

Uber's subdomains

Recon-ng Espial Linux

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

1 2 3 4

damsith@kali: ~/Desktop/SubDomainizer

File Actions Edit View Help

Selecting previously unselected package mailutils-mh.
Preparing to unpack .../7-mailutils-mh_1%3a3.15-3+b1_amd64.deb ...
Unpacking mailutils-mh (1:3.15-3+b1) ...
Setting up guile-3.0-libs:amd64 (3.0.8-2) ...
Setting up libntlm0:amd64 (1.6-4) ...
Setting up mailutils-common (1:3.15-3) ...
Setting up libgssglue1:amd64 (0.7-1) ...
Setting up libgsasl18:amd64 (2.2.0-1) ...
Setting up gsasl-common (2.2.0-1) ...
Setting up libmailutils9:amd64 (1:3.15-3+b1) ...
Setting up mailutils-mh (1:3.15-3+b1) ...
Processing triggers for libc-bin (2.36-4) ...
Processing triggers for kali-menu (2022.4.1) ...

(damsith@kali)-[~/Desktop/SubDomainizer]
$ nslookup -q=MX DOMAIN_NAME
Server:      108.166.149.2
Address:     108.166.149.2#53

** server can't find DOMAIN_NAME: NXDOMAIN

(damsith@kali)-[~/Desktop/SubDomainizer]
$ nslookup -q=MX uber.com
Server:      108.166.149.2
Address:     108.166.149.2#53

Non-authoritative answer:
uber.com      mail exchanger = 10 alt3.aspmx.l.google.com.
uber.com      mail exchanger = 10 alt4.aspmx.l.google.com.
uber.com      mail exchanger = 5 alt1.aspmx.l.google.com.
uber.com      mail exchanger = 5 alt2.aspmx.l.google.com.
uber.com      mail exchanger = 2 aspmx.l.google.com.

Authoritative answers can be found from:

(damsith@kali)-[~/Desktop/SubDomainizer]
$ apt-get install host
$: command not found

(damsith@kali)-[~/Desktop/SubDomainizer]
$ apt-get install host
E: Could not open lock file /var/lib/dpkg/lock-frontent - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), are you root?

(damsith@kali)-[~/Desktop/SubDomainizer]
$ apt-get install hos
E: Could not open lock file /var/lib/dpkg/lock-frontent - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), are you root?

(damsith@kali)-[~/Desktop/SubDomainizer]
$ apt-get instll hos
```

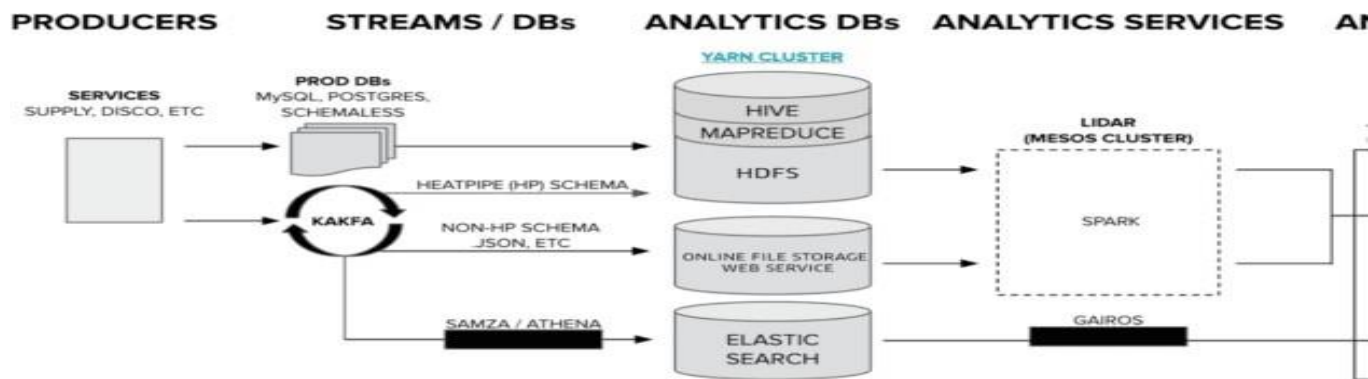
Uber's IP addresses

IP Address Ranges

- [IPv4 Ranges](#)
- [IPv6 Ranges](#)

Netblock	Company	Num of IPs
103.194.230.0/24	UBER SINGAPORE TECHNOLOGY PTE. LTD	256
103.194.231.0/24	UBER SINGAPORE TECHNOLOGY PTE. LTD	256
103.50.92.0/23	Uber Technologies, Inc	512
103.50.92.0/24	Uber Technologies, Inc	256
103.50.93.0/24	Uber Technologies, Inc	256
103.50.94.0/23	Uber Technologies, Inc	512
103.50.94.0/24	Uber Technologies, Inc	256
103.50.95.0/24	Uber Technologies, Inc	256
104.36.192.0/23	Uber Technologies, Inc	512
104.36.192.0/24	Uber Technologies, Inc	256
104.36.194.0/23	Uber Technologies, Inc	512
104.36.194.0/24	Uber Technologies, Inc	256
104.36.195.0/24	Uber Technologies, Inc	256
104.36.196.0/23	Uber Technologies, Inc	512
104.36.196.0/24	Uber Technologies, Inc	256
104.36.197.0/24	Uber Technologies, Inc	256
104.36.198.0/24	Uber Technologies, Inc	256
104.36.199.0/24	Uber Technologies, Inc	256

- **3 List all of Uber's website technology? Type of web server(s)**
- **Language(s)/stack**
- **Database(s) being used**



Python, Mongo also MySQL

Python ,Go,Java,also Node

Who hosts Uber's DNS?

uber.com

Updated 4 minutes ago

Domain Information

Domain:

uber.com

Registrar:

MarkMonitor Inc.

Registered On:

1995-07-14

Expires On:

2028-07-12

Updated On:

2021-12-15

Status:

clientDeleteProhibited

clientTransferProhibited

clientUpdateProhibited

Name Servers:

dns1.p04.nsone.net

dns2.p04.nsone.net

dns3.p04.nsone.net

dns4.p04.nsone.net

edns126.ultradns.biz
edns126.ultradns.com
edns126.ultradns.net
edns126.ultradns.org

Registrant Contact

Organization:
Uber Technologies, Inc.
State:
CA
Country:
US

Email:
Select Request Email Form at
<https://domains.markmonitor.com/whois/uber.com>

Administrative Contact

Organization:
Uber Technologies, Inc.
State:
CA
Country:
US

Email:
Select Request Email Form at
<https://domains.markmonitor.com/whois/uber.com>

Technical Contact

Organization:
Uber Technologies, Inc.
State:
CA
Country:
US

Email:
Select Request Email Form at
<https://domains.markmonitor.com/whois/uber.com>

Raw Whois Data

Domain Name: uber.com

Registry Domain ID: 2564976 DOMAIN COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

Registrar URL: <http://www.markmonitor.com>

Updated Date: 2021-12-15T22:42:22+0000

Creation Date: 1995-07-14T04:00:00+0000

Registrar Registration Expiration Date: 2028-07-12T07:00:00+0000

Registrar: MarkMonitor, Inc.

Registrar IANA ID: 292

Registrar Abuse Contact Email: **abusecomplaints**@markmonitor.com

Registrar Abuse Contact Phone: +1.2086851750

Domain Status: clientUpdateProhibited
(<https://www.icann.org/epp#clientUpdateProhibited>)

Domain Status: clientTransferProhibited
(<https://www.icann.org/epp#clientTransferProhibited>)

Domain Status: clientDeleteProhibited
(<https://www.icann.org/epp#clientDeleteProhibited>)

Registrant Organization: Uber Technologies, Inc.

Registrant State/Province: CA

Registrant Country: US

Registrant Email: Select Request Email Form at
<https://domains.markmonitor.com/whois/uber.com>

Admin Organization: Uber Technologies, Inc.

Admin State/Province: CA

Admin Country: US

Admin Email: Select Request Email Form at
<https://domains.markmonitor.com/whois/uber.com>

Tech Organization: Uber Technologies, Inc.

Tech State/Province: CA

Tech Country: US

Tech Email: Select Request Email Form at
<https://domains.markmonitor.com/whois/uber.com>

Name Server: dns1.p04.nsone.net

Name Server: dns2.p04.nsone.net

Name Server: dns3.p04.nsone.net

Name Server: edns126.ultradns.org

Name Server: edns126.ultradns.net

Name Server: edns126.ultradns.biz

Name Server: dns4.p04.nsone.net

Name Server: edns126.ultradns.com

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System:
<http://wdprs.internic.net/>

>>> Last update of WHOIS database: 2023-01-01T17:42:35+0000 <<<

For more information on WHOIS status codes, please visit:

<https://www.icann.org/resources/pages/epp-status-codes>

If you wish to contact this domain's Registrant, Administrative, or Technical

contact, and such email address is not visible above, you may do so via our web

form, pursuant to ICANN's Temporary Specification. To verify that you are not a

robot, please enter your email address to receive a link to a page that

facilitates email communication with the relevant contact(s).

Web-based WHOIS:

<https://domains.markmonitor.com/whois>

If you have a legitimate interest in viewing the non-public WHOIS details, send

your request and the reasons for your request to **whoisrequest**
@markmonitor.com

and specify the domain name in the subject line. We will review that request and

may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes,

and to assist persons in obtaining information about or related to a domain

name's registration record. While MarkMonitor believes the data to be accurate,

the data is provided "as is" with no guarantee or warranties regarding its

accuracy.

By submitting a WHOIS query, you agree that you will use this data only for

lawful purposes and that, under no circumstances will you use this data to:

(1) allow, enable, or otherwise support the transmission by email, telephone,

or facsimile of mass, unsolicited, commercial advertising, or spam; or

(2) enable high volume, automated, or electronic processes that send queries,

data, or email to MarkMonitor (or its systems) or the domain name contacts (or

its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management (TM)

Protecting companies and consumers in a digital world.

Visit MarkMonitor at <https://www.markmonitor.com>

Contact us at +1.8007459229

In Europe, at +44.02032062220

What are the MX records for Uber?

```
[damsithm@localhost ~]$ nslookup -q =MX uber.com
*** Invalid option: q
nslookup: couldn't get address for 'uber.com': not found
[damsithm@localhost ~]$ nslookup -q=MX gmail.com
Server: 108.166.149.2
Address: 108.166.149.2#53
```

Non-authoritative answer:

```
gmail.com mail exchanger = 30 alt3.gmail-smtp-in.l.google.com.
gmail.com mail exchanger = 20 alt2.gmail-smtp-in.l.google.com.
gmail.com mail exchanger = 40 alt4.gmail-smtp-in.l.google.com.
gmail.com mail exchanger = 10 alt1.gmail-smtp-in.l.google.com.
gmail.com mail exchanger = 5 gmail-smtp-in.l.google.com.
```


Authoritative answers can be found from:

```
[damsithm@localhost ~]$ nslookup -q=MX uber.com
Server: 108.166.149.2
Address: 108.166.149.2#53
```

Non-authoritative answer:

```
uber.com mail exchanger = 10 alt3.aspmx.l.google.com.
uber.com mail exchanger = 10 alt4.aspmx.l.google.com.
uber.com mail exchanger = 5 alt1.aspmx.l.google.com.
uber.com mail exchanger = 5 alt2.aspmx.l.google.com.
uber.com mail exchanger = 2 aspmx.l.google.com.
```

Authoritative answers can be found from:

```
[damsithm@localhost ~]$ nslookup
> ^C[damsithm@localhost ~]$ nslookup
>
Server: 108.166.149.2
Address: 108.166.149.2#53
```

```
** server can't find >: NXDOMAIN
> ^C[damsithm@localhost ~]$ dig -t mx gmail.com
```

```
; <<>> DiG 9.11.36-RedHat-9.11.36-5.el8_7.2 <<>> -t mx gmail.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41254
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 8192
;; QUESTION SECTION:
; gmail.com. IN MX
```

```
;; ANSWER SECTION:
gmail.com. 3600 IN MX 20 alt2.gmail-smtp-in.l.google.com.
gmail.com. 3600 IN MX 5 gmail-smtp-in.l.google.com.
gmail.com. 3600 IN MX 40 alt4.gmail-smtp-in.l.google.com.
gmail.com. 3600 IN MX 10 alt1.gmail-smtp-in.l.google.com.
gmail.com. 3600 IN MX 30 alt3.gmail-smtp-in.l.google.com.
```

```
;; Query time: 30 msec
;; SERVER: 108.166.149.2#53(108.166.149.2)
;; WHEN: Sun Jan 01 13:57:32 EST 2023
```

:: MSG SIZE rcvd: 161

[damsithm@localhost ~]\$ dig -t mx uber.com

; <<>> DiG 9.11.36-RedHat-9.11.36-5.el8_7.2 <<>> -t mx uber.com
;; global options: +cmd

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35786
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 8192
;; QUESTION SECTION:
; uber.com. IN MX

;; ANSWER SECTION:
uber.com. 100 IN MX 10 alt3.aspmx.l.google.com.
uber.com. 100 IN MX 10 alt4.aspmx.l.google.com.
uber.com. 100 IN MX 5 alt1.aspmx.l.google.com.
uber.com. 100 IN MX 5 alt2.aspmx.l.google.com.
uber.com. 100 IN MX 2 aspmx.l.google.com.

;; Query time: 47 msec
;; SERVER: 108.166.149.2#53(108.166.149.2)
;; WHEN: Sun Jan 01 13:57:47 EST 2023
;; MSG SIZE rcvd: 152

[damsithm@localhost ~]\$ dig +short mx uber.com
10 alt3.aspmx.l.google.com.
10 alt4.aspmx.l.google.com.
5 alt1.aspmx.l.google.com.
5 alt2.aspmx.l.google.com.
2 aspmx.l.google.com.

What are the whois points of contact?

Registrant Contact

Organization: Uber Technologies, Inc.
State: CA
Country: US
Email:

Select Request Email Form at
<https://domains.markmonitor.com/whois/uber.com>

Administrative Contact

Organization:
Uber Technologies, Inc.
State:
CA
Country:
US

Email:
Select Request Email Form at
<https://domains.markmonitor.com/whois/uber.com>

Technical Contact

Organization:
Uber Technologies, Inc.
State:
CA
Country:
US

Email:
Select Request Email Form at
<https://domains.markmonitor.com/whois/uber.com>

Identify 10 people that work at Uber ?



Login

Client Login

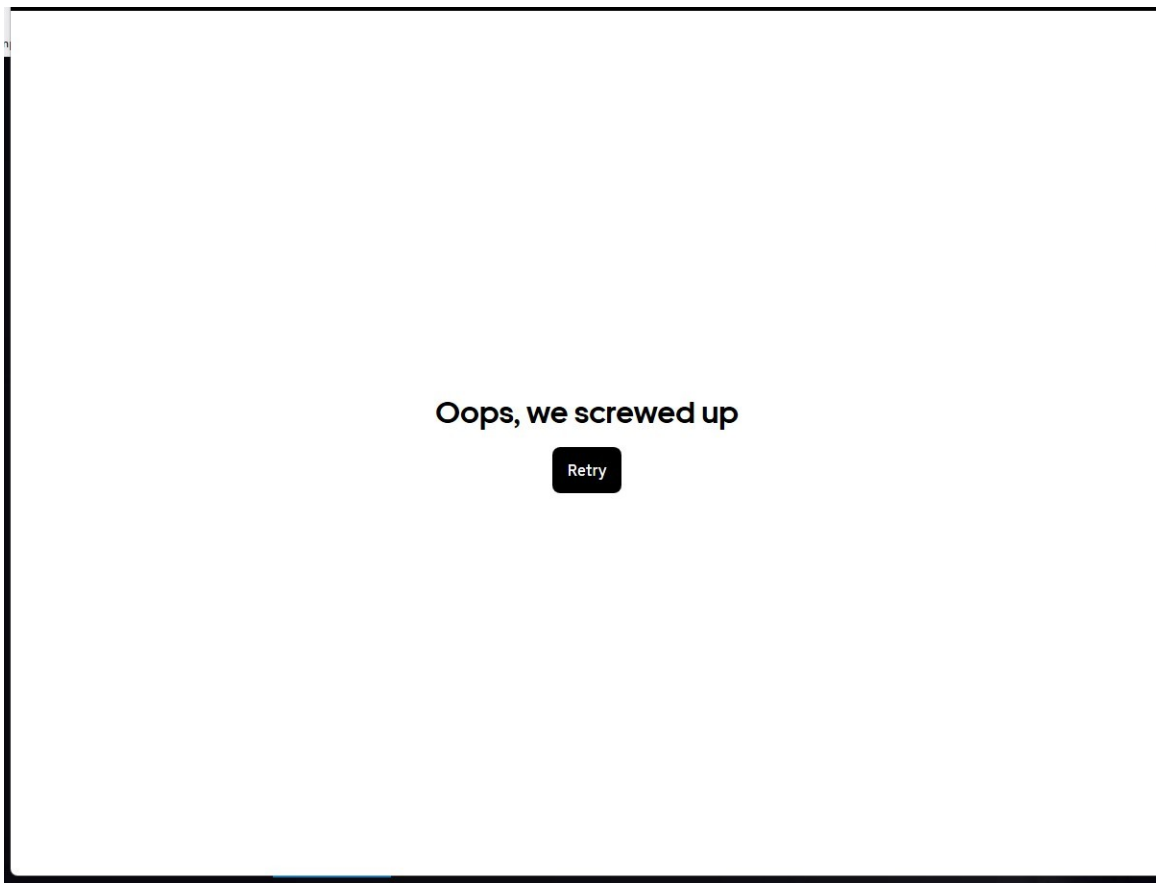
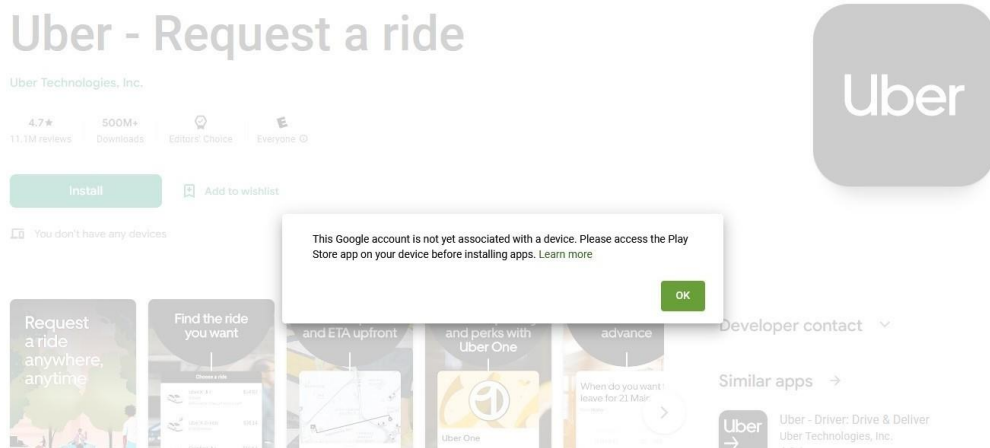
E-Mail or Username:

Password:

[Forgot password?](#)

Tried to register for account could not get individuals email addresses web recon doesn't download for me

Was any Uber application source code obtainable? No in both instances this does not work tried windows app store tried download uber app did not work did however download and installed google play store as you can see require android device order proceed even though I have a google account



What type of corporation is Uber?

Uber headquarters in started San Francisco
Transportation service,

How many services were discovered running on Uber's servers and what are they?

How many services were discovered running on Uber's servers and what are they?

```
(damsith@kali)-[~]  
$ nmap uber.com  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-01 15:01 CST  
Nmap scan report for uber.com (34.98.127.226)  
Host is up (0.021s latency).  
rDNS record for 34.98.127.226: 226.127.98.34.bc.googleusercontent.com  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp   open  https
```

Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds

```
(damsith@kali)-[~]
```

What is the naming convention of employee email addresses?

medium confidence

first_name last_name

score 2

(found Apr 2015 -)

gaurav@uber.com

score 1

(found Jul 2015 -)

leandre@uber.com

score 1

(found Jan 2014 -)

casper@uber.com

score 0

(found Mar 2014 -)

supporttoronto@uber.com

score 0

(found Jan 2014 -)

michellec@uber.com

score 0

(found Mar 2014 -)

marshall@uber.com

score 0

(found Aug 2015 -)

steeleinmusic@uber.com

score 0

(found Jul 2013 - www.steeleinmusic.com/blogs)

jinsun@uber.com

score 0

(found Jan 2014 -)

rachelm@uber.com

score 0

(found Feb 2014 -)

supportatl@uber.com

score 0

(found Dec 2013 -)

supportboston@uber.com

score 0

(found Feb 2014 -)

alin@uber.com

score 0

(found Mar 2015 -)

supportny@uber.com

score 0

(found Dec 2013 -)

amos@uber.com

score 0

(found Jan 2015 -)

whodunit@uber.com

score 0

(found Jul 2013 - www.uber.com)

supportsf@uber.com

score 0

(found Jan 2014 -)

supportmsp@uber.com

score 0

(found Apr 2014 -)

start@uber.com

score 0

(found Jul 2013 - start.uber.com)

supportseattle@uber.com

score 0

(found Jan 2014 -)

nyccm@uber.com

score 0

(found Mar 2014 -)

caitlin@uber.com

score 0

(found Sep 2013 - www.debbieschlussel.com/archives/2008/03)

supportdc@uber.com

score 0

(found Jan 2014 -)

supportsingapore@uber.com

score 0

(found Feb 2014 -)

aditya.phulwani@uber.com

score 0

(found Jul 2015 -)

supportla@uber.com

score 0

(found Dec 2013 -)

20supportdc@uber.com

score 0

(found Feb 2014 -)

supportmelbourne@uber.com

score 0

(found Mar 2015 -)

supportroma@uber.com

score 0

(found Dec 2013 -)

blaine@uber.com

score 0

(found Feb 2015 -)

supportdallas@uber.com

score 0

(found Jun 2014 -)

rockvine@uber.com

score 0

(found Jul 2013 - rockvine.uber.com/blogs)

supportsydney@uber.com

score 0

(found Jan 2014 -)

salle@uber.com

score 0

(found Mar 2014 -)

mack@uber.com

score 0

(found Oct 2013 - www.wrwalker.com)

supportsd@uber.com

score 0

(found Mar 2014 -)

archana.ashar@uber.com

score 0

(found Jul 2015 -)

emailsupport@uber.com

score 0

(found Dec 2013 -)

cait@uber.com

score 0

(found Dec 2013 -)

supportphx@uber.com

Mark as:  Real Person  Bad Address

score 0

(found Mar 2015 -)

e.g. JohnSmith@uber.com

low confidence

first_name



e.g. John@uber.com

last_name



e.g. Smith@uber.com

first_name last_initial



e.g. JohnS@uber.com

last_name first_initial



e.g. SmithJ@uber.com

first_initial last_name



e.g. JSmith@uber.com

first_name _ last_initial



e.g. John_S@uber.com

first_name _ last_name




e.g. John_Smith@uber.com

first_name . last_name



e.g. John.Smith@uber.com

What employee email addresses were found?



Login

Client Login

E-Mail or Username:

Password:

Login

[Forgot password?](#)

Tried to register for account could not get individuals email addresses web recon doesn't download for me can't login

What versions of SSL are supported?

**slscan uber.com
Version: 2.0.15-static
OpenSSL 1.1.1q-dev xx XXX xxxx**

Connected to 34.98.127.226

Testing SSL server uber.com on port 443 using SNI name uber.com

SSL/TLS Protocols:

SSLv2 disabled

SSLv3 disabled

TLSv1.0 disabled

TLSv1.1 disabled

TLSv1.2 enabled

TLSv1.3 enabled

TLS Fallback SCSV:

Server supports TLS Fallback SCSV

TLS renegotiation:

Session renegotiation not supported

TLS Compression:

Compression disabled

Heartbleed:

TLSv1.3 not vulnerable to heartbleed

TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):

Preferred TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253

Accepted TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253

Accepted TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253

Preferred TLSv1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253

Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253

Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253

Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253

Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve 25519 DHE 253

Accepted TLSv1.2 128 bits AES128-GCM-SHA256

Accepted TLSv1.2 256 bits AES256-GCM-SHA384

Accepted TLSv1.2 128 bits AES128-SHA

Accepted TLSv1.2 256 bits AES256-SHA

Server Key Exchange Group(s):

TLSv1.3 128 bits secp256r1 (NIST P-256)

TLSv1.3 128 bits x25519

TLSv1.2 128 bits secp256r1 (NIST P-256)

TLSv1.2 128 bits x25519

SSL Certificate:

Signature Algorithm: sha256WithRSAEncryption

RSA Key Strength: 2048

Subject: *.uber.com


Altnames: DNS:*.uber.com, DNS:uber.com

Issuer: DigiCert TLS RSA SHA256 2020 CA1

Not valid before: Sep 30 00:00:00 2022 GMT

Not valid after: Oct 3 23:59:59 2023 GMT

How many APIs were discovered?



Login

Client Login

E-Mail or Username:

Password:

Login

Forgot password?

does not download from the site not working for me after account creation
freetrial does not work

What are the highest risk vulnerabilities found?

INFO

Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

- Port 80/tcp was found to be open
To see debug logs, please visit individual host

Port

80 / tcp

Hosts

uber.com

- Port 246/tcp was found to be open
To see debug logs, please visit individual host

Port

246 / tcp

Hosts

uber.com

- Port 443/tcp was found to be open
To see debug logs, please visit individual host

Port

443 / tcp

Hosts

uber.com

- Port 519/tcp was found to be open
To see debug logs, please visit individual host

Port**519 / tcp**

- Port 693/tcp was found to be open
To see debug logs, please visit individual host

Port**693 / tcp**

- Port 723/tcp was found to be open
To see debug logs, please visit individual host

Port**723 / tcp**

- Port 1040/tcp was found to be open
To see debug logs, please visit individual host

Port**1040 / tcp**

- Port 1097/tcp was found to be open
To see debug logs, please visit individual host

Port**1097 / tcp**

- Port 1253/tcp was found to be open
To see debug logs, please visit individual host

Port**1253 / tcp**

- Port 1459/tcp was found to be open
To see debug logs, please visit individual host

Port**1459 / tcp**

- Port 1499/tcp was found to be open
To see debug logs, please visit individual host

Port**1499 / tcp**

- Port 1781/tcp was found to be open
To see debug logs, please visit individual host

Port**1781 / tcp**

- Port 1872/tcp was found to be open
To see debug logs, please visit individual host

Port**1872 / tcp**

- Port 1927/tcp was found to be open
To see debug logs, please visit individual host

Port**1927 / tcp**

- Port 2342/tcp was found to be open
To see debug logs, please visit individual host

Hostsuber.com**Hosts**uber.com**Hosts**uber.com**Hos**[ube](https://uber.com)**Hos**[ube](https://uber.com)**Hos**[ube](https://uber.com)**Hos**[ube](https://uber.com)**Hos**[ube](https://uber.com)**Hos**[ube](https://uber.com)**Hos**[ube](https://uber.com)**Hos**[ube](https://uber.com)

Port**2342 / tcp**

- Port 2405/tcp was found to be open
To see debug logs, please visit individual host

Port**2405 / tcp**

- Port 2448/tcp was found to be open
To see debug logs, please visit individual host

Port**2448 / tcp**

- Port 2458/tcp was found to be open
To see debug logs, please visit individual host

Port**2458 / tcp**

- Port 2559/tcp was found to be open
To see debug logs, please visit individual host

Port**2559 / tcp**

- Port 2633/tcp was found to be open
To see debug logs, please visit individual host

Port**2633 / tcp**

- Port 2721/tcp was found to be open
To see debug logs, please visit individual host

Port**2721 / tcp**

- Port 2993/tcp was found to be open
To see debug logs, please visit individual host

Port**2993 / tcp**

- Port 3165/tcp was found to be open
To see debug logs, please visit individual host

Port**3165 / tcp**

- Port 3364/tcp was found to be open
To see debug logs, please visit individual host

Port**3364 / tcp**

- Port 3374/tcp was found to be open
To see debug logs, please visit individual host

Port**3374 / tcp**

- Port 3452/tcp was found to be open
To see debug logs, please visit individual host

Port**3452 / tcp**

- Port 3545/tcp was found to be open
To see debug logs, please visit individual host

Port**3545 / tcp**

- Port 3595/tcp was found to be open
To see debug logs, please visit individual host

Port**3595 / tcp**

- Port 3627/tcp was found to be open
To see debug logs, please visit individual host

Port**3627 / tcp**

- Port 4885/tcp was found to be open
To see debug logs, please visit individual host

Port**4885 / tcp**

- Port 8206/tcp was found to be open
To see debug logs, please visit individual host

Port**8206 / tcp**

- Port 8733/tcp was found to be open
To see debug logs, please visit individual host

Port**8733 / tcp**

- Port 9909/tcp was found to be open
To see debug logs, please visit individual host

Port**9909 / tcp**

- Port 10607/tcp was found to be open
To see debug logs, please visit individual host

Port**10607 / tcp**

- Port 33568/tcp was found to be open
To see debug logs, please visit individual host

Port**33568 / tcp**

- Port 43188/tcp was found to be open
To see debug logs, please visit individual host

Port**43188 / tcp**

- Port 47000/tcp was found to be open
To see debug logs, please visit individual host

Port

47000 / tcp

What banner information was obtained?

dmitry -pb 104.36.192.0

Deepmagic Information Gathering Tool

"There be some deep magic going on"

ERROR: Unable to locate Host Name for 104.36.192.0

Continuing with limited modules

HostIP:104.36.192.0

HostName:

Gathered TCP Port information for 104.36.192.0

Port	State
------	-------

—(root@kali)-[~]

└─# dmitry -pb 104.36.192.0

Deepmagic Information Gathering Tool

"There be some deep magic going on"

ERROR: Unable to locate Host Name for 104.36.192.0

Continuing with limited modules

HostIP:104.36.192.0

HostName:

Gathered TCP Port information for 104.36.192.0

Port	State
------	-------

Do any Uber websites support BASIC authentication?

Web recon, Espial

E-Mail or Username:

Password:

[Login](#) [Forgot password?](#)

Espial does not download or work aftrter account creation still does not work

```
> curl spydersec.com/run
{"Result": "Success"}
Time Elapses...
> curl spydersec.com/status
{"Status": "Complete"}
> curl spydersec.com/output
Download complete!

Powerful, yet easy!
```

Enterprise Risk Rating
Inventory Validation
External Footprint Identification
Dozens of Data Points Returned
Wide and Deep Detection
Actionable Information
Robust API
Easy to Use/Understand

[illegible]

Web recon, Espial

Client Login

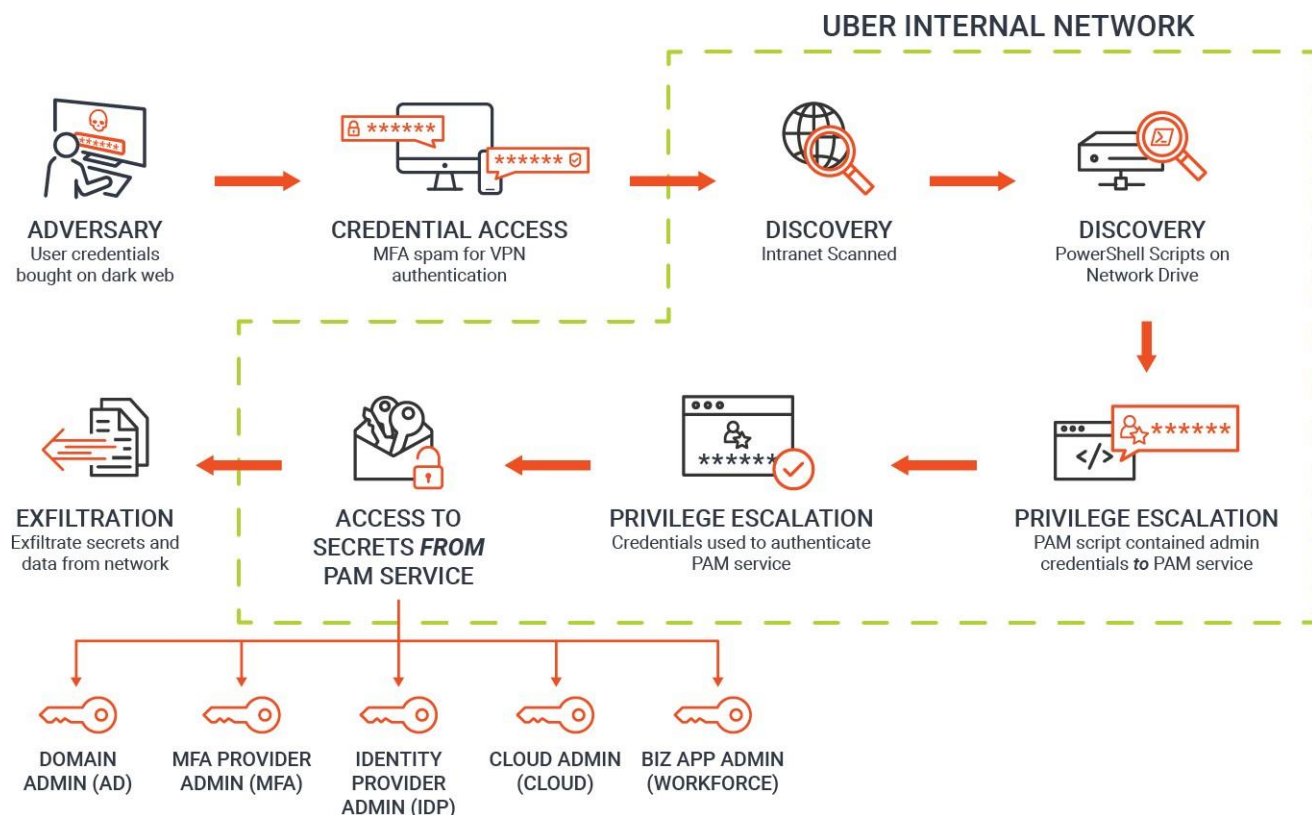
E-Mail or Username:

Password:

[Forgot password?](#)

does not download from the site not working for me after account creation
fretrial does not work

What is Uber's biggest cyber security risk?



Uber IT enviroment by gaining access to credentials to uber vpn
common contractor who do noy have special preivilages to sensitive
resources to network which exposes a power shell script to attacker
preivilage esclation Access PAM System by having hard corded admin
creditials for privilege access mangntment solution the attacker was futher
open privileges

data Exfiltration while uber is still investigation the incident the company confirmed attacker download slack messages as well access download information from internal tool our finance team to manage some invoices these are some security risks at uber

Referenes

<https://theappsolutions.com/blog/development/uber-tech-stack/>

<https://www.whois.com/whois/uber.com>