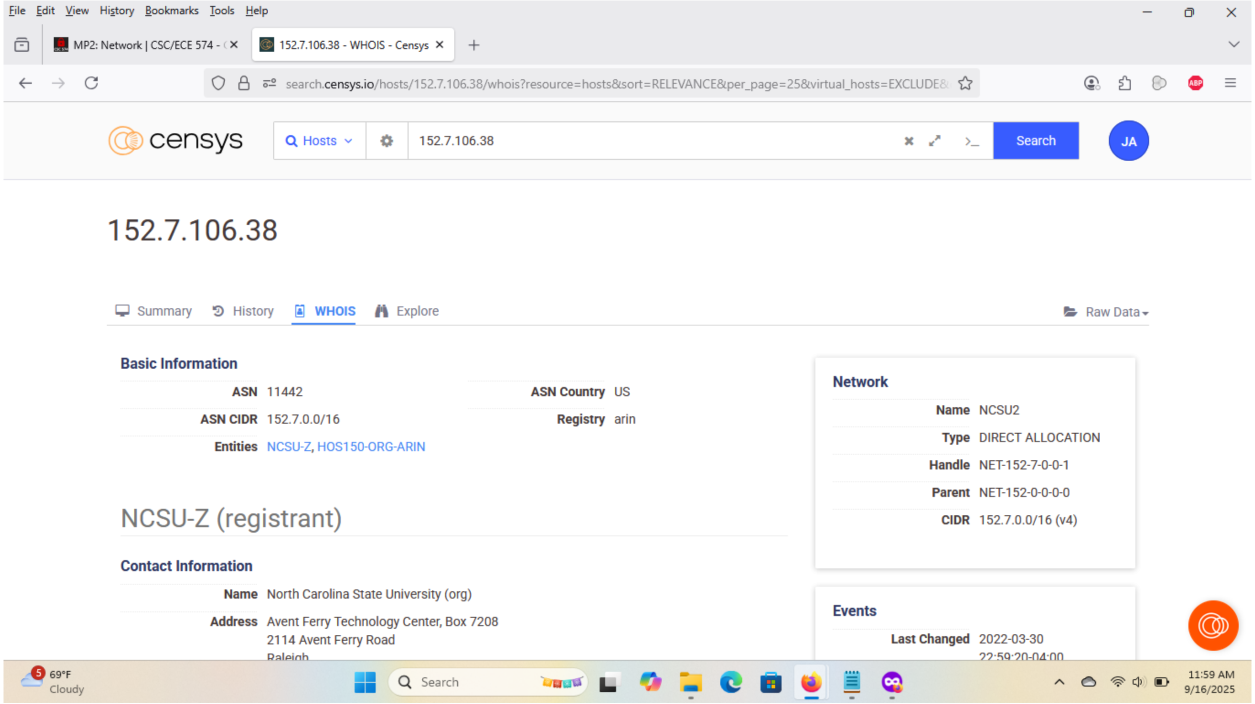
Introduction

The purpose of this audit is to conduct passive reconnaissance to identify publicly visible characteristics of the NCSU campus network. This includes analyzing key signifiers such as DNS records, IP address allocations, autonomous system information, web servers, operating systems, and network protocols. The goal is to examine the characteristics of hosts within the selected CIDR block, assess any potential vulnerabilities in the current setup, and identify indicators of Shadow IT or externally hosted services using the `ncsu.edu` domain. Additionally, the audit explores the impact of IPv6 on the effectiveness of the passive reconnaissance tools used.

IPv4 Blocks

In order to find the identified IPv4 blocks, I queried "North Carolina State University" into the Censys search engine. From the search results provided, I selected three IPv4 blocks and found the CIDR Block, Network Name, Autonomous System Number & Autonomous System Name. This information was obtained within each result by clicking on the WHOIS tab, as shown:


File Edit View History Bookmarks Tools Help
MP2: Network | CSC/ECE 574 -
152.7.106.38 - WHOIS - Censys
search.censys.io/hosts/152.7.106.38/whois?resource=hosts&sort=RELEVANCE&per_page=25&virtual_hosts=EXCLUDE&
censys
Hosts
152.7.106.38
Search
JA
Summary
History
WHOIS
Explore
Raw Data
69°F
Cloudy
Search
11:59 AM
9/16/2025

152.7.106.38

Basic Information

ASN 11442
ASN CIDR 152.7.0.0/16
Entities NCSU-Z, HOS150-ORG-ARIN
ASN Country US
Registry arin

NCSU-Z (registrant)

Contact Information

Name North Carolina State University (org)
Address Avent Ferry Technology Center, Box 7208
2114 Avent Ferry Road
Raleigh

Network

Name NCSU2
Type DIRECT ALLOCATION
Handle NET-152-7-0-0-1
Parent NET-152-0-0-0-0
CIDR 152.7.0.0/16 (v4)

Events

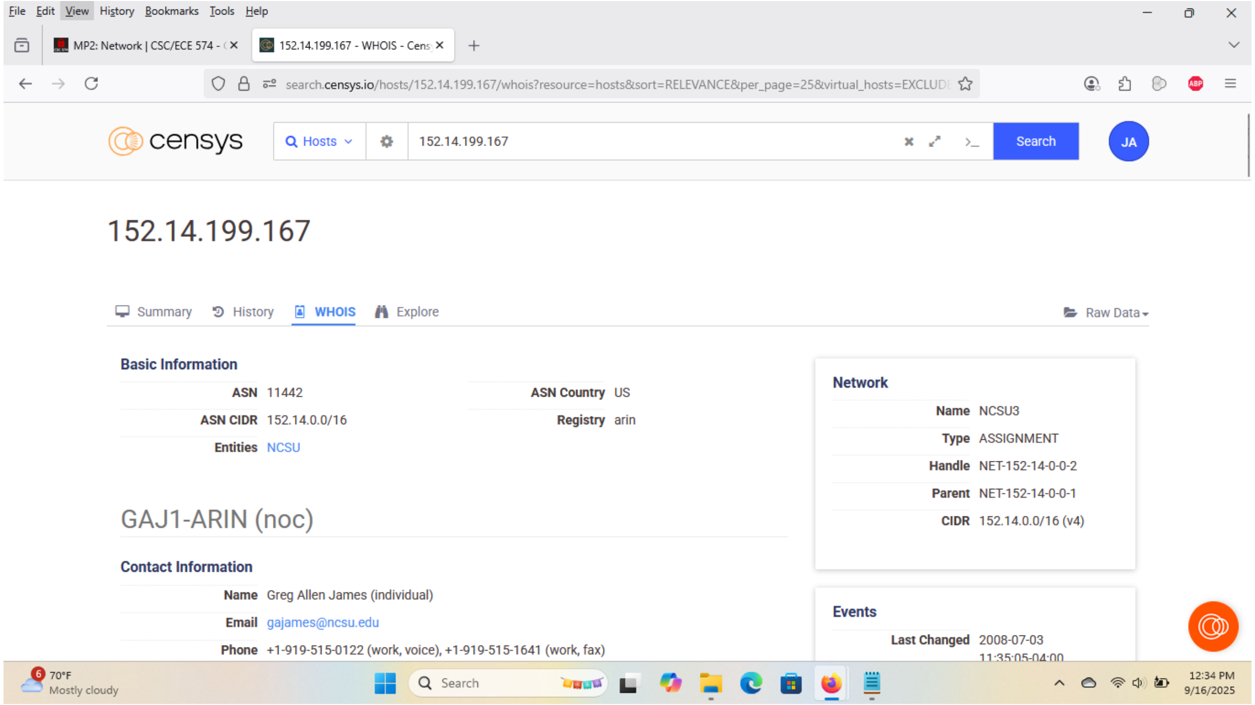
Last Changed 2022-03-30
22:59:20-04:00

CIDR Block: 152.7.0.0/16

Network Name: NCSU2

AS Number: 11442

AS Name: North Carolina State University (org)


File Edit View History Bookmarks Tools Help
MP2: Network | CSC/ECE 574 -
152.14.199.167 - WHOIS - Cens
search.censys.io/hosts/152.14.199.167/whois?resource=hosts&sort=RELEVANCE&per_page=25&virtual_hosts=EXCLUD
censys
Hosts
152.14.199.167
Search
JA
Summary
History
WHOIS
Explore
Raw Data
70°F
Mostly cloudy
Search
12:34 PM
9/16/2025

152.14.199.167

Basic Information

ASN	11442	**ASN Country**	US
ASN CIDR	152.14.0.0/16	**Registry**	arin
Entities	NCSU		

GAJ1-ARIN (noc)

Contact Information

Name	Greg Allen James (individual)
Email	gajames@ncsu.edu
Phone	+1-919-515-0122 (work, voice), +1-919-515-1641 (work, fax)

Network

Name	NCSU3
Type	ASSIGNMENT
Handle	NET-152-14-0-0-2
Parent	NET-152-14-0-0-1
CIDR	152.14.0.0/16 (v4)

Events

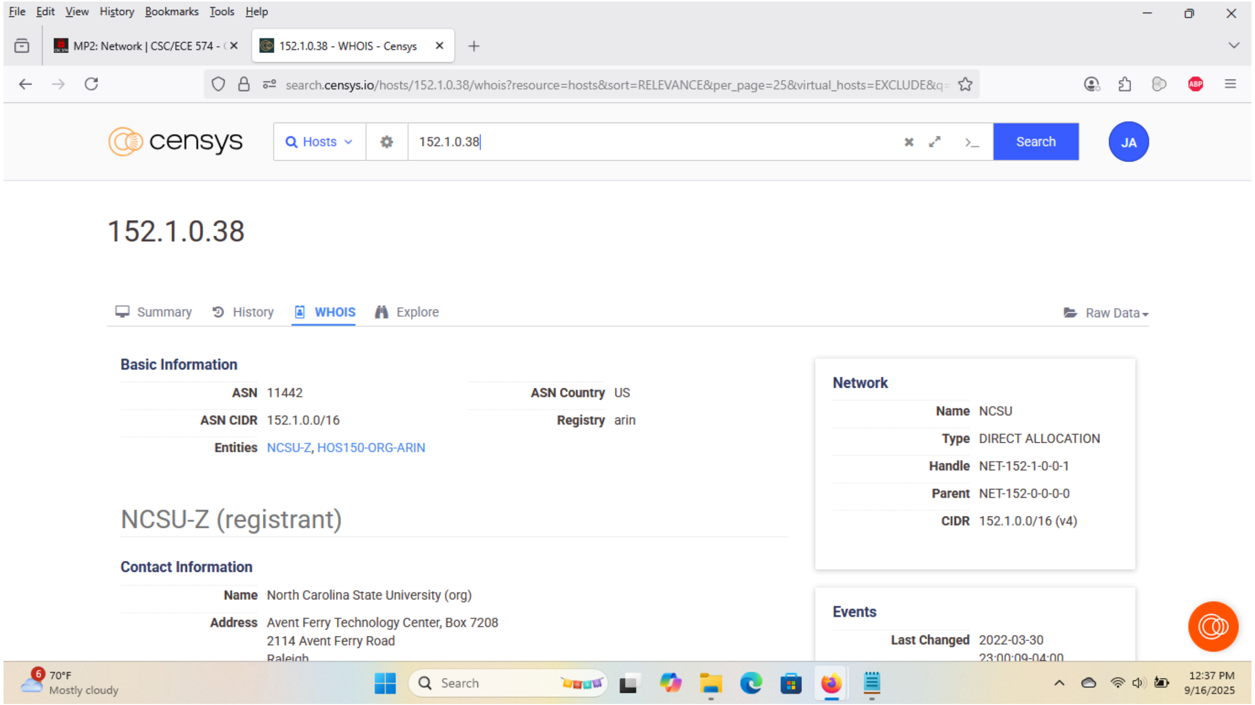
Last Changed	2008-07-03 11:35:05-04:00

CIDR Block: 152.14.0.0/16

Network Name: NCSU3

AS Number: 11442

AS Name: Greg Allen James (individual)


File Edit View History Bookmarks Tools Help
MP2: Network | CSC/ECE 574 -
152.1.0.38 - WHOIS - Censys
censys
Hosts
Search
JA
Summary
History
WHOIS
Explore
Raw Data
70°F
Mostly cloudy
Search
12:37 PM
9/16/2025

search.censys.io/hosts/152.1.0.38/whois?resource=hosts&sort=RELEVANCE&per_page=25&virtual_hosts=EXCLUDE&q=

152.1.0.38

152.1.0.38

Basic Information

ASN	11442	ASN Country	US
ASN CIDR	152.1.0.0/16	Registry	arin
Entities	NCSU-Z, HOS150-ORG-ARIN		

NCSU-Z (registrant)

Contact Information

Name	North Carolina State University (org)
Address	Avent Ferry Technology Center, Box 7208 2114 Avent Ferry Road Raleigh

Network

Name	NCSU
Type	DIRECT ALLOCATION
Handle	NET-152-1-0-0-1
Parent	NET-152-0-0-0-0
CIDR	152.1.0.0/16 (v4)

Events

Last Changed	2022-03-30 23:00:09-04:00

CIDR Block: 152.1.0.0/16

Network Name: NCSU

AS Number: 11442

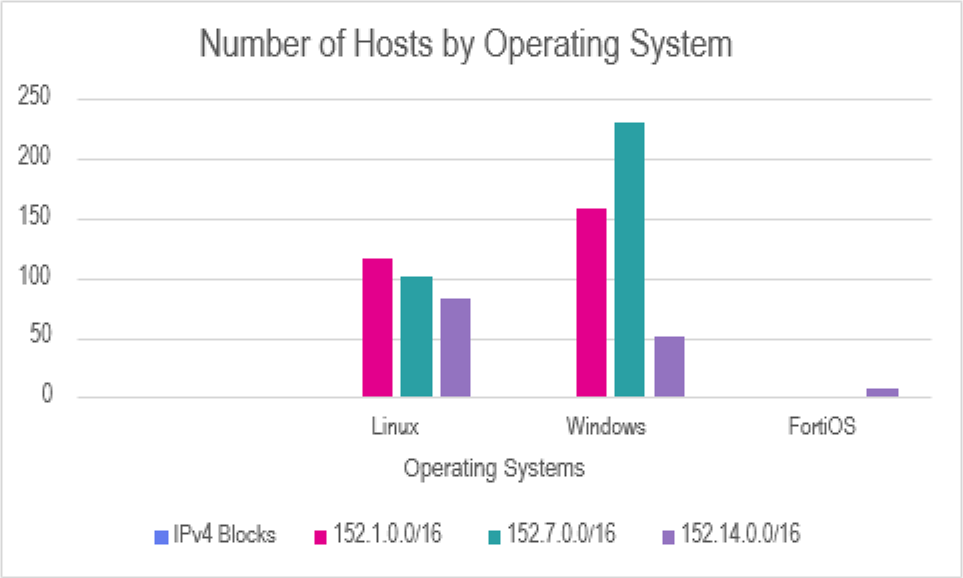
AS Name: North Carolina State University (org)

Network Summary

The data for this section was readily available and gathered directly from the original Censys search results used to identify the three IPv4 blocks. In the Censys interface, the left-hand panel provides summary information:

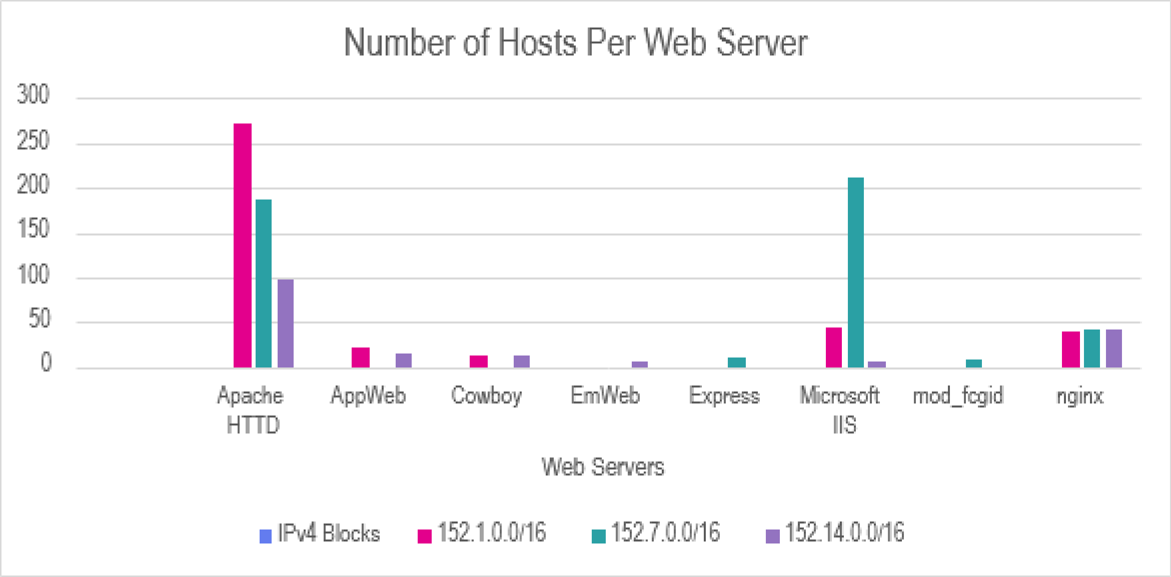
- **Software Product**: Lists the number of hosts running specific operating systems and web servers.
- **Ports and Service Names**: Shows the number of hosts using each protocol, based on open ports and identified services.

This information was used to quantify host distributions by OS, web server, and protocol for graphic visualization.



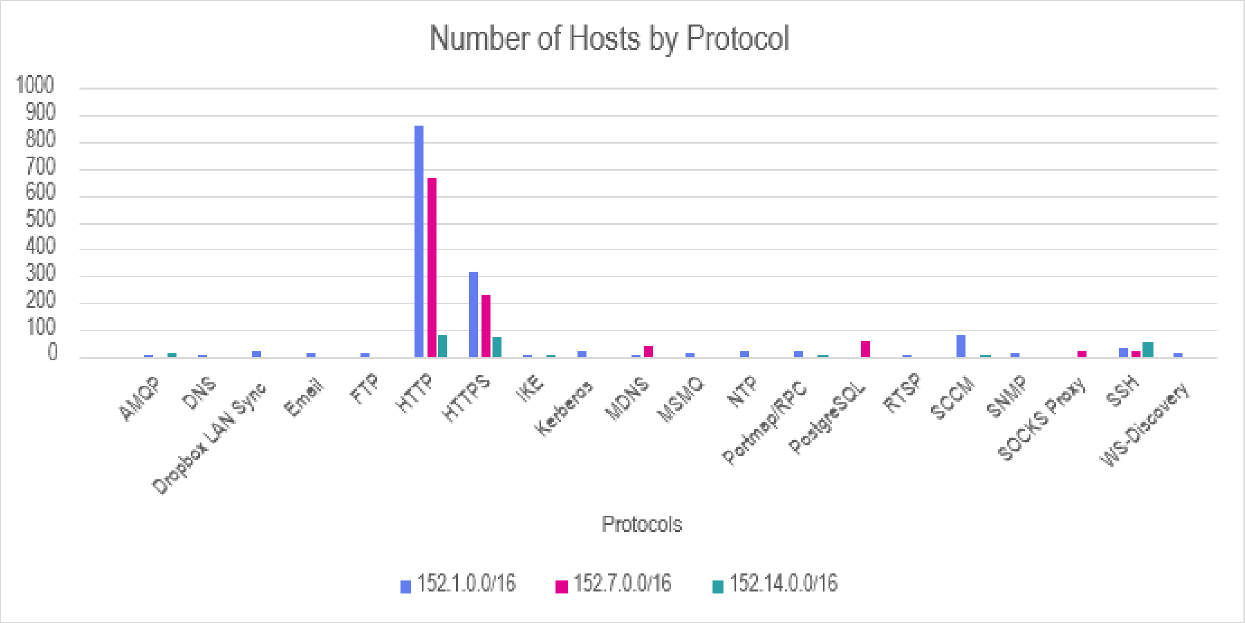
It is quite clear that due to their popularity, Windows and Linux are the most used operating systems amongst hosts in the observed IPv4 blocks. This distribution reflects common usage patterns in campus networks, where Windows is often favored for desktop and institutional applications, while Linux tends to be widely used for servers, academic research, and specialized systems. Each operating system presents distinct security challenges. Windows systems are often targeted by malware and require frequent patching to address vulnerabilities. Linux hosts, though generally more secure by design, can still be vulnerable if misconfigured or left unpatched.

A small number of hosts running FortiOS were also observed, likely representing network security appliances such as firewalls or VPN gateways. While purpose-built for security, these systems must also be regularly updated and monitored, as vulnerabilities in management interfaces or outdated firmware can pose critical risks to the broader network.



Apache is shown to be the most popular web server amongst the observed hosts, with Microsoft IIS shown to have significant use. Apache's popularity may stem from its widespread use in open-source and academic settings, where flexibility and cost-effectiveness are key. On the other hand, the presence of Microsoft IIS likely reflects institutional or departmental use of Windows-based services and "legacy" systems. That being said, Apache's flexibility and modularity can lead to misconfigurations if not properly managed, while IIS — often integrated into Windows environments — may introduce risks if "legacy" systems or default settings are left unmodified.

Although less prevalent in this environment, Nginx appears in limited use, often serving as a reverse proxy or load balancer in front of Apache or other application servers. Its high performance and low resource footprint make it attractive for high-traffic or containerized applications, particularly in modern DevOps workflows like research groups or student-led projects. However, its lightweight design also assumes a level of administrative familiarity, and like Apache, improper configuration can lead to security exposures.



The most widely observed protocols are HTTP and HTTPS. This is expected, given that most internet-based activity relies on web traffic. However, what's notable is that HTTP — the unencrypted version — appears more prevalent than HTTPS. This suggests that a significant portion of web communication may be occurring without encryption, which introduces potential security risks. For hosts on a campus network, where a broad mix of unmanaged personal devices, "legacy" systems, and transient users is common, this can complicate things and raise concerns. Unlike enterprise environments, campus networks often have less centralized control over end-user behavior, making them more susceptible to insecure configurations and outdated software. The high volume of HTTP traffic may indicate that many users are accessing non-secure websites, or that certain applications or internal services still rely on "legacy" protocols. An exposed systemic vulnerability could be leveraged by attackers to intercept data, hijack sessions, or inject malicious content.

In conclusion, the campus network represents a diverse and flexible computing environment typical of academic settings, supporting both open-source and proprietary technologies. While this allows for diverse application hosting, it introduces complexity in system management and potential security challenges, especially if unencrypted protocols or inconsistent patching policies exist. The more prevalent use of HTTP in comparison to HTTPS only underscores a potential loophole or vulnerability that can be exploited by malicious users.

Security Findings

HTTP over HTTPS

As previously mentioned, one such vulnerability is the widespread use of unsecured HTTP connections across more than three IPv4 blocks within the campus network identified from gathering data from Censys on the three IPv4 blocks (Shodan was considered for supplementary checks, but Censys provided the necessary, timestamped passive reconnaissance for the chosen IPv4 blocks). This is the most glaring vulnerability. Numerous hosts — which can include web applications, login pages, and administrative interfaces — were found to serve content over HTTP without redirecting to HTTPS. These systems are accessible over the public internet and do not enforce encrypted connections, exposing users and services to significant risk. HTTP (Hypertext Transfer Protocol) transmits data in plaintext, making it vulnerable to interception and tampering by attackers who can position themselves between the client and server — particularly on open or compromised networks. In contrast, HTTPS (HTTP Secure), which uses TLS, encrypts traffic to ensure data confidentiality, integrity, and server authenticity. Without HTTPS, users accessing university services — including students, staff, and researchers — may unknowingly transmit credentials, session cookies, or sensitive information in cleartext, leaving them susceptible to man-in-the-middle (MitM) attacks, phishing, or data leakage.

It is strongly recommended that all publicly accessible campus systems enforce HTTPS by default. Web servers should redirect all HTTP requests to HTTPS using permanent (301) redirects. TLS certificates — ideally issued and renewed automatically via a trusted certificate authority — should be deployed across all services. These steps will help secure the university's digital infrastructure, protect user data, and align with industry-standard security practices and regulatory expectations.

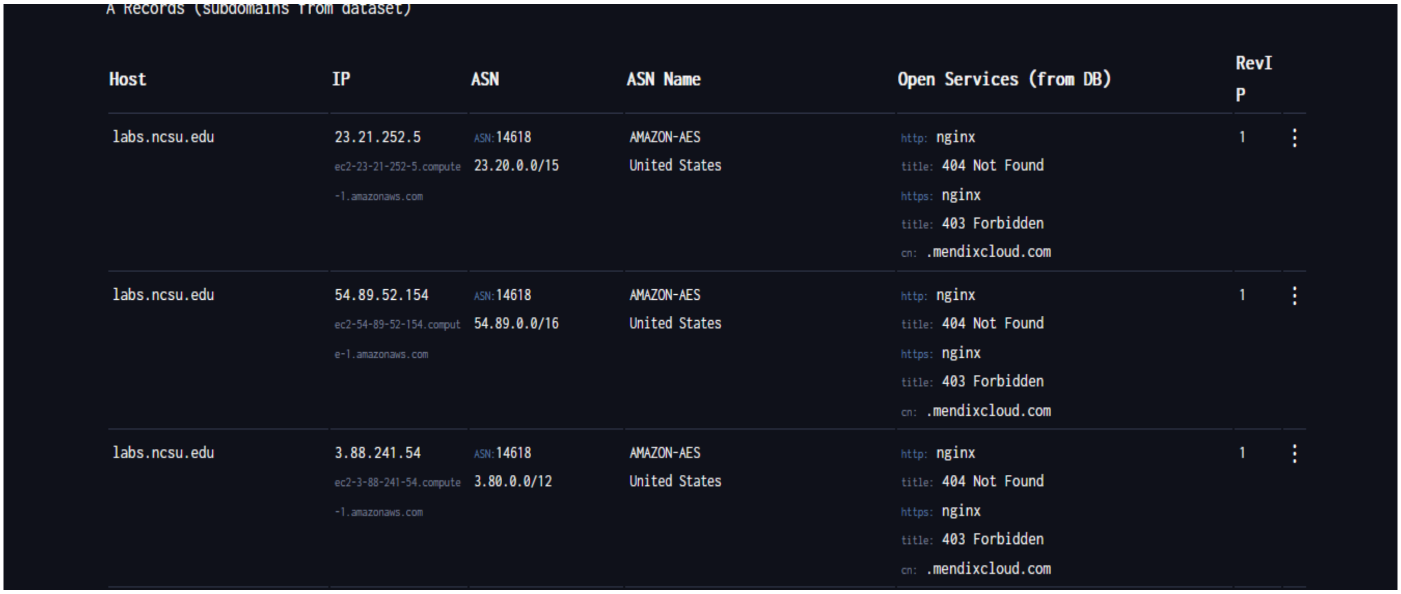
Web Servers

Apache HTTP Server, Microsoft IIS, and NGINX each have different operating system integrations and design philosophies. Apache is an open-source, modular server that runs on both Linux and Windows, though it's more commonly deployed in Unix-like environments. Microsoft IIS is a proprietary web server tightly integrated with the Windows operating system and the broader Microsoft ecosystem, such as Active Directory and .NET applications. NGINX is a high-performance, event-driven web server and reverse proxy that also runs on both Linux and Windows, though it is predominantly used in Linux-based deployments due to its speed, scalability, and compatibility with modern DevOps tools. Each server relies on configuration files and system services to handle web traffic, and their security posture is heavily influenced by the underlying OS, default settings, and how well they are maintained.

Apache, IIS, and NGINX each have known security challenges depending on their version, configuration, and role. For example, Apache can expose sensitive server information or directory listings if default modules are left enabled. IIS often includes “legacy” protocols and sample scripts that can be abused if not removed. NGINX, while lightweight and modern, can be vulnerable to misconfigured reverse proxy rules or weak access controls. Across all platforms, common issues such as weak TLS configurations, missing security headers, and exposed administrative interfaces can increase the attack surface and lead to data exposure, privilege escalation, or full system compromise — especially in a large, distributed environment like a university network. Performing a full review and standardization of web server configurations across all hosts would be the first step in mitigation. Unused modules and features should be disabled or removed. All web traffic should be forced over HTTPS with strong TLS settings (TLS 1.2+), and relevant HTTP security headers, which should be consistently applied. Additionally, default pages should be removed and access to administrative interfaces restricted by IP or authentication. In conjunction with the operating systems they are run over, regular patching and vulnerability scanning should be implemented to keep all web servers secure and compliant with institutional security policies.

Identifying External Shadow IT

Shadow IT refers to any hardware, software, or cloud services used within an organization without the knowledge, approval, or oversight of the IT department. Such unauthorized resources can introduce security, compliance, and operational risks by bypassing established control mechanisms. During passive reconnaissance using DNSDumpster, three hosts were identified that utilized the campus network’s domain name but resolved to external infrastructure, meeting the general criteria for Shadow IT.



A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP	
labs.ncsu.edu	23.21.252.5 ec2-23-21-252-5.compute-1.amazonaws.com	ASN: 14618 23.20.0.0/15	AMAZON-AES United States	http: nginx title: 404 Not Found https: nginx title: 403 Forbidden cn: .mendixcloud.com	1	⋮
labs.ncsu.edu	54.89.52.154 ec2-54-89-52-154.compute-1.amazonaws.com	ASN: 14618 54.89.0.0/16	AMAZON-AES United States	http: nginx title: 404 Not Found https: nginx title: 403 Forbidden cn: .mendixcloud.com	1	⋮
labs.ncsu.edu	3.88.241.54 ec2-3-88-241-54.compute-1.amazonaws.com	ASN: 14618 3.80.0.0/12	AMAZON-AES United States	http: nginx title: 404 Not Found https: nginx title: 403 Forbidden cn: .mendixcloud.com	1	⋮

Three subdomains under labs.ncsu.edu were identified that resolved to IP addresses outside the university's officially assigned network ranges. Specifically, three IP address blocks -- 23.20.0.0/15, 54.89.0.0/16, and 3.80.0.0/12 -- were observed. These IP ranges are not included in the previously collected NCSU CIDR blocks, which predominantly cover the campus network (such as 152.1.0.0/16). Furthermore, the AS Number associated with these IP ranges is 14618, registered to Amazon-AES (Amazon Web Services). This ASN is distinct from the university's official ASN, 11442, which governs the campus network infrastructure.

The presence of labs.ncsu.edu subdomains resolving to IP addresses within Amazon's AWS's ASN rather than NCSU's ASN strongly indicates the use of externally hosted services operating under the university's domain name. As these services exist outside the boundaries of the university's managed network space, they meet the definition of Shadow IT -- IT resources using the institutional domain but hosted and potentially managed outside the official university infrastructure. This situation may pose challenges for security oversight and compliance, emphasizing the importance of identifying and addressing such Shadow IT resources.

Impact of IPv6

The transition to IPv6 brings with it a fundamental shift in how internet-facing systems are discovered and monitored. Tools like Shodan and Censys, which rely heavily on broad IPv4 scanning, are far less effective in the IPv6 space due to the enormous 128-bit address space. Research by Gasser et al. (2016) highlights that exhaustive scanning of IPv6 is computationally infeasible, prompting the need for curated “hitlists” built from indirect sources such as DNS records, certificate transparency logs, and passive traffic data. Even with these strategies, discovery remains incomplete — many IPv6 hosts avoid detection by using privacy extensions, dynamic addressing, or simply not being indexed by public naming services.

This limitation has serious implications for both attackers and defenders. Security teams can no longer assume that scanning tools provide full visibility into exposed services when IPv6 is involved. The research also shows that many IPv6 addresses are ephemeral, meaning previously discovered systems may disappear or change addresses within days. As a result, IPv6 can unintentionally become a blind spot in asset inventories, vulnerability scans, and SIEM monitoring. To address this, organizations must ensure that IPv6 traffic is explicitly logged, firewalled, and audited — rather than relying on "legacy" IPv4-focused tooling — and regularly assess DNS and TLS metadata to identify services that may be exposed over IPv6 without proper controls. [1]

Conclusion

This audit successfully utilized passive reconnaissance techniques to uncover publicly accessible information about the NCSU campus network. The assessment revealed existing vulnerabilities that could be exploited — most notably the widespread use of unsecured HTTP instead of HTTPS, and the presence of externally hosted subdomains operating outside the university's autonomous system. Host data within the selected CIDR block was gathered through passive tools such as DNSDumpster and Censys, which enabled identification of IP ownership, service exposure, and hosting characteristics. These findings demonstrate how passive methods can be leveraged to build a broader profile of the campus network and its infrastructure. To mitigate potential risks, it is recommended that the university enhance DNS governance, enforce HTTPS across all web services, maintain accurate asset inventories for both legacy and modern systems, and regularly monitor for unauthorized or externally hosted subdomains.

Footnote:

[1] Gasser, O., Scheitle, Q., Holz, R., Korczyński, M., & Carle, G. (2016). *Scanning the IPv6 Internet: Towards a Comprehensive Hitlist*. arXiv preprint arXiv:1607.05179