

**ASSIGNMENT 1 - RECONNAISSANCE**

**DUNNES STORES**



**Student Name:** Emmanuela Ogbene

**Student ID:** R00076703

**Course:** IT Management (Yr 4)

**Lecturer:** Sean McSweeney

**Date:** 15th March 2015

Table of Contents

1. **Introduction …………………………………………………........1 – 1**
2. **Specification………..…………………………………………....1 – 26**
   1. Activities……………………………………………………….1 – 23
   2. Deliverables…………………………………………………. 24 – 26
3. **Conclusion……………………………………………………… 27 – 27**

1. **Introduction**

The organisation that I have chosen to use reconnaissance to find information is **Dunnes Stores**.

Dunnes Stores, also known as **Dunnes**, is a retail chain that is based in Dublin, Ireland. Dunnes Stores primarily sells food, clothes and household wares. The company is privately owned and was founded in 1944 in Cork City, by Ben Dunne.

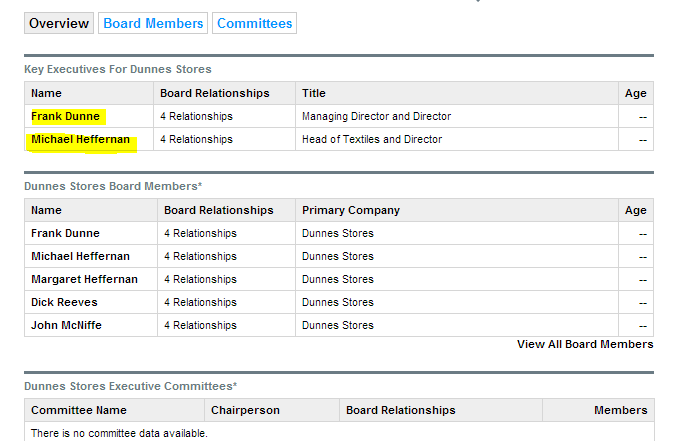
In addition to its main customer base in both parts of [Ireland](http://en.wikipedia.org/wiki/Ireland), the chain has operations in England, Scotland and Spain. The format of the chain’s stores includes a grocery [supermarket](http://en.wikipedia.org/wiki/Supermarket) operating alongside a clothing/textiles store.

1. **Specification**

# Activities

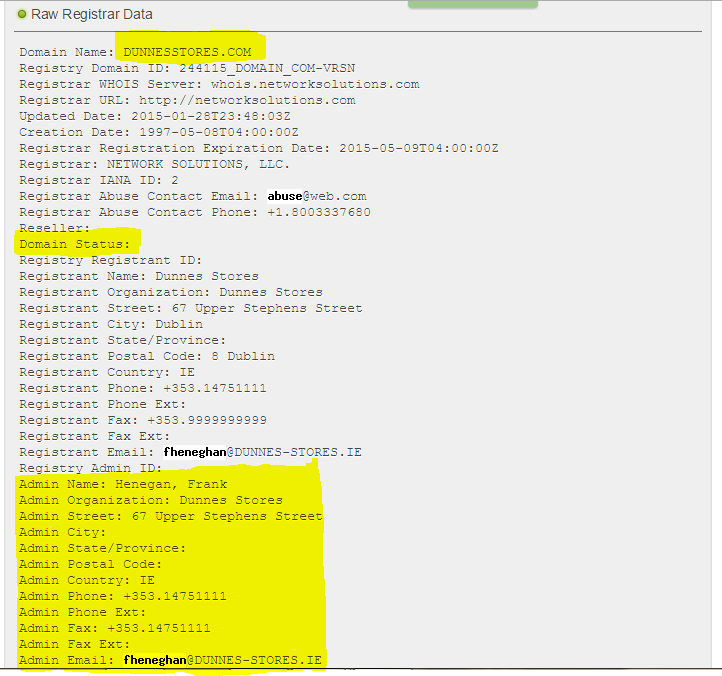
* + 1. **Find who is the boss, who are the IT people:**

1. **who is the boss:**



In other to find out who is the boss, I used the Search Engine **“Google”**. I was able to find out the information in the screen shot above i.e. **Frank Dunne** as the Managing Director and Director, **Michael Heffernan** as the Head of Textiles and Director, etc. This information was obtained on their website **“dunnesstores.com”**.

1. **who are the IT people:**



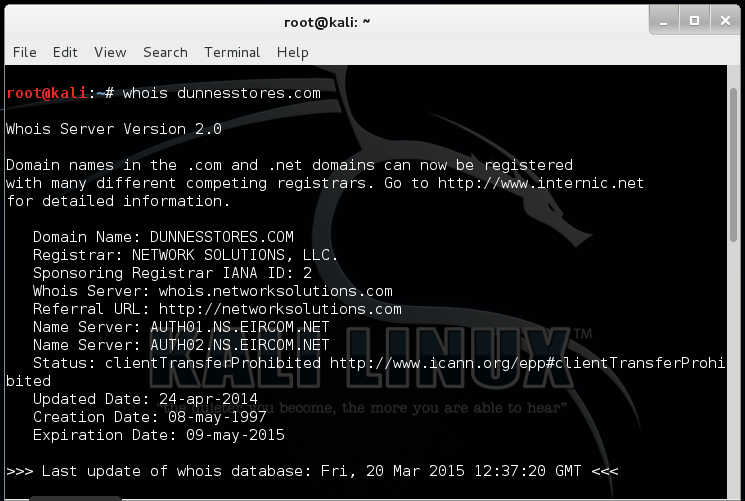
Using **whois**: [**https://who.is/**](https://who.is/)website, I was able to gather information on the IT people of the organisation. The screen shot above shows that **Henegan, Frank** is one of the Administrators for Dunnes Stores. Also, it shows more information such as the address, phone number, and email address about the IT person.

* + 1. **Find IP ranges and servers**

To find **IP ranges and servers** the following reconnaissance were used:

1. **whois**

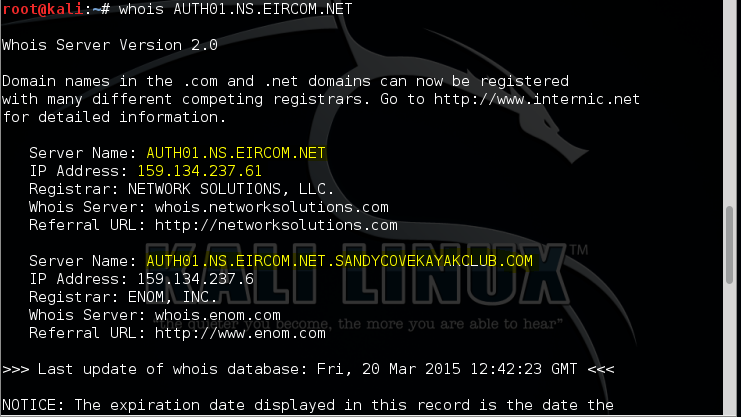
* Using the command: **“whois dunnesstores.com”**



With the above command, I was able to find the organisation’s **name servers**. From the screen shot above, it shows two name servers that the organisation is using: **AUTH01.NS.EIRCOM.NET** and **AUTH02.NS.EIRCOM.NET**. These name servers are provided by Eircom Net.

Apart from this information, you can see that with the command it shows the domain name as **Dunnesstores.com**, Registrar as **Network Solutions,** LLC, the whois server, updated date, the creation Date and the Expiration Date.

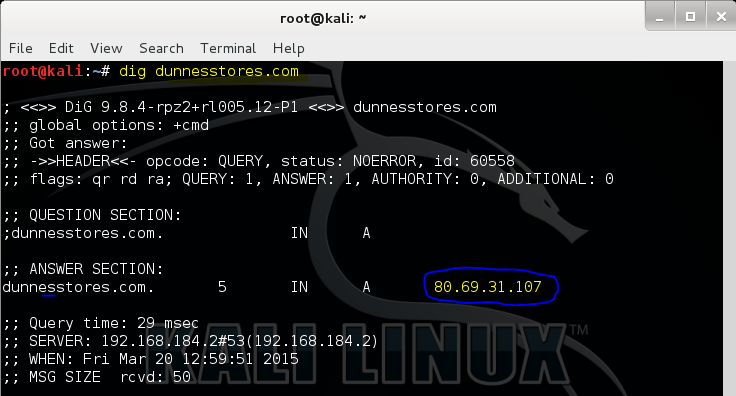
* Using the command: **“whois AUTH01.NS.EIRCOM.NET”**



With the above command, I was able to find information on the name server. This information includes IP Addresses associated with the name server: **159.134.237.61, 159.134.237.6.**

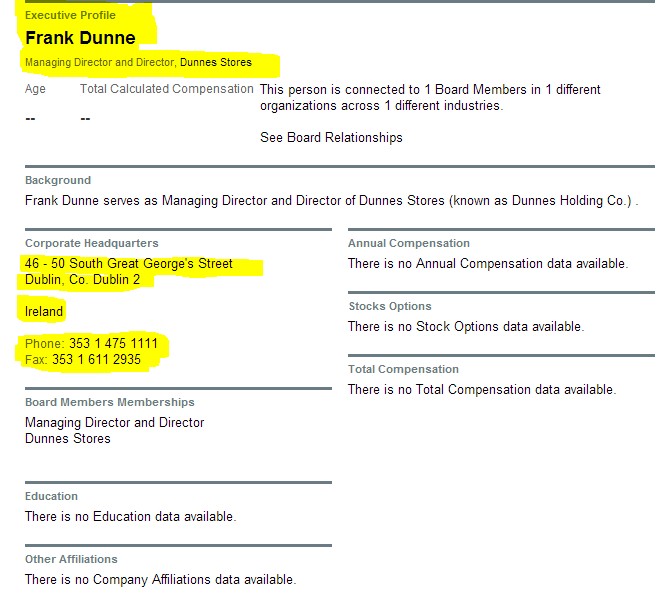
1. **dig**

* Using the command: **“dig dunnesstores.com”**



With **dig** command, I was able to find the IP ranges of Dunnes Stores. The screen shot above shows **80.69.31.107** as one of the ip addresses that Dunnes Stores use.

* + 1. **Find phone numbers and addresses**



1. Going to the organisation’s website by using the Search Engine, I was able to find out the phone numbers and addresses of the Managing Director and Director Frank Dunne. From the screen shot above, it shows an executive profile. The screen shot shows:

**The Address:** 46 – 50 South Great George’s Street Dublin, Co. Dublin 2 Ireland.

**The Phone Number:** 353 1475 1111

**The Fax Number:** 353 1611 2935

Apart from this information, it shows that **Frank Dunne** serves as **Managing Director and Director of Dunnes Stores (**known as **Dunnes Holding Co.)**. There is no information about his Education and other Affiliations because, these information are restricted.



1. Moreover, in order to gather more information on the phone numbers and addresses, **whois** web search engine was used. After providing the domain name on the whois search engine tool, the screen shot above was captured.

It displayed the following information about Dunnes Stores:

**Registrant Street Address:** 67 Upper Stephens Street

**Registrant City:** Dublin.

**Registrant Postal Code:** 8 Dublin

**Registrant Country:** IE

**Registrant Phone:** +353. 14751111

**Registrant Fax:** +353. 9999999999

**Admin Street:** 67 Upper Stephens Street

**Admin Country:** IE

**Admin Phone:** +353. 14751111

**Admin Fax:** +353.14751111

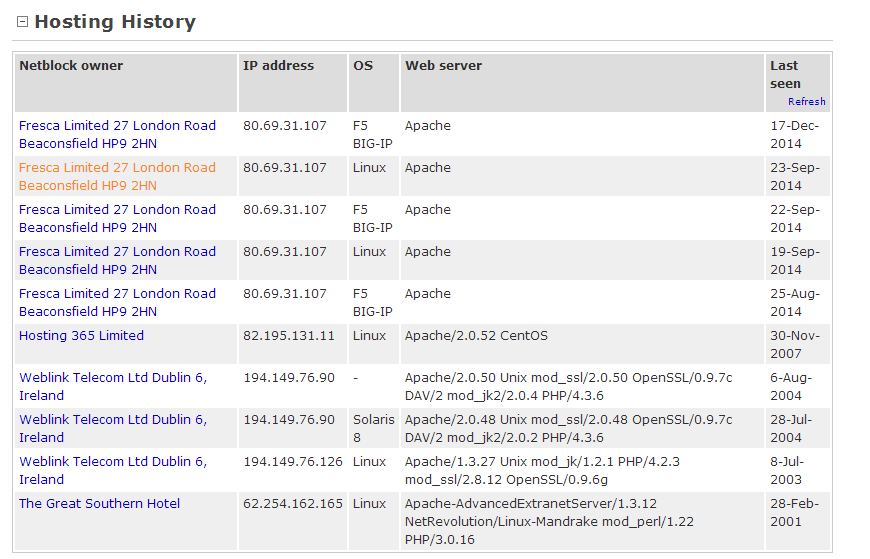
* + 1. **Find email addresses**



In order to find **email addresses**, **“whois”** web Search Engine was used. From the screen shot above, it shows the Registrant Email:[**fheneghan@**DUNNES-STORES.IE](mailto:fheneghan@DUNNES-STORES.IE).

Admin Email: [**fheneghan**@DUNNES-STORES.IE](mailto:fheneghan@DUNNES-STORES.IE).

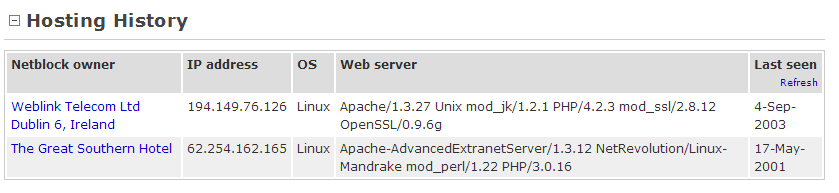
* + 1. **Use netcraft to find webserver version and OS**



1. With the company’s domain name: **“dunnesstores.com”,** I was able to use **netcraft** to find the webserver version and OS. From the screen shot above, it shows Dunnes Stores hosting history. Here, you can see a list of the Netblock owner, IP address, OS, Web server and Dates for last seen.

In addition, the list of **OS** used by Dunnes Stores varies from Linux, Solaris 8 and F5 BIG-IP. You can see that **F5 BIG-IP** is currently being used.

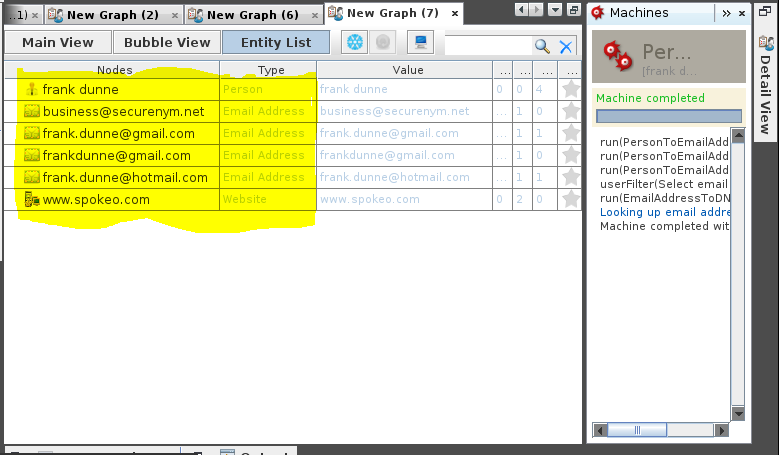
The currently used webserver version for Dunnes Stores is Apache. This is also last seen around 17th of December 2014. The version isn’t displayed for this current date. But from the screen shot, you can see that around 30th November 2007, Apache/ 2.0.52 CentOS was used. While the OS at that time was Linux.



1. On the other hand, I tried using another Dunnes Store’s domain name: **“dunnes-stores.ie”** on netcraft to find out webserver version and OS.

The information on the screen shot above was captured. I was able to find the Web server version: **Apache/1.3.27 Unix mod\_jk/1.2.1 PHP/4.2.3 mod\_ssl/2.8.12 OpenSSL/0.9.6g.** And the OS as: **Linux** that was used.

* + 1. **Use maltego to find staff email addresses, Web sites associated with the person, phone numbers associated with the person, social groups that are associated with the person, companies and organizations associated with the person.**



With the machine selected on the **“Person – Email Address”** using **Maltego**, I was able to find information about **Frank Dunne** the Managing Director and Director of Dunnes Stores. These information includes his Gmail, Hotmail and other email addresses associated with him. Also, it includes website associated with the same person.

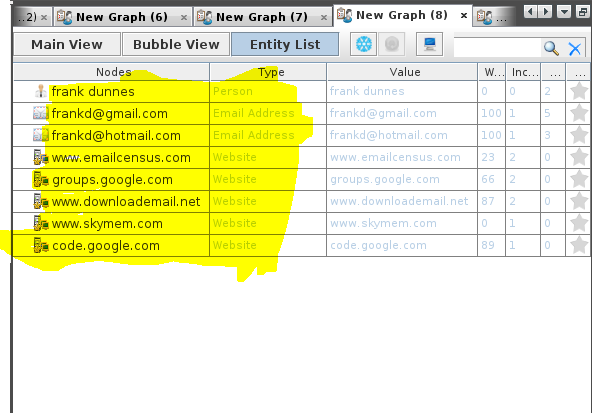
[business@securenym.net](mailto:business@securenym.net) – **Email Address**

[frank.dunne@gmail.com](mailto:frank.dunne@gmail.com) – **Email Address**

[frankdunne@gmail.com](mailto:frankdunne@gmail.com) – **Email Address**

[frank.dunne@hotmail.com](mailto:frank.dunne@hotmail.com) – **Email Address**

[www.spokeo.com](http://www.spokeo.com) – **Website**



Using **Maltego**, with the machine also selected on the **“Person – Email Address”** but with additional term being used to specify the person, I was able to find more information about the staff: **Frank Dunne**. These information includes his Gmail, Hotmail addresses associated with him. Also, it includes website associated with the same person. Such as:

[frankd@gmail.com](mailto:frankd@gmail.com) **Email Address**

[frankd@hotmail.com](mailto:frankd@hotmail.com) **Email Address**

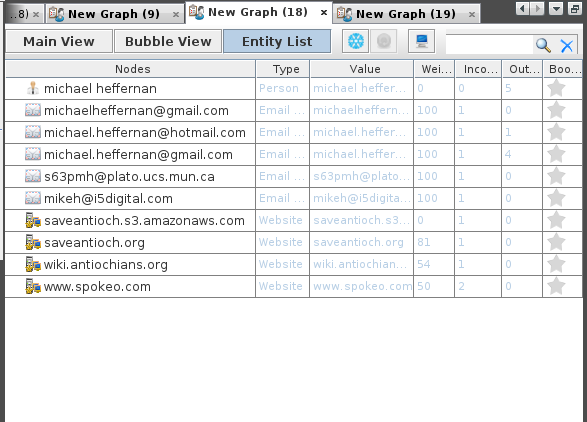
[www.emailcensus.com](http://www.emailcensus.com) **Website**

groups.google.com **Website**

[www.downloademail.net](http://www.downloademail.net) **Website**

[www.skymem.com](http://www.skymem.com) **Website**

code.google.com **Website**

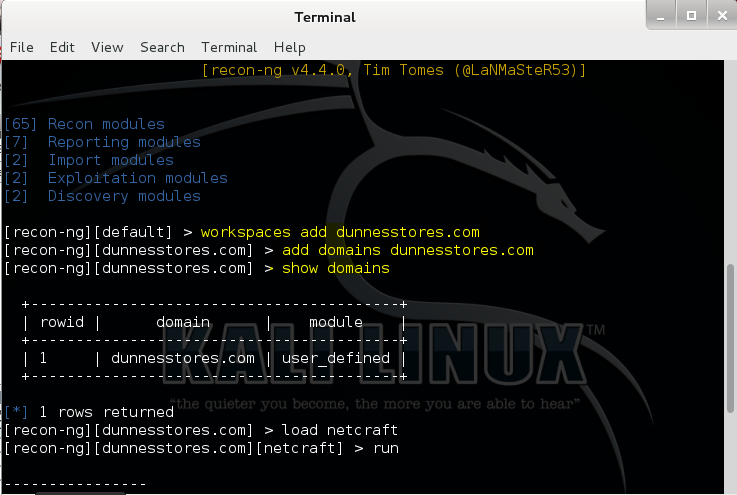


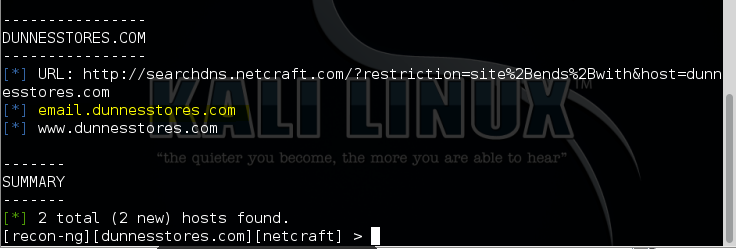
With the machine selected on the **“Person – Email Address”** using **Maltego**, I was able to find information about another staff: **Michael Heffernan**. These information also includes his Gmail, Hotmail and other email addresses associated with him. Also, it includes website associated with the same person such as:

[michaelheffernan@gmail.com](mailto:michaelheffernan@gmail.com) **Email Address**

saveantioch.org **Website**

* + 1. **Use recon-ng to webcrawl for information.**

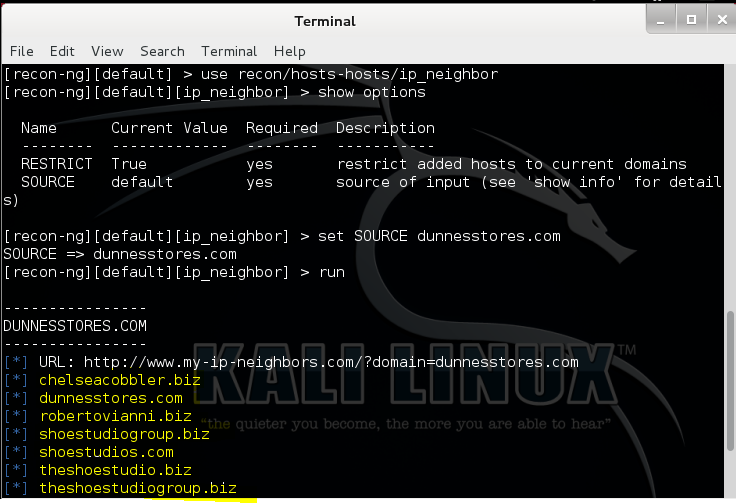


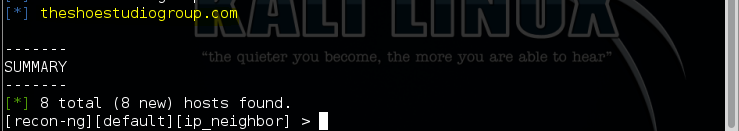


In order to webcrawl for information, the following commands shown in the screen shot above was entered. After running the above recon-ng commands, I was able to gather the following information such as:

**email.dunnesstores.com –** The email server used by Dunnes Stores Network.

[**www.dunnesstores.com**](http://www.dunnesstores.com) – The Domain Name Server.





To webcrawl for more information, the commands shown in the screen shot above was entered. These commands are my-ip-neighbors lookup recon module commands which checks and leverages my-ip-neighbors.com site for other hosts, hosted on the same server.

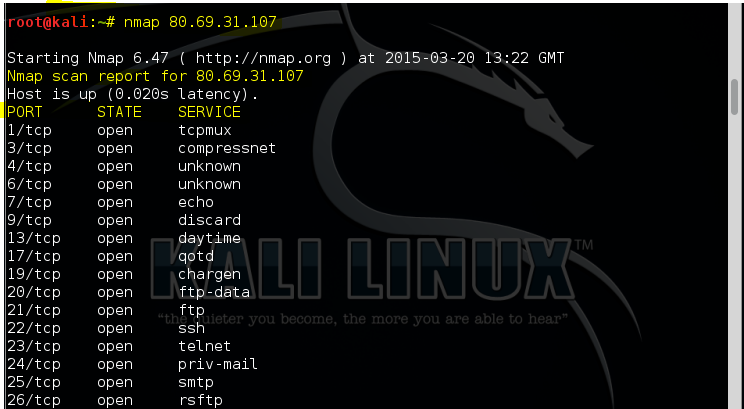
These commands are very useful because, it lets me discovery relationships. Therefore, the screen shot above shows that my website is hosted on a shared system with other sites that have vulnerabilities or exploits. That is **dunnesstores.com** web server shares the same server with any other hosts such as: **theshoestudio.biz, chelseacobbler.biz** and **theshowstudiogroup.com**.

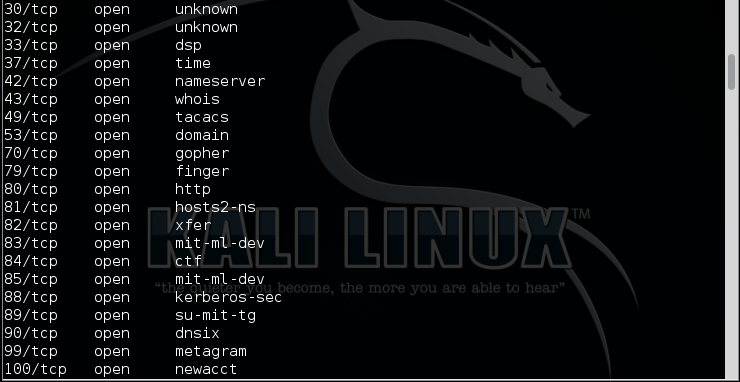
* + 1. **Use the other tools detailed in the lectures and any others available that you may find to improve your information.**

1. **nmap**

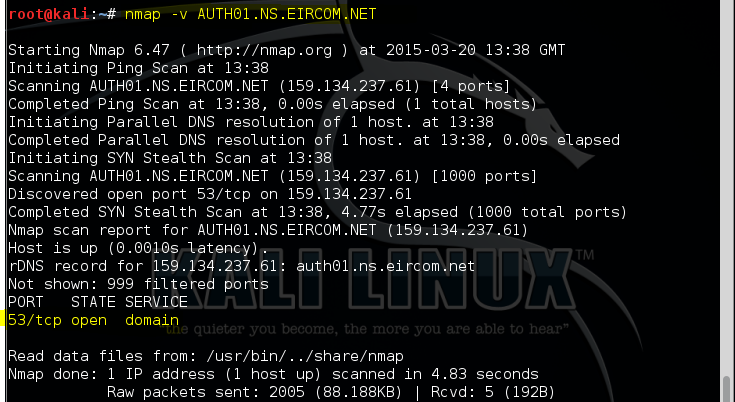
* In order to improve my information, the command **nmap <ip-address>** was used. The ip address is one of the ip ranges used by **dunnesstores.com**.

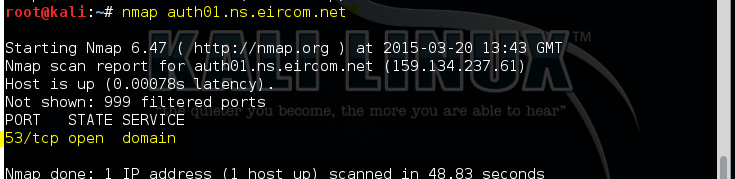
Using the command: **“nmap 80.69.31.107”**, I was able to find out so many ports that are open and their services. For instance, port 21/tcp is open on ftp service.





Using the command: **“nmap –v auth01.ns.eircom.net”** and **“nmap auth01.ns.eircom.net”**.

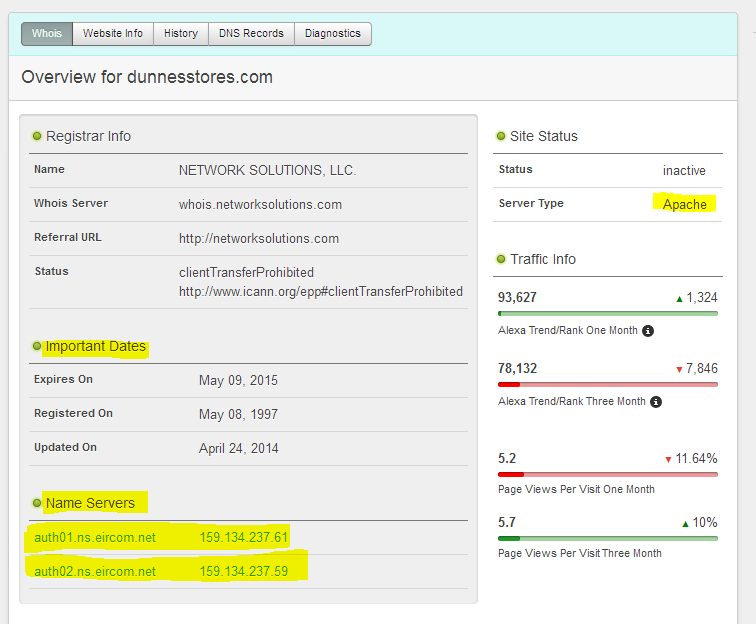




From the screen shot above, it shows the port, the type of port, the state and the service about the name server used by Dunnes Stores.

1. Using **“**[**https://who.is/**](https://who.is/)**”** web search

I was able to gather more information on **dunnesstores.com** name servers. The screen shot below shows the ip-addresses associated with the name servers.



1. Using[**http://whatmyip.co/**](http://whatmyip.co/) tool

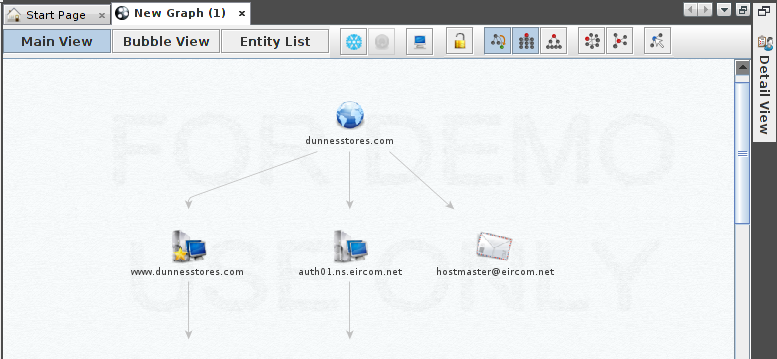
By using this tool, I was only able to get the information shown in the screen shot below i.e. the website Name servers and information on the IP Address: **80.69.31.107**. From the screen shot below, it shows that two live websites using the IP address.

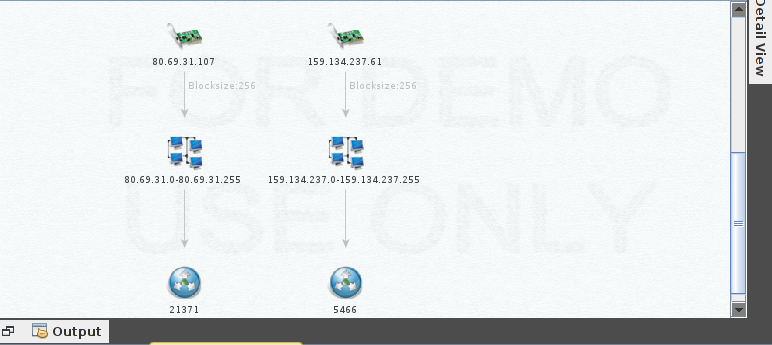




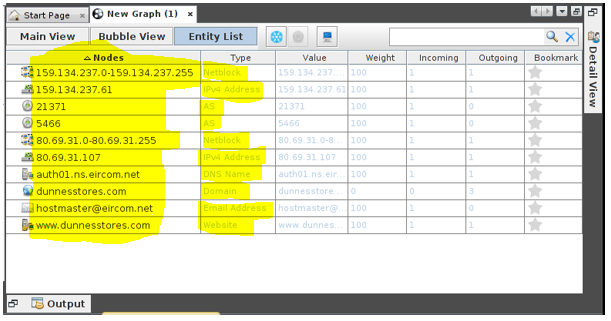
1. **Maltego (URL To Network And Domain Information)**

**Displayed as Main View**



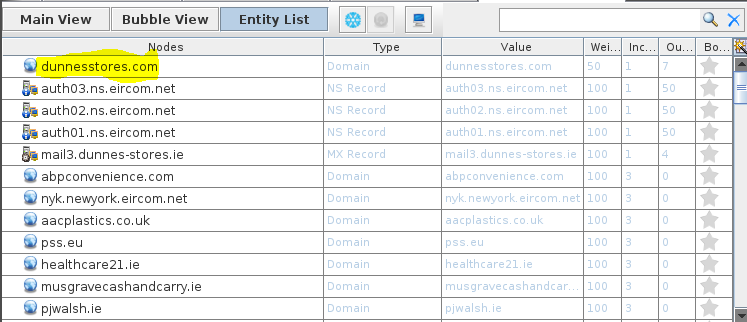


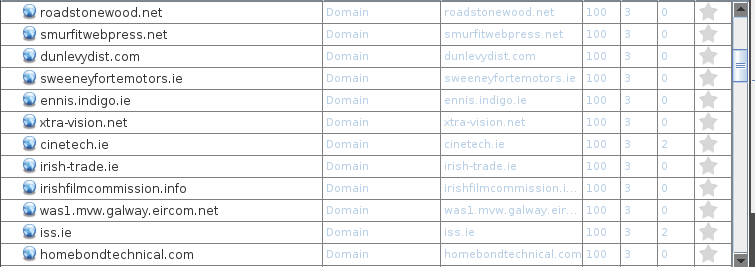
**Displayed as an Entity List**

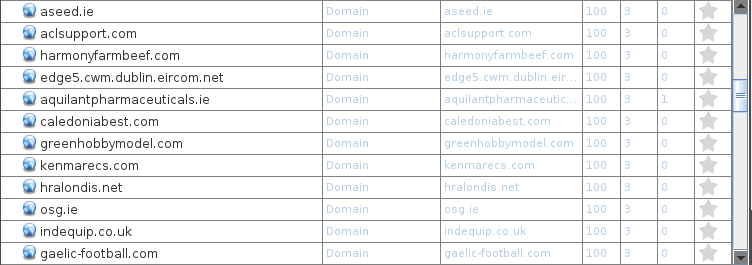


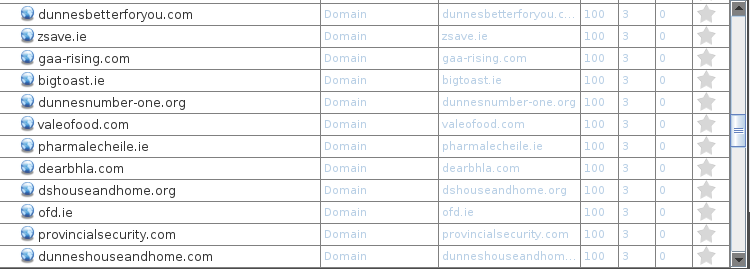
With the machine selected on **“URL To Network And Domain Information”** using **Maltego**, I was able to gather information about **dunnesstores.com** as shown in the screen shot above. These information includes different Netblock ranges, IPv4 Addresses, AS, DNS Name Servers, Domain Name, Email Address, and Website as shown above.

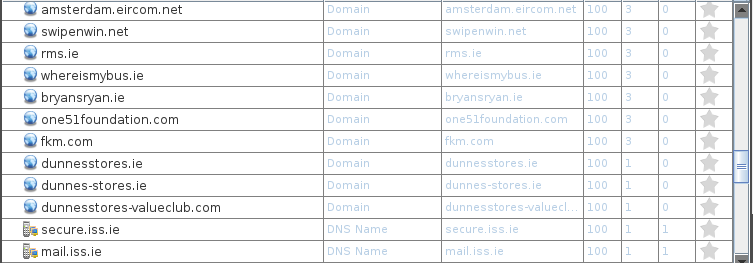
**Maltego** (i.e. **Footprint L3**)

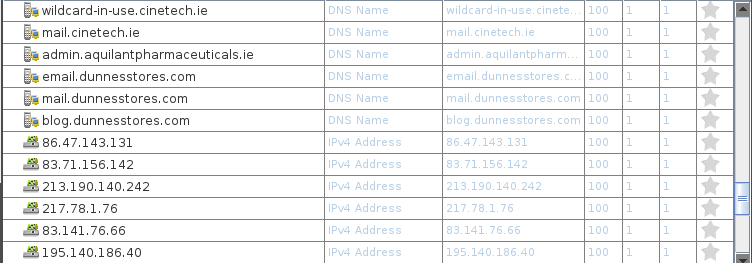


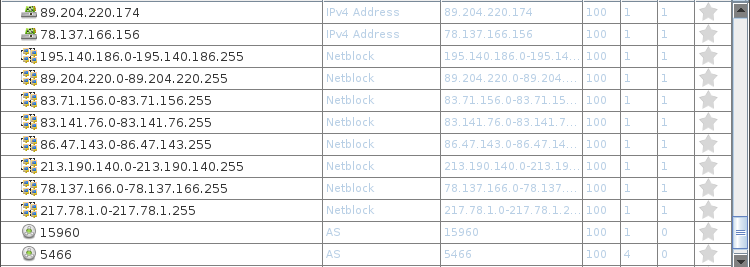








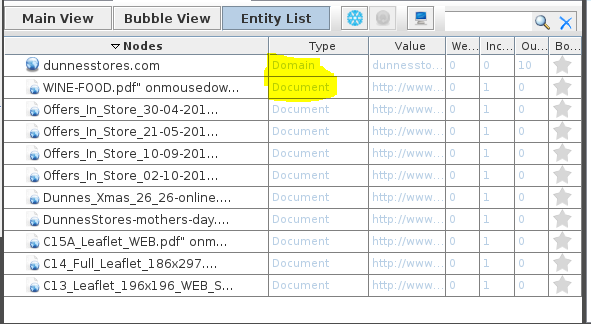






With the machine selected on **“Footprint Level 3”** using **Maltego**, I was able to gather more information about **dunnesstores.com**. These information includes the domain name, MX Records, Name Server (NS) Records, DNS Names, IPv4 Addresses, Netblock ranges, AS records, and other domains. All these details are shown in the screen shot above.

**Maltego** (i.e. **Company Stalker**)

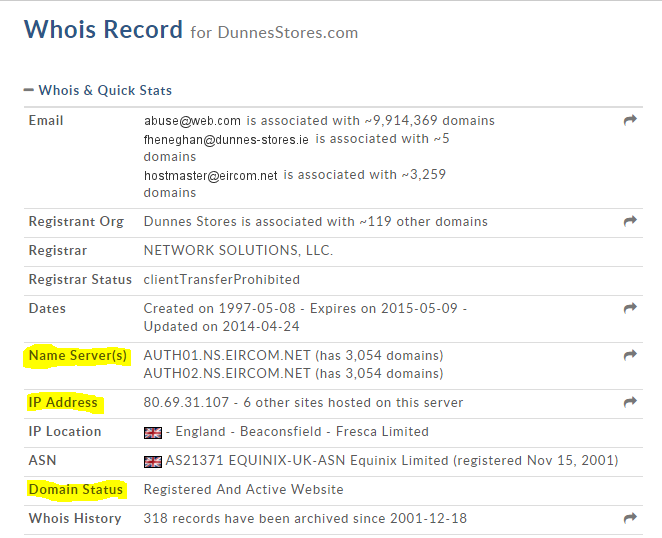


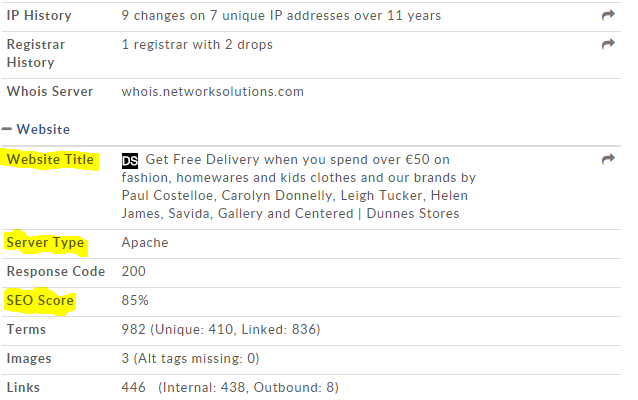
With the machine selected on **“Company Stalker”** using **Maltego**, I was able to gather the following information about **dunnesstores.com**. These information includes different types of documents as shown above.

1. Using[**http://whois.domaintools.com/**](http://whois.domaintools.com/) tool

By using the above tool, I was able to gather the more information about the domain: **dunnesstores.com**. These information are highlighted in the screen shot below.

**Name Server(s), IP Address, Domain Status, Website Title, Server Type, SEO Score** and other information mentioned before.





# Deliverables

* + 1. **Write a detailed technical report on your reconnaissance activity and the information you have gleamed using the output of Maltego and other tools to visually show/detail connections in the organization.**

Firstly, using the reconnaissance tools mentioned above such as **whois** and **search engine**, I was able to gather information about Dunnes Stores. I was able to find out, in my opinion, the boss of Dunnes Stores, other board Members and the administrator. In addition, these tools were able to obtain sensitive information relating to the company from their web page. This includes: staff names, title, email addresses, phone numbers, fax numbers, office addresses, name servers, etc. These information can be useful if an attacker needs to use social engineering techniques to reach their objectives. An attacker can find other ways to use these information to intrude into the environment. An intruder can use the following methods such as Pretexting, Phone Phishing, Trojan Horse, Shoulder Surfing, Something for Something, etc. to impersonate co-workers in the company.

From what we can see from the screen shots above, an attacker can use **Spear Phishing** technique to target the company through email or telephone scam. They can send email messages or even make calls that appears genuine to all the associates or members within the company. The hijacker might make the message look like it came from the company or from a colleague who might send an email message to everyone in this company, such as the Managing Director and Director (**Frank Dunne**) or the Head of Textiles and Director (**Michael Heffernan**). This message might ask for Usernames or Passwords or may contain malicious software like virus or Trojan.

Furthermore, finding IP ranges and servers using **whois** and **dig** reconnaissance toolsshows details of weaknesses which could be exploited in this company. An attacker could use these information to gain access to the organisation’s network and steal confidential data. The hacker can also attack and cause damage to their systems by having access to their network.

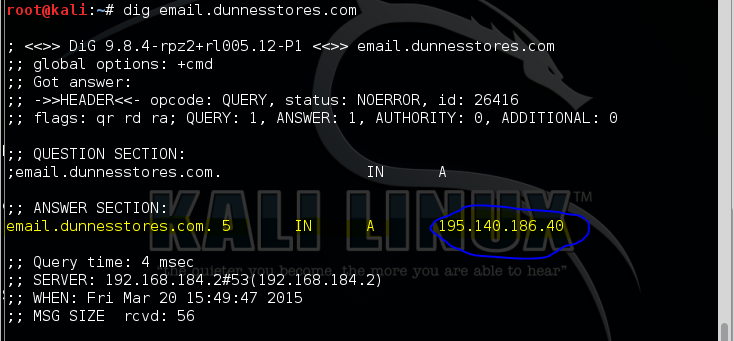
The most interesting information the tools, particularly **dig** collected is the **ip-address** (i.e. **80.69.31.107**). With this, it will make it effortless for an attacker to intrude into their system and will be able to obtain valuable information that might be used against the company.

Secondly, using **maltego** I was able to find out more information about Dunnes Stores than any other reconnaissance tools I used. With maltego set at different levels of penetration, I was able to find staff email addresses, websites associated with the person and other details such as the IPv4 addresses, Netblock, Domain, DNS Names, AS, NS and MX Records. This process can disclose system vulnerabilities and alleviate the effortlessness with which data can be used. For instance, the combination of the hostname, IP address and the ISP information provided will make it easy for an intruder to re-route their traffic through the use of **Wireshark**.

With the help of Wireshark, an intruder or attacker could enter Dunnes Stores’s hostname and port number 21 (ie one of the port numbers shown using the **nmap** tool) into the Wireshark and will be able to see the organisation’s network traffic which the attacker can study and use to gain valuable information from them.

When **recon-ng** was used to webcrawl for more information, email servers used by Dunnes Stores network such as **email.dunnesstores.com** and **mail.dunnesstores.com** were displayed. With the email servers, an attacker can use these information to find out the IP Address, check ports that are open on it and also exploit some of the services running on it.

For instance, an attacker can use **dig** to find out the IP Address of the email server as shown in the screen shot below:



**This is the email exchange server:**

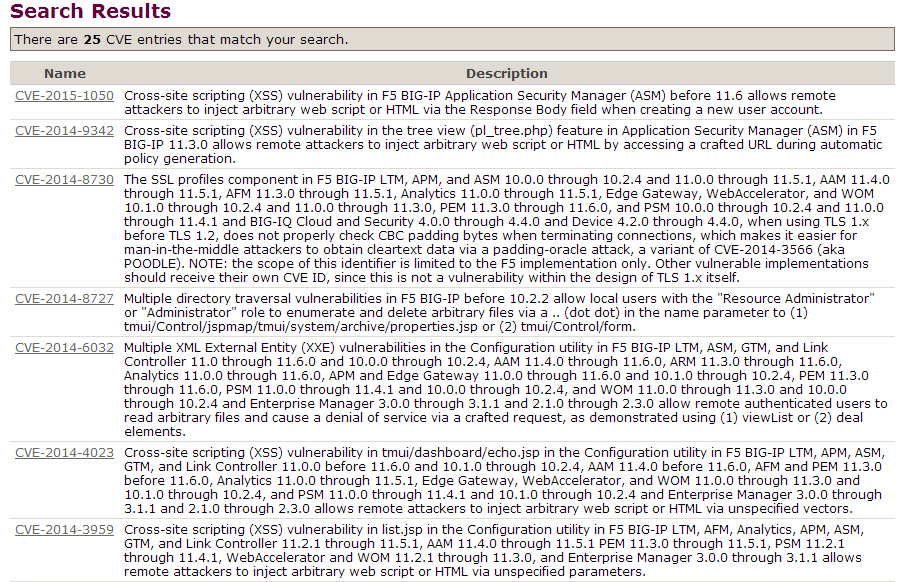
**Hostname:** email.dunnesstores.com

**IP Address:** 195.140.186.40

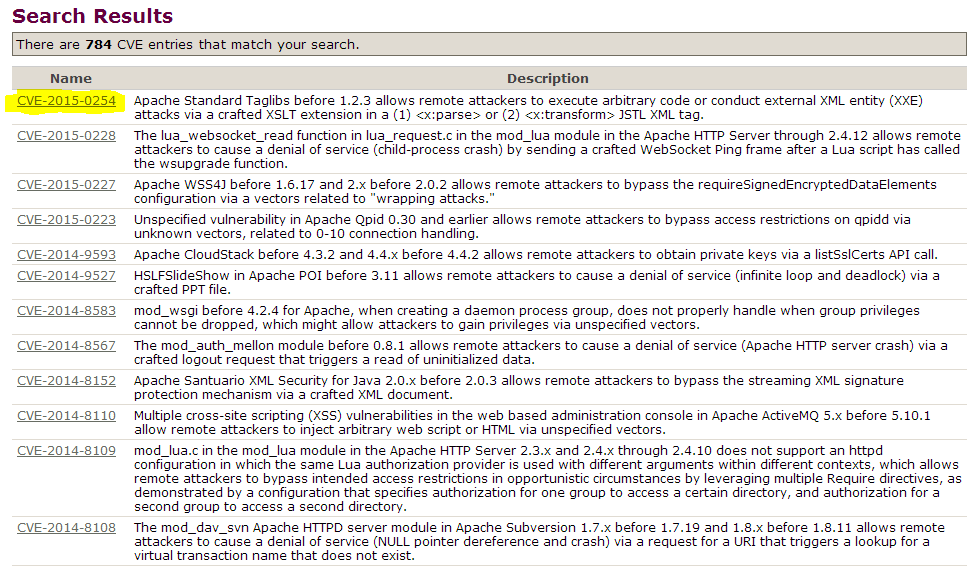
It is a serious vulnerability because, an attacker can scan it to see what services are open and exploit them.

Using netcraft to find webserver version and OS of Dunnes Stores shows that an attacker can do the same with more advanced tools to exploit the organisation’s vulnerabilities and gain great control over their system. This will eventually pose some threat to the company’s system. For instance, the **CVE** numbers for the OS F5 BIG-IP and the **CVE** numbers for the Web server Apache can pose vulnerabilities to the organisation. An attacker can use these information as shown below for their own benefit.

**CVE Numbers for OS F5 BIG-IP Vulnerabilities Results**



**CVE Numbers for Web Server Apache Vulnerabilities Results**



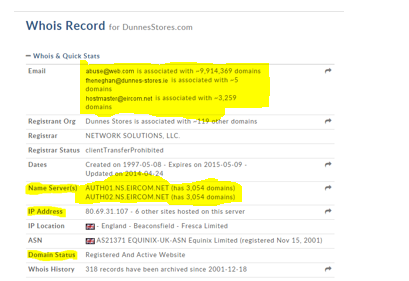
Additionally, with the information on the port numbers obtained by **nmap**, an attacker can use this to scan all the open port using other advanced tools available. The attacker will not only find out ports that are open, he/she will find out the type of port and check the services running the ports.

1. **Conclusion**

In conclusion, all these information obtained from the reconnaissance activity and the information gleamed using the output of Maltego and other tools shows how vulnerable the organisation could be. These information can be used against them at any time and can be used to cause damage to their system.

Moreover, other web based recon tools such as **whatmyip.co, who.is,** and **whois.domaintools.com** used to gather more information on dunnesstores.com showed/ detailed the same connections in the organisation. In comparison, majority of the information were the same in each of the tools. Meanwhile, when using **maltego** some information such as phone numbers associated with the staff did not show. This means that the security in the organisation is very high. Majority of the information required were very difficult to obtain. For instance, **whois** did not display as much information as possible.

The screen shots below illustrates different tools displaying the same information.



Using[**http://whois.domaintools.com/**](http://whois.domaintools.com/) tool





Using **whois dunnesstores.com** on command-line.