**Question 1**

You have just joined a cyber security company and you are about to assist one of the engineers with the preparation of security audit for two of the company customers. It is just an initial phase and your customers haven't signed penetration testing authorisation form, NDA is not in place yet. However, you have been asked to establish what digital footprint, important to security audit, can be obtained using an open source intelligence technic.

 You are specifically asked to **do not engage your target objective in any active form** - any form of scanning, phishing, social engineering is outside of scope of the engagement at the moment.

 Your target objectives are:

<https://www.sossupport.net/>

<https://www.siskgroup.com/>

**Investigation Method:**

1)For DNS enumerations we are using **Nslookup**.

**Description**: This is the procedure to find out all the DNS (Domain Name server) servers and the records which are associated to the organization. Several details can be obtained such as, IP addresses, computer and usernames.

Under DNS enumerations I have explained various DNS records which has been used to gather all possible information about DNS servers.

We have used this method because it queries the specified server and obtains the records that are requested with the name of the domain we provide. It is feasible to obtain information about a website or an IP Address just by using DNS records. As the main use of this is to solve DNS related problems, I used this approach to obtain all the details related the IP address.

2)For Organization Domain details we are using **Whoislookup.**

**Description**: This is a record listing which recognizes the owner of the domain and the contact details of the owner of the domain. Regulation of domain name and its registration is done by ICANN (The Internet Corporation for Assigned names and Numbers). These details are useful as it contains all the information associated with group or a company that has a specific domain name.

I have used this method as it is helpful to obtain information about the registrar, Admin, Domain under one website, and important details such as name servers, the expiration date and the registered date of the domain can also be obtained.

**1)**[**https://www.sossupport.net/-**](https://www.sossupport.net/-)

**A close up of a sign

Description automatically generated**

SOS support was established in the year 2004, the author and CEO of the organization is Jason Kidman he was fond of PC’s and IT administrations from an early age. His skills with computer fixes, servers and other PC systems were good. Jason is an alumni of Goldman sachs 10,000 small business programs.

This company deals with Networking, Fiber, Advanced networks and phone cabling, Computer Repairs, Active Directory, DSL, Managed Services, Low Voltage Cabling, Domain Servers, VOIP, Cable, Remote Backups, Onsite Backups, Remote Support, Pro-Active Maintenance, Monthly Maintenance, Printers, Everything with I.T.

**LinkedIn Profile:** <https://www.linkedin.com/company/sos-support/>

**Website:** <http://www.sossupport.net>

**Industry:** Information Technology and Services

**Headquarters:** South Jordan, Utah

**Type:** Private

**Founded:** 2004

**Specialties:** Monthly Maintenance, Backups, Gateway Security, Repairs and Managed Services

**Domain Name:**  SOSSUPPORT.NET

**Registry Domain ID:** 122099776\_DOMAIN\_NET-VRSN

**Registry WHOIS Server:** whois.godaddy.com

**Registrar URL:** http://www.godaddy.com

**Updated Date**: 2019-06-10T14:24:18Z

**Creation Date:** 2004-06-09T15:14:49Z

**Registrar Registration Expiration Date:** 2020-06-09T15:14:49Z

**Admin Name:** Jason Kidman

**Admin Organization:** SOS Support

**Admin Street:** PO Box 1443

**Admin City:** Draper

**Admin State/Province:** Utah

**Admin Postal Code:** 84020

**Admin Country:** US

**Admin Phone**: +1.8015639700   
  
**Admin Fax**: +1.8015639700   
  
**Admin Email**: jason@sossupport.net

**Information about IP address ranges related to the organisation:**

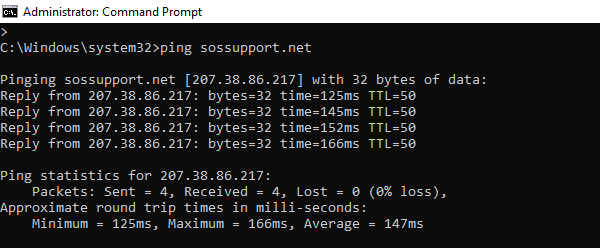
* Website:207.38.86.217
* IP addresses range from ‘207.38.80.0-207.38.95.255’
* ns31.domaincontrol.com:97.74.105.16
* ns32.domaincontrol.com:173.201.73.16
* sossupport-net.mail.protection.outlook.com: 104.47.44.36

**DNS Enumerations:**

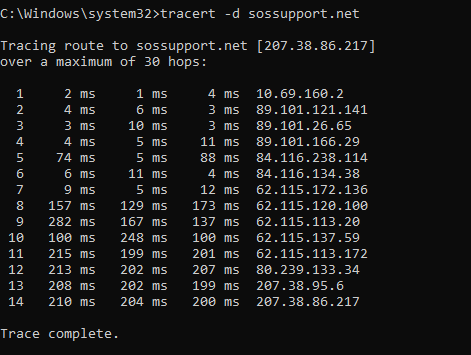
* **ping sossupport.net**- PING command is used to send data packets from one to another mentioned IP address on a network. Usually the ping command is used with an IP address or a URL. In the below screenshot, we use the ping command with the URL (sossupport.net) of the website, 4 packets are sent, and 4 packets are received with 0% loss. The four lines below the pinging shows the replies of every individual packet.

A drawing of a face

Description automatically generated



* **tracert -d sossupport.net-** Traceroute command is used to trace or show us the path of the data packet taken from host to destination. All the routers which are passed until it reaches the destination will be listed and even the ones which failed and discarded would be listed. Also, this tells you how long every ‘hop’ from router to router is taken in the below screenshot we are tracing the route to sossupport.net, IP address and the maximum number of hops before it times out.

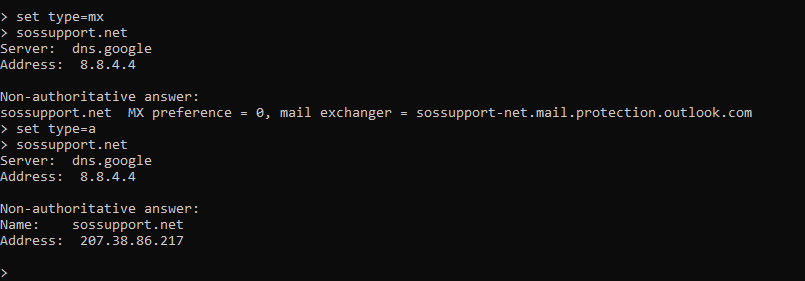


* **nslookup-** It is a very powerful network command line tool which can be used by many operating systems for querying DNS to access IP addresses or domain names. Under Nslookup there are various records which are written further.



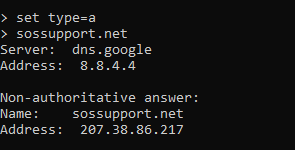
* **set type=mx**
* **sossupport.net**

MX Lookup is a tool which provides details about the MX records every domain contains or the ones which have added to the DNS records. Every email server first checks the MX record of the server of any email domain before sending them an email, if the MX record is not present then it fails to send. In the below screenshot we set the type to MX to get the mail exchange server.



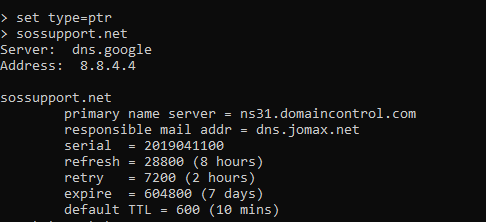
* **set type=a**
* **sossupport.net**

A is one of the lookup records which helps specifying the IP address of a computer. The A in A record stands for the address. These are one of the simplest records of the DNS records.



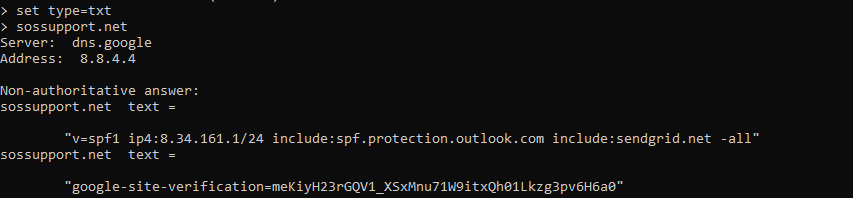
* **set type=ptr**
* **sossupport.net**

PTR is an opposite of A record. In simple words A record maps, the domain name to IP address however PTR maps IP address to a host name but these two records are not dependent on each other. This is useful for outgoing mail servers, this record is useful for protection against remote attackers and spammers who use false domain names to send spam. Mail providers such as Yahoo, Google do reverse lookup before they receive any emails.



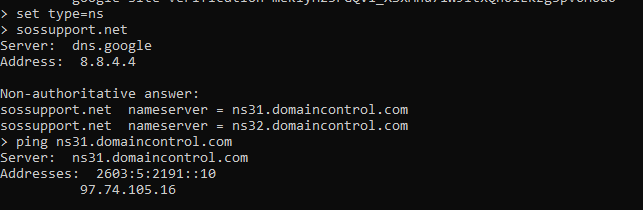
* **set type=txt**
* **sossupport.net**

This DNS type TXT record is kind of a resource record in the Domain name system which is used to provide the ability to associate arbitrary text with a host or other name which will be in a human readable format mostly about the server, network and other information   
We use this record to verify domain ownership and to ensure email security.

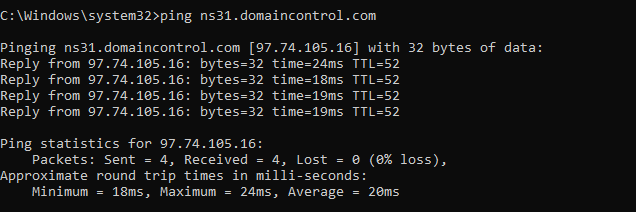


* **set type=ns**
* **sossupport.net**

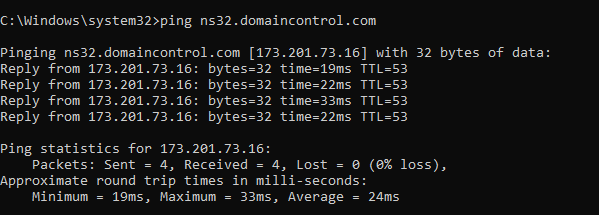
This type of DNS record specifies the name server for a named zone, this is needed to find the details about the name servers of the current DNS provider. This DNS is a database where the domain name (Sossupport.net) is converted into readable IP address and obtains the name servers.



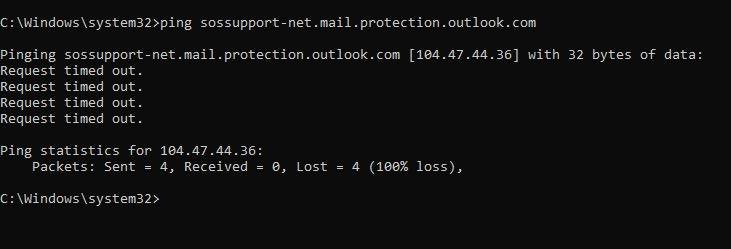
* **ping ns31.domaincontrol.com**



* **ping ns32.domaincontrol.com**

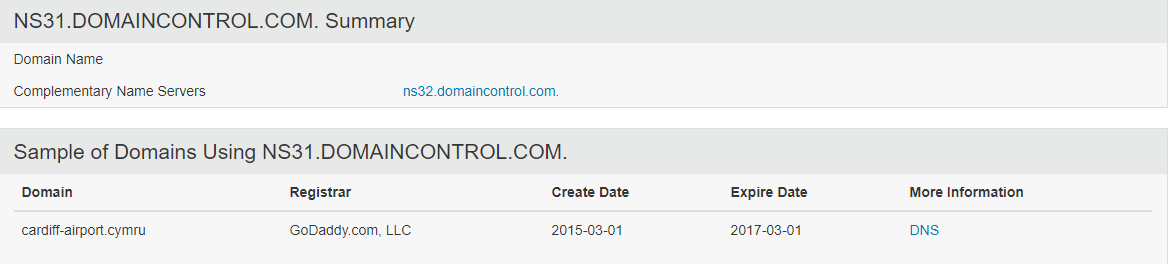


* **ping sossupport-net.mail.protection.outlook.com**

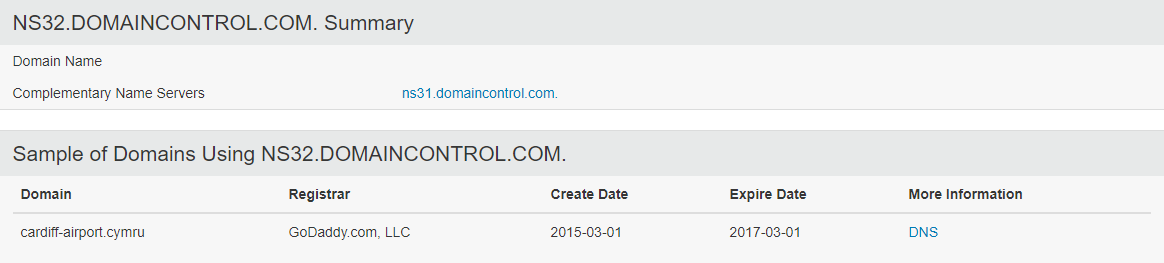


**Name Servers-**

* **ns31.domaincontrol.com-** This is the name server which has been hosted on www.godaddy.com, we ping this server to check if the IP address is within the range of the Sossupport.net organization IP address. In the screen shot mentioned above, the IP address for this is within the range (‘207.38.80.0-207.38.95.255’) .



* **ns32.domaincontrol.com-** This is the name server which has been hosted on www.godaddy.com, we ping this server to check is the IP address is within the range of the Sossupport.net organization IP address. In the screen shot mentioned above, the IP address for this is within the range (‘207.38.80.0-207.38.95.255’).



**LinkedIn-**

## Jason Kidman (Chief Executive Officer at SOSSupport)

South Jordan, Utah

<https://www.linkedin.com/in/jasonkidman/>

SOSSupport was founded by Jason Kidman in the year 2004. This company was one of the two IT support organizations recognized as Utah Top 100 fastest growing companies in both the years 2017&2018. It was also recognized by CRN as a “Next Gen 250” National Award winner in 2017&2018. As mentioned by the CEO of the company the company has transformed the business to “Effectively changed their business to satisfy the needs of rising advancements, for example, cloud computing, IoT, virtualization, mobility, business analytics and intelligence”

And the company has also received the Global Top 501 MSP award. This award was based on the quality of service provided by the company.

* **Larry Jones** (Networking and System Admin)Salt Lake City, Utah. <https://www.linkedin.com/in/larry-jones-2970a768/> Larry jones is an employee of SOS support, he is a Network and System Admin where he handles all the IT related issues like maintenance and implementation of all the security systems to identify the vulnerabilities and for the documentation of network design, to also help the clients of the company to improve their set up for the company which he has been working from 2017 to present.
* **Crystal Welch-Painter** (Service Delivery Manager)<https://www.linkedin.com/in/crystalpainter/> Sandy Utah Crystal is an employee of SOS support she is working with the company from 2016 , she joined the company as Executive Assistant Officer and has been working with this job profile for about 2 years 8 months and later she was promoted as Service Delivery manager who handles the client needs and oversees the delivery of the services within the context of the business.

**List of internal Email Addresses-**

|  |
| --- |
| 1. Jason Kidman (CEO)   +1 801 563 9700  [jason@sossupport.net](mailto:jason@sossupport.net)   1. L.Michelle Atkinson(VP of Operations)   [michelle@sossupport.net](mailto:michelle@sossupport.net)   1. Tatiana Rivers(Blog Contributor, Social Media Manager-ex employee)   [tatianarivers@sossupport.net](mailto:tatianarivers@sossupport.net)   1. James Fillmore(Chief Technology Officer)   [james@sossupport.net](mailto:james@sossupport.net)   1. Crystal Welchpainter(Service Delivery Manager)   [crystal@sossupport.net](mailto:crystal@sossupport.net)   1. Ryan Waddell   [ryan.waddell@sossupport.net](mailto:ryan.waddell@sossupport.net)   1. Aaron Butler(IT Technician and QA)   [Aaronbutler@sossupport.net](mailto:Aaronbutler@sossupport.net)  aaron@sossupport.net   1. Organization Email Addresses-   info@sossupport.net   1. [support@sossupport.net](mailto:support@sossupport.net). |

**Software used by the organization-**

* **Nginx-** This software was first created by Igor Sysoev and was first released publicly in 2004. Nginx can be deployed to access HTTP content(dynamic) using SCGI handlers on the network. It is also used as a load balancer for software.
* **Sos.guardian**
* **Office 365-** This is a platform under which many subscription services are offered by Microsoft for business, such as MS Word, MS Excel and many more.
* **G-Suite-** It Is a brand or a platform which comprises of Gmail,Calendar,Hangouts and Google+ for communication. It is a cloud computing branch which brings many tools together and many software products developed by Google.
* **Skype/Lync-**This is an application used for telecommunication through voice calls and video across the world. It is usually used in companies to conduct meetings and conferences with the clients.
* **Vipre-** Also known as Vipre security, this develops many cybersecurity products with development risk intellect solutions.

**Vulnerabilities present in Infrastructure-**

**These are the Vulnerabilities found in the IT infrastructure :**

* **CVE-2018-1115**
* **CVE-2019-9193**
* **CVE-2017-15906**
* **CVE-2016-5423**
* **CVE-2017-14798**
* **CVE-2016-5424**
* **CVE-2018-1058**
* **CVE-2017-12172**
* **CVE-2017-7484**
* **CVE-2017-7548**
* **CVE-2017-7486**
* **CVE-2016-0773**
* **CVE-2018-15919**
* **CVE-2017-7547**
* **CVE-2017-7546**
* **CVE-2017-15098**
* **CVE-2016-0766**
* **CVE-201-7485**

**2)** [**www.siskgroup.com**](http://www.siskgroup.com)

SISK group is into the construction company and it is a property which was founded in Cork in 1859. They started the business in Ireland, UK, Belgium, Poland. It is a 5th generation, 157-year-old business which runs in family. This company employs over 2000 people. The company was moved to Dublin in 1937, the main two divisions of the healthcare are

1)Sicon(construction)

2)SHG(SISK Healthcare Group).

**Website:** <http://www.siskgroup.com>

**Industry:** Construction

**Company size:** 1,001-5,000 employees

**Headquarters:** Clondalkin, Dublin 22

**Type:** Private

**Founded:** 1859

**Specialties:** Construction, Power Tools, and Distributor of Consumer Appliances & Property.

**LinkedIn**: <https://www.linkedin.com/company/sisk-group/people/>

**Registrar WHOIS Server:** whois.tucows.com

**Registrar URL:** <http://www.tucows.com>

**Updated Date:** 2019-01-15T13:10:33Z

**Creation Date:** 2003-02-26T15:06:42Z

**Registry Expiry Date:** 2020-02-26T15:06:42Z

**Registrar:** Tucows Domains Inc.

**Registrar IANA ID:** 69

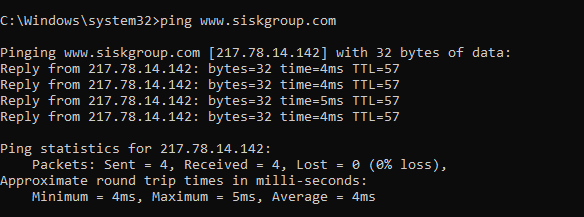
**Information about IP address ranges related to the organisation:**

* Website:217.78.14.142
* IP addresses range from ‘217.78.14.0-217.78.14.255’
* ns-cloud1.googledomains.com:216.239.32.106
* ns-cloud2.googledomains.com:216.239.34.106
* ns-cloud3.googledomains.com:216.239.36.106
* ns-cloud4.googledomains.com:216.239.38.106
* mail3.sisk.ie:82.198.141.134
* mail4.sisk.ie:93.94.119.196

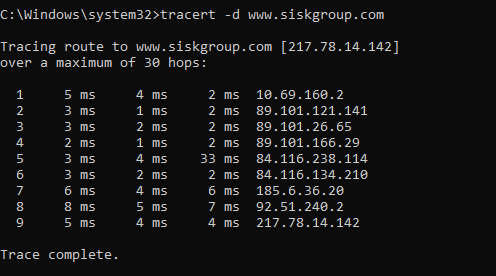
**Dns Enumerations:**

The explanation for the below mentioned records has been explained in the Question 1(www.sossupport.net).

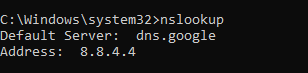
* **ping** [**www.siskgroup.com**](http://www.siskgroup.com)



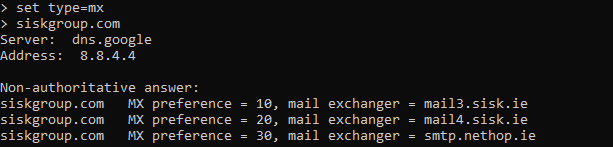
* **tracert -d siskgroup.com**



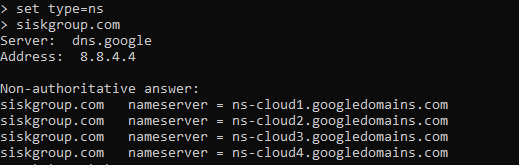
* **Nslookup**



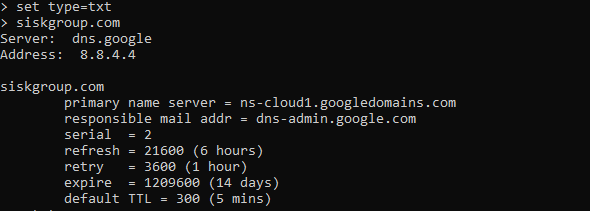
* **set type=mx**
* **siskgroup.com**



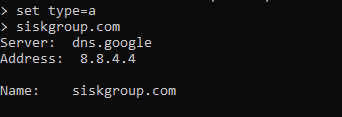
* **set type=ns**
* **siskgroup.com**



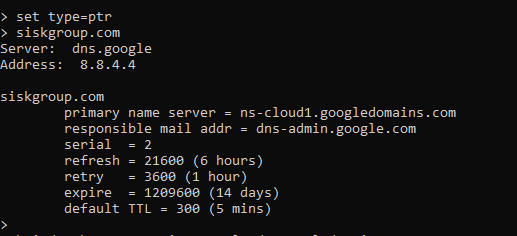
* **set type=txt**
* **siskgroup.com**



* **set type=a**
* **siskgroup.com**

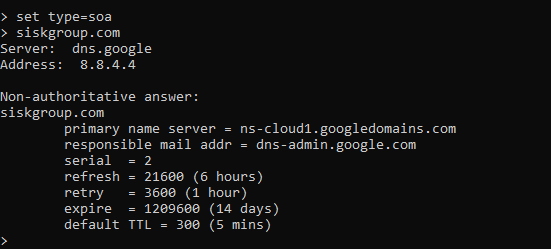


* **set type=ptr**
* **siskgroup.com**

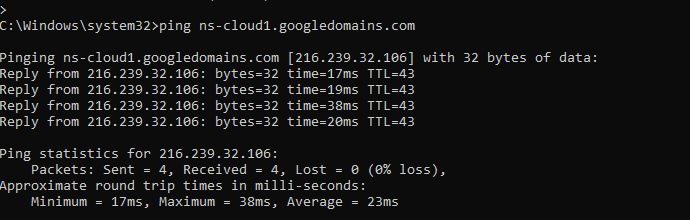


* **set type=soa**
* **siskgroup.com**

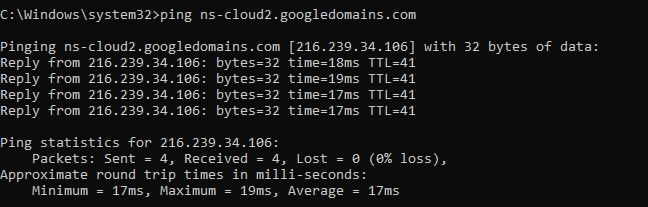
The server for SOA is- SOA Server: ns1.onp.io, this is also called start of authority record which contains administrative information about the server. Basically, the SOA contains the zone transfers between the clusters of DNS servers.



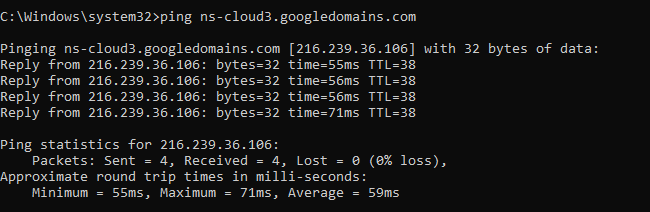
* **ping ns-cloud1.googledomains.com**



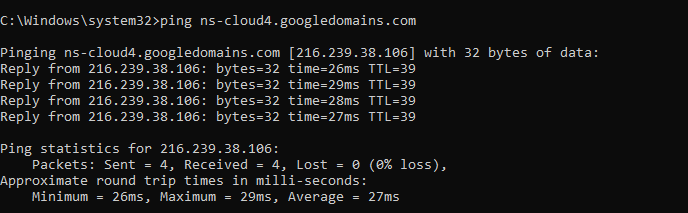
* **ping ns-cloud2.googledomains.com**



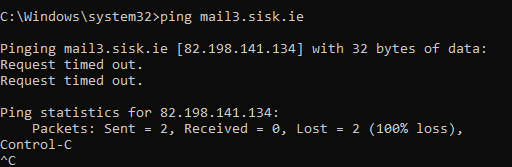
* **ping ns-cloud3.googledomains.com**



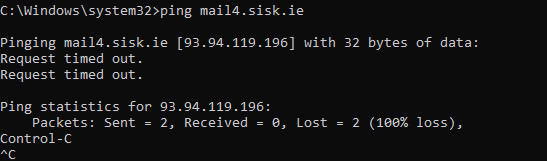
* **ping ns-cloud4.googledomains.com**



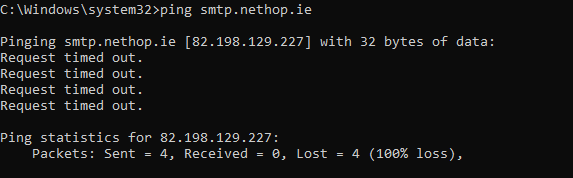
* **ping mail3.sisk.ie**



* **ping mail4.sisk.ie**



* **ping smtp.nethop.ie**



**Name Servers-**

* ns-cloud1.googledomains.com
* ns-cloud2.googledomains.com
* ns-cloud3.googledomains.com
* ns-cloud4.googledomains.com

**Internal Email Addresses-**

1.Richard Sisk(Director)

[richard@richardsiskproductions.com](mailto:richard@richardsiskproductions.com)

2. J.P Sisk(Director at SISK group, Head of Property)

[jp.sisk@siskgroup.com](mailto:jp.sisk@siskgroup.com)

3. Charlie Corcoran(IT Enterprise Architect)

[charlie.corcoran@siskgroup.com](mailto:charlie.corcoran@siskgroup.com)

[charles.corcoran@gmail.com](mailto:charles.corcoran@gmail.com)

4. Ken Kennedy(Head of Group Information technology)

[kenkennedy@siskgroup.com](mailto:kenkennedy@siskgroup.com)

[ken@siskgroup.com](mailto:ken@siskgroup.com)

5. Mike Peasland(Non-Executive Director)

[mikepeasland@siskgroup.com](mailto:mikepeasland@siskgroup.com)

[mike@siskgroup.com](mailto:mike@siskgroup.com)

6. Stephen parsons(Head of Information Security)

[stephen.parsons@siskgroup.com](mailto:stephen.parsons@siskgroup.com)

[steparsons06@googlemail.com](mailto:steparsons06@googlemail.com)

7. Tim Petch(Director Business Development)

[tim.petch88@gmail.com](mailto:tim.petch88@gmail.com)

[tim.petch@siskgroup.com](mailto:tim.petch@siskgroup.com)

8. Bevan Lloyd(Head of Group Finance)

[bevanlloyd@siskgroup.com](mailto:bevanlloyd@siskgroup.com)

9. Mark Honcoop(Head of IT Operations)

[mhoncoop@siskgroup.com](mailto:mhoncoop@siskgroup.com)

1. Andrew Bradley(Business Application Analyst)

[abradley@siskgroup.com](mailto:abradley@siskgroup.com)

1. William Parsons(Applications Support Analyst)

##### [wparsons@siskgroup.com](mailto:wparsons@siskgroup.com)

1. Colm Jeffrey(System Administrator)

[cjeffrey@siskgroup.com](mailto:cjeffrey@siskgroup.com)

1. John Gaffney(Commissioning and Qualification manager)

[jgaffney@siskgroup.com](mailto:jgaffney@siskgroup.com)

1. Paraic Curley(Senior Engineer)

[pcurley@siskgroup.com](mailto:pcurley@siskgroup.com)

**Software used by the organization:**

**Question 2**

One of the customers mentioned in question 1, have reported that they have discovered a suspicious activity detected on their firewall. They have asked you to obtain as much information as possible about attack source IP address. You have been asked to use Open Source Intelligence technics only. Any active engagement like scanning, or social engineering is outside of the scope now.

 Your target IPs are:

170.246.98.143

46.161.55.108

119.226.175.133

128.199.223.220

193.201.224.238

1)170.246.98.143

It is blacklisted by **RATS-Dyna** - On the list. Worst Offender Alert.

**This is a Worst Offender Alert** and this means that not only this IP address, but the whole class 'C' is also on the indicated SpamRats List. Usually this means the whole range has the same issue of naming conventions or no reverse DNS AND that many IP's from this Class C have been used in Spam Attacks, Dictionary attacks or other forms of attacks, as detected by Mail Servers in the Data Collection Grid. You will NOT be able to use the removal form to remove your IP Addresses. If you have recently been assigned the IP Addresses, or have changed what these IP Addresses are used for, you can use the contact form and ask for a reclassification, but you will have to provide full disclosure, including whois for the ip addresses, your affiliation with the company that owns them, and a description of what the IP's were previously used for, and what they will be used for, in order for a Spam Auditor to consider reclassification. Remember, the majority of the IP's in this space WERE detected as being involved in some form of attack or abusive behaviour, so you had better have a good reason to ask for removal, and you need to own or control the IP addresses, as evidenced by ARIN whois.

2) 46.161.55.108

It is blacklisted by **dnsbl.spfbl.net(DNSBL website)** and **dnsbl.justspam.org**.(Justspam.org)

**IP 46.161.55.108 is BLACKLISTED by dnsbl.justspam.org.**  
  
**You can delist this IP from dnsbl.justspam.org if following criterias are met:**

1. The IP 46.161.55.108 must not be listed by other well-known blacklists.
2. A valid non-generic and consistent PTR must be set.
3. You must be able to send an e-mail with an verifycode from 46.161.55.108 to delist.

There was no prior removal of this IP 46.161.55.108 from dnsbl.justspam.org within the last 30 days.

* rcode **FORMERR**: invalid query format;
* rcode **NXDOMAIN**: no abuse of this address has been reported;
* rcode **REFUSED**: exceeded the limit of queries;
* **127.0.0.2**: blacklisted due to bad reputation and confirmed by anonymous complaints;
* **127.0.0.3**: flagged due difficulty to identify the responsible for abuses or MTA not in compliance with RFC 5321 and
* **127.0.0.4**: could not identify an email service running at this address, it’s a NAT router, or because it’s residential connection.

Service’s zone: **dnsbl.spfbl.net**

It is noteworthy that, in the case of returning 127.0.0.3, we flag all IPs which we consider unsuitable for hosting mail transfer agents. In that case, the DNSBL does not only list systems that send spam, so it’s up to each administrator to decide how to use it. Making an analogy with the RFC Ignorant list (now [RFC Clueless](http://rfc-clueless.org/)), we also require a number of important settings, so we could be called the “SPF ignorant” or “[FCrDNS](https://spfbl.net/en/fcrdns/) ignorant” system. In addition, any machine with no purpose of email service is a potential vector of a hacker attack, so this flagging also prevents any possible attack rather than waiting for the first damage to blacklist the IP after the injury caused. More about our rules, in the our [delist page](https://spfbl.net/en/delist).

<https://www.blacklistmaster.com/check?t=128.199.223.220>

2)[www.siskgroup.com](http://www.siskgroup.com)

Hosting Provider

Dediserve

IP Address

170.246.98.143



Name Servers

ns-cloud1.googledomains.com

ns-cloud2.googledomains.com

Jump to last read

Let's chat on Hangouts!

[https://ie.godaddy.com/whois/results.aspx?domain=sossupport.net&recaptchaResponse=03AOLTBLR33628q\_dMeMhTMK6fJbqcypp3aeNY6mVx0eiS-Pgw-zl-7q8Cv-TJG0H4SaPtIq6rz9pfwXxW1es8BwgHM0d\_eRef5eZ4DCOabNOBmjLjc4ZOszy\_YMU4y37fUP2Aziw\_I\_deuMh6gW8Vr-vrsWrYRtHzlEU7rf4iTcC3Keveda7SYX4rvzq6wMoi7ID4m9PBK3WcQ\_MhbmYuCxfNdos5dbzXr4CXN\_8aZcC7faGFvqyAN1NTpw9rcsanW3ZVdaKts0RxYVMJWharQmeRArnD24Dziafm9ltWom-rbTC204vSvBXhq11s7mAwmlUZzA\_0EDYl&isc=cjc99com](https://www.google.com/url?q=https://ie.godaddy.com/whois/results.aspx?domain%3Dsossupport.net%26recaptchaResponse%3D03AOLTBLR33628q_dMeMhTMK6fJbqcypp3aeNY6mVx0eiS-Pgw-zl-7q8Cv-TJG0H4SaPtIq6rz9pfwXxW1es8BwgHM0d_eRef5eZ4DCOabNOBmjLjc4ZOszy_YMU4y37fUP2Aziw_I_deuMh6gW8Vr-vrsWrYRtHzlEU7rf4iTcC3Keveda7SYX4rvzq6wMoi7ID4m9PBK3WcQ_MhbmYuCxfNdos5dbzXr4CXN_8aZcC7faGFvqyAN1NTpw9rcsanW3ZVdaKts0RxYVMJWharQmeRArnD24Dziafm9ltWom-rbTC204vSvBXhq11s7mAwmlUZzA_0EDYl%26isc%3Dcjc99com&sa=D&source=hangouts&ust=1564058170935000&usg=AFQjCNGTOlHl9jDJRBiuPgjbyWNTomQx8A)

1:36 PM

nikhilaasnikar@gmail.com (nikhilaasnikar@gmail.com)

[https://www.similartech.com/dashboard/websites/analysis/url/sossupport.net](https://www.google.com/url?q=https://www.similartech.com/dashboard/websites/analysis/url/sossupport.net&sa=D&source=hangouts&ust=1564065471583000&usg=AFQjCNECyKkJVcPyGtGUMxx1pnCLEzl8Xg)

nikhilaasnikar@gmail.com • 3:37 PM

 1 new message

nikhilaasnikar@gmail.com (nikhilaasnikar@gmail.com)

·        [richard@richardsiskproductions.com](mailto:richard@richardsiskproductions.com) Director(Richard Sisk)  
·          [jp.sisk@siskgroup.com](mailto:jp.sisk@siskgroup.com)**20**(Director)  
·        [siskowen@siskgroup.com](mailto:siskowen@siskgroup.com)(Director)  
·          [mikepeasland@siskgroup.com](mailto:mikepeasland@siskgroup.com)(Non Executive Director)  
·          [mike@siskgroup.com](mailto:mike@siskgroup.com)**14**(Non Executive Director)  
·         [g.penny@sicon.ie](mailto:g.penny@sicon.ie)BEST PROFESSIONAL(Financial director) Gerard penny

170.246.98.143

http://www.spamrats.com- IP Blacklist

