Ramdhanush Venkatakrishnan
rvenka26

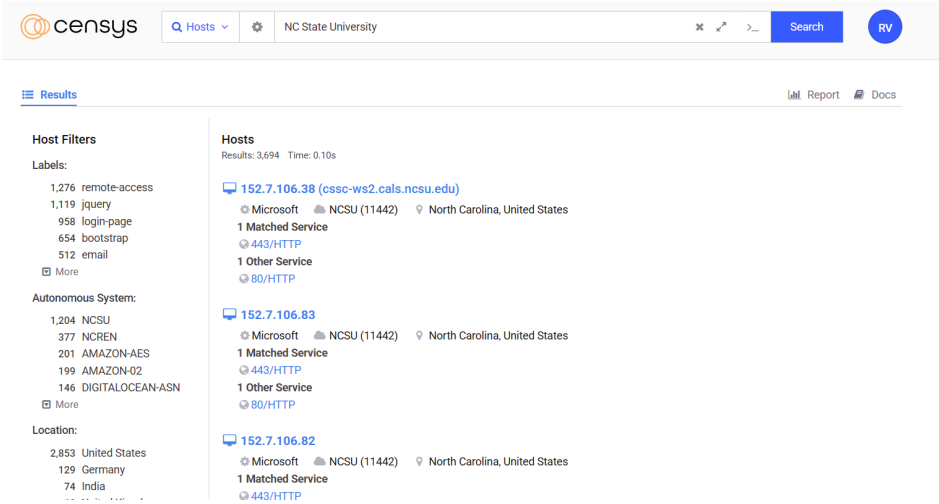
Mini Project 2 Report

Part 1

Some of the IPv4 blocks owned by NC State include:

CIDR Block	Network Name	AS Number	AS Name
152.7.0.0/16	NCSU2	AS11442	NCSU, US
152.1.0.0/16	NCSU	AS11442	NCSU, US
152.14.0.0/16	NCSU3	AS11442	NCSU, US

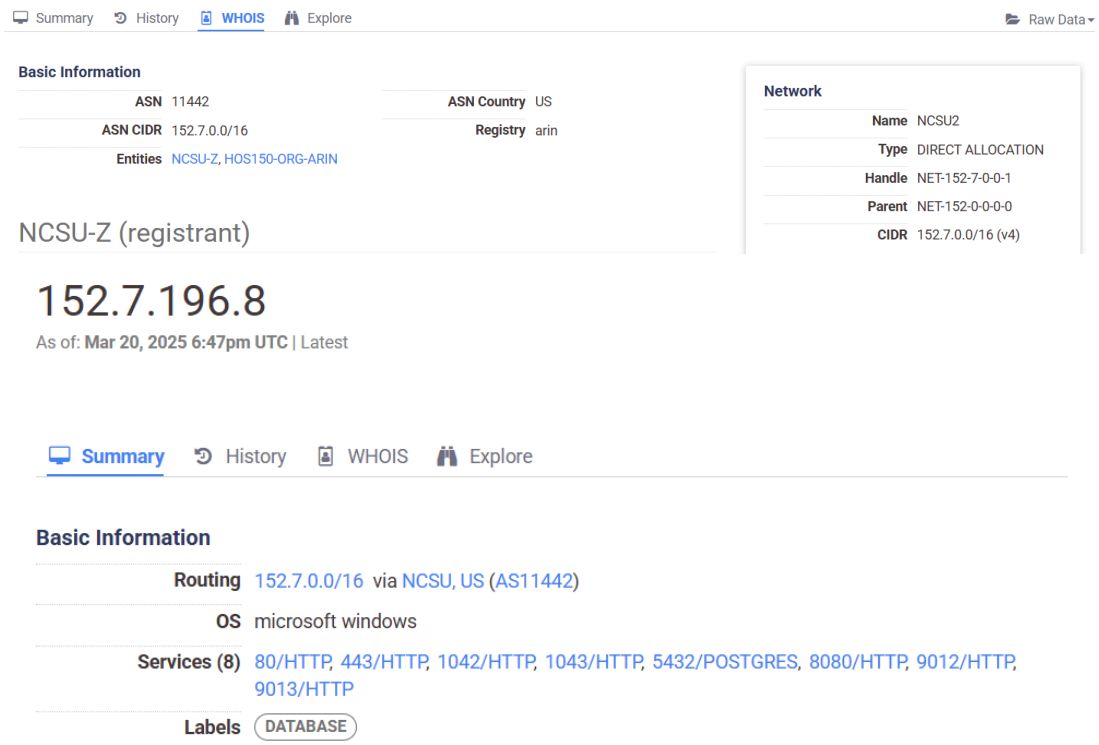
The natural starting place for the search was a query in Censys for "NC State University".



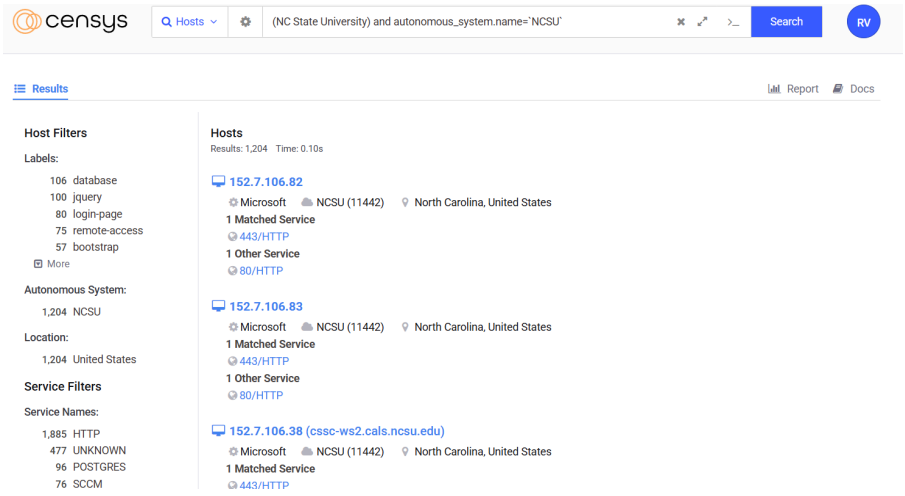
The other details such as the CIDR block, ASN, AS name were found within individual host pages.

Ramdhanush Venkatakrishnan
rvenka26

152.7.196.8



Following this, the individual hosts were filtered to cover unique networks within the autonomous system.



Ramdhanush Venkatakrishnan
rvenka26

152.1.47.61

As of: **Mar 20, 2025 6:58pm UTC** | Latest

Summary History WHOIS Explore

Basic Information

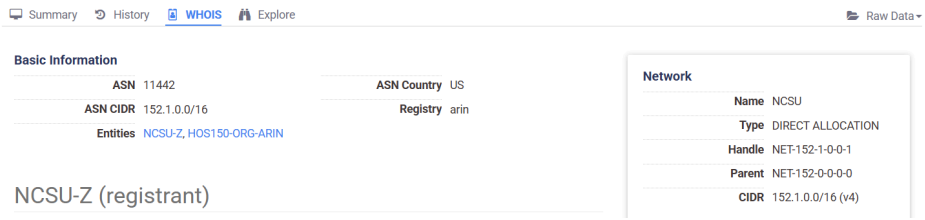
Routing 152.1.0.0/16 via NCSU, US (AS11442)

OS Microsoft Windows

Services (10) 80/HTTP, 3071/UNKNOWN, 5013/UNKNOWN, 5015/HTTP, 5357/HTTP, 8020/UNKNOWN, 9875/UNKNOWN, 17500/UNKNOWN, 49259/UNKNOWN, 49260/UNKNOWN

Labels BOOTSTRAP JQUERY LOGIN PAGE

152.1.47.61



152.14.44.55

As of: **Mar 20, 2025 6:37pm UTC** | Latest

Summary History WHOIS Explore

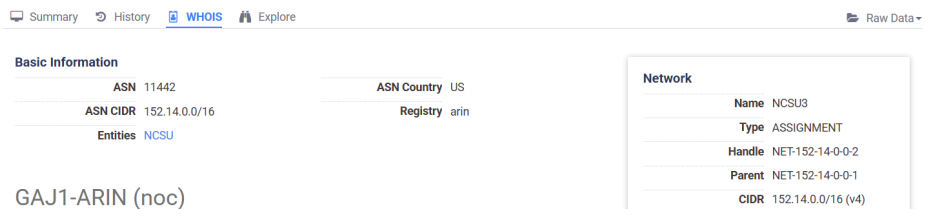
Basic Information

Routing 152.14.0.0/16 via NCSU, US (AS11442)

Services (4) 80/HTTP, 443/HTTP, 3911/HTTP, 8080/HTTP

Labels JQUERY NETWORK.DEVICE.WEB UI PRINTER

152.14.44.55

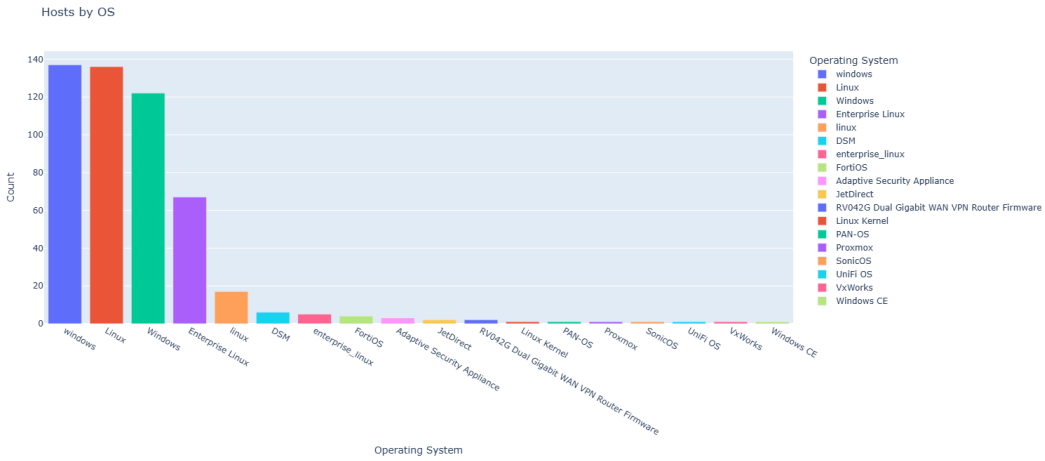


Ramdhanush Venkatakrishnan
rvenka26

Part 2

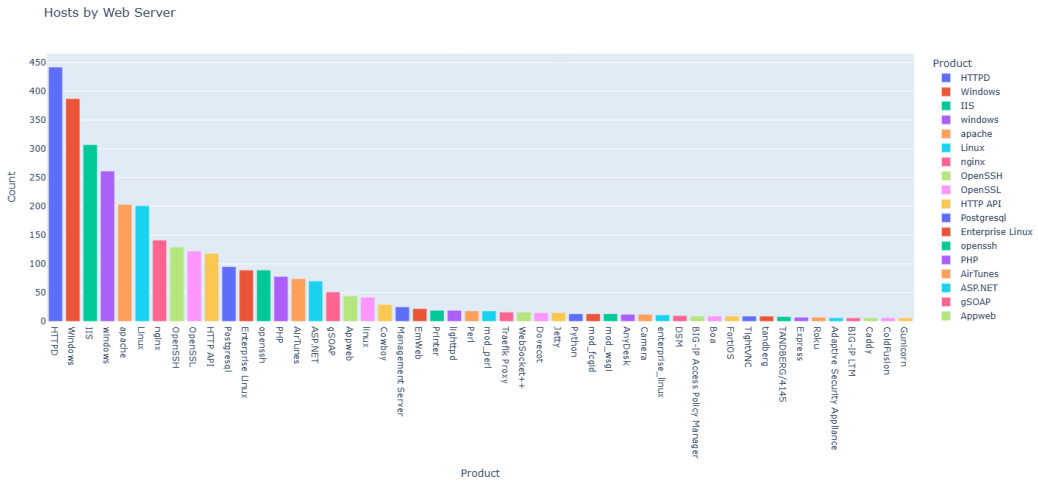
The network blocks identified were investigated using the Python API for Censys. The API was queried to collect data and streamline it into a data structure. The statistics collected subsequently were plotted using Plotly. Some insight into the networks scanned are:

1) Hosts by Operating System



The number of systems under each type of operating system were listed as shown. The most obvious conclusion drawn is that Windows is the most popular choice of operating system for large scale servers. There are many reasons for this, but the reason here is the number of Windows hosts, which outnumber the combined total of all flavours of Linux.

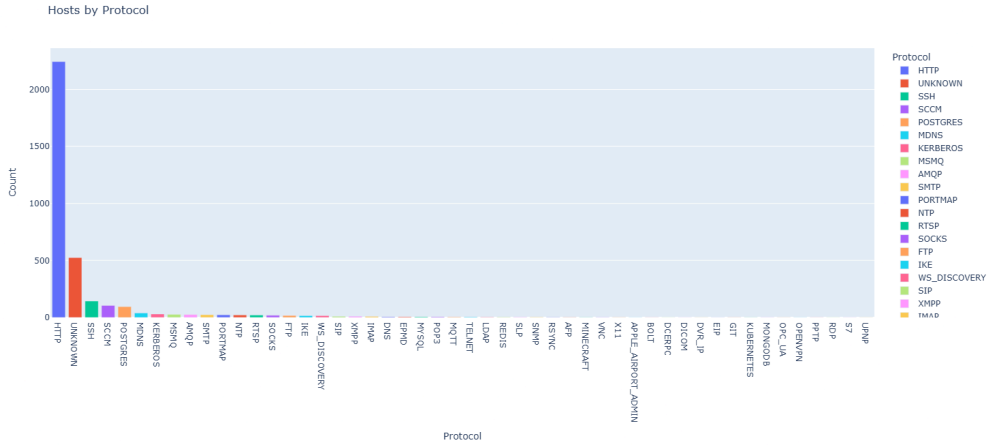
2) Hosts by Web Server



Ramdhanush Venkatakrishnan
rvenka26

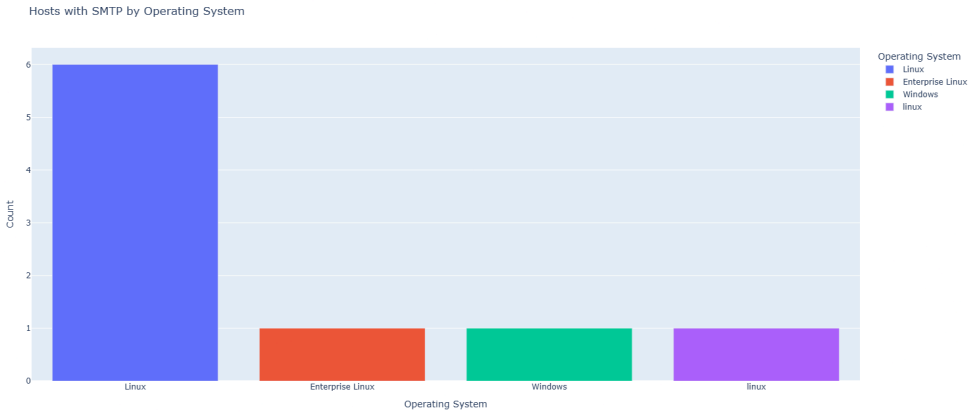
The number of systems running different types of software were listed as shown. The top three software being run are Windows, HTTPD, and IIS. Of these, two (HTTPD and IIS) are web server architectures, and two (Windows and IIS) are part of the Windows family of softwares. It can also be observed that adding the double entries for Windows makes it the highest hosted software.

3) Hosts by Protocol



The above diagram shows the distribution of hosts by the protocol they run. The most used is obviously HTTP, owing to the nature of networked systems. However, SSH is also used by a fair number of systems. SCCM is also a common protocol, used for deploying and configuring the network systems.

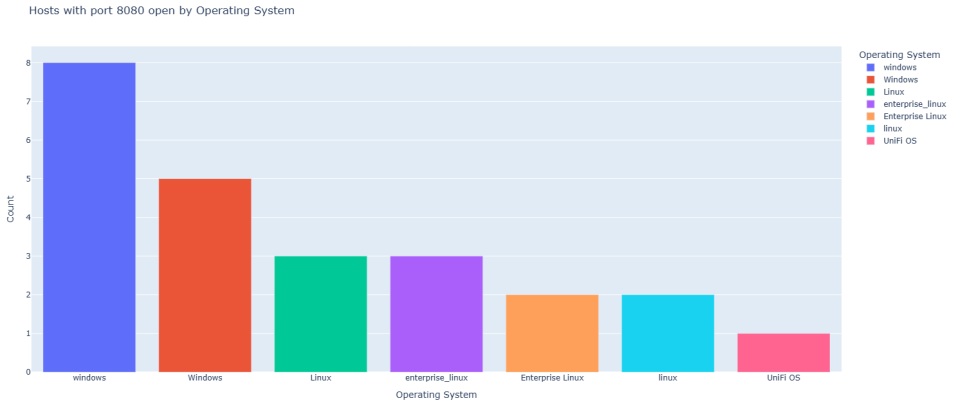
4) Hosts running SMTP by Operating System



The above diagram shows the operating systems preferred by hosts running SMTP. The main takeaway is the overwhelming preference

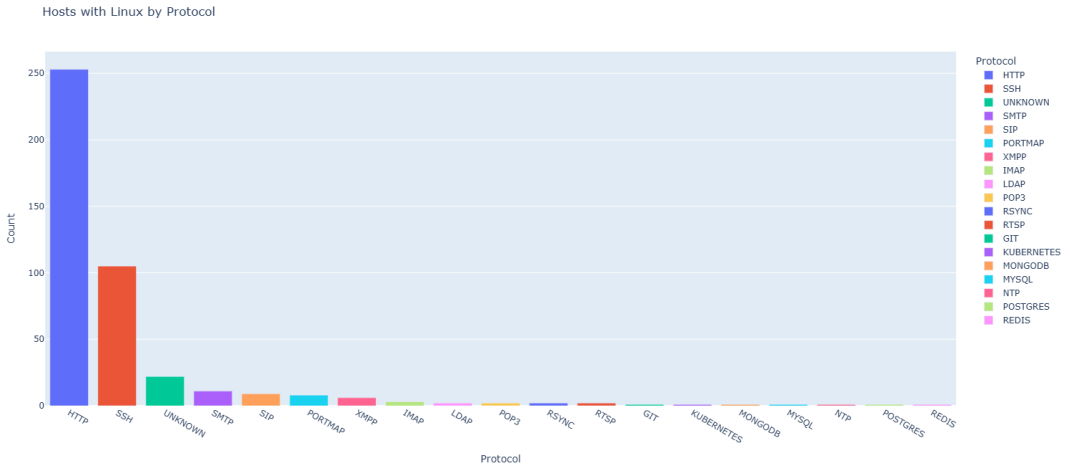
for Linux variations, making it the clear choice. The usage of Windows can also be noted for hosting email servers.

5) Hosts with port 8080 open by Operating System



The number of hosts with an open 8080 port were categorized under their operating system as shown above. The Windows variations closely overtake the Linux in terms of numbers, making both close competitors. The usage of 8080 suggests usage of HTTP and web server activities for development, testing etc. Another interesting thing to note is the presence of UniFi OS, which reveals more about the underlying network stack used, and could be useful information for OSINT research.

6) Hosts running Linux by Protocol

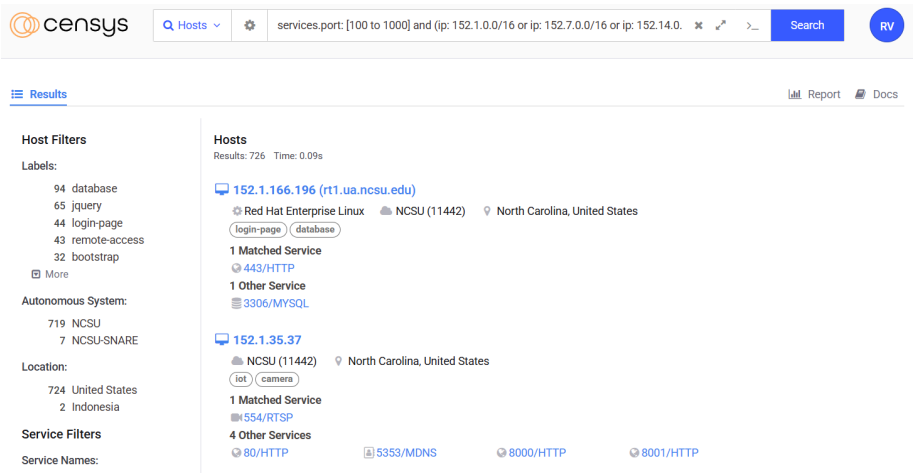


Linux being a recurring choice for a lot of network applications, this graph shows the protocols commonly used by Linux hosts in the network. The majority just use the widely

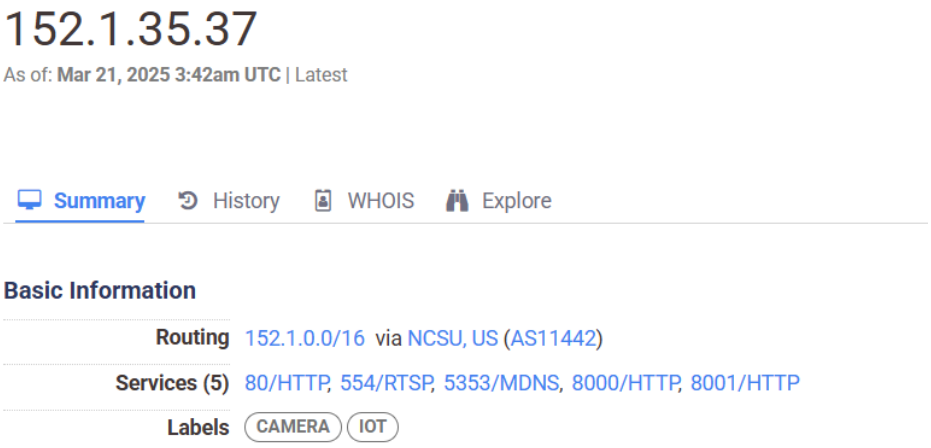
common HTTP protocol. But the second highest is SSH, which is useful in making remote connections.

Part 3

The approach to finding interesting security phenomena in the network was done by studying the most common ports used in a network setting. In addition to the ports used by the hosts on the network (in Part 2), there are a lot of common ports that may be associated with vulnerabilities. Thus, searching for specific ports yielded good results when referenced with vulnerability databases. A Censys query was made to identify such hosts.



Two hosts of particular interest are:
1) 152.1.35.37



This host is part of NC State's autonomous system (NCSU, US) within the 152.1.0.0/16 IPv4 block. This device is labeled as an

IoT/Camera device. The main ports of interest are ports 5353 and 554.

Port 5353 is used by Multicast DNS, which is useful for network discovery in an IoT setting - endpoints could use it to announce their presence to a new node in the network. However, this is a possible cause for concern due to denial of service (DoS)attacks owing to assertive behavior like above. Some common CVEs associated with this port are CVE-2017-6519, CVE-2017-6520, CVE-2015-0650. All of them amplified traffic using special packets and/or source addresses to cause DoS.

Port 554 is used by Real Time Streaming Protocol (RTSP) to accept connection requests from clients. However, insufficient authentication could lead to problems as well. Issues like CVE-2013-4985 and CVE-2013-1596 both demonstrate this - the lack of or insufficient access controls could lead to authentication bypass or adversary access to the video stream.

2) 152.1.109.117

This host is part of NC State's autonomous system (NCSU, US) within the 152.1.0.0/16 IPv4 block. The device has multiple labels, but the main ports of interest are ports 4567 and 110.

Port 4567 is not associated with a well known protocol or service, but has a history of CVEs. Attackers in CVE-2023-5157 used simple port scans to cause uncontrolled consumption of network resources, leading to a DoS ultimately. In an older

instance in CVE-2012-2606, adversaries abused lack of authentication to mount replay attacks and send arbitrary messages to the affected system's display.

Port 110 is well known to be associated with Post Office Protocol version 3 (POP3), one of the most commonly used protocols to retrieve mail from a server. However, this also means that it is the target of many malicious attempts at compromise, of which successful ones like in CVE-2024-24736 are especially dangerous. In this attack, the adversaries managed to cause a remote DoS by using a very long string that couldn't be processed by the victim machine.

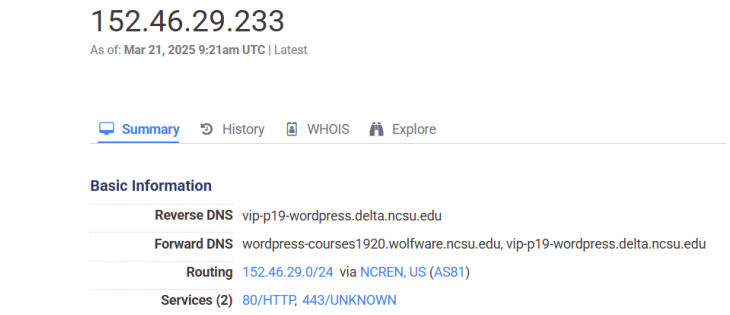
The issues of DoS and weak authentication are recurring and relevant for network systems. To prevent them altogether, the easiest thing would be to disable unused ports, avoiding the problem completely. While this works for obscure, unwanted port numbers, more commonly used standard ports like POP3 can't be disabled, and more often than not, the service needs to be operated on ports while ensuring secure communications. The best way to solve this problem is to use the secure versions of protocols whenever available and applicable. Even otherwise, strong encryption and authentication mechanisms must be put into place so that the wrong person does not obtain access to potentially sensitive data.

Part 4

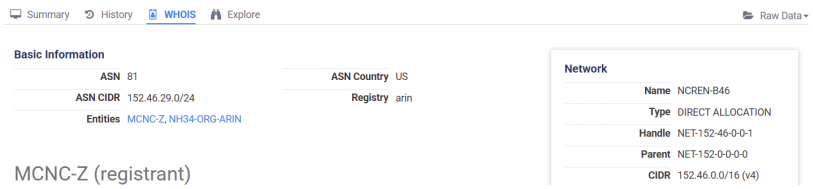
The search for "NC State University" in Part 1 yielded not only systems from within NC State's AS (NCSU, US), but also individual systems from other autonomous systems, notably the NCREN autonomous system (NCREN, US) with an AS number AS81. More details on these hosts were obtained by querying the Python API for DNS records. Some of them are:

1) 152.46.29.233 - vip-p19-wordpress.delta.ncsu.edu

Ramdhanush Venkatakrishnan
rvenka26

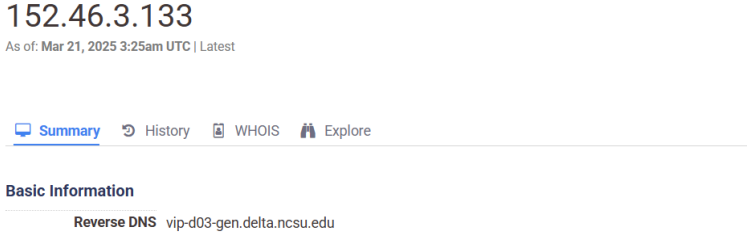


152.46.29.233

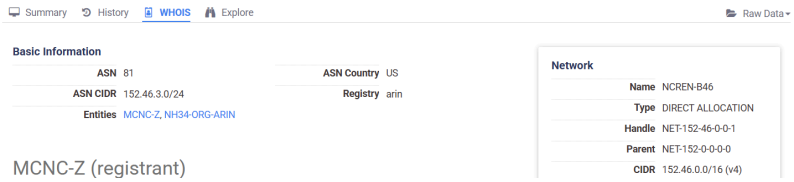


MCNC-Z (registrant)

2) 152.46.3.133 - vip-d03-gen.delta.ncsu.edu



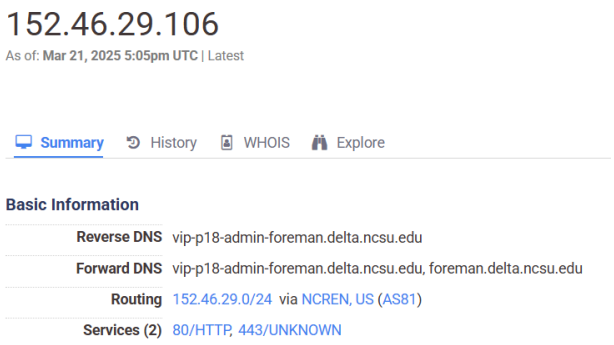
152.46.3.133

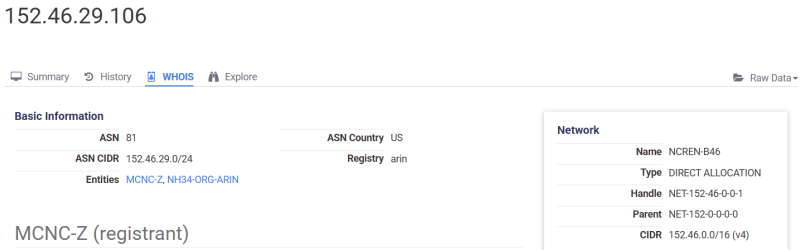


MCNC-Z (registrant)

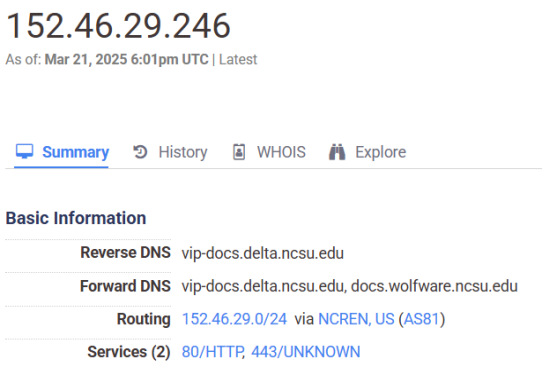
3) 152.46.29.106 - vip-p18-admin-foreman.delta.ncsu.edu

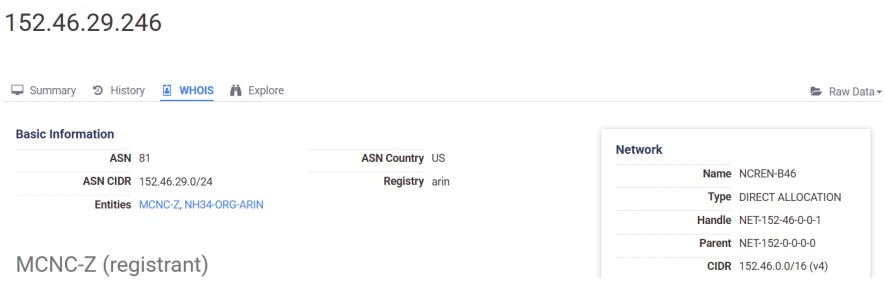
Ramdhanush Venkatakrishnan
rvenka26





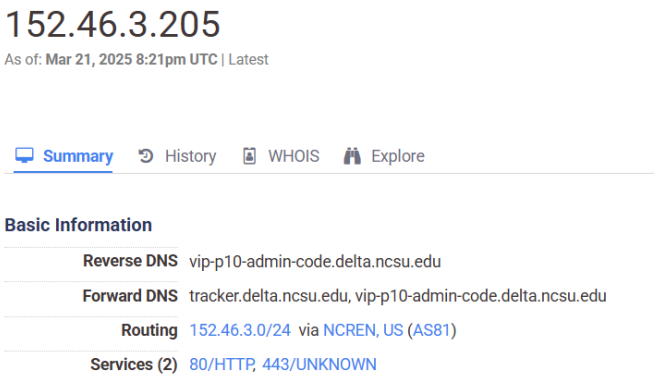
4) 152.46.29.246 - vip-docs.delta.ncsu.edu

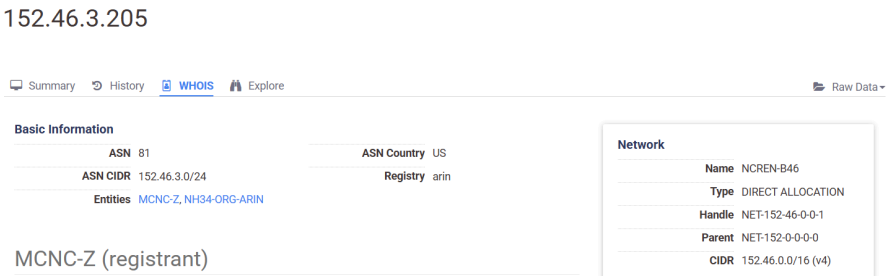




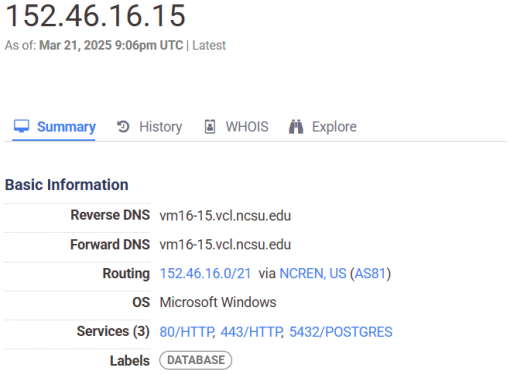
5) 152.46.3.205 - vip-p10-admin-code.delta.ncsu.edu

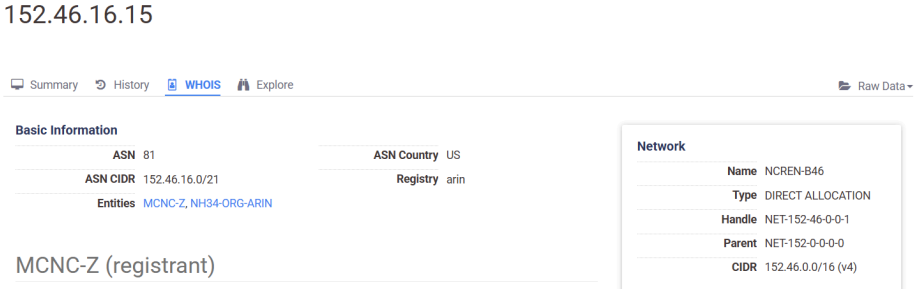
Ramdhanush Venkatakrishnan
rvenka26





6) 152.46.16.15 - vm16-15.vcl.ncsu.edu





Note that the delta.ncsu.edu and vcl.ncsu.edu domains repeat multiple times throughout the search. NCREN stands for the North Carolina Research and Education Network, which is a research and education network owned and operated by MCNC. This fact can also

be verified by using the results of DNS records from earlier. In addition to ncsu.edu, the network contains hosts from other institutions such as ncat.edu, uncfsu.edu, wssu.edu, mcnc.org, appstate.edu, etc. Since the NC State hosts found were part of a different autonomous system, they fall under the definition of “shadow IT”.

Part 5

The increasing use of IPv6 has a major impact on the operation of network scanning tools like Shodan and Censys. The biggest and most important change is the usage of longer addresses. IPv4 uses 32-bit addressing, while IPv6 uses 128-bit addressing. This means that scanning every address in the IPv6 web will be exponentially slower than that of IPv4.

However, there are points to be considered for practical purposes. The switch to IPv6 hasn’t been completed, making it orders of magnitude easier than in theory. Likewise, breakthroughs in computing could offset the delay by a non-trivial amount as well. An important factor is that only about 4% of the IPv6 addresses are stable for 4 days or more, and the rest are not. This is a great source for optimizing the runtime of scans, by considering only stable hosts.

Another thing to consider is the traffic flow patterns of the larger web. Nearly 40-45% of traffic flows through TCP ports 443 or 80 - the HTTP(S) family. Considering that the receiving ends of these connections have higher port numbers, it can be reasonably estimated that nearly 80-90% of all traffic originates from or reaches a HTTP(S) server. This fact is crucial to reducing search and scan times, since only the more commonly used ports could be considered. As an extension to this, a priority list of ports and protocols could further assist optimization efforts.

Ramdhanush Venkatakrishnan
rvenka26

Sources

1. Censys Search, Censys Python API, Censys Search Language Documentation
2. Shodan Search, Shodan API
3. MITRE CVE
4. Exploit DB
5. Scanning the IPv6 Internet: Towards a Comprehensive Hitlist (Oliver Gasser, Quirin Scheitle, Sebastian Gebhard, Georg Carle)