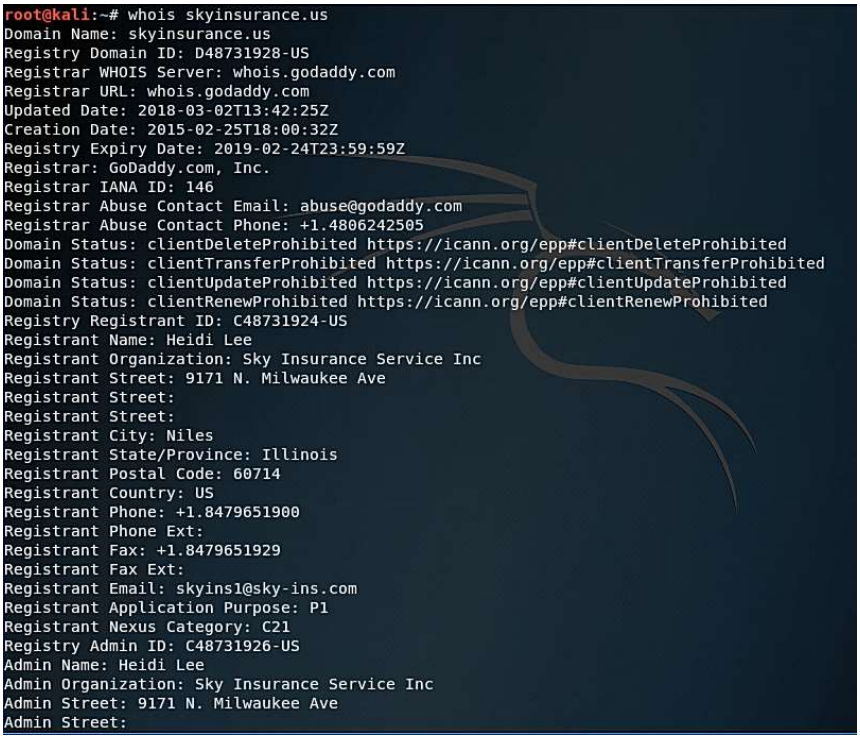
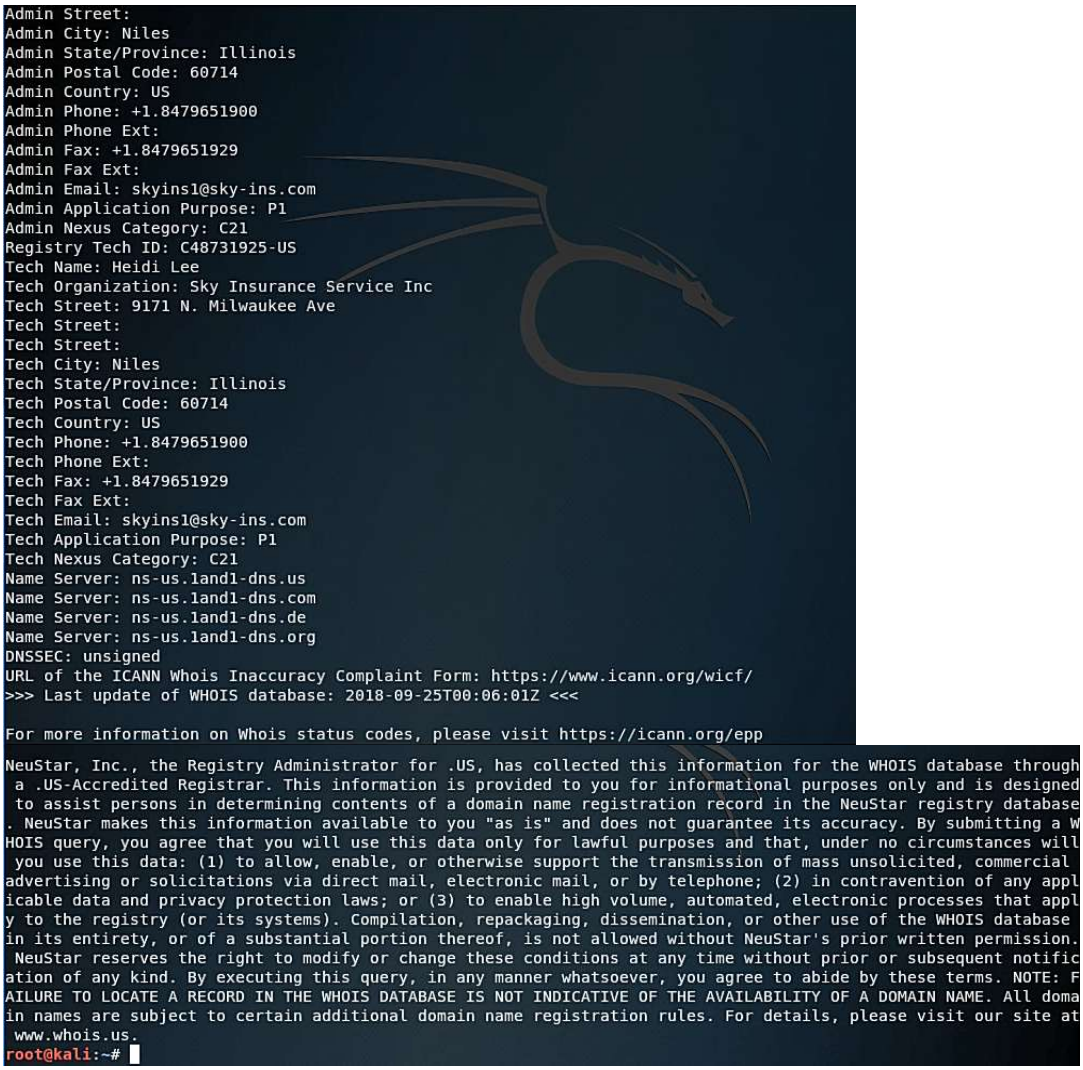
Timothy Kang
Assignment #2- OSINT
ITMS 543-02

Target: Sky Insurance
Domain Name: skyinsurance.us

Contents

Command: whois skyinsurance.us





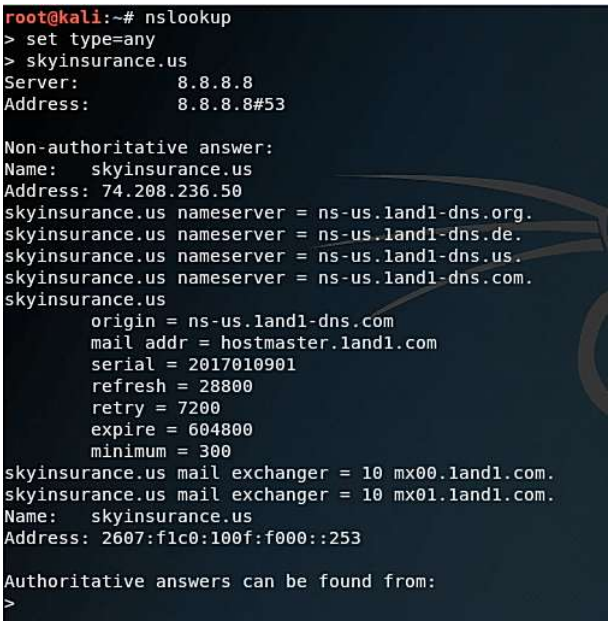
Information found (important is highlighted yellow):

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



Information found (important is highlighted yellow):

Server: 8.8.8.8

Address: 74.208.236.50

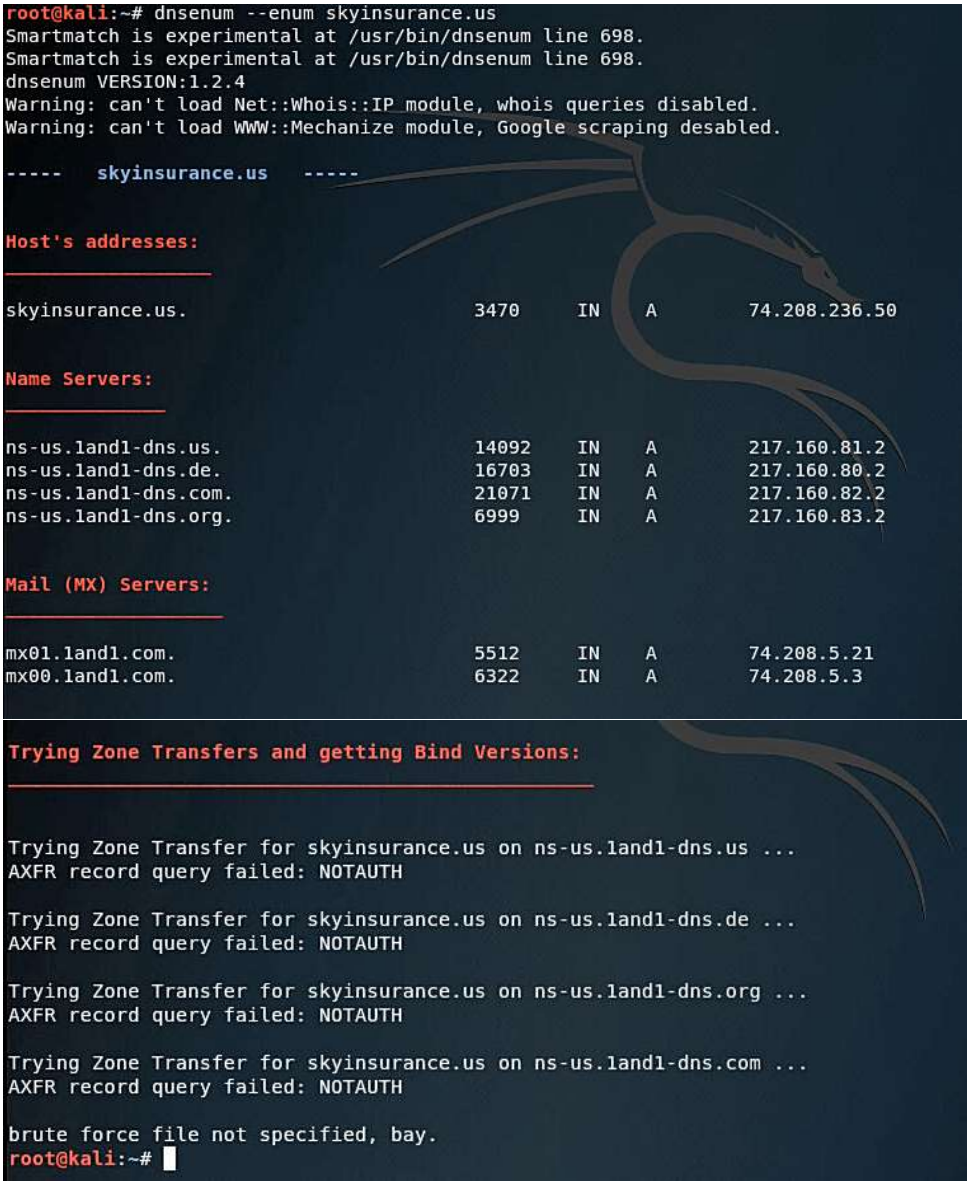
Address: 2607:f1c0:100f:f000::253

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



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

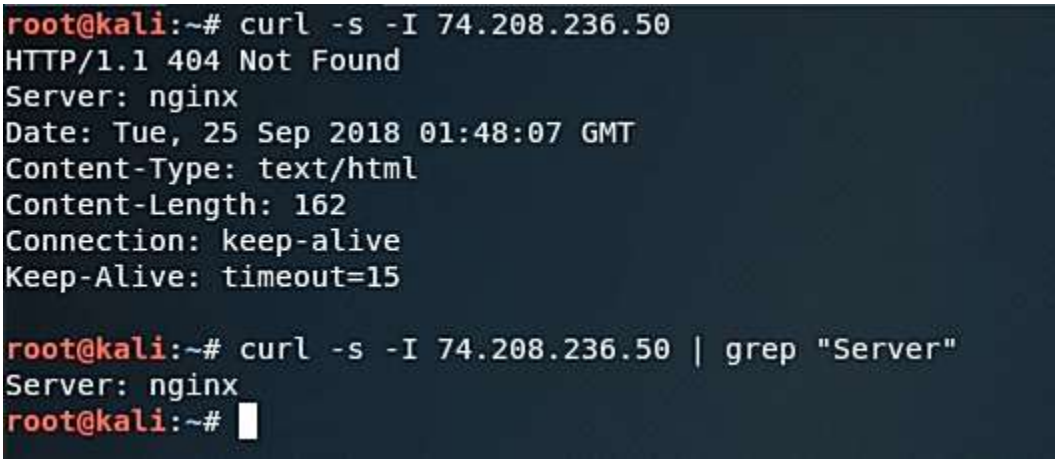
This confirms the host address as 74.208.236.50. Similarly to nslookup, the name servers and mail servers are displayed but this time, the addresses to each server are given. Successful zone transfers can be a security risk so it is not surprising that it failed.

Command: sublist3r -d skyinsurance.us

Information found (important is highlighted yellow):
There are no subdomains

Using sublist3r shows that are no subdomains for Sky Insurance.

Command: curl -s -I 74.208.236.50



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

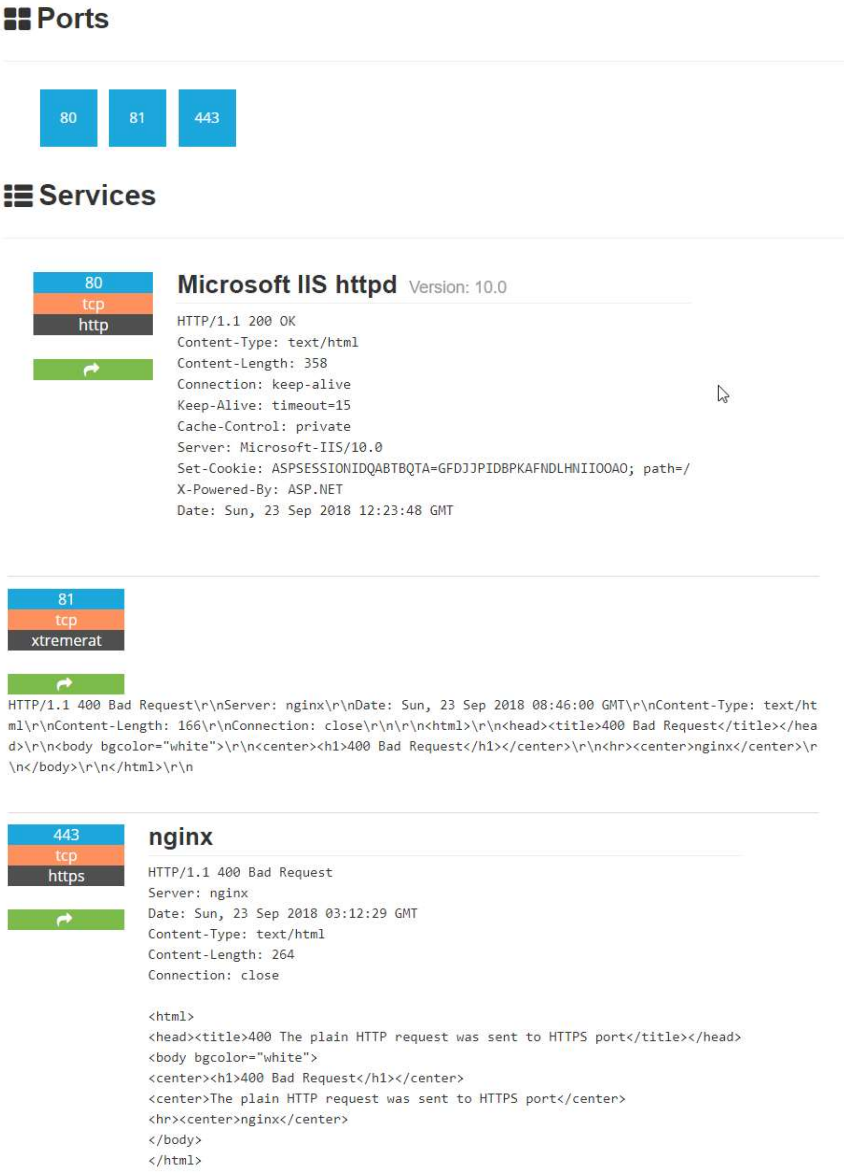
PORT	Service	Status
21	FTP	✗
22	SSH	✗
23	Telnet	✗
25	SMTP	✗
53	DNS	✗
80	HTTP	✓
110	POP3	✗
139	NETBIOS	✗
143	IMAP	✗
443	HTTPS	✓
445	SMB	✗
1433	MSSQL	✗
1521	ORACLE	✗
3306	MySQL	✗
3389	Remote Desktop	✗

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



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.