**OpenTable Footprint Report**

Dustin McClure

Whatcom Community College

CIS 214: Footprinting Report

January 21, 2022

**OpenTable Footprint Report**

In this report, we will examine the findings of a footprint conducted on the domain opentable.com to assess it’s vulnerability to an attack. Included information encompasses multiple physical locations, executive and technical contacts, and technological infrastructure. This information is included as an attachment and was obtained using a variety of passive, open-source intelligence and network query tools.

The initial point of focus for this footprint was publicly available contact information for executive and technical contacts. In a cursory search we were able to locate direct contact information for multiple department directors and multiple C-Suite personnel. This information included office locations, names, company email addresses, and in some cases direct personal and business lines.

After searching for publicly available contact information, we moved on to a footprint of OpenTable’s technological infrastructure, including: domain registration information, name server enumeration, assigned ip ranges, exploration of sub-domains and their associated ip addresses, and services, frameworks, and applications in use.

In our search for information about OpenTable’s technological infrastructure, we were able to find multiple current job postings that were tagged by location and provided detailed descriptions of the programming languages, applications, and frameworks required for each opening, sometimes even noting the version of software an applicant should be proficient in. Given that each job posting is location specific, and in some cases domain specific, this level of detail could allow a potential threat actor to create a detailed inventory of services to scan/probe by assigned ip range and port number.

Furthermore, in conjunction with information uncovered in our technological footprint, the public availability of contact information for key technical and C-Suite employees at OpenTable may allow threat actors to establish what seems a plausible line of communication with those that have direct access to some of the most sensitive resources in the organization.

When considering the type of information that an attacker would have at their fingertips to formulate a successful social engineering attack, it is important to look at what was uncovered when searching for DNS Host Records (subdomains of opentable.com). These included domain records and associated ip addresses for staging and pre-production environments, mail servers, ftp servers, proxies, and employee self-service tools. Armed with this information, an attacker could communicate in a convincing way about what they need access to and why.

Below is a list of recommended counter-measures to combat social engineering techniques and footprinting:

* Sanitize publicly available contact information for technical contacts and C-Suite employees.
* Centralize contact with the company based on need, and implement a chain of escalation so that incoming queries or requests are properly vetted as they move up.
* Implement a review process for public job postings to ensure sensitive information about infrastructure is guarded
* Restructure internal and external subdomains to limit public exposure