Hacking Research Report

Course NO.	**IA 5010**
Lab No	**13**
Instructor	**Themis Papageorge**
Author	**Yifan Zhang(nuid: 001616011)**
Date	**09/23/2015**

Table of Contents

1. Executive Summary

With the study of the lab and by doing actual experiments on the virtual network systems, we know how to use tools like Sam Spade version 1.14 to investigate a target. In this lab, we have three target servers which are apples.com, oranges.com and bananas.com. Through running different utilities of Sam Spade, we could collect information of domain user, domain IP, some critical roles within a particular host like administrator, the possible physical location of the server and even how many notes it passes between source IP address and destination IP addresses.

Besides the lab, we also learn how to use public available search engine to select a target from real world. In this report, we utilize Google Search engine as one of our investigation tools at reconnaissance stage of hacking. From Google, we collect information like the physical location of a company, the employees' geographic distribution and the CEO, CFO's name and email address and so on.

In the first part of the lab, we find that through Whois utility, we could easily obtain user information including user cellphone number, email addresses and domain information like primary IP for DNS server. And, in the second part of the lab, with the help of Google, we could know more about the company's background in order to identify potential targets within this company. With this easy-available information, attackers could do various attacks in terms of phishing, fraud, spoofing, physical sabotage …etc. to the user or to the company which might cause seriously information leakage. The company or the user may suffer great loss when hackers exploit all of the information together. We will explain this in latter section.

2. Methodology

2.1 Tools & Technology used in Technique research

In this part of research, we mainly use Sam Spade tool to investigate the detailed information of the three provided domains – apples.com, oranges.com and bananas.com. Sam Spade is a free utility containing tools to gather information on Internet hosts, analyze email headers, display web site code, and perform several other tasks (SANS Institute InfoSec, 2003). Although Sam Spade provides us a powerful set of tools to analysis the Internet environment, particularly in this experiment, we mainly use the functionalities like Whois, ping, traceroute, nslookup, finger, time, IP Block, dig, abuse lookup and traceroute.

2.2 Tools & Technology used in Public Domain research

For public domain research, we prefer to use an online search engine to look up the materials that we need in this experiments. And, we will collect the essential information of a company (Oracle) and this information includes the members of director board, the total employee's number and its distribution, the location of its headquarters … etc. Therefore, we choose to use the most powerful search engine of the world – Google. By using Google, we can easily get the things that we need and it saves huge amount of time.

3. Technical Research Result

After the overall investigation that is performed in technical section, we can find some critical information such as the server name, host name, staff information, and where the possible location might be … etc.

Firstly, we applied Whois utility on the three domains apples.com, oranges.com and bananas.com and we got the following information.

	Apples.com	**Oranges.com**	**Bananas.com**
Domain name	apples.com	ORANGES.com	BANANAS.COM
Host name	APPLES1-HOST	ORANGES1-HOST	BANANAS1-HOST
Company name	Apples	ORANGES	BANANAS
Primary IP address	10.20.100.20	192.168.40.9	192.168.3.5
Country	GM (Gambia)	US	US
Administrative contact	Werner Speissl	Bob Jones , JD1-ORANGES	Linda Stone, JD1-BANANAS
…continue next page			

	Apples.com	**Oranges.com**	**Bananas.com**
Technical contact	JD1-APPLES	Sparrow JD1-ORANGES	Linda Stone, JD1-BANANAS
DNS server	ns1.apple.com	ns2.oranges.com	ns1.BANANAS.com
User name	Werner Speissl	Bob Jones	Linda Stone
User Email	werner.speissl@apples.com	bob.jones@ORANGES.com	Linda.stone@BANANAS.com
User telephone number	0800-184-4293	800-292-4532	800-342-9832

Based on the above table, we can know a lot of detailed information. This above disclosed information is potential threat for the company. For example, the attackers can send phishing emails, or spooling emails to staffs which might cause great loss for that company.

Secondly, we applied rest of the tools and they also expose some information of the target. The information is summarized as a table below.

	Information we got
nslookup	we got the detailed DNS information about those three domains
ping	Through this, we know about the alive servers within this target network
IP Block	Through this, we know about the ownership and contact information
Dig	Through this, we know about all of the available resources records within the domain
finger	Through this, we know about the information related to host and user

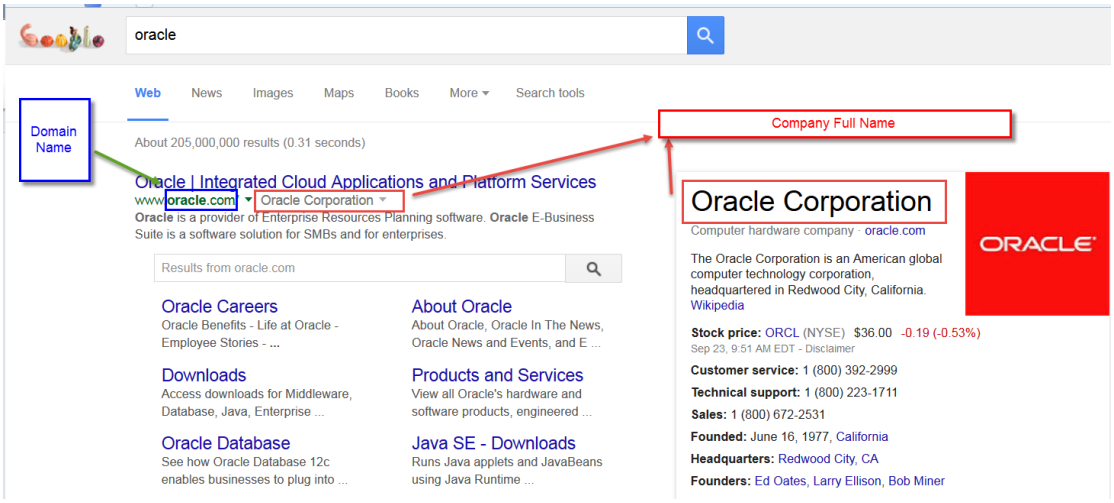
4. Public Domain Research Results

By using google, everything becomes such easier and you just enter what you want to search and google will tell you all the tings related to your search. In this part, we chose Oracle Corporation as our target this time because personally I am extremely interested in this company. Oracle Corporation once was the third-largest software maker by revenue, just behind Microsoft in 2011 (Kooten, 2011). For Oracle, their products cover every aspect of business, especially in field like database, ERP management and middleware and so on. This time, in this article, we want to collect information such as full name of this company, Domain name, URLs for the ecommerce website and social networking sites, location of main headquarter of this company, name of their director board, number of employees and business partners or clients.

4.1 Company Name & Domain name

Based on the previous brief introduction, we find that the full company name of Oracle is ***Oracle Corporation*** and its official site's domain is ***oracle.com***.

Figure 1. Target company full name & Domain name



4.2 E-commerce website & Social Netwroking site

Also through google, we find the Oracle online store URLs and social media link as below pictures.

Figure 2. E-commerce website of Oracle

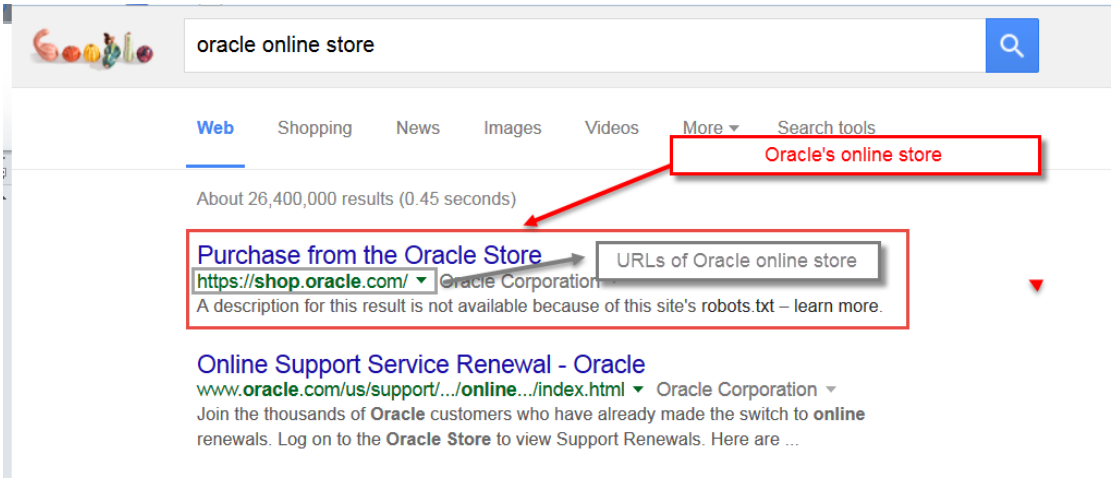
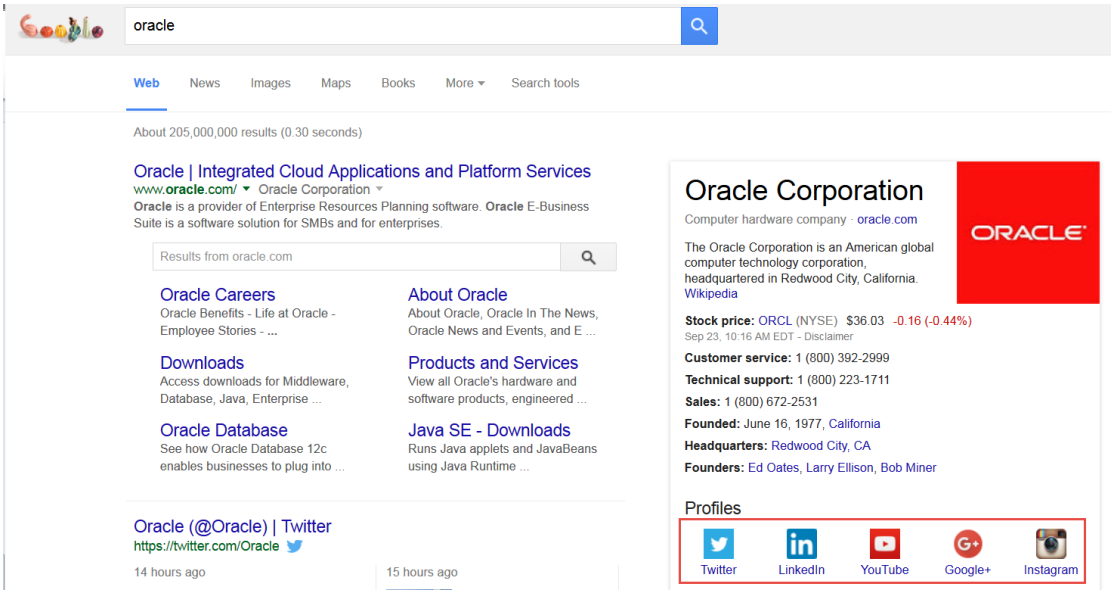


Figure 3. Social Networking sites



When we search Oracle in google, it also shows all the social networking sites that Oracle has. The URLs information is summarized as follow table.

Social media type	URLs
Twitter	http://www.twitter.com/oracle
Facebook	https://www.facebook.com/Oracle
Linkedin	https://www.linkedin.com/company/oracle
Youtube	http://www.youtube.com/user/Oracle
Google+	http://plus.google.com/+Oracle

4.3 Physical location of the headquarter

For this part, we use two tools of google and the first one is Google search engine and another is Google Map. By using Google search engine we can know the address literally but if we want to view the where this address is, we need use Google Map. Another benefit of using Google Map is that they provide us real images of particular street and buildings which may allow us know better about the target.

Figure 4. Google literal address

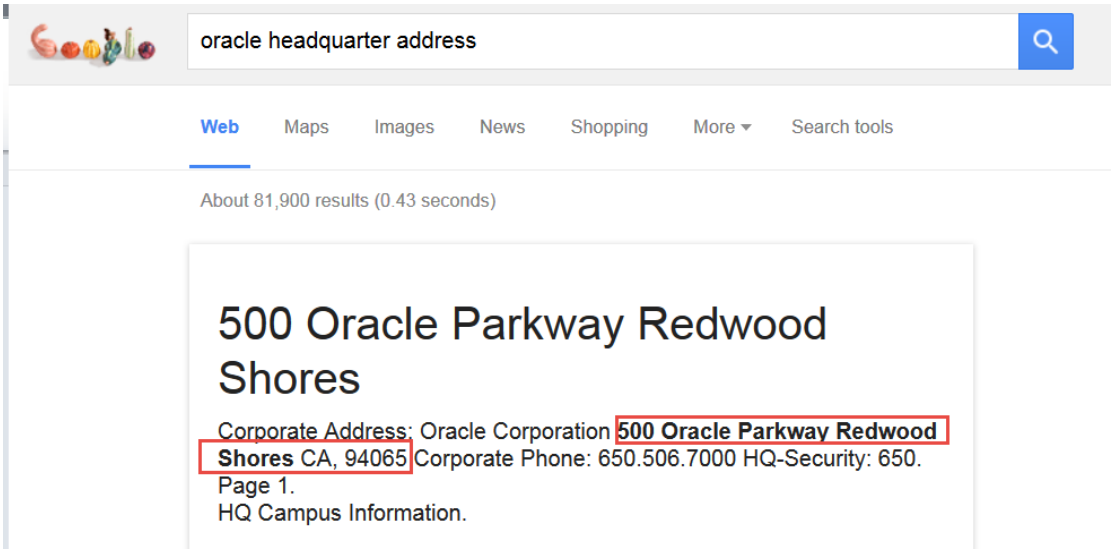


Figure 5. Google Map

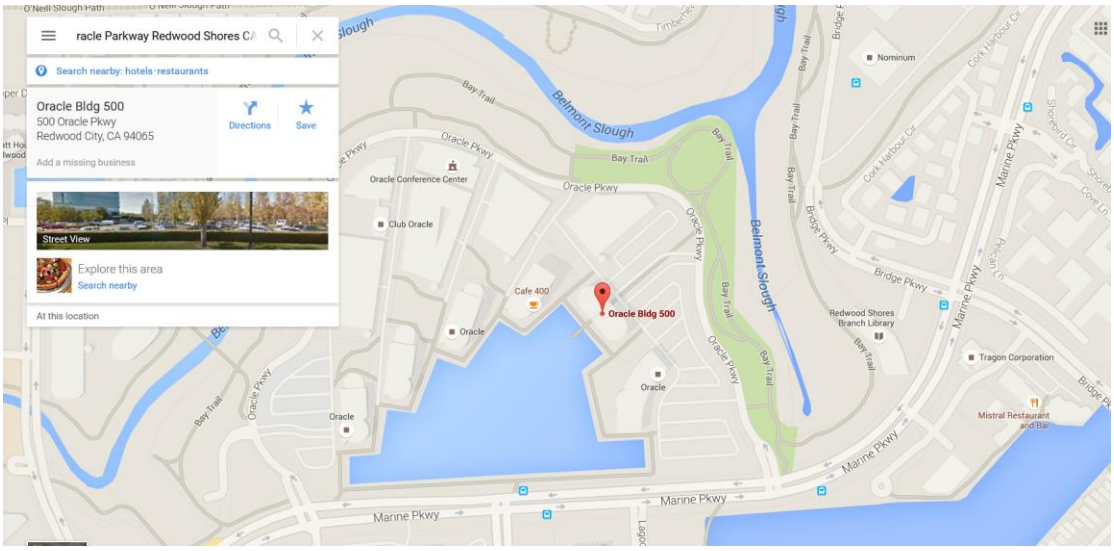
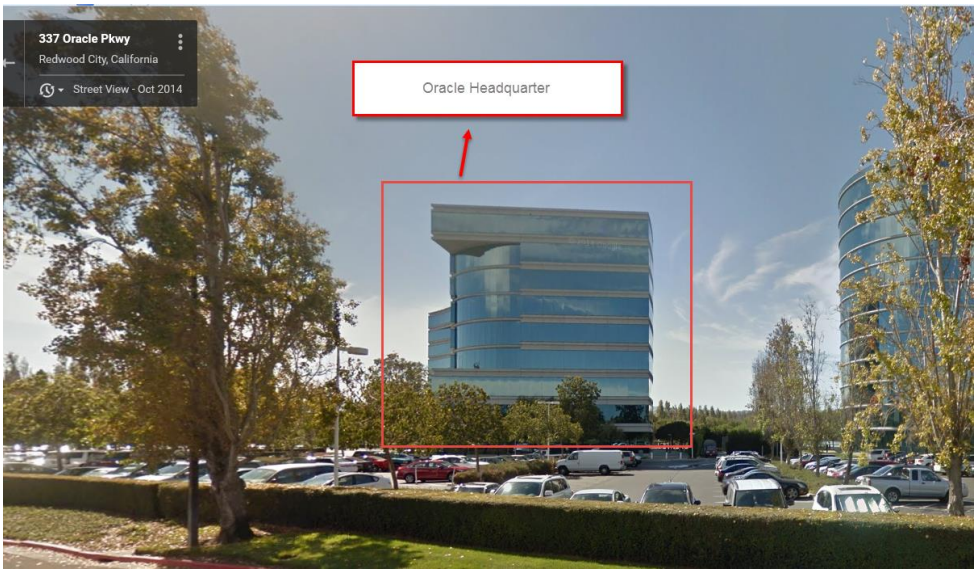


Figure 5. Google Map Street view



4.4 Persons in director board

Through google, we can know all the executives in this company. But in this report, we just give some persons in director board and their responsibilities. This information is summarized as below table.

Name	Position
Larry Ellison	Co-founder of Oracle
Lawrence J.Ellison	Executive Chairman of the Board and Chief Technology Officer
Jeffrey O. Henley	Vice Chairman of the Board
Safra Catz	Chief Finance Officer

4.5 Number of employees in major branches

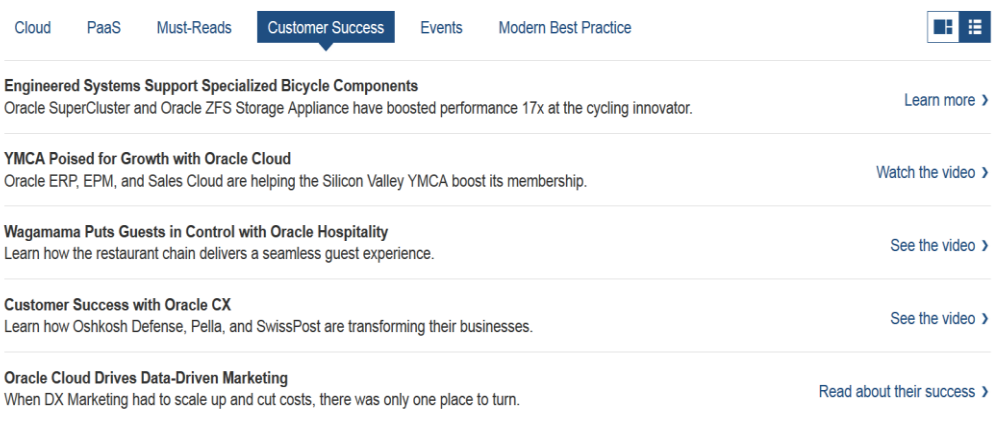
As the google search results shows that in 2015, Oracle totally has 132,000 employees from world-wide (macro axis, 2015). In the following part, we just list the number of employees of several large branches.

Branch Name	Employees' number
Oracle's World Headquarters	Around 5,500
China	Around 4000
India	Around 30,000

4.6 Clients & Partners

In this part, we find several Oracle's clients which successfully implement Oracle products to their production. These clients cover many different fields and industries and the following picture gives the details.

Figure 6. Oracle successful clients



5. Findings and Conclusions

Through the overall investigation, we find that there are many potential threats to all of the four companies. For apples.com, oranges.com and bananas.com, the most risky thing is that their sensitive data are disclosed when we use Sam Spade tools. For example, through Sam Spade's Whois utility, we get the detailed sensitive information like cell phone number and email address about domain users. Hackers can exploit this potential vulnerability and they might send phishing emails or huge amount of spam emails. If some of employees click these phishing emails, it could cause serious information breach and hackers may use the leaked information to perform further attacks or just extort a person or a company for fulfilling their needs. Furthermore, attackers also can degrade the efficiency of particular person through sending huge amount of spoofing emails.

Another potential attack for apples.com, oranges.com and bananas.com is the DNS contamination. For black-hat hackers, they can use DNS contamination techniques to disguise a phishing site with a reliable domain name. For instance, a user may want to access amazon.com. He/she enters http://www.amazon.com in his/her browser and everything looks like real site of Amazon but actually they may be directed to another unreliable IP addresses.

However, for Oracle Corporation, too much public information is available on Google search engines. Through this kind of information disclosure, attackers can gather everything that they interested in and make a good preparation for future attack.

Therefore, for an attacker, they will firstly use public available search engine like bing.com, google.com or yahoo.com to collect various information that they interested in. Then, they will analyze this available information and select an attacking target. After they choose a target, they will hack into the network systems of their target and execute tools like Spam Spade to gather further detailed information to find out the potential weakness point. Lastly, they will perform real attacks.

As information security professionals, we need to use tools like Spam Spade to detect the potential vulnerabilities in advance. If we want to stop information leakage from Whois utility of Spam Spade, we could set up an agent server to isolate the real important assets from outside world.

6. Avenues of Further Research

Although this lab let us get a start on using investigation tools, we still need to drill down to the details that how we can use these tools effectively in practice. In future, I want to do some researches on the existing vulnerabilities of these four companies and how to attack and how to defense their systems. For next step, I prepared to use tools like zenmap, OpanVAS, Wireshark, NetWitness Investigator to do a deep analysis about those companies.

If I were preparing a hacking attack, I would try to figure out the following questions.

a Which company should I hacking?
b What are currently available resources and tools that I could use?
c How to get-in their internal systems bypassing authentication and authorized?
d If I get-in to their system, what kind of vulnerabilities that I can exploit?
e How could I hide myself after hacking attack?

Reference:

CFO.com. (2014, 7 29). *Oracle CFO Safra Catz Is Highest-Paid Woman Exec*. Retrieved 9 23, 2015, from CFO: http://ww2.cfo.com/compensation/2014/07/oracle-cfo-safra-catz-highest-paid-woman-exec/

Kooten, M. V. (2011, 8 23). *Global Software Top 100*. Retrieved 9 23, 2015, from SOFTWARE TOP 100: http://www.softwaretop100.org/global-software-top-100-edition-2011

macro axis. (2015). *Oracle Number of Employees ORCL NYSE*. Retrieved 9 23, 2015, from Macro Axis.com: https://www.macroaxis.com/invest/ratio/ORCL--Number-of-Employees

SANS Institute InfoSec. (2003). *Using Sam Spade*.

WebcorBuilders. (2004, 1). *Oracle World Headquarters*. Retrieved 9 23, 2015, from webcor.com: http://www.webcor.com/projects/oracle-world-headquarters/?view=all