

Timothy Kang  
Assignment #2- OSINT  
ITMS 543-02

**Target:** Sky Insurance  
**Domain Name:** skyinsurance.us

## Contents

<b>Command:</b> whois skyinsurance.us .....	1
<b>Command:</b> nslookup skyinsurance.us .....	3
<b>Command:</b> dnsenum -enum skyinsurance.us.....	4
<b>Command:</b> sublist3r -d skyinsurance.us .....	5
<b>Command:</b> curl -s -I 74.208.236.50 .....	5
<b>Site: Port Scan:</b> https://viewdns.info/portscan/?host=skyinsurance.us .....	6
<b>Site: Shodan:</b> https://www.shodan.io/host/74.208.236.50#81 .....	6
<b>Site: IP Location Finder:</b> https://viewdns.info/iplocation/?ip=74.208.236.50.....	8

## Command: whois skyinsurance.us

```
root@kali:~# whois skyinsurance.us
Domain Name: skyinsurance.us
Registry Domain ID: D48731928-US
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: whois.godaddy.com
Updated Date: 2018-03-02T13:42:25Z
Creation Date: 2015-02-25T18:00:32Z
Registry Expiry Date: 2019-02-24T23:59:59Z
Registrar: GoDaddy.com, Inc.
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Registry Registrant ID: C48731924-US
Registrant Name: Heidi Lee
Registrant Organization: Sky Insurance Service Inc
Registrant Street: 9171 N. Milwaukee Ave
Registrant Street:
Registrant Street:
Registrant City: Niles
Registrant State/Province: Illinois
Registrant Postal Code: 60714
Registrant Country: US
Registrant Phone: +1.8479651900
Registrant Phone Ext:
Registrant Fax: +1.8479651929
Registrant Fax Ext:
Registrant Email: skyins1@sky-ins.com
Registrant Application Purpose: P1
Registrant Nexus Category: C21
Registry Admin ID: C48731926-US
Admin Name: Heidi Lee
Admin Organization: Sky Insurance Service Inc
Admin Street: 9171 N. Milwaukee Ave
Admin Street:
```

```
Admin Street:
Admin City: Niles
Admin State/Province: Illinois
Admin Postal Code: 60714
Admin Country: US
Admin Phone: +1.8479651900
Admin Phone Ext:
Admin Fax: +1.8479651929
Admin Fax Ext:
Admin Email: skyins1@sky-ins.com
Admin Application Purpose: P1
Admin Nexus Category: C21
Registry Tech ID: C48731925-US
Tech Name: Heidi Lee
Tech Organization: Sky Insurance Service Inc
Tech Street: 9171 N. Milwaukee Ave
Tech Street:
Tech Street:
Tech City: Niles
Tech State/Province: Illinois
Tech Postal Code: 60714
Tech Country: US
Tech Phone: +1.8479651900
Tech Phone Ext:
Tech Fax: +1.8479651929
Tech Fax Ext:
Tech Email: skyins1@sky-ins.com
Tech Application Purpose: P1
Tech Nexus Category: C21
Name Server: ns-us.1and1-dns.us
Name Server: ns-us.1and1-dns.com
Name Server: ns-us.1and1-dns.de
Name Server: ns-us.1and1-dns.org
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2018-09-25T00:06:01Z <<<
```

For more information on Whois status codes, please visit <https://icann.org/epp>

```
NeuStar, Inc., the Registry Administrator for .US, has collected this information for the WHOIS database through a .US-Accredited Registrar. This information is provided to you for informational purposes only and is designed to assist persons in determining contents of a domain name registration record in the NeuStar registry database. NeuStar makes this information available to you "as is" and does not guarantee its accuracy. By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data: (1) to allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, electronic mail, or by telephone; (2) in contravention of any applicable data and privacy protection laws; or (3) to enable high volume, automated, electronic processes that apply to the registry (or its systems). Compilation, repackaging, dissemination, or other use of the WHOIS database in its entirety, or of a substantial portion thereof, is not allowed without NeuStar's prior written permission. NeuStar reserves the right to modify or change these conditions at any time without prior or subsequent notification of any kind. By executing this query, in any manner whatsoever, you agree to abide by these terms. NOTE: FAILURE TO LOCATE A RECORD IN THE WHOIS DATABASE IS NOT INDICATIVE OF THE AVAILABILITY OF A DOMAIN NAME. All domain names are subject to certain additional domain name registration rules. For details, please visit our site at www.whois.us.
```

### Information found (important is highlighted yellow):

Registrar: GoDaddy.com, Inc.

Registry Registrant, Admin, Tech ID: C48731925-US

Registrant, Admin, Tech Name: Heidi Lee

Registrant, Admin, Tech Organization: Sky Insurance Service Inc

Registrant, Admin, Tech Street: 9171 N. Milwaukee Ave

Registrant, Admin, Tech City: Niles

Registrant, Admin, Tech State/Province: Illinois

Registrant, Admin, Tech Postal Code: 60714

Registrant, Admin, Tech Phone: 1-847-965-1900

Registrant, Admin, Tech Fax: 1-847-965-1929

Registrant, Admin, Tech Email: skyins1@sky-ins.com

DNSSEC: unsigned

From this information, we can see a name from someone at Sky Insurance and an email from this company. No information is being hidden by the host server. The domain of the email address is clearly unique to the company and not something common like Gmail. Therefore, it is highly

likely that other employees will share this domain name. Since DNSSEC is unsigned, this could possibly be a vulnerability. Lastly, the ID might be a nice thing to know for possible future uses.

## Command: nslookup skyinsurance.us

```
root@kali:~# nslookup
> set type=any
> skyinsurance.us
Server:      8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
Name:   skyinsurance.us
Address: 74.208.236.50
skyinsurance.us nameserver = ns-us.land1-dns.org.
skyinsurance.us nameserver = ns-us.land1-dns.de.
skyinsurance.us nameserver = ns-us.land1-dns.us.
skyinsurance.us nameserver = ns-us.land1-dns.com.
skyinsurance.us
    origin = ns-us.land1-dns.com
    mail addr = hostmaster.land1.com
    serial = 2017010901
    refresh = 28800
    retry = 7200
    expire = 604800
    minimum = 300
skyinsurance.us mail exchanger = 10 mx00.land1.com.
skyinsurance.us mail exchanger = 10 mx01.land1.com.
Name:   skyinsurance.us
Address: 2607:f1c0:100f:f000::253

Authoritative answers can be found from:
>
```

### Information found (important is highlighted yellow):

Server: 8.8.8.8

Address: 74.208.236.50

Address: 2607:f1c0:100f:f000::253

Nameserver =

Mail exchanger =

The 8.8.8.8 shows that Google is the DNS server that is configured for this DNS lookup. The IPv4 and IPv6 addresses of the domain can be seen. The DNS nameserver and mail exchanger that is being used is displayed through this command.

## Command: dnsenum --enum skyinsurance.us

```
root@kali:~# dnsenum --enum skyinsurance.us
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4
Warning: can't load Net::Whois::IP module, whois queries disabled.
Warning: can't load WWW::Mechanize module, Google scraping disabled.

-----  skyinsurance.us  -----

Host's addresses:
-----
skyinsurance.us.                3470    IN      A       74.208.236.50

Name Servers:
-----
ns-us.land1-dns.us.            14092   IN      A       217.160.81.2
ns-us.land1-dns.de.            16703   IN      A       217.160.80.2
ns-us.land1-dns.com.           21071   IN      A       217.160.82.2
ns-us.land1-dns.org.           6999    IN      A       217.160.83.2

Mail (MX) Servers:
-----
mx01.land1.com.                5512    IN      A       74.208.5.21
mx00.land1.com.                6322    IN      A       74.208.5.3

Trying Zone Transfers and getting Bind Versions:
-----

Trying Zone Transfer for skyinsurance.us on ns-us.land1-dns.us ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for skyinsurance.us on ns-us.land1-dns.de ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for skyinsurance.us on ns-us.land1-dns.org ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for skyinsurance.us on ns-us.land1-dns.com ...
AXFR record query failed: NOTAUTH

brute force file not specified, bay.
root@kali:~# █
```

### Information found (important is highlighted yellow):

Host's addresses: 74.208.236.50

Name Servers addresses

Mail Servers addresses

Trying Zone Transfers: AXFR record query failed: NOTAUTH

This confirms the host address as 74.208.236.50. Similarly to nslookup, the name servers and mail servers are displayed but this time, the addresses to each server are given. Successful zone transfers can be a security risk so it is not surprising that it failed.

Command: sublist3r -d skyinsurance.us

```
root@kali:~# sublist3r -d skyinsurance.us

          SUBLIST3R
          # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for skyinsurance.us
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
root@kali:~#
```

Information found (important is highlighted yellow):

There are no subdomains

Using sublist3r shows that there are no subdomains for Sky Insurance.

Command: curl -s -I 74.208.236.50

```
root@kali:~# curl -s -I 74.208.236.50
HTTP/1.1 404 Not Found
Server: nginx
Date: Tue, 25 Sep 2018 01:48:07 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Keep-Alive: timeout=15

root@kali:~# curl -s -I 74.208.236.50 | grep "Server"
Server: nginx
root@kali:~#
```

Information found (important is highlighted yellow):

Server: nginx

Knowing nginx can be used with <https://www.cvedetails.com/> for known vulnerabilities.

Site: Port Scan: <https://viewdns.info/portscan/?host=skyinsurance.us>

Legend:



- port is OPEN



- port is CLOSED

PORT	Service	Status
21	FTP	✘
22	SSH	✘
23	Telnet	✘
25	SMTP	✘
53	DNS	✘
80	HTTP	✔
110	POP3	✘
139	NETBIOS	✘
143	IMAP	✘
443	HTTPS	✔
445	SMB	✘
1433	MSSQL	✘
1521	ORACLE	✘
3306	MySQL	✘
3389	Remote Desktop	✘

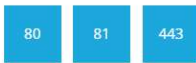
Passive port scan that shows that HTTP and HTTPS ports are open.

Site: Shodan: <https://www.shodan.io/host/74.208.236.50#81>

 **74.208.236.50** 74-208-236-50.elastic-ssl.ui-r.com

City	Wayne
Country	United States
Organization	1&1 Internet AG
ISP	1&1 Internet AG
Last Update	2018-09-23T12:23:50.088673
Hostnames	74-208-236-50.elastic-ssl.ui-r.com
ASN	AS8560

## Ports



## Services

**80**  
tcp  
http

Microsoft IIS httpd Version: 10.0

HTTP/1.1 200 OK  
Content-Type: text/html  
Content-Length: 358  
Connection: keep-alive  
Keep-Alive: timeout=15  
Cache-Control: private  
Server: Microsoft-IIS/10.0  
Set-Cookie: ASPSESSIONIDQABTBQTA=GFDJJPIDBPKAFNLDHNII00A0; path=/  
X-Powered-By: ASP.NET  
Date: Sun, 23 Sep 2018 12:23:48 GMT

**81**  
tcp  
xtremerat

HTTP/1.1 400 Bad Request\r\nServer: nginx\r\nDate: Sun, 23 Sep 2018 08:46:00 GMT\r\nContent-Type: text/html\r\nContent-Length: 166\r\nConnection: close\r\n\r\n<html>\r\n<head><title>400 Bad Request</title></head>\r\n<body bgcolor="white">\r\n<center><h1>400 Bad Request</h1></center>\r\n<hr><center>nginx</center>\r\n</body>\r\n</html>\r\n

**443**  
tcp  
https

nginx

HTTP/1.1 400 Bad Request  
Server: nginx  
Date: Sun, 23 Sep 2018 03:12:29 GMT  
Content-Type: text/html  
Content-Length: 264  
Connection: close

```
<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>nginx</center>
</body>
</html>
```

### Information found (important is highlighted yellow):

Organization and ISP: 1&1 Internet AG

ASN: AS8560

Hostnames: 74-208-236-50.elastic-ssl.ui-r.com

Ports: 80, 81, 443

Services: Microsoft IIS httpd Version: 10.0, nginx

Shows port 81 which was not visible on basic port scan. Knowing the services for each port could also be helpful in finding known vulnerabilities. The ASN (autonomous system number) is a unique number that identifies each network on the Internet so it may come in handy.

Site: IP Location Finder: <https://viewdns.info/iplocation/?ip=74.208.236.50>

IP Location Results for 74.208.236.50  
=====

City: Wayne  
Zip Code: 19087  
Region Code: PA  
Region Name: Pennsylvania  
Country Code: US  
Country Name: United States  
Latitude: 40.0548  
Longitude: -75.4083  
GMT Offset:  
DST Offset:

Shows precise location of the IP address which in this case is for 1&1 Internet AG.