Henry Post

ITMS 443

Lab 2: Passive reconnaissance

Contents

[Target 1](#_Toc524544060)

[Research 1](#_Toc524544061)

[Preliminary Research 1](#_Toc524544062)

[Custom-made websites 2](#_Toc524544063)

[Other notes 2](#_Toc524544064)

[Similar error pages 2](#_Toc524544065)

[Open FTP server 2](#_Toc524544066)

[Outlook Web App Server 2](#_Toc524544067)

[What did we get? 3](#_Toc524544068)

[Personal Information 3](#_Toc524544069)

[Websites that Quest owns 3](#_Toc524544070)

[Websites that Quest has made 3](#_Toc524544071)

[Misconfigured servers/URLs 3](#_Toc524544072)

[Open servers 3](#_Toc524544073)

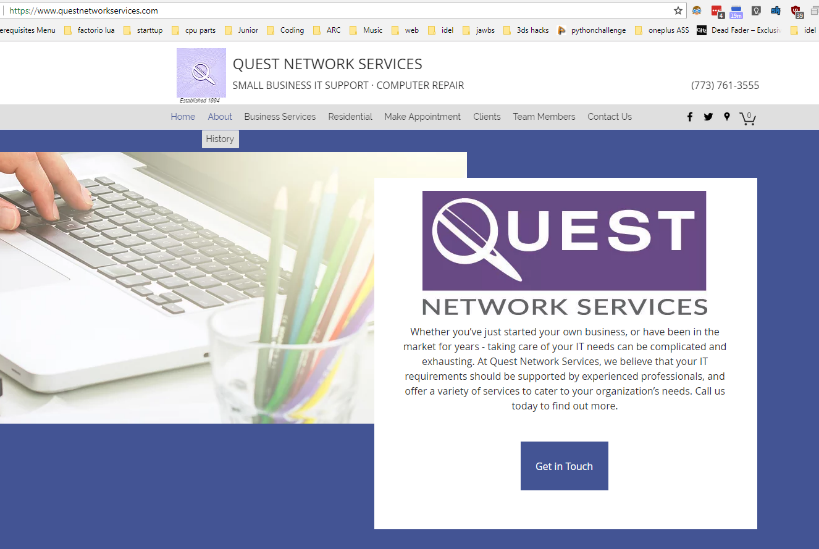
# Target

My target was a small computer repair company based in Chicago, IL called ‘**Quest Network Services**’.

I have had my computer repaired there once before, and thought that their (previously) hand-made website could mean that they have configured other things, such as mail servers or FTP servers.

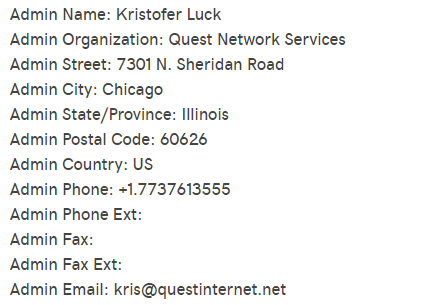
# Research

## Preliminary Research

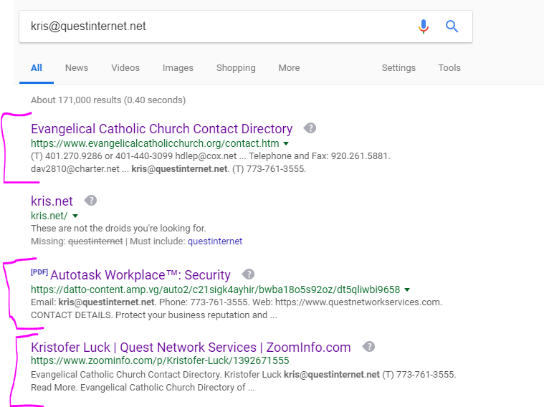
To begin, I simply googled ‘Quest Network Services’. This yielded me their website, at <https://www.questnetworkservices.com/>.

To me, this was a newer-looking website than their previous website, and the domain was different as well.

I started with a WHOIS, just to see what I could find. The results of the WHOIS lookup contained a street address, an email, a full name, and a phone number!

Curious about the email being under a different domain (as well as being crucial to discovering what other sites Kristofer had worked on), I went to <http://questinternet.net/> and was redirected back to the first site.

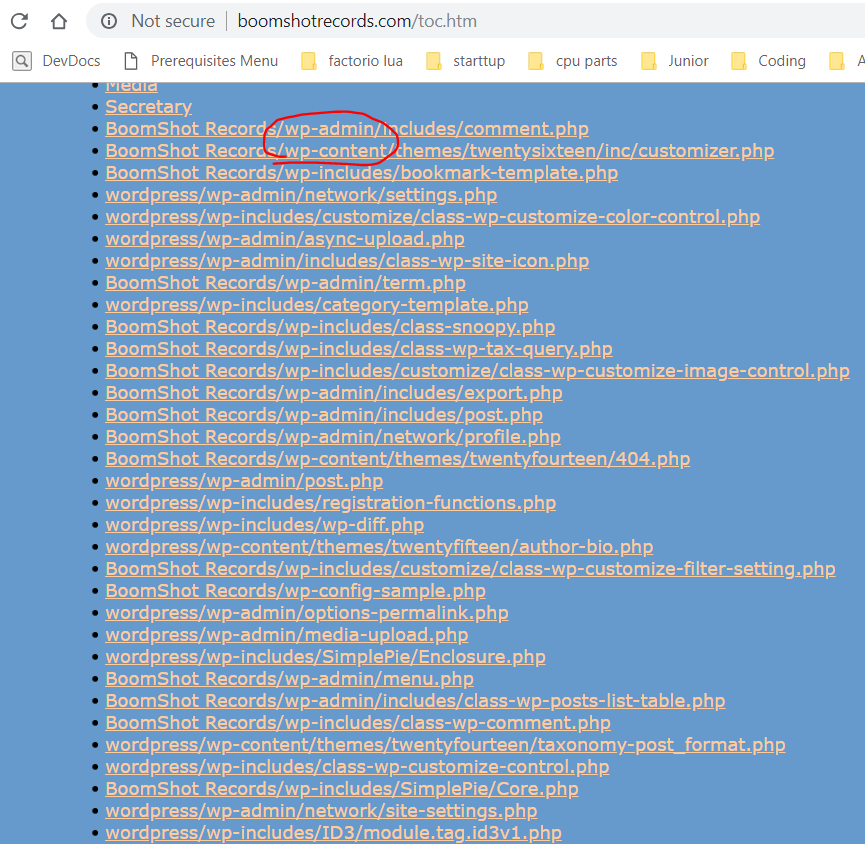
A WHOIS on **questinternet.net** gave me the same results.

I then looked up Kristofer’s email, [kris@questinternet.net](mailto:kris@questinternet.net), on Google. It gave me a lot of interesting results, mainly the websites of clients that Kristofer had created for them, as well as some miscellaneous things.

I also discovered, through using Maltego, that there were some subdomains of **questinternet.net** pointing to the same superdomain’s IP, namely **ftp**, **imap**, **pop**, and **mail**.

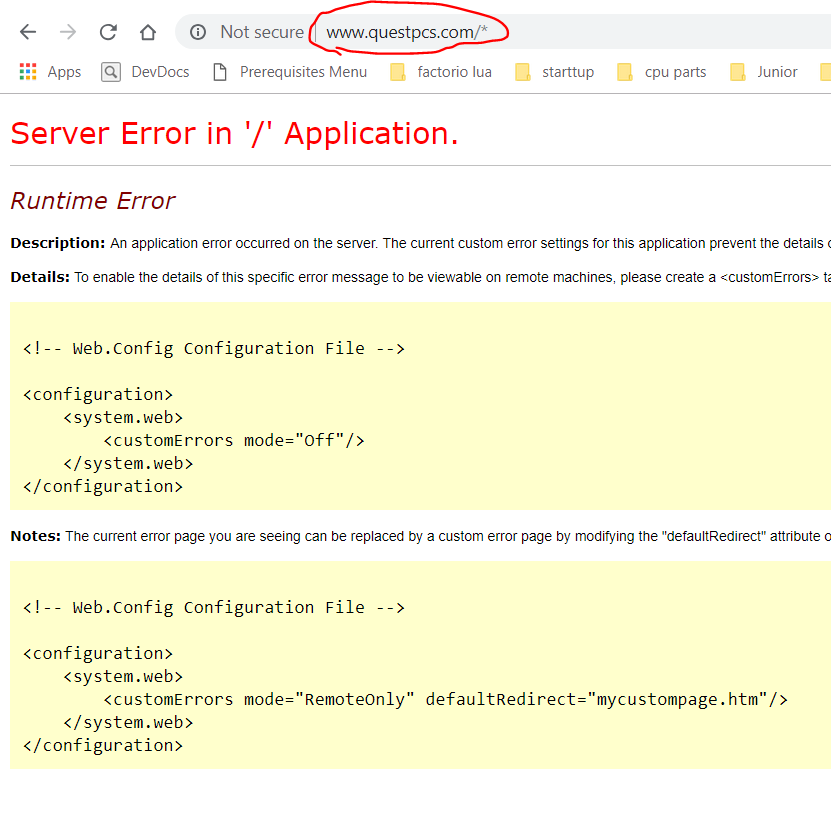
There is indeed an FTP server under the **ftp** subdomain, and this means there is likely an IMAP, POP, and mail server.

## Custom-made websites

As previously mentioned, when searching Kristofer’s information on Google, I found some websites that he had designed. Most of them were very quaint, 2000’s-esque hand-coded (uuuugly!) sites, but one stuck out.

A WordPress website under the name “Boomshot Records” that looked normal at first glance, but I explored the site, and eventually came to their Table of Contents page, which showed me what seemed to be a full directory map of their site, PHP files included!

Unfortunately (for me), when asking for the PHP files, I didn’t get any source code, just the result of the webserver running them.

Included in this directory is the results of a recursive wget of the site and PHP files, so we can see their structure, guess what version of wordpress they have, and see all addons!

# Other notes

## Similar error pages

It seems that if I navigate to {sitename}/\*, or {sitename}/&, I can cause a handful of websites to throw an error, all in the same format. They are listed below:

* [http://boomshotrecords.com/\*](http://boomshotrecords.com/*)
* [http://questinternet.net/\*](http://questinternet.net/*)
* [http://questpcs.com/\*](http://questpcs.com/*)

This error page format tells me that they are all running ASP.NET.

## Open FTP server

There is an open FTP server running at <ftp://ftp.questinternet.net/>. Funnily enough, because the sub-domains all point to the same IP, you can connect to <ftp://mail.questinternet.net/> and still get a connection.

## Outlook Web App Server

At <https://mail.questinternet.net/owa>, you get a login screen for “Outlook® Web App”.

# What did we get?

## Personal Information

We know the following about Kris:

* Kristofer M. Luck
* [kris@questinternet.net](mailto:kris@questinternet.net),
* [info@questinternet.net](mailto:info@questinternet.net),
* 773761356
* 7301 N Sheridan Rd, Chicago, IL, 60626-2261

## Websites that Quest owns

* <https://www.questnetworkservices.com/>
* <http://questpcs.com/>
* <http://questinternet.net/>
* <http://questnetwork.wix.com/>
* <http://questpcs.blogspot.com/>
* <https://www.facebook.com/questservices/>
* <https://twitter.com/questcomputer>

## Websites that Quest has made

* <http://www.boomshotrecords.com/>
* <https://www.evangelicalcatholicchurch.org/>

## Misconfigured servers/URLs

* <http://boomshotrecords.com/toc.htm>

* [http://questpcs.com/\*](http://questpcs.com/*)
* [https://mail.questinternet.net/\*](https://mail.questinternet.net/*)
* [http://boomshotrecords.com/\*](http://boomshotrecords.com/*)
* <http://boomshotrecords.com/wordpress/wp-admin/>
* <http://questinternet.net/wordpress/wp-admin/>

## Open servers

* <ftp://questinternet.net/>
* <ftp://boomshotrecords.com/>
* Maybe more!