Midterm Review

Patch Notes

Midterm: In class on Thursday

- Open internet, bring anything except a friend
- Entire exam is free response

The exam is in person! Reach out if you need an exception!

Patch Notes

Midterm:

- 40 points: 10 short-answer questions, you need to answer 8
- 60 points: 5 medium-answer questions, you need to answer 4
- 1 extra credit question
- Not planning on curving it unless I grossly misjudged how hard it is.

Patch Notes

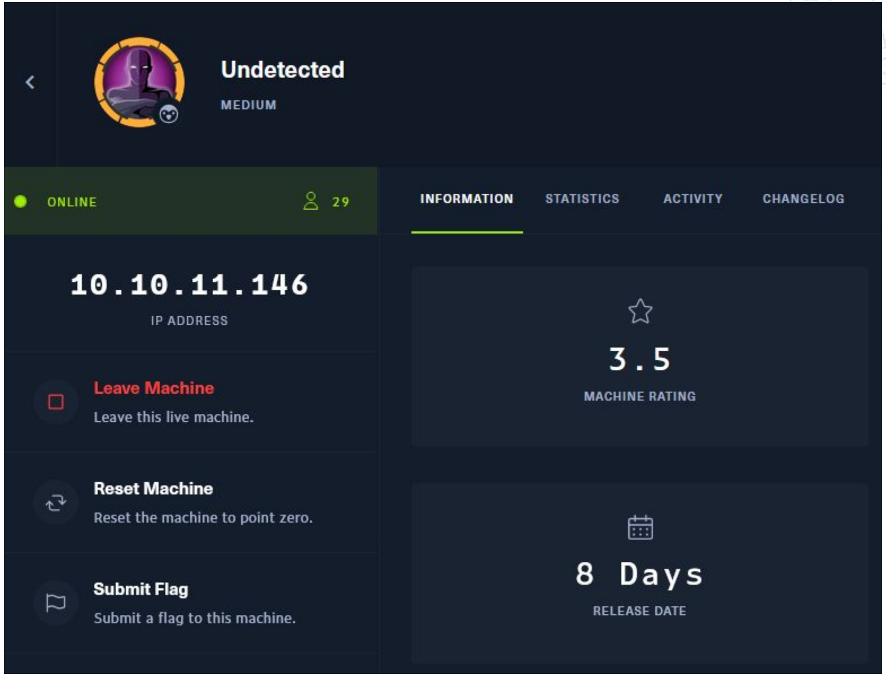
Quizzes:

- Quiz due today, deadline extended to 7:00

Patch Notes

HackTheBox: As close to "real" hacking as you can get

1. Start with only an IP
2. Need to scan for targets, e.g. with nmap.
3. From there, brute force passwords, hunt for logic bugs, etc.



Undetected

MEDIUM

ONLINE 29

10.10.11.146

IP ADDRESS

Leave Machine

Leave this live machine.

Reset Machine

Reset the machine to point zero.

Submit Flag

Submit a flag to this machine.

3.5

MACHINE RATING

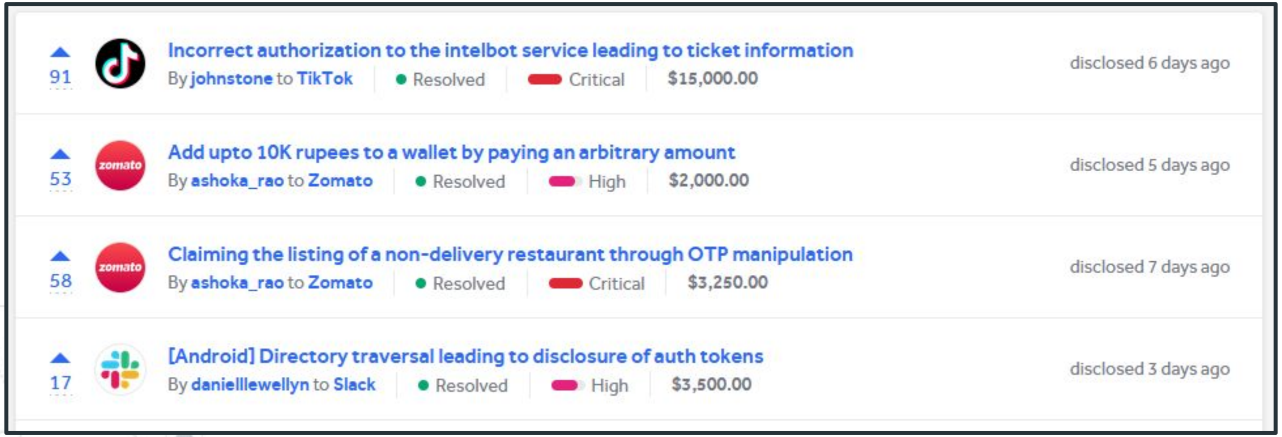
8 Days

RELEASE DATE

Patch Notes

Bug Bounty programs: Learning and getting paid?

- Hackerone.com: Used by most companies
- “Hacktivity” list shows common vulnerabilities
- Site offers training exercises and lessons



▲ 91
Incorrect authorization to the intelbot service leading to ticket information
By johnstone to TikTok | ● Resolved | Critical | $15,000.00
disclosed 6 days ago

▲ 53
Add upto 10K rupees to a wallet by paying an arbitrary amount
By ashoka_rao to Zomato | ● Resolved | High | $2,000.00
disclosed 5 days ago

▲ 58
Claiming the listing of a non-delivery restaurant through OTP manipulation
By ashoka_rao to Zomato | ● Resolved | Critical | $3,250.00
disclosed 7 days ago

▲ 17
[Android] Directory traversal leading to disclosure of auth tokens
By danielllewellyn to Slack | ● Resolved | High | $3,500.00
disclosed 3 days ago

Passwords

Problem: Most users do not use random passwords

- Users with identical passwords have identical hashes

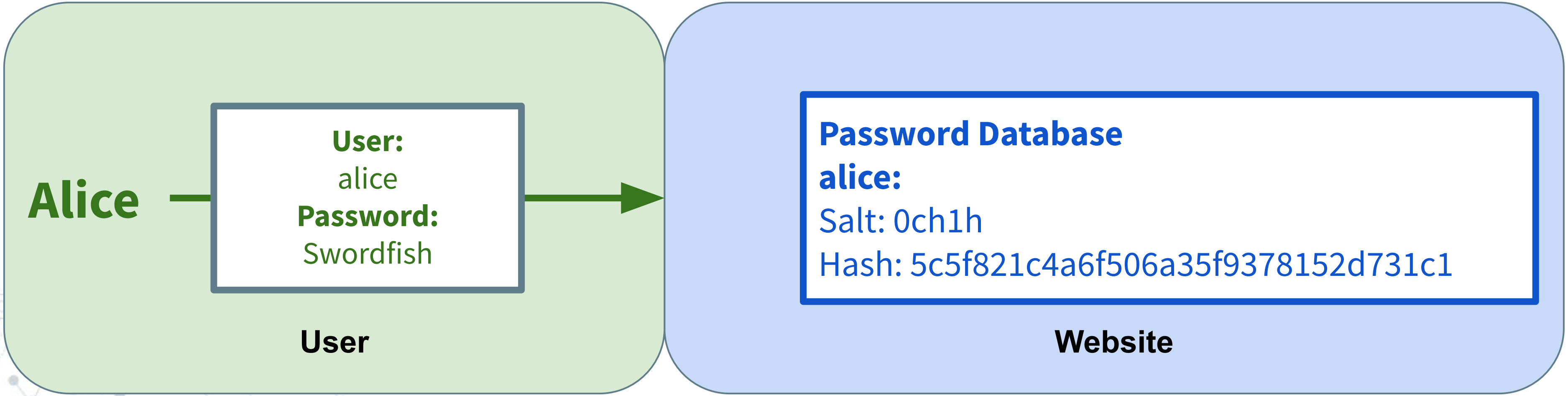
Alice and Bob probably have a very common password!

Password Database
alice:
5c5f821c4a6f506a35f9378152d731c1
Bob:
5c5f821c4a6f506a35f9378152d731c1
Eve:
cc78fe3fc231895879e726ff46a16131

Passwords

Solution: Salts

- Pick a random (non-secret) value, a “salt”, for each user
- Add the salt to the password before hashing it



Alice

User:
alice
Password:
Swordfish

User

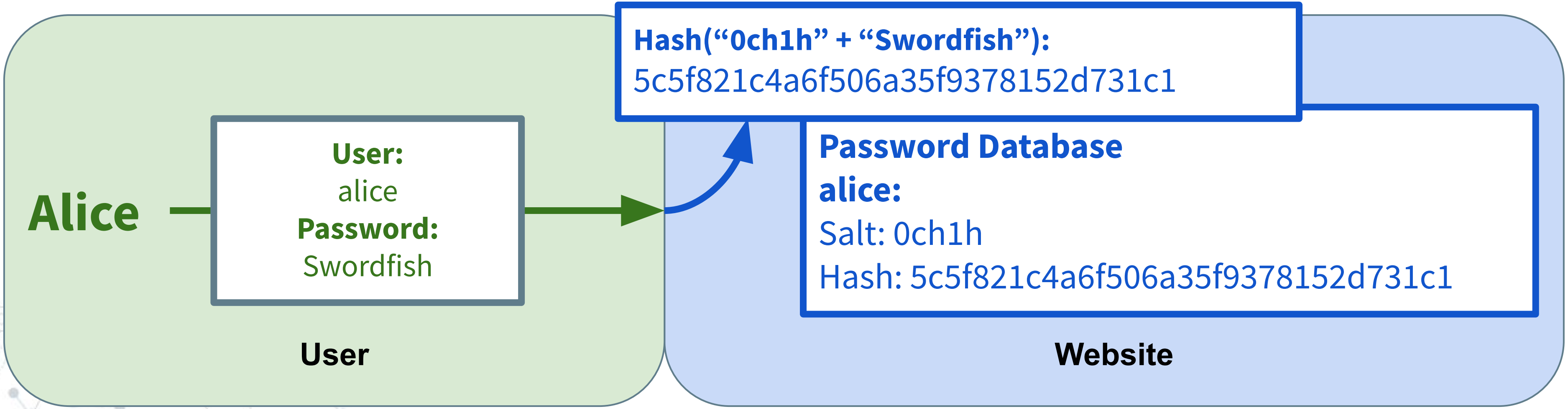
Password Database
alice:
Salt: 0ch1h
Hash: 5c5f821c4a6f506a35f9378152d731c1

Website

Passwords

Solution: Salts

- Pick a random (non-secret) value, a “salt”, for each user
- Add the salt to the password before hashing it



Alice

User:
alice
Password:
Swordfish

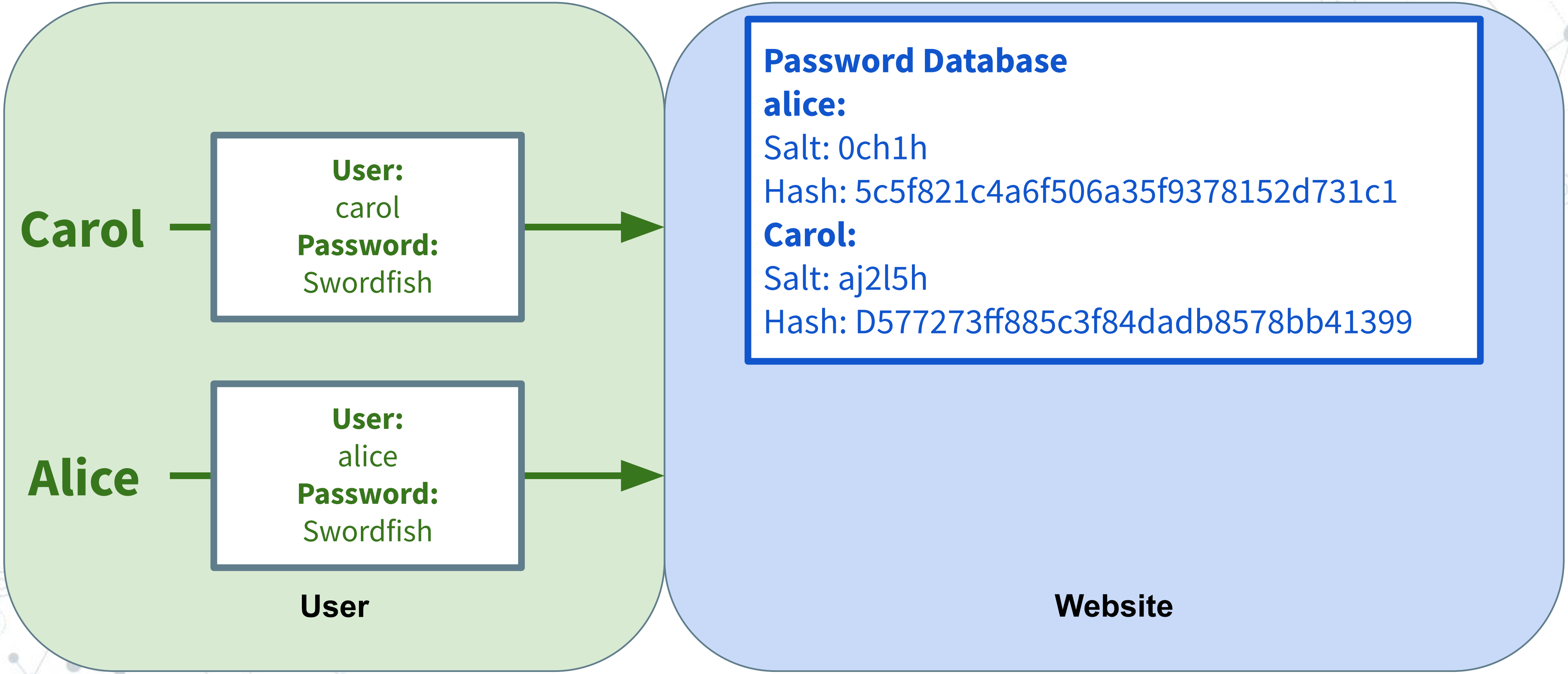
User

Hash(“0ch1h” + “Swordfish”):
5c5f821c4a6f506a35f9378152d731c1

Password Database
alice:
Salt: 0ch1h
Hash: 5c5f821c4a6f506a35f9378152d731c1

Website

Passwords



Carol

User:
carol
Password:
Swordfish

Alice

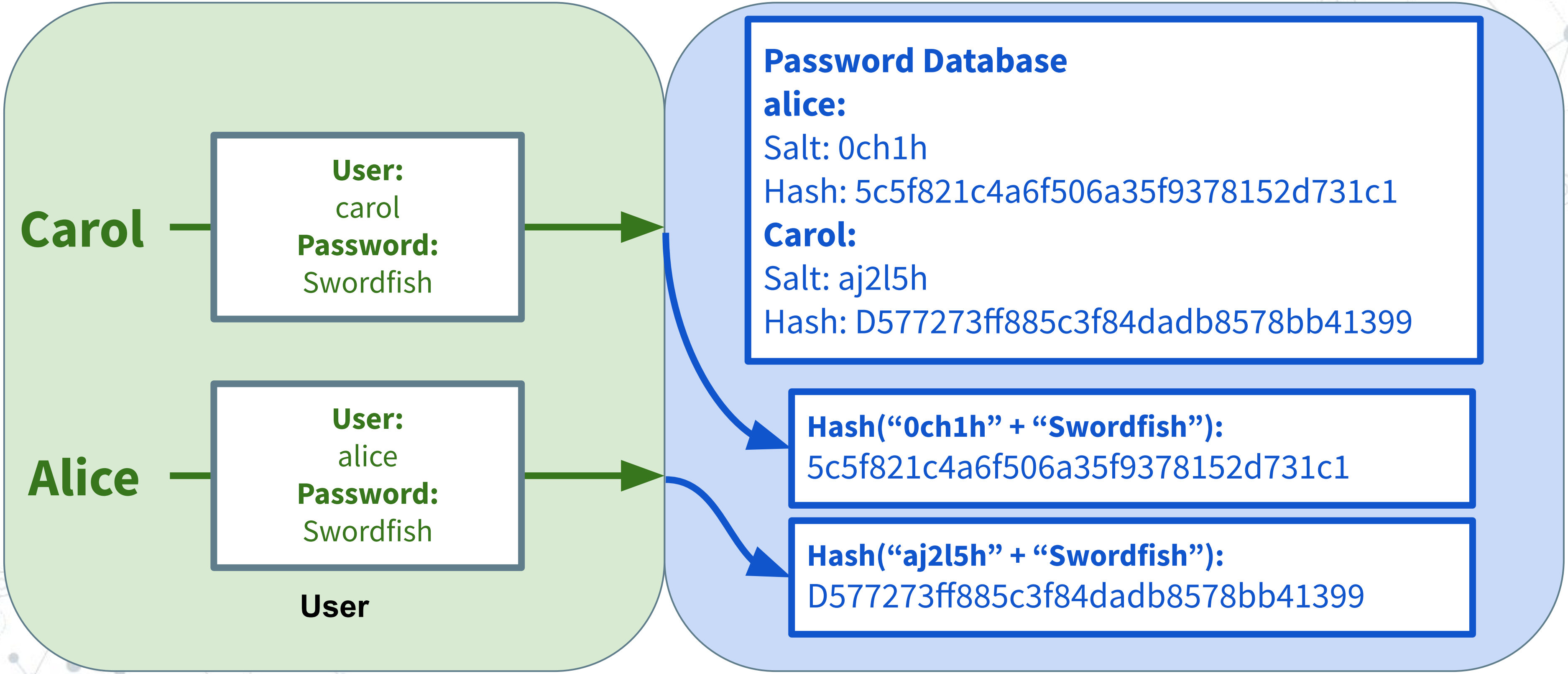
User:
alice
Password:
Swordfish

User

Password Database
alice:
Salt: 0ch1h
Hash: 5c5f821c4a6f506a35f9378152d731c1
Carol:
Salt: aj2l5h
Hash: D577273ff885c3f84dadb8578bb41399

Website

Passwords



Carol

User:
carol
Password:
Swordfish

Alice

User:
alice
Password:
Swordfish

User

Password Database
alice:
Salt: 0ch1h
Hash: 5c5f821c4a6f506a35f9378152d731c1
Carol:
Salt: aj2l5h
Hash: D577273ff885c3f84dadb8578bb41399

Hash("0ch1h" + "Swordfish"):
5c5f821c4a6f506a35f9378152d731c1

Hash("aj2l5h" + "Swordfish"):
D577273ff885c3f84dadb8578bb41399

Passwords

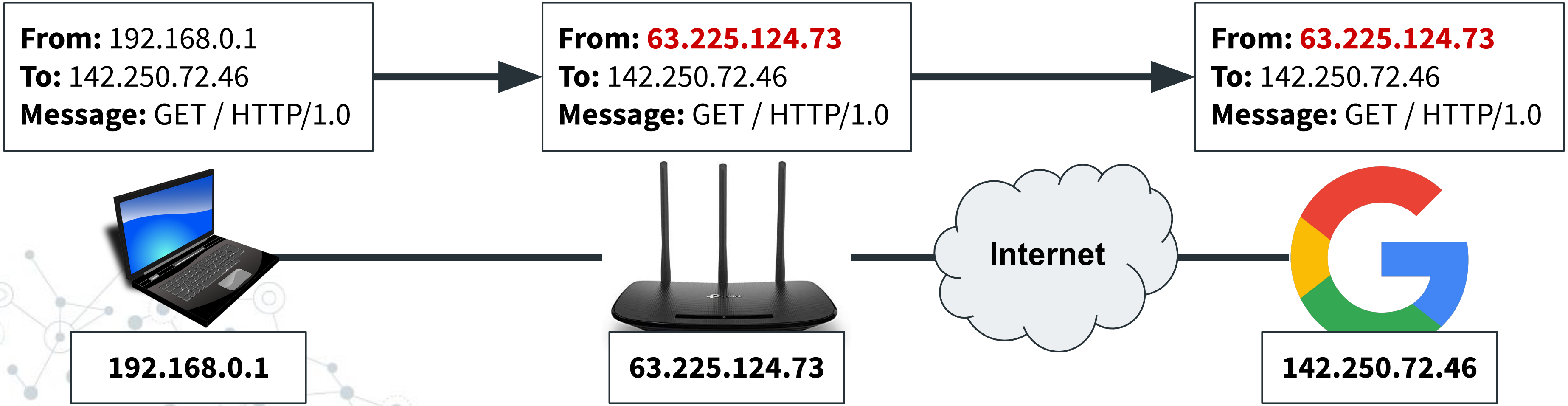
Salts

- Randomizes user hashes, even if the password is the same
  - ***Does not*** slow down the cracking of a single password
  - ***Does*** slow down the cracking of multiple passwords, as each one must be down individually

Password Database
alice:
Salt: 0ch1h | Hash: 5c5f821c4a6f506a35f9378152d731c1
Carol:
Salt: aj2l5h | Hash: D577273ff885c3f84dadb8578bb41399

Private IP addresses

The IP address that websites see is the IP of your router, not your own computer!



From: 192.168.0.1
To: 142.250.72.46
Message: GET / HTTP/1.0

From: 63.225.124.73
To: 142.250.72.46
Message: GET / HTTP/1.0

From: 63.225.124.73
To: 142.250.72.46
Message: GET / HTTP/1.0

Network scanning

Security concern #1:

There are only 4,294,967,296 IP addresses worldwide.

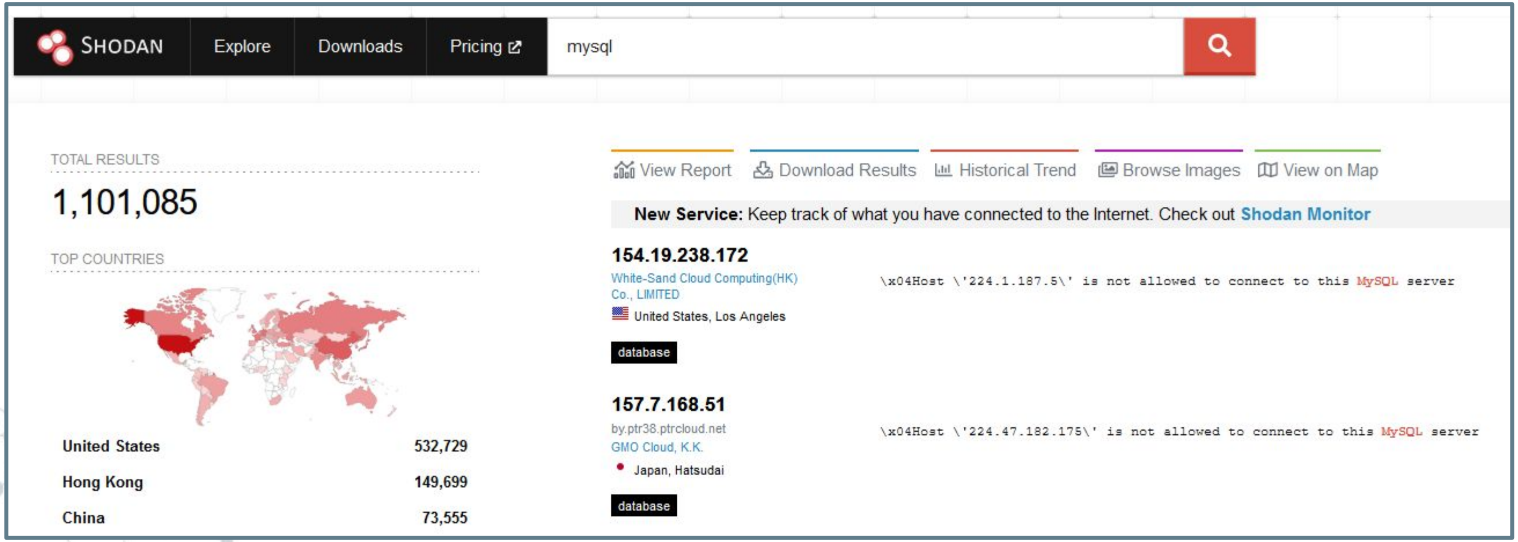
There are only 65,536 ports.

99% of these are unused.

That is not *that* many addresses!

Network scanning

Network scanning: Testing many IP addresses and ports to see which ones are in use (and poorly protected)



TOTAL RESULTS

1,101,085

TOP COUNTRIES

United States	532,729
Hong Kong	149,699
China	73,555

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

154.19.238.172
White-Sand Cloud Computing(HK) Co., LIMITED
United States, Los Angeles
database

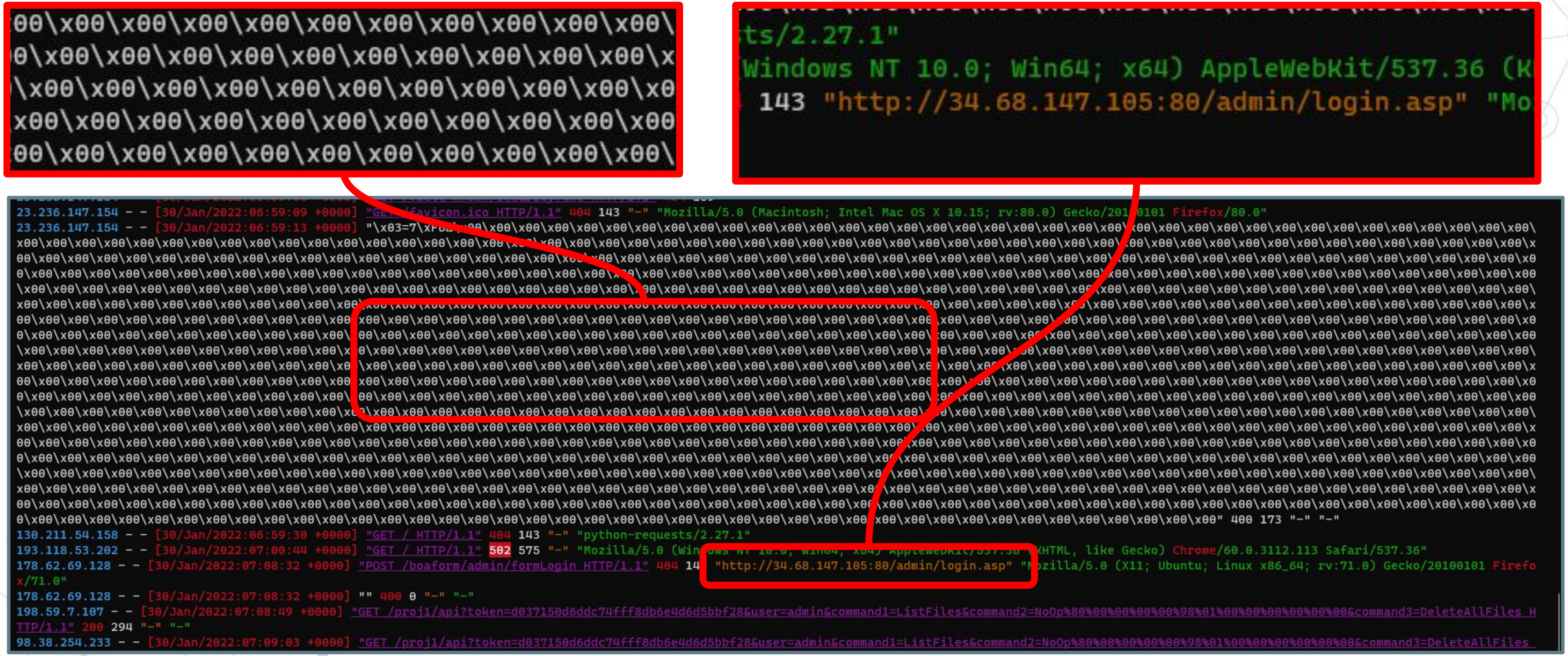
```
\x04Host \'224.1.187.5\' is not allowed to connect to this MySQL server
```

157.7.168.51
by.ptr38.ptrcloud.net
GMO Cloud, K.K.
Japan, Hatsudai
database

```
\x04Host \'224.47.182.175\' is not allowed to connect to this MySQL server
```

shodan.io

Network scanning



```
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
```

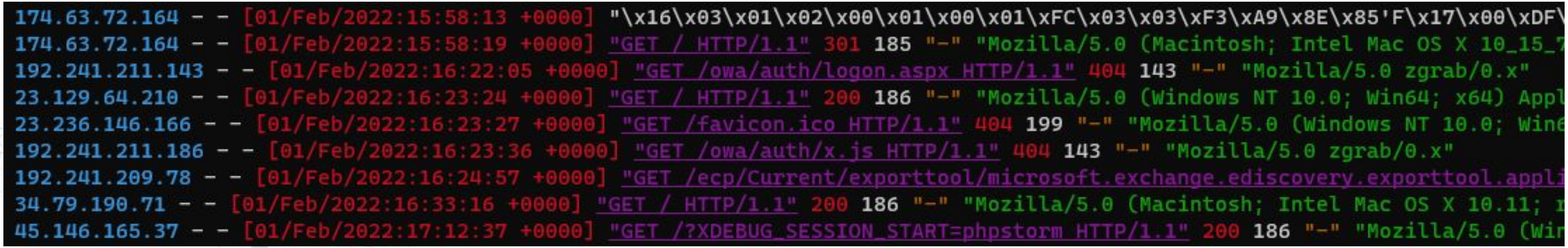
```
ts/2.27.1"
Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
 143 "http://34.68.147.105:80/admin/login.asp" "Mo
```

```
23.236.147.154 - - [30/Jan/2022:06:59:09 +0000] "GET /favicon.ico HTTP/1.1" 404 143 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:80.0) Gecko/20100101 Firefox/80.0"
23.236.147.154 - - [30/Jan/2022:06:59:13 +0000] "\x03=7\xF0a\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00" 400 173 "-" "-"
130.211.54.158 - - [30/Jan/2022:06:59:30 +0000] "GET / HTTP/1.1" 404 143 "-" "python-requests/2.27.1"
193.118.53.202 - - [30/Jan/2022:07:00:44 +0000] "GET / HTTP/1.1" 502 575 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
178.62.69.128 - - [30/Jan/2022:07:08:32 +0000] "POST /boaform/admin/formLogin HTTP/1.1" 404 143 "http://34.68.147.105:80/admin/login.asp" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefo
x/71.0"
178.62.69.128 - - [30/Jan/2022:07:08:32 +0000] "" 400 0 "-" "-"
198.59.7.107 - - [30/Jan/2022:07:08:49 +0000] "GET /proj1/api?token=d037150d6ddc74fff8db6e4d6d5bbf28&user=admin&command1=ListFiles&command2=NoOp%80%00%00%00%00%98%01%00%00%00%00%00%00&command3=DeleteAllFiles H
TTP/1.1" 200 294 "-" "-"
98.38.254.233 - - [30/Jan/2022:07:09:03 +0000] "GET /proj1/api?token=d037150d6ddc74fff8db6e4d6d5bbf28&user=admin&command1=ListFiles&command2=NoOp%80%00%00%00%00%98%01%00%00%00%00%00%00&command3=DeleteAllFiles
```

Network security

Security concern #2: IP data leaks

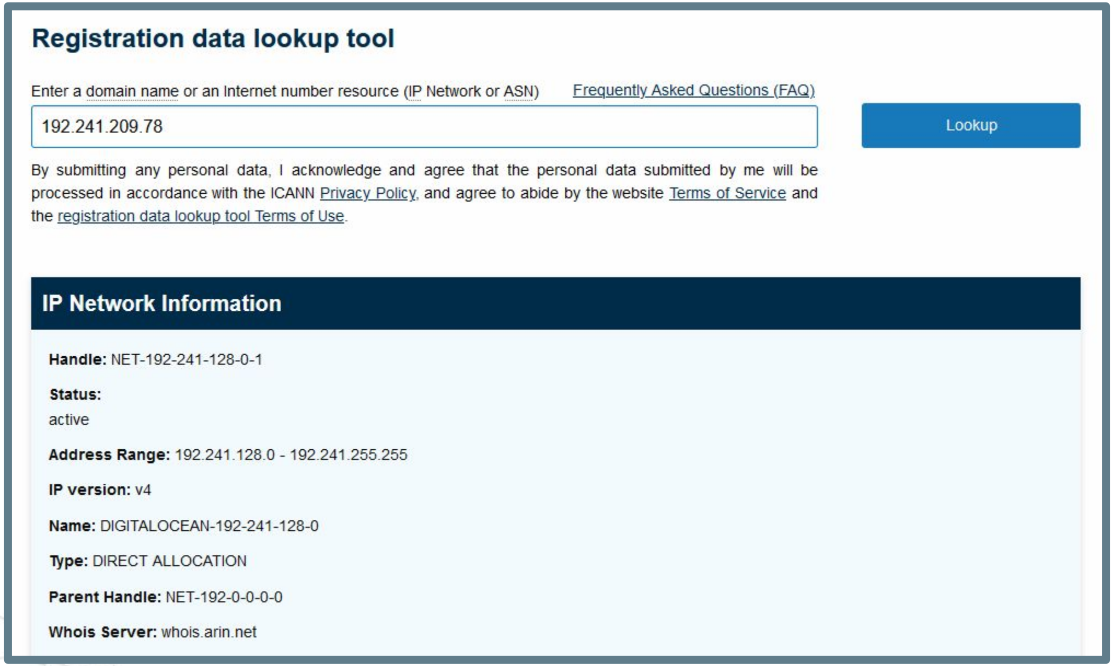
- Your IP address is included with every request
- The owner of an IP address is public knowledge
  - Can be used to find your ISP or cloud provider
  - Roughly correlated with location



```
174.63.72.164 - - [01/Feb/2022:15:58:13 +0000] "\x16\x03\x01\x02\x00\x01\x00\x01\xFC\x03\x03\xF3\xA9\x8E\x85'F\x17\x00\xDF\
174.63.72.164 - - [01/Feb/2022:15:58:19 +0000] "GET / HTTP/1.1" 301 185 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7
192.241.211.143 - - [01/Feb/2022:16:22:05 +0000] "GET /owa/auth/logon.aspx HTTP/1.1" 404 143 "-" "Mozilla/5.0 zgrab/0.x"
23.129.64.210 - - [01/Feb/2022:16:23:24 +0000] "GET / HTTP/1.1" 200 186 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Appl
23.236.146.166 - - [01/Feb/2022:16:23:27 +0000] "GET /favicon.ico HTTP/1.1" 404 199 "-" "Mozilla/5.0 (Windows NT 10.0; Win6
192.241.211.186 - - [01/Feb/2022:16:23:36 +0000] "GET /owa/auth/x.js HTTP/1.1" 404 143 "-" "Mozilla/5.0 zgrab/0.x"
192.241.209.78 - - [01/Feb/2022:16:24:57 +0000] "GET /ecp/Current/exporttool/microsoft.exchange.ediscovery.exporttool.appli
34.79.190.71 - - [01/Feb/2022:16:33:16 +0000] "GET / HTTP/1.1" 200 186 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; r
45.146.165.37 - - [01/Feb/2022:17:12:37 +0000] "GET /?XDEBUG_SESSION_START=phpstorm HTTP/1.1" 200 186 "-" "Mozilla/5.0 (Wir
```

Network security

Public registries: https://lookup.icann.org/lookup



Registration data lookup tool

Enter a domain name or an Internet number resource (IP Network or ASN)   Frequently Asked Questions (FAQ)

192.241.209.78

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN Privacy Policy, and agree to abide by the website Terms of Service and the registration data lookup tool Terms of Use.

IP Network Information

Handle: NET-192-241-128-0-1

Status:
active

Address Range: 192.241.128.0 - 192.241.255.255

IP version: v4

Name: DIGITALOCEAN-192-241-128-0

Type: DIRECT ALLOCATION

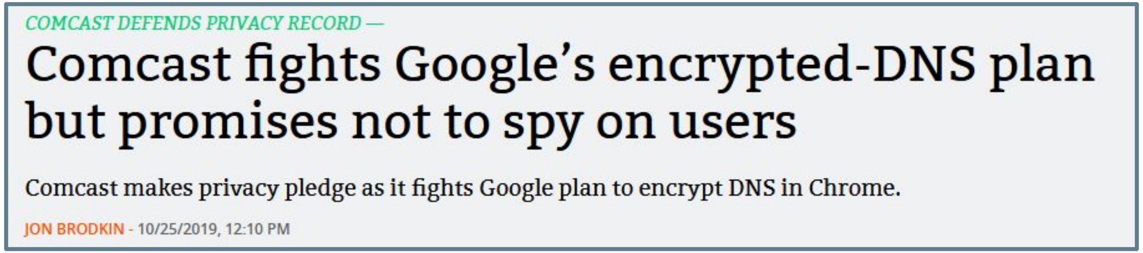
Parent Handle: NET-192-0-0-0-0

Whois Server: whois.arin.net

Network security

Security concern #3: DNS leaks and spoofing

- DNS queries are sometimes unencrypted
- DNS servers are hosted by ISPs or browsers who want your data



COMCAST DEFENDS PRIVACY RECORD —

Comcast fights Google's encrypted-DNS plan but promises not to spy on users

Comcast makes privacy pledge as it fights Google plan to encrypt DNS in Chrome.

JON BRODKIN - 10/25/2019, 12:10 PM

https://arstechnica.com/tech-policy/2019/10/comcast-fights-googles
-encrypted-dns-plan-but-promises-not-to-spy-on-users/

Recap

IP/port scanning: Public IPs only

Public IP information: Public IPs, and related private IPs to a lesser extent

DNS: Not really associated with IP

Good things to know

- How encryption and Certificate Authorities work
- Public IP threats
- Client-side trust