Jason Hodge

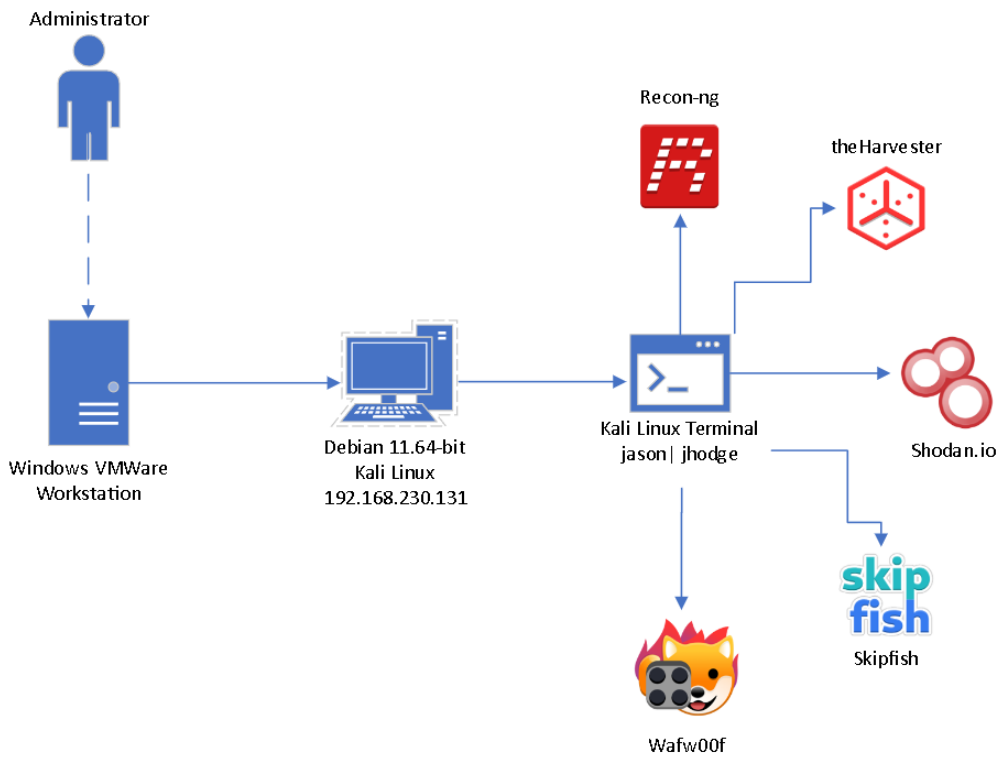
Lab 03 – Open Source Intelligence Gathering

October 25, 2023

Description:

In the first part of this lab, I dove into researching my target organization Marist College. Then, through utilizing free and Open-Source Intelligence (OSINT) framework tools, I was able to find quite the trove of valuable information to conduct penetration tests with Kali Linux tools about the Marist domain. Then through using passive reconnaissance tools I discovered more information about Marist College including Ip addresses, firewalls, subdomains, hosts, networks, etc. Passive tools utilized in this lab include Recon-ng, TheHarvester, Shodan.io, Skipfish, and Wafw00f. All five of these tools are information gathering tools used to find potential vulnerability areas to assist with building an overall profile of a target's security. With the found information I conducted an analysis of each tool and its importance.

Topology:



This is an overview of the entire lab and the passive open-source Kali tools used within my Debian Kali Linux machine on VMWare Workstation.

Key Syntax:

- The name of the Kali tool you are using always goes before the command you are running.
- Various commands to download and run all of these tools are included throughout the report.

Verification:

TASK ONE: Passive Discovery

Some public information I discovered through gathering Open Source Intelligence (OSINT)(OSINT framework) from using Google include:

- Various Marist email addresses with the format firstname.lastname1@marist.edu
- Marist standard phone number is 845-575-3000
    - A whole directory of phone numbers: https://www.marist.edu/directory
- Marist Instagram, Facebook, Twitter(X), LinkedIn, TikTok, YouTube, Pinterest.
- Many web pages: https://www.marist.edu/about/marist-at-a-glance, https://maristpoll.marist.edu/, https://www.marist.edu/marist100, https://www.marist.edu/student-life/campus-services, etc.
- The domain is https://www.marist.edu/

Information below was found utilizing Whois.com:

- Domain Name: MARIST.EDU
- Registrant:
  Marist College
  3399 North Road
  Poughkeepsie, NY 12601
  USA

- Administrative Contact:
  A Williams
  Marist College
  North Road
  Poughkeepsie, NY 12601-1387
  USA
  +1.8455753252
  email@vm.marist.edu

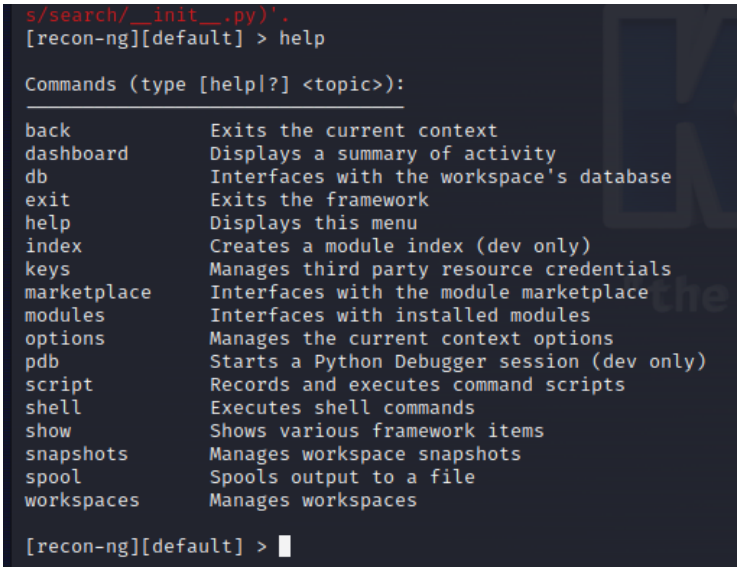
- Technical Contact:
  A Williams
  Marist College
  North Road
  Poughkeepsie, NY 12601-1387
  USA
  +1.8455753252
  email@vm.marist.edu

- Name Servers:
  NS1.MARIST.EDU
  NS3.MARIST.EDU
  NS4.MARIST.EDU
  NS2.MARIST.EDU

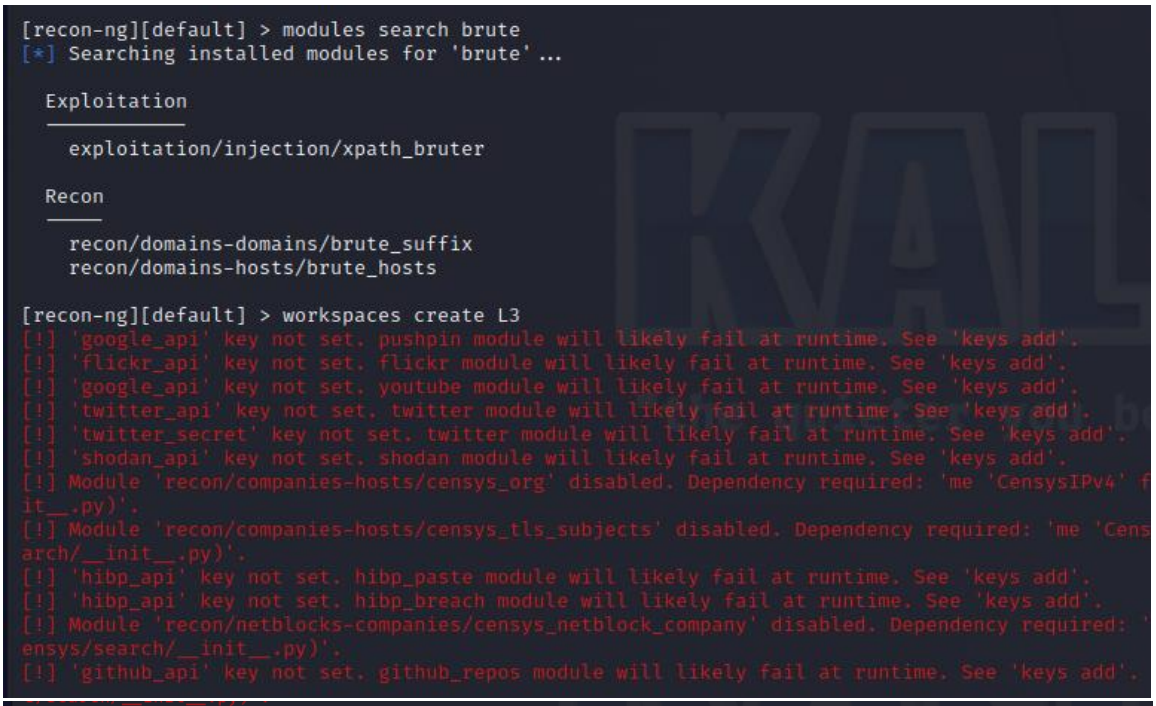
- Domain record activated: 31-Aug-1989
- Domain record last updated: 07-Jul-2023
- Domain expires: 31-Jul-2024
- IP Address ranges 48.100.172.0 - 148.100.172.255 and 148.100.131.0 - 148.100.131.255 (db ip)

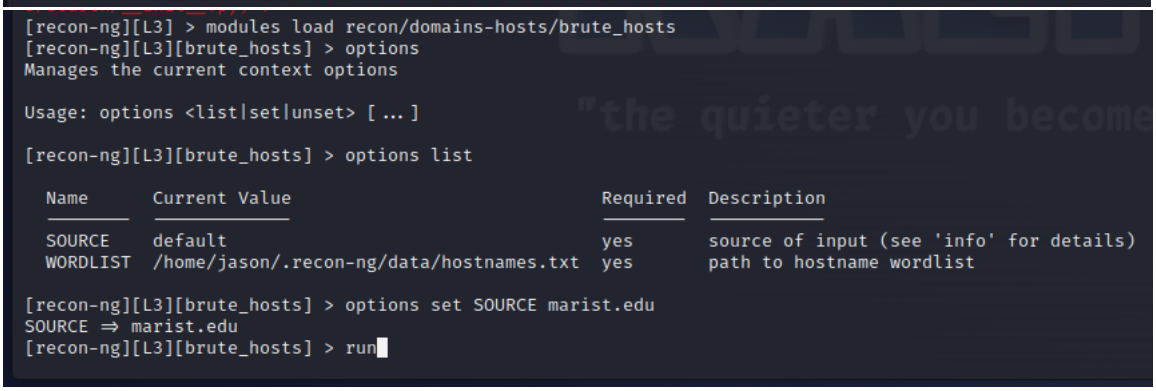
Recon-ng: A reconnaissance framework that is useful to gain opensource intelligence for vulnerability assessment regarding hosts and IP addresses, if applicable, on a domain.

First, in order to use Recon-ng and other Kali Linux environment tools I used the “marketplace install all” command to install all the package modules within Kali.



The help command, “-h” shows the available commands that could be utilized in a recon-ng scan.





In this part, I used the “modules search brute” command to search for the brute module. I used the reconnaissance module “recon/domains-hosts/brute_hosts” to find list of subdomains on the Marist network. I then created a workspace called L3 to load and run the source Marist.edu in.

```
SUMMARY
[*] 221 total (126 new) hosts found.
[recon-ng][L3][brute_hosts] > show hosts

+-------+-----------------------------------------------------------+---------------+--------+---------+----------+-----------+-------+-------------+
| rowid |                           host                            |   ip_address  | region | country | latitude | longitude | notes |    module   |
+-------+-----------------------------------------------------------+---------------+--------+---------+----------+-----------+-------+-------------+
| 1     | www.marist.edu                                            |               |        |         |          |           |       | brute_hosts |
| 2     | admin.marist.edu                                          |               |        |         |          |           |       | brute_hosts |
| 3     | www.ha.marist.edu                                         |               |        |         |          |           |       | brute_hosts |
| 4     | admin.marist.edu                                          | 148.100.2.4   |        |         |          |           |       | brute_hosts |
| 5     | autodiscover.outlook.com                                  |               |        |         |          |           |       | brute_hosts |
| 6     | autodiscover.marist.edu                                   |               |        |         |          |           |       | brute_hosts |
| 7     | atod-g2.tm-4.office.com                                   |               |        |         |          |           |       | brute_hosts |
| 8     | autodiscover.marist.edu                                   | 52.96.109.184 |        |         |          |           |       | brute_hosts |
| 9     | autodiscover.marist.edu                                   | 52.96.35.8    |        |         |          |           |       | brute_hosts |
| 10    | autodiscover.marist.edu                                   | 52.96.69.8    |        |         |          |           |       | brute_hosts |
| 11    | autodiscover.marist.edu                                   | 52.96.182.104 |        |         |          |           |       | brute_hosts |
| 12    | autodiscover.marist.edu                                   | 52.96.111.40  |        |         |          |           |       | brute_hosts |
| 13    | autodiscover.marist.edu                                   | 52.96.87.232  |        |         |          |           |       | brute_hosts |
| 14    | autodiscover.marist.edu                                   | 52.96.9.184   |        |         |          |           |       | brute_hosts |
| 15    | autodiscover.marist.edu                                   | 52.96.109.232 |        |         |          |           |       | brute_hosts |
| 16    | marist.catalog.acalog.com                                 |               |        |         |          |           |       | brute_hosts |
| 17    | catalog.marist.edu                                        |               |        |         |          |           |       | brute_hosts |
| 18    | hera-c.aws.acalog.com                                     |               |        |         |          |           |       | brute_hosts |
| 19    | acalog-production-dir-new-6ee7eb4fb0a2b456.elb.us-east-1.amazonaws.com |          |        |         |          |           |       | brute_hosts |
```

This is part of the list of host subdomains found on the Marist network. We can see that 126 hosts were found. The “show hosts” command expanded the results for easier viewing.

```
[*] 126 rows returned
[recon-ng][L3][brute_hosts] > modules search reporting
[*] Searching installed modules for 'reporting'...

  Reporting
  ---------
    reporting/csv
    reporting/html
    reporting/json
    reporting/list
    reporting/proxifier
    reporting/pushpin
    reporting/xlsx
    reporting/xml

[recon-ng][L3][brute_hosts] > modules load reporting/html
[recon-ng][L3][html] > options
Manages the current context options

Usage: options <list|set|unset> [ ... ]

[recon-ng][L3][html] > options list

  Name      Current Value                                  Required  Description
  --------  ---------------                                --------  -----------
  CREATOR                                                  yes       use creator name in the report footer
  CUSTOMER                                                 yes       use customer name in the report header
  FILENAME  /home/jason/.recon-ng/workspaces/L3/results.html  yes     path and filename for report output
  SANITIZE  True                                           yes       mask sensitive data in the report
```

```
[recon-ng][L3][html] > options set CREATOR J
CREATOR ⇒ J
[recon-ng][L3][html] > options set CUSTOMER Oops
CUSTOMER ⇒ Oops
```

```
[recon-ng][L3][html] > options set FILENAME /home/jason/Documents/Marist_Report.html
FILENAME ⇒ /home/jason/Documents/Marist_Report.html
[recon-ng][L3][html] > run
[*] Report generated at '/home/jason/Documents/Marist_Report.html'.
[recon-ng][L3][html] >
```

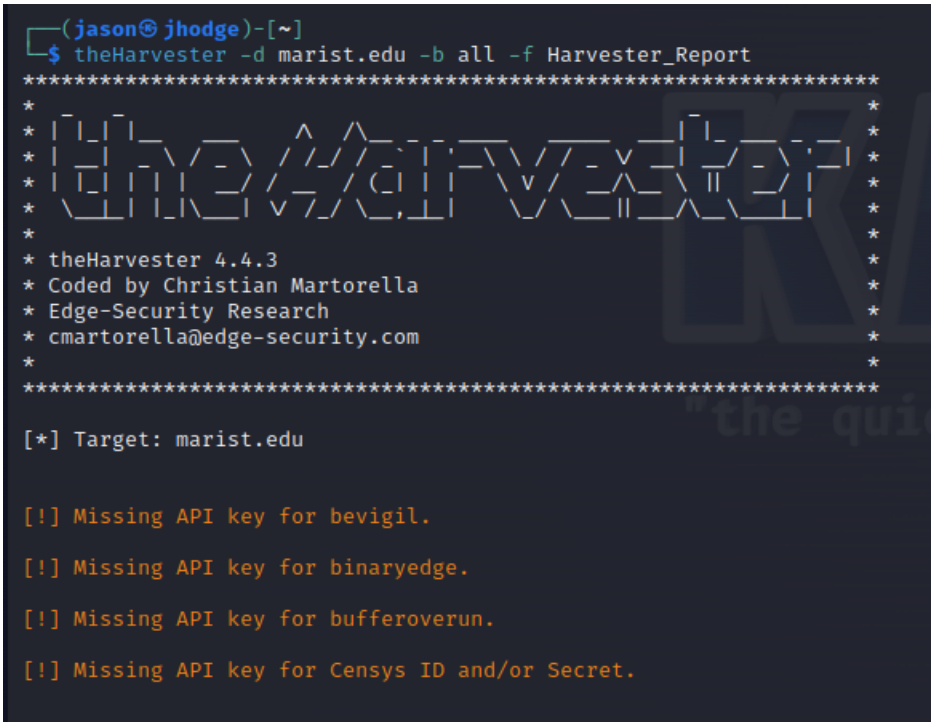
In this last part I wanted to save the results of the test as an html file type. To do this I had to set a creator of the file, a customer, set the file save location, and name the file before generating the report.

Subdomains are susceptible to hijacking, which can be used for various purposes such as hurting companies' reputations, stealing users' data, various phishing scams, etc. Some best practices to prevent against threats like these include constantly updating subdomains, setting up proper firewalls, utilize honeypots to capture the attacker in an isolated environment and learn about them to reinforce the protective layers (HackerNoon)

TheHarvester: A passive reconnaissance tool used to gather names, email addresses, subdomains, hosts, and more from various search engines and other public resources. TheHarvester is normally used for the early stages of a penetration test to fully understand the customer or target being pursued.

```
┌──(jason㉿jhodge)-[~]
└─$ sudo apt install theharvester
[sudo] password for jason:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
  python3-texttable
Use 'sudo apt autoremove' to remove it.
The following packages will be upgraded:
  theharvester
1 upgraded, 0 newly installed, 0 to remove and 1325 not upgraded.
Need to get 679 kB of archives.
After this operation, 67.6 kB of additional disk space will be used.
Get:1 http://kali.darklab.sh/kali kali-rolling/main amd64 theharvester all 4.4.3-0kali1 [679 kB]
Fetched 679 kB in 1s (741 kB/s)
(Reading database ... 392649 files and directories currently installed.)
Preparing to unpack .../theharvester_4.4.3-0kali1_all.deb ...
Unpacking theharvester (4.4.3-0kali1) over (4.2.0-0kali1) ...
Setting up theharvester (4.4.3-0kali1) ...
Installing new version of config file /etc/theHarvester/api-keys.yaml ...
Processing triggers for kali-menu (2023.1.7) ...
```

Here we can see the Kali Linux tool, theHarvester being installed on the machine with the command "sudo apt install theharvester".



Before running any command the tool you are using needs to be initialized ahead of the scan or test you are about to run. In this test, the command “theHarvester -d marist.edu -b all -f Harvester_Report” identifies the Marist domain as what we are searching for and then searches information from all sources. The last part creates a report of the results as both JSON and XML files.

```
54.164.4.253
54.175.250.58
54.210.232.132
54.243.238.66
54.243.250.147
54.81.232.47
54.85.246.96
54.87.189.131
54.88.35.99
64.225.35.74
64.91.243.43
72.52.5.200
88.221.168.234

[*] Emails found: 16
---------------------
admission@marist.edu
anthony.proia@marist.edu
deborah.holtman@marist.edu
graduate@marist.edu
helpdesk@marist.edu
international.studentservices@marist.edu
international@marist.edu
mc.cls@marist.edu
michelle.eggink@marist.edu
registrar@marist.edu
safety@marist.edu
studentfinancialservices@marist.edu
tracey.niemotko@marist.edu
transcript.request@marist.edu
veterans@marist.edu

[*] Hosts found: 13460
---------------------
148-100-128-100.foxnet.marist.edu
148-100-128-101.foxnet.marist.edu
148-100-128-102.foxnet.marist.edu
148-100-128-104.foxnet.marist.edu
148-100-128-105.foxnet.marist.edu
148-100-128-108.foxnet.marist.edu
148-100-128-109.foxnet.marist.edu
148-100-128-11.foxnet.marist.edu
```

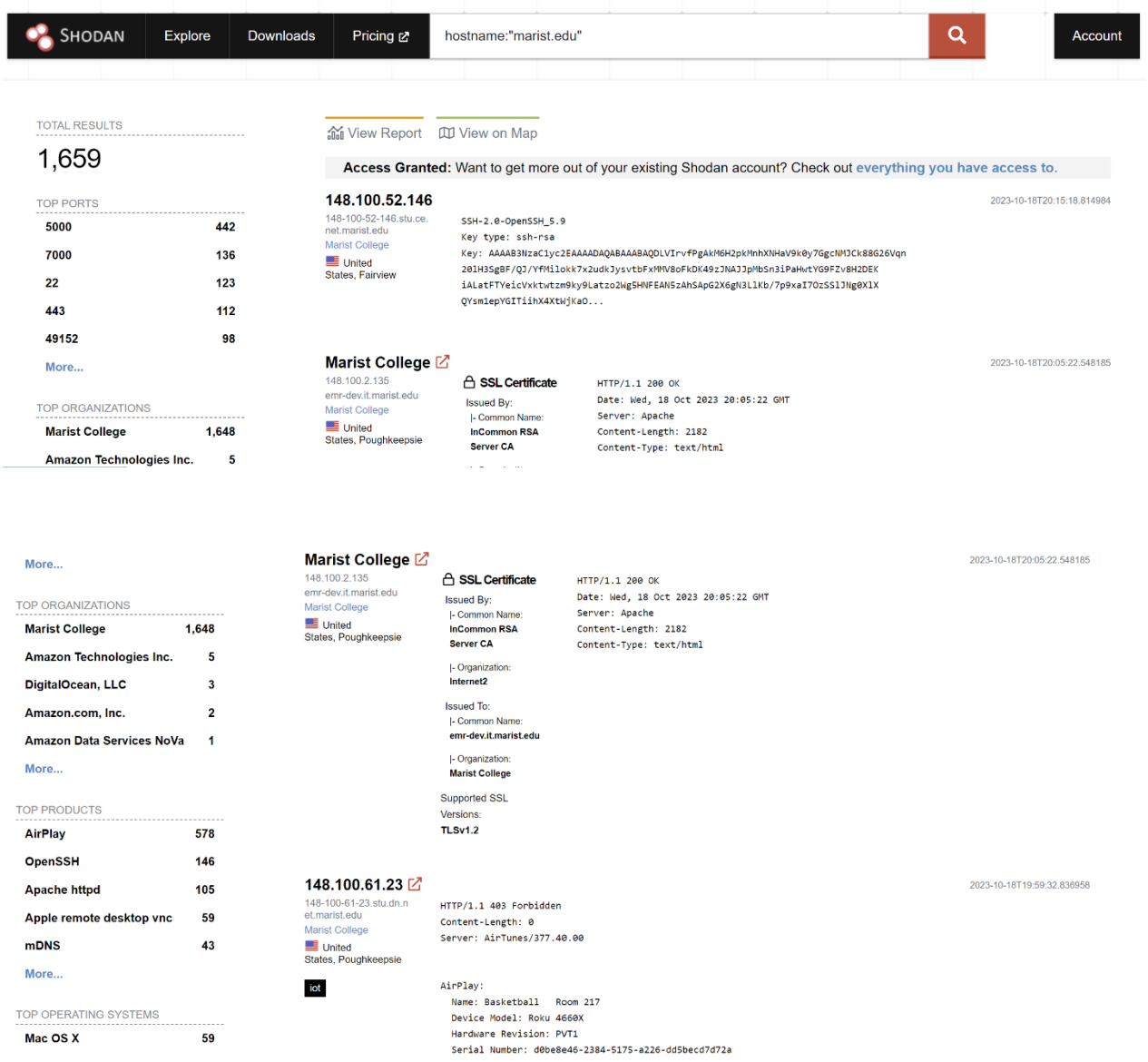
This is a preview of ip addresses, email addresses, and hosts discovered on Marist's network. 13460 is a lot of devices on the foxnet network.

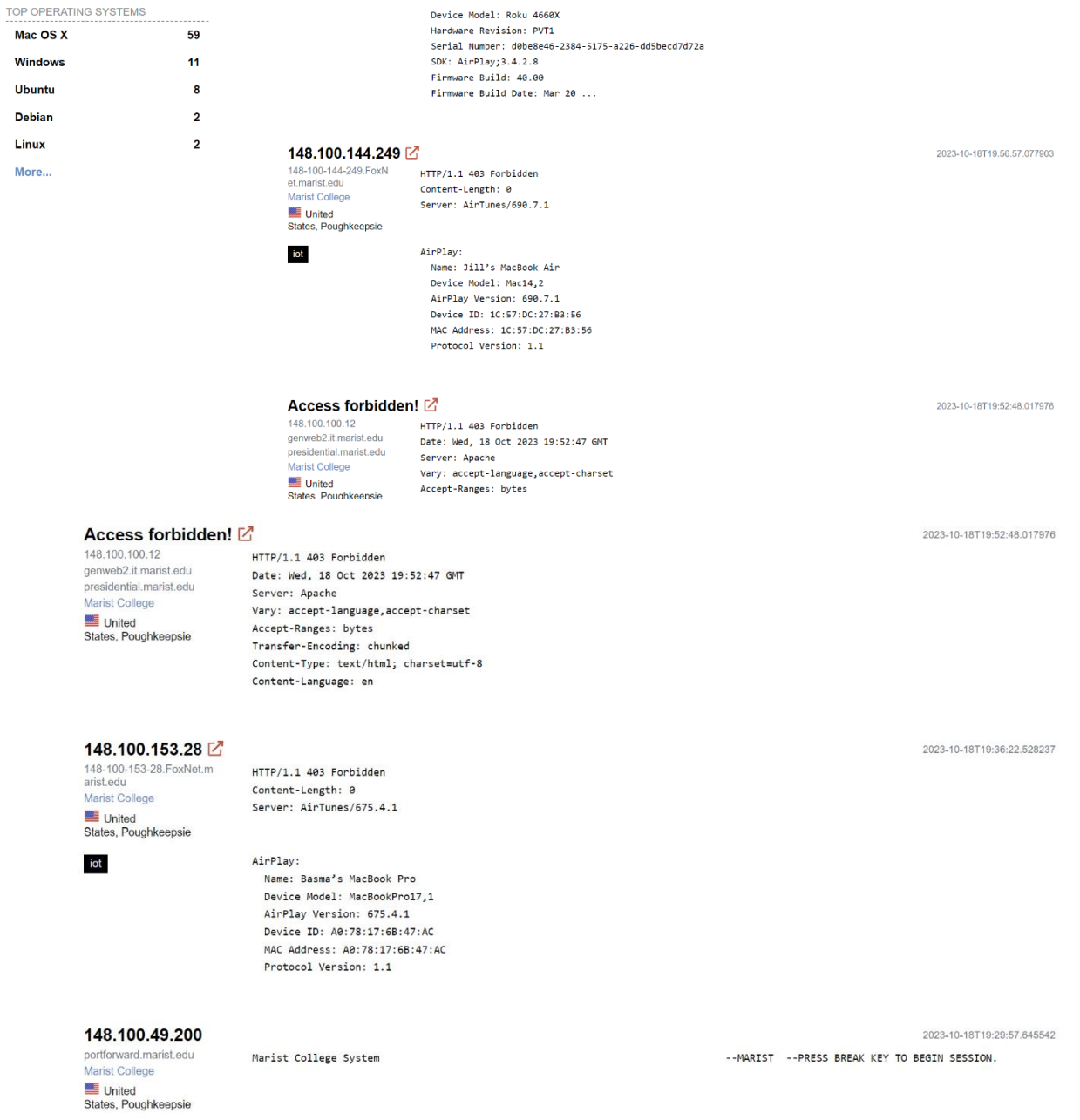
```
xymon-remote.it.marist.edu:64.225.35.74
xymon.it.marist.edu
xymon.it.marist.edu:hobbit.it.marist.edu
xymon.it.marist.edu:hobbit.it.marist.edu.
xymontst.is.marist.edu
xynet.it.marist.edu
xynet.it.marist.edu:10.13.8.62
zcloud.marist.edu
zcloud.marist.edu:148.100.42.42
zos.kctr.marist.edu
zos.kctr.marist.edu:148.100.96.12
zos.kctr.marist.edu:vm.marist.edu
zsakai.marist.edu
zseries.marist.edu
zseries.marist.edu:cart.it.marist.edu
zseries.marist.edu:cart.it.marist.edu.
zvmclass.marist.edu

[*] Reporting started.
[*] XML File saved.
[*] JSON File saved.



┌──(jason㉿jhodge)-[~]
└─$
```

Here we can see that the report was saved as both an XML file and JSON file to the scans folder on the machine.

The result of this test provides a list of Ip addresses, email addresses, and hosts that can all be targeted by various attacking methods such as phishing, ip spoofing, DDoS, malware, etc. These can all be prevented by using best practices such as not opening suspicious emails and changing passwords regularly, keeping software up to date, etc.

Shodan.io: The Shodan.io browser tool is used to find vulnerabilities in systems by regularly crawling the internet for information on network systems. This tool was used to search Marist for devices on its network and provides identifiable information about them.





I ran the Shodan.io browser tool with the command hostname:"marist.edu". With this command I was able to discover information about network devices on Marist's system. What was found pertains to host device information such as Ip address, location, type of device and model, etc. This is just a small portion of what was found.

Shodan Report

`hostname:"marist.edu"`

Total: 1,660

// GENERAL

Countries

United States	1,660

Ports

5000	442
7000	137
22	123
443	112
49152	98

MORE...

Organization

Marist College	1,649
Amazon Technologies Inc.	5
DigitalOcean, LLC	3
Amazon.com, Inc.	2
Amazon Data Services NoVa	1

MORE...

Vulnerabilities

No information available.

Products

AirPlay	579
OpenSSH	146
Apache httpd	105
Apple remote desktop vnc	59
mDNS	43

MORE...

Tags

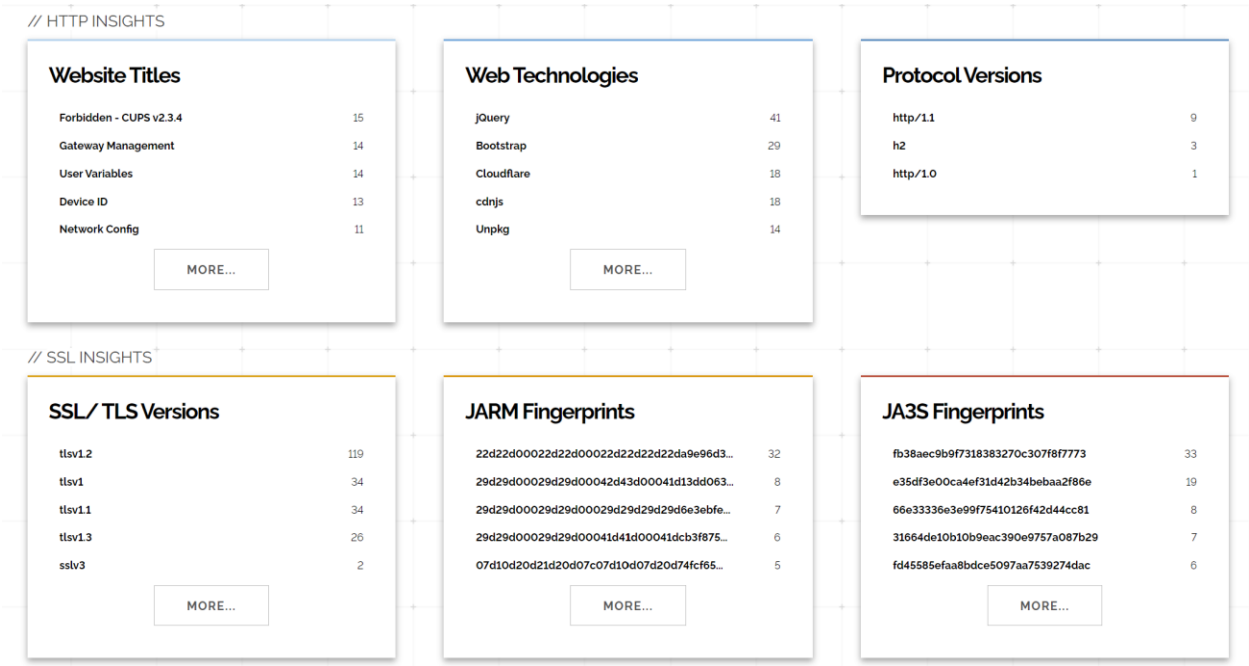
iot	582
database	31
self-signed	26
cloud	11
eol-product	5

MORE...

Operating Systems

Mac OS X	59
Windows	11
Ubuntu	8
Debian	2
Linux	2

MORE...

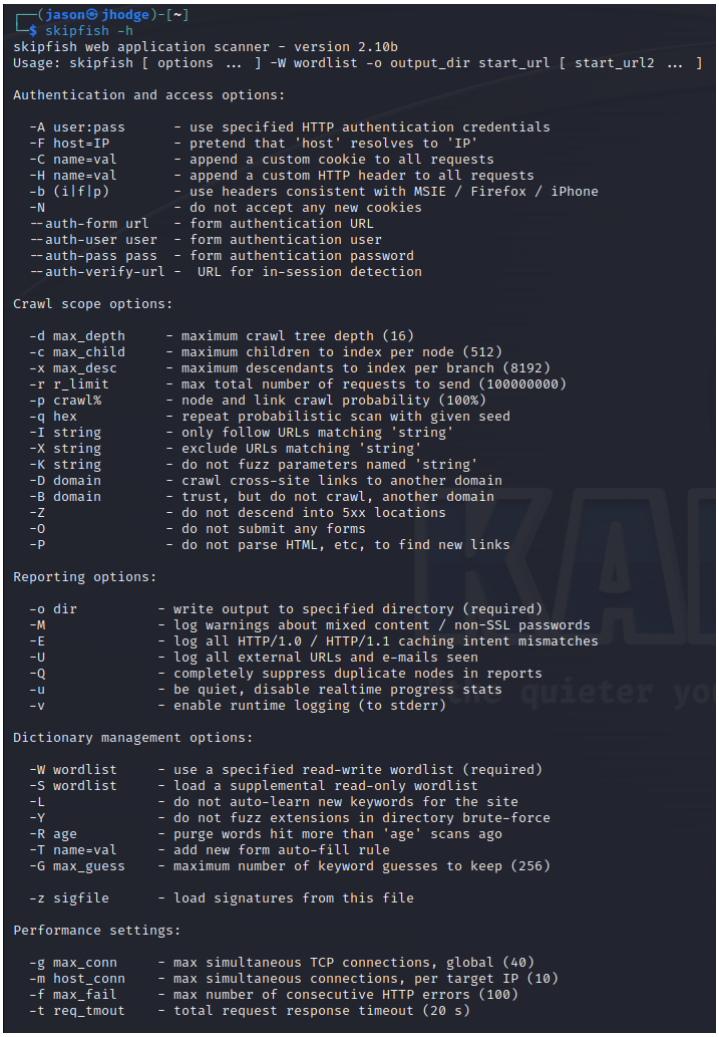


Here we see an overview of the Marist network search information discovered as a report form.

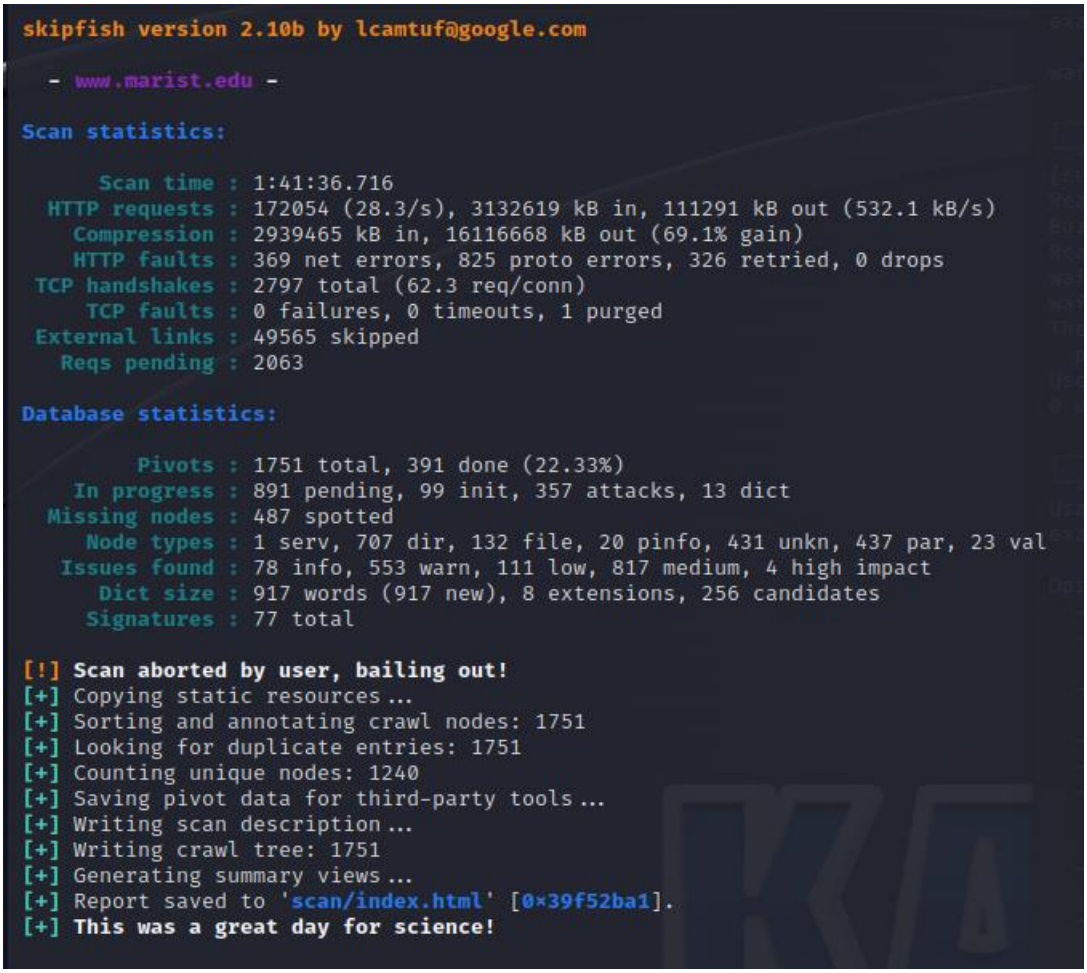
Skipfish: A passive reconnaissance tool used to gain information about system vulnerabilities where a hacker can gain entry to a system. The scan I used did not limit the crawling depth, by using the -o command to adjust a certain time constraint. This simply allows the user to adjust the crawls depth if needed. Skipfish identifies vulnerabilities in a system as high, medium, and low priorities, based on severity.

```
┌──(jason㉿jhodge)-[~]
└─$ sudo apt install skipfish
[sudo] password for jason:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
skipfish is already the newest version (2.10b-2kali7).
skipfish set to manually installed.
The following package was automatically installed and is no longer required:
  python3-texttable
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 1378 not upgraded.
```

Here we can see the passive Kali Linux tool of my choosing, Skipfish being installed on the machine using the command “sudo apt install skipfish”.



The help command, “-h” shows the available commands that could be utilized in a skipfish scan.



This shows the brief results of the skipfish test I ran. In order to gain a substantial amount of data I let this test run for quite a long time and eventually ended the test. As I stated above, I chose not to limit the crawl search depth time in an effort to give the search time to find those high impact potential threats. As you can see, I discovered 4 high impact, 817 medium, 111 low, and 78 information issues.

Most of the results of this scan are all relatively low risk. That being said, there are a couple vulnerable areas for SQL injection and XML or XXE injection attacks, which can potentially be dangerous. SQL injection attacks are where an attacker can query their way into a part of a database through an application page, if this page is a login page it can be even more dangerous as they can get their hands on login information and user records. An XML or XXE injection attack is where an attacker can “interfere with the way an application processes XML data. Successful exploitation allows an attacker to view files from the application’s server and interact with any external or backend systems that the application can access” (OneHackMan). This would be something the Marist cybersecurity team can look into and make sure the system is well protected.

Wafw00f (WAF): A passive reconnaissance web application firewall (WAF) detector tool that sends HTTP requests to find out which WAF is protecting a domain.

```
┌──(jason㉿jhodge)-[~]
└─$ sudo apt install wafw00f
[sudo] password for jason:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
wafw00f is already the newest version (2.2.0-1).
wafw00f set to manually installed.
The following package was automatically installed and is no longer required:
  python3-texttable
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 1377 not upgraded.
```

Here we can see another passive Kali Linux tool of my choosing, Wafw00f being installed on the machine using the command “sudo apt install wafw00f”.

```
┌──(jason㉿jhodge)-[~]
└─$ wafw00f -h
Usage: wafw00f url1 [url2 [url3 ... ]]
example: wafw00f http://www.victim.org/

Options:
  -h, --help            show this help message and exit
  -v, --verbose         Enable verbosity, multiple -v options increase
                        verbosity
  -a, --findall         Find all WAFs which match the signatures, do not stop
                        testing on the first one
  -r, --noredirect      Do not follow redirections given by 3xx responses
  -t TEST, --test=TEST  Test for one specific WAF
  -o OUTPUT, --output=OUTPUT
                        Write output to csv, json or text file depending on
                        file extension. For stdout, specify - as filename.
  -f FORMAT, --format=FORMAT
                        Force output format to csv, json or text.
  -i INPUT, --input-file=INPUT
                        Read targets from a file. Input format can be csv,
                        json or text. For csv and json, a `url` column name or
                        element is required.
  -l, --list            List all WAFs that WAFW00F is able to detect
  -p PROXY, --proxy=PROXY
                        Use an HTTP proxy to perform requests, examples:
                        http://hostname:8080, socks5://hostname:1080,
                        http://user:pass@hostname:8080
  -V, --version         Print out the current version of WafW00f and exit.
  -H HEADERS, --headers=HEADERS
                        Pass custom headers via a text file to overwrite the
                        default header set.
```

The help command, “-h” shows the available commands that could be utilized in a wafw00f test scan.

Here we see the results after running the command “wafw00f marist.edu” which is simply just checking the domain for what type of firewall is protecting a network. Here we see the Marist network is using an AWS Elastic Load Balancer (Amazon) WAF. Load balancers are typically placed as initial layers before getting to the actual firewall, which is a good practice for layering protective services to help prevent potential risks. By knowing the firewall system, a domain is using, it can be susceptible to Ip spoofing, distributed denial of service attacks (DDoS) and malware. Some best practices include following the principle of least privilege where users are granted minimal access required, keeping software up to date, regular security audits, etc. (Yasar, K., & Lutkevich, B). So, it is important to keep relevant and follow best practices with all processes.

Conclusion:

Everything went smoothly in this lab as I was able to accurately run all five of the passive security tools, the three chosen and the two I chose. With these tools I was able to gain quite a bit of knowledge about the Marist domain that in the wrong hands could be used to launch attacks with active discovery techniques.

Furthermore, I believe the results I gained from Skipfish and Wafw00f are beneficial to making an overall profile on my target organization (Marist). More so the results from Skipfish are what interests me the most because it provides information about some potential points of entry to get into vital systems on the Marist network. If you would like me to send you the results of the Skipfish scan, please let me know.

References:

AS6124 Marist College details. IPinfo. (n.d.). https://ipinfo.io/AS6124

Free Whois Lookup. whois.com. (n.d.). https://www.whois.com/whois/

How hackers attack subdomains and how to protect them. HackerNoon. (n.d.). https://hackernoon.com/how-hackers-attack-subdomains-and-how-to-protect-them-rc7j37f2

IP addresses 148.100.131.0 to 148.100.131.255. IP Geolocation API and database. (n.d.-a). https://db-ip.com/all/148.100.131

IP addresses 148.100.172.0 to 148.100.172.255. IP Geolocation API and database. (n.d.-b). https://db-ip.com/all/148.100.172

OneHackMan. (2020, January 4). *Exploiting XML external entity (XXE) injections*. Medium. https://medium.com/@onehackman/exploiting-xml-external-entity-xxe-injections-b0e3eac388f9

OSINT framework. OSINT Framework. (n.d.). https://osintframework.com/

Recon-NG: Kali linux tools. Kali Linux. (2022a, November 16). https://www.kali.org/tools/recon-ng/

WAFW00F: Kali linux tools. Kali Linux. (2022b, August 5). https://www.kali.org/tools/wafw00f/

Yasar, K., & Lutkevich, B. (2023, April 19). *What is a firewall and why do I need one?: Definition from TechTarget*. Security. https://www.techtarget.com/searchsecurity/definition/firewall

YouTube. (2019, April 19). *Use shodan to look for vulnerable targets in a domain: Passive recon*. YouTube. https://www.youtube.com/watch?v=Vn-0p9JEGBY