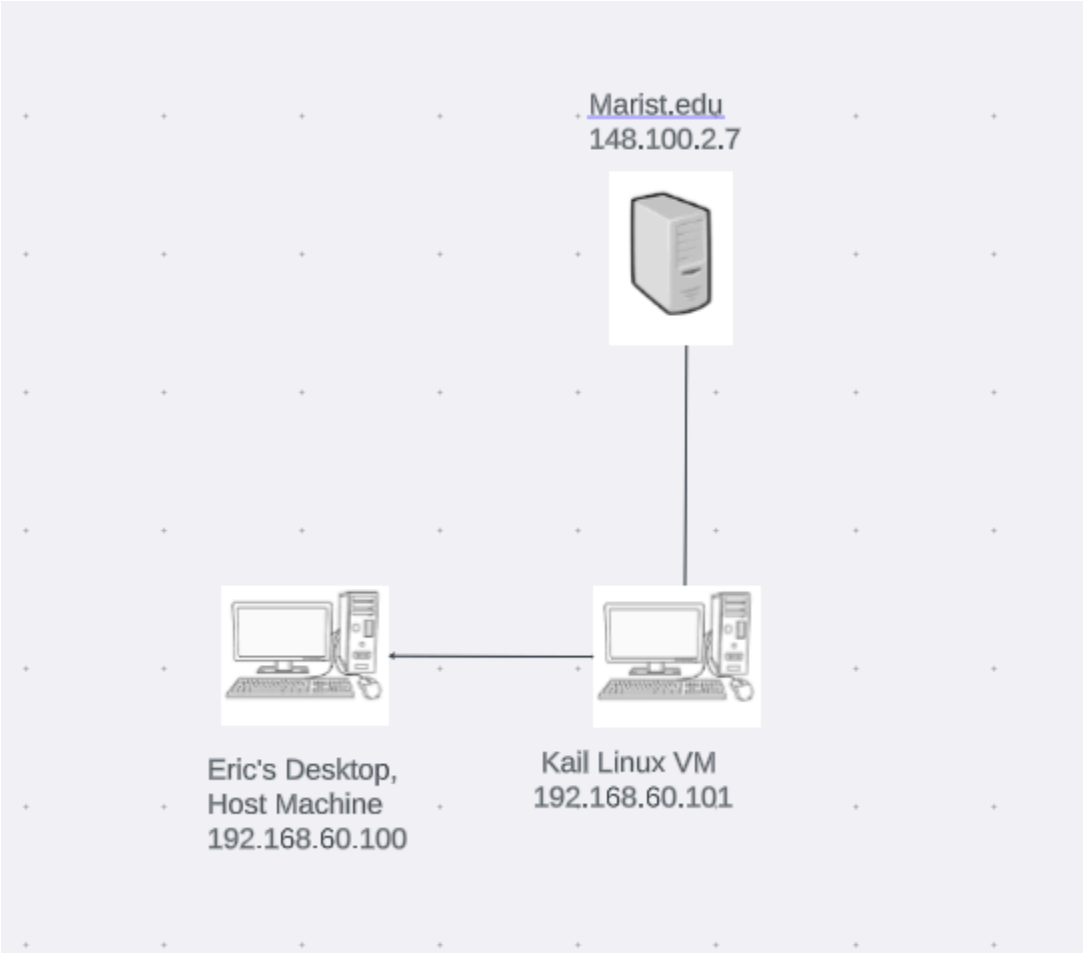
Eric Guzman 11/1/2023
Professor Cannistra Network Security

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:

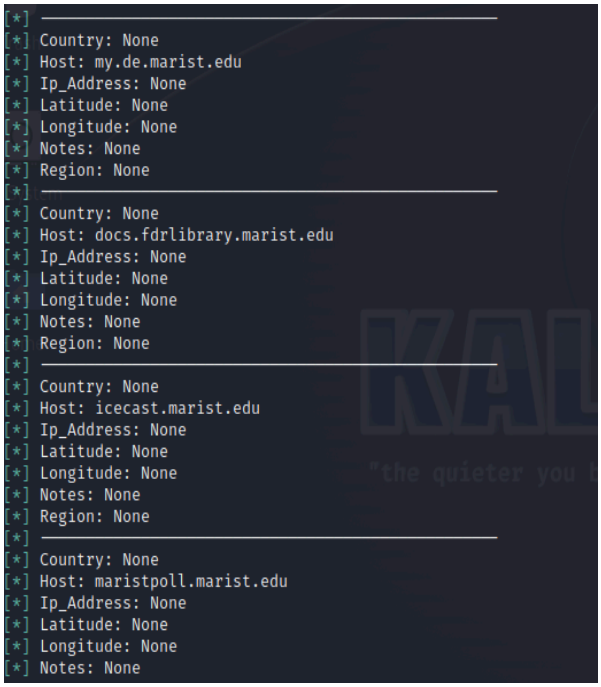
A. Target Profile:
Target - Marist

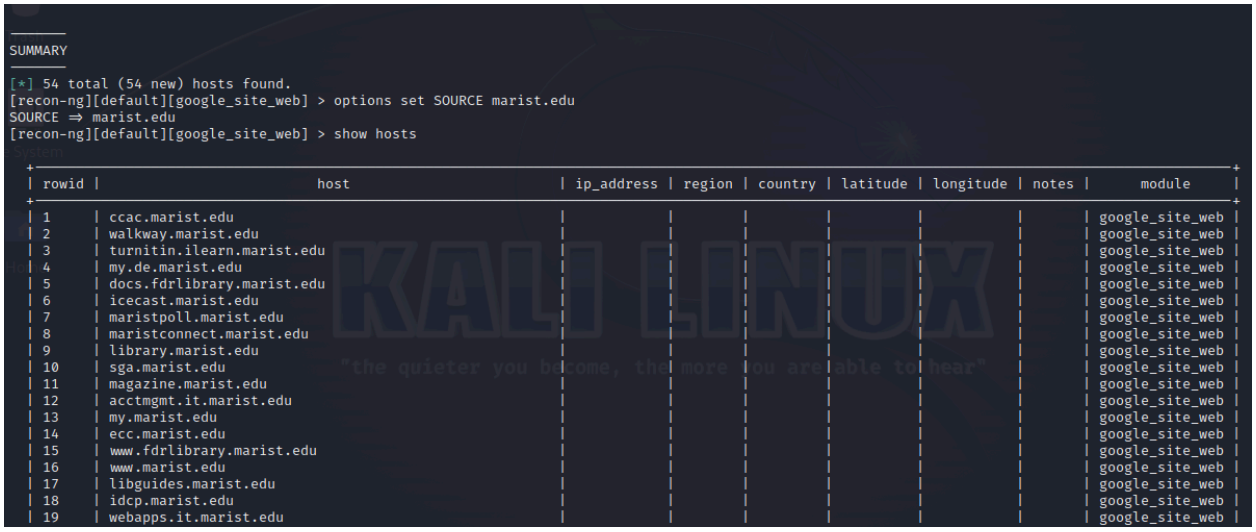
Technologies -
Firewall - Juniper SRX
Virtualization technology: z/VM on IBM z14 server
Email Service - LISTSERV
Database - QIP
LMS - Brightspace

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.

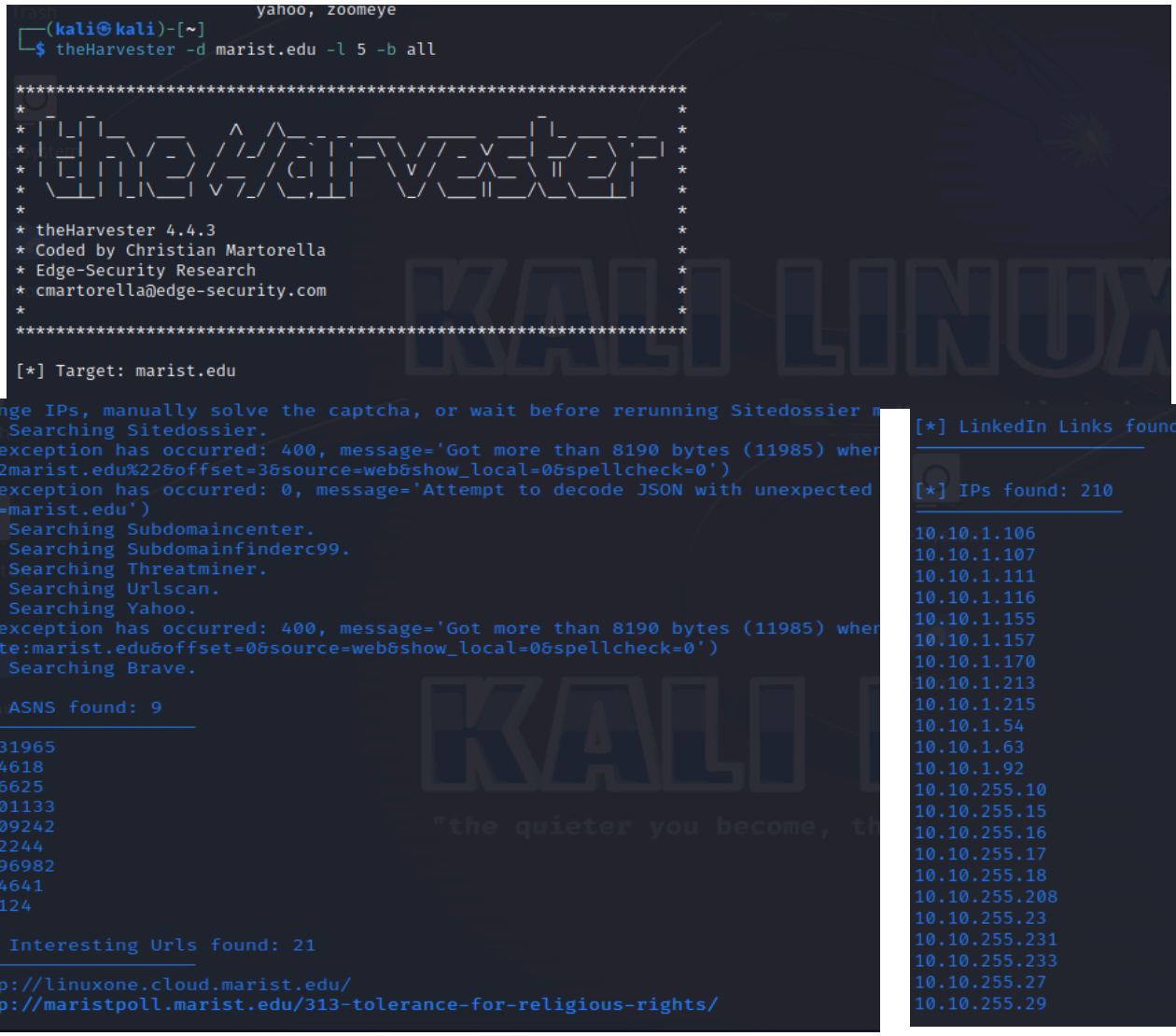


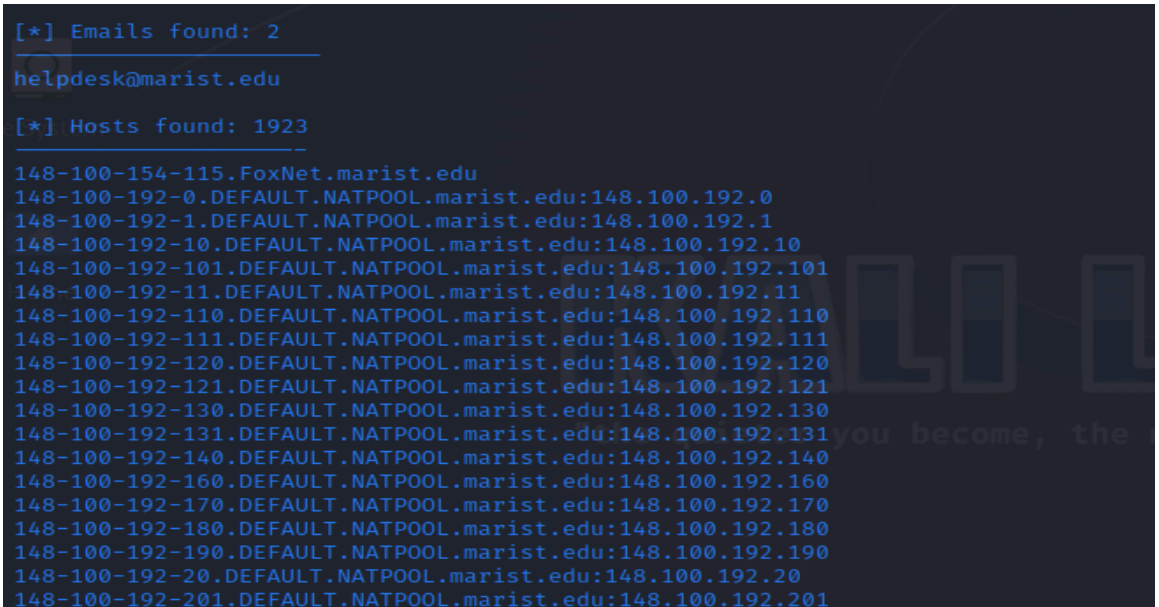


The results for using the modules recon/domain-hosts on marist.edu are that Marist has many subdomains associated with marist.edu. The IP addresses are obviously not visible, as there are security measures in place that are not allowing recon-ng to resolve the IPs of these domains. This is to be expected 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.

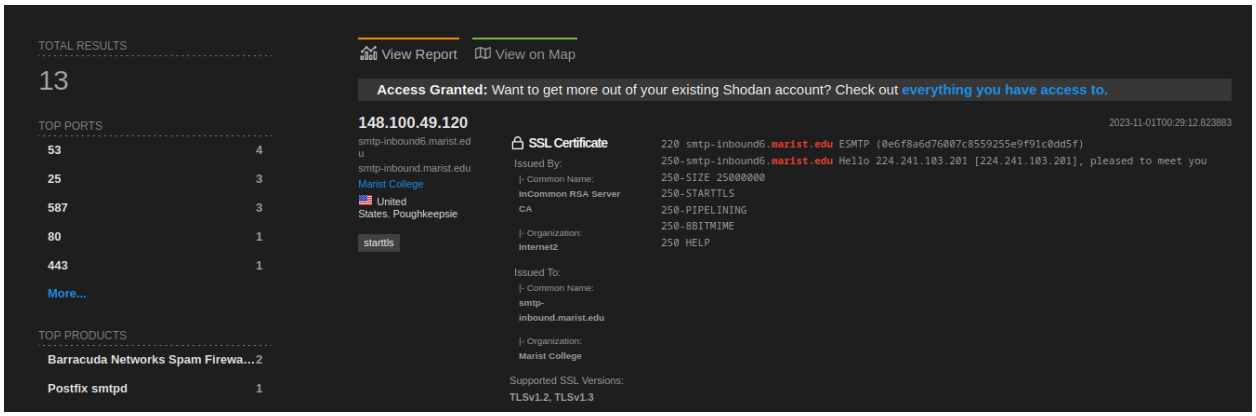


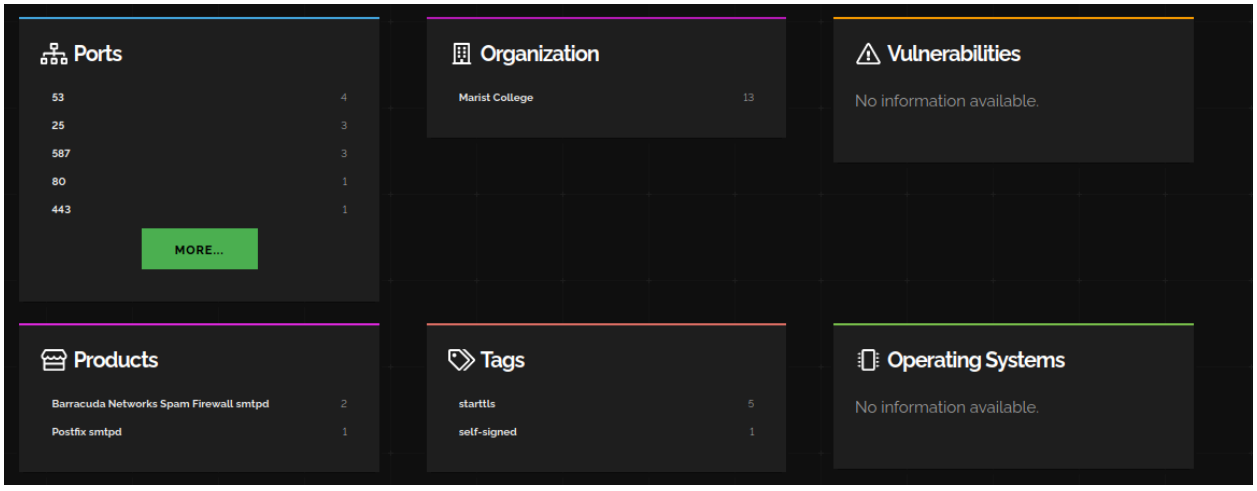


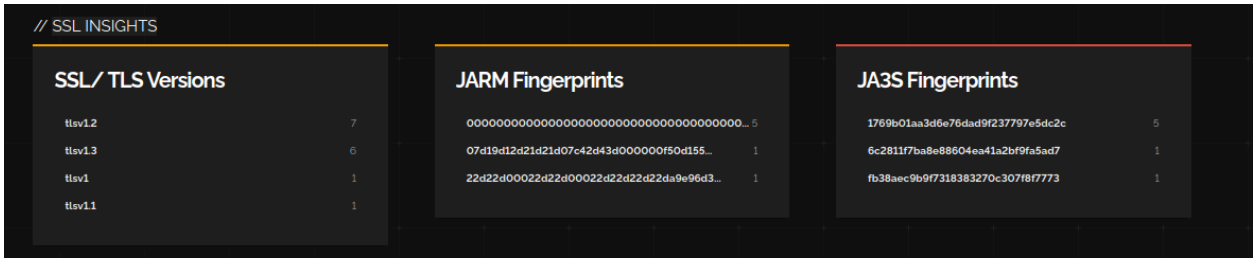
The results I received from the harvester were that it found ASNS, some interesting URLs, failed to find any linkedin links, found many IPs, hosts and some emails. I was surprised to find something called ASNS as I did not know what they were until I looked them up. It makes sense why such a large organization 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.



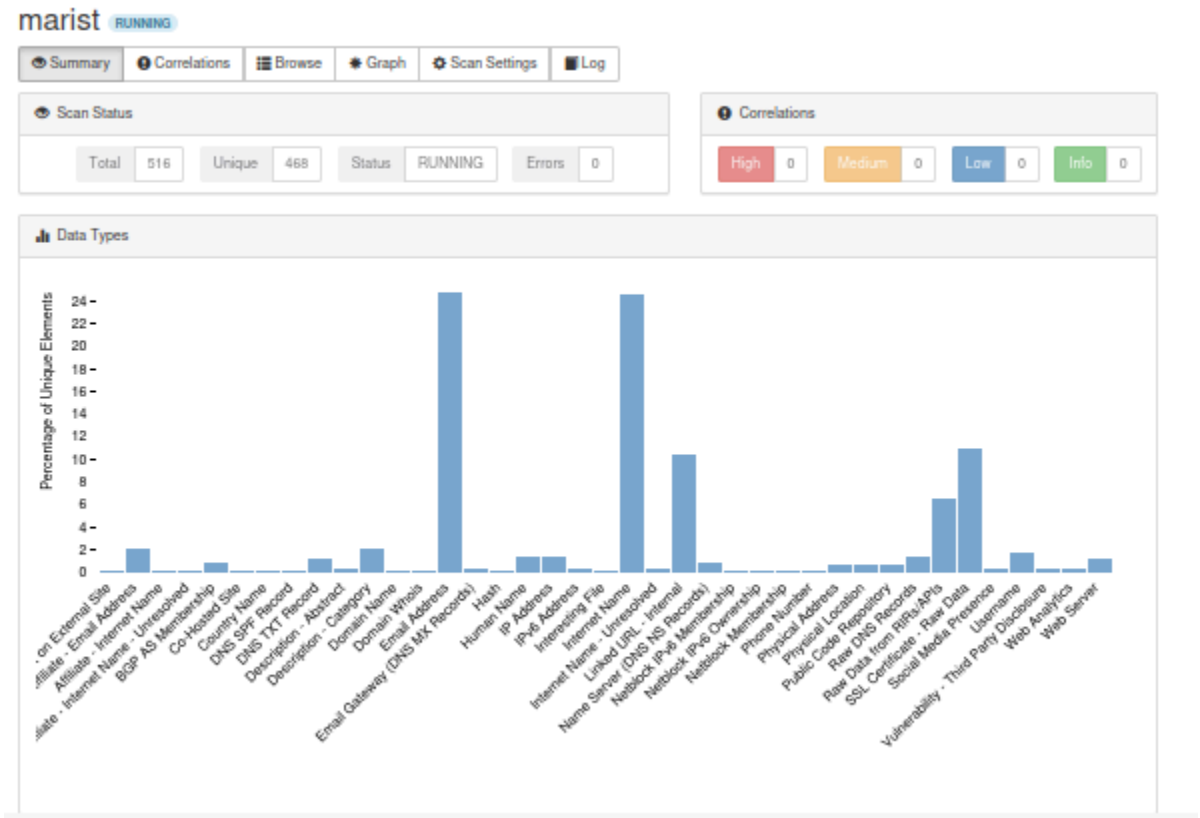




The results I found from Shodan.io are the ports, products, SSL/TLS versions, JARM and JA35 fingerprints. All of these results seem pretty standard for a college's website, I do not see anything out of the ordinary. The value someone could gain from this tool is probably the specific port numbers being 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.



marist RUNNING

Summary | Correlations | Browse | Graph | Scan Settings | Log

Search...

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 06:28:25
Co-Hosted Site	1	1	2023-11-01 06:27:06
Country Name	1	3	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 06:18:13
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 06:28:49
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

marist RUNNING

Summary | Correlations | Browse | Graph | Scan Settings | Log

Search...

Browse / Email Address

Data Element	Source Data Element	Source Module	Identified
.michael.doughty1@marist.edu	marist.edu	sfp_emailformat	2023-11-01 06:18:13
Connor.mcstay1@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:20:03
Emilio.paganyourno1@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:20:03
Jack.McKenna1@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:20:03
Julio.Cabrera2@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:20:03
Kathryn.Silberger@marist.edu	marist.edu	sfp_flickr	2023-11-01 06:18:11
Madison.Kaplan1@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:20:03
Mark.Ferraro@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:20:03
Mark.ferraro52@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:20:03
Michael.Cummins1@marist.edu	marist.edu	sfp_pgp	2023-11-01 06:20:03

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.

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/