COMP707

Passive Reconnaissance: Dimension Data

UNIVERSITY OF KWAZULU-NATAL ™

INYUVESI YAKWAZULU-NATALI

Group Members

Verosha Pillay : 214539347

Kershen Sivanarain: 215042892

Divyan Hirasen : 215018696

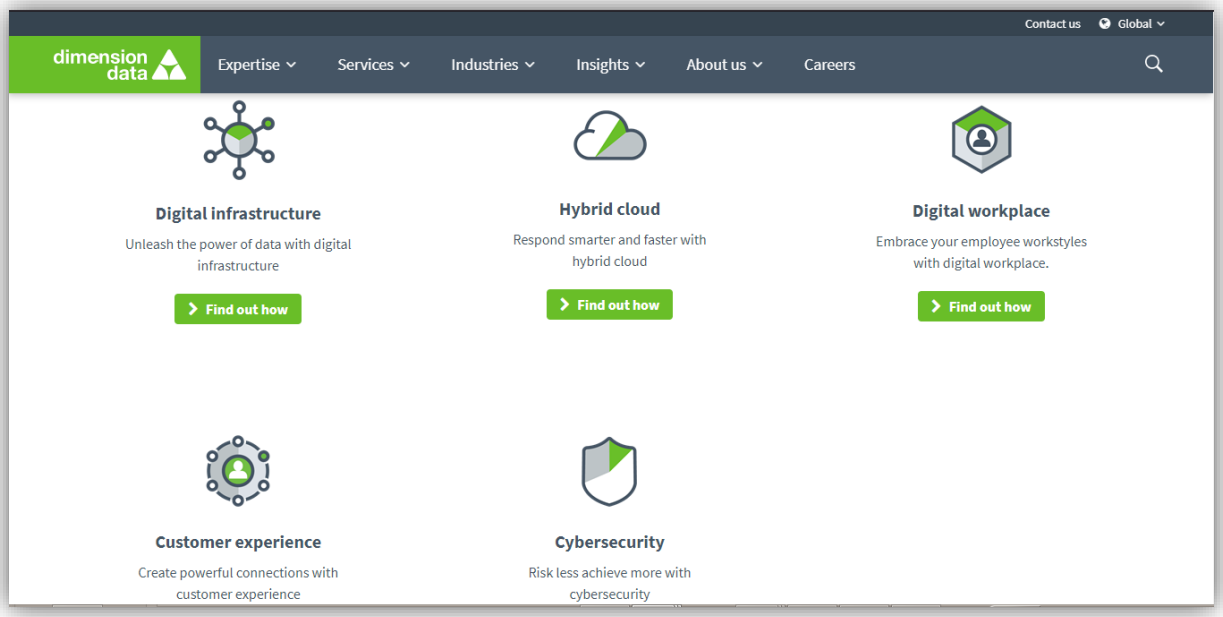
Table of Contents

Introduction

Quickly mapping an organisation's attack surface is an essential skill for network attackers (penetration testers, bug bounty hunters etc.) as well as those who are defending the network (network security, system administrators, blue teams etc).The idea behind passive reconnaissance is to gather information about a target using only publicly available records. This is done by using various tools and techniques without coming in contact with the organization. Some of the tools that are used in this report are Maltego, Recon-ng, FOCA etc. By performing these activities we will gain some insight about a company's network presence. Passive reconnaissance can include physical observation of an organization's building, sorting through discarded computer equipment in an attempt to find equipment that contains data or discarded paper with usernames and passwords, eavesdropping on employee conversations, researching the target through common Internet tools such as Whois, impersonating an employee in an attempt to collect information, and packet sniffing.

About the Company

The company we have selected to do our reconnaissance report on is Dimension Data. Dimension Data is a specialized information systems Company based in Johannesburg, South Africa and having offices around the world. The company focuses on services such as network integration, security and data centres which include: digital infrastructure, hybrid cloud, workspaces, and cyber security. Dimension Data also manages and operates servers and storage and provides backup services in case of damage or disaster.



Objectives

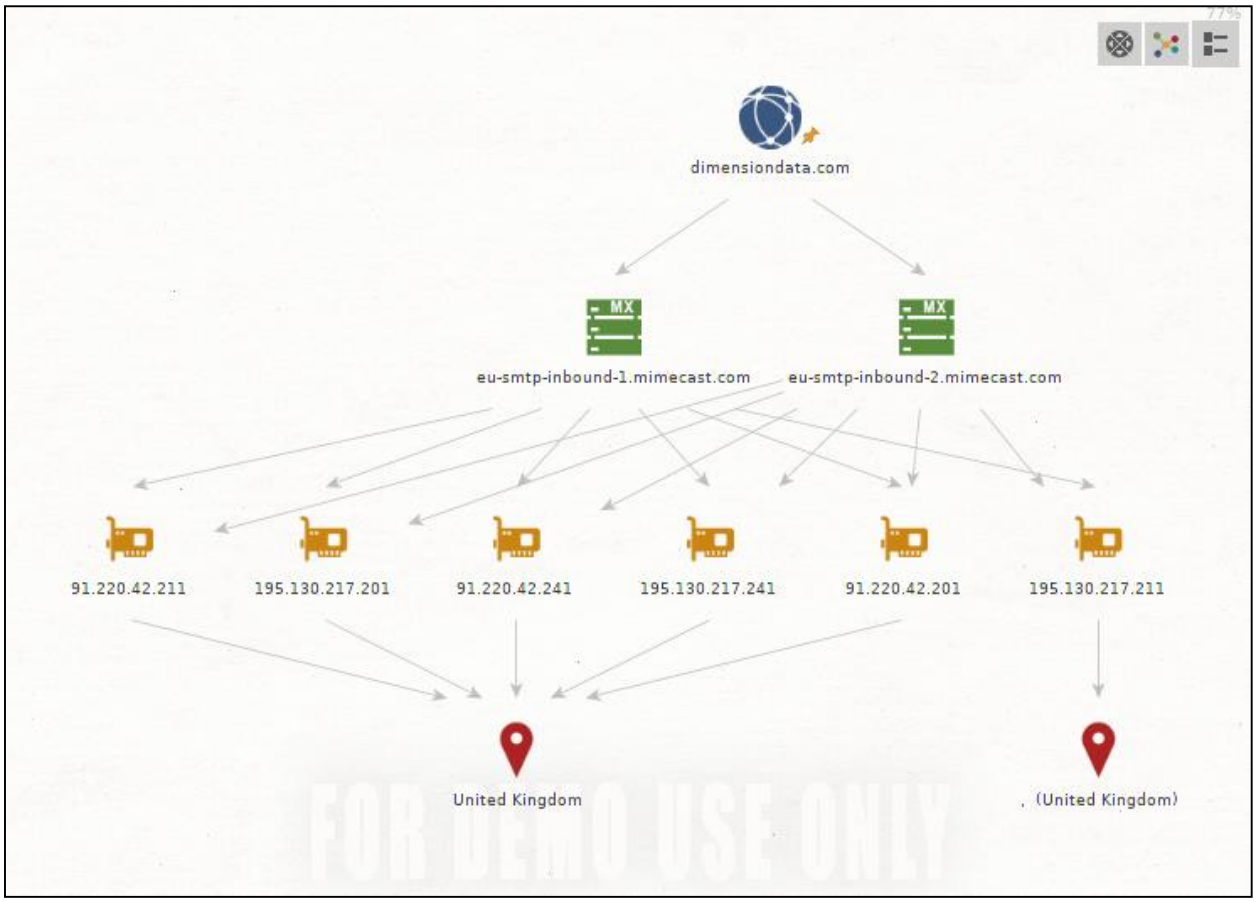
This report aims to provide insight on:

- Methods and tools for information gathering
- Analysis of company data
- Vulnerabilities identified and exploited
- How future attacks can be conducted
- Sources of information that can be used by attackers

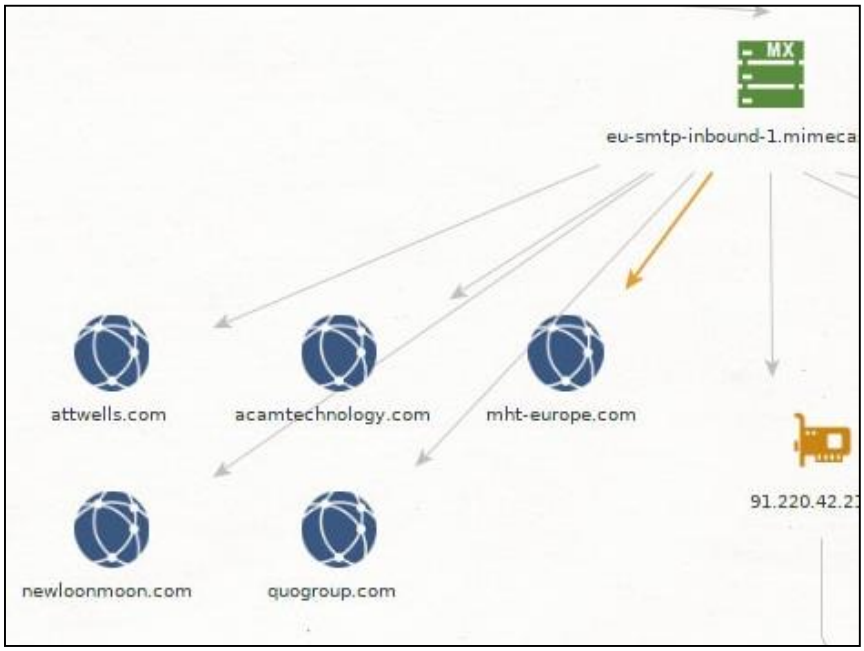
Maltego

Maltego is an interactive data mining tool that renders directed graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the Internet. We have used Maltego to try and mine as much data as possible about our target company Dimension Data and generate a diverse set of data. Below is a demonstration of the different transforms applied to obtain useful information about our target.

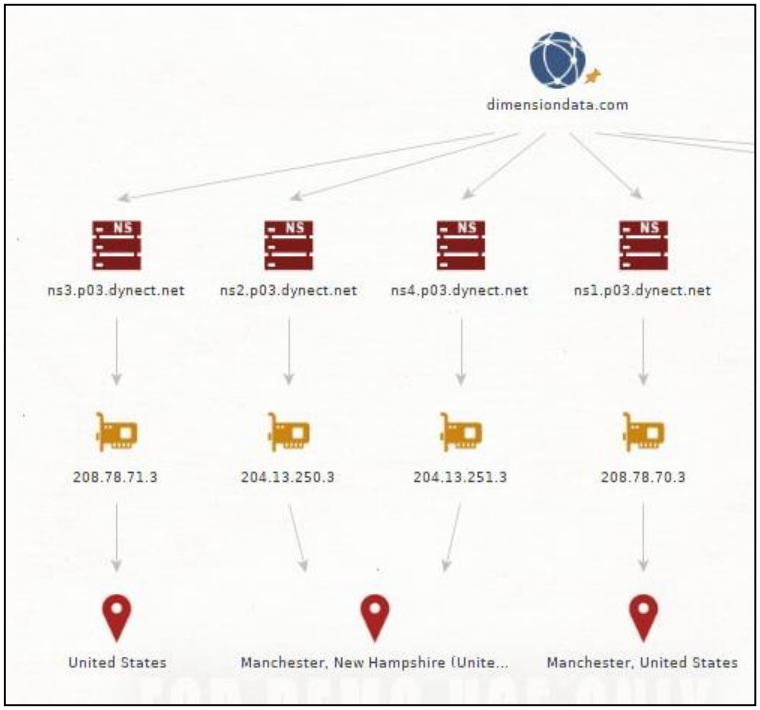
- **Domain To MX (mail server)**
  - The IP Address of this record gives a good indication of the network location of the target as most organisations keep their mail close to their network.
  - This is normally used in the infrastructure foot printing of an organisation.
  - Here we can see that the mail servers are located in United Kingdom.



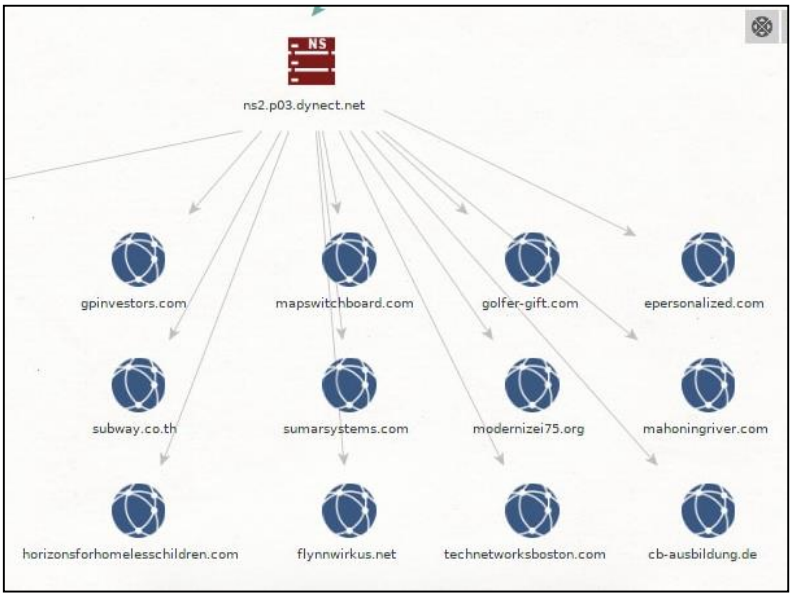
- **MX To Domain (Sharing this MX)**
  - It determines which other domains use this DNS Name as an MX record.
  - This is very useful in the infrastructure footprint of an organization as it **could** reveal other domains that the organization uses. In our case, it gave us unrelated domains to dimension data.



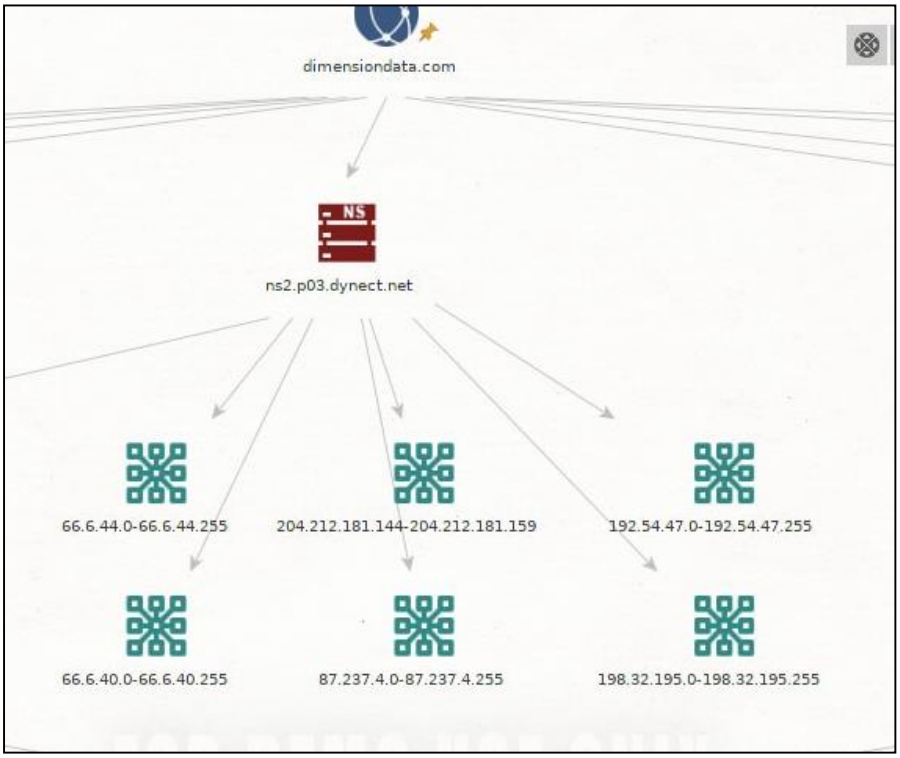
- **Domain To NS (name server)**
  - It is not uncommon for organizations to outsource their name servers to their ISP or to the registrar of their domain. Thus - in terms of finding the network (e.g. resolving this to an IP address) of the target this may have limited value.



- **NS To Domain (Sharing this NS)**
  - It determines which other domains use this DNS Name as a name server.
  - This is very useful in the infrastructure footprint of an organisation as it can reveal other domains that the organisation uses. However as noted above, it won't be the case if the name server is outsourced to the ISP.

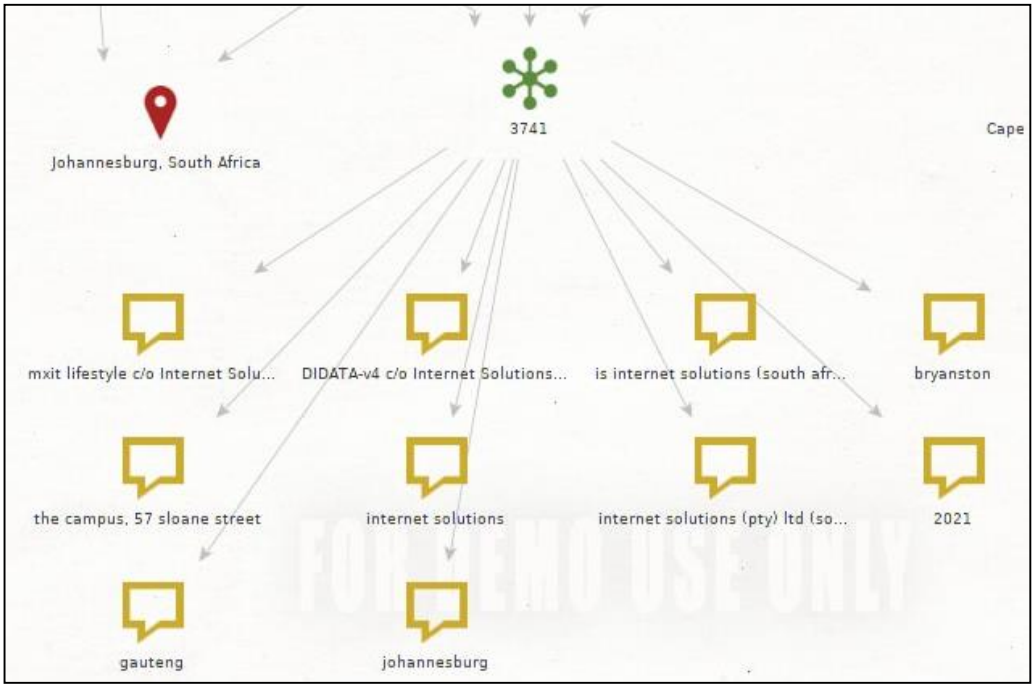


- **NS To Netblock**
  - This transform is useful for finding Netblocks of an organization.
  - A netblock is basically a range of IP addresses that a specific ISP or datacentre owns.
  - Below are 6 netblocks of a specific Name Server of Dimension Data.



- **Netblock To AS number**
  - This transform determines the **Autonomous System** (AS) number of the supplied network. This is useful for determining if two (or more) networks are related. If two networks are in the same AS (e.g. have the same AS number) we can say they are at least loosely routed to the same destination.
  - If the network belongs to an organisation (as opposed to ISP splitting), we get a good indication that both networks belong to the same organisation.

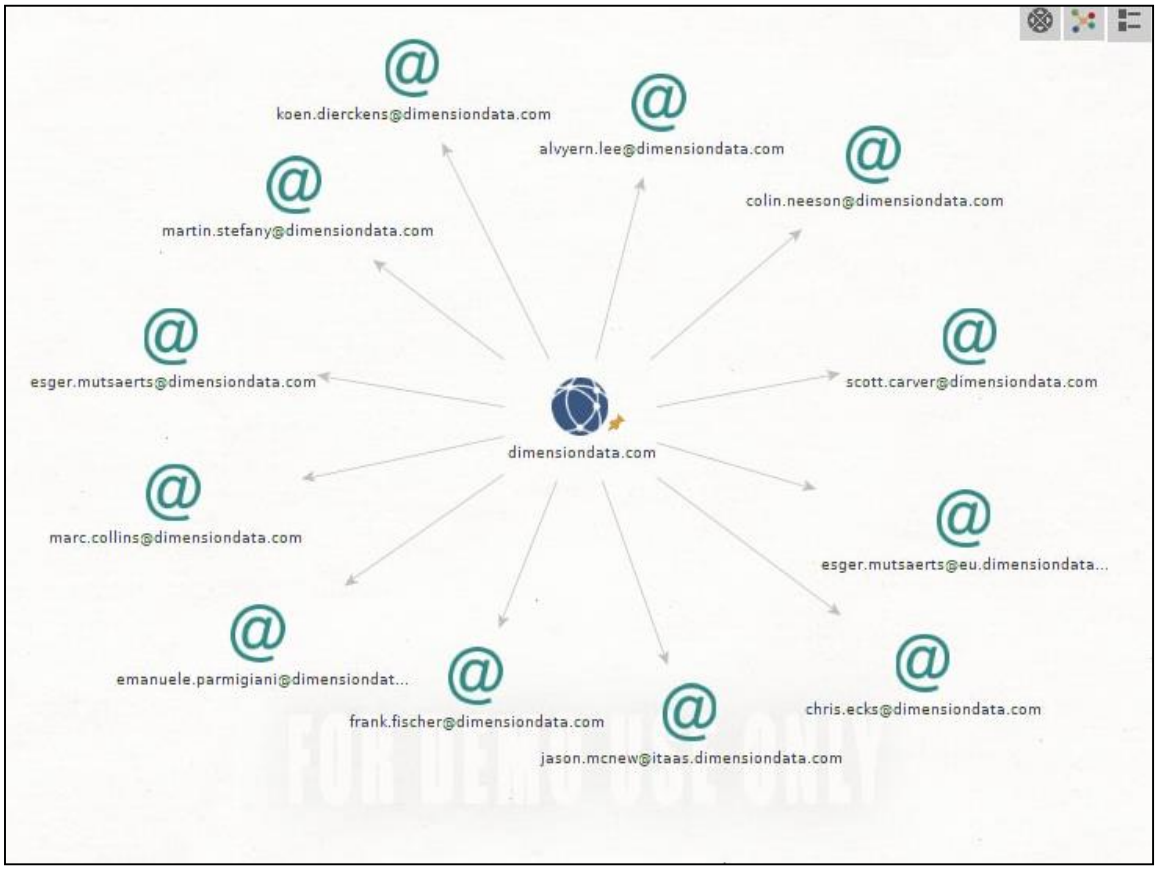
- **AS number to Owner**
  - We can also use a transform from AS number to Company (Owner) to find the owners of the AS. Here's an example the Transform applied on one specific AS number.



- **Domain To DNS Name (Find common DNS names)**
  - This transform attempts to find DNS names for the specified Domain. This is done by testing a list of DNS Names and seeing if they exist. The list of names that are tested for can be configured inside the transform.
  - The specified domain is appended to the name and tested. If it exists it is returned as a DNS Name. The IP Address of our DNS shown below point to United Kingdom.

- **Domain To Entities from whois**
  - Obtains useful whois information about domain

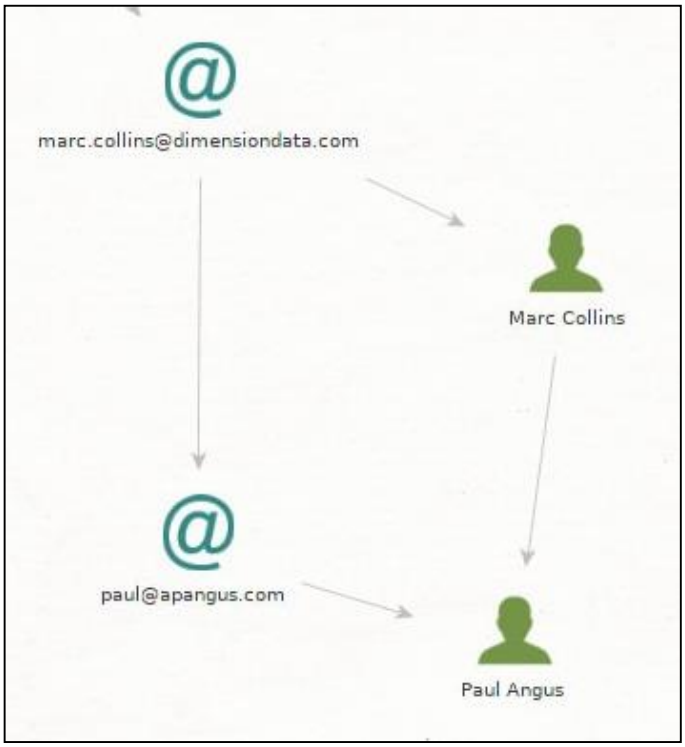
- **Domain To Email Addresses (PGP)**
  - This transform queries a public PGP key server and asks the question - "show me all the email addresses that ends in the supplied domain name' - results are returned as email address entities. Below are some of the email addresses of our target company Dimension Data.



- **Email To Person (PGP)**
  - Used to obtain the person who owns the email addresses.

- **Person to Email Addresses(PGP)**
  - Obtains all email addresses linked to the person.

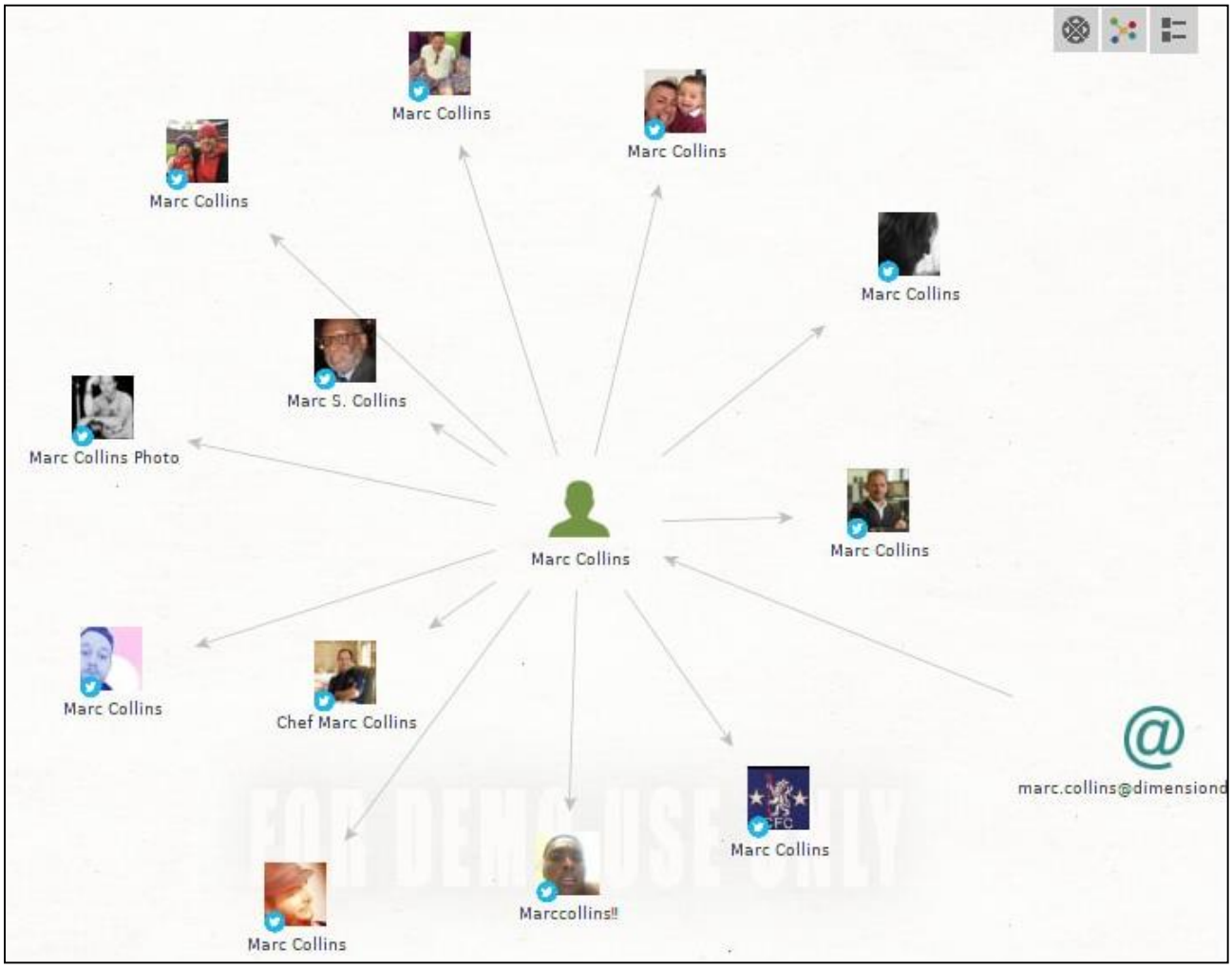
- **Person To Person (PGP(signed))**
  - This transform queries a public PGP key server and asks the question 'show me the names of persons that the owner of the supplied email address have signed'. This is useful for determining trust relationships between people.
  - The transform shows you these people communicated encrypted (or at least exchanged keys).



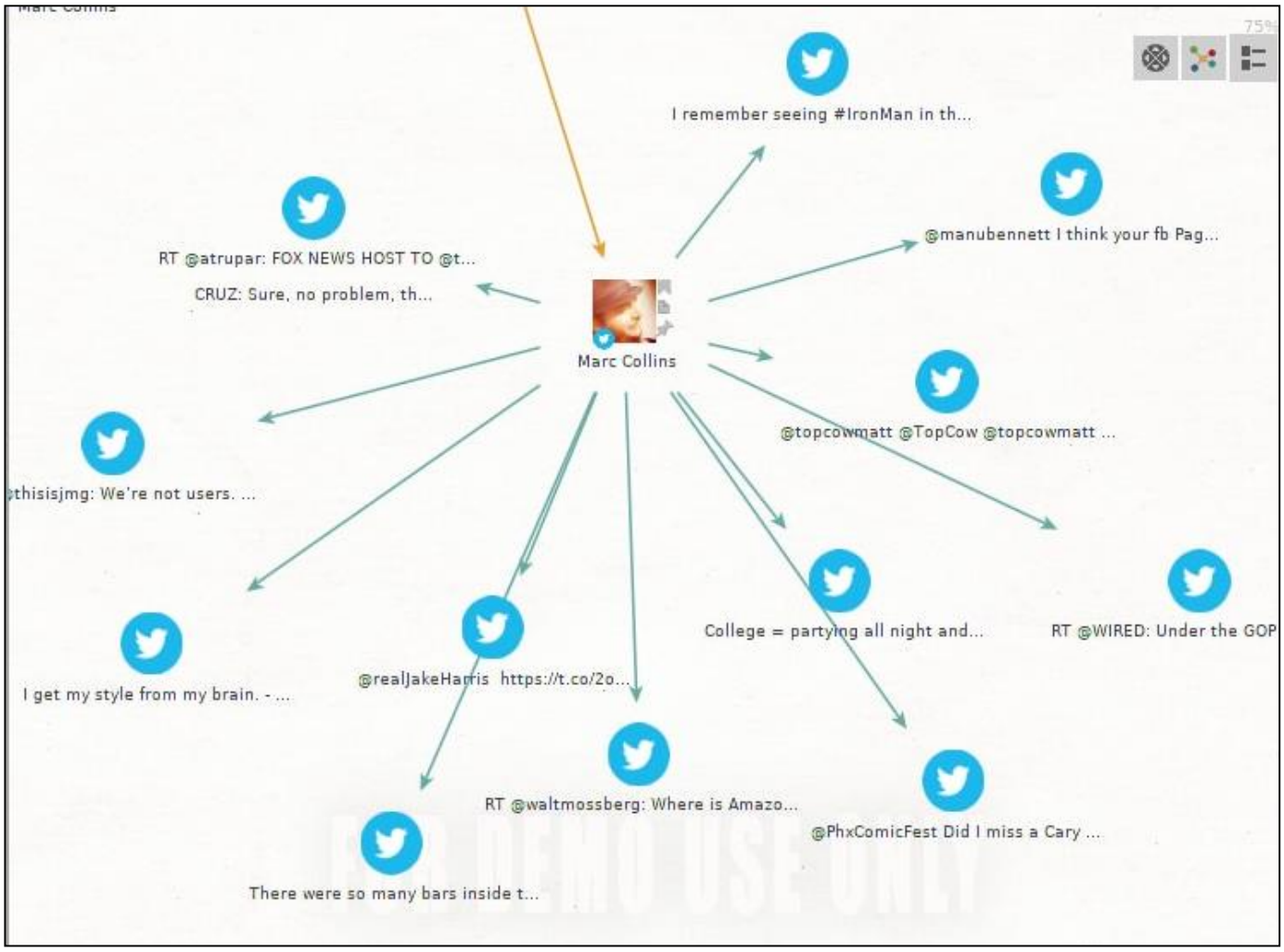
Many manipulations can be done to dig deeper into more personal information.

These are a few of the Twitter Transforms that were done on a person after finding names of people that work at the company.

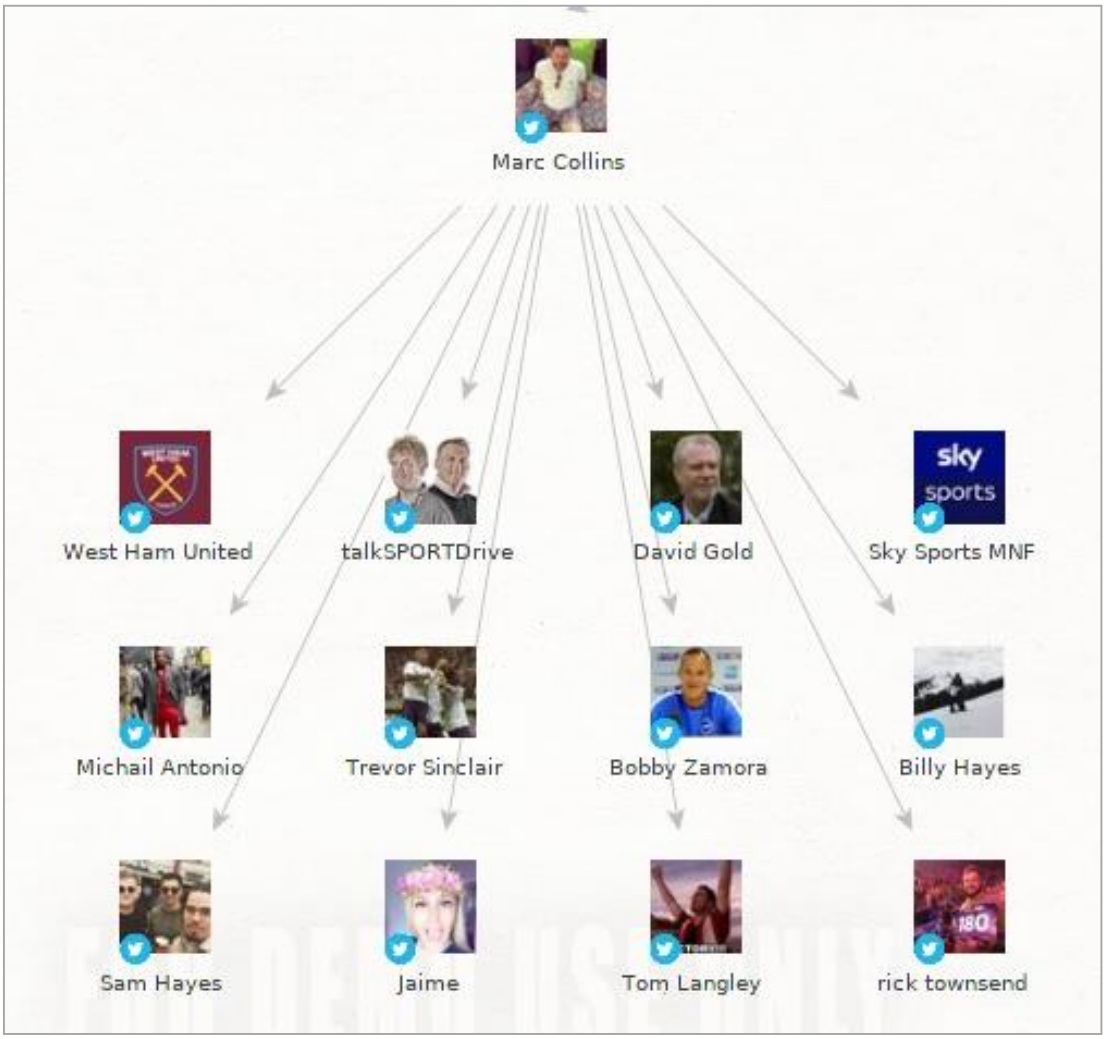
- **Person to Twitter Affiliation**
  - Searches Twitter for the person and returns all instances found.



- **Person to Tweet**
  - Obtains Twitter Posts from the user



- **Person to Twitter Affiliation**
  - Can obtain People that wrote tweets TO the person or People that the person wrote tweets TO. *This transform is of People that the Person wrote tweets TO*



The amount of mining that can be done with Maltego is extensive, and as shown above can produce vital information needed to exploit vulnerabilities and assist in attacking the network. We could not present the effect of the transforms on every single Entity but we have shown at least one application of each, to display the capability and type of data mined. We have used Maltego to understand the basic structure of the Network and how all the entities relate with each other. This gave us guidance as to which aspects we could dig deeper into. Its major strength is that it has provided us with a diverse range of data covering all aspects of reconnaissance. We have thus used this as a platform for reconnaissance and below have used a wide range of tools to expand on the different aspects discovered above as well as introduce other forms of reconnaissance. The threats and vulnerabilities of each aspect are discussed as we unfold each tool below.

The Harvester

The objective of this program is to gather **emails, subdomains, hosts, employee names, open ports and banners** from different public sources like search engines, PGP key servers and SHODAN computer database.

This tool is intended to help Penetration testers in the early stages of the penetration test in order to understand the customer footprint on the Internet.

Data found after using the harvester

Emails found:

David.Danto@dimensiondata.com	EBaboomian@www2.dimensiondata.com	Frank.Fischer@dimensiondata.com
Julie.carlill@dimensiondata.com	Lava@dimensiondata.com	Matthias.Kaden@dimensiondata.com
Olivier.posty@dimensiondata.com	Peterson@dimensiondata.com	Vincent.Pisciotta@dimensiondata.com
VoiceofourClient@dimensiondata.com	ai.information@dimensiondata.com	alvyern.lee@dimensiondata.com
andre.vanschalkwyk@dimensiondata.com	areya.jarupoom@dimensiondata.com	avinash.vasudeva@dimensiondata.com
balaji.subramaniam@dimensiondata.com	ben.christian@dimensiondata.com	channappa.nandi@dimensiondata.com
cheret@dimensiondata.com	chris.Erasmus@dimensiondata.com	chris.ecks@dimensiondata.com
colin.neeson@dimensiondata.com	debbie.anders@dimensiondata.com	dennis.koenig@dimensiondata.com
ed.bosak@dimensiondata.com	emanuele.parmigiani@dimensiondata.com	esger.mutsaerts@dimensiondata.com
esger.mutsaerts@eu.dimensiondata.com	felix.meixner@dimensiondata.com	frederic.declerck@dimensiondata.com
groupprivacy@dimensiondata.com	hannes.botha@dimensiondata.com	info.cz@dimensiondata.com
info.id@dimensiondata.com	info@dimensiondata.com	info@ug.dimensiondata.com
jason.mcnew@itaas.dimensiondata.com	johan.grobler@dimensiondata.com	john.howell@dimensiondata.com
jolene.emmanuel@dimensiondata.com	katerina.chalupova@dimensiondata.com	koen.dierckens@dimensiondata.com
kongdumrongkiat@dimensiondata.com	last@dimensiondata.com	licensing.nz@dimensiondata.com
marc.nicolaus@dimensiondata.com	martin.erbloweit@dimensiondata.com	martin.stefany@dimensiondata.com
mike.deheer@dimensiondata.com	namibia.hr@dimensiondata.com	nick.bettison@dimensiondata.com
pamela.posch@dimensiondata.com	patrice.cheret@dimensiondata.com	paul.jung@dimensiondata.com
paulo.coito@dimensiondata.com	peter.jackson@dimensiondata.com	raphael.delvaux@dimensiondata.com
reception.ap@dimensiondata.com	regina@dimensiondata.com	rimmpls.in@dimensiondata.com
scott.carver@dimensiondata.com	scott.santana@dimensiondata.com	see-yen.wong@dimensiondata.com
shaun.chivers@dimensiondata.com	steve.jones@dimensiondata.com	us.accudyne.servicedesk@dimensiondata.com
us.answers@dimensiondata.com	van-trung.truong@dimensiondata.com	victor.hernandez@dimensiondata.com
vincent.pisciotta@dimensiondata.com		

(A1.1)

Hosts found:

185.3.28.38:	WWW.dimensiondata.com
83.217.252.132:	api-eu.dimensiondata.com
52.56.78.139:	blog.dimensiondata.com
185.3.28.77:	cloud.dimensiondata.com
185.3.28.60:	glldcsvexns01.dimensiondata.com
175.184.209.24:	webmail.aucsfme.dimensiondata.com
185.3.28.38:	www.dimensiondata.com
45.60.118.88:	www2.dimensiondata.com
185.3.28.38:	www.dimensiondata.com
185.3.28.38:	cloud.dimensiondata.com
185.3.28.38:	www.nexusis.com
52.56.78.139:	www.nexusis.com

(A1.1)

Virtual hosts found:

185.3.28.38:	cloud.dimensiondata.com
185.3.28.38:	www.dimensiondata.com
185.3.28.38:	www.nexusis.com
52.56.78.139:	www.thegreenhouse

(A1.1)

Employee Names found:

David Danto	EBaboomian	Frank Fischer
Julie carlill	Matthias Kaden	Olivier posty
Peterson	Vincent Pisciotta	VoiceofourClient
alvyern lee	andre vanschalkwyk	areya jarupoom
avinash vasudeva	balaji subramaniam	ben christian
channappa nandi	cheret	chris Erasmus
chris ecks	colin neeson	debbie anders
dennis koenig	ed bosak	emanuele parmigiani
esger mutsaerts	esger mutsaerts	felix meixner
frederic declerck	hannes botha	jason mcnew
johan grobler	john howell	jolene emmanuel
katerina chalupova	koen dierckens	kongdumrongkiat
licensing nz	marc nicolaus	martin erbloweit
martin stefany	mike deheer	namibia hr
nick bettison	pamela posch	patrice cheret
paul jung	paulo coito	peter jackson
raphael delvaux	rimmpls in	scott carver
scott santana	see-yen wong	shaun chivers
steve jones	van-trung truong	victor hernandez
vincent pisciotta		

Summary:

TheHarvester had gathered

- 91 Emails
- 12 hosts
- 4 virtual hosts
- 57 Employee Names

How this gathered information can be used by the attacker

Emails:

- **Additional tools** can be used to gain unauthorised access to the above email addresses.
- Tools such as Kali Linux's **Hydra** uses a list of over a thousand potential passwords to try and hack an email account all while avoiding IP Address bans. (A1)
- Once an email address is hacked, attackers could
    - **Scam** the victims contact list
        - The success of this type of attack will be high since the victim's contacts will assume that they are sending harmless emails or attachments, while in fact the attacker could be sending harmful attachments or links
    - Gain access to **online accounts**
        - Accounts such as Uber, Netflix, Amazon can also be accessed through the hacked email address and potentially sold to other people. (A2)
    - Access **social media** accounts
        - Moreover, the attacker can begin to damage the victim's **reputation** over social media by posting or sharing inappropriate material
        - The attacker can also **catfish** other contacts of the victim over social media.

Hosts:

- DNS servers work by translating IP addresses into domain names.
- When a DNS or Host is compromised, the first thing an attacker can do is **redirect** all incoming traffic to a server of their choosing. This enables them to launch additional attacks or **collect traffic logs** that contain sensitive information. (A3)
- An attacker can attempt to capture all **inbound emails**.
- This also allows the attacker to **send email on their behalf**, using the victim organization's domain and cashing-in on their positive reputation (A3)

Virtual Hosts:

- VM-based servers are just as vulnerable to **malware** or targeted attacks as hardware-based servers are. (A4)
- Attackers can attempt to target the Virtual Host **snapshots** using malware.
- In turn VM-Servers could end up attacking other VM-Servers over the network.

Employee Names:

- Social engineering techniques can be used on the employee names to gather information such as social media accounts, social media activity, online profiles and subscriptions. **Maltego** is a tool which can perform social engineering and gather such information.

Online References

(A1) https://www.sunnyhoi.com/hack-email-accounts-using-hydra-kali-linux/

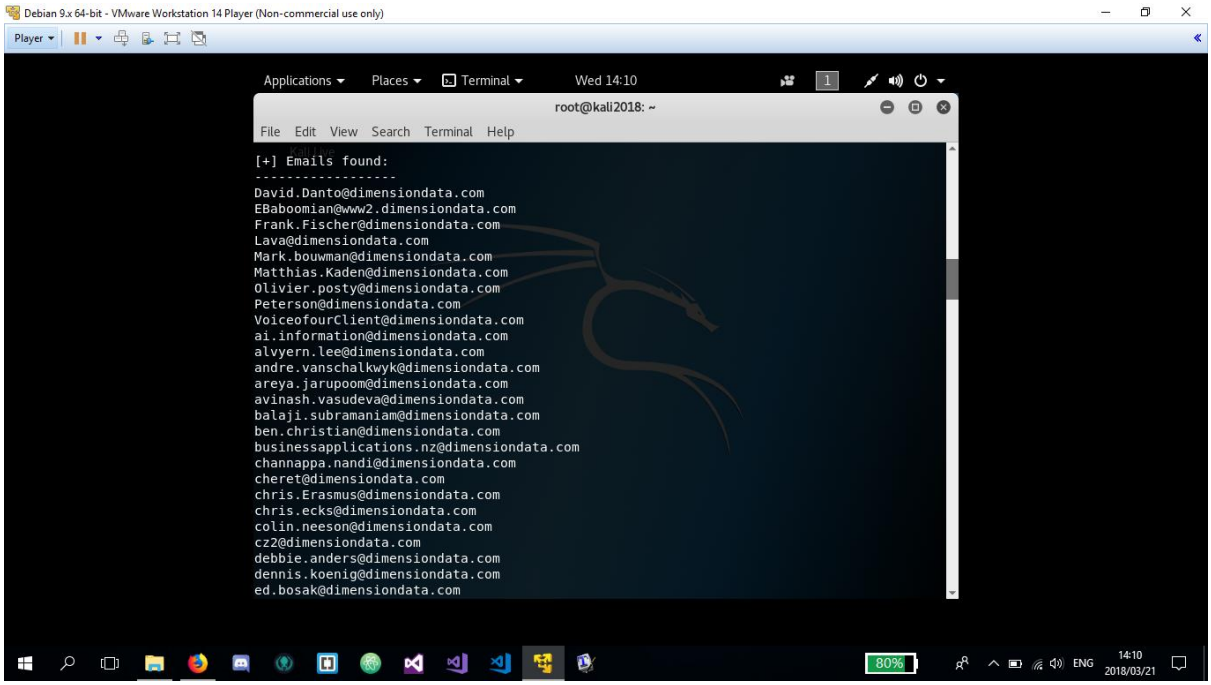
(A2) https://heimdalsecurity.com/blog/hacked-email-why-cyber-criminals-want-inbox/

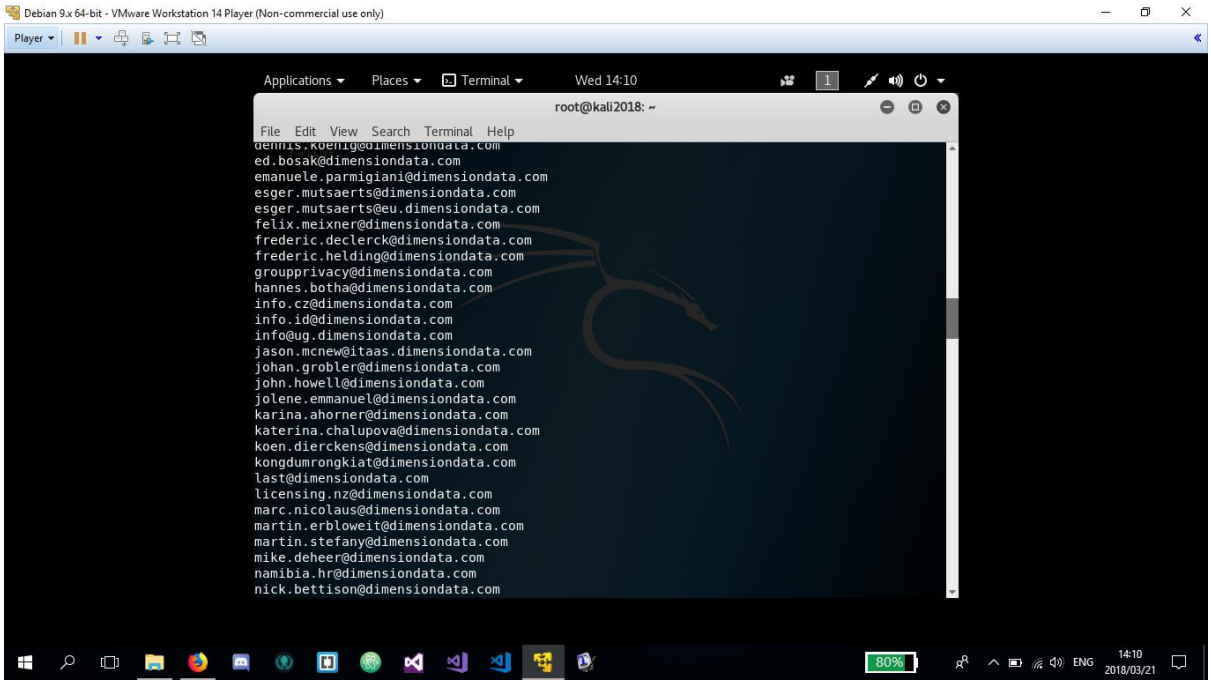
(A3) https://www.csoonline.com/article/2133916/malware-cybercrime/three-types-of-dns-attacks-and-how-to-deal-with-them.html

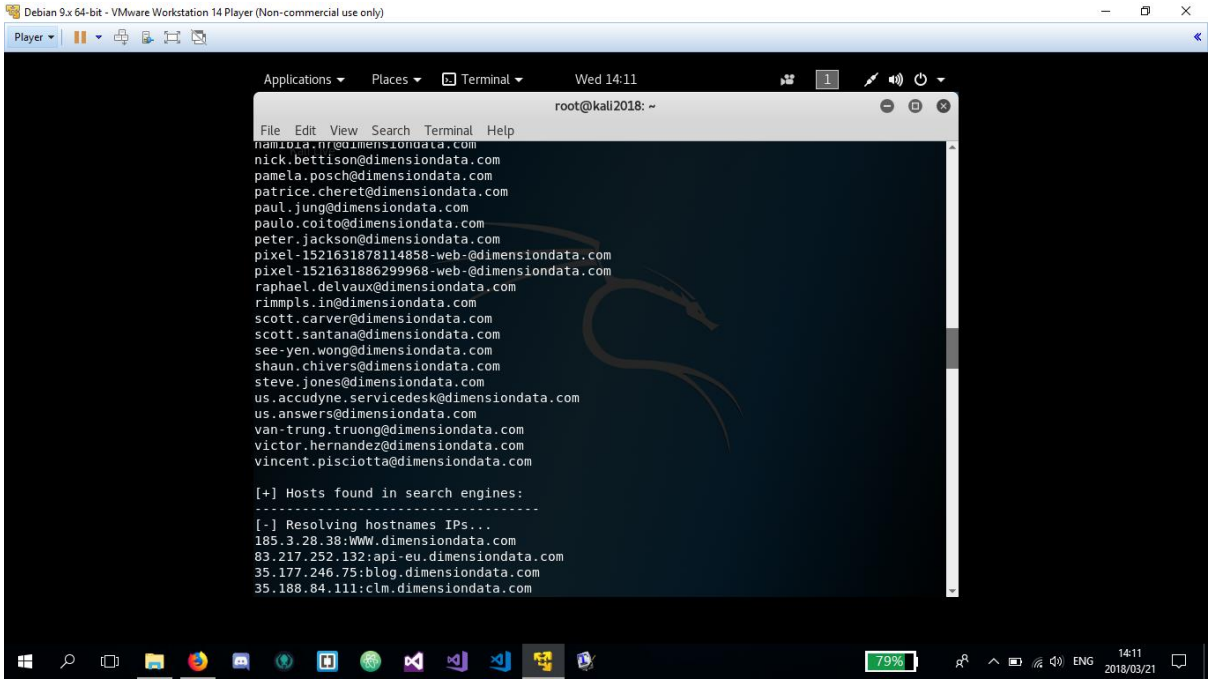
(A4) http://www.zdnet.com/article/virtual-servers-no-safer-than-any-other-kind/

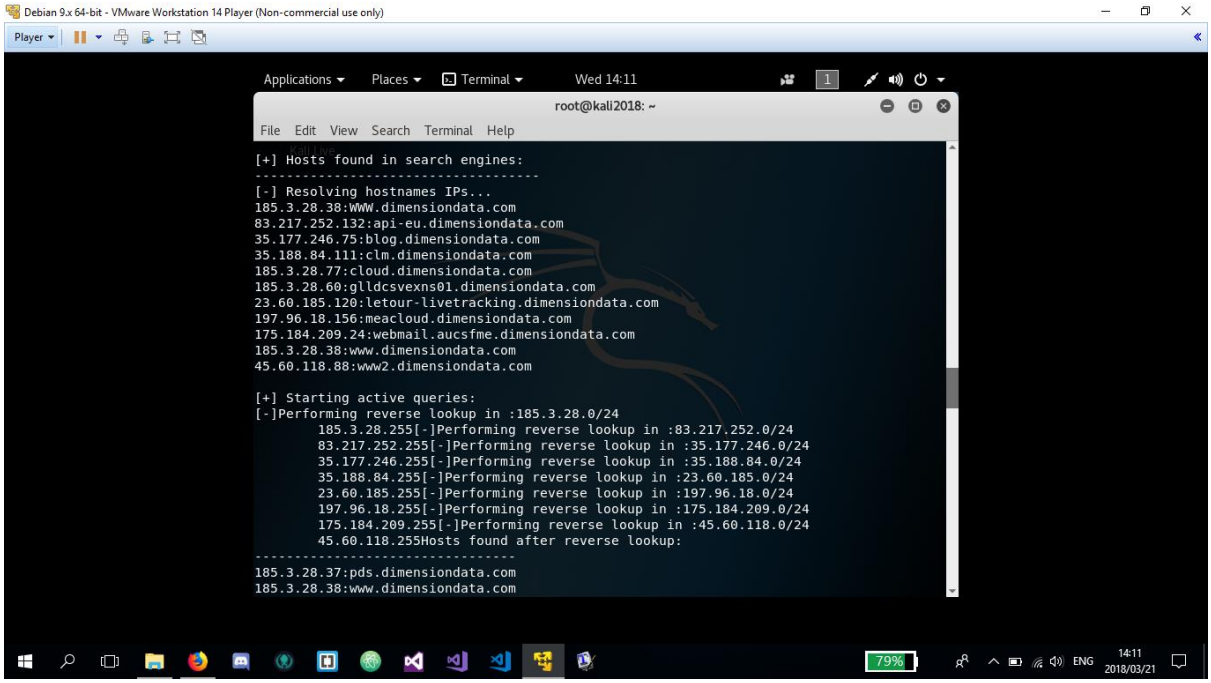
Screenshots of The Harvester

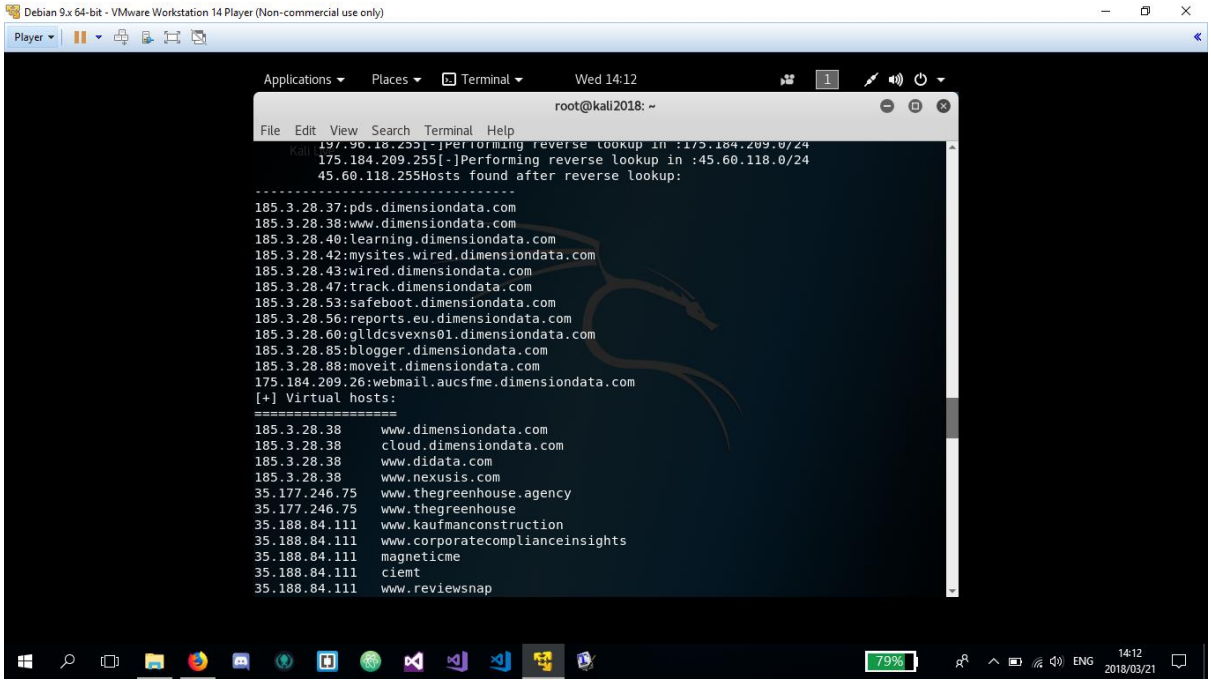
(A1.1)

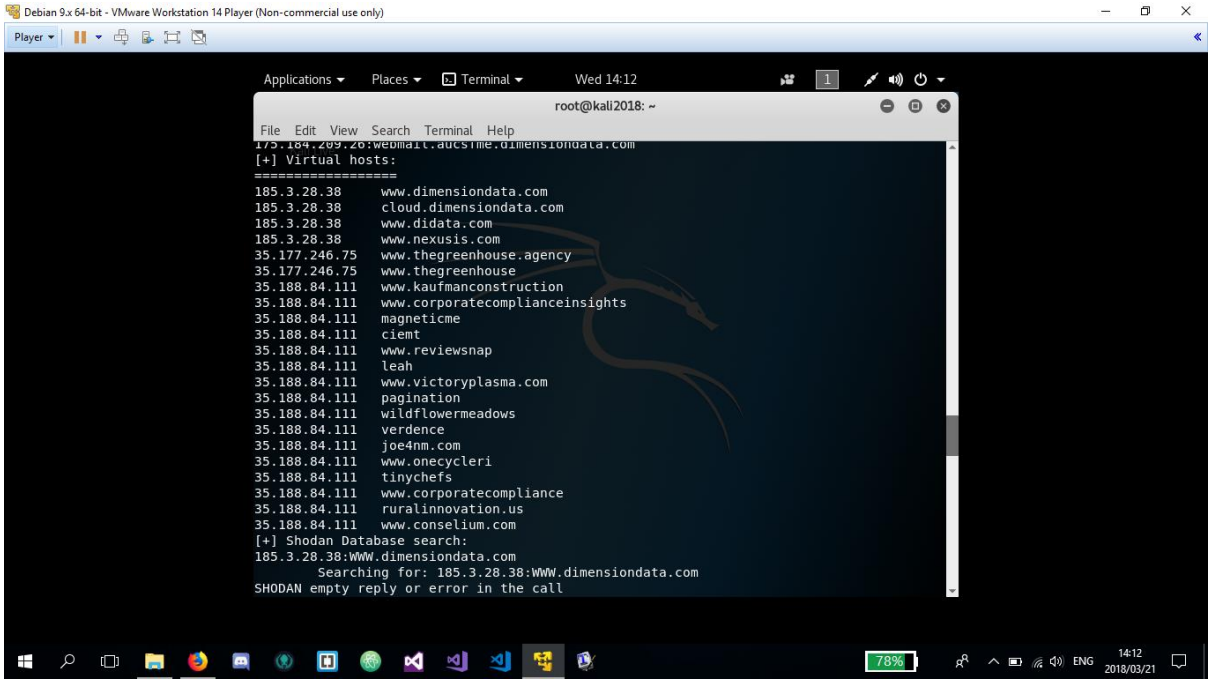


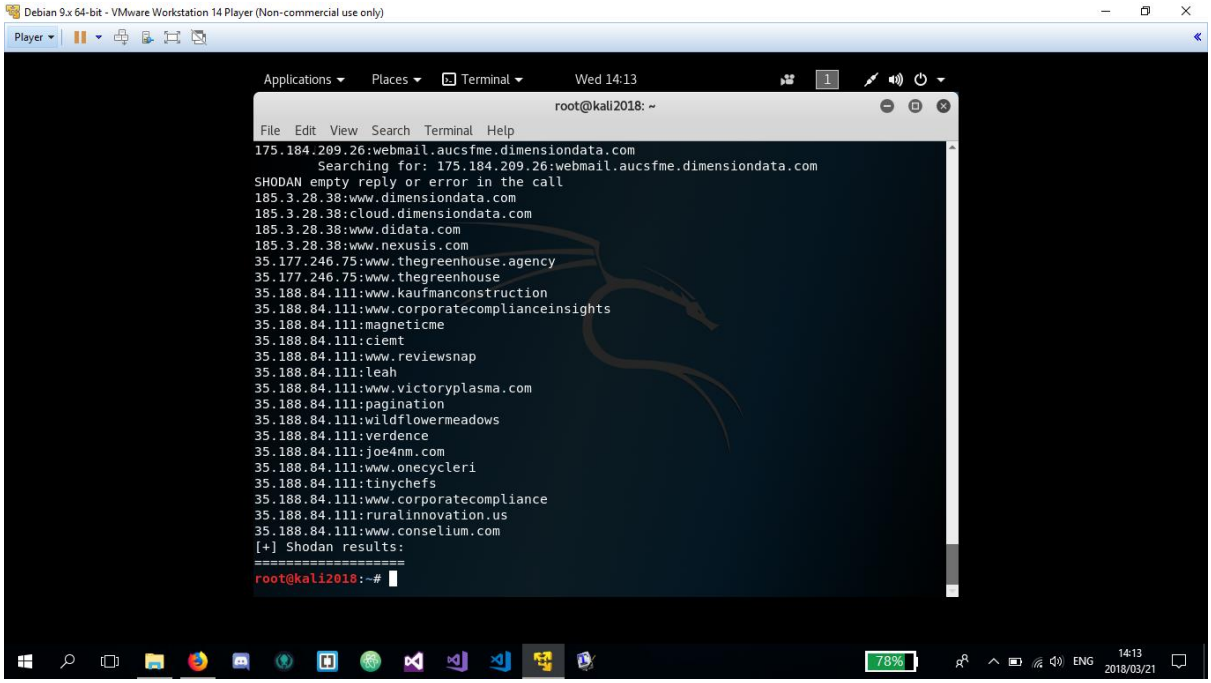


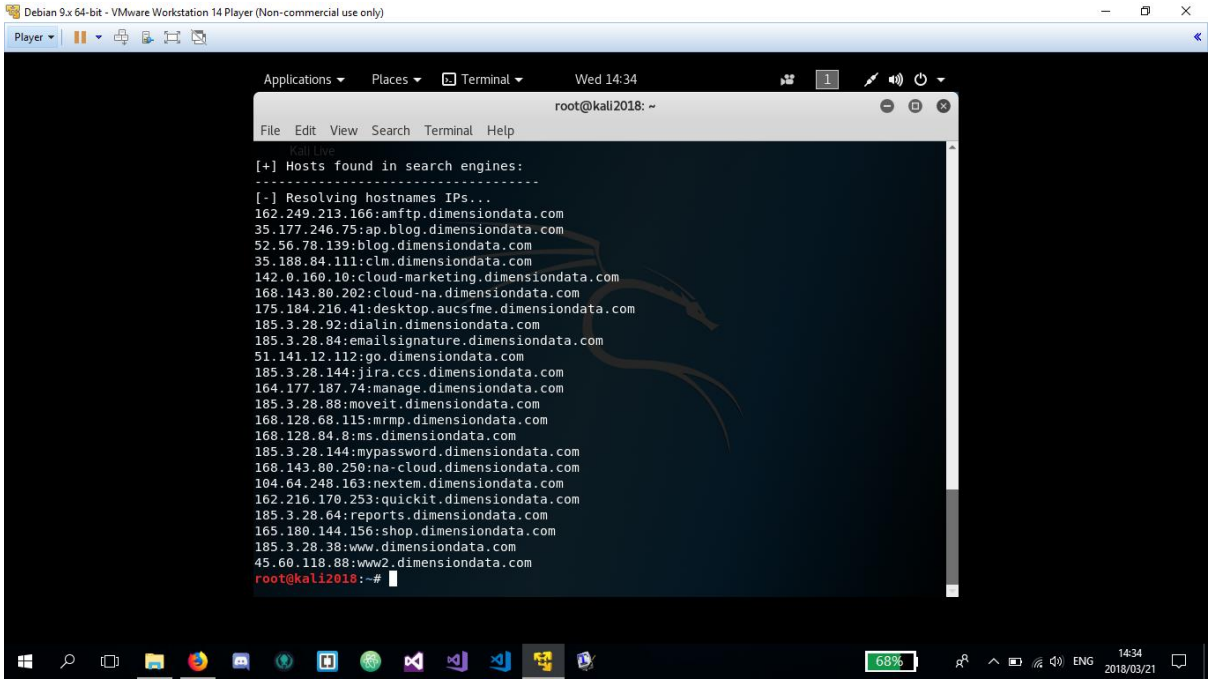

Debian 9.x 64-bit - VMware Workstation 14 Player (Non-commercial use only)
Player
Applications Places Terminal Wed 14:11
root@kali2018: ~
File Edit View Search Terminal Help
nick.bettison@dimensiondata.com
pamela.posch@dimensiondata.com
patrice.cheret@dimensiondata.com
paul.jung@dimensiondata.com
paulo.coito@dimensiondata.com
peter.jackson@dimensiondata.com
pixel-1521631878114858-web-@dimensiondata.com
pixel-1521631886299968-web-@dimensiondata.com
raphael.delvaux@dimensiondata.com
rimmpls.in@dimensiondata.com
scott.carver@dimensiondata.com
scott.santana@dimensiondata.com
see-yen.wong@dimensiondata.com
shaun.chivers@dimensiondata.com
steve.jones@dimensiondata.com
us.accudyne.servicedesk@dimensiondata.com
us.answers@dimensiondata.com
van-trung.truong@dimensiondata.com
victor.hernandez@dimensiondata.com
vincent.pisciotta@dimensiondata.com
[+] Hosts found in search engines:
[-] Resolving hostnames IPs...
185.3.28.38:WWW.dimensiondata.com
83.217.252.132:api-eu.dimensiondata.com
35.177.246.75:blog.dimensiondata.com
35.188.84.111:clm.dimensiondata.com
79%
ENG
14:11
2018/03/21


Debian 9.x 64-bit - VMware Workstation 14 Player (Non-commercial use only)
Player
Applications Places Terminal Wed 14:11
root@kali2018: ~
File Edit View Search Terminal Help
[+] Hosts found in search engines:
[-] Resolving hostnames IPs...
185.3.28.38:WWW.dimensiondata.com
83.217.252.132:api-eu.dimensiondata.com
35.177.246.75:blog.dimensiondata.com
35.188.84.111:clm.dimensiondata.com
185.3.28.77:cloud.dimensiondata.com
185.3.28.60:glldcsvexns01.dimensiondata.com
23.60.185.120:letour-livetracking.dimensiondata.com
197.96.18.156:meacloud.dimensiondata.com
175.184.209.24:webmail.aucsfme.dimensiondata.com
185.3.28.38:www.dimensiondata.com
45.60.118.88:www2.dimensiondata.com
[+] Starting active queries:
[-]Performing reverse lookup in :185.3.28.0/24
185.3.28.255[-]Performing reverse lookup in :83.217.252.0/24
83.217.252.255[-]Performing reverse lookup in :35.177.246.0/24
35.177.246.255[-]Performing reverse lookup in :35.188.84.0/24
35.188.84.255[-]Performing reverse lookup in :23.60.185.0/24
23.60.185.255[-]Performing reverse lookup in :197.96.18.0/24
197.96.18.255[-]Performing reverse lookup in :175.184.209.0/24
175.184.209.255[-]Performing reverse lookup in :45.60.118.0/24
45.60.118.255Hosts found after reverse lookup:
185.3.28.37:pds.dimensiondata.com
185.3.28.38:www.dimensiondata.com
79%
ENG
14:11
2018/03/21


Debian 9.x 64-bit - VMware Workstation 14 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Wed 14:12
root@kali2018: ~
File Edit View Search Terminal Help
175.184.209.255[-]Performing reverse lookup in :45.60.118.0/24
45.60.118.255Hosts found after reverse lookup:
185.3.28.37:pds.dimensiondata.com
185.3.28.38:www.dimensiondata.com
185.3.28.40:learning.dimensiondata.com
185.3.28.42:mysites.wired.dimensiondata.com
185.3.28.43:wired.dimensiondata.com
185.3.28.47:track.dimensiondata.com
185.3.28.53:safeboot.dimensiondata.com
185.3.28.56:reports.eu.dimensiondata.com
185.3.28.60:glldcsvexns01.dimensiondata.com
185.3.28.85:blogger.dimensiondata.com
185.3.28.88:moveit.dimensiondata.com
175.184.209.26:webmail.aucsfme.dimensiondata.com
[+] Virtual hosts:
185.3.28.38 www.dimensiondata.com
185.3.28.38 cloud.dimensiondata.com
185.3.28.38 www.didata.com
185.3.28.38 www.nexusis.com
35.177.246.75 www.thegreenhouse.agency
35.177.246.75 www.thegreenhouse
35.188.84.111 www.kaufmanconstruction
35.188.84.111 www.corporatecomplianceinsights
35.188.84.111 magneticme
35.188.84.111 ciemt
35.188.84.111 www.reviewsnap
79%
ENG
14:12
2018/03/21


Debian 9.x 64-bit - VMware Workstation 14 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Wed 14:12
root@kali2018: ~
File Edit View Search Terminal Help
[+] Virtual hosts:
185.3.28.38 www.dimensiondata.com
185.3.28.38 cloud.dimensiondata.com
185.3.28.38 www.didata.com
185.3.28.38 www.nexusis.com
35.177.246.75 www.thegreenhouse.agency
35.177.246.75 www.thegreenhouse
35.188.84.111 www.kaufmanconstruction
35.188.84.111 www.corporatecomplianceinsights
35.188.84.111 magneticme
35.188.84.111 ciemt
35.188.84.111 www.reviewsnap
35.188.84.111 leah
35.188.84.111 www.victoryplasma.com
35.188.84.111 pagination
35.188.84.111 wildflowermeadows
35.188.84.111 verdence
35.188.84.111 joe4nm.com
35.188.84.111 www.onecycleri
35.188.84.111 tinychefs
35.188.84.111 www.corporatecompliance
35.188.84.111 ruralinnovation.us
35.188.84.111 www.conselium.com
[+] Shodan Database search:
185.3.28.38:WWW.dimensiondata.com
Searching for: 185.3.28.38:WWW.dimensiondata.com
SHODAN empty reply or error in the call
78%
ENG
14:12
2018/03/21


Debian 9.x 64-bit - VMware Workstation 14 Player (Non-commercial use only)
Player
Applications Places Terminal Wed 14:13
root@kali2018: ~
File Edit View Search Terminal Help
175.184.209.26:webmail.aucsfme.dimensiondata.com
Searching for: 175.184.209.26:webmail.aucsfme.dimensiondata.com
SHODAN empty reply or error in the call
185.3.28.38:www.dimensiondata.com
185.3.28.38:cloud.dimensiondata.com
185.3.28.38:www.didata.com
185.3.28.38:www.nexusis.com
35.177.246.75:www.thegreenhouse.agency
35.177.246.75:www.thegreenhouse
35.188.84.111:www.kaufmanconstruction
35.188.84.111:www.corporatecomplianceinsights
35.188.84.111:magneticme
35.188.84.111:ciemt
35.188.84.111:www.reviewsnap
35.188.84.111:leah
35.188.84.111:www.victoryplasma.com
35.188.84.111:pagination
35.188.84.111:wildflowermeadows
35.188.84.111:verdence
35.188.84.111:joe4nm.com
35.188.84.111:www.onecycleri
35.188.84.111:tinychefs
35.188.84.111:www.corporatecompliance
35.188.84.111:ruralinnovation.us
35.188.84.111:www.conselium.com
[+] Shodan results:
==========
root@kali2018:~#
78%
ENG
14:13
2018/03/21


Debian 9.x 64-bit - VMware Workstation 14 Player (Non-commercial use only)
Player
Applications Places Terminal Wed 14:34
root@kali2018: ~
File Edit View Search Terminal Help
Kali Live
[+] Hosts found in search engines:
[-] Resolving hostnames IPs...
162.249.213.166:amftp.dimensiondata.com
35.177.246.75:ap.blog.dimensiondata.com
52.56.78.139:blog.dimensiondata.com
35.188.84.111:clm.dimensiondata.com
142.0.160.10:cloud-marketing.dimensiondata.com
168.143.80.202:cloud-na.dimensiondata.com
175.184.216.41:desktop.aucsfme.dimensiondata.com
185.3.28.92:dialin.dimensiondata.com
185.3.28.84:emailsignature.dimensiondata.com
51.141.12.112:go.dimensiondata.com
185.3.28.144:jira.ccs.dimensiondata.com
164.177.187.74:manage.dimensiondata.com
185.3.28.88:moveit.dimensiondata.com
168.128.68.115:mrmp.dimensiondata.com
168.128.84.8:ms.dimensiondata.com
185.3.28.144:mypassword.dimensiondata.com
168.143.80.250:na-cloud.dimensiondata.com
104.64.248.163:nextem.dimensiondata.com
162.216.170.253:quickit.dimensiondata.com
185.3.28.64:reports.dimensiondata.com
165.180.144.156:shop.dimensiondata.com
185.3.28.38:www.dimensiondata.com
45.60.118.88:www2.dimensiondata.com
root@kali2018:~#
68%
ENG
14:34
2018/03/21

Recon-ng

Recon-ng is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules, database interaction, built in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in **which open source web-based reconnaissance** can be conducted quickly and thoroughly. (B1)

Data found after using recon-ng

(Using XSSPOSED Module) (B1.1)

The XSS module (cross-site scripting) scans for vulnerabilities XSS vulnerabilities.

[*] Category: XSS

[*] Example: https://www.virustotal.com/url/submission/?force=1&url=dimensiondata.com

[*] Host: dimensiondata.com

[*] Publish_Date: 2017-09-22 19:44:58

[*] Reference: https://www.openbugbounty.org/reports/307439/ (B1.1.1 & B1.1.2)

[*] Status: unfixed

[*] Category: XSS

[*] Example: https://www.virustotal.com/url/submission/?force=1&url=dimensiondata.com

[*] Host: dimensiondata.com

[*] Publish_Date: 2017-09-20 23:55:29

[*] Reference: https://www.openbugbounty.org/reports/300444/ (B2.1.1 & B2.1.2)

[*] Status: unfixed

[*] Category: XSS

[*] Example: https://www.virustotal.com/url/submission/?force=1&url=dimensiondata.com

[*] Host: dimensiondata.com

[*] Publish_Date: 2017-09-19 22:55:19

[*] Reference: https://www.openbugbounty.org/reports/299903/ (B3.1.1 & B3.1.2)

[*] Status: unfixed

[*] Category: XSS

[*] Example: https://www.virustotal.com/url/submission/?force=1&url=dimensiondata.com

[*] Host: dimensiondata.com

[*] Publish_Date: 2017-09-11 18:03:54

[*] Reference: https://www.openbugbounty.org/reports/293418/ (B4.1.1 & B4.1.2)

[*] Status: unfixed

[*] Category: XSS

[*] Example: https://www.virustotal.com/url/submission/?force=1&url=dimensiondata.com

[*] Host: dimensiondata.com

[*] Publish_Date: 2017-09-07 13:44:01

[*] Reference: https://www.openbugbounty.org/reports/290364/ (B5.1.1 & B5.1.2)

[*] Status: unfixed

Summary:

Recon-ng (XSS Module) had gathered:

- 5 XSS vulnerabilities which are still not resolved by the company

How this gathered information can be used by the attacker

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. (B2)

An attacker can use XSS to **send a malicious script** to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any **cookies, session tokens**, or other sensitive information retained by the browser and used with that site. These scripts can **even rewrite the content** of the HTML page. (B2)

An attacker can analyse the cookies and gather information such as user ID's, login states or sessions.

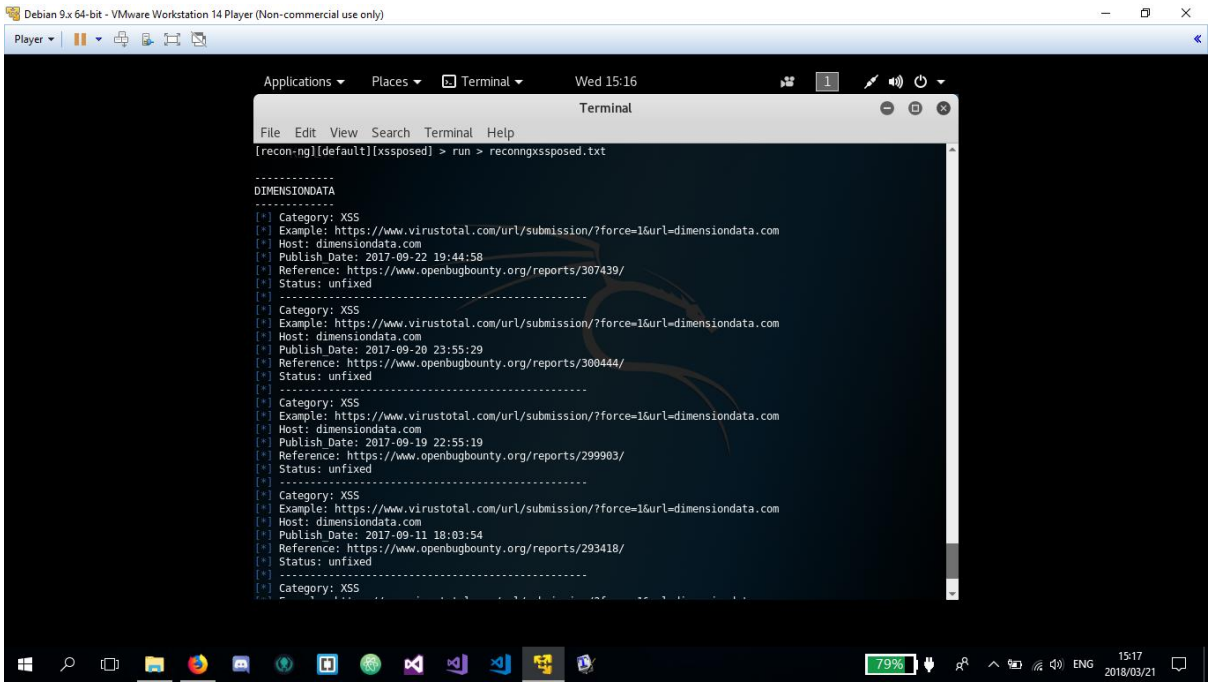
Online References

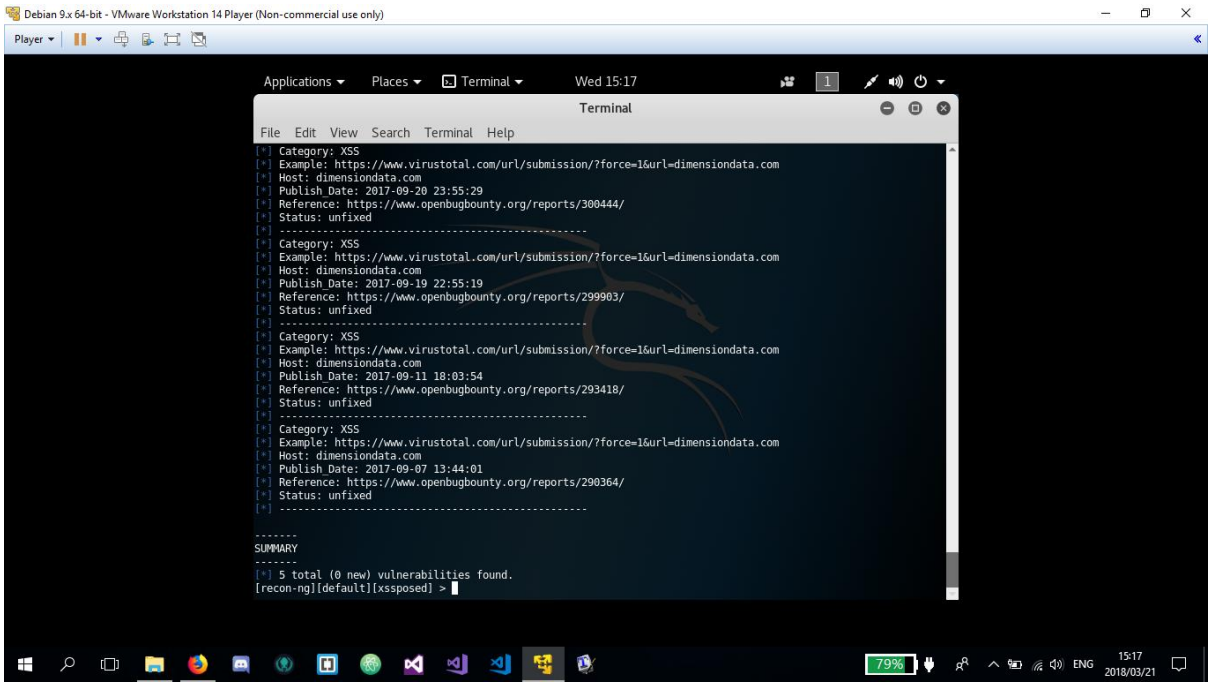
(B1) https://bitbucket.org/LaNMaSteR53/recon-ng

(B2) https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Screenshots of Recon-ng

(B1.1)





(B1.1.1)

Open Bug Bounty ID: OBB-307439

Security Researcher **M0r3h4x**, a holder of 3 badges for responsible and coordinated disclosure, found a security vulnerability affecting **dimensiondata.com** website and its users.

Following coordinated and responsible vulnerability disclosure guidelines of the **ISO 29147**, Open Bug Bounty has:

a. verified the vulnerability and confirmed its existence;
b. notified the website operator about its existence.

Affected Website:	**dimensiondata.com**
Vulnerable Application:	Custom Code
Vulnerability Type:	**XSS (Cross Site Scripting)** / CWE-79
CVSSv3 Score:	6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]
Discovered and Reported by:	**M0r3h4x**
Remediation Guide:	**OWASP XSS Prevention Cheat Sheet**

Vulnerable URL:

```
https://www.dimensiondata.com/en-NZ/Pages/Forms
/Approvereject%20Items.aspx?FollowSite=0&SiteName=%27-
confirm(%27OPENBUGBOUNTY%27)-%27
```

(B1.1.2)

Coordinated Disclosure Timeline

Vulnerability Reported:	22 September, 2017 19:44 GMT
Vulnerability Verified:	22 September, 2017 19:48 GMT
Website Operator Notified:	22 September, 2017 19:48 GMT
a. Using publicly available security contacts	✔
b. Using Open Bug Bounty notification framework	✔
c. Using security contacts provided by the researcher	✔
Vulnerability Published:	22 September, 2017 19:48 GMT [without any technical details]
Public Disclosure:	21 December, 2017 19:44 GMT

(B2.1.1)

Open Bug Bounty ID: OBB-300444

Security Researcher **M0r3h4x**, a holder of 3 badges for responsible and coordinated disclosure, found a security vulnerability affecting **dimensiondata.com** website and its users.

Following coordinated and responsible vulnerability disclosure guidelines of the **ISO 29147**, Open Bug Bounty has:

a. verified the vulnerability and confirmed its existence;
b. notified the website operator about its existence.

Affected Website:	**dimensiondata.com**
Vulnerable Application:	Custom Code
Vulnerability Type:	**XSS (Cross Site Scripting)** / CWE-79
CVSSv3 Score:	6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]
Discovered and Reported by:	**M0r3h4x**
Remediation Guide:	**OWASP XSS Prevention Cheat Sheet**

Vulnerable URL:

```
https://www.dimensiondata.com/en-NZ/Pages/Forms
/AllItems.aspx?FollowSite=0&SiteName=%27-
confirm(%27OPENBUGBOUNTY%27)-%27
```

(B2.1.2)

Coordinated Disclosure Timeline

Vulnerability Reported:	20 September, 2017 23:55 GMT
Vulnerability Verified:	20 September, 2017 23:57 GMT
Website Operator Notified:	20 September, 2017 23:57 GMT
a. Using publicly available security contacts	✔
b. Using Open Bug Bounty notification framework	✔
c. Using security contacts provided by the researcher	✔
Vulnerability Published:	20 September, 2017 23:57 GMT [without any technical details]
Public Disclosure:	19 December, 2017 23:55 GMT

(B3.1.1)

Open Bug Bounty ID: OBB-299903

Security Researcher **M0r3h4x**, a holder of 3 badges for responsible and coordinated disclosure, found a security vulnerability affecting **dimensiondata.com** website and its users.

Following coordinated and responsible vulnerability disclosure guidelines of the **ISO 29147**, Open Bug Bounty has:

a. verified the vulnerability and confirmed its existence;
b. notified the website operator about its existence.

Affected Website:	**dimensiondata.com**
Vulnerable Application:	Custom Code
Vulnerability Type:	**XSS (Cross Site Scripting)** / CWE-79
CVSSv3 Score:	6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]
Discovered and Reported by:	**M0r3h4x**
Remediation Guide:	**OWASP XSS Prevention Cheat Sheet**

Vulnerable URL:

```
https://www.dimensiondata.com/de-de/solutions/_layouts
/15/viewlsts.aspx?FollowSite=0&SiteName=%27-
confirm(%27OPENBUGBOUNTY%27)-%27
```

(B3.1.2)

Coordinated Disclosure Timeline

Vulnerability Reported:	19 September, 2017 22:55 GMT
Vulnerability Verified:	19 September, 2017 22:58 GMT
Website Operator Notified:	19 September, 2017 22:58 GMT
a. Using publicly available security contacts	✔
b. Using Open Bug Bounty notification framework	✔
c. Using security contacts provided by the researcher	✔
Vulnerability Published:	19 September, 2017 22:58 GMT [without any technical details]
Public Disclosure:	18 December, 2017 22:55 GMT

(B4.1.1)

Open Bug Bounty ID: OBB-293418

Security Researcher **Thirup**, a holder of 2 badges for responsible and coordinated disclosure, found a security vulnerability affecting **dimensiondata.com** website and its users.

Following coordinated and responsible vulnerability disclosure guidelines of the **ISO 29147**, Open Bug Bounty has:

a. verified the vulnerability and confirmed its existence;
b. notified the website operator about its existence.

Affected Website:	**dimensiondata.com**
Vulnerable Application:	Custom Code
Vulnerability Type:	**XSS (Cross Site Scripting)** / CWE-79
CVSSv3 Score:	6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]
Discovered and Reported by:	**Thirup**
Remediation Guide:	**OWASP XSS Prevention Cheat Sheet**

Vulnerable URL:

```
https://www.dimensiondata.com/en-US/_layouts
/15/viewlsts.aspx?FollowSite=0&SiteName=%27-
confirm(%27OPENBUGBOUNTY%27)-%27
```

(B4.1.2)

Coordinated Disclosure Timeline

Vulnerability Reported:	11 September, 2017 18:03 GMT
Vulnerability Verified:	11 September, 2017 18:06 GMT
Website Operator Notified:	11 September, 2017 18:06 GMT
a. Using publicly available security contacts	✔
b. Using Open Bug Bounty notification framework	✔
c. Using security contacts provided by the researcher	✔
Vulnerability Published:	11 September, 2017 18:06 GMT [without any technical details]
Public Disclosure:	10 December, 2017 18:03 GMT

(B5.1.1)

Open Bug Bounty ID: OBB-290364

Security Researcher **Thirup**, a holder of 2 badges for responsible and coordinated disclosure, found a security vulnerability affecting **dimensiondata.com** website and its users.

Following coordinated and responsible vulnerability disclosure guidelines of the **ISO 29147**, Open Bug Bounty has:

a. verified the vulnerability and confirmed its existence;
b. notified the website operator about its existence.

Affected Website:	**dimensiondata.com**
Vulnerable Application:	Custom Code
Vulnerability Type:	**XSS (Cross Site Scripting)** / CWE-79
CVSSv3 Score:	6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]
Discovered and Reported by:	**Thirup**
Remediation Guide:	**OWASP XSS Prevention Cheat Sheet**

Vulnerable URL:

```
https://www.dimensiondata.com/en-IE/Buyer-Personas/Security-Officer
/_layouts/15/viewlsts.aspx?FollowSite=0&SiteName=%27-
confirm(%27OPENBUGBOUNTY%27)-%27
```

(B5.1.2)

Coordinated Disclosure Timeline

Vulnerability Reported:	7 September, 2017 13:44 GMT
Vulnerability Verified:	7 September, 2017 13:46 GMT
Website Operator Notified:	7 September, 2017 13:46 GMT
a. Using publicly available security contacts	✔
b. Using Open Bug Bounty notification framework	✔
c. Using security contacts provided by the researcher	✔
Vulnerability Published:	7 September, 2017 13:46 GMT [without any technical details]
Public Disclosure:	6 December, 2017 13:44 GMT

WHOIS

WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format (C1)

Data found after using WHOIS

Domain Information

Domain:	dimensiondata.com
Registrar:	Network Solutions, LLC.
Registration Date:	1995-08-01
Expiration Date:	2018-07-31
Updated Date:	2017-07-19
Status:	clientTransferProhibited

(C1.1)

Name Servers

ns1.p03.dynect.net

ns2.p03.dynect.net

ns3.p03.dynect.net

ns4.p03.dynect.net

(C1.1)

Registrant Contact

Registrant Contact	
Name:	Dimension Data
Organization:	Dimension Data
Street:	Private Bag X163
City:	Bryanston
State:	Gauteng
Postal Code:	2021
Country:	ZA
Phone:	+27.115754867
Fax:	+27.115760520
Email:	email@za.didata.com

(C1.1)

Administrative Contact

Registrant Contact	
Name:	Dimension Data
Organization:	Dimension Data
Street:	Private Bag X163
City:	Bryanston
State:	Gauteng
Postal Code:	2021
Country:	ZA
Phone:	+27.115754867
Fax:	+27.115760520
Email:	email@za.didata.com

(C1.1)

Technical Contact

Registrant Contact	
Name:	Dimension Data
Organization:	Dimension Data
Street:	Private Bag X163
City:	Bryanston
State:	Gauteng
Postal Code:	2021
Country:	ZA
Phone:	+27.115754867
Fax:	+27.115760520
Email:	email@za.didata.com

(C1.1)

Summary:

WHOIS had gathered:

- Domain information
- Name servers
- Registrant contact details
- Administrative contact details
- Technical contact details

How this gathered information can be used by the attacker

By knowing the domain details an attacker can carry out 'Typosquatting' attacks

Typosquatting is where hijackers register misspelt versions of your domain name to send the traffic to malicious sites. Examples would **be dimensiondatr.com, dimensindata.com**, and so on. Registering all possible versions of your domain name including singular and plural versions, all common domain extensions and hyphenated and non-hyphenated word compounds. (C2)

Moreover, by knowing the registrant details, the attacker can attempt **to hack the website registrar**. When a registrar is hacked, attackers have access to all domains in their database. (C2)

The attacker can also attempt to **hijack the domain** to take it offline or to transfer it to another person.

Domain phishing and **DNS attacks** are also possible. The attacker can trick email recipients into handing over their account details via links in **emails posing as their registrar**. The link can forward the victims to a **fake registrar website** looking to obtain sensitive information. The attacker can also carry out a DNS attack and by changing the DNS records visitors may land on a different website. Moreover, they could cause the sever to crash by sending too much traffic to the DNS server.

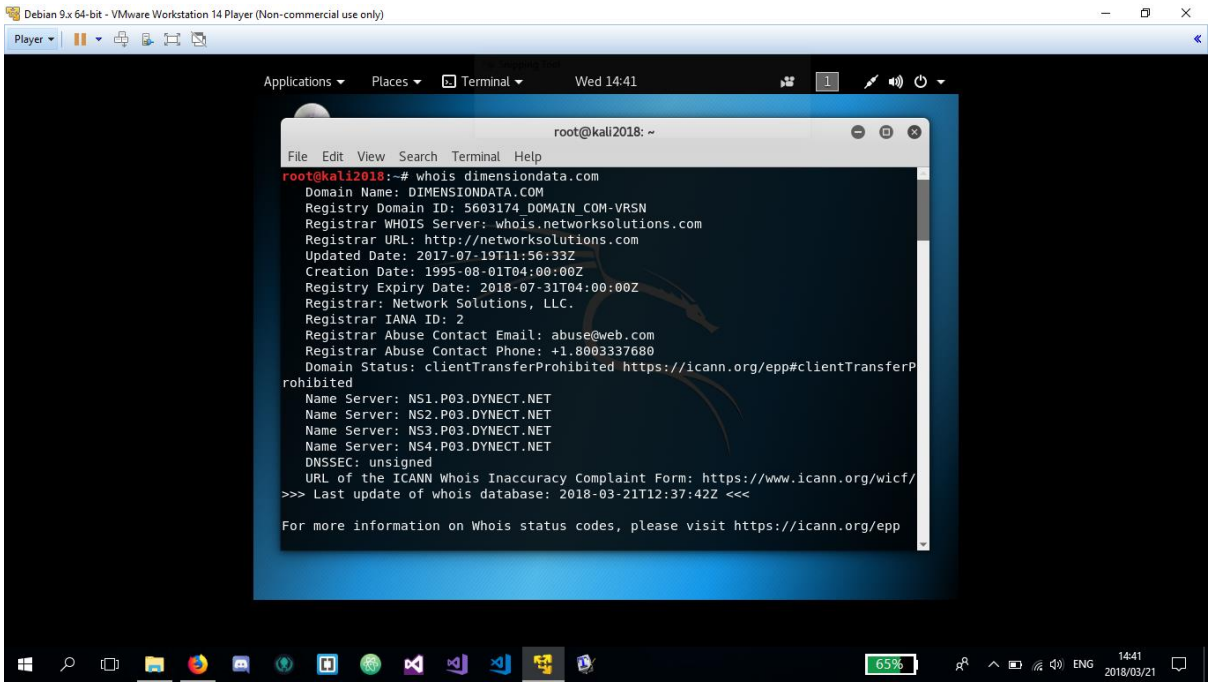
Online References

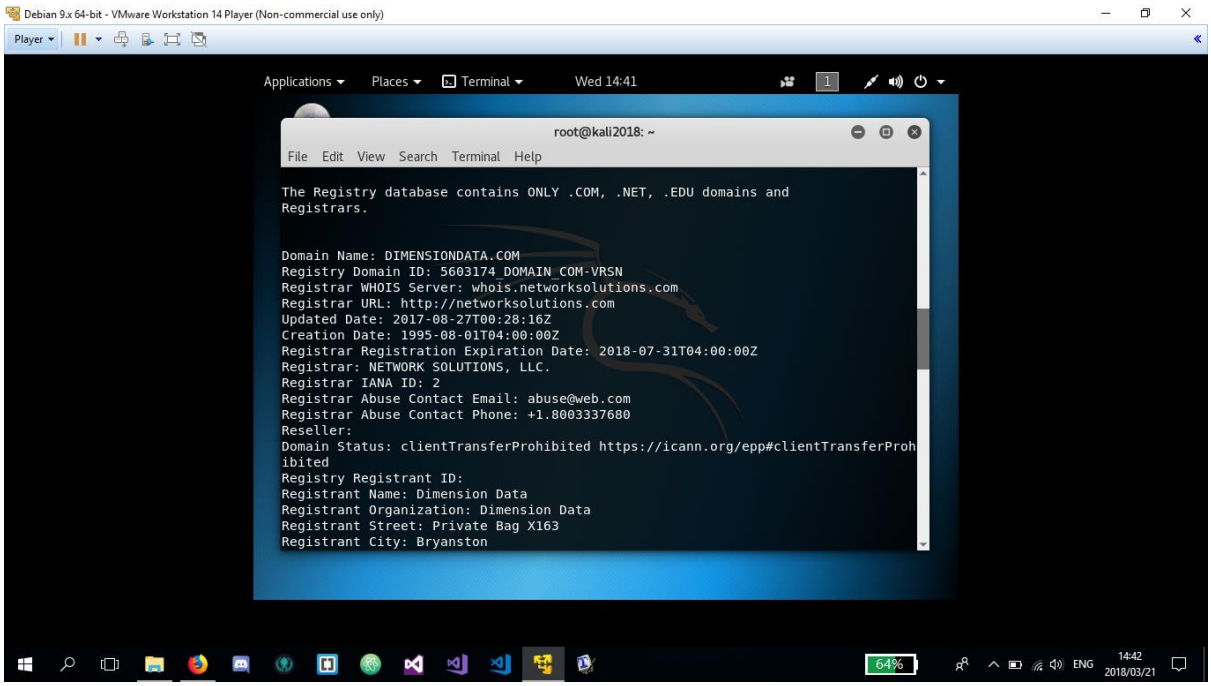
(C1) https://en.wikipedia.org/wiki/WHOIS

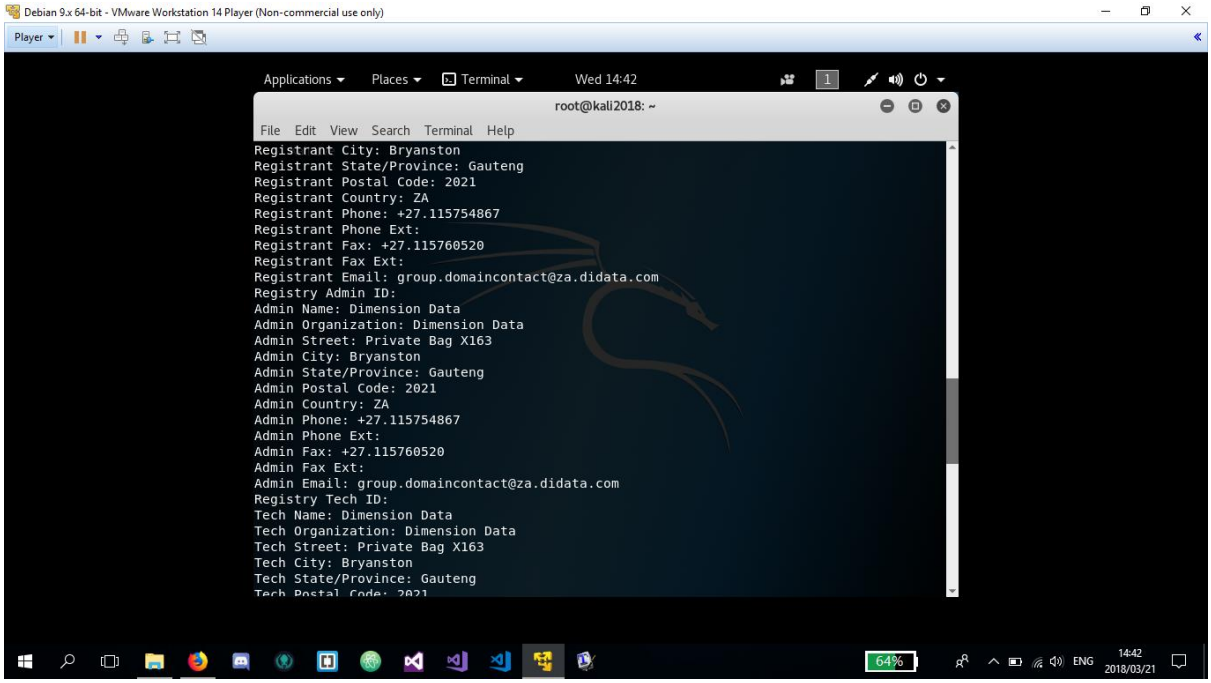
(C2) https://www.namecheap.com/security/domain-phishing-security-attacks-guide/

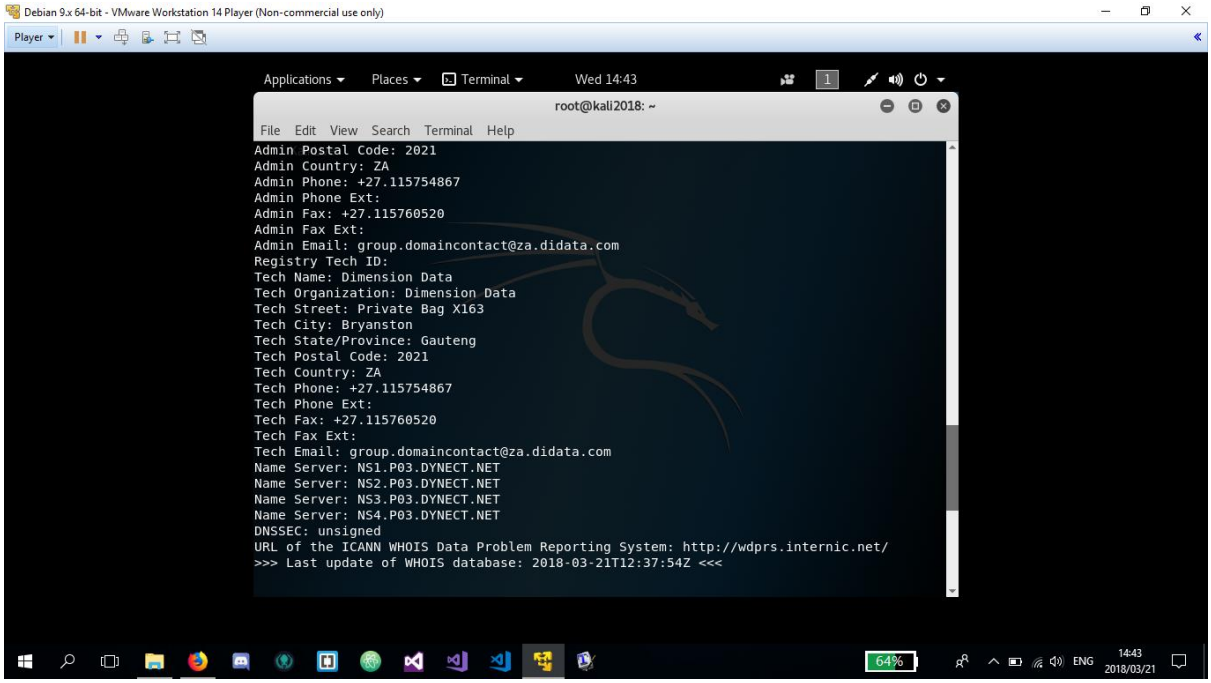
Screenshots of WHOIS

(C1.1)






Debian 9.x 64-bit - VMware Workstation 14 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Wed 14:42
root@kali2018: ~
File Edit View Search Terminal Help
Registrant City: Bryanston
Registrant State/Province: Gauteng
Registrant Postal Code: 2021
Registrant Country: ZA
Registrant Phone: +27.115754867
Registrant Phone Ext:
Registrant Fax: +27.115760520
Registrant Fax Ext:
Registrant Email: group.domaincontact@za.didata.com
Registry Admin ID:
Admin Name: Dimension Data
Admin Organization: Dimension Data
Admin Street: Private Bag X163
Admin City: Bryanston
Admin State/Province: Gauteng
Admin Postal Code: 2021
Admin Country: ZA
Admin Phone: +27.115754867
Admin Phone Ext:
Admin Fax: +27.115760520
Admin Fax Ext:
Admin Email: group.domaincontact@za.didata.com
Registry Tech ID:
Tech Name: Dimension Data
Tech Organization: Dimension Data
Tech Street: Private Bag X163
Tech City: Bryanston
Tech State/Province: Gauteng
64%
ENG
14:42
2018/03/21


Debian 9.x 64-bit - VMware Workstation 14 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Wed 14:43
root@kali2018: ~
File Edit View Search Terminal Help
Admin Postal Code: 2021
Admin Country: ZA
Admin Phone: +27.115754867
Admin Phone Ext:
Admin Fax: +27.115760520
Admin Fax Ext:
Admin Email: group.domaincontact@za.didata.com
Registry Tech ID:
Tech Name: Dimension Data
Tech Organization: Dimension Data
Tech Street: Private Bag X163
Tech City: Bryanston
Tech State/Province: Gauteng
Tech Postal Code: 2021
Tech Country: ZA
Tech Phone: +27.115754867
Tech Phone Ext:
Tech Fax: +27.115760520
Tech Fax Ext:
Tech Email: group.domaincontact@za.didata.com
Name Server: NS1.P03.DYNECT.NET
Name Server: NS2.P03.DYNECT.NET
Name Server: NS3.P03.DYNECT.NET
Name Server: NS4.P03.DYNECT.NET
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2018-03-21T12:37:54Z <<<
64%
ENG
14:43
2018/03/21

DNSDumpster

DNSDumpster is a domain research tool to **find host related information**. Not just subdomain but it gives us information about **DNS server**, **MX record**, **TXT record** and a **mapping** of the domain for dimensiondata.com.

DNSDumpster can also carry out **sub-domain enumeration** which will **increase the scope** for vulnerabilities to be found. This could also **revel lost applications** running on sub-domains which can be exploited. (D1)

Data found after using DNS Dumpster

DNS Servers

ns3.p03.dynect.net.	208.78.71.3 ns3.p03.dynect.net	AS33517 Dynamic Network Services, Inc. United States
ns4.p03.dynect.net.	204.13.251.3 ns4.p03.dynect.net	AS33517 Dynamic Network Services, Inc. United States
ns1.p03.dynect.net.	208.78.70.3 ns1.p03.dynect.net	AS33517 Dynamic Network Services, Inc. United States
ns2.p03.dynect.net.	204.13.250.3 ns2.p03.dynect.net	AS33517 Dynamic Network Services, Inc. United States

MX Records

10 eu-smtp-inbound-2.mimecast.com.	195.130.217.201 eu-smtp-inbound-1.mimecast.com	AS42427 Mimecast Services Limited United Kingdom
10 eu-smtp-inbound-1.mimecast.com.	195.130.217.211 eu-smtp-inbound-2.mimecast.com	AS42427 Mimecast Services Limited United Kingdom

TXT Records

"AXXj6MDMQTCemJzsU6U7eeVATzhR49cQzwXNQPw5yw541TEEsbVOBUOZIFR/abWrdVwfIInbapvY2dT3soAiRw=="
"v=spf1 include:spf.mailjet.com include:_netblocks.mimecast.com include:spf.mandrillapp.com include:mailsenders.netsuite.com include:stspg-customer.com ~all"
"OLBHPUeyGP8zkElgMNqec1doxuWXW9h+I6F4SPjrn9EznwZWpD8uhCWyd4r1CUhbW6tn9hk3hNUyQMrfVnkwkA=="
"google-site-verification=EPUio7XedNrPQEiVTsChWWVz1EkX2EsEnDGrjRTTrG0"
"status-page-domain-verification=cwjb898p224h"
"status-page-domain-verification=f9qss9c3dr04"
"FnxtPU8tmpPL61UGREdXzAUaxlpCyWIqfXXtI08ZxV1LV+Q7L5mgyk57fHSisKIc3qmwh5KeY/tvFxlTYOdupA=="
"rao2/6j+Nwg3/2bgRoZ+iDMCIpjpED5dV3fzFXIty0+Ot9c566unswbcp+nxsRbz/rvXlBhYwl0XTi9eMVsgNQ=="

Host Records

aplyncfe01.dimensiondata.com	152.102.144.23
sfbwebau01.dimensiondata.com	148.182.16.161
webappsau01.dimensiondata.com	148.182.16.163
remotesal1.dimensiondata.com	87.215.135.235
. . . 150 Records	

(D1.1.1)

Summary:

DNS Dumpster had gathered:

- 4 DNS Servers,
- 2 MX Records (Mail Exchange)
- 8 TXT Records (Text Record)
- +150 Host Records

How this gathered information can be used by the attacker

By doing **reverse searches on the targets domain name**, the attacker can acquire **a list of domain servers** owned by the organisation which can significantly **increase the attack surface**. Moreover, from the host records, some give **information regarding the operating system and server role** of the host, which can **reveal the security posture** of the organisation. (D2)

A **mail exchanger** record (MX record) is a type of certified and verified resource record in the Domain Name System that specifies a mail server responsible for accepting email messages on behalf of a recipient's domain. An attacker can use the information gathered regarding the MX Records of dimension data and **alter the contents of the record** such that **emails** sent to the company are **rerouted** to the attacker instead. These emails could contain sensitive information about the business and its processes or clients. (D4)

A **TXT record** is a type of resource record in the Domain Name System (DNS) used to provide the ability to associate arbitrary text with a host or other name, such as human readable information about a server, network, data centre, or other accounting information. (D5)

Attackers can use TXT Records to keep **control over any trojans** they may send through to the system, rather than relying on a command and control server which can be shut down by the government at any given time. By using the Domain Name System, attackers can effectively establish **two-way communication** between themselves and the victim's computer without going through centralized entities or service providers. Moreover, it also makes the communication virtually invisible, which would make it difficult for the attacker to get tracked down. (D3)

Online References

(D1) https://blog.appsecco.com/a-penetration-testers-guide-to-sub-domain-enumeration-7d842d5570f6

(D2) https://dnsdumpster.com/footprinting-reconnaissance/

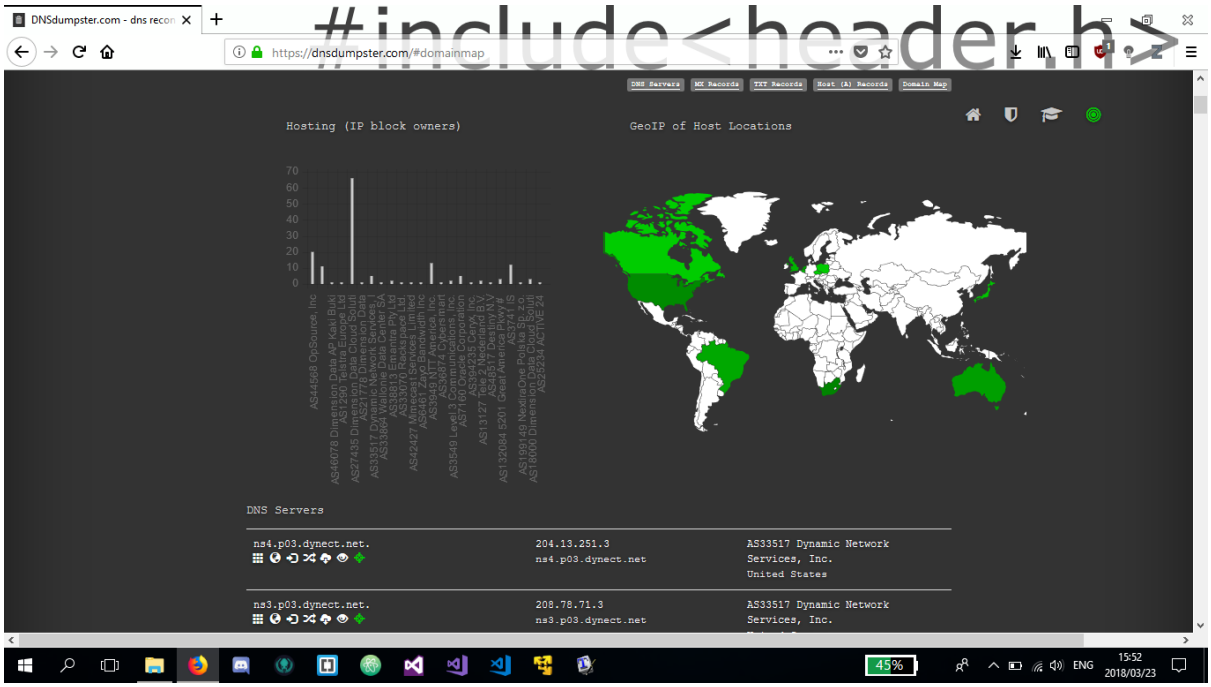
(D3) https://themerkle.com/cyber-criminals-start-to-use-dns-txt-records-to-control-remote-access-trojans/

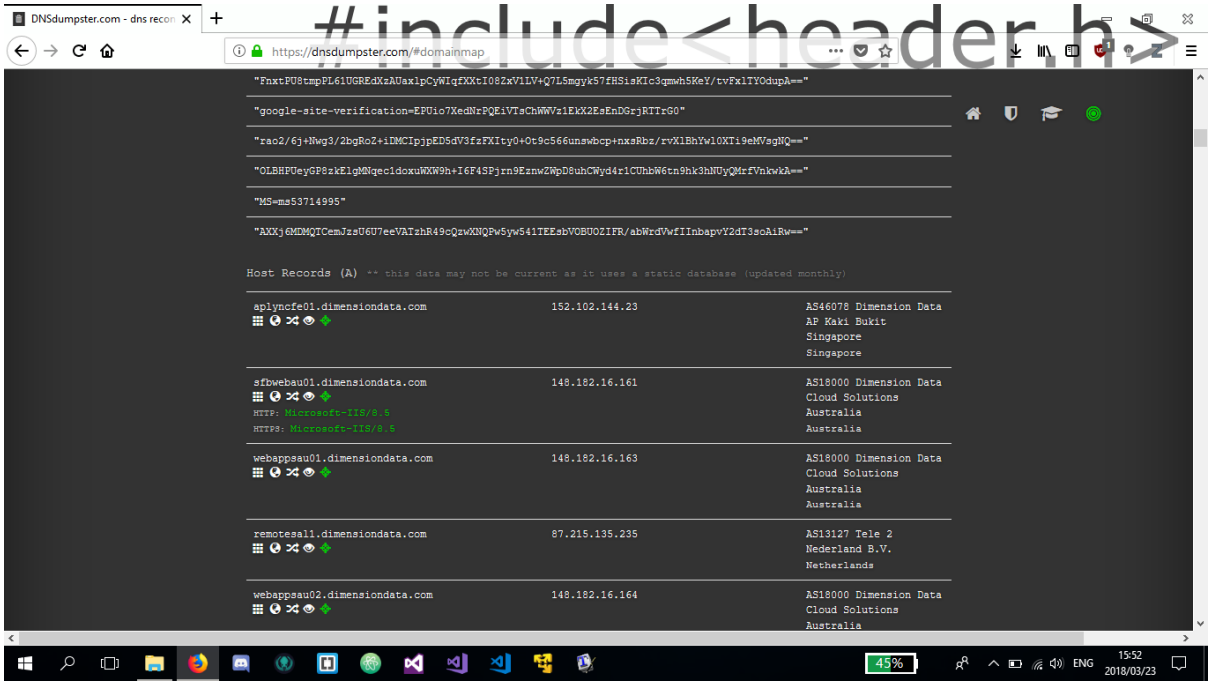
(D4) https://en.wikipedia.org/wiki/MX_record

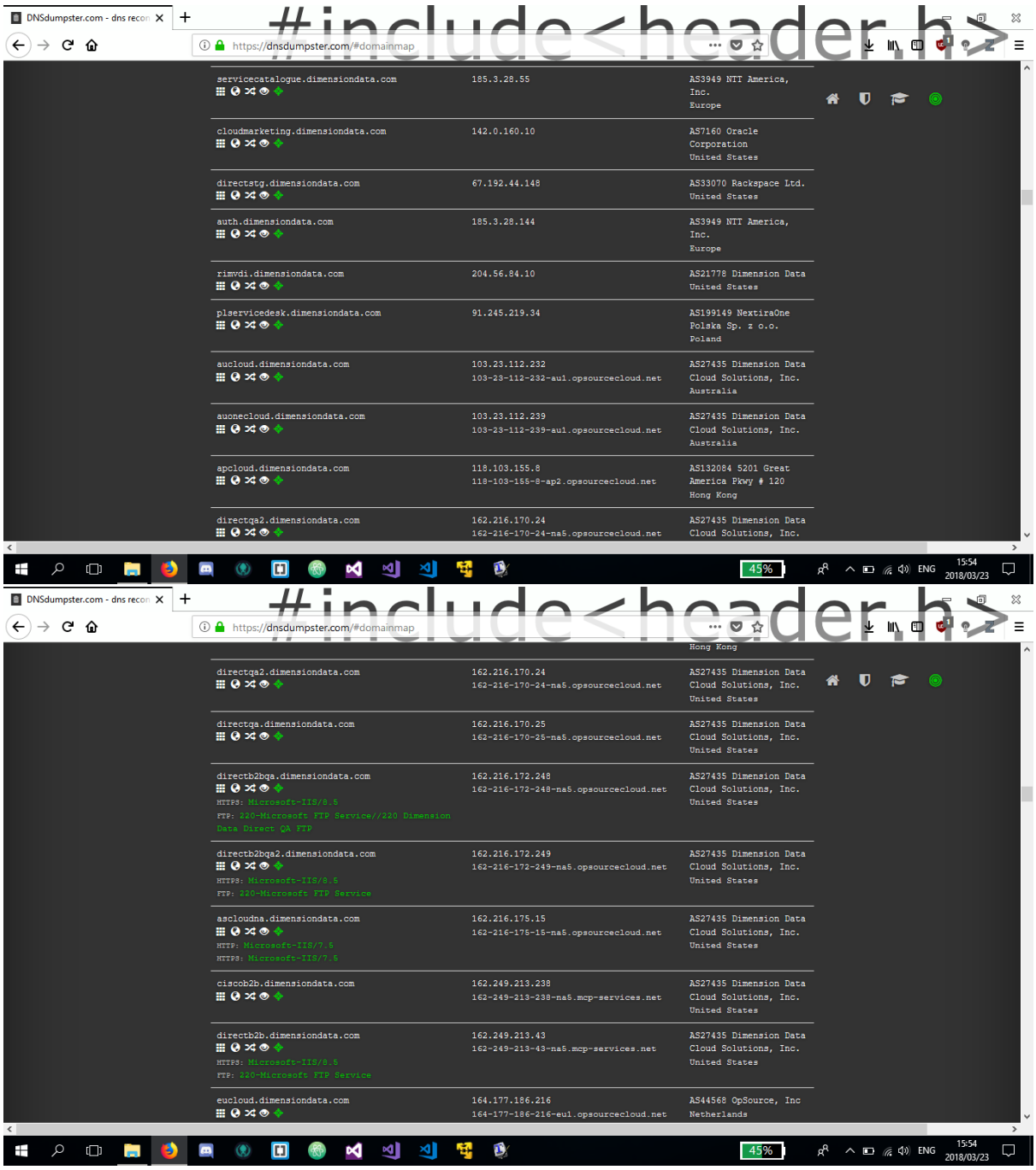
(D5) https://en.wikipedia.org/wiki/TXT_record

Screenshots of DNSDumpster

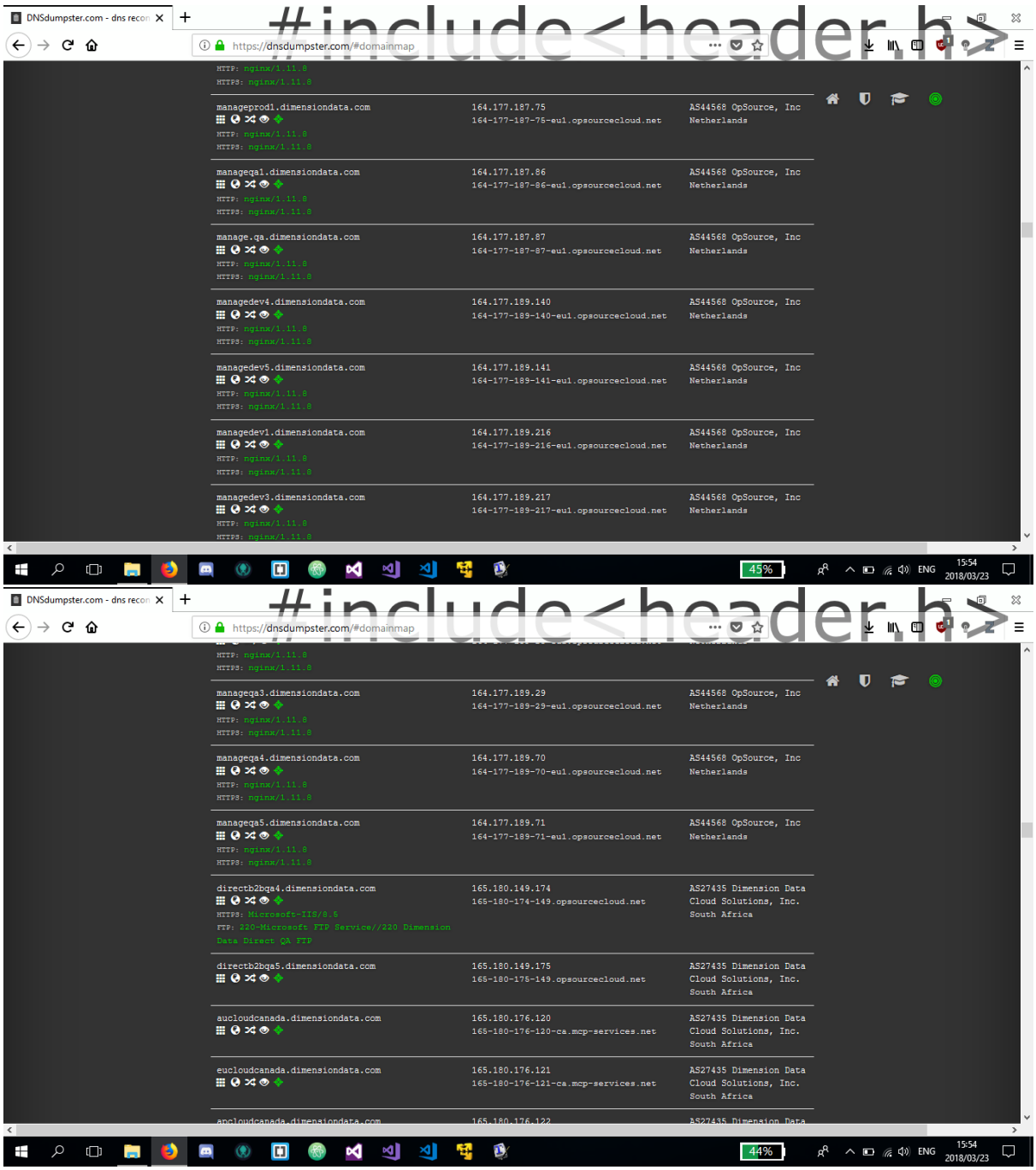
(D1.1)





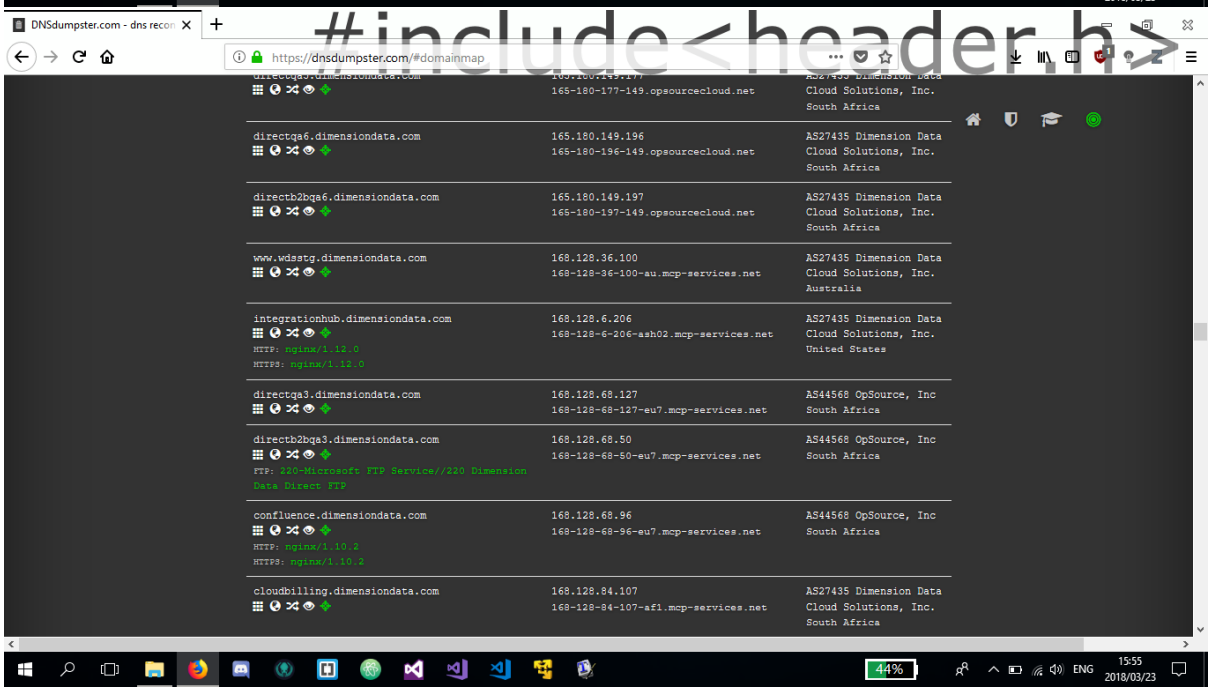

#include<header.h>
DNSdumpster.com - dns recon
https://dnsdumpster.com/#domainmap
servicecatalogue.dimensiondata.com 185.3.28.55 AS3949 NTT America, Inc. Europe
cloudmarketing.dimensiondata.com 142.0.160.10 AS7160 Oracle Corporation United States
directstg.dimensiondata.com 67.192.44.148 AS33070 Rackspace Ltd. United States
auth.dimensiondata.com 185.3.28.144 AS3949 NTT America, Inc. Europe
rimvdi.dimensiondata.com 204.56.84.10 AS21778 Dimension Data United States
plservicedesk.dimensiondata.com 91.245.219.34 AS199149 NextiraOne Polska Sp. z o.o. Poland
aucloud.dimensiondata.com 103.23.112.232 103-23-112-232-au1.opsourcecloud.net AS27435 Dimension Data Cloud Solutions, Inc. Australia
auonecloud.dimensiondata.com 103.23.112.239 103-23-112-239-au1.opsourcecloud.net AS27435 Dimension Data Cloud Solutions, Inc. Australia
apcloud.dimensiondata.com 118.103.155.8 118-103-155-8-ap2.opsourcecloud.net AS132084 5201 Great America Pkwy # 120 Hong Kong
directqa2.dimensiondata.com 162.216.170.24 162-216-170-24-na5.opsourcecloud.net AS27435 Dimension Data Cloud Solutions, Inc.
45%
ENG
15:54
2018/03/23

#include<header.h>
DNSdumpster.com - dns recon
https://dnsdumpster.com/#domainmap
Hong Kong
directqa2.dimensiondata.com 162.216.170.24 162-216-170-24-na5.opsourcecloud.net AS27435 Dimension Data Cloud Solutions, Inc. United States
directqa.dimensiondata.com 162.216.170.25 162-216-170-25-na5.opsourcecloud.net AS27435 Dimension Data Cloud Solutions, Inc. United States
directb2bqa.dimensiondata.com 162.216.172.248 162-216-172-248-na5.opsourcecloud.net AS27435 Dimension Data Cloud Solutions, Inc. United States
HTTPS: Microsoft-IIS/8.5
FTP: 220-Microsoft FTP Service//220 Dimension Data Direct QA FTP
directb2bqa2.dimensiondata.com 162.216.172.249 162-216-172-249-na5.opsourcecloud.net AS27435 Dimension Data Cloud Solutions, Inc. United States
HTTPS: Microsoft-IIS/8.5
FTP: 220-Microsoft FTP Service
ascloudna.dimensiondata.com 162.216.175.15 162-216-175-15-na5.opsourcecloud.net AS27435 Dimension Data Cloud Solutions, Inc. United States
HTTP: Microsoft-IIS/7.5
HTTPS: Microsoft-IIS/7.5
ciscob2b.dimensiondata.com 162.249.213.238 162-249-213-238-na5.mcp-services.net AS27435 Dimension Data Cloud Solutions, Inc. United States
directb2b.dimensiondata.com 162.249.213.43 162-249-213-43-na5.mcp-services.net AS27435 Dimension Data Cloud Solutions, Inc. United States
HTTPS: Microsoft-IIS/8.5
FTP: 220-Microsoft FTP Service
eucloud.dimensiondata.com 164.177.186.216 164-177-186-216-eu1.opsourcecloud.net AS44568 OpSource, Inc Netherlands
45%
ENG
15:54
2018/03/23

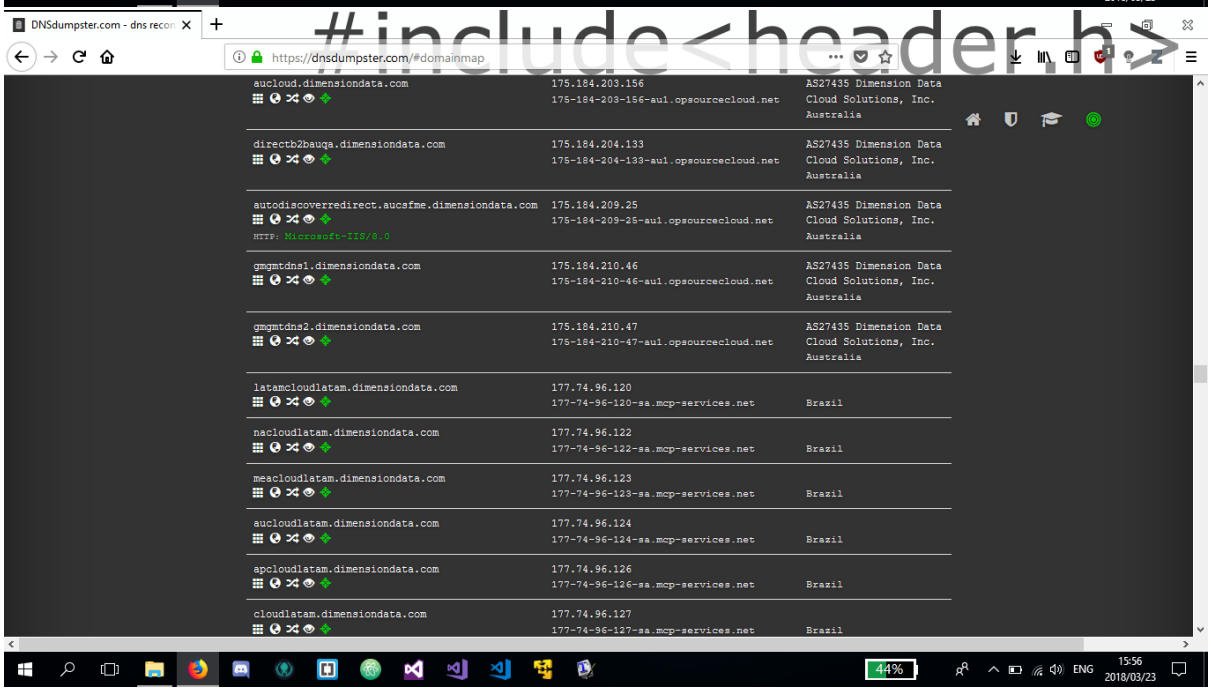

DNSdumpster.com - dns recon
https://dnsdumpster.com/#domainmap
#include<header.h>
manageprod1.dimensiondata.com
164.177.187.75
164-177-187-75-eu1.opsourcecloud.net
AS44568 OpSource, Inc
Netherlands
manageqa1.dimensiondata.com
164.177.187.86
164-177-187-86-eu1.opsourcecloud.net
AS44568 OpSource, Inc
Netherlands
manage.qa.dimensiondata.com
164.177.187.87
164-177-187-87-eu1.opsourcecloud.net
AS44568 OpSource, Inc
Netherlands
managedev4.dimensiondata.com
164.177.189.140
164-177-189-140-eu1.opsourcecloud.net
AS44568 OpSource, Inc
Netherlands
managedev5.dimensiondata.com
164.177.189.141
164-177-189-141-eu1.opsourcecloud.net
AS44568 OpSource, Inc
Netherlands
managedev1.dimensiondata.com
164.177.189.216
164-177-189-216-eu1.opsourcecloud.net
AS44568 OpSource, Inc
Netherlands
managedev3.dimensiondata.com
164.177.189.217
164-177-189-217-eu1.opsourcecloud.net
AS44568 OpSource, Inc
Netherlands
45%
ENG
15:54
2018/03/23

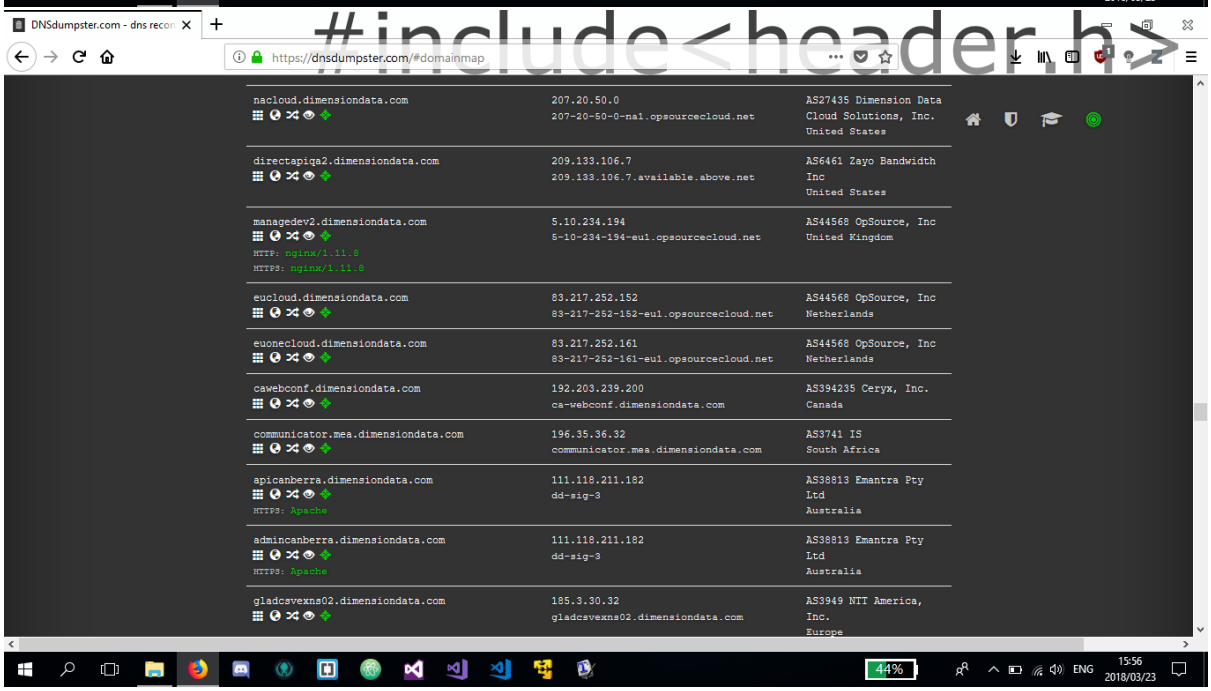
DNSdumpster.com - dns recon
https://dnsdumpster.com/#domainmap
#include<header.h>
manageqa3.dimensiondata.com
164.177.189.29
164-177-189-29-eu1.opsourcecloud.net
AS44568 OpSource, Inc
Netherlands
manageqa4.dimensiondata.com
164.177.189.70
164-177-189-70-eu1.opsourcecloud.net
AS44568 OpSource, Inc
Netherlands
manageqa5.dimensiondata.com
164.177.189.71
164-177-189-71-eu1.opsourcecloud.net
AS44568 OpSource, Inc
Netherlands
directb2bqa4.dimensiondata.com
HTTPS: Microsoft-IIS/8.5
FTP: 220-Microsoft FTP Service//220 Dimension Data Direct QA FTP
165.180.149.174
165-180-174-149.opsourcecloud.net
AS27435 Dimension Data Cloud Solutions, Inc. South Africa
directb2bqa5.dimensiondata.com
165.180.149.175
165-180-175-149.opsourcecloud.net
AS27435 Dimension Data Cloud Solutions, Inc. South Africa
aucloudcanada.dimensiondata.com
165.180.176.120
165-180-176-120-ca.mcp-services.net
AS27435 Dimension Data Cloud Solutions, Inc. South Africa
eucloudcanada.dimensiondata.com
165.180.176.121
165-180-176-121-ca.mcp-services.net
AS27435 Dimension Data Cloud Solutions, Inc. South Africa
44%
ENG
15:54
2018/03/23

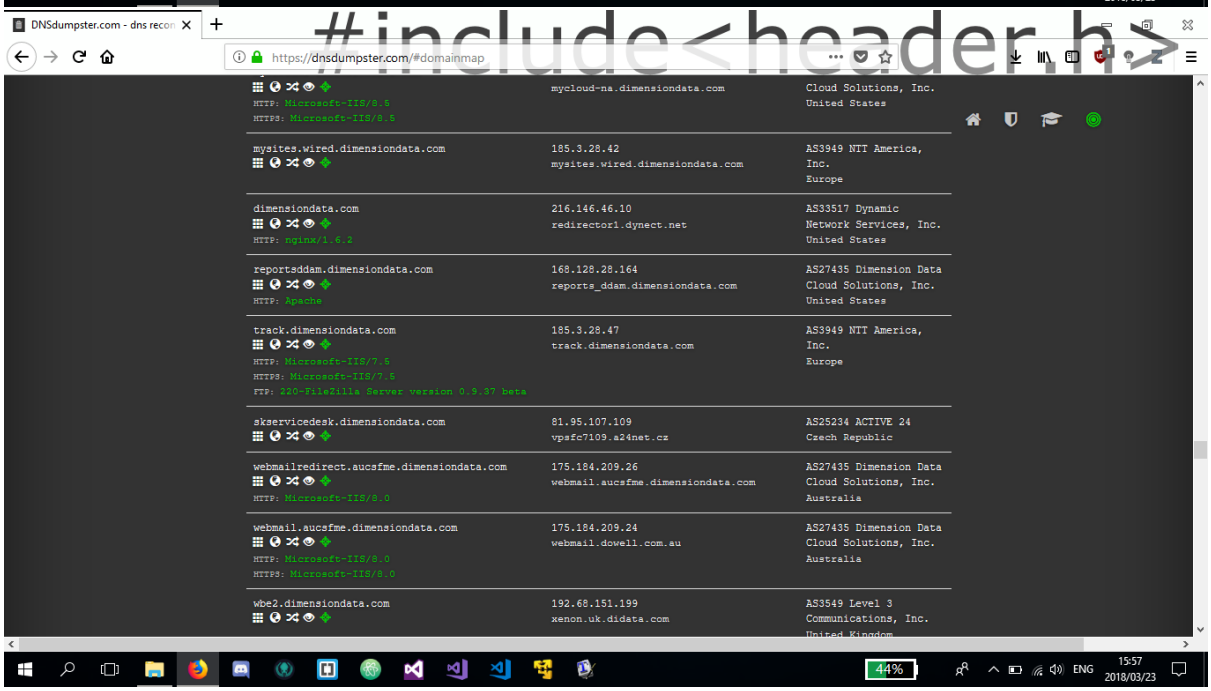
#include<header.h>



#include<header.h>








DNSdumpster.com - dns recon
https://dnsdumpster.com/#domainmap
South Africa
eucloudmea.dimensiondata.com 197.96.16.218 AS27435 Dimension Data Cloud Solutions, Inc. South Africa
ddasbbq01.mea.dimensiondata.com 197.96.22.78 AS27435 Dimension Data Cloud Solutions, Inc. South Africa
meapool3.mea.dimensiondata.com 196.36.188.132 AS3741 IS South Africa
meapool4.mea.dimensiondata.com 196.36.188.133 AS3741 IS South Africa
salavayasa.mea.dimensiondata.com 196.41.108.45 AS36874 Cybersmart South Africa
HTTPS: Apache-Coyote/1.1
lync13wc.mea.dimensiondata.com 196.35.36.37 AS3741 IS South Africa
webmail.mea.dimensiondata.com 196.35.34.106 AS3741 IS South Africa
emm.mea.dimensiondata.com 196.14.162.20 AS3741 IS South Africa
vmnetedge01.zoom.mea.dimensiondata.com 196.35.36.34 AS3741 IS South Africa
vmnetedge02.zoom.mea.dimensiondata.com 196.35.36.53 AS3741 IS South Africa
vmnetedge03.zoom.mea.dimensiondata.com 196.35.36.33 AS3741 IS South Africa
45%
ENG
15:53
2018/03/23

FOCA

Fingerprinting Organizations with Collected Archives

FOCA is a reconnaissance tool which is used for information gathering about a targeted organization. FOCA finds metadata and hidden information by downloading all of the organization's public documents, of a wide variety of formats, directly from the target's domain. Some techniques which are used in order to locate these documents include search engines such as Google, Bing and Exalead, DNS queries and reverse DNS lookup. The data is then extracted and analysed. FOCA matches information to identify which documents have been created by the same team of people and what servers and clients may be inferred from them. The software and operating system information that FOCA provides can be used in crafting exploits.

Data found after using FOCA:

Network:

Clients:	(1)
Name:	PC_TShirvil
Operating System:	Windows
Users:	TShirvil
Software:	Microsoft Office

Domains:

Name:	www2.dimensiondata.com
Software:	www2.dimensiondata.com
Fingerprinting Banner:	Microsoft – IIS/8.5
IP Address Source:	DNS resolution [45.60.118.88]
Related Domains:	www2.dimensiondata.com – DNS resolution [216.146.46.11]

Roles:

Roles in IP:	Https Http
FingerPrinting HTTP:	www2.dimensiondata.com.80 www2.dimensiondata.com.443

Vulnerabilities:

Insecure Methods:	45.60.118.80 [www2.dimensiondata.com]
Roles in IP:	HTTPS HTTP
Source in IP:	www2.dimensiondata.com

Metadata:

Documents:	100
	71 pdf documents found and analysed
Users: (4)	TShirvil Dimension Data Irosenberg GeneVanLoggerenberg – Full name, Eugene Van Loggerenberg

Software:

Attribute	Value
All software found (18) - Times found	
Microsoft Office	3
Adobe PDF Library 15.0	19
Adobe InDesign CC 2015 (Macintosh)	11
Adobe InDesign CC 13.0 (Macintosh)	1
Adobe InDesign CC 2017 (Macintosh)	7
Preview	3
Mac OS X 10.12.6 Quartz PDFContext	2
Adobe PDF Library 9.9	1
Adobe InDesign CS5 (7.0)	1
Adobe PDF Library 10.0.1	12
Adobe InDesign CS6 (Macintosh)	12
Adobe PDF Library 11.0	3
Adobe InDesign CC 2014 (Macintosh)	2
Mac OS X 10.12.5 Quartz PDFContext	1
www.adlibsoftware.com: CTP (5.4.3.32930) OS...	1
Adobe InDesign CC (Macintosh)	1
Adobe PDF Library 15.00	1
Adobe Illustrator CC 22.0 (Macintosh)	1

How this gathered information can be used by the attacker

Since FOCA provided us with the **software** that Dimension Data uses and the **version** of each of the software, we can exploit this information. E.g.: if a user uses **a vulnerable version** of Adobe PDF reader or Microsoft Excel files with exploit macros can be sent to users to compromise the PC. Folder names can sometimes be useful to enumerate users and in understanding the directory structure. **Details of printers** are another set of useful information as **printer networks** are often ignored or **access controls will not be properly enforced**. Once in the internal network, access to printer network can help in escalating access to other parts of network or sensitive information being printed. [1]

Vulnerabilities in software used by Dimension Data:

Further research was conducted on the software which the company currently use to find out what vulnerabilities are already present in those particular versions.

Adobe InDesign CS5 (7.0)

This version of Adobe InDesign has some vulnerabilities which can be used to an attacker's advantage.

Vulnerabilities include: [2]

- Untrusted search path
- Allows local users, and possibly remote attackers, to execute arbitrary code
- Conduct DLL hijacking attacks via a Trojan horse ibfs32.dll that is located in the same folder as an .indl, .indp, .indt, or .inx file.

– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	CWE id is not defined for this vulnerability

Mac OS X 10.12.5 Quartz PDF Reader

This version of Mac OS has vulnerabilities which can be exploited by an attacker.

Vulnerabilities include: [3][4]

- Multiple memory corruption issues exist in the Kernel component that allow a local attacker to gain kernel-level privileges.
- A local privilege escalation vulnerability exists in the Kernel component due to a race condition. A local attacker can exploit this to execute arbitrary code with kernel-level privileges.
- A memory corruption issue exists in the Intel graphics driver component that allows a local attacker to execute arbitrary code with kernel-level privileges.
- Multiple memory corruption issues exist in SQLite due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit these, by convincing a user to visit a specially crafted website, to execute arbitrary code.
- A denial of service vulnerability exists in the CoreText component due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, via a specially crafted file, to crash an application.

Apple » Mac Os X » 10.12.5 : Vulnerability Statistics

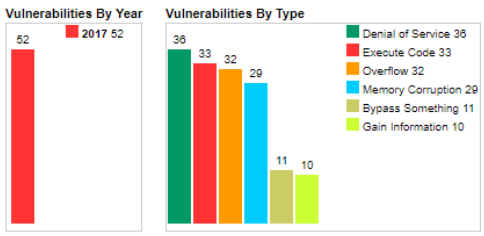
Vulnerabilities (52) Related Metasploit Modules (Cpe Name:cpe:/o:apple:mac_os_x:10.12.5)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2017	52	36	33	32	29					11	10				
Total	52	36	33	32	29					11	10				
% Of All		69.2	63.5	61.5	55.8	0.0	0.0	0.0	0.0	21.2	19.2	0.0	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may n in those years.)



Adobe PDF Library 11.0

Adobe PDF Library 11.0 has vulnerabilities which can be exploited by

an attacker.

Vulnerabilities include: [5]

- The vulnerability is caused by the computation that writes data past the end of the intended buffer, the computation is part of the image conversion module that handless TIFF data.
- An attacker can potentially leverage the vulnerability to corrupt sensitive data or execute arbitrary code.

– CVSS Scores & Vulnerability Types

CVSS Score	6.8
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	787

Adobe PDF Library 10.0.1

Vulnerabilities include: [6]

- Allow attackers to execute arbitrary code
- Cause a denial of service (memory corruption) via unspecified vectors

– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service Execute Code Overflow Memory corruption
CWE ID	119

Microsoft FingerPrinting IIS/8.5:

Vulnerabilities present which can be exploited by an attacker.

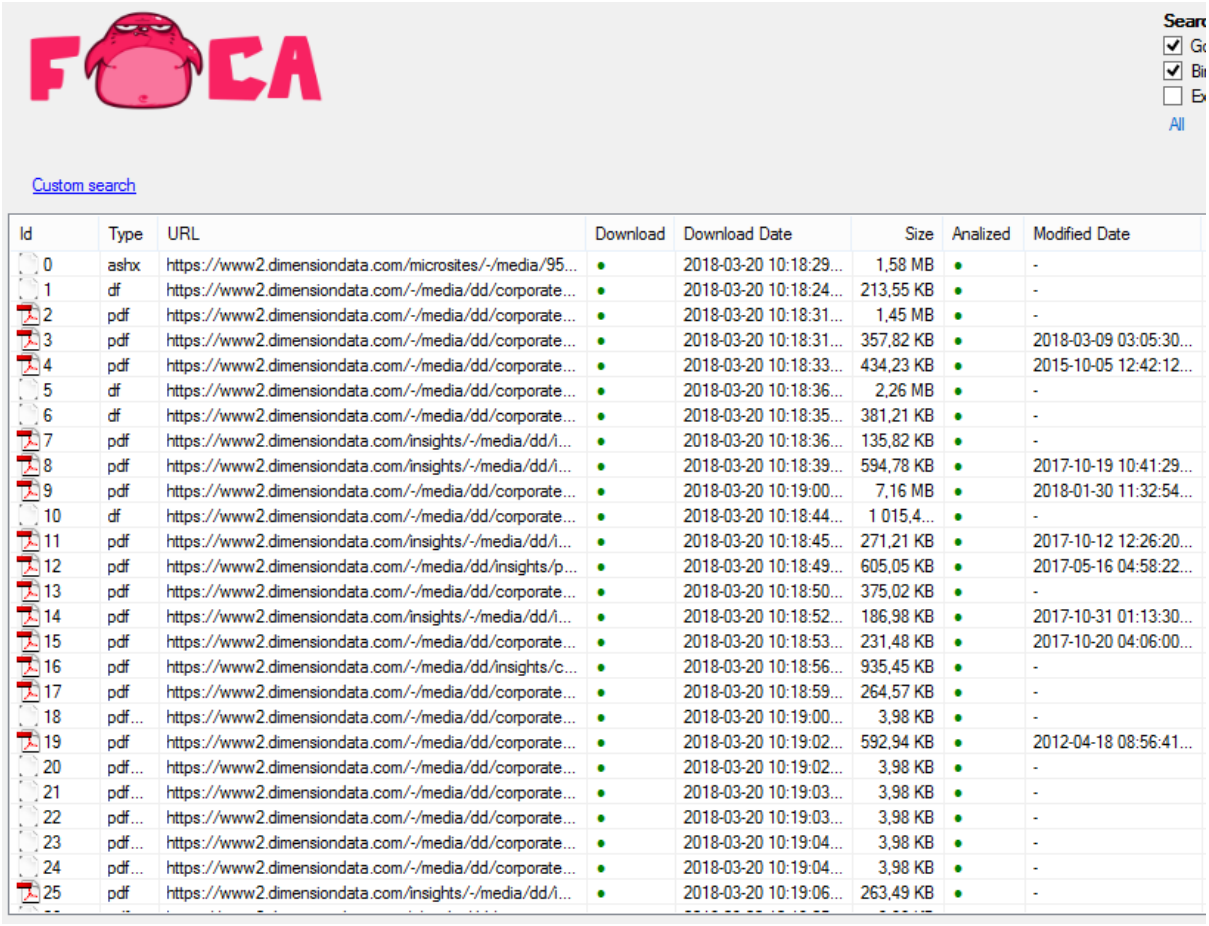
Vulnerabilities include: [7]

- Microsoft Internet Information Services 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list
- This makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability."

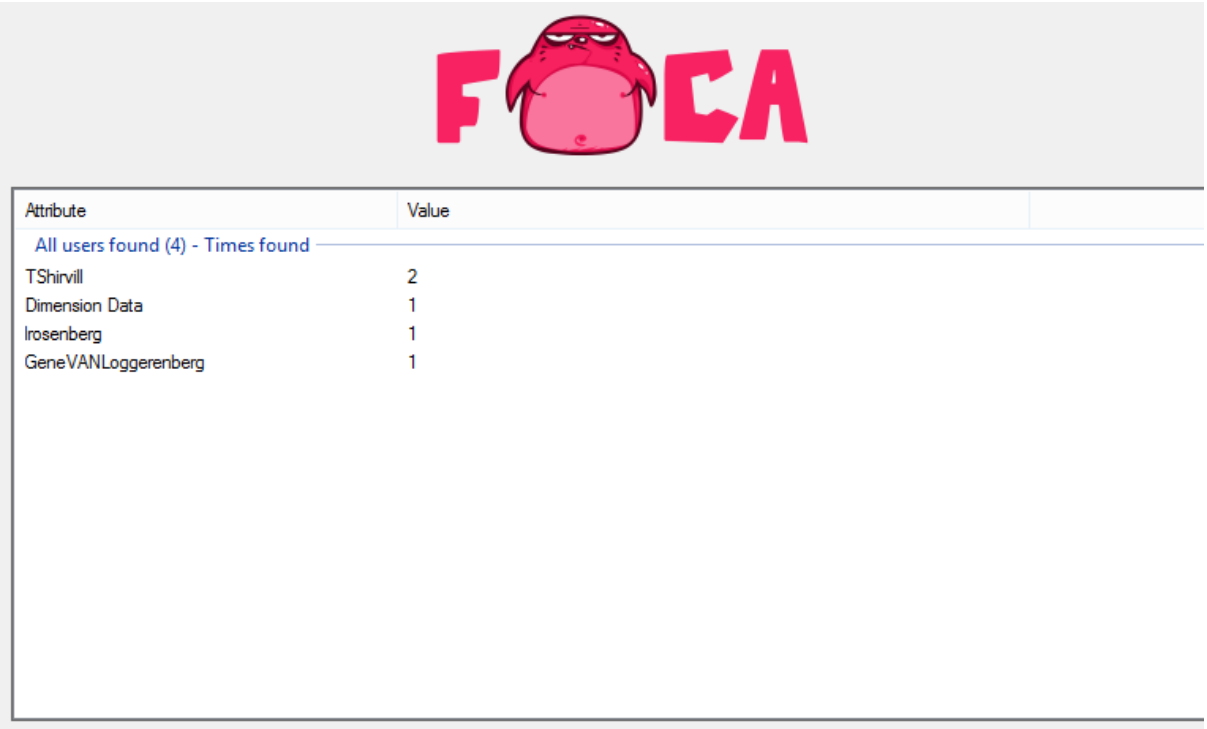
– CVSS Scores & Vulnerability Types

CVSS Score	5.1
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	High (Specialized access conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Bypass a restriction or similar
CWE ID	264

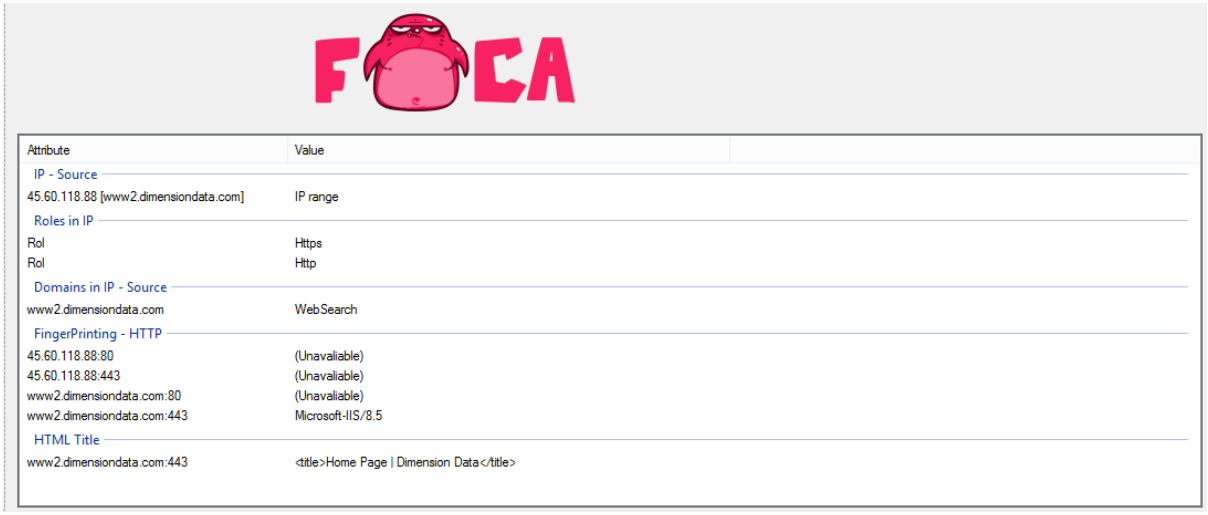
Screenshots of FOCA Data:



Id	Type	URL	Download	Download Date	Size	Analized	Modified Date
0	ashx	https://www2.dimensiondata.com/microsites/-/media/95...	•	2018-03-20 10:18:29...	1,58 MB	•	-
1	df	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:18:24...	213,55 KB	•	-
2	pdf	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:18:31...	1,45 MB	•	-
3	pdf	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:18:31...	357,82 KB	•	2018-03-09 03:05:30...
4	pdf	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:18:33...	434,23 KB	•	2015-10-05 12:42:12...
5	df	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:18:36...	2,26 MB	•	-
6	df	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:18:35...	381,21 KB	•	-
7	pdf	https://www2.dimensiondata.com/insights/-/media/dd/i...	•	2018-03-20 10:18:36...	135,82 KB	•	-
8	pdf	https://www2.dimensiondata.com/insights/-/media/dd/i...	•	2018-03-20 10:18:39...	594,78 KB	•	2017-10-19 10:41:29...
9	pdf	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:19:00...	7,16 MB	•	2018-01-30 11:32:54...
10	df	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:18:44...	1 015,4...	•	-
11	pdf	https://www2.dimensiondata.com/insights/-/media/dd/i...	•	2018-03-20 10:18:45...	271,21 KB	•	2017-10-12 12:26:20...
12	pdf	https://www2.dimensiondata.com/-/media/dd/insights/p...	•	2018-03-20 10:18:49...	605,05 KB	•	2017-05-16 04:58:22...
13	pdf	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:18:50...	375,02 KB	•	-
14	pdf	https://www2.dimensiondata.com/insights/-/media/dd/i...	•	2018-03-20 10:18:52...	186,98 KB	•	2017-10-31 01:13:30...
15	pdf	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:18:53...	231,48 KB	•	2017-10-20 04:06:00...
16	pdf	https://www2.dimensiondata.com/-/media/dd/insights/c...	•	2018-03-20 10:18:56...	935,45 KB	•	-
17	pdf	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:18:59...	264,57 KB	•	-
18	pdf...	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:19:00...	3,98 KB	•	-
19	pdf	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:19:02...	592,94 KB	•	2012-04-18 08:56:41...
20	pdf...	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:19:02...	3,98 KB	•	-
21	pdf...	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:19:03...	3,98 KB	•	-
22	pdf...	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:19:03...	3,98 KB	•	-
23	pdf...	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:19:04...	3,98 KB	•	-
24	pdf...	https://www2.dimensiondata.com/-/media/dd/corporate...	•	2018-03-20 10:19:04...	3,98 KB	•	-
25	pdf	https://www2.dimensiondata.com/insights/-/media/dd/i...	•	2018-03-20 10:19:06...	263,49 KB	•	-

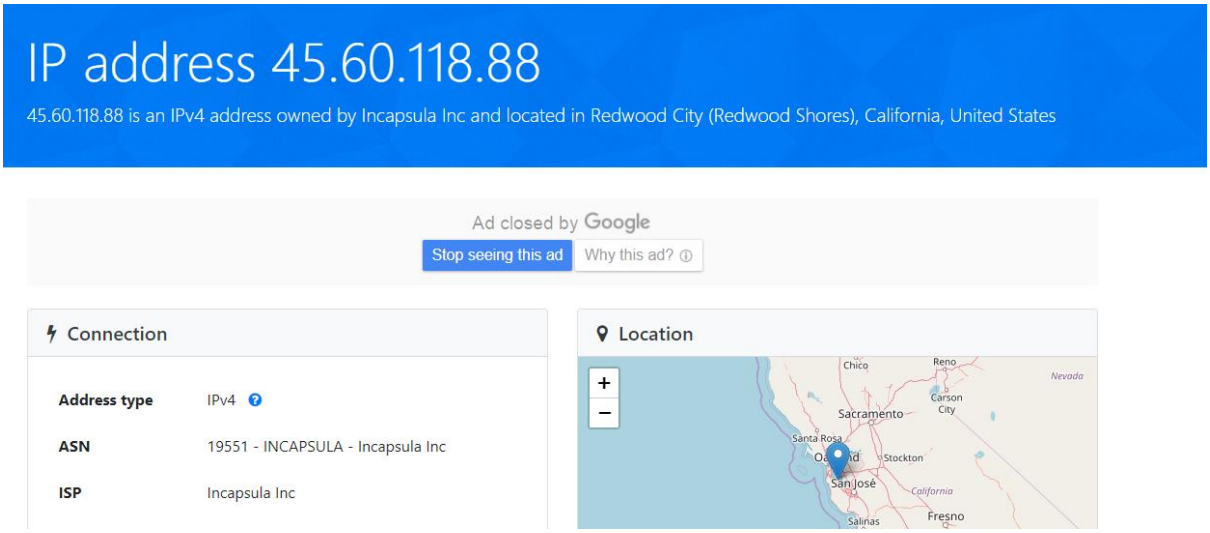


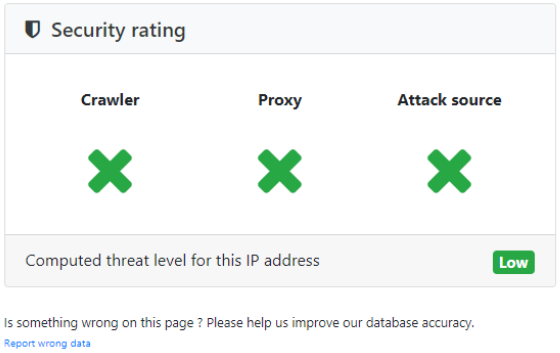
Attribute	Value
All users found (4) - Times found	
TShirvill	2
Dimension Data	1
lrosenberg	1
GeneVANLoggerenberg	1

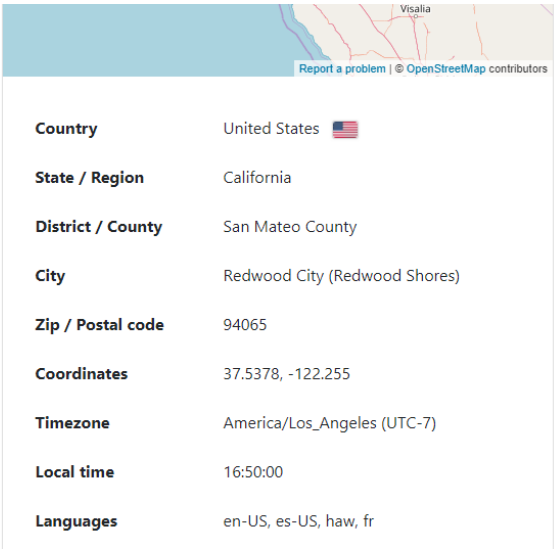


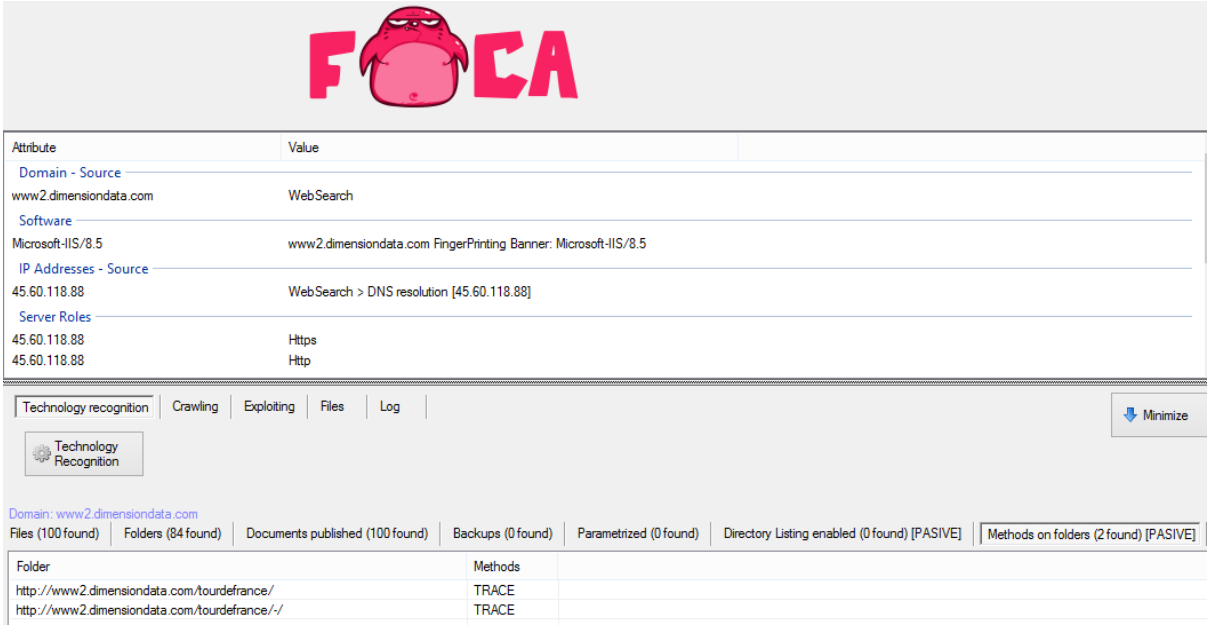
Attribute	Value
IP - Source	
45.60.118.88 [www2.dimensiondata.com]	IP range
Roles in IP	
Rol	Https
Rol	Http
Domains in IP - Source	
www2.dimensiondata.com	WebSearch
FingerPrinting - HTTP	
45.60.118.88:80	(Unavaliable)
45.60.118.88:443	(Unavaliable)
www2.dimensiondata.com:80	(Unavaliable)
www2.dimensiondata.com:443	Microsoft-IIS/8.5
HTML Title	
www2.dimensiondata.com:443	<title>Home Page | Dimension Data</title>

Attribute	Value
Name	www2.dimensiondata.com [45.60.118.88]
Domains - Source	
www2.dimensiondata.com	WebSearch
IP Addresses - Source	
45.60.118.88	WebSearch > DNS resolution [45.60.118.88]
0.0.0.0-255.255.255.255 [Generated by FOCA]	Netrange
FingerPrinting - HTTP	
45.60.118.88:80	(Unavaliable)
45.60.118.88:443	(Unavaliable)
www2.dimensiondata.com:80	(Unavaliable)
www2.dimensiondata.com:443	Microsoft-IIS/8.5
HTML Title	
www2.dimensiondata.com:443	<title>Home Page | Dimension Data</title>
Software	
Microsoft-IIS/8.5	www2.dimensiondata.com FingerPrinting Banner: Microsoft-IIS/8.5









Online References:

[1]https://secvibe.com/non-intrusive-reconnaissance-a-step-by-step-guide-e1cc3a88e679

[2]https://www.cvedetails.com/cve/CVE-2010-3153/

[3]https://vulners.com/nessus/MACOS_10_12_5.NASL

[4]http://seclists.org/fulldisclosure/2017/May/47

[5]https://www.cvedetails.com/cve/CVE-2018-4916/

[6]https://www.cvedetails.com/cve/CVE-2015-5115/

[7] https://www.cvedetails.com/cve/CVE-2014-4078/

Nmap

The Network Mapper

Nmap is **a network scanning and host detection** reconnaissance tool. It is used as a vulnerability detector or security scanner. Nmap uses different techniques to perform scanning including: TCP connect () scanning, TCP reverse indent scanning, etc. It uses raw IP packets to determine what **hosts** are available on the network, what **services** (application name and version) those hosts are offering, what **operating systems** (OS versions) they are running, what type of **packet filters** or **firewalls** are being utilised, and various other characteristics.

Data found after doing an intense, regular, udp, trace route and ping scan:

Hosts and Services

- Service: cisco-sccp

Hostname	Port	Protocol	State	Version
www2.dimensiondata.com[45.60.118.88]	2000	tcp	open	

- Service: domain

Hostname	Port	Protocol	State	Version
www2.dimensiondata.com[45.60.118.88]	53	tcp	open	Incapsula WAF DNS
www2.dimensiondata.com[45.60.118.88]	53	udp	open	

- Service: sip

Hostname	Port	Protocol	State	Version
www2.dimensiondata.com[45.60.118.88]	5060	udp	open	

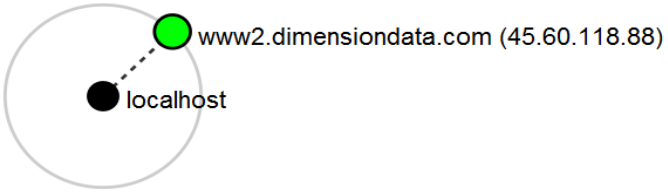
- Service: jetdirect

Hostname	Port	Protocol	State	Version
www2.dimensiondata.com[45.60.118.88]	9100	tcp	open	
www2.dimensiondata.com[45.60.118.88]	9101	tcp	open	
www2.dimensiondata.com[45.60.118.88]	9102	tcp	open	
www2.dimensiondata.com[45.60.118.88]	9103	tcp	open	

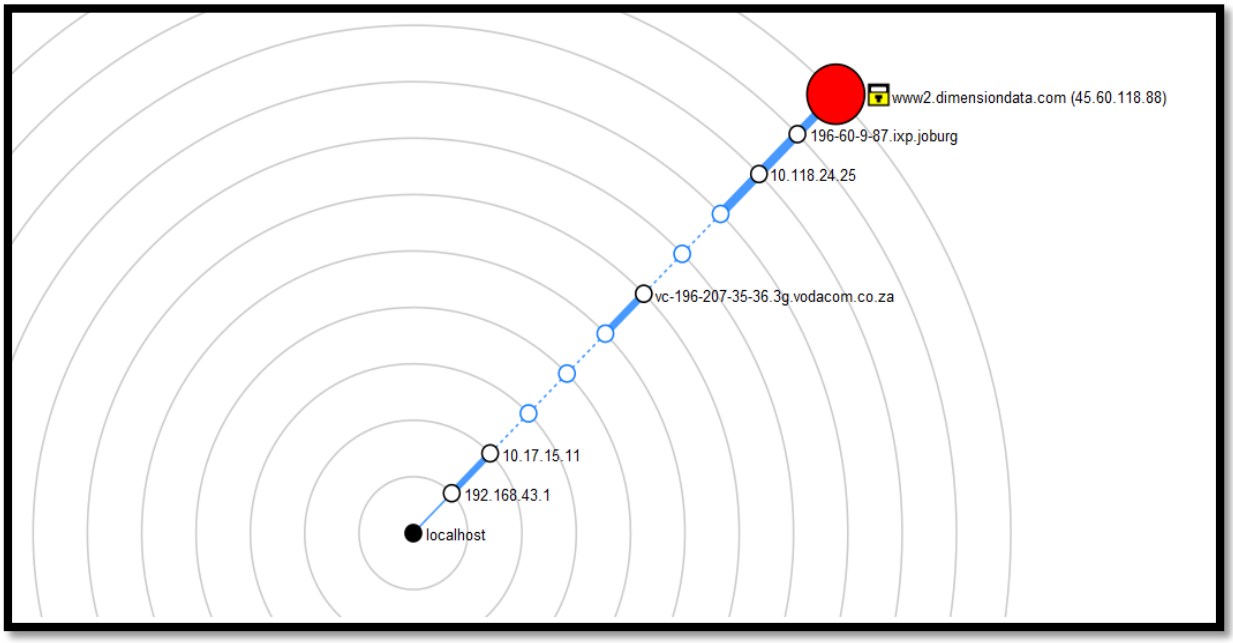
- Service: http

Hostname	Port	Protocol	State	Version
www2.dimensiondata.com[45.60.118.88]	25	tcp	open	Incapsula CDN httpd
www2.dimensiondata.com[45.60.118.88]	80	tcp	open	
www2.dimensiondata.com[45.60.118.88]	81	tcp	open	Incapsula CDN httpd
www2.dimensiondata.com[45.60.118.88]	82	tcp	open	Incapsula CDN httpd
www2.dimensiondata.com[45.60.118.88]	83	tcp	open	Incapsula CDN httpd
www2.dimensiondata.com[45.60.118.88]	85	tcp	open	Incapsula CDN httpd
www2.dimensiondata.com[45.60.118.88]	88	tcp	open	Incapsula CDN httpd
www2.dimensiondata.com[45.60.118.88]	89	tcp	open	Incapsula CDN httpd
. . . . www2.dimensiondata.com[45.60.118.88]	 60443	. . . . tcp	. . . . open	. . . . Incapsula CDN httpd

Ping scan topology:



Topology: Displays an interactive view of the connections between hosts in a network



Host Details

- Host status:

State	Open ports	Filtered ports	Closed ports	Scanned ports	Up time	Last boot
up	1184	1814	0	2000	6241391	Thur,11 Jan 2018 21:06

Addresses:

IPv4: 45.60.118.88

Hostnames:

www2.dimensiondata.com - user(type)

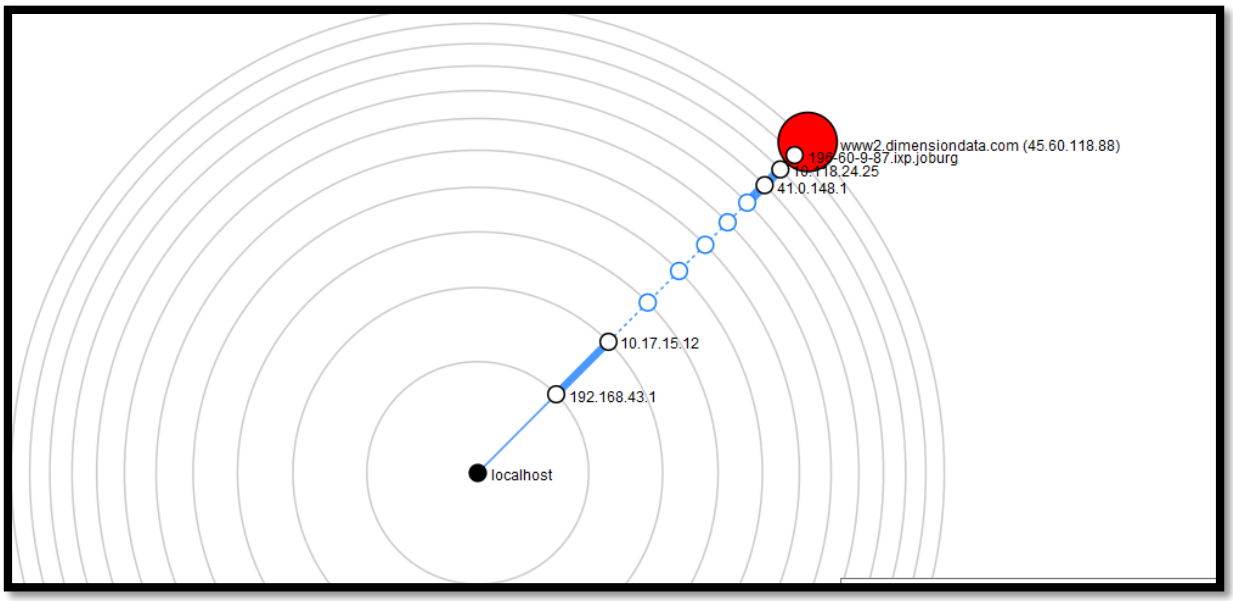
Operating System:

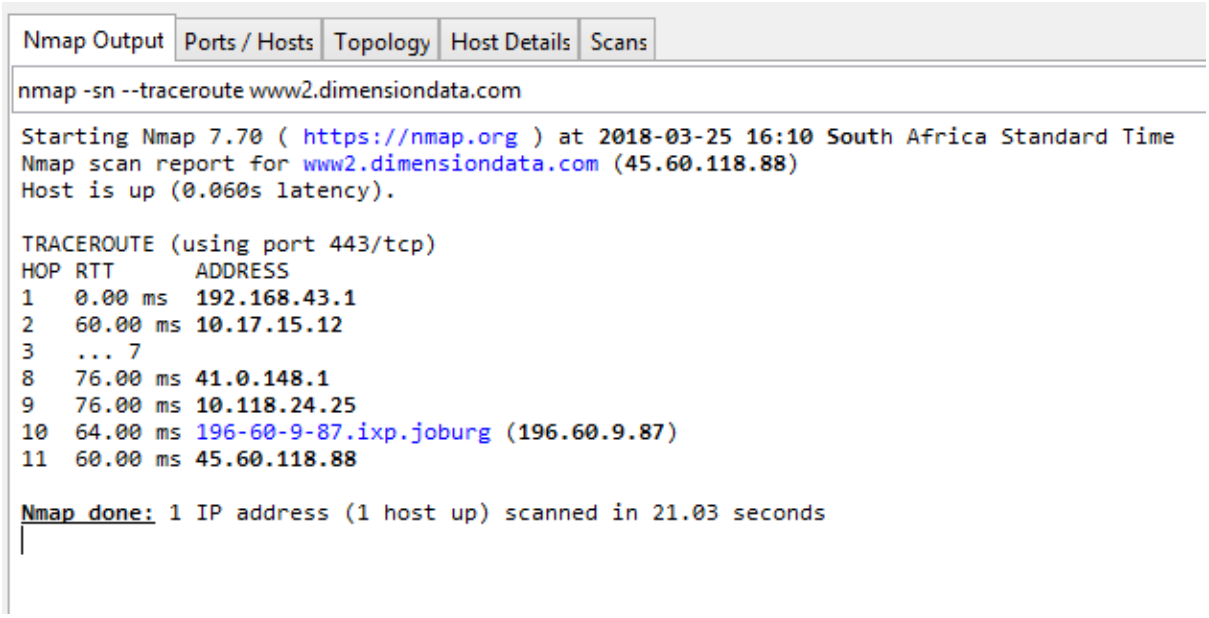
Linux 3.18

Accuracy: 91%

Ports used: 25-tcp-open

Trace Route Topology and output screen





How can this gathered information be used by the attacker:

Knowing the **open ports** of Dimension Data can help:[1]

- To find a vulnerability, the attacker needs to fingerprint all services which run on the machine by finding out which protocol is used, the programs which implement them and preferably the versions of those programs.
- To fingerprint a service, the attacker needs to know that there is one running on a publicly accessible port.
- To find out which publicly accessible ports run services.

Linux 3.18 vulnerabilities:

- Vulnerable to a stack overflow in the processing of L2CAP configuration responses.
- Resulting in Remote code execution in kernel space.

– CVSS Scores & Vulnerability Types

CVSS Score	8.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	Admin
Vulnerability Type(s)	Execute Code Overflow
CWE ID	119

- Allows local users to cause a denial of service
- Which can possibly have unspecified other impact by triggering a creation failure

– CVSS Scores & Vulnerability Types

CVSS Score	7.2
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	415

Online References

[1]https://security.stackexchange.com/questions/120711/why-do-hackers-scan-for-open-ports

[2] https://www.cvedetails.com/cve/CVE-2018-7480/

Nmap Screenshots of data:

```
555/tcp   open  http        Incapsula CDN httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://www2.dimensiondata.com/
636/tcp   open  ssl/http    Incapsula CDN httpd
| http-robots.txt: 5 disallowed entries
| /sitecore modules/ /sitecore_files/ /temp/ /upload/
|_*/registration
| ssl-cert: Subject: commonName=*.dimensiondata.com/organizationName=Dimension Data Holdings Plc/stateOrProvinceName=Gauteng/countryName=ZA
| Subject Alternative Name: DNS:*.dimensiondata.com, DNS:dimensiondata.com, DNS:www2.dimensiondata.com
| Issuer: commonName=DigiCert SHA2 High Assurance Server CA/organizationName=DigiCert Inc/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-02-11T00:00:00
| Not valid after:  2019-05-01T12:00:00
| MD5:   c0c8 1a57 9380 8a1c 02d3 ab82 fcab 4ca8
|_SHA-1: 5d32 cfa7 879a 9690 7b09 2b5f df29 7616 c0e6 308c
|_ssl-date: TLS randomness does not represent time
| tls-nextprotoneg:
|_  http/1.1
800/tcp   open  http        Incapsula CDN httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://www2.dimensiondata.com/
801/tcp   open  http        Incapsula CDN httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://www2.dimensiondata.com/
843/tcp   open  http        Incapsula CDN httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://www2.dimensiondata.com/
1000/tcp  open  http        Incapsula CDN httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

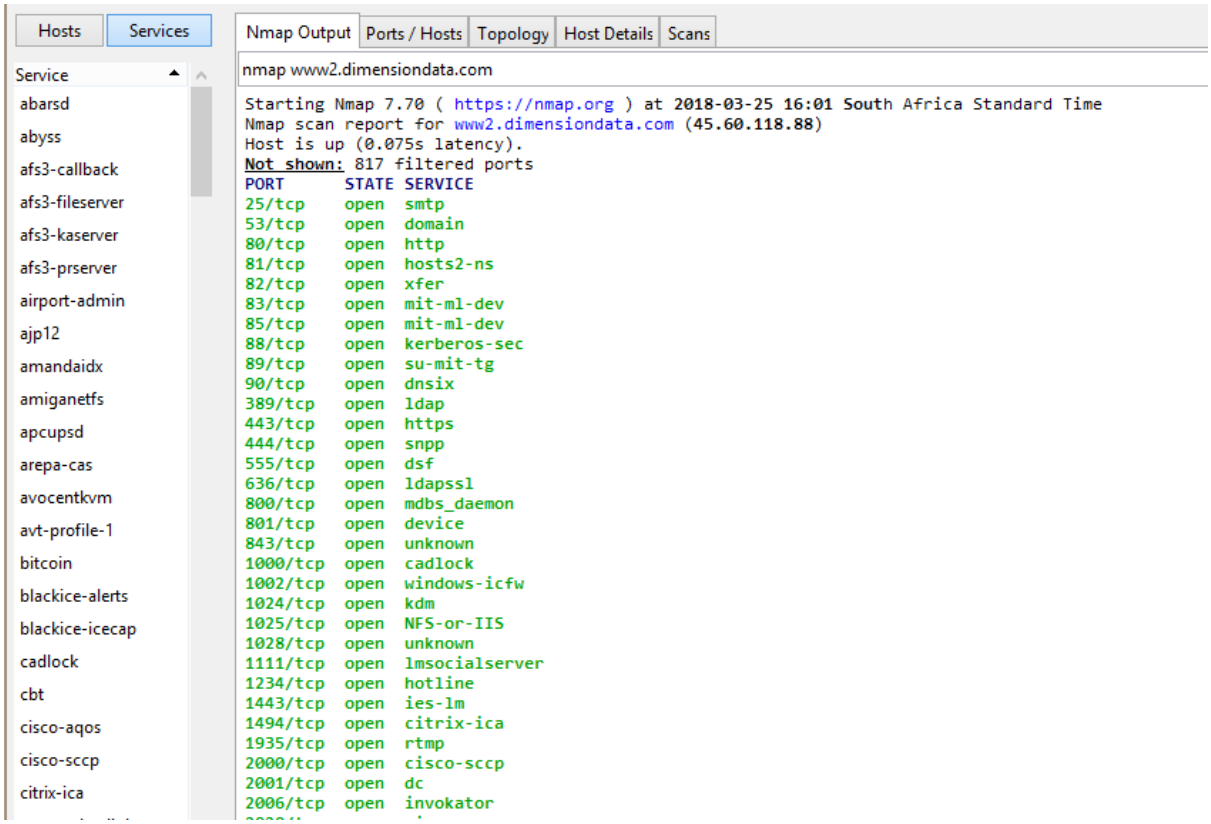
- www2.dimensiondata.com (45.60.118.88)
  - **Host Status**
    - State: up
    - Open ports: 1184
    - Filtered ports: 1814
    - Closed ports: 0
    - Scanned ports: 2000
    - Up time: 6241391
    - Last boot: Thu Jan 11 21:06:45 2018
  - **Addresses**
    - IPv4: 45.60.118.88
    - IPv6: Not available
    - MAC: Not available
  - **Hostnames**
    - Name - Type: www2.dimensiondata.com - user
  - **Operating System**
    - Name: Linux 3.18
    - Accuracy: 91%
    - **Ports used**
    - **OS Classes**
  - **TCP Sequence**
  - **IP ID Sequence**

nmap -T4 -A -v www2.dimensiondata.com

```
Discovered open port 6000/tcp on 45.60.118.88
Discovered open port 636/tcp on 45.60.118.88
Discovered open port 6510/tcp on 45.60.118.88
Discovered open port 5555/tcp on 45.60.118.88
Discovered open port 1000/tcp on 45.60.118.88
Discovered open port 8088/tcp on 45.60.118.88
Discovered open port 88/tcp on 45.60.118.88
Discovered open port 8010/tcp on 45.60.118.88
Discovered open port 55055/tcp on 45.60.118.88
Discovered open port 5998/tcp on 45.60.118.88
Discovered open port 8087/tcp on 45.60.118.88
Discovered open port 2000/tcp on 45.60.118.88
Discovered open port 9099/tcp on 45.60.118.88
Discovered open port 8042/tcp on 45.60.118.88
Discovered open port 3000/tcp on 45.60.118.88
Discovered open port 389/tcp on 45.60.118.88
Discovered open port 7999/tcp on 45.60.118.88
Discovered open port 9220/tcp on 45.60.118.88
Completed SYN Stealth Scan at 23:19, 7.65s elapsed (1000 total ports)
Initiating Service scan at 23:19
Scanning 179 services on www2.dimensiondata.com (45.60.118.88)
Service scan Timing: About 25.14% done; ETC: 23:21 (0:01:32 remaining)
Service scan Timing: About 55.74% done; ETC: 23:21 (0:00:49 remaining)
Completed Service scan at 23:22, 162.08s elapsed (183 services on 1 host)
Initiating OS detection (try #1) against www2.dimensiondata.com (45.60.118.88)
Retrying OS detection (try #2) against www2.dimensiondata.com (45.60.118.88)
Initiating Traceroute at 23:22
Completed Traceroute at 23:22, 3.02s elapsed
Initiating Parallel DNS resolution of 6 hosts. at 23:22
Completed Parallel DNS resolution of 6 hosts. at 23:22, 11.10s elapsed
NSE: Script scanning 45.60.118.88.
Initiating NSE at 23:22
Completed NSE at 23:34, 725.75s elapsed
Initiating NSE at 23:34
Completed NSE at 23:34, 5.57s elapsed
Nmap scan report for www2.dimensiondata.com (45.60.118.88)
```

nmap -T4 -A -v www2.dimensiondata.com

```
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-02-11T00:00:00
| Not valid after:  2019-05-01T12:00:00
| MD5:   c0c8 1a57 9380 8a1c 02d3 ab82 fcab 4ca8
|_SHA-1: 5d32 cfa7 879a 9690 7b09 2b5f df29 7616 c0e6 308c
|_ssl-date: TLS randomness does not represent time
| tls-nextprotoneg:
|_  http/1.1
1028/tcp  open  http        Incapsula CDN httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://www2.dimensiondata.com/
1111/tcp  open  ssl/http    Incapsula CDN httpd
| http-robots.txt: 5 disallowed entries
| /sitecore modules/ /sitecore_files/ /temp/ /upload/
|_*/registration
| ssl-cert: Subject: commonName=*.dimensiondata.com/organizationName=Dimension Data Holdings Plc/stateOrProvinceName=Gauteng/countryName=ZA
| Subject Alternative Name: DNS:*.dimensiondata.com, DNS:dimensiondata.com, DNS:www2.dimensiondata.com
| Issuer: commonName=DigiCert SHA2 High Assurance Server CA/organizationName=DigiCert Inc/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-02-11T00:00:00
| Not valid after:  2019-05-01T12:00:00
| MD5:   c0c8 1a57 9380 8a1c 02d3 ab82 fcab 4ca8
|_SHA-1: 5d32 cfa7 879a 9690 7b09 2b5f df29 7616 c0e6 308c
|_ssl-date: TLS randomness does not represent time
| tls-nextprotoneg:
|_  http/1.1
1234/tcp  open  http        Incapsula CDN httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://www2.dimensiondata.com/
1443/tcp  open  ssl/http    Incapsula CDN httpd
```


Hosts
Services
Service
abarsd
abyss
afs3-callback
afs3-fileserver
afs3-kaserver
afs3-prserver
airport-admin
ajp12
amandaidx
amiganetfs
apcupsd
arepa-cas
avocentkvm
avt-profile-1
bitcoin
blackice-alerts
blackice-icecap
cadlock
cbt
cisco-aqos
cisco-sccp
citrix-ica
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap www2.dimensiondata.com
Starting Nmap 7.70 (https://nmap.org) at 2018-03-25 16:01 South Africa Standard Time
Nmap scan report for www2.dimensiondata.com (45.60.118.88)
Host is up (0.075s latency).
Not shown: 817 filtered ports
PORT STATE SERVICE
25/tcp open smtp
53/tcp open domain
80/tcp open http
81/tcp open hosts2-ns
82/tcp open xfer
83/tcp open mit-ml-dev
85/tcp open mit-ml-dev
88/tcp open kerberos-sec
89/tcp open su-mit-tg
90/tcp open dnsix
389/tcp open ldap
443/tcp open https
444/tcp open snpp
555/tcp open dsf
636/tcp open ldapssl
800/tcp open mdbs_daemon
801/tcp open device
843/tcp open unknown
1000/tcp open cadlock
1002/tcp open windows-icfw
1024/tcp open kdm
1025/tcp open NFS-or-IIS
1028/tcp open unknown
1111/tcp open lmsocialserver
1234/tcp open hotline
1443/tcp open ies-lm
1494/tcp open citrix-ica
1935/tcp open rtmp
2000/tcp open cisco-sccp
2001/tcp open dc
2006/tcp open invokator

Profiler

This Recon-ng module performs website enumeration on a set of input names and attempts to find all associated online accounts.

Data found after using profiler

(Using Profiler Module)

Input Values:

David Danto, Julia Carlill, Matthias Kaden, Vincent Pisciotta, Avinash Vasudeva, Esger Musaerts

(E1.1)

Results:

username	resource	url	category	notes	module
Avinash Vasudeva	Slashdot	https://slashdot.org/~Avinash%20Vasudeva	news		profiler
Avinash Vasudeva	VideoLike	http://videolike.org/video/Avinash%20Vasudeva	video		profiler
David Danto	Internet Archive	http://archive.org/search.php?query=David%20Danto	search		profiler
David Danto	Slashdot	https://slashdot.org/~David%20Danto	news		profiler
David Danto	VideoLike	http://videolike.org/video/David%20Danto	video		profiler
David Danto	AdultFriendFinder	http://imcservices.passion.com/profile/David%20Danto	dating		profiler
Esger Mutsaerts	Slashdot	https://slashdot.org/~Esger%20Mutsaerts	news		profiler
Esger Mutsaerts	VideoLike	http://videolike.org/video/Esger%20Mutsaerts	video		profiler
Julie Carlill	Slashdot	https://slashdot.org/~Julie%20Carlill	news		profiler
Julie Carlill	VideoLike	http://videolike.org/video/Julie%20Carlill	video		profiler
Matthias Kaden	Internet Archive	http://archive.org/search.php?query=Matthias%20Kaden	search		profiler
Matthias Kaden	Slashdot	https://slashdot.org/~Matthias%20Kaden	news		profiler
Matthias Kaden	VideoLike	http://videolike.org/video/Matthias%20Kaden	video		profiler
Vincent Pisciotta	Slashdot	https://slashdot.org/~Vincent%20Pisciotta	news		profiler
Vincent Pisciotta	VideoLike	http://videolike.org/video/Vincent%20Pisciotta	video		profiler

Summary:

Recon-ng (Profiler Module) had gathered:

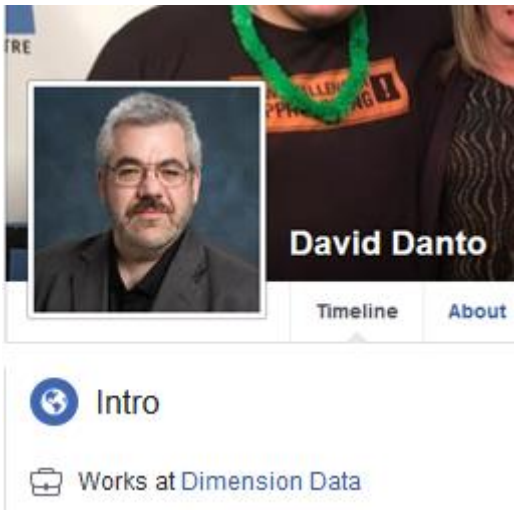
- 15 online accounts from 6 input employee names

How this gathered information can be used by the attacker

Attackers can now look to exploit employees by using their online accounts. From the results above, we see that David Danto has an AdultFriendFinder account. Attacker can attempt to catfish this employee into giving up more information or even his personal home address. Moreover, any material gained from this site can be used to blackmail employees into giving up sensitive company information. (E1)

An example of blackmail in this specific scenario is explained below. A simple Facebook search allowed us to find the employee and we were able to gain personal information about the employee. This allowed us to deduce that this employee has been married for the past 26 years to Helen Danto. We were also able to gain complete details of the employee's family. As a result, he could be targeted and blackmailed to give up company secrets due to proof of his activity on AdultFriendFinder. Screenshots of simple investigation are shown below.

Attacker can also perform identity theft and attempt to hack any of the victim's online accounts. Once hacked, the attacker can pose as the victim and trick their contacts into giving up sensitive information.



David Danto

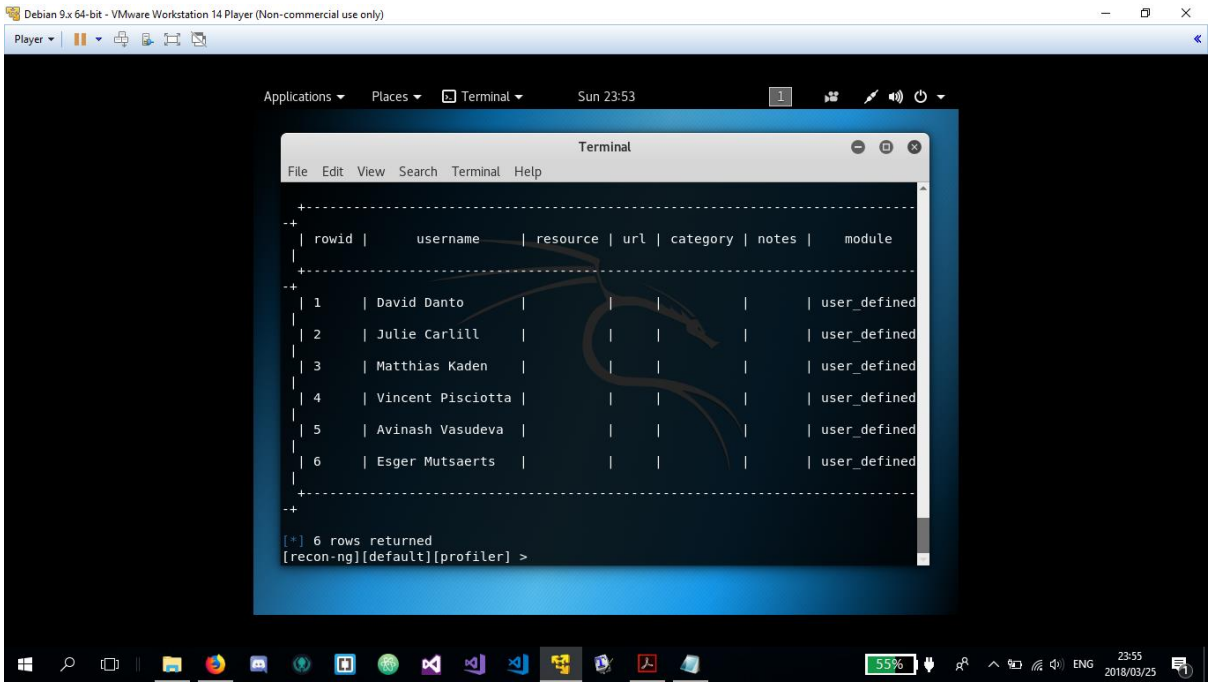
Helen Danto (Target's Wife)

Online References

(E1) http://time.com/money/3724976/bizarre-identity-theft/

Screenshots of Profiler

(E1.1)



Summary

Summary of tools used, and information gathered

Maltego	MX Servers for Domain (Servers which accept emails on behalf of domain)
	Domains sharing MX Records
	Name servers for Domain
	Domains sharing Name servers
	Netblocks of Dimension Data (IP Range assigned to domain)
	Netblocks to Autonomous System number
	Autonomous System number to owner
	Domain to DNS Names (Finds common DNS)
	WHOIS information of Domain
	Domain to Email Addresses (Staff email addresses)
	Email to Person (Acquires employees Name)
	Person to Email Address (Obtains all emails of specified person)
	Person to Person (People who communicated with each other over email)
	Person to Twitter Affiliation (Account instances of person)
	Person to Tweet (Posts made by person)
	Person to Twitter (People that the Person wrote tweets TO/People that wrote tweets TO the person)
The Harvester	91 Domain (Company) emails found
	12 Hosts (Inclusive of IP Address and Domain Name)
	4 Virtual Hosts (Inclusive of IP Address and Domain Name)
	57 Employee Name and Surname instances
Recon-Ng (XSS)	5 XSS Vulnerabilities
WHOIS	Domain Information
	Domain Name Servers (4)
	Registrant Contact
	Administrative Contact
	Technical Contact
DNS Dumpster	Domain Name Servers (4)
	MX Records (2)
	TXT Records (8)
	Host Records (+150)
FOCA	Network Information (Clients, OS, Software)
	Domain Information (Software, FingerprintBanner, IP Source...)
	Roles (HTTPS, HTTP, Fingerprinting HTTP)
	Vulnerabilities (Insecure methods, Roles in IP, Source in IP)
	Metadata (100 Docs, 71 PDF, 4 Users)
	Software Used (18 instances)
	Vulnerabilities within Software Used

NMap	Host and Services Information (Ports, Protocols, Port State)
	Ping scan Topology
	Network Topology (Connections between hosts in network)
	Host Details (1184 Open Ports, 1814 Filtered Ports, UpTime, LastBoot)
Recon-Ng (Profiler)	Input of 6 Employee Names Rendered 15 Online Associated Profiles
	6 Video Like Profiles
	6 Slashdot Profiles
	2 Internet Archive Profiles
	1 AdultFriendFinder Profile

Conclusion

By obtaining a large number of DNS hostnames, IP Addresses, Host servers, Reverse DNS etc. the attacker can further the depth of their reconnaissance by carrying out active techniques on this data. This will result in much more valuable data being extracted such as:

- Server traffic
- Server capacity
- Insecure protocols on the domain
- SQL Injections into form fields
- DDoS attacks on targeted servers

If attackers can identify weak links, such as SQL injections into form fields, they can gain access to much more valuable information and further construct a stronger attack and knowledge base.

Moreover, by actively analysing all the DNS data obtained, attackers can identify vulnerabilities and attempt to hijack the vulnerable DNS and redirect traffic, compromising the functioning of the company

By knowing the server capacity from active reconnaissance, DDOS attacks could be carried out to severely hinder the functioning of high priority servers.

User information was also gathered in this passive reconnaissance process which can be used to gain more knowledge about the people working in the organization and can be used for various social engineering attacks. From using just 6 employee names profiler managed to extract 15 online profiles. An attacker could potentially run profiles on all of the company's employees and begin to understand each employee more personally. This could result in the identification of weak individuals who could be targeted and blackmailed to give up company secrets.

We now also know the software used in the organization and their version number. An attacker could pose as the administrator of the software companies and send out emails requesting the software to be updated, along with fake links. This could easily result in employees installing malware, spyware, adware, backdoor software, rootkits etc.

By using all the information gathered by this passive reconnaissance process, the attacker is exposed to a lot of avenues on which they can further dive deep into using active reconnaissance or penetration testing methods.