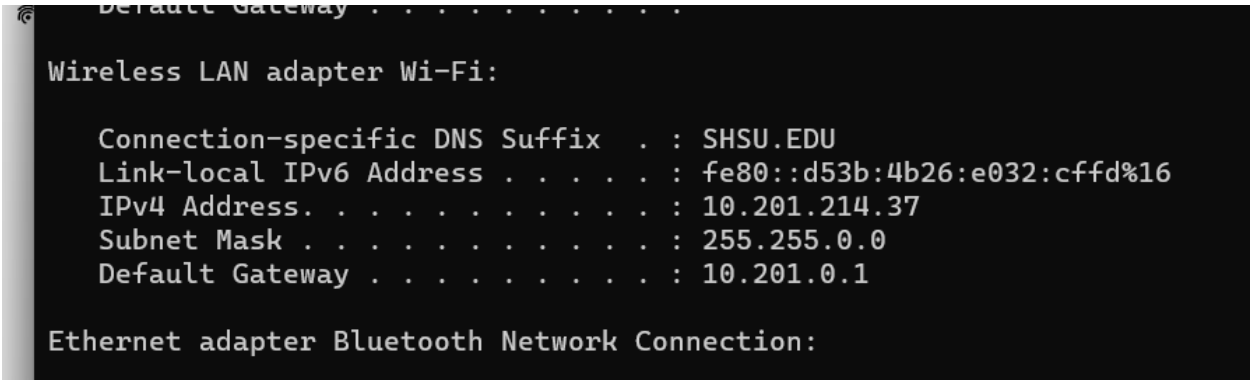
Bryan Barber and Falynne Armstrong

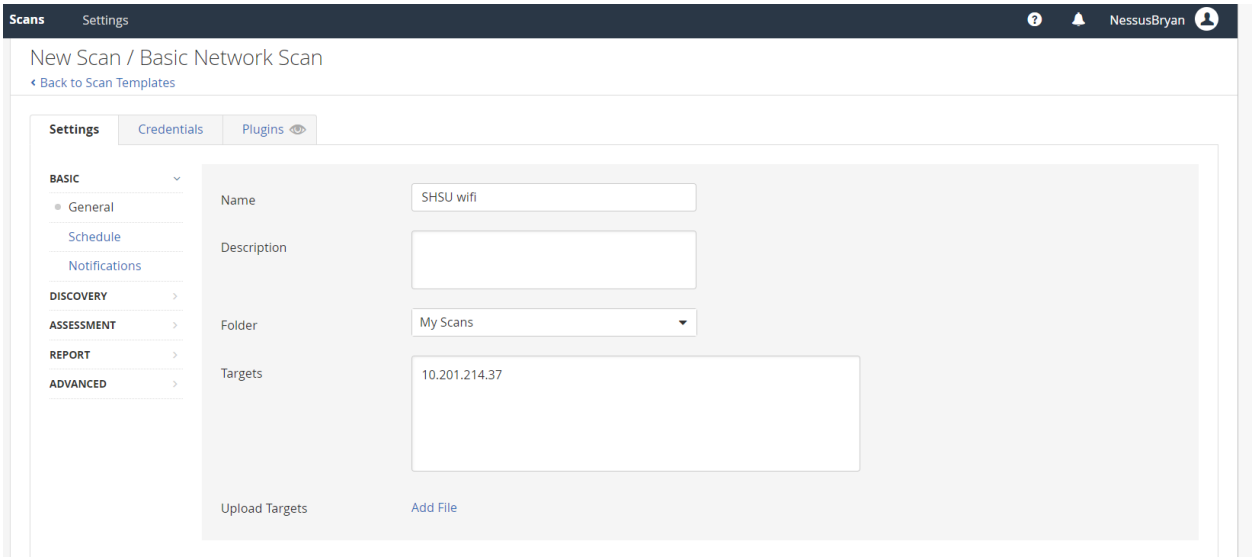
Vulnerability Scanning:

Nessus:

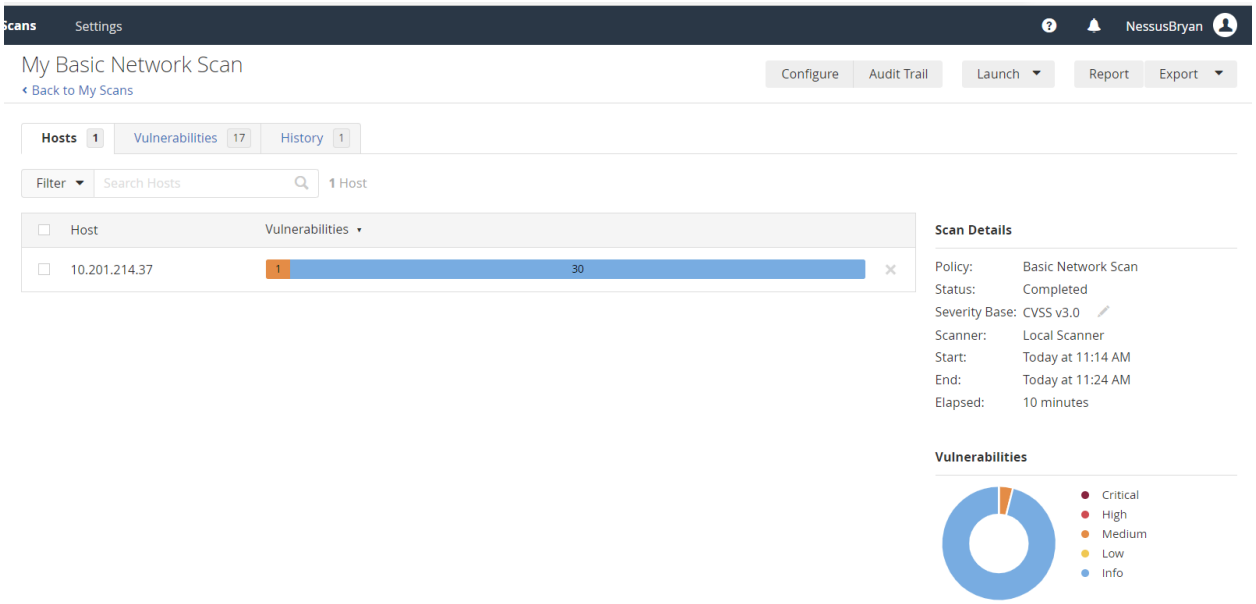
Nessus is a web client that you can use to do things like network and port scans in order to see vulnerabilities in them, and it will categorize them with a threat level and provide a detailed section of each and every vulnerability that comes up. Nessus can also scan for broad types of malware or specific types of malware like wannacry for example. It also has a multitude of other scan options if needed. Nessus has a very nice GUI that makes it simple to use and it is very straightforward and not complicated to interpret and understand the data. Nessus provides detailed reports over every vulnerability that is flagged and it can write a report for you over the entire scan itself. It does all of these operations within the web applicant itself so there is no need for any outside research. Nessus is by far the most verbose tool I have used while also being one of the easiest tools as well, someone who is not well versed with computers or computer security should have no problem with this tool for their own system.



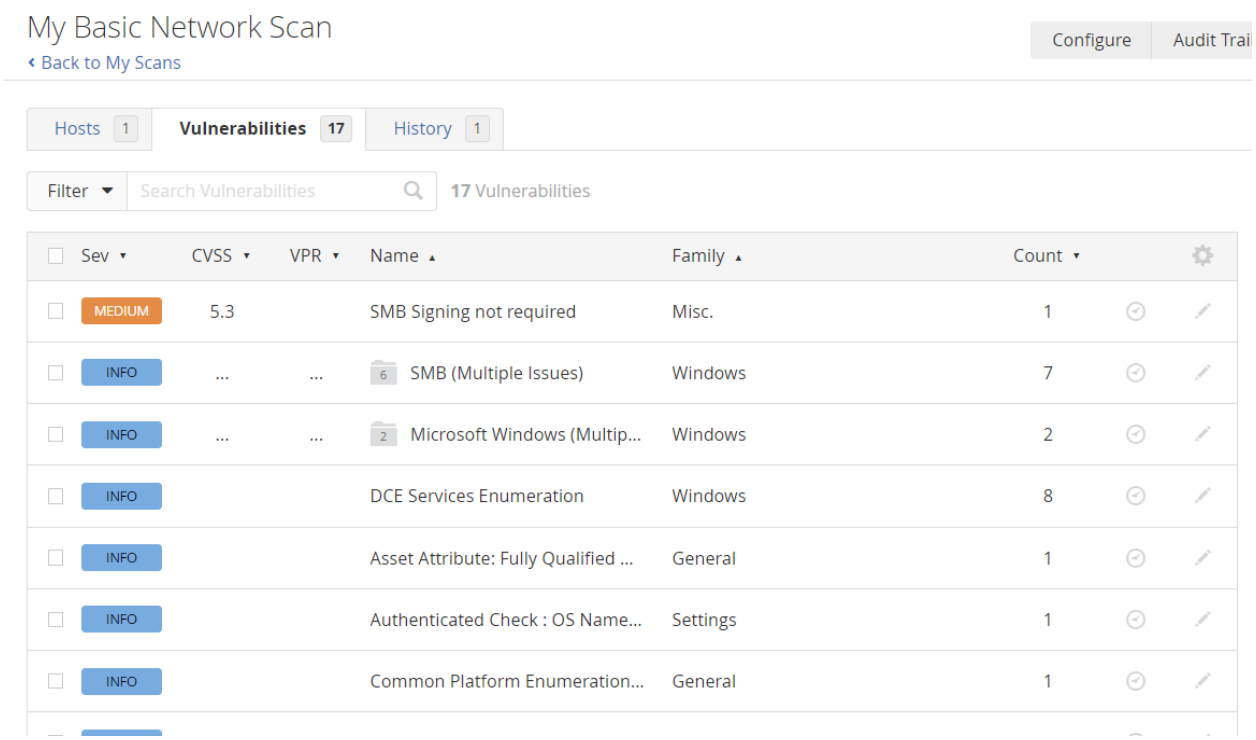
I ran the ipconfig command in the windows terminal to get the IP of my system while on SHSU.EDU wifi.



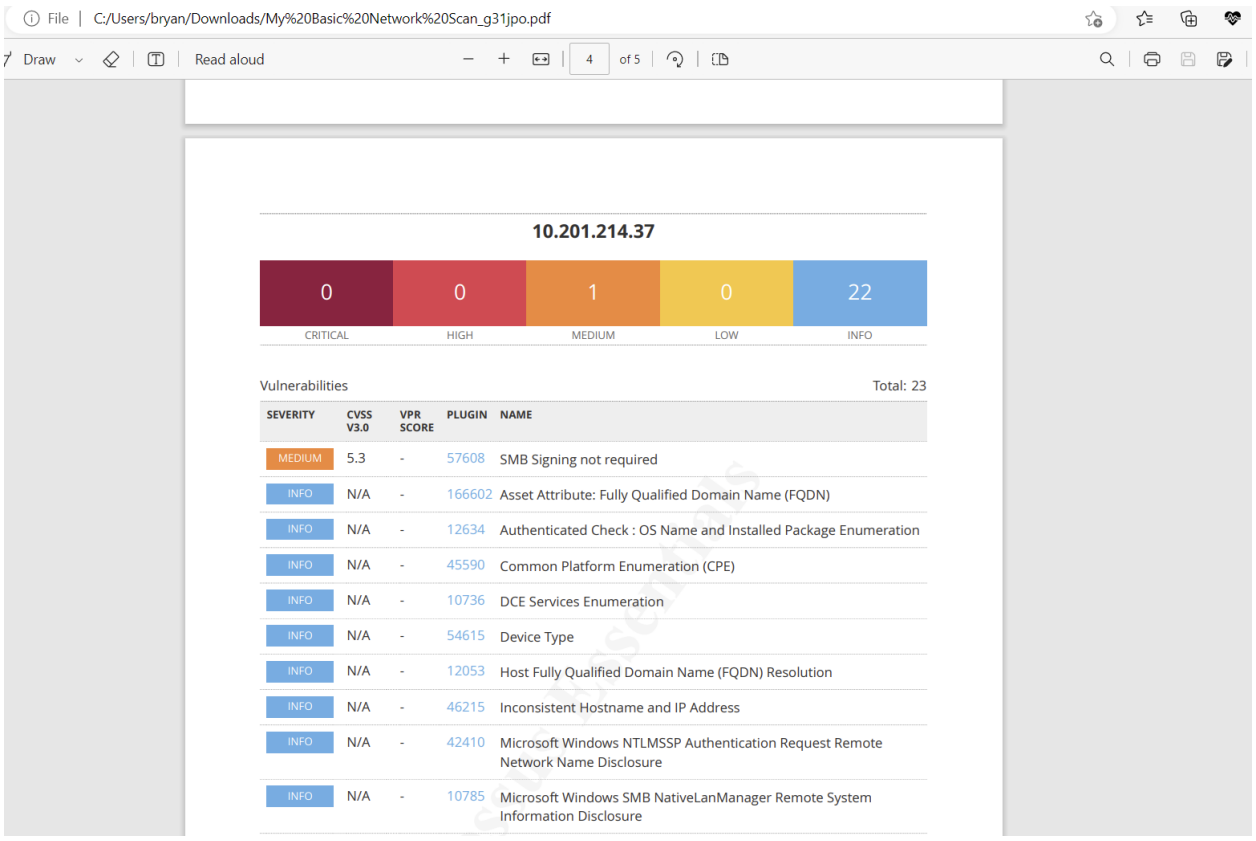
You would then go to the Nessus Essentials web application and create a scan with the IP you got from the command prompt.



Once the scan is complete you can now see all of the vulnerabilities in a neat chart and in avery visible way for the user.



Once you click on the vulnerabilities tab you can see a full list of the vulnerabilities on the system and if you click on any of these you can go to a page with all of the information you need and a suggested action in order to fix this vulnerability.



If you wish to, you can also have Nessus generate a report for you in the form of a .pdf file that has all of the information in a very easy to read format that you can distribute and use for whatever needs you may have.

Nmap:

Nmap can be used as a port scanner and a vulnerability scanner in Kali Linux. It can be used for a multitude of other actions but for this project we will be using it as a vulnerability scanner. The GUI is pretty straightforward, it is just using the terminal and an IP address to find this information. It is relatively easy to use although it does not give as much data as other tools like Nessus. Nmap only lists the services and you have to do further research yourself to see the information of these services and the vulnerabilities of them. Although it is a simple search on the internet to get to the end goal of this project, it is less verbose in the actual tool itself compared to other tools used.

```
┌──(root㉿kali)-[~]
└─# ping shsu.edu
PING shsu.edu (158.135.0.149) 56(84) bytes of data.
64 bytes from bearkatcourse.com (158.135.0.149): icmp_seq=1 ttl=128 time=14.2 ms
64 bytes from bearkatcourse.com (158.135.0.149): icmp_seq=2 ttl=128 time=14.5 ms
^C
── shsu.edu ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 14.241/14.380/14.520/0.139 ms

┌──(root㉿kali)-[~]
```

This is the Ping command used to get the IP address of www.shsu.edu

```
┌──(root㉿kali)-[~]
└─# nmap -Pn -sV 158.135.0.149
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-19 10:59 CDT
Stats: 0:03:00 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 11:03 (0:01:45 remaining)
Nmap scan report for bearkatcourse.com (158.135.0.149)
Host is up (0.12s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE        VERSION
80/tcp   open  http-proxy     F5 BIG-IP load balancer http proxy
443/tcp  open  ssl/http-proxy F5 BIG-IP load balancer http proxy
5060/tcp open  sip?
8080/tcp open  http-proxy?
Service Info: Device: load balancer

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 279.43 seconds
```

If you then run this nmap command with that IP address that you found you will then find the open ports using TCP and the services that the ports use.

You can then look up the service and version of the service to see the vulnerabilities of that port.

Impact of the OpenSSL Infinite Loop Vulnerability CVE-2022-0778

Severity: 5

CVSS: (AV:N/AC:L/Au:N/C:N/I:N/A:P)

Published: 03/15/2022

Created: 04/02/2022

Added: 04/01/2022

Modified: 05/12/2022

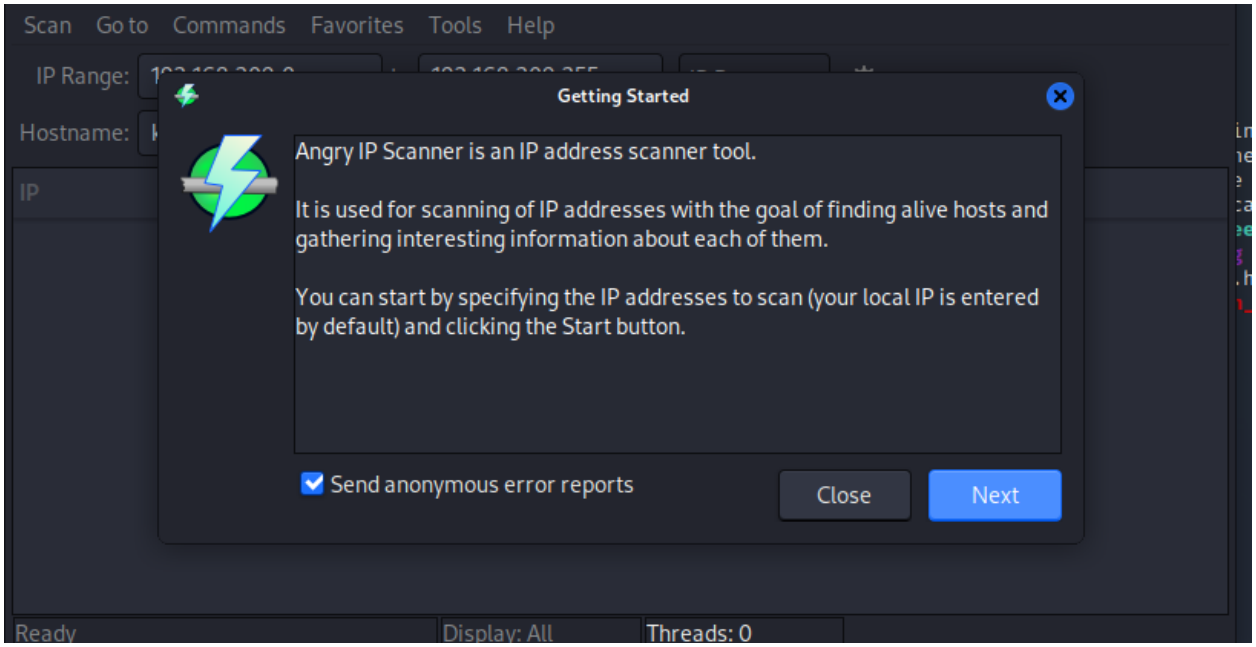
This specific port service that www.shsu.edu uses has an Infinite Loop Vulnerability that is a level 5 severity vulnerability.

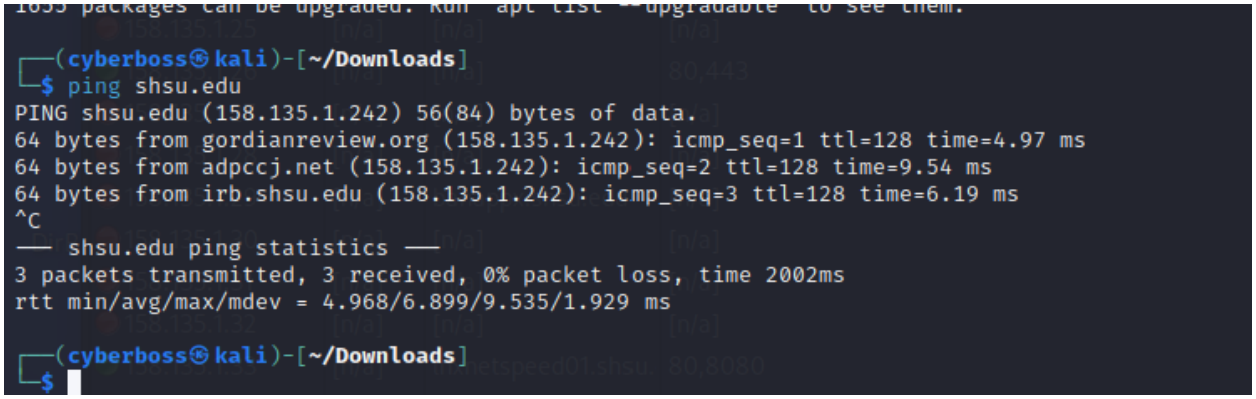
AngryIPScanner:

“Angry IP scanner is a very fast IP address and port scanner.

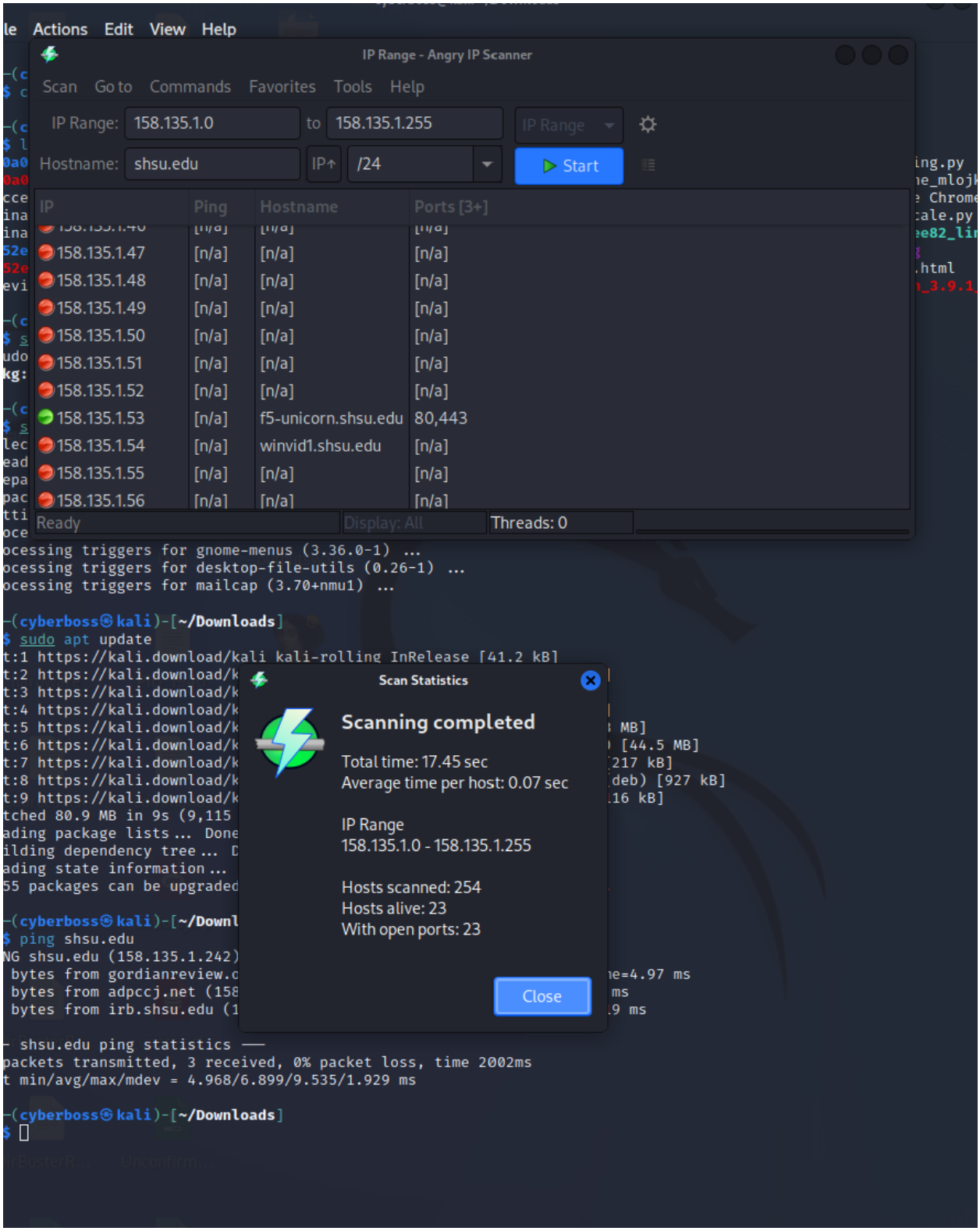
It can scan IP addresses in any range as well as any their ports. It is cross-platform and lightweight. Not requiring any installations, it can be freely copied and used anywhere.

Angry IP scanner simply pings each IP address to check if it’s alive, then optionally it is resolving its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be extended with plugins.”

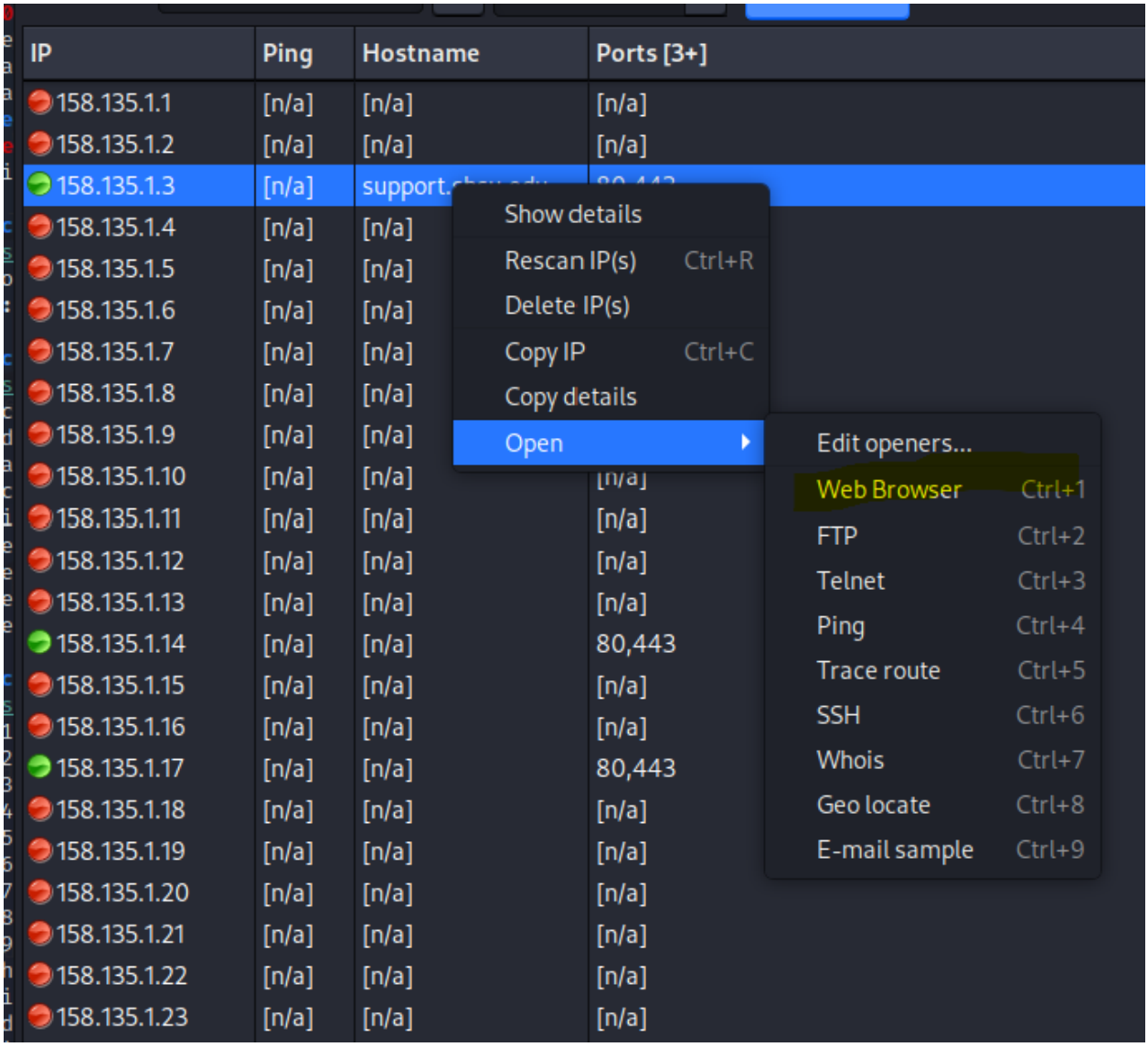




To find our targeted IP address, I was able to ping the website shsu.edu within terminal

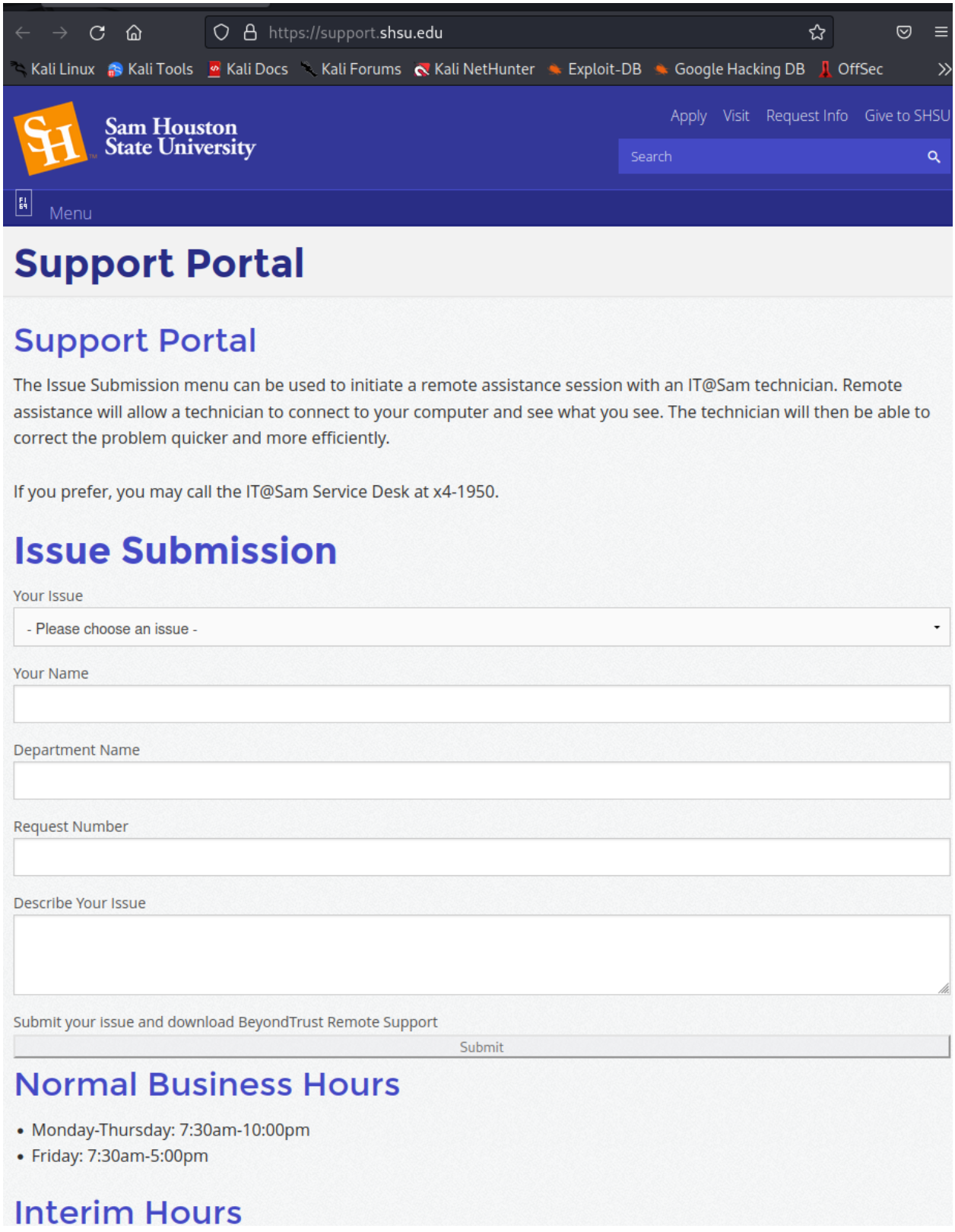


After finding the IP address I inserted the IP and did a wide range scan within its range, and adding the host name as well to find any subdomains, and to find any open ports.



After running the scanner I was able to view the many IPs under shsu.edu, and observe the alive and dead IPs within the network. With this tool one is able to view the subdomains for example I was able to retrieve that shsu.edu has a subdomain of support.shsu.edu. By right-clicking the options of the following subdomain I was able to retrieve and open the website that follows. Although the tool has many other features for educational purposes I only used the web browser option.

Green light - alive IP address
Red light- dead IP address


https://support.shsu.edu
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Sam Houston State University
Apply
Visit
Request Info
Give to SHSU
Search
Menu
Support Portal
Support Portal
The Issue Submission menu can be used to initiate a remote assistance session with an IT@Sam technician. Remote assistance will allow a technician to connect to your computer and see what you see. The technician will then be able to correct the problem quicker and more efficiently.
If you prefer, you may call the IT@Sam Service Desk at x4-1950.
Issue Submission
Your Issue
- Please choose an issue -
Your Name
Department Name
Request Number
Describe Your Issue
Submit your issue and download BeyondTrust Remote Support
Submit
Normal Business Hours
Monday-Thursday: 7:30am-10:00pm
Friday: 7:30am-5:00pm
Interim Hours