****

**Open Source Intelligence [Passive Reconnaissance]**

**Submitted by:  
 Cathal Murphy – B00095643**

**James Finglas – B00094138**

**Primrose R Nyagwaya – B00099882**

*School of Informatics*

*Department of Informatics and Engineering*

*Institute of Technology, Blanchardstown*

*Dublin 15.*

**Word Count: 4674**

**Bachelor of Science**

**Computing in Information Technology**

**01/11/2018**

Contents

[Abstract 3](#_Toc528874169)

[Introduction / Scope 3](#_Toc528874170)

[Tools Used 4](#_Toc528874171)

[Media Article Search: 5](#_Toc528874172)

[Employment Search: 5](#_Toc528874173)

[Social Media & Profile Searches: 6](#_Toc528874174)

[Vision-net 7](#_Toc528874175)

[TheHarvester: 9](#_Toc528874176)

[TheHarvester continued 10](#_Toc528874177)

[CRO (Companies Registration Office) 11](#_Toc528874178)

[Recon-NG 12](#_Toc528874179)

[Visual Inspection of Website & Physical Premises 14](#_Toc528874180)

[Gathering Information about the Webserver 17](#_Toc528874181)

[Network Analysis 20](#_Toc528874182)

[Header, Burp Suite, Wire Shark & Network Miner Examination 20](#_Toc528874183)

[Plan of Attack 23](#_Toc528874184)

[Conclusions 24](#_Toc528874185)

[References 25](#_Toc528874186)

# Abstract

The goal of this report is to lay out the methods and tools used, in a passive sweep of the website https://www.diamondfurniture.ie/ with a view to preparing an active penetration test against the company. We will lay out the methods used, tools, datamined results and analysis of data mined.

# Introduction / Scope

Here, we lay out our scope for our passive penetration, which determines the active phase of the penetration test. As this was merely the planning stage, we obviously did not want the company or staff to become aware of our attempts to compromise or breach the security, therefore only passive tools and public level physical access were used for data mining. This naturally ruled out social engineering of staff during this phase. Our goal was as follows: to gather as much information as possible to map out a plan for carrying out a fast-active penetration, which targets all data points, and to compromise the company’s website to discover as many points of vulnerability as possible to be fixed.

The website and premises of the target company shall be included in the scope, as well as all external data points. However, no data points will be followed up beyond the plain text or source code of the site, or any data mined from the physical premises which relates to any third parties. Third parties may be listed as potential data points or points of vulnerability but may not be actively pursued at this passive stage.

First, we attempted to data mine as much information as possible form local media sources such as news articles be they online or offline. We then sought to determine if any employment opportunities were listed to the company or indeed if we could find any old employment listings. Next, we determined which tools to deploy and begun to data mine the website. This stage was crucial to laying out an effective plan for the follow up of an active penetration test. During this phase we also sought to discover any government official records pertaining to the company and staff.

The second stage began with gathering information from the website both plain text and source code and a visual inspection of the premises. Since an actual onsite inspection of the premises was not viable we chose to use google earth as a means of visually inspecting the premises.

The final stage included gathering information about the webserver and the technologies it was running allowing us to find potential exploits. This included a network analysis of traffic which was intercepted between the website and the client using third party tools. This intercepted traffic was then analysed for potential vulnerabilities.

## Tools Used

* The harvester
* Internet Archives (WayBackMachine)
* Discover (with custom scripts)
* ZabaSearch.com
* Youtube.Com
* Facebook.com
* Instagram.com
* Twiter.com
* Linkedin.com
* PIPL.com
* phonenumbers.address.com
* advancedbackgroundchecks.com
* 411.com
* Google
* CRO.ie
* Whois.com
* Recon-NG
* Shodan
* ipinfo.info
* netcraft.com
* cvetdails.com
* Wire Shark
* google chrome
* Burp Suite
* Network miner
* Yelp.com
* Vision-net.com

The deployment of our passive tools for datamining was the next and most crucial phase of the passive data mining.  
  
Finally, we collated all the data mined from our data points for analysis and present our conclusions and plan for the active penetrations test.

# Media Article Search:

A search for media articles, local national and international through google revealed very little. However, one article did turn up which had a high potential social engineering value.

*Diamond Living Foreclosure Article May 31, 2011 by John Mulligan independent.ie [1]*

This articled told us that the company, under its previous registered name ‘Diamond Living’, had acted as a trading agent for ‘Amaranth furniture’ operated by Mr. William Diamond since 2001. It also revealed that this previous agent had three premises, one in Airside (Swords), another in Liffey Valley and the final store in Longmile Road (current premises).  
  
The article goes on to highlight important financial information showing arrears at the time the article went to print. But one of the most useful bits of information is the revelation of an address for the parent company Amaranth Furniture at Beacon South Quarter, Sandyford Dublin. Finally, we learned that a fresh mortgage agreement had been arranged with the Bank of Scotland.

# Employment Search:

A search of all local and national employment data bases revealed no jobs currently being advertised. However, www.jobs.ie did list a yet undiscovered email: anders@diamondfurniture.ie.

# 

# Social Media & Profile Searches:

Since no social media is listed on the website a google search was undertaken to search for social media accounts related to the company and any profiles related to staff on indexing sites. It seems the company attempted to get some traction on twitter and failed. The first and last post was in 2014. [2] With only 19 followers and no retweets or posts it seems clear this account is now very much inactive.

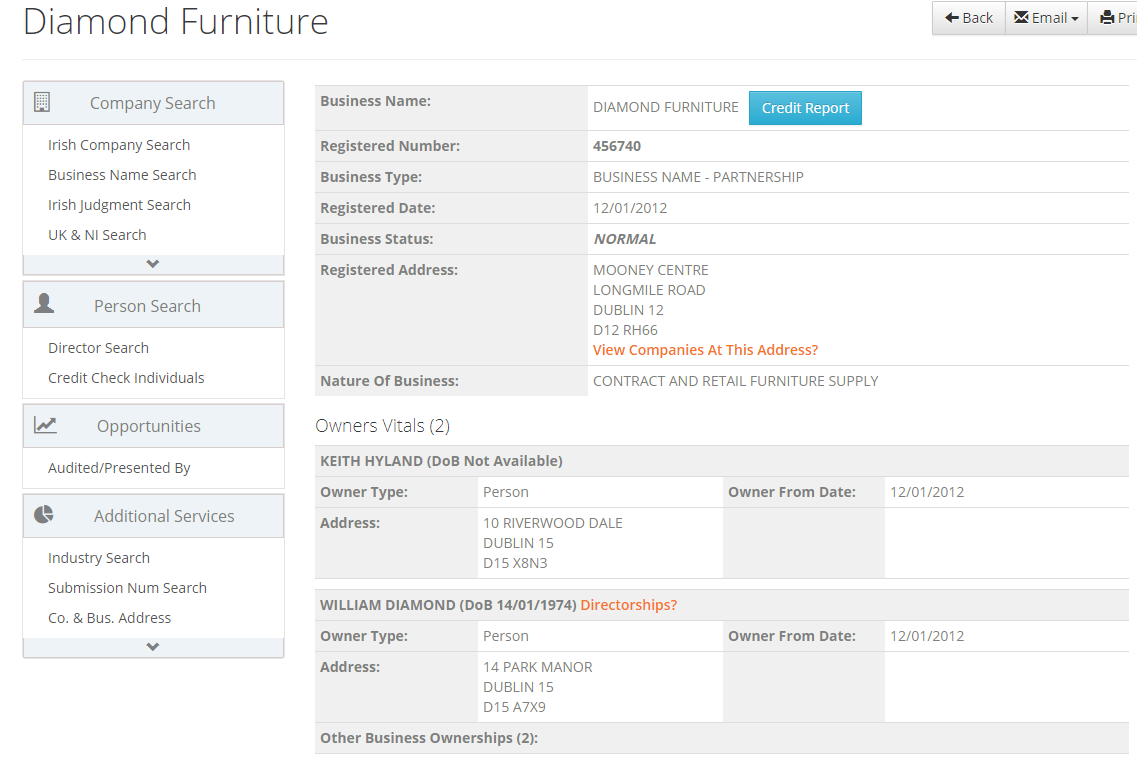
A Facebook account was found and is active, however, this account is managed incognito. Having searched through the account for any useful information, a post is noted speaking of a recent marriage of a staff member named Karl. Following this link takes us to his profile page (https://www.facebook.com/karl.wade.5?fref=ufi&rc=p) and his new wife (https://www.facebook.com/leanne.mcdonagh.395?fref=ufi&rc=p). A messenger link is provided (m.me/diamondfurnituredublin). Finally, an email is provided (info@diamondfurniture.ie). The page information reveals the page has been in use since 2013. A post from 2015 from a customer mentions a staff member named “Owen”. This is our first and only reference to this potential staff member. One man named William in seen in all promotional videos displayed on the page.

A Google search of William Diamond Furniture led us back to this page https://www.diamondfurniture.ie/pages/contract. Interestingly this page is not currently listed as a link on the site and reveals that a Mr. William Diamond is the current company director, but this information is un dated. This page also has a broken referral link with some unauthenticated log on code. This must be investigated further during the active penetration test.  
  
These data points might prove useful for social engineering in the future. However, all in all it must be noted that yet again, data mining proves very difficult. This Is a good management strategy in terms of reducing the likely hood of social engineering.  
  
As a follow up on Mr. William Diamond, the following sites where also used to attempt to data mine information: ZabaSearch.com, Youtube.com, Twitter.com, linkedIn.com, PIPL.com, phonenumbers.addreses.com, advancedbackgroundchecks.com and 411.com. Despite this extensive search only 1 result was found at LinkedIn.com https://www.linkedin.com/in/william-diamond-53730b65.

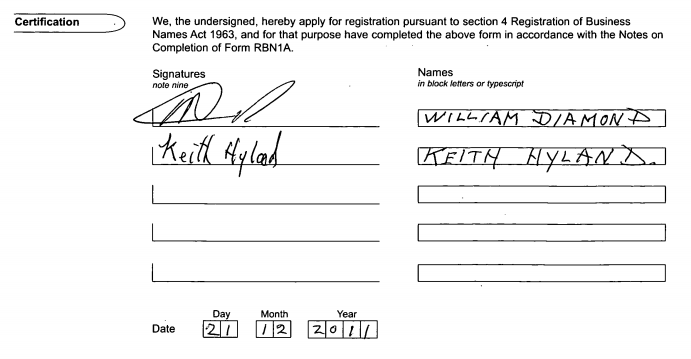
A search of Instagram revealed an account believed to belong to the target company. [3] However, a crawl of this account revealed only the company’s current phone number which is of course declared on the website.

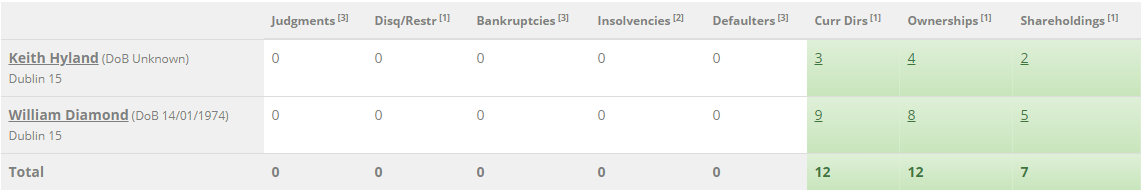
A curious google search highlighted a Yelp.com review https://www.yelp.ie/biz/diamond-furniture-dublin which talks about a “Keith” being the manager, which when put together with the E-mail we data mined earlier this gives us an interesting data point for social engineering. Having established the social media footprint seemed to be small, it was appropriate to make use of automated tools.

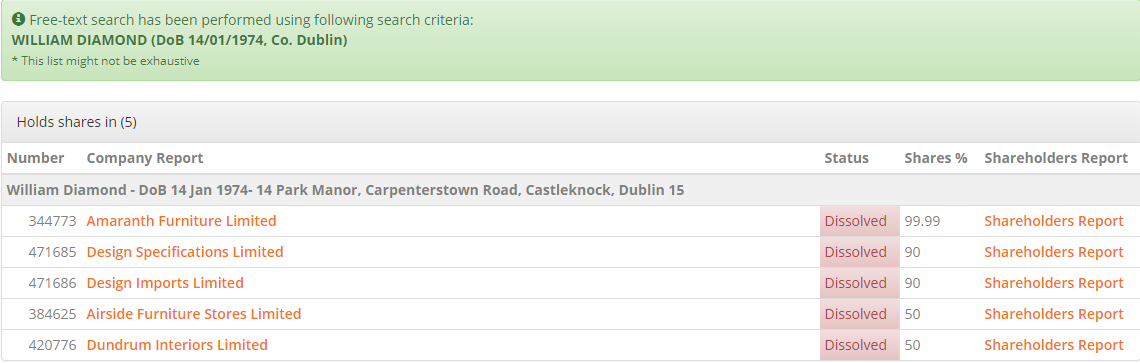
## Vision-net

Vision-net is a website that holds information on all companies in Ireland and the UK. Usually this is a paid service and subscriptions can be set up to be paid annually or per-click usage. We, however, discovered that on the Meath county council website, they have a link to the website that allows you to input your library card and access the website’s tools for free. [4]

*Vision-net search results on Diamond Furniture*

As shown in the image above we gathered a lot of information on the company, including who has ownership of the company along with their addresses. We also retrieved their documents from the Companies Registration Office (C.R.O) here which gives us more information on the owners as well as their signature.

*Screenshot from vision-net*

Vision-net also showed us information on the owners via a credit report. As shown in the picture above we can see a lot of information on the owners past including judgments, directorship (or disqualification thereof), bankruptcies, insolvencies, defaulters, ownerships and shareholdings. The website also lists each of these as shown in the example below.

*Screenshot from vision-net. William Diamond’s shareholdings*

This is all good information to have because now we developed an in depth look at not only the company’s history and ownership but also the owner’s other companies or even bankruptcies he may have. This also tied into previous information gathered about the company’s liquidation of “Diamond Living”. [1]

## TheHarvester:

The initial passive sweep with the harvester began with an unlimited sweep through Google’s API. This returned 4 hosts:

* .diamondfurniture.ie: empty
* www.diamond furniture.ie: 23.227.38.32
* mail2.diamondfurniture.ie: empty
* www.diamondfurnite.ie: 23.227.38.32.

*Initial Harvester sweep.*

And 4 E-mail addresses:

* Anderson@diamondfurntiure.ie
* deirbhile@diamondfurniture.ie
* info@diamondfurniture.ie,
* keith@diamondfurniture.ie.

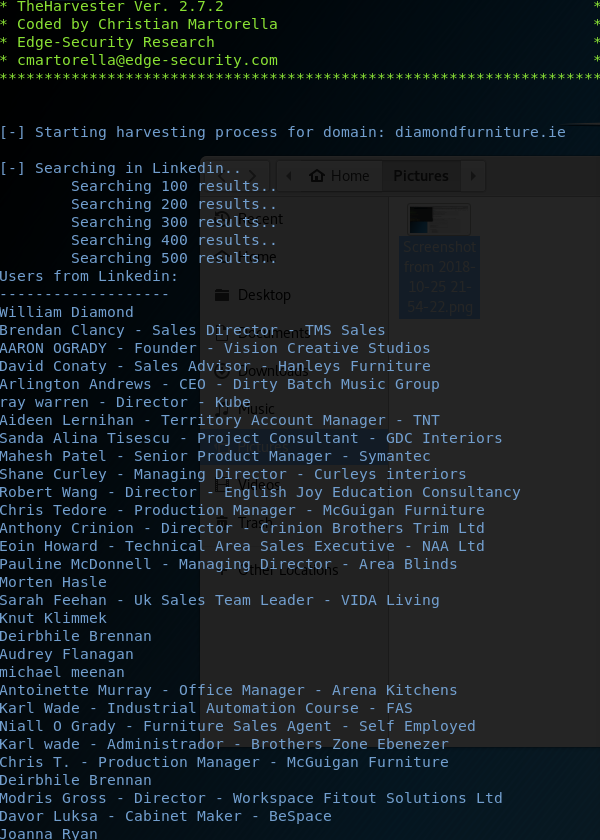
## TheHarvester continued

Next the same passive sweep was performed but through all non-google APIs (some sources are excluded and will be searched manually). This search returned the same results with one additional email: William@diamondfurniture.ie.   
  
The next sweep was directed through LinkedIn.com and returned a lot of interesting results. One of the results appears to be directly related to the target company. Looking back at one of the E-mails The Harvester revealed we see this E-mail listed: deirbhile@diamondfurniture.ie. We also see that name listed here: Deirbhile Brennan. This gives us a new target of opportunity and a new data point. A quick Facebook search reveals her account: https://www.facebook.com/deirbhbrennan. A recent post posted on 21 September 2018 tells us she is still currently in the employ of the target company.

One resulted is listed as a self-employed furniture sales person so this result was examined closer: Niall O’ Grady. Social media accounts failed to return any accounts connected to this individual. While the other results do not immediately appear to be directly connected to the company there is value in the results from a social engineering perspective.

Finally, we added in a reverse DNS query search just to double check to see any other hosts where found to be alive and connected to our previously discovered host however no new hosts where detected.

Purely on intuition, it was felt that we should have received more information on the search although the harvester is a strong tool. We thought it was important to double check our results using other tools that we could perhaps incorporate the use of more APIs (Advanced Programming Interfaces). For this purpose, we selected Recon-NG as it is a much stronger tool which was likely to both confirm our previous results and expand upon our current result set.

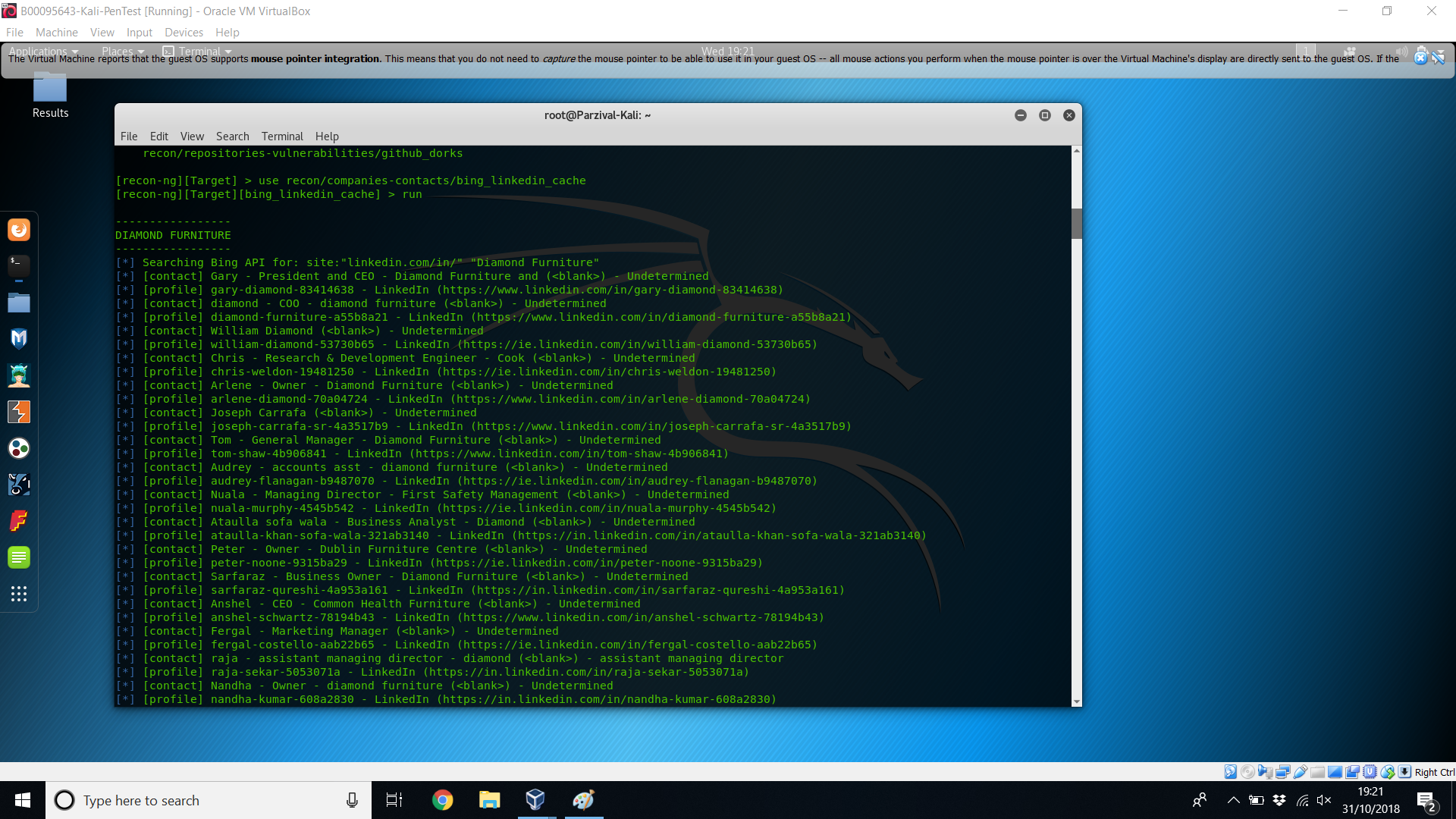


*LinkedIn harvester sweep.*

## CRO (Companies Registration Office)

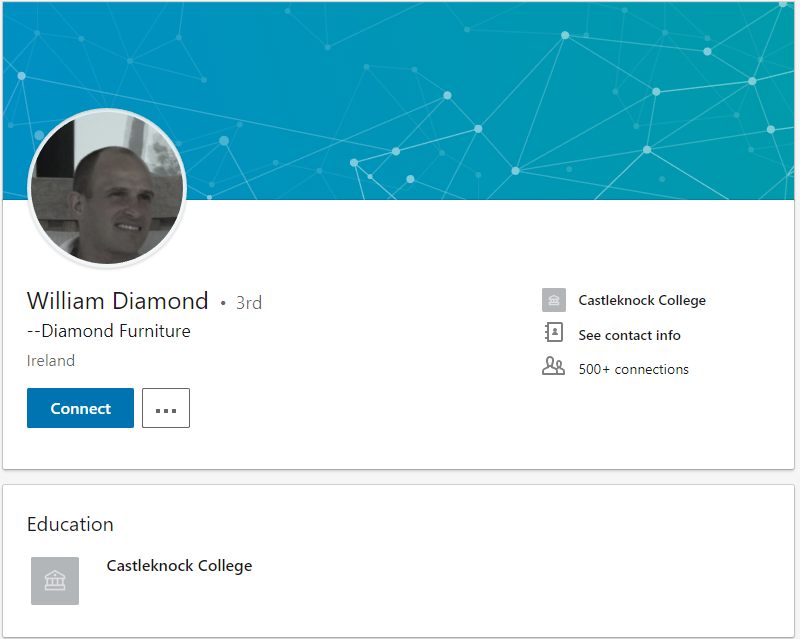
A CRO search of the company reveals that the company formally traded as diamond living and has existed since 2002 with yearly renewals of the business license. No other useful information is revealed in the search. The most recent license listed (457998) is a body corporate license. This information could be used to request tax data however due to time constraints this step was deemed to be out of scope at this stage.

## Recon-NG

Recon-NG is a web reconnaissance framework that comes with a suite of modules that gather information about a target (Must have API Keys to use this tool). We first used Recon-NG’s Bing-linked-in-cache search which harvests profiles related to a given company.

*Recon-ng results*

In the screenshot above, you can see the results of the harvest. It gave us details on people who may have worked or are currently working at diamond furniture. It also gave us a link to each profile, so we could data mine more details on each of them. This confirmed our previous results as well as giving us some extra potential data points.

As discovered earlier, we know that an owner of the company is William Diamond. So, when we looked through the result set we found him. In the results of the search there were three William Diamonds who came up, two of which were living in America, however the last one has information saying he went to Castleknock college and has Diamond Furniture in his profile which tied in with the information previously discovered. This is the confirmation we sought.

*Screenshot from LinkedIn page*

While the other results do not appear to be directly connected to the target company it was felt that there was strong potential that vendors/suppliers would be found therein.

# Visual Inspection of Website & Physical Premises

The initial visual inspection of the website suggests a modular design. The headers, banners, navigation bars and footers all appear to be modular with the main body being an object-oriented style of page calling. This is of course hard to say for certain without in depth analysis with tools and perhaps server-side access. However, our previous experience with PHP and object-oriented design and analysis helps us make some accurate guesses here. These guesses helped us determine the tools we used.

Having viewed all the main navigation bar links no plain useful plain text information is revealed in the body of the website.  
  
The header/banner reveals the year the company was established. Which could potentially be used in social engineering, or perhaps with a view to requesting tax records.  
  
A “My Account”, “Cart” and “Search” function was included in the navigation bar. A database is being used of some sort and some sort of query language is implemented. Again Netcraft.com determined which platforms are being deployed.  
  
The footer of the site did reveal some very basic information. A contact us link led to a useful map containing the physical address of the company. Unit 1, E.P. Mooney Business Park, Walkinstown Ave, Walkinstown, Dublin 12, Ireland. The “About Us” page is merely an abstract. Unlike many web sites this reveals no useful information pertaining to staff, this was a frustration from the perspective of data mining. This is very good in terms of security and certainly makes social engineering more difficult.

The “Contact Us” link reveals only the most basic information. Two phone numbers are provided (1850 45 44 44 / +353 1 450 8443) and a fax number (+353 1 450 5255). This Fax number may be a point of vulnerability. Fax machines can be easy to intercept and manipulate using exploits such as “Faxploit” [5] which could allow a hacker full control of a victim’s network. Furthermore, just having access to the fax number can often be used to implement social engineering strategies. The FAQ page revealed a pair of E-mails info@diamondfurniture.ie and keith@diamondfurniture.ie.  
  
Taking the companies address and entering it into google earth allowed us to perform a cursory analysis of the onsite security. The store had no external cameras covering the parking lot and rear areas to either deter, or video intruders after business hours.

  
  
*Google Maps Image of Diamond Furniture Store 1*



*Google Maps Image of Diamond Furniture Store 2*



*Public access to Rear loading area and refuse storage*

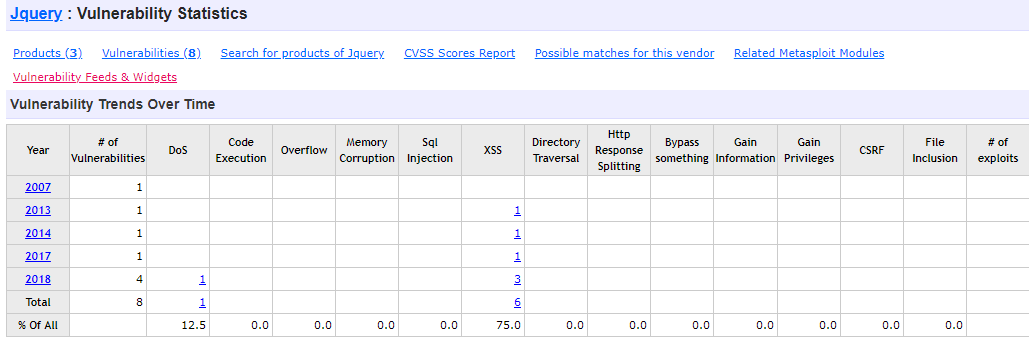
The visual inspection of the website revealed very little useful information which is good from the company perspective, but it does however make the job of datamining more difficult.  
  
The source code revealed client-side CSS, JavaScript and jQuery. This provides potential for manipulation. We can also see that the Shopify external module has been deployed. This provides potential for request intercepts via a proxy manager such as Burp suite.

As a final step in examining the website it was decided to take a shot in the dark to see if they had a Robots.txt file by searching for it on https://web.archive.org/ directly and it did have one. Luckily, it had been archived on the day the search was performed so it was as up to date as we could have hoped for. Over the course of the websites history the websites home page has been indexed 157 times however the sub-pages have less indexing. A sampling of these pages was examined. From the main index page, to the contact us page and the about us page to check for consistency and to see if any other useful data could be mined such as phone numbers, E-mails, or staff details. The data is quite consistent, with only the phone number changing (the old number is no longer in service).

# Gathering Information about the Webserver

To gather information about the webserver we used multiple online tools. Firstly, to use a wider range of tools we need to confirm the IP address of the domain (www.diamondfurniture.ie). This had been revealed using TheHarvester but to confirm, we used a website called ipinfo.info we ensured the IP address of the website is 23.227.38.32. It also gave us other useful information like the Geolocation of the IP which is where it is hosted. CA (Canada), ON, Ontario, K2P Ottawa.

Once we confirmed the IP address of the webserver a wider range of tools became available for use for analysis of the website. Before we used them however we first used a tool on a website called www.netcraft.com. This website displayed plenty of information on our target such as client-side scripting frameworks like jQuery which is great information to have it allowed us to use another website to check the current exploits of such technologies. The website we used is called www.cvedtails.com and it showed for instance that for several versions of jQuery there is potential for XSS (Cross-Site Scripting) and DDoS (Deliberate Denial of Service attacks). Using the combination of information gathered here, we have established a starting point for potential attacks to the server.



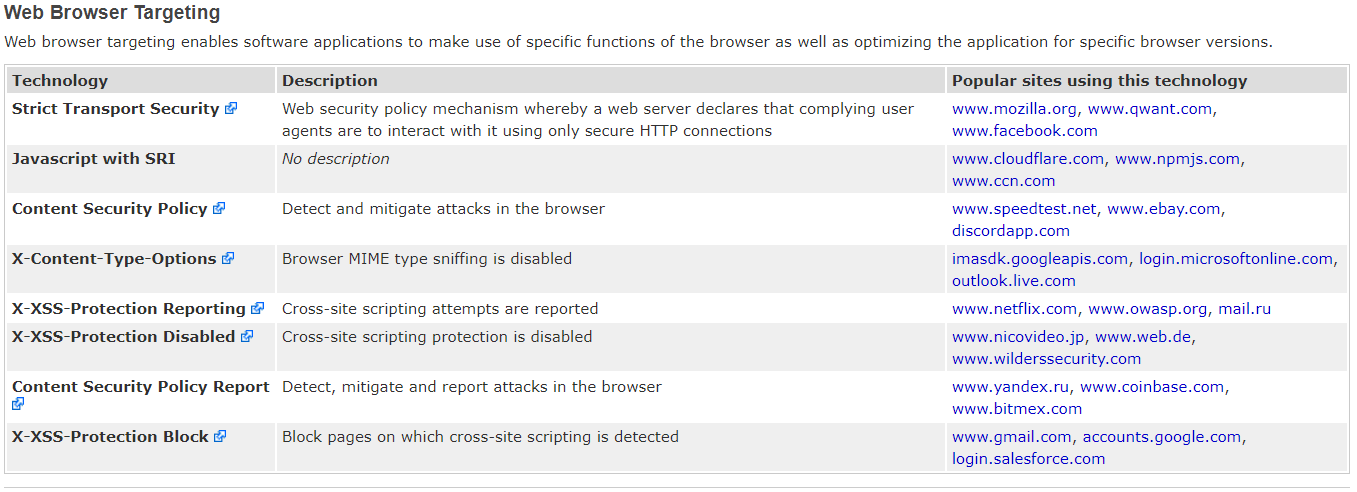
*www.cvedetails.com for jQuery*

In this case for jQuery it is possible to conduct a DDoS (Deliberate Denial of Service) attack due to...

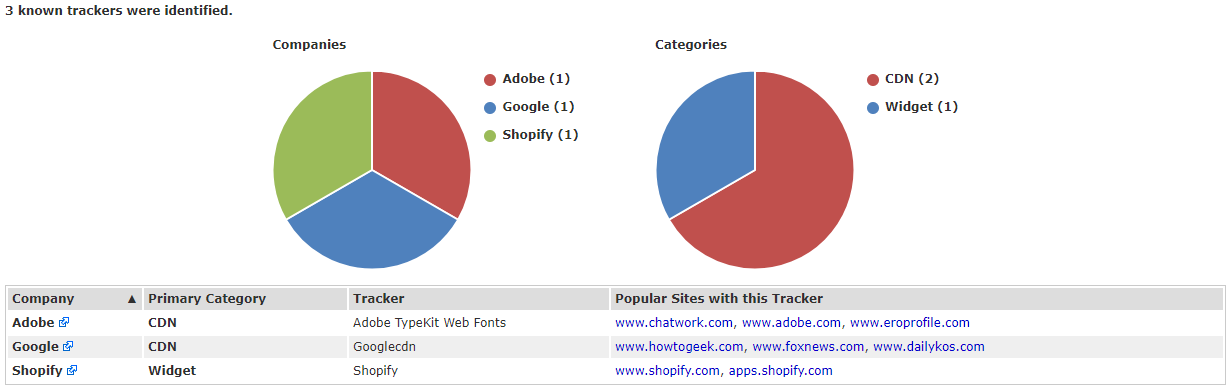
“removing a logic that lowercased attribute names. Any attribute getter using a mixed-cased name for Boolean attributes goes into an infinite recursion exceeding the stack call limit.” [6]

However, this exploit may only be on certain versions of jQuery, so it is important to find out what version the webserver is running first. However, this is currently out of scope for the passive phase.

Among the details of the Netcraft analysis, there was a section called Web Browser Targeting. In this section there were technologies that detect, report and mitigate Cross Site Scripting. This means that it would be unwise to attempt cross site scripting on this site.



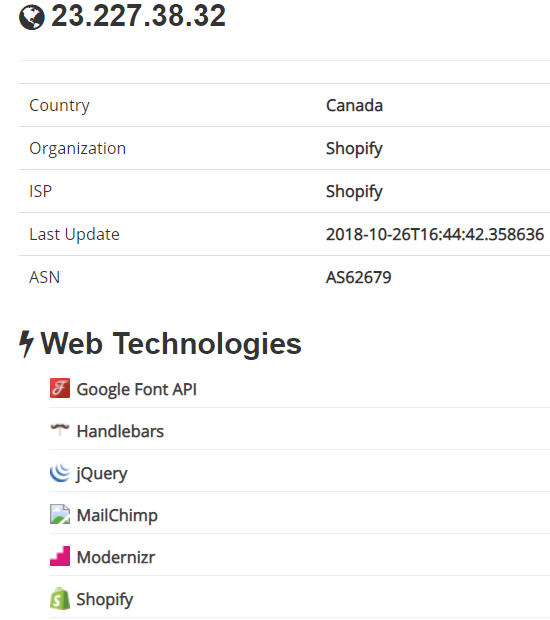
*NetCraft Web Browser Targeting.*

Netcraft also discovered multiple web trackers on the website which are third-party resources loaded onto a webpage

*Netcraft Web Trackers*

As shown in the picture above, there were three web trackers. Adobe Typekit Web Fonts, Googlecdn and Shopify. Shopify is an Ecommerce platform which gives us an idea where they got the website layout from.

Using another webtool called www.shodan.io we discovered other technologies on the webpage such as MailChimp and Handlebars which are both susceptible to Cross Site Scripting attacks however, as mentioned earlier, this website has technology that blocks cross site scripting. Shodan also revealed that ports 80 and 443 are open on the webserver. A port scan would be needed to see if there are any more ports open on the network however we did not port scan as it would not be passive reconnaissance.

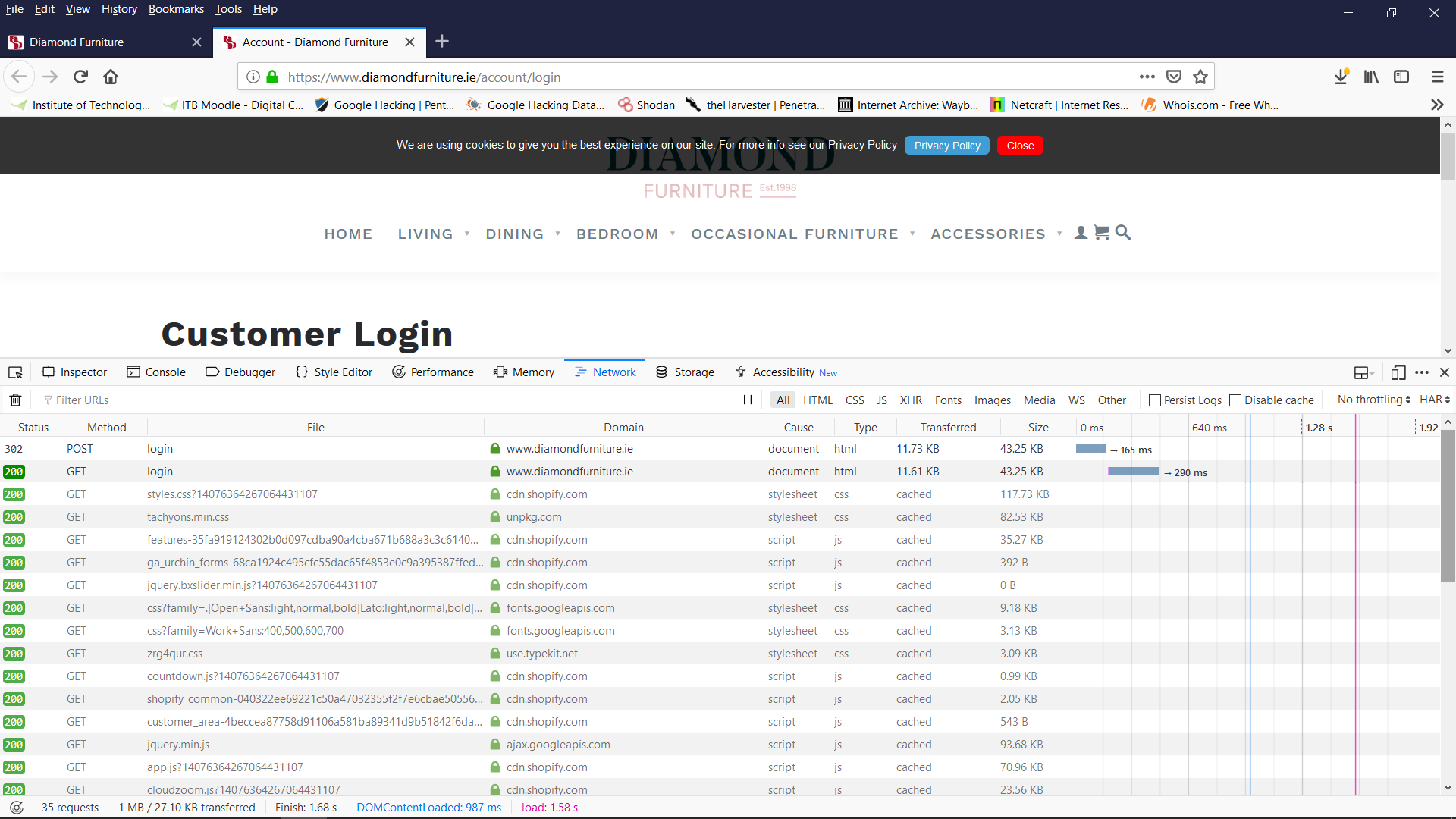


*www.shodan.io results for our target*

## 

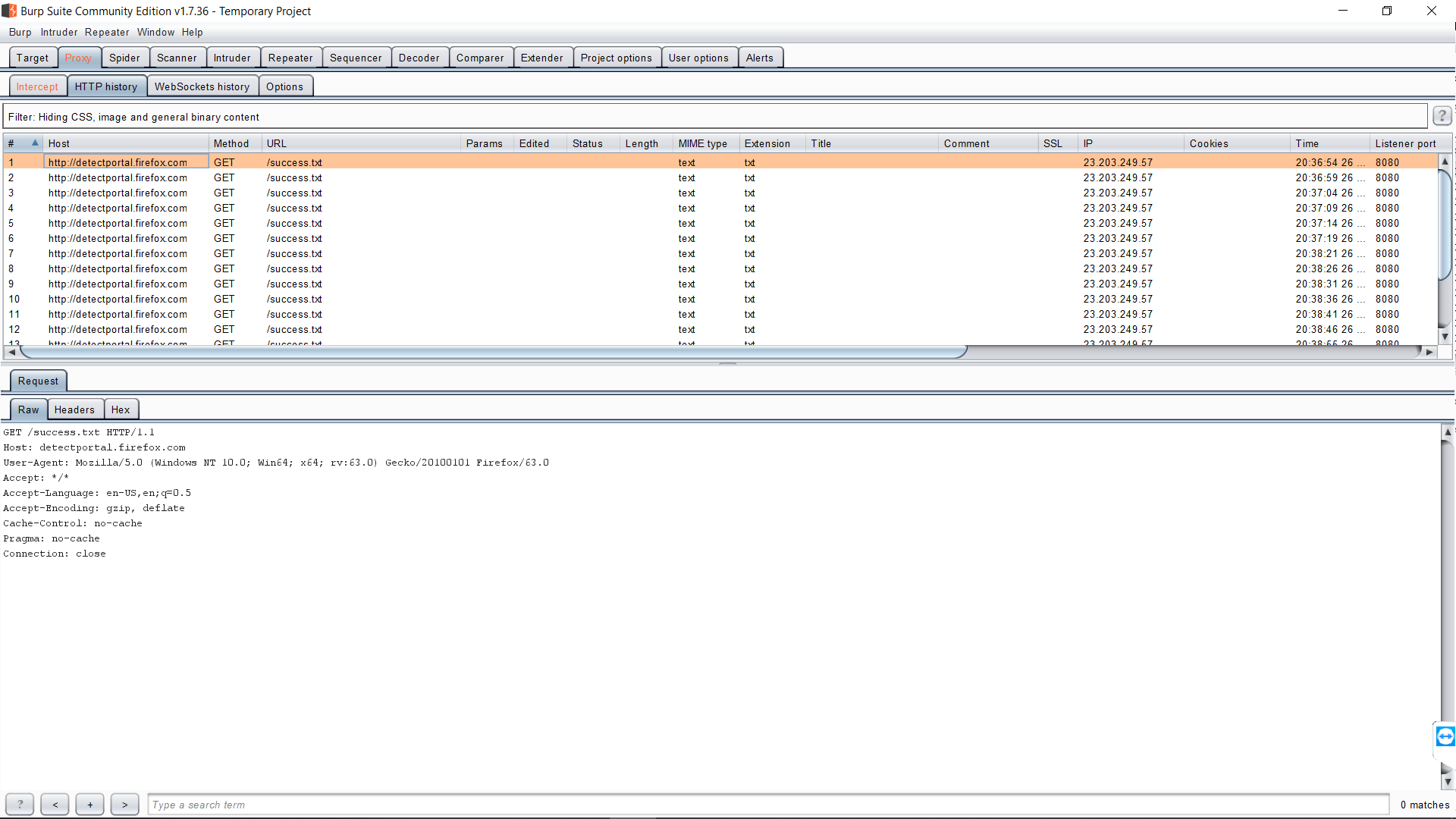
# Network Analysis

## Header, Burp Suite, Wire Shark & Network Miner Examination

An examination of the header was undertaken to see if any vulnerabilities might be found. No immediate vulnerabilities were found visually but it was noted that a post request was accompanied by a get request in the header. This means that potential there is some data being sent in plain text. So, to examine this possibility we needed to add in some more tools.

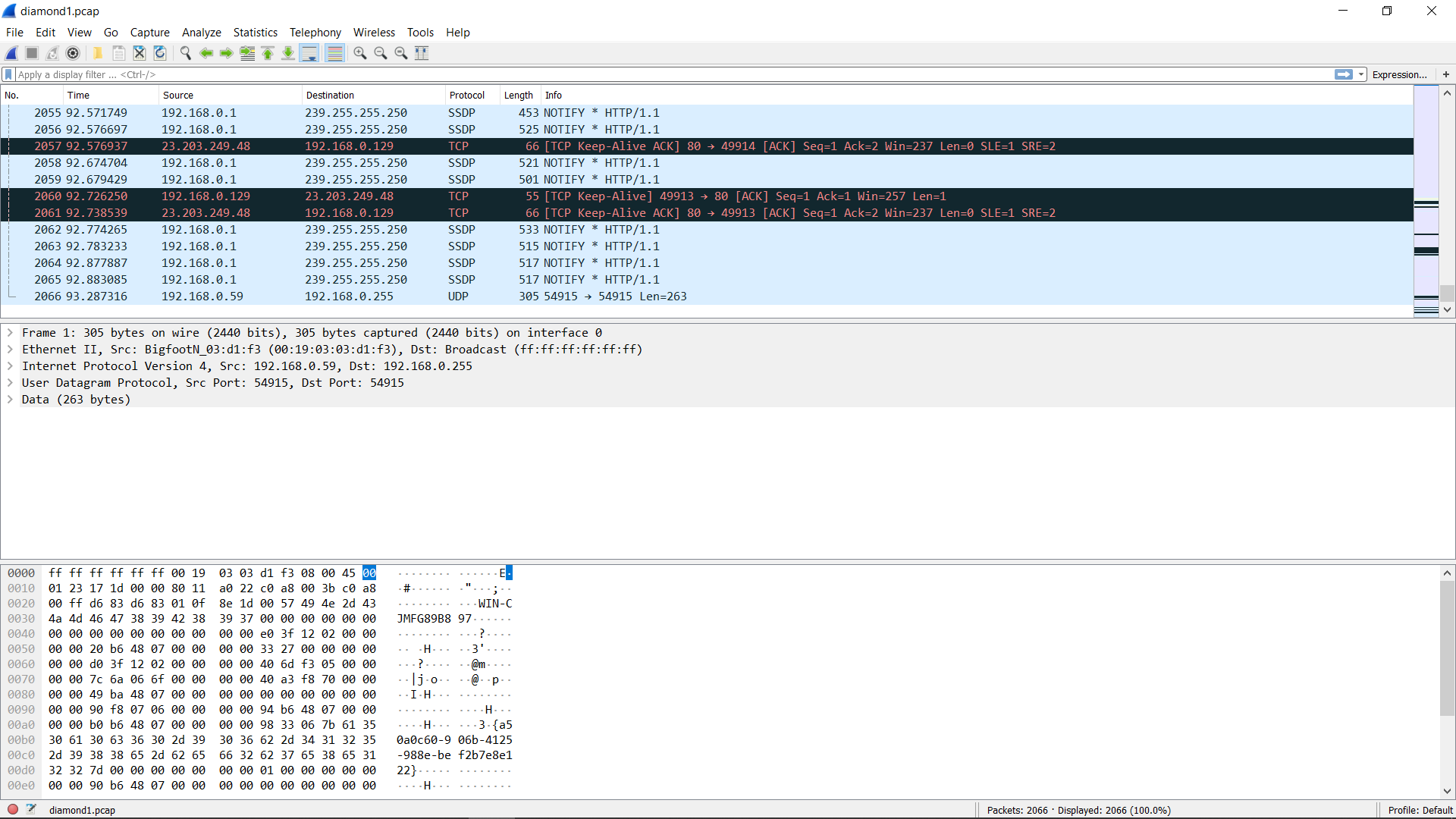
*Login in page header.*

Passing the header request through Burp Suite did not reveal any plain text information. This tells us that while we could potentially intercept data and manipulate it, with no client-side authentication, it is unlikely that this form of attack will help us.

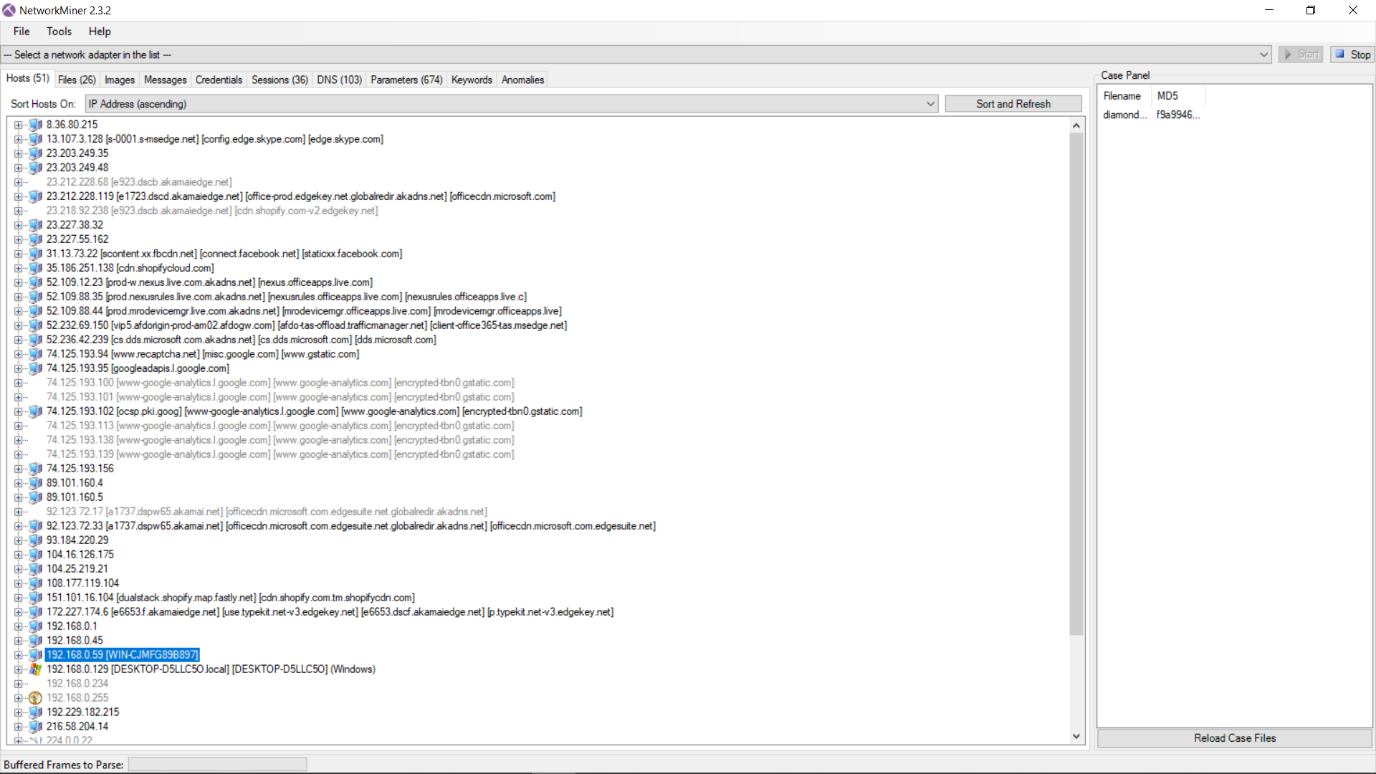


*Burp Suite examination of Log in page header.*

As a final step to rule out vulnerabilities that may not be as obvious, or beyond our ability to identify by a visual exam, we decided to first pass header traffic through Wire Shark for interception before passing the intercepted traffic through Network Miner to test for potential vulnerabilities.



*Wire Shark Intercept of Log in page header traffic.*



*Network Miner Analysis of Wireshark packet intercepts*

The Wire Shark intercepts and Network Miner Analysis did not reveal any points of vulnerability or obvious anomalies. This told us that before we begin to deploy aggressive active penetration tools, the client-side generated traffic was robust, and we would expect it to stand up to the most basic levels attacks.

# Plan of Attack

The goal of the active penetration will be to compromise the systems of the company, be they technical, online, or real-world staff manipulation via social engineering. The website, physical premises, staff (including any online account), external vendors/suppliers and tax records shall all be considered in scope for the active penetration test. No third-party websites, host, or systems beyond the host server of the website shall be deemed in scope, however all traffic coming from third party servers will be considered in scope for intercepting and manipulation before being forwarded back to the website should the need arise.

While the analysis of the Website did not reveal any obvious vulnerabilities, it would be foolish to simply presume basic level attack using SQL injection and XSS attacks would not work. However, as discovered earlier in netcraft, the website has mitigation and documentation of XSS attacks therefore care for consideration must be given to the deployment of XSS attacks.

The first phase of the attack should be an active port scan (Nmap) of the website IP address to determine what systems may be running and what ports may be vulnerable. System versions and operating details should also be scanned. In preparation for a potential brute force attack of vulnerable services such as FTP/SSH a word list should be prepared using all known staff details.  
  
Having combined the list of known technologies running on the host server with the system versions running on the website, a list of likely vulnerabilities and the strongest attacks against these vulnerabilities should be compiled.  
  
Fax vulnerabilities will be prepared and deployed against the stores local systems when appropriate to coincide with the technical penetration phase.   
  
While this phase of the attack is underway, a social engineering attack can be undertaken. Tax records should be sought to aid in the preparation of this attack. The store can be visited under the guise of a customer seeking to buy furniture, and as many staff as possible should be identified including delivery drivers. The purpose of this gathering of information will be to build up a picture of the current day to day operation of the company. Combining this information with previously gathered information, we can then attempt to contact the company to illicit as much financial, tax, and customer records as possible under the guise of an audit with members of our team posing as members of revenue services.

With our working knowledge of the company’s previous liquidation issues, it would be hoped that the company would likely be forth coming to avoid any unnecessary lengthy dealing with revenue services. Depending on the success of the social engineering, an attempt might even be made to physically gain access to the companies records at the store as part of our fake audit. Fax can also be used to help with this phase of the operation.

Should access be gained and our team be left alone to ‘examine’ records we will seek access to computerized records also. If any computers are locked our team will attempt boot up using a live kali Operating System to alter the SAM files to gain access to any systems running under windows. A flag will be deployed on any machines on which access is gained in store.

As this phase of the operation is deployed, it would be hoped that the company would be distracted; and the attack against the technical infrastructure could be deployed. While we do not anticipate any files regarding tax records being stored on the website server, we would hope to gain administrator access, and gain full database access which would allow us to gain customer records which could then be used to exploit customers.

Finally, we will investigate the existence of any data back-ups. Should data back-ups be found these should be copied too. As a proof of compromise flag, we will deploy a fake ransomware file which when executed will simulate a denial of service black mail attack.

# Conclusions

The investigation was reasonably difficult from a passive perspective with the website and staff having a surprisingly small footprint even at the national level. With the company being one of the more recognizable furniture sales stores in the greater Dublin area it was anticipated that the footprint would be larger. While it is not evident that this is an intended business practice, the anonymous management of the Twitter, Instagram and Facebook pages helps the company to avoid scrutiny. It would be recommended however that the staff should be encouraged from not posting to their personal accounts about the activities of the store as this makes them much easier to identify as potential soft social engineering targets.

It is also recommended that should any jobs be advertised externally, the company hosting the advertisement remove all record of the advertisement once the position has been filled.  
  
One area of potential weakness was the LinkedIn account of Mr. William Diamond, who’s account revealed at least one member of staff and several leads of potential vendors/suppliers to the company. It is recommended that all business links be held under a pseudonym account which could be managed anonymously similarly to the management of the Facebook page.

It is recommended that the fax machine use be immediately discontinued upon issuance of this report. This is a very vulnerable medium of communications not to mention outdated and serves no practical purpose in the advent of E-mail technology. This would be considered a high-risk area of vulnerability.  
  
From a technical perspective the company’s website again proved reasonably robust. No immediate points of vulnerability where detected at the passive level. While some information was gained that might lead to exploitation when more aggressive methods are employed, this is to be expected as the methods used to gain this information cannot easily be avoided. The Company seems reasonably insulated from basic level attacks.  
  
Our active penetration test will therefore be principally aimed at testing the staff adherence to company policy and resistance to being manipulated, which could put the company’s private access and records at risk. Should any weakness be documented in this area new company policy should be drawn up to negate this vulnerability and immediate staff retraining is recommended.  
  
Lastly, we shall test the how robust the server hosts technology is in defending against a determined aggressive active attack. The success or failure of this attack will determine the online risk to the company’s ability to generate custom from their website. Should it prove necessary recommendations can then be made as to improvements in security or even, potentially, a better host.

# References

1. John Mulligan, “Diamond Living to shut its doors and call in liquidator”, “<https://www.independent.ie/business/irish/diamond-living-to-shut-its-doors-and-call-in-liquidator-26737928.html>” , (accessed 01/11/18).
2. Diamond Furniture Twitter, <https://twitter.com/diamondfurni> , (accessed 01/11/18)
3. Diamond Furniture Instagram, <https://www.instagram.com/diamondfurniture_dublin/> , (accessed 01/11/18)
4. Meath county council website, <http://www.meath.ie/Community/Libraries/SupportforBusinessandEmployment/BusinessDirectory/#d.en.60873> , (accessed 01/11/18)
5. Check Point software technologies, “FAXPLOIT”, <https://blog.checkpoint.com/2018/08/12/faxploit-hp-printer-fax-exploit/> ,

(accessed 01/11/18)

1. CVE Details**,** jQuery Vulnerabilities, <https://www.cvedetails.com/vulnerability-list/vendor_id-6538/opdos-1/Jquery.html>, (accessed 01/11/18)