**Lab 3: Data Gathering and Footprinting on a Targeted Web Site – Research Report**

**By**

**Natnael Kebede**

**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 7359 – Penetration Testing and Vulnerability Assessment

Spring 2020

Presented to Dr. Renita Murimi

Table of Contents

Executive Summary……………………………………………………………………….……………iii

Methodology………………………………………………………….….……….…….….………....…1

Technical Research Results……………………………………………………….………….….……2

Public Domain Research Results…………………………………………………………….….……7

Findings and Conclusions………………………………………………………………………...……8

Avenues of Further Research……………………………………….…….……….….….….….….…9

ii

# 

# **Executive Summary**

The Internet has been a rich source of information about any organization providing data that is free, easily searchable, and obtainable through various methods. These characteristics of the Internet allow a hacker to perform reconnaissance, the first phase of hacking, which is designed to gain as much information as possible about a target organization and its assets.

This report details a data gathering and foot-printing investigation that is performed using open source intelligence techniques and network information tools of target domains and an e-commerce website. It describes the methodology, that is, the tools and techniques that were used to conduct both the technical research and public domain research.

The results that were obtained as well as a discussion of the findings and possible avenues of further research is also addressed in this report. The analysis of the results is crucial to deduce what happens if a hacking attack was to be attempted, such as spear phishing or performing vulnerability scanning with owasp-cap, Nessus, or Nmap.

# 

iii

**Methodology**

The tools and techniques that were used to conduct both the technical and public domain research include the following:

1. SamSpade: An all-in-one network information gathering tool that was used to collect various common network information functions.
2. WHOIS: A query that is used with Sam Spade tool to perform domain lookup and record the name of the domain owner, nameservers, registration details, and contact information of individuals associated with a target domain
3. ping:  A network administration command-line tool that used to test the reachability of a host on an Internet Protocol (IP) network. It was used to uncover additional information to what was gathered from utilizing SamSpade.
4. nslookup: A network administration command-line tool that used to perform Domain Name System (DNS) queries and look up the Internet Protocol (IP) addresses associated with specific domain names. It was used to uncover additional information to what was gathered from utilizing SamSpade.
5. tracert: The traceroute tool is a network diagnostic command used to identify the network path that must be followed to reach a system from another one. It displays the names and Internet Protocol (IP) addresses of all intermediate systems. This tool can also be used to analyze possible attack points and estimate the geographic location of a server.
6. Google: Used to lookup company information and get primary data.
7. LinkedIn: Used to find key personnel information such as the names of officers.

1

1. Bloomberg, Hoover, Reuters, and U.S. Securities and Exchange commission Websites: These websites were used to identify any recorded information of publicly traded companies.
2. Target company’s website: Used to collect information such as the statistics of the company and personnel information as well as office locations.

**Technical Research Results**

Using the tools and techniques that were mentioned above to conduct the technical and public domain research, it was discovered that [x128bit.com](http://x128bit.com/), [iSkytap.com](http://iskytap.com/), and [cloudparadox.com](http://cloudparadox.com/) are all registered using the same registrar agent called Network Solutions LLC, with email address is abuse@web.com and contact phone number: +18003337680.

Figure 1: WHOIS results for all three domains

A screenshot of a social media post

Description automatically generated

2

A screenshot of a social media post

Description automatically generated

A screenshot of a social media post

Description automatically generated

According to the data collected from the ping command tool, the domains [x128bit.com](http://x128bit.com/) and [iSkytap.com](http://iskytap.com/) were found to be pointing to the 208.91.197.27 Internet Protocol (IP) address while [cloudparadox.com](http://cloudparadox.com/) was pointing to 50.225.131.227.

3

Figure 2: Ping results for all three domains

A screenshot of text

Description automatically generated

A screenshot of text

Description automatically generatedA screenshot of text

Description automatically generated

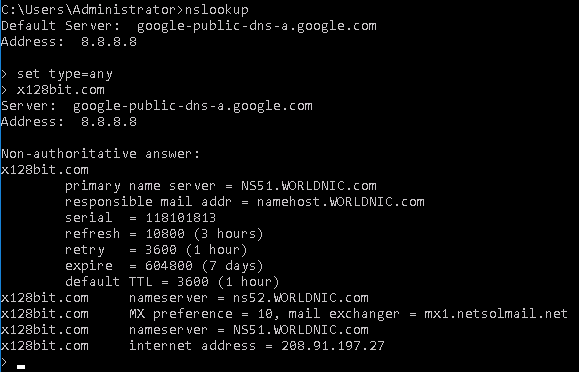
4

Geographically, [x128bit.com](http://x128bit.com/) and [iSkytap.com](http://iskytap.com/) are in the same location and probably even the same server since the domains are associated with the same IP address. Using an online IP lookup query tool, this server was found to be in Jacksonville, Florida, USA. On the other hand, [cloudparadox.com](http://cloudparadox.com/) was found to be using a different IP, which, upon further research, was found to be located in Washington DC, USA.

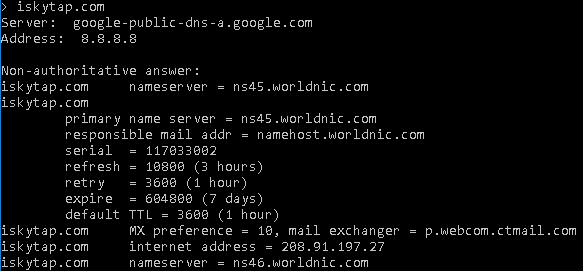
Furthermore, it was also discovered that there are related mail servers responsible for handling email messages for the three domains, as shown below:

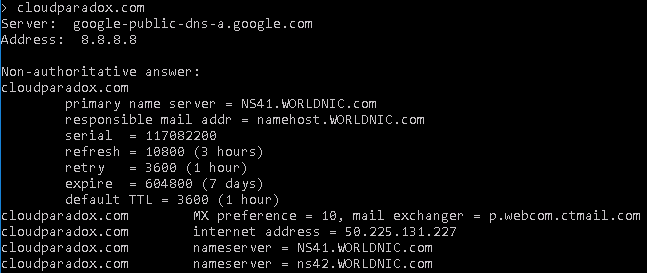
* [x128bit.com](http://x128bit.com/) - [mx1.netsolmail.net](http://mx1.netsolmail.net/)
* [iSkytap.com](http://iskytap.com/) and cloudparadox.com - [p.webcom.ctmail.com](http://p.webcom.ctmail.com/)

Figure 3: nslookup results for all three domains



5



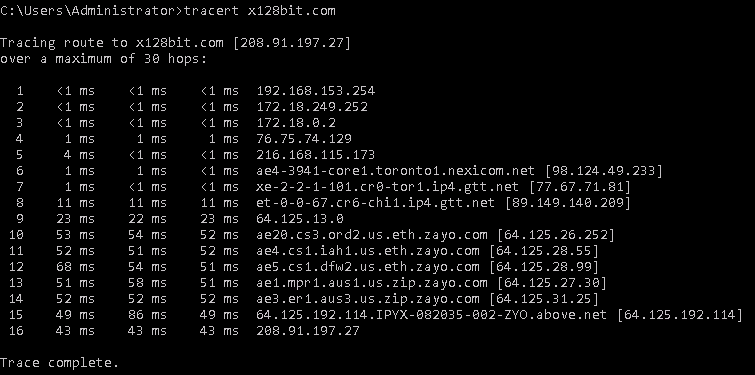


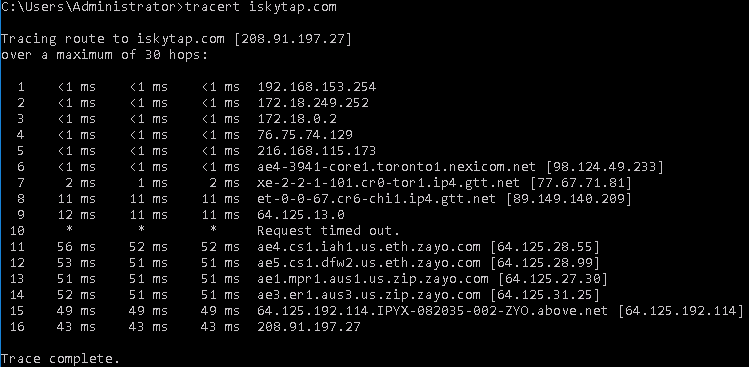
Lastly, the nameservers responsible (as identified by the nslookup command above and their associated IP address identified by the traceroute command below) for the resolution of the domain names are:

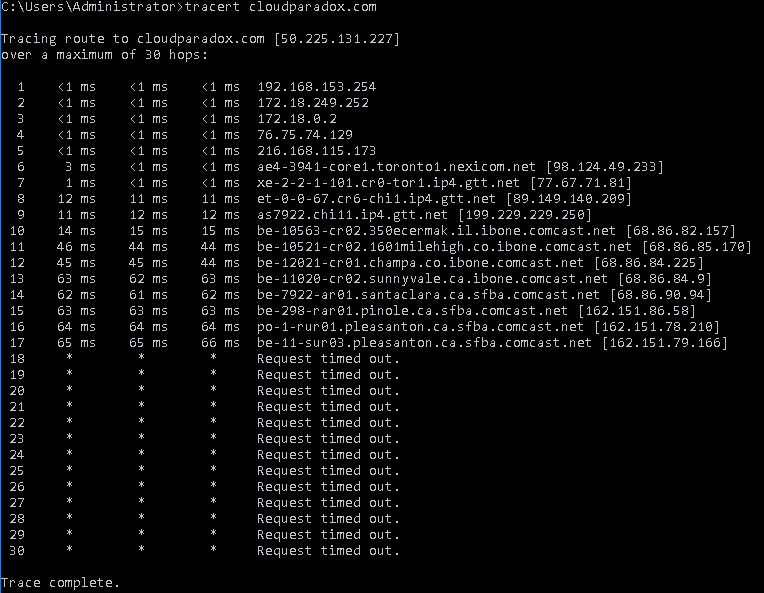
1. [x128bit.com](http://x128bit.com/)
   * [nS51.worldnic.com](http://ns51.worldnic.com/) - 207.204.40.126 and [nS52.worldnic.com](http://ns52.worldnic.com/) - 207.204.21.126
2. [iSkytap.com](http://iskytap.com/)
   * [ns45.worldnic.com](http://ns45.worldnic.com/) - 207.204.40.123 and [ns46.worldnic.com](http://ns46.worldnic.com/) - 207.204.21.123
3. [cloudparadox.com](http://cloudparadox.com/)
   * [ns41.worldnic.com](http://ns41.worldnic.com/) - 207.204.40.121 and [ns42.worldnic.com](http://ns42.worldnic.com/) - 207.204.21.121

6

Figure 4: tracert results for all three domains (3x);







# **Public Domain Research Results**

A summary of the results for the conducted public domain research of the targeted company, [Target.com](http://target.com/) using Open-Source Intelligence gathering includes the following:

1. Full name of the organization and symbol: Target Corporation (TGT)

7

1. Domain name owner: The domain name [target.com](http://target.com/) is disguised by Target Corporation, the company that owns it. Instead, it is registered through the agent CSC Corporate Domains, Inc. The agent’s contact information: +18887802723 also appears in the WHOIS query results of the Sam Spade tool.

Figure 5: Target’s WHOIS results

A screenshot of a social media post

Description automatically generated

1. Social Networking sites:
   * [twitter.com/Target](http://twitter.com/Target), [instagram.com/target](http://instagram.com/target), [facebook.com/target](http://facebook.com/target) , and [youtube.com/user/Target](http://youtube.com/user/Target)
2. Location of the company’s headquarters: 1000 Nicollet Mall, Minneapolis, MN 55403
3. Key personnel
   * Brian Cornell - Board Chairman and CEO, John J. Mulligan - Executive VP and COO, Michael E. McNamara - Executive VP, CIO, and Rich Agostino - Senior VP, CISO
4. Number of employees at major locations
   * Headquarters in Minnesota, MN: 10,000+ team members
   * India 2,500+ team members

# **Findings and Conclusions**

The results above show that it is a common practice to employ a registrar agent to maintain privacy, as seen from all the domains (including the targeted company) discussed above.

8

Additionally, it has been deduced that cloudparadox.com is most likely behind a firewall due to ping requests being blocked/dropped. Nevertheless, all three domains are owned by the same organization, which is either Network Solutions LLC or use Network Solutions LLC as a registrar agent.

Lastly, the targeted company, Target Corporations, is a large organization with multiple locations and many employees. This scenario means that a large surface of possible attacks is also possible for an attacker to take advantage of and explore them. Furthermore, a diverse amount of information about the company exists online due to the nature of the company being publicly traded. This case provides the attacker with data that is free, easily searchable, and obtainable through various methods.

# **Avenues of Further Research**

When it comes to additional research that one might conduct to learn more about the four companies, I would further scan and investigate the services hosted on the systems using tools such as Nmap, Nessus, NetWitness, recon-ng, and owasp zap. Additionally, I would investigate the business partners of the organizations and try to find connected systems to utilize as an attack vector. Finally, I would conduct a spear-phishing campaign to harvest credentials once I have a very clear strategy or plan, and I am ready to execute an attack on the company.

If I was planning a hacking attack, some of the questions I might try to answer include which computer systems aren’t managed properly, what attack methods are possible with existing vulnerabilities, how to start the attack, when will be a good time to execute the attack, and what strategies to use to remain undetected in the victim’s environment.

9