Penetration Test Report

APP 100-M4-1-Final Assignment

Peter Treacy

August 19, 2023

This penetration test report contains sensitive and confidential information about the security of the tested system. It is intended solely for the use of the organization that commissioned the penetration test and its authorized personnel. Unauthorized access, distribution, or disclosure of this report, in whole or in part, is strictly prohibited.

The information contained in this penetration test report is based on the findings and observations made during the testing period. While every effort has been made to ensure the accuracy of this report, it is not possible to guarantee complete security. The security landscape is continually evolving, and new vulnerabilities may emerge after the completion of this test. The organization that commissioned this penetration test should use this report as a tool to improve security but should not consider it an exhaustive assessment.

The penetration testers involved in this assessment have conducted the test in accordance with industry best practices and ethical guidelines. However, the organization acknowledges that the penetration testers may have caused potential disruption or damage to the systems being tested inadvertently. The organization assumes full responsibility for any such disruptions and releases the testers from liability for any unintentional harm caused.

Contact Information:

For questions, clarifications, or further assistance regarding this penetration test report, please contact:

Peter Treacy
Student- Flatiron School
(845) 661-5877
treacy.peter7@gmail.com

DigiCert Global Root CA
SHA256 2020 CA1
Subject Name: Uber
Country or Region: US
State/Province: California
Locality: San Francisco
Organization: Uber Technologies, Inc
Common Name *.uber.com
Issued by: DigiCert TLS RSA SHA256 2020 CA1
Expires: Wednesday, July 31, 2024 at 4:59:59 PM Pacific Daylight Time

host	ip_address	module
activedirectory-dca1.uber.com	192.168.108.110	hackertarget
activedirectory-sjc1.uber.com	192.168.44.110	hackertarget
activedirectory.uber.com	192.168.44.110	hackertarget
api-an-settlement.uber.com	34.243.40.136	hackertarget
backup.uber.com	207.231.168.151	hackertarget
bastion-dca.uber.com	104.36.195.186	hackertarget
bastion-dca8.uber.com	104.36.195.188	hackertarget
bastion-geo.uber.com	104.36.195.187	hackertarget
bastion-phx.uber.com	104.36.197.131	hackertarget
bastion-phx2.uber.com	104.36.196.134	hackertarget
blogapi.uber.com	208.93.16.10	hackertarget
bounce.uber.com	192.28.144.217	hackertarget
brandarchive.uber.com	104.130.42.190	hackertarget
click.et.uber.com	198.245.92.61	hackertarget
cn-dc1-staging.uber.com	104.36.192.150	hackertarget
cn-dc1.uber.com	104.36.192.148	hackertarget
cn-dca-staging.uber.com	104.36.192.150	hackertarget
cn-dca.uber.com	104.36.192.148	hackertarget
cn-ecg.cfe.uber.com	34.98.127.226	hackertarget
cn-phx-staging.uber.com	104.36.197.138	hackertarget
cn-phx.uber.com	104.36.197.136	hackertarget
cn-staging.cfe.uber.com	130.211.23.192	hackertarget

cn.cfe.uber.com	35.201.81.34	hackertarget
dba.usuppliers.uber.com	207.231.171.31	hackertarget
dev.usuppliers.uber.com	207.231.169.199	hackertarget
email.uber.com	34.98.127.226	hackertarget
fake.uber.com	127.0.0.1	hackertarget
freightembeddedanalytics.uber.com	44.224.52.223	hackertarget
health.uber.com	34.98.127.226	hackertarget
ittools01-dmz1.prod.uber.com	97.64.98.164	hackertarget
kerberos.uber.com	10.6.0.74	hackertarget
lab.usuppliers.uber.com	207.231.169.245	hackertarget
ldap.uber.com	10.30.14.3	hackertarget
logs.uber.com	10.6.0.1	hackertarget
logs2.uber.com	10.6.0.1	hackertarget
metrics.uber.com	10.6.0.1	hackertarget
mgmt.uber.com	204.51.170.233	hackertarget
mta.et.uber.com	198.245.86.114	hackertarget
mta10.et.uber.com	198.245.86.116	hackertarget
mta11.et.uber.com	136.147.138.193	hackertarget
mta12.et.uber.com	136.147.138.194	hackertarget
mta13.et.uber.com	136.147.138.195	hackertarget
mta14.et.uber.com	136.147.138.196	hackertarget
mta15.et.uber.com	136.147.138.197	hackertarget
mta16.et.uber.com	136.147.138.198	hackertarget
mta17.et.uber.com	136.147.138.199	hackertarget
mta18.et.uber.com	136.147.138.200	hackertarget
mta19.et.uber.com	136.147.138.201	hackertarget
mta2.et.uber.com	136.147.138.172	hackertarget
mta20.et.uber.com	136.147.138.202	hackertarget
mta21.et.uber.com	136.147.184.63	hackertarget

mta22.et.uber.com	136.147.184.181	hackertarget
mta23.et.uber.com	136.147.184.183	hackertarget
mta24.et.uber.com	13.111.64.154	hackertarget
mta25.et.uber.com	13.111.64.155	hackertarget
mta26.et.uber.com	13.111.64.156	hackertarget
mta27.et.uber.com	13.111.64.157	hackertarget
mta28.et.uber.com	13.111.64.158	hackertarget
mta29.et.uber.com	13.111.64.173	hackertarget
mta3.et.uber.com	136.147.138.173	hackertarget
mta30.et.uber.com	13.111.64.174	hackertarget
mta31.et.uber.com	13.111.64.175	hackertarget
mta32.et.uber.com	13.111.64.176	hackertarget
mta33.et.uber.com	13.111.64.177	hackertarget
mta4.et.uber.com	136.147.138.174	hackertarget
mta5.et.uber.com	136.147.138.175	hackertarget
mta6.et.uber.com	136.147.138.176	hackertarget
mta7.et.uber.com	136.147.138.178	hackertarget
mta8.et.uber.com	136.147.138.179	hackertarget
mta9.et.uber.com	198.245.86.115	hackertarget
o10.email.uber.com	50.31.36.130	hackertarget
o11.email.uber.com	50.31.36.134	hackertarget
o12.email.uber.com	50.31.36.137	hackertarget
o13.email.uber.com	50.31.36.14	hackertarget
o14.email.uber.com	50.31.36.143	hackertarget
o15.email.uber.com	50.31.36.149	hackertarget
o16.email.uber.com	167.89.40.119	hackertarget
o17.email.uber.com	167.89.42.131	hackertarget
o18.email.uber.com	167.89.42.140	hackertarget
o19.email.uber.com	167.89.42.142	hackertarget

o2.email.uber.com	192.254.112.88	hackertarget
o20.email.uber.com	167.89.42.166	hackertarget
o21.email.uber.com	167.89.42.176	hackertarget
o22.email.uber.com	167.89.42.251	hackertarget
o23.email.uber.com	167.89.42.46	hackertarget
o24.email.uber.com	167.89.42.88	hackertarget
o25.email.uber.com	167.89.44.106	hackertarget
o3.email.uber.com	192.254.112.89	hackertarget
o4.email.uber.com	167.89.12.210	hackertarget
o8.email.uber.com	167.89.17.53	hackertarget
o9.email.uber.com	50.31.36.127	hackertarget
pages.et.uber.com	198.245.92.62	hackertarget
partners-testing.uber.com	204.51.170.236	hackertarget
pat.usuppliers.uber.com	207.231.169.199	hackertarget
prj.usuppliers.uber.com	207.231.169.199	hackertarget
registration.uber.com	192.168.46.229	hackertarget
reset.uber.com	192.168.46.229	hackertarget
rpt.usuppliers.uber.com	207.231.169.199	hackertarget
sbx.usuppliers.uber.com	207.231.171.31	hackertarget
science.uber.com	173.1.57.101	hackertarget
sftp-dca.uber.com	104.36.192.149	hackertarget
sit.usuppliers.uber.com	207.231.171.31	hackertarget
sup.usuppliers.uber.com	207.231.169.199	hackertarget
tst.usuppliers.uber.com	207.231.169.199	hackertarget
uat.usuppliers.uber.com	207.231.171.31	hackertarget
usuppliers.uber.com	207.231.169.247	hackertarget
vault-dca1.uber.com	104.36.194.200	hackertarget
view.et.uber.com	198.245.92.63	hackertarget
z.uber.com	52.2.56.64	hackertarget

Uber's Website/Server Technology

Analytics - Google Analytics, Facebook Pixel
Widgets- Facebook
JavaScript Libraries - core-.js (3.28.0)
Tag Managers - Tealium, Google Tag Manager

Source: www.Bisnow.com (02/13/2023)

Uber is ditching its own data centers in favor of the cloud. The San Francisco-based ride-hailing giant is switching from largely operating its own IT infrastructure to using cloud platforms operated by Google and Oracle, the companies announced Monday in separate releases. Uber signed seven-year agreements with both cloud providers, and it plans to fully migrate from its self-operated data center assets and close those facilities in the coming months.

Around 95% of Uber's IT infrastructure is housed in data centers it owns or leases from colocation providers, according to The Wall Street Journal. Experts say this makes Uber an outlier among tech companies of similar scale, most of whom have long been outsourcing sizable chunks of their computing needs to cloud giants like Google, Amazon Web Services or Microsoft.

"At the end of the day, everyone's looking to cut internal costs so they can maximize their profits," said Gartner Vice President Sid Nag, according to the WSJ. "I think this was an inevitable outcome for a company like Uber. They eventually had to do this."

Indeed, the use of cloud platforms — where computing power is purchased as a service from a third party — is often less expensive than self-operated data centers and makes it far easier for a company to scale its computing resources up or down as needed. Since 2020, global spending on cloud infrastructure has grown by around 20% annually.

Domain Information

Name: UBER.COM

Registry Domain ID: 2564976_DOMAIN_COM-VRSN

Domain Status: clientDeleteProhibited

clientTransferProhibited

clientUpdateProhibited

Nameservers: 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

Dates

Registry Expiration: 2028-07-13 04:00:00 UTC

Updated: 2021-12-15 22:42:22 UTC

Created: 1995-07-14 04:00:00 UTC

Employees (Working URLS)

Uber Management

Name	Position	Location
Ariele Rosch	Creative Director	Texas, USA
Nathan Brown	Director	Illinois, USA
Nina Golik	Art Director	California, USA
Prasanna Vijayan	Director	California, USA
Shiva Shailendran Sekar	Director	Bengaluru, Karnataka
Sundar Rajan Ganapathisubramanian	Director	Washington, USA
Caitlin Chicu	Director	USA
sachin malhotra	Director	Delhi
David Zhou	Account Director	Shanghai
Venkatesh Kancharla	Director	Chengalpattu, Tamil Nadu

Uber's 2022 Data breach (Link NY Times)

The Uber data breach began with a hacker purchasing stolen credentials belonging to an Uber employee from a dark web marketplace. An initial attempt to connect to Uber's network with these credentials failed because the account was protected with MFA. To overcome this security obstacle, the hacker contacted the Uber employee via What's App and, while pretending to be a member of Uber's security, asked the employee to approve the MFA notifications being sent to their phone. The hacker then sent a flood of MFA notifications to the employee's phone to pressure them into succumbing to this request. To finally put an end to this notification storm, the Uber employee approved an MFA request, granting the hacker network access, which ultimately led to the data breach. After completing the attack, the hacker compromised an Uber employee's Slack account and announced the successful breach to the entire company. After successfully connecting to Uber's intranet, the hacker gained access to the company's VPN and discovered Microsoft Powershell scripts containing the login credentials of an admin user in Thycotic - the company's Privileged Access Management (PAM) solution. This discovery significantly increased the severity of the breach by facilitating full admin access to all of Uber's sensitive services, including DA, DUO, Onelogin, Amazon Web Services (AWS), and GSuite. The hacker also allegedly accessed Uber's bug bounty reports which usually contain details of security vulnerabilities yet to be remediated.