SC

SEBURN
SECURITY CONSULTING

Penetration Testing Report

12/6/23

Table of Contents

Executive Summary

Overview

The penetration test conducted on Uber.com employed a thorough methodology, utilizing Kali-linux, web-recon, and specific tools like recon-ng, nessus, and whois lookups. Strict adherence to HackerOne guidelines ensured a comprehensive testing approach. Reconnaissance involved OSINT techniques, identifying assets such as IP addresses, subdomains, technology, servers, employees, and email structures. Scanning utilized recon-ng on a Kali-linux machine, while Nessus served as the primary tool for the vulnerability assessment, yielding no significant vulnerabilities.

Medium findings included the exposure of Uber's IP addresses, subdomains, and person-of-contact information, recommending measures to mitigate DDoS risks and enhance naming conventions. Low-risk findings covered website terminology, server hosts and DNS, and identifying ten Uber employees, posing a minimal risk of phishing attacks. Understanding Uber's corporation type was also identified as a low-risk factor. In conclusion, Uber's security systems effectively safeguarded data, with identified vulnerabilities addressed through recommendations. The publicly available data for OSINT research highlights the importance of minimizing information exposure. Contact information for further inquiries: Scott Seburn - scott.seburn@comcast.net.

Scope

- **Client:** Uber.com
- **Engagement Period:** 12/6/23
- **Scope:** Uber.com and all subdomains except subdomains listed as out-of-the-scope

Objectives

- Identify vulnerabilities to assess the security posture.
- Evaluate the effectiveness of existing security controls.
- Provide recommendations for improving the overall security of the environment.

Recommendations

- High-level recommendations for addressing identified vulnerabilities.
- Prioritization of remediation efforts.

Methodology

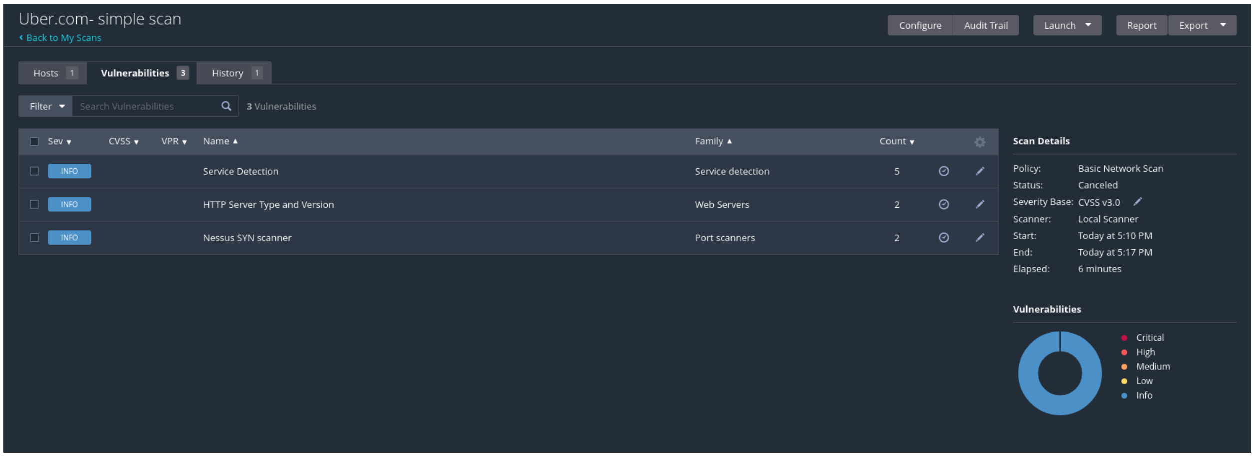
Testing Approach

- Various testing methods, such as kali-linux and web-recon, were employed during this penetration test to optimize identification of security risks and vulnerabilities. Methods used in this test were used with zero knowledge beforehand of any potential security risks or exploits on uber.com.

- Tools and techniques utilized in this report are as follows: Kali-linux, recon-ng, web reconnaissance, nessus, and whois lookups.
- All methodologies followed the listed rules on the uber.com HackerOne website: https://hackerone.com/uber?type=team

Testing Phases

1. **Reconnaissance:**
    - Multiple methods were utilized to gather the appropriate data available. All of the methods used were OSINT, therefore all information gathered is publicly available.
    - Assets identified were related to: uber's ip addresses and subdomains, site technology and servers, various employees, and company email structure.
2. **Scanning:**
    - Details on scanning methodologies.
    - The scanning done on this test was mainly through recon-ng, on a kali-linux machine. Recon-ng allowed for testing multiple points of interest on uber.com and returned many pieces of data.
3. **Vulnerability Assessment:**
    - The main tool used for the vulnerability assessment was nessus.
    - This assessment did not return any notable vulnerabilities.



3 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
INFO			Service Detection	Service detection	5
INFO			HTTP Server Type and Version	Web Servers	2
INFO			Nessus SYN scanner	Port scanners	2

Scan Details

Policy:	Basic Network Scan
Status:	Canceled
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 5:10 PM
End:	Today at 5:17 PM
Elapsed:	6 minutes

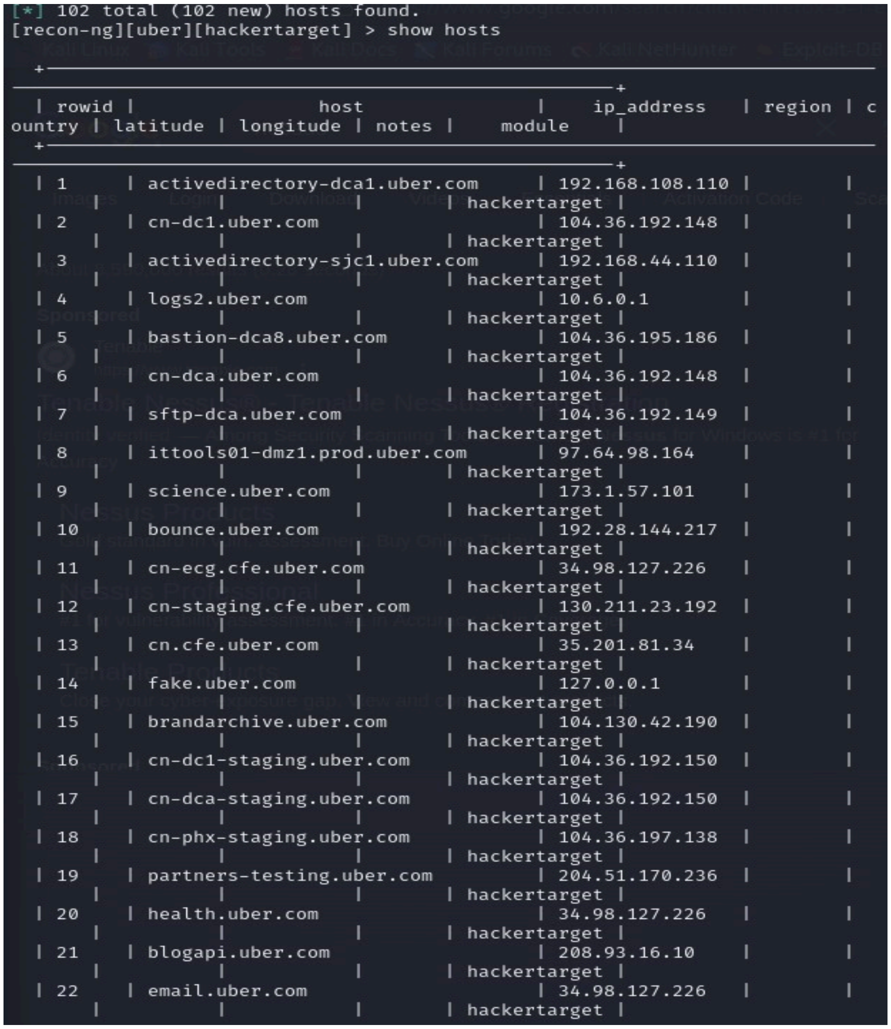
Vulnerabilities

Findings

These findings present medium damage and medium probability for damage to the company.

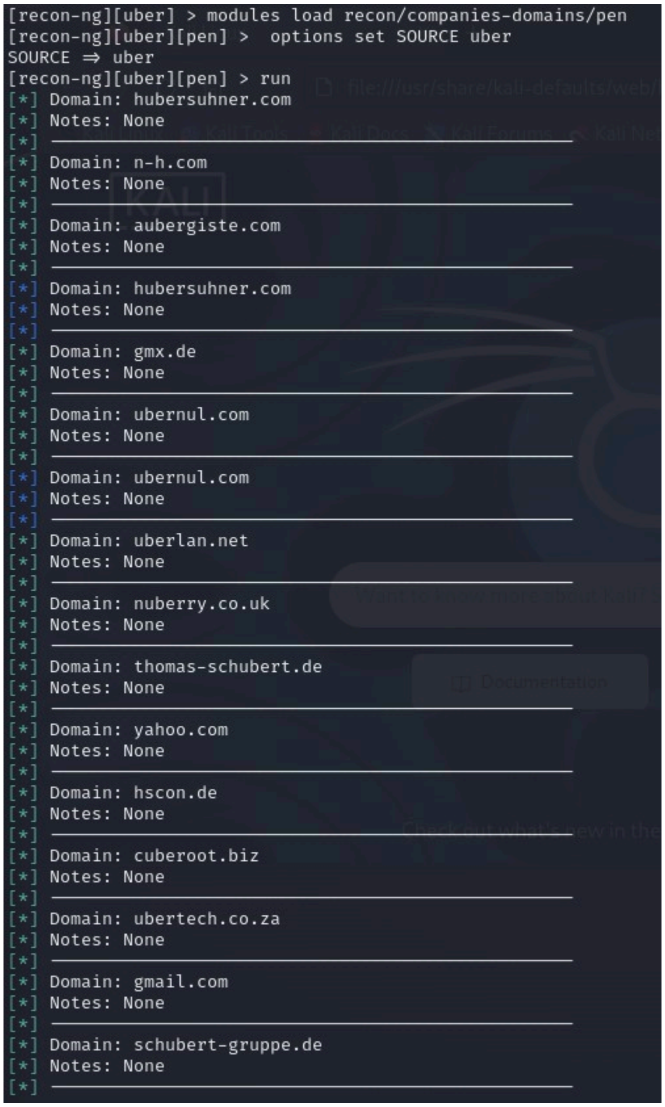
Medium Findings

1. List of all of Uber’s IP addresses
    - Impact: Medium
    - Recommendation: Harden IPs so no DDos attack can take place.



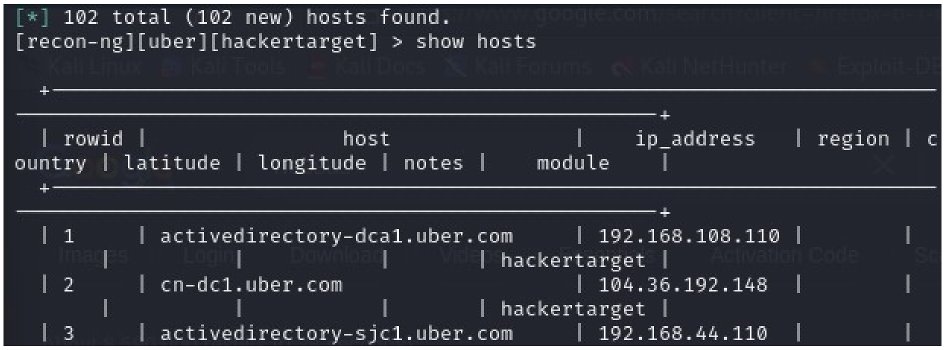
```
[*] 102 total (102 new) hosts found.
[recon-ng][uber][hackertarget] > show hosts

  +-------------------------------------------------------------------------
-----------------------------------------------------+
  | rowid |                host                |    ip_address    | region | c
ountry | latitude | longitude | notes |    module    |
  +-------------------------------------------------------------------------
-----------------------------------------------------+
  | 1     | activedirectory-dca1.uber.com     | 192.168.108.110 |        |
       |          |           |       | hackertarget |
  | 2     | cn-dc1.uber.com                   | 104.36.192.148  |        |
       |          |           |       | hackertarget |
  | 3     | activedirectory-sjc1.uber.com     | 192.168.44.110  |        |
       |          |           |       | hackertarget |
  | 4     | logs2.uber.com                    | 10.6.0.1        |        |
       |          |           |       | hackertarget |
  | 5     | bastion-dca8.uber.com             | 104.36.195.186  |        |
       |          |           |       | hackertarget |
  | 6     | cn-dca.uber.com                   | 104.36.192.148  |        |
       |          |           |       | hackertarget |
  | 7     | sftp-dca.uber.com                 | 104.36.192.149  |        |
       |          |           |       | hackertarget |
  | 8     | ittools01-dmz1.prod.uber.com      | 97.64.98.164    |        |
       |          |           |       | hackertarget |
  | 9     | science.uber.com                  | 173.1.57.101    |        |
       |          |           |       | hackertarget |
  | 10    | bounce.uber.com                   | 192.28.144.217  |        |
       |          |           |       | hackertarget |
  | 11    | cn-ecg.cfe.uber.com               | 34.98.127.226   |        |
       |          |           |       | hackertarget |
  | 12    | cn-staging.cfe.uber.com           | 130.211.23.192  |        |
       |          |           |       | hackertarget |
  | 13    | cn.cfe.uber.com                   | 35.201.81.34    |        |
       |          |           |       | hackertarget |
  | 14    | fake.uber.com                     | 127.0.0.1       |        |
       |          |           |       | hackertarget |
  | 15    | brandarchive.uber.com             | 104.130.42.190  |        |
       |          |           |       | hackertarget |
  | 16    | cn-dc1-staging.uber.com           | 104.36.192.150  |        |
       |          |           |       | hackertarget |
  | 17    | cn-dca-staging.uber.com           | 104.36.192.150  |        |
       |          |           |       | hackertarget |
  | 18    | cn-phx-staging.uber.com           | 104.36.197.138  |        |
       |          |           |       | hackertarget |
  | 19    | partners-testing.uber.com         | 204.51.170.236  |        |
       |          |           |       | hackertarget |
  | 20    | health.uber.com                   | 34.98.127.226   |        |
       |          |           |       | hackertarget |
  | 21    | blogapi.uber.com                  | 208.93.16.10    |        |
       |          |           |       | hackertarget |
  | 22    | email.uber.com                    | 34.98.127.226   |        |
       |          |           |       | hackertarget |
```

2. List of all of Uber’s sub-domains
    - Impact: Medium
    - Recommendation: Harden IPs so no DDos attack can take place.



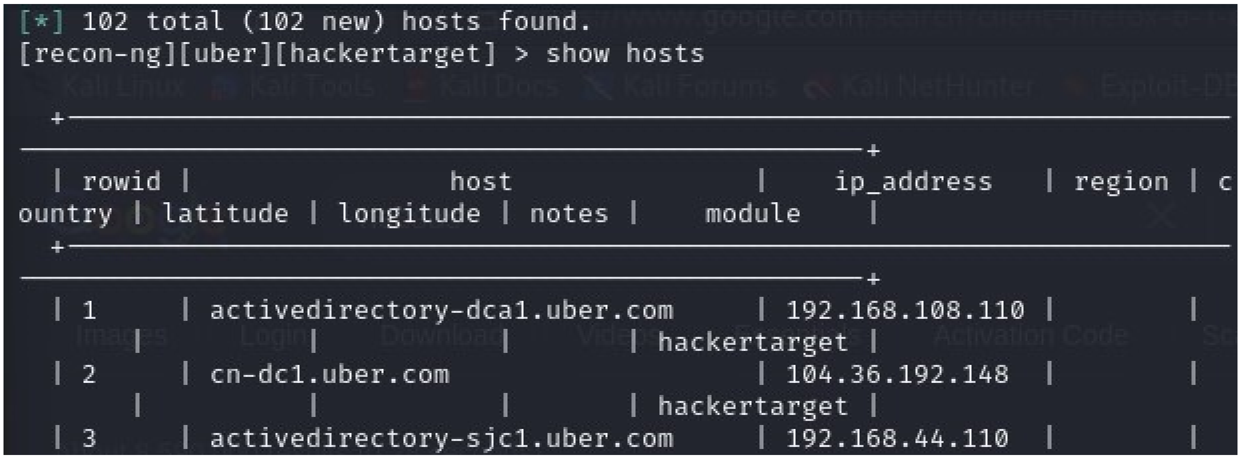
```
[recon-ng][uber] > modules load recon/companies-domains/pen
[recon-ng][uber][pen] >  options set SOURCE uber
SOURCE ⇒ uber
[recon-ng][uber][pen] > run
[*] Domain: hubersuhner.com
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: n-h.com
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: aubergiste.com
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: hubersuhner.com
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: gmx.de
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: ubernul.com
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: ubernul.com
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: uberlan.net
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: nuberry.co.uk
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: thomas-schubert.de
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: yahoo.com
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: hscon.de
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: cuberoot.biz
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: ubertech.co.za
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: gmail.com
[*] Notes: None
[*] ──────────────────────────────────────────────────
[*] Domain: schubert-gruppe.de
[*] Notes: None
[*] ──────────────────────────────────────────────────
```

3. Whois Person of Contact
    - Impact: Medium
    - Recommendation: Remove person of contact information.



```
[*] 102 total (102 new) hosts found.
[recon-ng][uber][hackertarget] > show hosts

  +------------------------------------------------------------------------------
------------------------------------------------------------+
  | rowid |                host                |    ip_address   | region | c
ountry | latitude | longitude | notes |    module    |
  +------------------------------------------------------------------------------
------------------------------------------------------------+
  | 1     | activedirectory-dca1.uber.com     | 192.168.108.110 |        |
        |          |           |       | hackertarget |
  | 2     | cn-dc1.uber.com                   | 104.36.192.148  |        |
        |          |           |       | hackertarget |
  | 3     | activedirectory-sjc1.uber.com     | 192.168.44.110  |        |
```

4. Company email and active directory naming convention
    - Impact: Medium
    - Recommendation: Change naming convention from “name@uber.com”

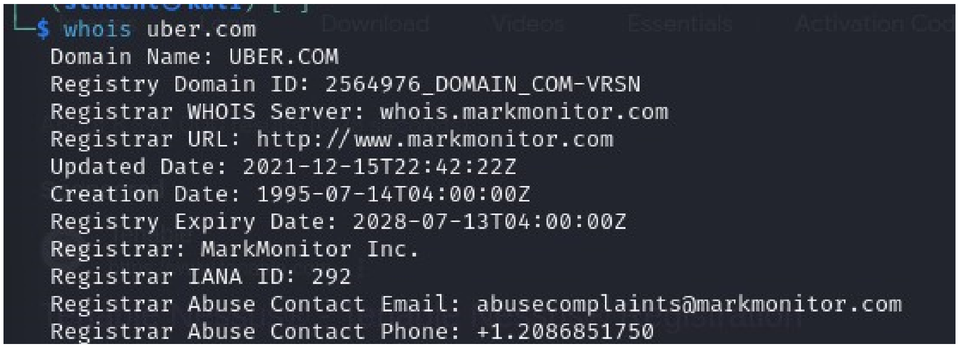


```
[*] 102 total (102 new) hosts found.
[recon-ng][uber][hackertarget] > show hosts

  +------------------------------------------------------------------------------
------------------------------------------------------------+
  | rowid |                host                |    ip_address   | region | c
ountry | latitude | longitude | notes |    module    |
  +------------------------------------------------------------------------------
------------------------------------------------------------+
  | 1     | activedirectory-dca1.uber.com     | 192.168.108.110 |        |
        |          |           |       | hackertarget |
  | 2     | cn-dc1.uber.com                   | 104.36.192.148  |        |
        |          |           |       | hackertarget |
  | 3     | activedirectory-sjc1.uber.com     | 192.168.44.110  |        |
```

Low Findings

These findings present low damage and low probability for damage to the company.

1. Website Terminology
    - Impact: Low
    - Uber.com utilizes MySQL for its databases, PHP and Node.js for its programming language, Envoy for its reverse proxies, Google Cloud for its Iaas, Amazon Web Services for its Paas, and Stripe for its payment process.
2. Who hosts servers and DNS
    - Impact: Low



```
└─$ whois uber.com
   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: 2021-12-15T22:42:22Z
   Creation Date: 1995-07-14T04:00:00Z
   Registry Expiry Date: 2028-07-13T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
```

3. 10 people who work at Uber
    - Impact: Low
    - Employees found to work at Uber through the reconnaissance assessment: Brian Tam, Gabriel Ramos, Sreeja Kannagundla, Ankit Bhargava, Hao Song, Allen Zeng, Xhuljiano Dhima, Jennifer Chou, James Zhou, and David Lee.
    - Their information being public is a potential risk for phishing attacks.
4. What type of Corporation
    - Impact: Low
    - This is a low risk in that knowing what kind of corporation Uber is does not tend to lead to security risks.
    - https://s23.q4cdn.com/407969754/files/doc_governance/Certificate-of-Incorporation-Uber.pdf

Conclusion

- Overall, the security systems in place, found during this penetration test, effectively protect Uber's data and user data. The few security risks found open up medium-low risk vulnerabilities. These vulnerabilities, however, only put the company at risk of slight exploitation. One major issue is the amount of data available for OSINT research.

Contact Information

- Contact Information: scott.seburn@comcast.net