/tcp (HTTP)

default (42.0.0.42)

www.antani.com

admin.antani.com

Enumeration process



42.0.0.42

DNS Query

Vulnerability

Brute force

Public DB

Info leaks

Check

IP list
Name list

DNS names enumeration

DNS queries

- PTR (reverse lookup)
- NS (name server lookup)
- MX (mail server lookup)
- AXFR (zone transfer vuln)
- SRV (service location lookup)
- Many resource record types
  http://en.wikipedia.org/wiki/List_of_DNS_record_types

DNS names brute force

- Perform many A (AAAA) queries
- It takes a lot of time
- It could overload DNS servers
- You need a good wordlist
- Not stealth

Service fingerprints

Banner grabbing

- Services prone to host name leak
- Host names in response banner
- By default, by design

```
$ nc 216.18.179.54 25
220 barracuda.ord1.reflected.net ESMTP
(e5fb20dbadbd8bd56b3600247242f162)
```

SSL/TLS

X.509 Certificate

- Services over SSL/TLS
- Some properties could expose host names or IP
- Example: Common Name (CN)

```
$  openssl s_client -showcerts -connnect
151.22.70.92:443
....
subject=/C=IT/ST=Venezia/L=Venezia/OU=IT/
O=SAVE S.P.A./CN=my.veniceairport.it
```

Application layer

Tough applications

- Host name leak in application/protocol
- Following HTTP redirects, crawling website
- Host names in application errors
- Virtual host names brute forcing at application layer
- Application host names could be missing in DNS

Passive enumeration

Public data

- Search engines (dorking)
- GPG key databases
- WHOIS
- DNS history sites
- Passive DNS
- Shodan
- Webarchive
- Internet census / scans
- Pick one...

Tools

Tools

- Bile suite
- Blacksheepwall
- DNSenum.pl
- DNSrecon
- Hostmap
- Fierce2
- Maltego
- Metasploit
- Nmap
- Recon-ng
- Theharvester
- Txdns
- A pleteora of small scripts...

END