Lab 3 – Network Information Gathering

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Ian Coston

Date – 28st SEP 2023

Introduction

In this lab, get familiar with OSINT techniques, websites that can be utilized as well as automated tools which can be utilized to perform OSINT.

Pre-Lab

For this lab, you will require Kali Linux and Wireshark

Practical

1. OSINT Collection

1. Open a browser and go to: http://www.netcraft.com. In the "what's that site running box", type, www.umbc.edu. Note the IP Address, Operating System, and version of the Web server Software

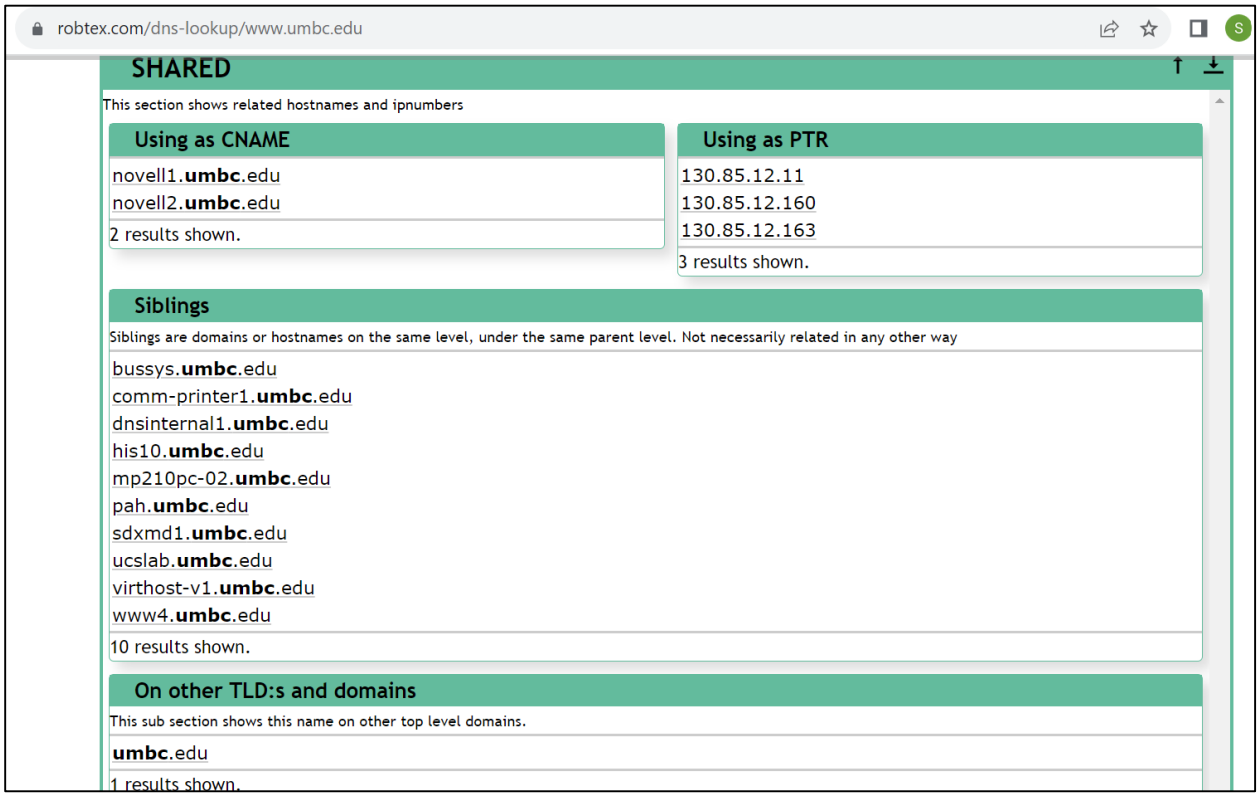
   IP Address - 23.185.0.4

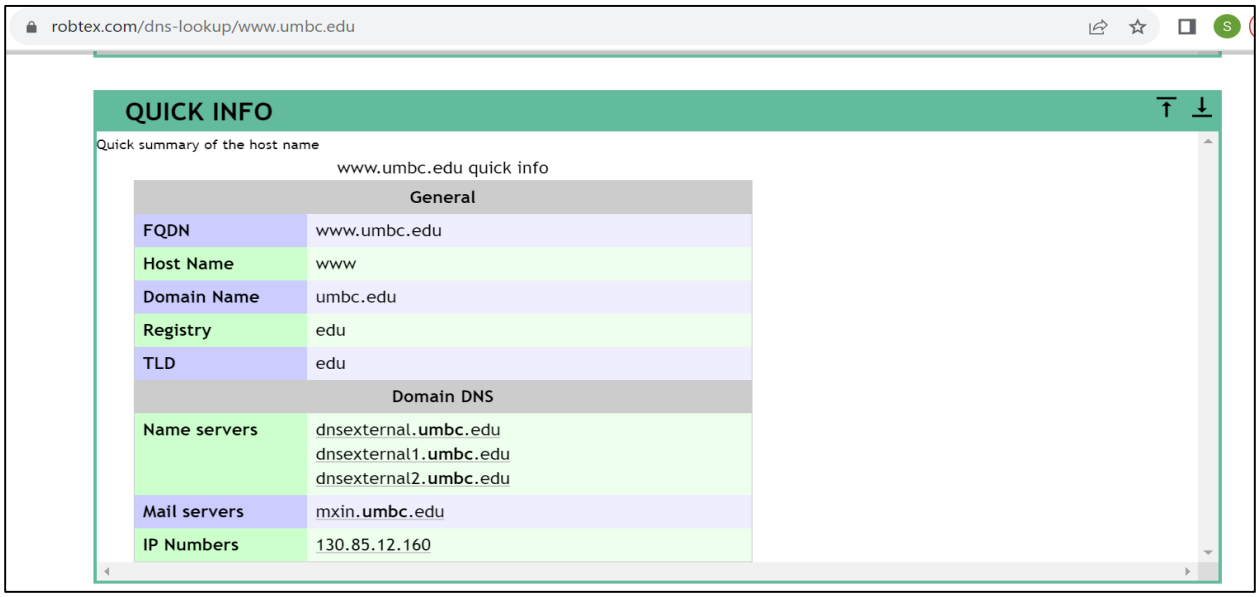
   IPv6 Address - 2620:12a:8001:0:0:0:0:4

Operating System – Linux

Webserver – nginx

2. Get DNS Records for UMBC by browsing http://www.robtex.com/dns/www.umbc.edu





3. Get the whois information by checking: http://www.whois.net/whois/umbc.edu or using http://centralops.net/co

whois.com/whois/umbc.edu

```
Domain Name: UMBC.EDU

Registrant:
        University of Maryland Baltimore County (UMBC-DOM
        UMBC Division of Information Technology
        1000 Hilltop Circle / Engineering 125
        Baltimore, MD 21250
        USA

Administrative Contact:
        John Suess
        UMBC Division of Information Technology
        Engineering 125
        1000 Hilltop Circle
        Baltimore, MD 21250
        USA
        +1.4104552582
        whois-admin@umbc.edu

Technical Contact:
        Ray Soellner
        UMBC Division of Information Technology
        Engineering 125
        1000 Hilltop Circle
        Baltimore, MD 21250
        USA
        +1.4104553256
        whois-technical@umbc.edu

Name Servers:
        DNSEXTERNAL1.UMBC.EDU
        DNSEXTERNAL.UMBC.EDU
        DNSEXTERNAL2.UMBC.EDU

Domain record activated:    12-Aug-1988
Domain record last updated: 11-Jan-2023
Domain expires:             31-Jul-2024
```

4. Google “UMBC network jobs” and look for details concerning technologies used within the college

After searching “UMBC network jobs” I saw seen few of the technologies used within the university such as AWS IaaS architecture, DevOps, Oracle Database, RDS/ EC2 instance, Docker, ECS environment, SQL, Azure, GCP, Informatica, weblogic, Tuxedo, Peoplesoft patches

5. Try using https://viewdns.info to gather the same information within their "One Stop Shopping" website

- I am able to find more details using viewdns.info such as below
  DNS nameservers - dnsexternal1.umbc.edu.
  dnsexternal.umbc.edu
  dnsexternal2.umbc.edu
- Primary nameserver: umbc10.umbc.edu.
- Hostmaster E-mail address: HOSTMASTER.UMBC.EDU
- MX record: mxin.umbc.edu
- WWW record: www.UMBC.EDU. A 23.185.0.4

viewdns.info/dnsreport/?domain=umbc.edu

Tryhackme | Blackboard Reports... | International Stude... | Hacking | CyberDaily News | general - WiCyS+IS... | apa format | Badges - Credly

DNS Report for umbc.edu
==========

Parent Nameserver Tests

Status	Test Case	Information
i	NS records listed at parent servers	Nameserver records returned by the parent servers are: dnsexternal1.umbc.edu. [130.85.1.9] [TTL=172800] dnsexternal.umbc.edu. [130.85.1.6] [TTL=172800] dnsexternal2.umbc.edu. [130.85.1.11] [TTL=172800] This information was kindly provided by i.edu-servers.net.
✓	Domain listed at parent servers	Good! The parent servers have information on your domain. Some other domains (like .co.us) do not have a DNS zone at the parent servers.
✓	NS records listed at parent servers	Good! The parent servers have your NS records listed. If they didn't, people wouldn't be able to find your domain!
✓	Parent servers return glue	Good! The TLD of your domain (edu) matches the TLD of your nameservers (edu) and hence the parent servers MUST return the IP (glue) for your NS records... AND THEY DO!
✓	A record for each NS at parent	Good! The parent servers have A records for each of your nameservers.

Local Nameserver Tests

Status	Test Case	Information
i	NS records at your local servers	NS records retrieved from your local nameservers were: dnsexternal.umbc.edu. [NO GLUE] [TTL=86400] dnsexternal1.umbc.edu. [NO GLUE] [TTL=86400]

viewdns.info/dnsreport/?domain=umbc.edu

Tryhackme | Blackboard Reports... | International Stude... | Hacking | CyberDaily News | general - WiCyS+IS... | apa format | Badges - Credly

✔	Glue at local nameservers	Good! Your local nameservers send the IP address (glue) along with your NS records.
✘	Same glue at local and parent servers	Oops! The IP addresses (GLUE) returned for your nameserver don't match! You should closely observe the nameserver details above and identify where the differences lie.
✔	Same NS records at each local nameserver	Good! All your local nameservers have identical NS records for your domain.
✔	Check that all nameservers respond	Good! All of your nameservers listed at the parent servers responded.
✔	Check all nameservers are valid	Good! All of your nameservers appear to be valid (e.g. are not IP addresses or partial domain names)
✔	Number of nameservers	Good! You have at least 2 nameservers. Whilst RFC218 section 2.5 specifies a minimum of 3, as long as you have 2 or more, you should be ok!
✔	Local nameservers answer authoritatively	Good! All your nameservers answer authoritatively for your domain.
✔	Missing NS records at parent servers	Good! The parent servers have all the nameservers listed for your domain as your local nameservers!
✔	Missing NS records at local servers	Good! Your local servers have all the nameservers listed for your domain that are listed at the parent servers!
✔	No CNAME records for domain	Good! No CNAME records are present for 'umbc.edu'. RFC1912 section 2.4 and RFC2181 section 10.3 state that there should be no CNAME records if any other records are present for a given domain.

Start of Authority (SOA) Tests

Status	Test Case	Information
ℹ	SOA Record	Your Start of Authority (SOA) record is: Primary nameserver: umbc10.umbc.edu. Hostmaster E-mail address: HOSTMASTER.UMBC.EDU. Serial number: 2010200824 Refresh: 10800 Retry: 1800 Expire: 3600000 Minimum TTL: 21700

Status	Test Case	Information
ℹ	MX Records	Your Mail eXchanger (MX) records are: 10 mxin.umbc.edu. [TTL=86400]
✔	MX records have reverse DNS entries	Good! All your MX IP addresses have reverse DNS entries. The reverse entries returned were: 177.12.85.130.in-addr.arpa <--> mxin.umbc.edu.

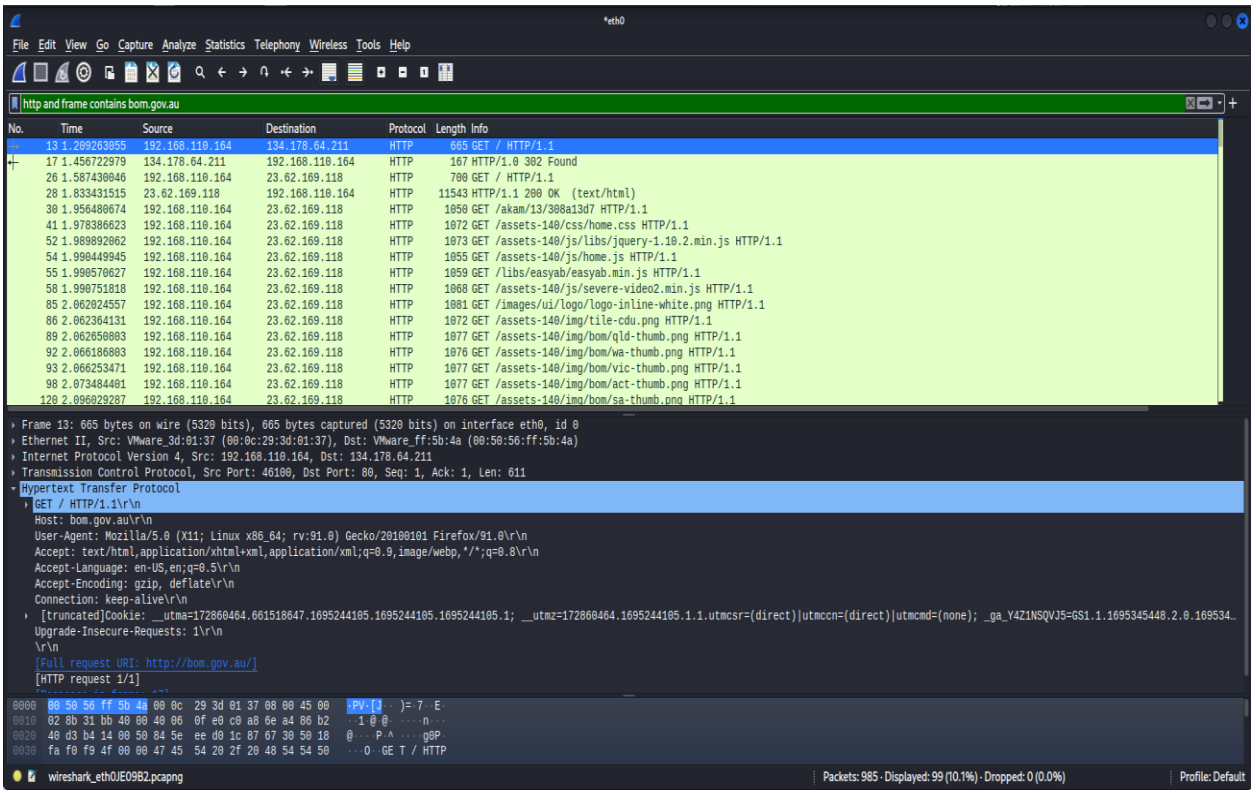
WWW Record Tests

Status	Test Case	Information
ℹ	WWW record	www.umbc.edu A records are: www.UMBC.EDU. A 23.185.0.4 [TTL=86400]

2. Information Collection by visiting a site

After comparing result of both sites ‘bom.gov.au’ and ‘lairnet.academy’ respectively.

After analyzing both requests, I have found that in the first site pcap details, cookies are getting sent with its request which is showing session-based interaction. Server mention is BigIP. However, in the second request cookies are not getting sent. But, in the second request, many details are there like it is accepting files such as Etage and some of the encrypted contents are there. Server mention is eCorp Gibson.



Wireshark · Follow TCP Stream (tcp.stream eq 1) · eth0

```
GET / HTTP/1.1
Host: bom.gov.au
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: __utma=172860464.661518647.1695244105.1695244105.1695244105.1; __utmz=172860464.1695244105.1.1.utmcsr=(direct)|utmccn=(direct)|
utmcmd=(none); _ga_Y4Z1NSQVJ5=GS1.1.1695345448.2.0.1695345448.0.0.0; _ga=GA1.1.769348929.1695244107;
_ga_MQWM1SE6FW=GS1.1.1695244112.1.0.1695244118.0.0.0
Upgrade-Insecure-Requests: 1

HTTP/1.0 302 Found
Location: http://www.bom.gov.au
Server: BigIP
Connection: Keep-Alive
Content-Length: 0
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (724 bytes) | Show data as ASCII | Stream 1

Find: | Find Next

Filter Out This Stream | Print | Save as… | Back | Close | Help

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http and frame contains lairnet.academy

No.	Time	Source	Destination	Protocol	Length	Info
110	20.621491185	23.96.39.152	192.168.110.164	HTTP	2292	HTTP/1.1 200 OK
166	20.952227324	192.168.110.164	142.251.167.94	OCSP	470	Request
168	20.979963218	142.251.167.94	192.168.110.164	OCSP	755	Response
170	20.989299731	192.168.110.164	142.251.167.94	OCSP	470	Request
177	21.010842309	192.168.110.164	142.251.167.94	OCSP	470	Request
179	21.017273759	142.251.167.94	192.168.110.164	OCSP	755	Response
196	21.037289913	192.168.110.164	23.96.39.152	HTTP	349	GET /assets/images/favicon.png HTTP/1.1
206	21.048263989	142.251.167.94	192.168.110.164	OCSP	755	Response
220	21.054636240	23.96.39.152	192.168.110.164	HTTP	875	HTTP/1.1 200 OK (PNG)

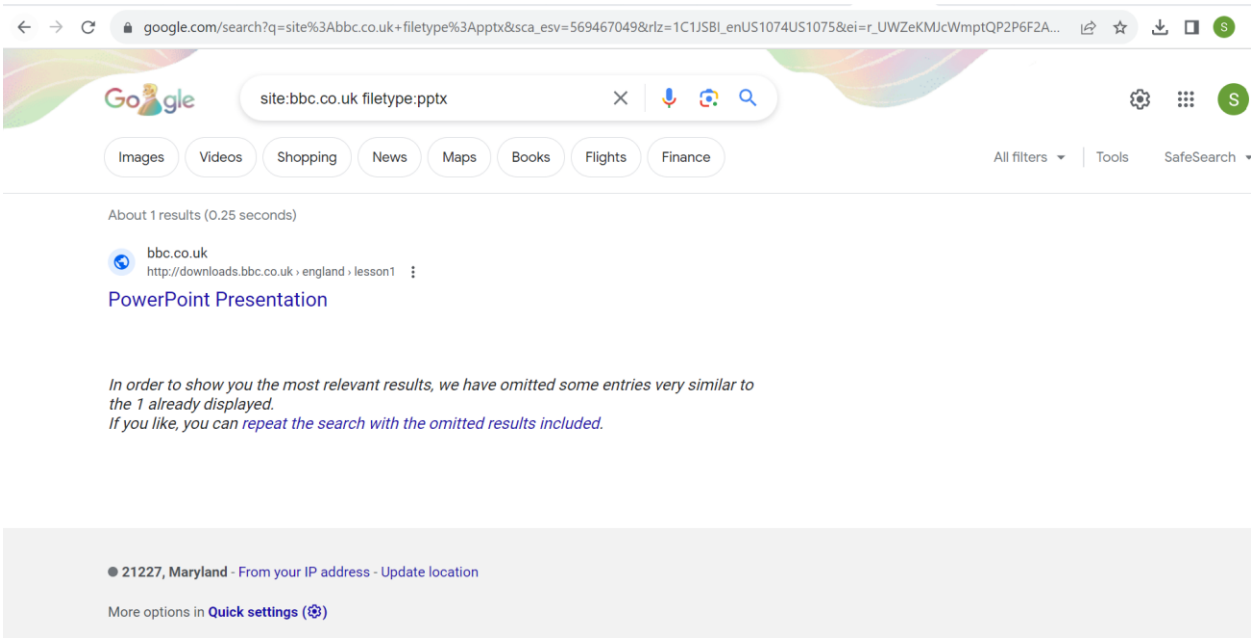
```
▸ Frame 20: 380 bytes on wire (3040 bits), 380 bytes captured (3040 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_3d:01:37 (00:0c:29:3d:01:37), Dst: VMware_ff:5b:4a (00:50:56:ff:5b:4a)
▸ Internet Protocol Version 4, Src: 192.168.110.164, Dst: 23.96.39.152
▸ Transmission Control Protocol, Src Port: 35666, Dst Port: 80, Seq: 1, Ack: 1, Len: 326
▾ Hypertext Transfer Protocol
  ▾ GET / HTTP/1.1\r\n
    Host: lairnet.academy\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://lairnet.academy/]
    [HTTP request 1/3]
    [Response in frame: 24]
    [Next request in frame: 28]

0000  00 50 56 ff 5b 4a 00 0c  29 3d 01 37 08 00 45 00   PV·[J·· )=·7··E·
0010  01 6e c5 0e 40 00 40 06  06 37 c0 a8 6e a4 17 60   ·n··@·@· ·7··n··`
0020  27 98 8b 52 00 50 cb b6  db 8c 4e ef 0b c4 50 18   '··R·P·· ··N···P·
0030  fa f0 6f a5 00 00 47 45  54 20 2f 20 48 54 54 50   ··o···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 6c 61 69 72   /1.1··Ho st: lair
0050  6e 65 74 2e 61 63 61 64  65 6d 79 0d 0a 55 73 65   net.acad emy··Use
0060  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
0070  2f 35 2e 30 20 28 58 31  31 3b 20 4c 69 6e 75 78   /5.0 (X1 1; Linux
0080  20 78 38 36 5f 36 34 3b  20 72 76 3a 39 31 2e 30    x86_64;  rv:91.0
0090  29 20 47 65 63 6b 6f 2f  32 30 31 30 30 31 30 31   ) Gecko/ 20100101
00a0  20 46 69 72 65 66 6f 78  2f 39 31 2e 30 0d 0a 41    Firefox /91.0··A
```

wireshark_eth0HXZAC2.pcapng | Packets: 317 · Displayed: 22 (6.9%) | Profile: Default

3. Information Collection via Search Engine

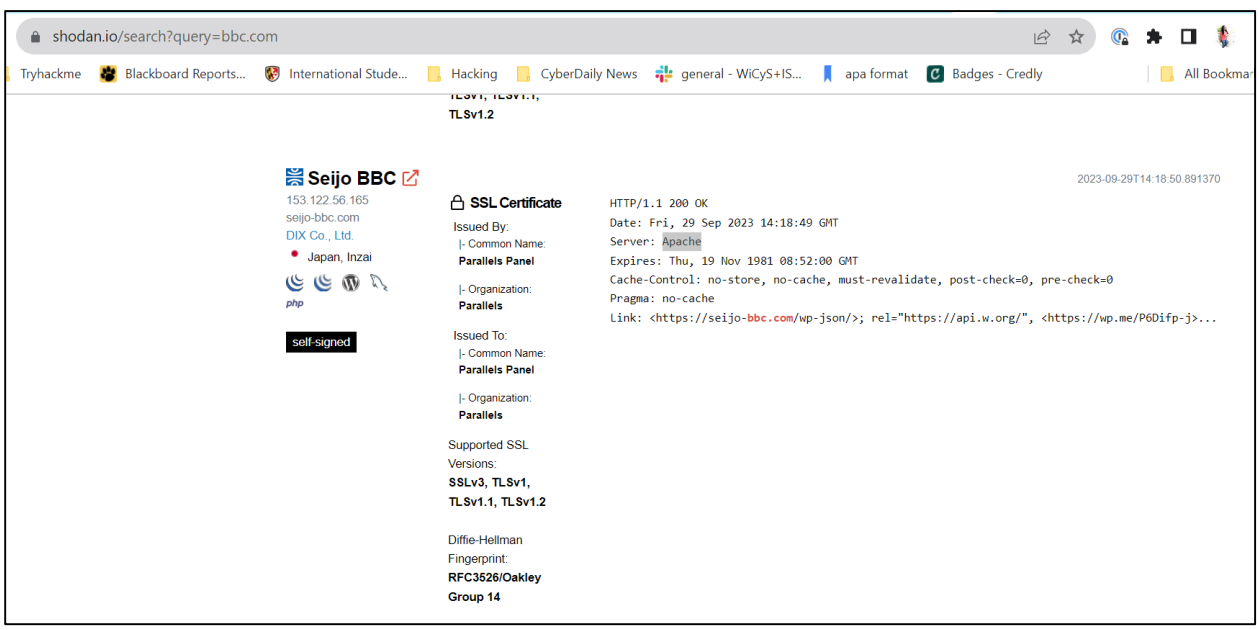
1. Perform a Google Hacking Search for all PowerPoint Documents (.pptx extension). Narrow that search to a specific domain or site

- To perform this task I am using Google Dorking and I am using filetype: pptx to search .pptx extension files.



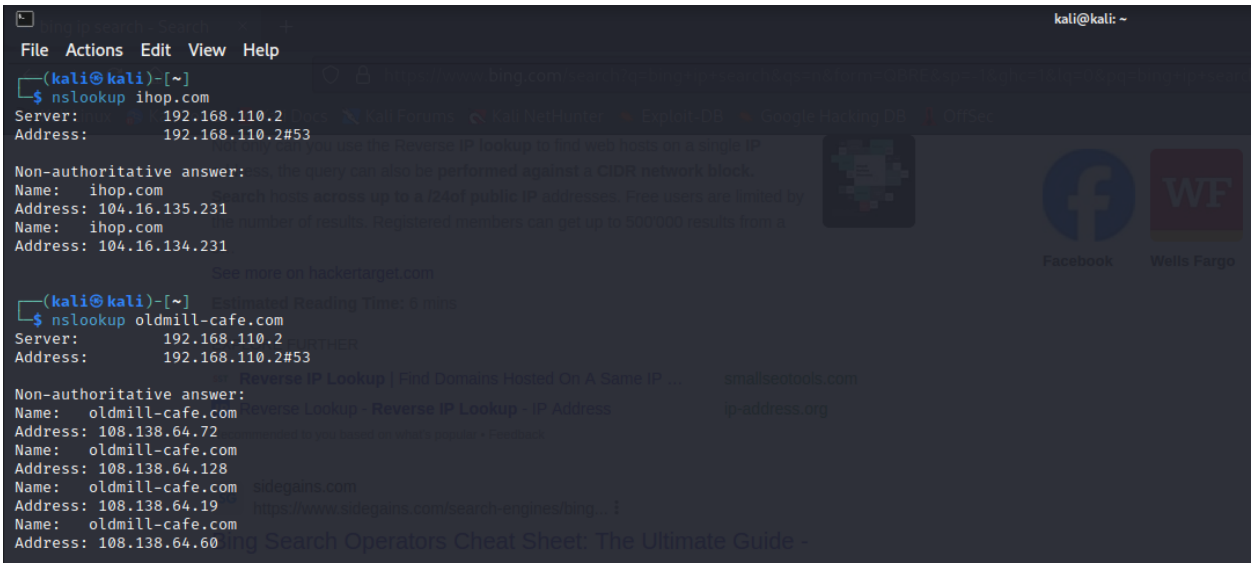
2. Perform a Shodan search for Apache webservers. Find any with an HTTP 200 OK response

- I am able to find one apache server with HTTP 200 ok response



3. Perform a Bing IP search on a small business website such as shops in old Ellicott City, mainstreet Catonsville, a local coffee shop (not Starbucks), etc.

- I couldn't IP search on Bing for this website. However, I did nslookup to check IP address of the website from the address mentioned.



4. Automated Tools for Information Gathering

1. Using The Harvester, search for all email addresses from the umbc.edu domain from google and linkedin

- I am using the theHarvester command line tool to search for all email addresses from umbc.edu from google and linkedin. Below is the command where –d is used to specify domain name and –b is used to specify

  Command : theHarvester -d umbc.edu -b google, linkedin

  I have found below 9 email addresses using above command

  aok@umbc.edu

  blackwel@umbc.edu

  blaney@umbc.edu

bowen@umbc.edu

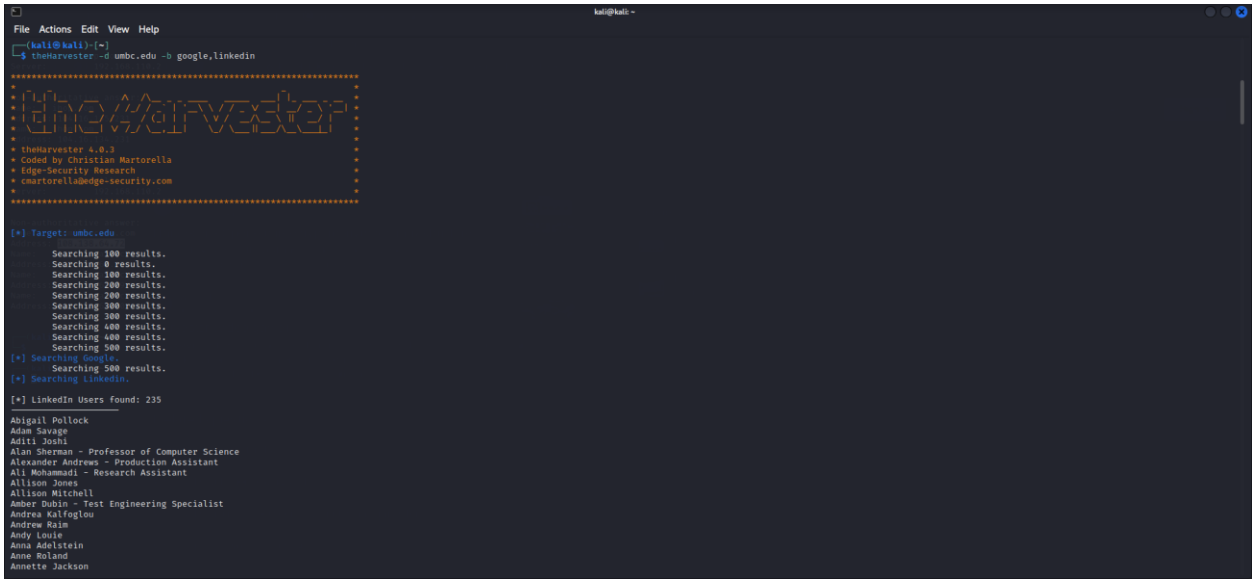
disher@umbc.edu

isss@umbc.edu

sunildasgupta@umbc.edu

x22bowen@umbc.edu

x22sunildasgupta@umbc.edu



2. Using Recon-ng, search for all points of contact for a large company (defense contractors work well), by loading the /recon/domains-contacts/whois_pocs and setting the source to the domain name of your target.

- To perform this task first I have started Recon-ng and then install modules and installed 'whois_pocs' using the command 'marketplace install recon/domains-contacts/whois_pocs'

```
Interfaces with installed modules
Usage: modules <load|reload|search> [...]

[recon-ng][default] > marketplace
Interfaces with the module marketplace
Usage: marketplace <info|install|refresh|remove|search> [...]

[recon-ng][default] > marketplace search whois
[*] Searching module index for 'whois' ...
+------------------------------------------------------------------------------------------+
|                Path                      | Version |     Status    |  Updated   | D | K |
+------------------------------------------------------------------------------------------+
| recon/companies-domains/viewdns_reverse_whois | 1.1     | not installed | 2021-08-24 |   |   |
| recon/companies-multi/whois_miner             | 1.1     | not installed | 2019-10-15 |   |   |
| recon/domains-companies/whoxy_whois           | 1.1     | not installed | 2020-06-24 |   | * |
| recon/domains-contacts/whois_pocs             | 1.0     | not installed | 2019-06-24 |   |   |
| recon/netblocks-companies/whois_orgs          | 1.0     | not installed | 2019-06-24 |   |   |
+------------------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][default] > marketplace install recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules ...
```

Now load the 'whois_pocs' using command – 'modules load recon/domains-contacts/whois_pocs'.

Set the domain name as a source using the command – 'options set SOURCE <domain_name>'. Once the SOURCE is set use the 'run' command.

lockheedmartin.com domain hasn't contain any contact details.

```
[recon-ng][default] > modules load recon/domains-contacts/whois_pocs
[recon-ng][default][whois_pocs] > info

      Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
  'contacts' table with the results.

Options:
  Name   Current Value  Required  Description
  ------ -------------  --------  -----------
  SOURCE  default       yes       source of input (see 'info' for details)

Source Options:
  default          SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>         string representing a single input
  <path>           path to a file containing a list of inputs
  query <sql>      database query returning one column of inputs

[recon-ng][default][whois_pocs] > options set SOURCE lockheedmartin.com
SOURCE => lockheedmartin.com
[recon-ng][default][whois_pocs] > run

------------------
LOCKHEEDMARTIN.COM
------------------
[*] URL: http://whois.arin.net/rest/pocs;domain=lockheedmartin.com
[*] No contacts found.
```

So I have search for two more domains northopgrumman did shown one contact details

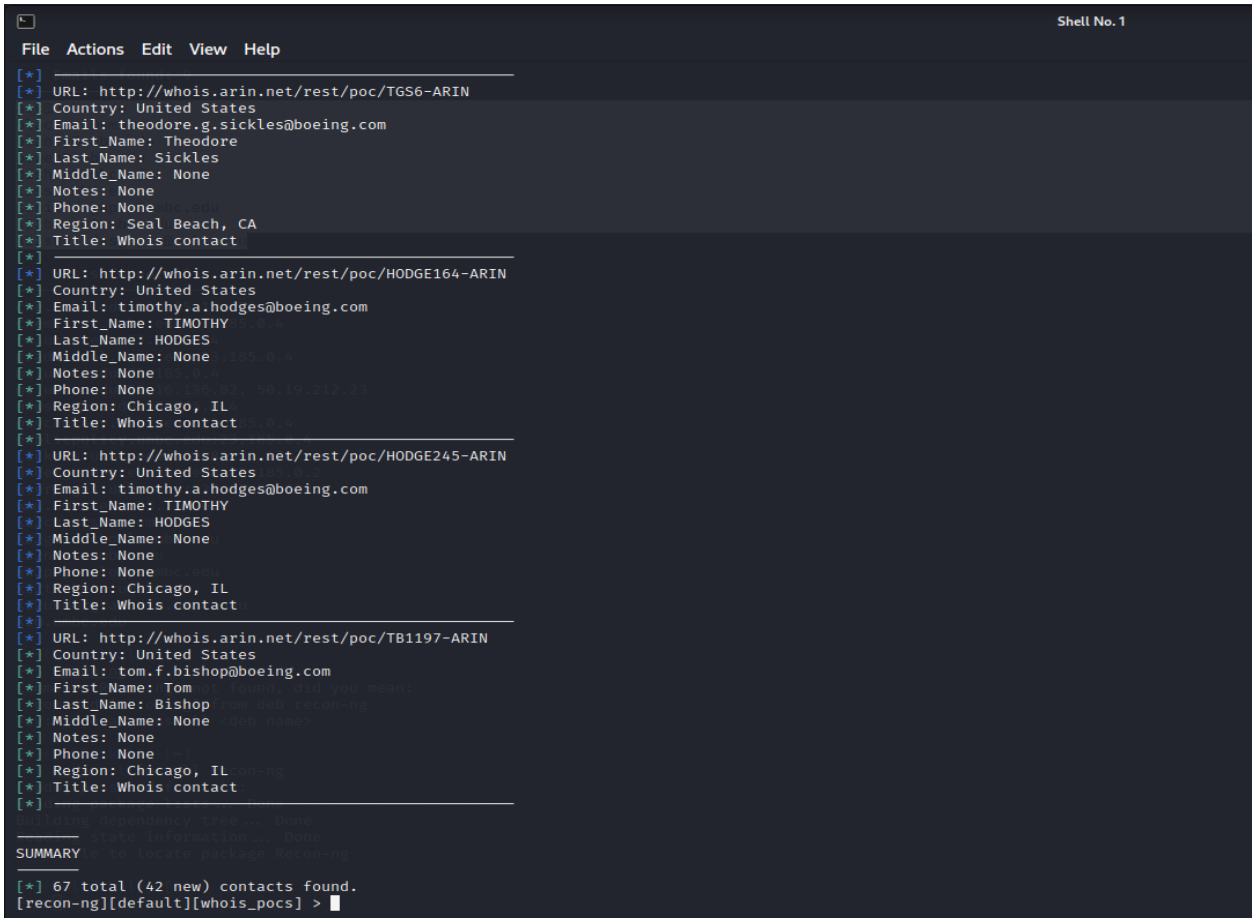
```
[recon-ng][default][whois_pocs] > options unset SOURCE
SOURCE => None
[recon-ng][default][whois_pocs] > options set SOURCE northropgrumman.com
SOURCE => northropgrumman.com
[recon-ng][default][whois_pocs] > run

----------------------
NORTHROPGRUMMAN.COM
----------------------
[*] URL: http://whois.arin.net/rest/pocs;domain=northropgrumman.com
[*] URL: http://whois.arin.net/rest/poc/BAHUS-ARIN
[*] Country: United States
[*] Email: fbahus@northropgrumman.com
[*] First_Name: Frank
[*] Last_Name: Bahus
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Annapolis Junction, MD
[*] Title: Whois contact
[*] ------------------------------------------------------------
-------
SUMMARY
-------
[*] 1 total (1 new) contacts found.
[recon-ng][default][whois_pocs] >
```

I have search for domain boeing.com which have shown total 67 contact details.

Shell No. 1

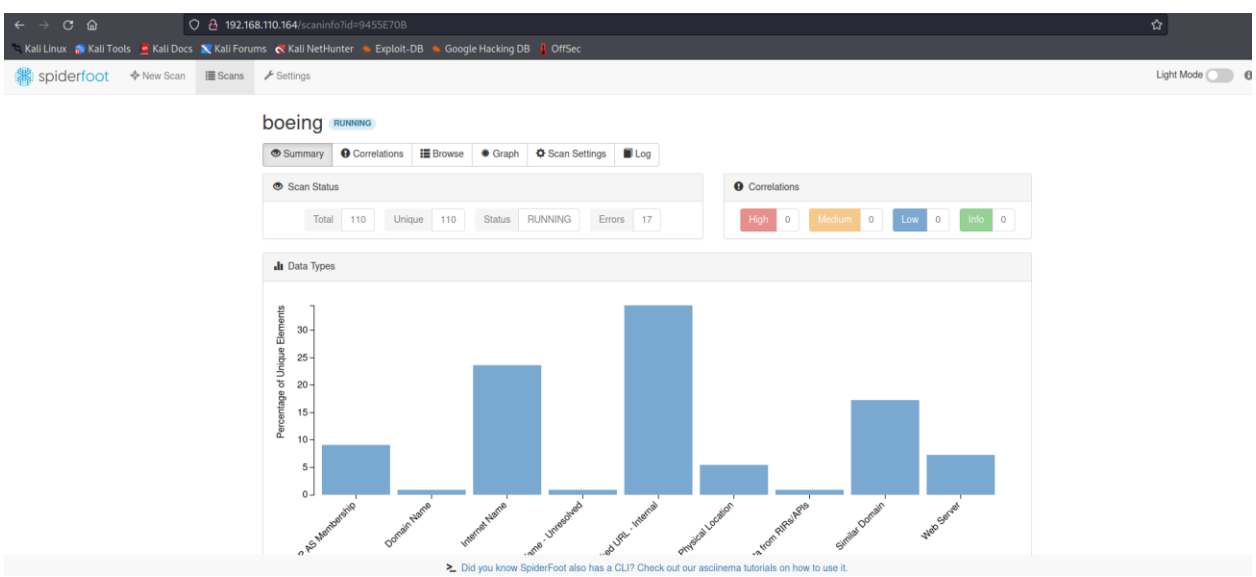
File Actions Edit View Help

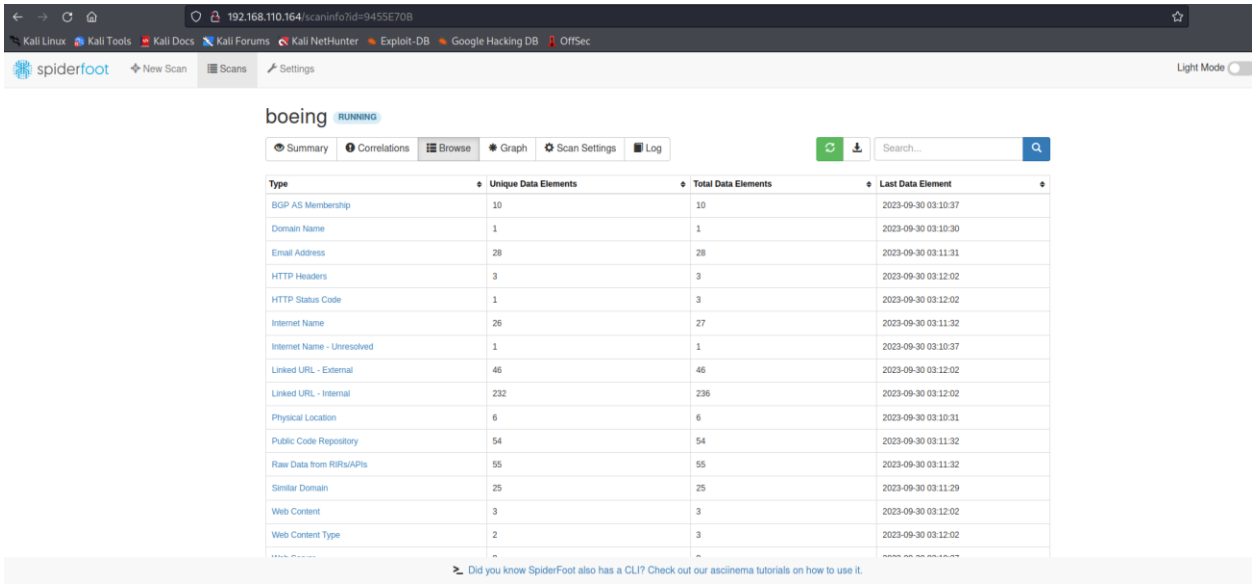
```
[recon-ng][default][whois_pocs] > options unset SOURCE
SOURCE => None
[recon-ng][default][whois_pocs] > options set SOURCE boeing.com
SOURCE => boeing.com
[recon-ng][default][whois_pocs] > run
----------
BOEING.COM
----------
[*] URL: http://whois.arin.net/rest/pocs;domain=boeing.com
[*] URL: http://whois.arin.net/rest/poc/AIR4-ARIN
[*] Country: United States
[*] Email: network.registrar@boeing.com
[*] First_Name: None
[*] Last_Name: Abuse and Incident Response
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Chicago, IL
[*] Title: Whois contact
[*] ----------
[*] Country: United States
[*] Email: abuse@boeing.com
[*] First_Name: None
[*] Last_Name: Abuse and Incident Response
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Chicago, IL
[*] Title: Whois contact
[*] ----------
[*] URL: http://whois.arin.net/rest/poc/AWO19-ARIN
[*] Country: United States
[*] Email: AL.WOOD@boeing.com
[*] First_Name: Al
[*] Last_Name: Wood
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Seal Beach, CA
[*] Title: Whois contact
[*] ----------
[*] URL: http://whois.arin.net/rest/poc/HOFFM353-ARIN
[*] Country: United States
[*] Email: aodhan.hoffman@boeing.com
[*] First_Name: Aodhan
[*] Last_Name: Hoffman
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Kent, WA
```



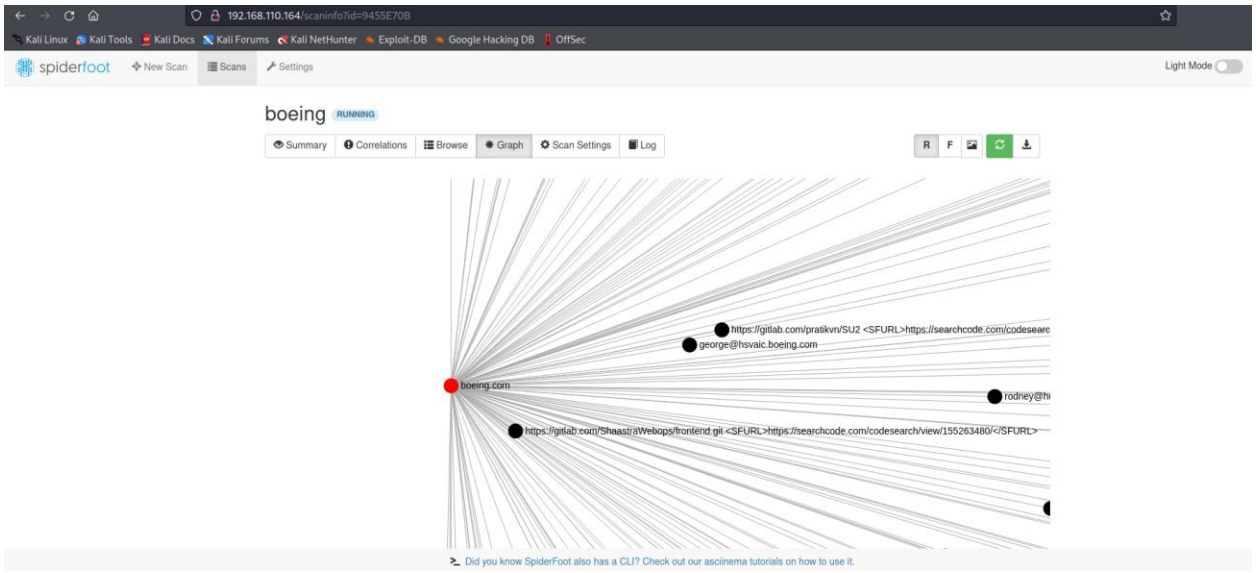
3. Using Spiderfoot, perform a search against a domain related to your target.

- I have started the Spiderfoot command line tool





Type	Unique Data Elements	Total Data Elements	Last Data Element
BGP AS Membership	10	10	2023-09-30 03:10:37
Domain Name	1	1	2023-09-30 03:10:30
Email Address	28	28	2023-09-30 03:11:31
HTTP Headers	3	3	2023-09-30 03:12:02
HTTP Status Code	1	3	2023-09-30 03:12:02
Internet Name	26	27	2023-09-30 03:11:32
Internet Name - Unresolved	1	1	2023-09-30 03:10:37
Linked URL - External	46	46	2023-09-30 03:12:02
Linked URL - Internal	232	236	2023-09-30 03:12:02
Physical Location	6	6	2023-09-30 03:10:31
Public Code Repository	54	54	2023-09-30 03:11:32
Raw Data from RIRs/APIs	55	55	2023-09-30 03:11:32
Similar Domain	25	25	2023-09-30 03:11:29
Web Content	3	3	2023-09-30 03:12:02
Web Content Type	2	3	2023-09-30 03:12:02



5. Dox the instructor

Answer the following questions:

1. Who do I work for and who have I worked for?
    a. You are working as a
        i. System Vulnerability Analyst for INNOPLEX, LLC,
        ii. Adjunct Professor for UMBC, Towson University, University of Arizona.
        iii. Graduate Teaching Assistant at FAU College.
    b. You were working as a
        i. Reverse Engineer in INNOPLEX, LLC
        ii. System Vulnerability Analyst in the United States Department of Defense

iii. DevOps Engineer at Cox Automotive Inc.
iv. Graduate Research Assistant at FAU
v. Information Technology Specialist at FAU

2. When did I get married?

- 1/27/24

3. Where do I/have I lived?

- You are living in Miami, Florida.

4. Who are my relatives?

- Toni Wood
  Amy Rodriguez
  Melissa Coston Martin
  Jim Rodriguez
  Chris Coston

5. What schools have I attended?

- Florida Atlantic University

6. What are some of the people I know (three or four is enough)?

- Amy Rodriguez
  Jim Rodriguez
  Ashley Rubio Er
  Toni Wood
  Jose Miguel Martin

7. What are some of my interests (two or three is enough)?

- Cybersecurity
  Learning new technology
  Teaching students

8. Do I have children? Names?

- No kids

9. Did/do I own a domain name?

- Haven’t found any as per my search