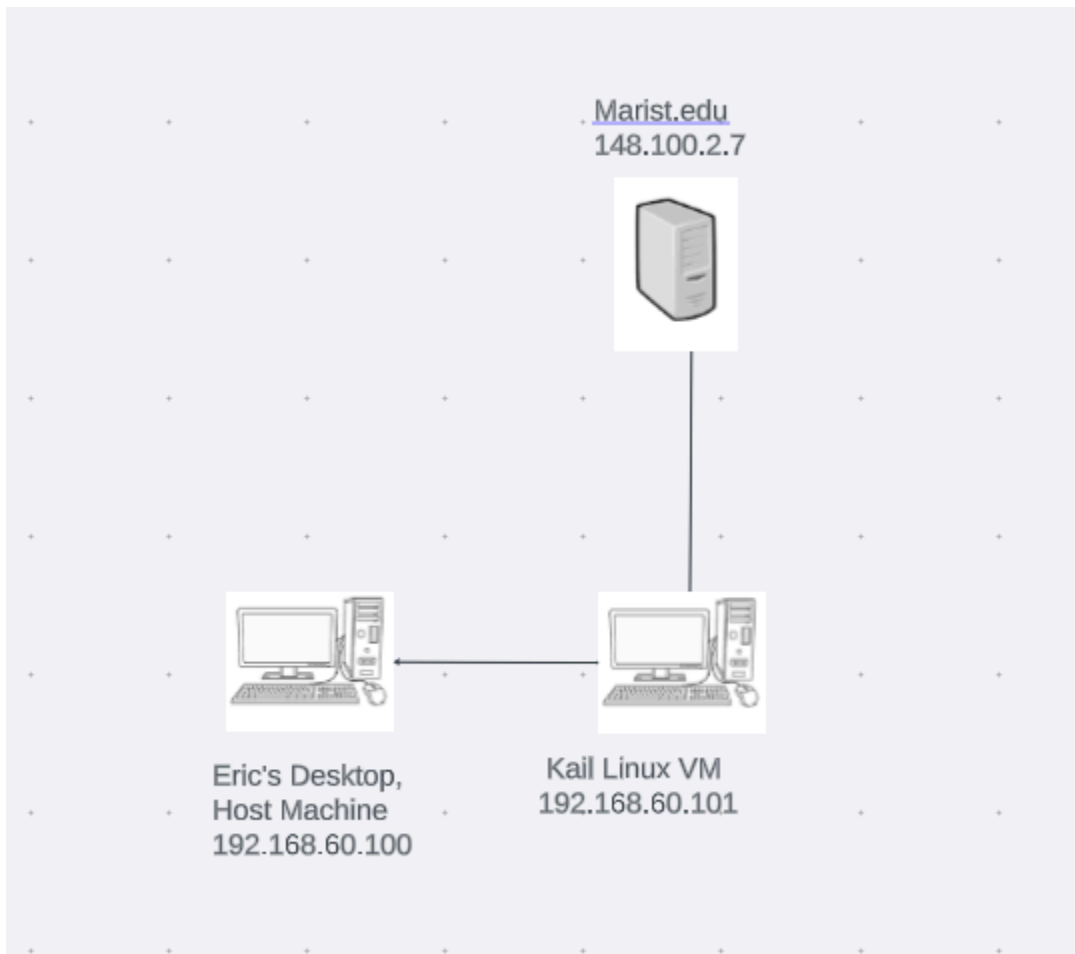


Lab 3

Description: In this lab we used OSINT techniques and discovery tools on a target organization.

Topology:



Syntax:

Command	Description
Modules load recon/domain-hosts/	Used in Recon-ng to choose a module that discovers certain data

Set SOURCE Marist.edu	Sets the source of the data collection to Marist.edu (recon-ng)
theHarvester -d Marist.edu -l 5 -b all	Sets the domain and parameters for theHarvester to harvest from
Python3 ./sf.py -l 127.0.0.1:5001	Starts the spiderfoot web server

Verification:

A. Target Profile:

Target - Marist

Technologies -

Firewall - Juniper SRX

Virtualization technology: z/VM on IBM z14 server

Email Service - LISTSERV

Database - QIP

LMS - Brightspace

IP Addresses and ranges -

Public IP: 148.100.2.7

IP Address Range: 148.100.0.0 - 148.100.255.255

Services -

Public Website: <https://www.marist.edu/>

Student Portal: <https://my.marist.edu/student>

Outlook Web Access - <https://mymail.marist.edu>

LMS - <https://brightspace.marist.edu/d2l/home>

C. Recon-ng:

These three screenshots show the commands I input into recon-ng and the output I received.

```
[recon-ng][default] > modules load recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] > options set SOURCE marist.edu
SOURCE => marist.edu
[recon-ng][default][google_site_web] > run
```

MARIST.EDU

```
[*] Searching Google for: site:marist.edu
[*] Country: None
[*] Host: ccac.marist.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: walkway.marist.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: turnitin.ilearn.marist.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
```

```
[*] Country: None
[*] Host: my.de.marist.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: docs.fdrlibrary.marist.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: icecast.marist.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: maristpoll.marist.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

SUMMARY

```
[*] 54 total (54 new) hosts found.
[recon-ng][default][google_site_web] > options set SOURCE marist.edu
SOURCE => marist.edu
[recon-ng][default][google_site_web] > show hosts
```

rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	ccac.marist.edu							google_site_web
2	walkway.marist.edu							google_site_web
3	turnitin.ilearn.marist.edu							google_site_web
4	my.de.marist.edu							google_site_web
5	docs.fdrlibrary.marist.edu							google_site_web
6	icecast.marist.edu							google_site_web
7	maristpoll.marist.edu							google_site_web
8	maristconnect.marist.edu							google_site_web
9	library.marist.edu							google_site_web
10	sga.marist.edu							google_site_web
11	magazine.marist.edu							google_site_web
12	acctgmt.it.marist.edu							google_site_web
13	my.marist.edu							google_site_web
14	ecc.marist.edu							google_site_web
15	www.fdrlibrary.marist.edu							google_site_web
16	www.marist.edu							google_site_web
17	libguides.marist.edu							google_site_web
18	idcp.marist.edu							google_site_web
19	webapps.it.marist.edu							google_site_web

The results for using the modules recon/domain-hosts on marist.edu are that Marist has many subdomains associated with marist.edu. The IP addresses are obviously not visible, as there are security measures in place that are not allowing recon-ng to resolve the IPs of these domains. This is to be expected from an organization like Marist, that wants to keep their domains secure from anyone who wants to attack them. The value I gained from this tool is that I can now see every domain associated with Marist.edu which allows someone with malicious intent to start looking for vulnerabilities.

The Harvester:

These screenshots show the commands I input into the harvester and the output I received.

```
(kali@kali)-[~]
$ theHarvester -d marist.edu -l 5 -b all

*****
*                                     *
* [L] [I] [N] [E] [X] [T] [E] [R] [V] [E] [S] [T] [E] [R] [E] [S] [E] [A] [R] [C] [H] *
* [L] [I] [N] [E] [X] [T] [E] [R] [V] [E] [S] [T] [E] [R] [E] [S] [E] [A] [R] [C] [H] *
*                                     *
* theHarvester 4.4.3                 *
* Coded by Christian Martorella      *
* Edge-Security Research             *
* cmartorella@edge-security.com      *
*                                     *
*****

[*] Target: marist.edu
```

```
Change IPs, manually solve the captcha, or wait before rerunning Sitedossier
[*] Searching Sitedossier.
An exception has occurred: 400, message='Got more than 8190 bytes (11985) when
=%22marist.edu%22&offset=36&source=web&show_local=0&spellcheck=0')
An exception has occurred: 0, message='Attempt to decode JSON with unexpected
ain=marist.edu')
[*] Searching Subdomaincenter.
[*] Searching SubdomainfinderC99.
[*] Searching Threatminer.
[*] Searching Urlscan.
[*] Searching Yahoo.
An exception has occurred: 400, message='Got more than 8190 bytes (11985) when
=site:marist.edu&offset=0&source=web&show_local=0&spellcheck=0')
[*] Searching Brave.

[*] ASNS found: 9
AS131965
AS14618
AS16625
AS201133
AS209242
AS32244
AS396982
AS54641
AS6124

[*] Interesting Urls found: 21
http://linuxone.cloud.marist.edu/
http://maristpoll.marist.edu/313-tolerance-for-religious-rights/

[*] LinkedIn Links found: 0
[*] IPs found: 210
10.10.1.106
10.10.1.107
10.10.1.111
10.10.1.116
10.10.1.155
10.10.1.157
10.10.1.170
10.10.1.213
10.10.1.215
10.10.1.54
10.10.1.63
10.10.1.92
10.10.255.10
10.10.255.15
10.10.255.16
10.10.255.17
10.10.255.18
10.10.255.208
10.10.255.23
10.10.255.231
10.10.255.233
10.10.255.27
10.10.255.29

[*] Emails found: 2
helpdesk@marist.edu

[*] Hosts found: 1923
148-100-154-115.FoxNet.marist.edu
148-100-192-0.DEFAULT.NATPOOL.marist.edu:148.100.192.0
148-100-192-1.DEFAULT.NATPOOL.marist.edu:148.100.192.1
148-100-192-10.DEFAULT.NATPOOL.marist.edu:148.100.192.10
148-100-192-101.DEFAULT.NATPOOL.marist.edu:148.100.192.101
148-100-192-11.DEFAULT.NATPOOL.marist.edu:148.100.192.11
148-100-192-110.DEFAULT.NATPOOL.marist.edu:148.100.192.110
148-100-192-111.DEFAULT.NATPOOL.marist.edu:148.100.192.111
148-100-192-120.DEFAULT.NATPOOL.marist.edu:148.100.192.120
148-100-192-121.DEFAULT.NATPOOL.marist.edu:148.100.192.121
148-100-192-130.DEFAULT.NATPOOL.marist.edu:148.100.192.130
148-100-192-131.DEFAULT.NATPOOL.marist.edu:148.100.192.131
148-100-192-140.DEFAULT.NATPOOL.marist.edu:148.100.192.140
148-100-192-160.DEFAULT.NATPOOL.marist.edu:148.100.192.160
148-100-192-170.DEFAULT.NATPOOL.marist.edu:148.100.192.170
148-100-192-180.DEFAULT.NATPOOL.marist.edu:148.100.192.180
148-100-192-190.DEFAULT.NATPOOL.marist.edu:148.100.192.190
148-100-192-20.DEFAULT.NATPOOL.marist.edu:148.100.192.20
148-100-192-201.DEFAULT.NATPOOL.marist.edu:148.100.192.201
```

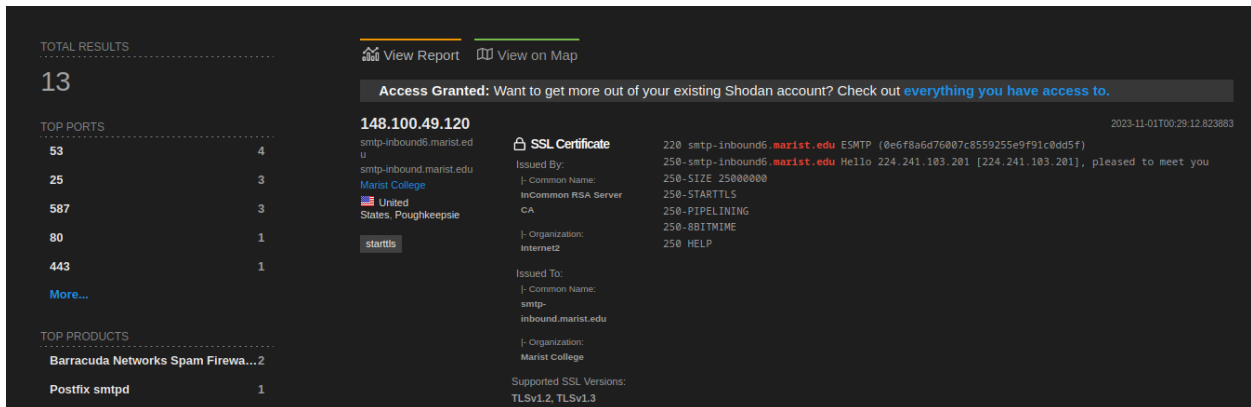
```
[*] Emails found: 2
helpdesk@marist.edu

[*] Hosts found: 1923
148-100-154-115.FoxNet.marist.edu
148-100-192-0.DEFAULT.NATPOOL.marist.edu:148.100.192.0
148-100-192-1.DEFAULT.NATPOOL.marist.edu:148.100.192.1
148-100-192-10.DEFAULT.NATPOOL.marist.edu:148.100.192.10
148-100-192-101.DEFAULT.NATPOOL.marist.edu:148.100.192.101
148-100-192-11.DEFAULT.NATPOOL.marist.edu:148.100.192.11
148-100-192-110.DEFAULT.NATPOOL.marist.edu:148.100.192.110
148-100-192-111.DEFAULT.NATPOOL.marist.edu:148.100.192.111
148-100-192-120.DEFAULT.NATPOOL.marist.edu:148.100.192.120
148-100-192-121.DEFAULT.NATPOOL.marist.edu:148.100.192.121
148-100-192-130.DEFAULT.NATPOOL.marist.edu:148.100.192.130
148-100-192-131.DEFAULT.NATPOOL.marist.edu:148.100.192.131
148-100-192-140.DEFAULT.NATPOOL.marist.edu:148.100.192.140
148-100-192-160.DEFAULT.NATPOOL.marist.edu:148.100.192.160
148-100-192-170.DEFAULT.NATPOOL.marist.edu:148.100.192.170
148-100-192-180.DEFAULT.NATPOOL.marist.edu:148.100.192.180
148-100-192-190.DEFAULT.NATPOOL.marist.edu:148.100.192.190
148-100-192-20.DEFAULT.NATPOOL.marist.edu:148.100.192.20
148-100-192-201.DEFAULT.NATPOOL.marist.edu:148.100.192.201
```

The results I received from the harvester were that it found ASNS, some interesting URLs, failed to find any linkedin links, found many IPs, hosts and some emails. I was surprised to find something called ASNS as I did not know what they were until I looked them up. It makes sense why such a large organization such as Marist has 9 ASNS. I was also not surprised to find as many IPs and hosts as I did since Marist needs that many to operate. I gained a lot from this, as this OSINT tool gave me actual relevant data. The information gained here could be used by a penetration tester to probe the IPv4 addresses that were gained, and may allow them to find a weakness.

Shodan.io

These screenshots show the results of looking up Marist.edu on Shodan.io.



This screenshot shows the Shodan.io search results for the domain Marist.edu. The interface is dark-themed. On the left, under 'TOTAL RESULTS', the number '13' is displayed. Below this, 'TOP PORTS' are listed: 53 (4), 25 (3), 587 (3), 80 (1), and 443 (1). 'TOP PRODUCTS' include 'Barracuda Networks Spam Firewa...' (2) and 'Postfix smtpd' (1). The main content area displays the IP address '148.100.49.120' and an 'SSL Certificate' issued by 'Marist College' to 'smtp-inbound.marist.edu'. A banner at the top right says 'Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.'

TOTAL RESULTS
13

TOP PORTS

Port	Count
53	4
25	3
587	3
80	1
443	1

More...

TOP PRODUCTS

Product	Count
Barracuda Networks Spam Firewa...	2
Postfix smtpd	1

148.100.49.120

smtp-inbound.marist.edu

Marist College

United States, Poughkeepsie

starttls

SSL Certificate

Issued By: 220 smtp-inbound5.marist.edu ESMTP (0e6f8a6d76807c8559255e9f91c0dd5f) 2023-11-01T00:29:12.823883

Issued To: 250-smtp-inbound5.marist.edu Hello 224.241.183.201 [224.241.183.201], pleased to meet you

Common Name: 250-SIZE 250000000

Organization: 250-STARTTLS

250-PIPELINING

250-8BITTIME

250 HELP

Issued To: 250-SIZE 250000000

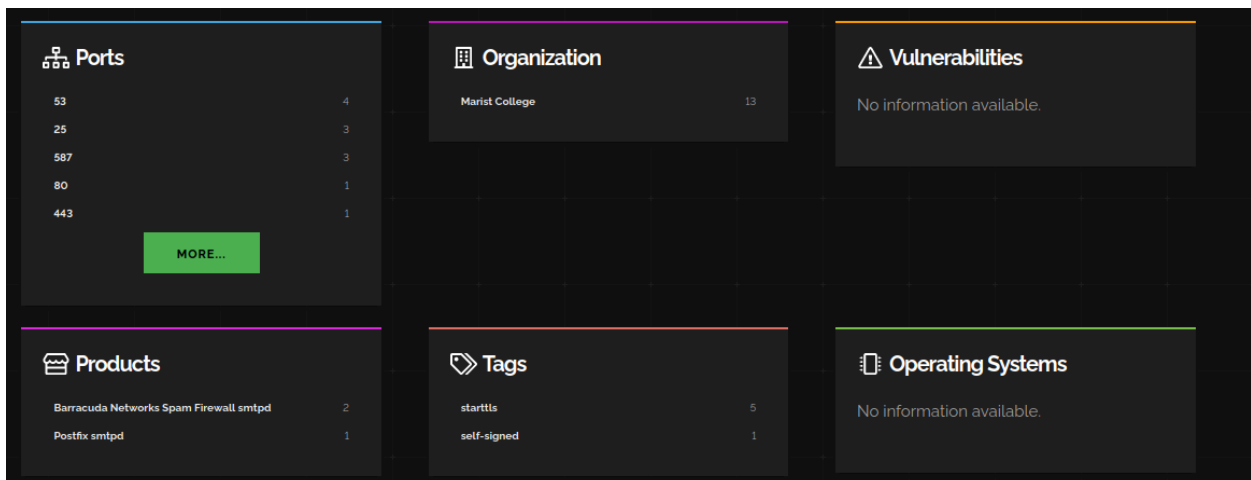
Common Name: 250-STARTTLS

Organization: 250-PIPELINING

250-8BITTIME

250 HELP

Supported SSL Versions: TLSv1.2, TLSv1.3



This screenshot shows the Shodan.io dashboard with search results for Marist.edu. The dashboard is organized into six panels: 'Ports' (53, 25, 587, 80, 443), 'Organization' (Marist College, 13), 'Vulnerabilities' (No information available), 'Products' (Barracuda Networks Spam Firewall smtpd, 2; Postfix smtpd, 1), 'Tags' (starttls, 5; self-signed, 1), and 'Operating Systems' (No information available).

Ports

Port	Count
53	4
25	3
587	3
80	1
443	1

MORE...

Organization

Marist College

13

Vulnerabilities

No information available.

Products

Product	Count
Barracuda Networks Spam Firewall smtpd	2
Postfix smtpd	1

Tags

Tag	Count
starttls	5
self-signed	1

Operating Systems

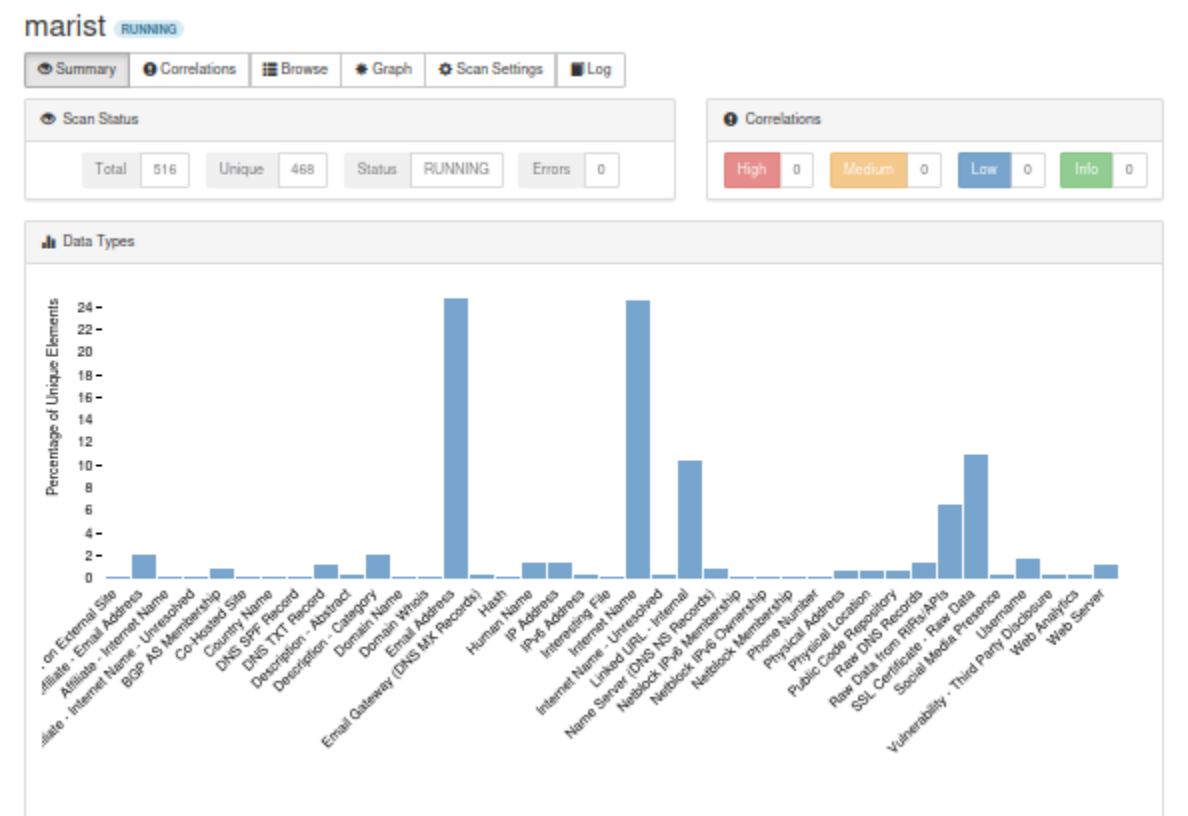
No information available.

// SSL INSIGHTS		
SSL/ TLS Versions		
tlsv12	7	
tlsv13	6	
tlsv1	1	
tlsv11	1	
JARM Fingerprints		
00000000000000000000000000000000..._5		
07d19d12d21d07c42d43d00000f50d155...	1	
22d22d00022d22d00022d22d22da9e96d3...	1	
JA3S Fingerprints		
1769b01aa3d6e76dad9f237797e5dc2c	5	
6c281f7ba8e88604ea41a2bf9fa5ad7	1	
fb38aec9b9f7318383270c307f8f7773	1	

The results I found from Shodan.io are the ports, products, SSL/TLS versions, JARM and JA35 fingerprints. All of these results seem pretty standard for a college's website, I do not see anything out of the ordinary. The value someone could gain from this tool is probably the specific port numbers being used, SSL and TLS being displayed. Someone could scan the ports to find any open one and exploit them. They may also analyze the SSL and TLS to see if the encryption versions are weak or misconfigured, prompting an attack if anything is found.

SpiderFoot:

The screenshots here show my SpiderFoot scan on Marist.edu.



Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	1	1	2023-11-01 06:29:57
Affiliate - Email Address	10	10	2023-11-01 06:21:52
Affiliate - Internet Name	1	1	2023-11-01 06:18:19
Affiliate - Internet Name - Unresolved	1	1	2023-11-01 06:18:18
BGP AS Membership	4	8	2023-11-01 06:26:25
Co-Hosted Site	1	1	2023-11-01 06:27:06
Country Name	1	2	2023-11-01 06:29:27
DNS SPF Record	1	1	2023-11-01 06:18:08
DNS TXT Record	6	6	2023-11-01 06:18:08
Description - Abstract	2	2	2023-11-01 06:26:20
Description - Category	10	11	2023-11-01 06:26:20
Domain Name	1	2	2023-11-01 06:18:12
Domain Whois	1	1	2023-11-01 06:21:56
Email Address	116	117	2023-11-01 06:29:57
Email Gateway (DNS MX Records)	2	4	2023-11-01 06:26:49
Hash	1	1	2023-11-01 06:21:48
Human Name	7	8	2023-11-01 06:29:57
IP Address	7	7	2023-11-01 06:29:27
IPv6 Address	2	2	2023-11-01 06:18:27

Browse / Email Address

<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	.michael.doughty1@marist.edu	marist.edu	sfp_emailformat	2023-11-01 06:18:13
<input type="checkbox"/>	Connor.mcstay1@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:26:03
<input type="checkbox"/>	Emilio.paganyournol@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:26:03
<input type="checkbox"/>	Jack.McKenna1@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:26:03
<input type="checkbox"/>	Julio.Cabrera2@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:26:03
<input type="checkbox"/>	Kathryn.Silberger@marist.edu	marist.edu	sfp_flickr	2023-11-01 06:18:11
<input type="checkbox"/>	Madison.Kaplan1@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:26:03
<input type="checkbox"/>	Mark.Ferraro@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:26:03
<input type="checkbox"/>	Mark.ferraro52@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:26:03
<input type="checkbox"/>	Michael.Cummins1@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:26:03

The results I received varied greatly. The most important information I got was email addresses, internet names, internal linked urls, some human names, usernames and some raw api/ssl data. I was surprised to find actual Marist emails since I selected the least intrusive option on the tool. I was thinking I would find some IP addresses but to find actual emails seems pretty crazy to me. I gained over 100 Marist.edu email addresses. Phishing attacks could be used on these Marist emails all from someone who just input Marist.edu into this tool, this could be a decently big security threat.

Amass

These screenshots show the command I input into Amass and its results.

```
(kali㉿kali)-[~]
$ amass enum -d marist.edu -o results.txt

marist.edu (FQDN) → mx_record → marist-edu.mail.protection.outlook.com (FQDN)
www.marist.edu (FQDN) → cname_record → www.ha.marist.edu (FQDN)
brightspace.marist.edu (FQDN) → cname_record → marist.brightspace.com (FQDN)
smtp-inbound.marist.edu (FQDN) → a_record → 148.100.49.120 (IPAddress)
smtp-inbound.marist.edu (FQDN) → a_record → 148.100.49.27 (IPAddress)
ecc.marist.edu (FQDN) → cname_record → nucolr.ha.marist.edu (FQDN)
ml021.zcloud.marist.edu (FQDN) → a_record → 148.100.104.56 (IPAddress)
jss.it.marist.edu (FQDN) → cname_record → nymaristcollege.jamfcloud.com (FQDN)
careers.marist.edu (FQDN) → cname_record → 8y5uymmdqh.36199c6c748d8adafab47e4b6e312c61.careersite.pageuppeople.com (FQDN)
8y5uymmdqh.36199c6c748d8adafab47e4b6e312c61.careersite.pageuppeople.com (FQDN) → cname_record → d1oul2vf72cqt.cloudfront.net (FQDN)
dropbox.it.marist.edu (FQDN) → cname_record → dropbox.it.ha.marist.edu (FQDN)
degreeworks.banner.marist.edu (FQDN) → cname_record → degreeworks.ha.marist.edu (FQDN)
superconference.marist.edu (FQDN) → cname_record → nucolr.ha.marist.edu (FQDN)
it.marist.edu (FQDN) → cname_record → www.marist.edu (FQDN) become, the more you are able to hear"
admit.marist.edu (FQDN) → cname_record → admit.ha.marist.edu (FQDN)
idpv3.it.marist.edu (FQDN) → cname_record → idpv3.ha.marist.edu (FQDN)
som.marist.edu (FQDN) → cname_record → www.marist.edu (FQDN)
libguides.marist.edu (FQDN) → cname_record → v2.libguides.com (FQDN)
v2.libguides.com (FQDN) → cname_record → region-us.libguides.com (FQDN)
sga.staging.it.marist.edu (FQDN) → cname_record → sga-test.it.marist.edu (FQDN)
library.marist.edu (FQDN) → cname_record → library1.marist.edu (FQDN)
security.marist.edu (FQDN) → cname_record → www.ha.marist.edu (FQDN)
italy.marist.edu (FQDN) → cname_record → www.ha.marist.edu (FQDN)

ml026.zcloud.marist.edu (FQDN) → a_record → 148.100.104.61 (IPAddress)
search.marist.edu (FQDN) → cname_record → www.ha.marist.edu.marist.edu (FQDN)
music.marist.edu (FQDN) → cname_record → www.marist.edu (FQDN)
www.facit.marist.edu (FQDN) → cname_record → www.marist.edu (FQDN)
remote4.csits.marist.edu (FQDN) → cname_record → remote4.cs.marist.edu (FQDN)
148.100.0.0/16 (Netblock) → contains → 148.100.100.35 (IPAddress)
148.100.0.0/16 (Netblock) → contains → 148.100.3.50 (IPAddress)
148.100.0.0/16 (Netblock) → contains → 148.100.49.51 (IPAddress)
148.100.0.0/16 (Netblock) → contains → 148.100.3.25 (IPAddress)
148.100.0.0/16 (Netblock) → contains → 148.100.2.45 (IPAddress)
148.100.0.0/16 (Netblock) → contains → 148.100.49.31 (IPAddress)
148.100.0.0/16 (Netblock) → contains → 148.100.104.61 (IPAddress)
148.100.0.0/16 (Netblock) → contains → 148.100.49.120 (IPAddress)
148.100.0.0/16 (Netblock) → contains → 148.100.49.27 (IPAddress)
148.100.0.0/16 (Netblock) → contains → 148.100.104.56 (IPAddress)
10.0.0.0/8 (Netblock) → contains → 10.13.9.72 (IPAddress)
6124 (ASN) → managed_by → MARIST - Marist College (RIROrganization)
6124 (ASN) → announces → 148.100.0.0/16 (Netblock)
0 (ASN) → managed_by → Reserved Network Address Blocks (RIROrganization)
0 (ASN) → announces → 10.0.0.0/8 (Netblock)
remote4.cs.marist.edu (FQDN) → a_record → 148.100.49.129 (IPAddress)
degreeworks.it.marist.edu (FQDN) → cname_record → degreeworks.ha.marist.edu (FQDN)
vm.it.marist.edu (FQDN) → a_record → 10.13.3.69 (IPAddress)
timeclockplus.it.marist.edu (FQDN) → a_record → 148.100.2.52 (IPAddress)
slip-8.marist.edu (FQDN) → a_record → 148.100.32.12 (IPAddress)
ml014.zcloud.marist.edu (FQDN) → a_record → 148.100.104.49 (IPAddress)
148.100.0.0/16 (Netblock) → contains → 148.100.49.129 (IPAddress)
v1.marist.edu (FQDN) → a_record → 148.100.40.66 (IPAddress)
elasticsearch003.syr.marist.edu (FQDN) → a_record → 148.100.241.173 (IPAddress)
10.0.0.0/8 (Netblock) → contains → 10.13.3.69 (IPAddress)
```


The results I got from Amass were pretty similar to other OSINT tools, as it was really only subdomains and IP addresses. This was all really expected, nothing seems out of the ordinary. The value I gained from this tool is that I can see many of Marist's subdomains and IP addresses that are being actively used. Penetration testers can identify web apps and resources being used on these subdomains and look if there are any vulnerabilities that are exploitable.

D. OSINT is very valuable in network and cyber security. There is so much information you can get just by inputting a website name into one of the previously used tools. This makes these tools extremely useful for penetration testers and malicious actors alike. To keep their data from these actors, organizations should have frequent testers using a variety of OSINT tools to see how much and what data is available and accessible to the public. Once found, this data should be taken down and they should do everything in their power to fix the vulnerability that caused this data to become public.

Conclusion:

This lab was really fun. I personally have never used linux before, so it was challenging and interesting to get to learn a new operating system. Learning how to operate all of the applications was pretty interesting too. I had to use many tutorials for some of the apps, which was a little frustrating, but was worth it in the end when I saw all of the Marist.edu data populating on screen. Except for having to spend some time learning each app, everything else worked great.

References:

1. <https://www.kali.org/tools/recon-ng/>
2. <https://securitytrails.com/blog/theharvester-tool>
3. <https://www.geeksforgeeks.org/spiderfoot-a-automate-osint-framework-in-kali-linux/>
4. <https://www.dionach.com/en-us/blog/how-to-use-owasp-amass-an-extensive-tutorial/>