Assessing Georgia Tech’s Network Vulnerabilities

Dhruv Rauthan
Georgia Institute of Technology
dhruvrauthan@gatech.edu

Akshat Deo
Georgia Institute of Technology
akshatdeo@gatech.edu

Abstract

Cyberattacks on universities have become increasingly common, posing significant threats to their security and integrity. With universities serving as custodians of vast amounts of private and sensitive data, safeguarding their network infrastructure is paramount. This project addresses these concerns by conducting an extensive network scanning and vulnerability assessment of Georgia Tech’s network using Nmap. We find the network to be generally safe, with isolated issues discussed in the report.

1 Introduction

In an age where cyber-threats are becoming increasingly sophisticated and pervasive, the security of network infrastructure at Universities like Georgia Tech is of concern. These institutions are not just centers of learning, but also repositories of large amounts of sensitive data, making them an attractive target for cyberattacks.

Universities globally have been victims of co-ordinated cyberattacks, leading to large scale data breaches and financial losses. Incidents at universities like UCLA, Uniersity of Minnesota, Michigan State University and even Georgia Tech raises serious questions about how safe our university networks are.

Our aim was to identify potential vulnerabilities that could be exploited by malicious actors. We also wanted to compare how an attacker inside the network could target services as compared to someone outside the network. In an effort to answer this question, we make the following contributions.

- Perform scans of all subnets under Georgia Tech’s Network using Nmap.
- Analyze results found and compare them with known vulnerability databases.
- Compare internal scan results (Nmap) with external scan data (Censys)

2 Dataset

We perform Nmap scans on 31 subnets managed by Georgia Tech [3]. These include a /10, multiple /16s and a few smaller networks. These amount to a total of approximately 6 million IP addresses. We aggregate this data from our internal network scans into [5].

To compare our internal Nmap scans with external data we use Censys. Censys is a public search engine and data processing facility backed by data collected from ongoing Internet-wide scans [1]. It continually scans the public address space across a range of important ports and protocols and maintains up-to-date snapshots of the hosts and services running across the public IPv4 address space. This includes the publicly accessible Georgia Tech networks. Censys exposes this data through a search engine and API, which we utilize.

To identify existing or previous vulnerabilities for particular system services, we utilize the CVE database. CVE is a centralized repository that contains information about publicly known network security vulnerabilities and provides a standardized way to track them [2].

3 Methodology

In network scanning, the first step is to narrow down a list of active hosts from a large set of IP ranges. Instead of scanning every port of every IP address, Nmap provides flexible options for customizing host discovery techniques. Host discovery, or ping scanning, involves sending different types of probes to identify active IP addresses (which are ’up’). Nmap’s default probes include ICMP echo requests, TCP SYN to port 443, TCP ACK to port 80, and ICMP timestamp requests.

After identifying the active hosts, we perform 5 different types of scans: SYN, UDP, Protocol, Service and Application Version Detection, and OS detection.

3.1 Nmap Scans

3.1.1 SYN

The TCP SYN Stealth scan allows for rapid scanning of thousands of ports per second on a high-speed network without being hindered by intrusive firewalls. It operates by initiating the first part of a TCP connection but never completes it. Nmap starts by sending a TCP packet with the SYN flag set to a particular port. The target device can respond with one of these 3 responses:

1. SYN/ACK: the port is open. The scanning device sends back an RST packet to close the connection.
2. RST: the port is closed.
3. No response: the port is filtered, i.e, it is either blocked by the firewall or the host is down. After a timeout period, Nmap resends the packet. After yet another timeout period, Nmap gives up and marks the port filtered.

The responses are summarized in Table 1.

Probe Response	Assigned State
TCP SYN/ACK	open
TCP RST	closed
No response received (even after re-transmissions)	filtered
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

Table 1: How Nmap interprets responses to a SYN probe

We use the -sS flag to request an Nmap SYN scan.

3.1.2 UDP

Although the majority of widely used Internet services operate on the TCP protocol, UDP services are also extensively utilized. The process of UDP scanning involves sending a UDP packet to each designated port. In most cases, this packet is empty with no payload; however, for certain commonly used ports, a protocol-specific payload is included in the packet.

The UDP scan responses are summarized in Table 2.

However, unlike the RST packets sent back by the target device in the TCP SYN scans, the UDP scan analyzes ICMP responses. The problem here is that many hosts rate limit ICMP port unreachable messages they send back by default. To overcome this, there exist certain performance improvements which we discuss in Section 3.3. The -sU flag is used for a UDP Nmap scan.

3.1.3 Protocol

IP protocol scan allows us to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target devices. It works in a similar way to a UDP scan wherein it sends different IP packet headers by iterating through the eight-bit IP protocol field. Similar to open ports within the TCP or UDP protocols, any such open protocol presents a potential avenue for exploitation. Furthermore, the outcomes of a protocol scan play a crucial role in identifying a device's purpose and the type of packet filtering implemented. Usually, end hosts have limited open protocols, such as TCP, UDP and ICMP, whereas routers have a lot more, including routing-specific protocols like GRE and EGP.

Probe Response	Assigned State
Any UDP response from target port (unusual)	open
No response received (even after re-transmissions)	open|filtered
ICMP port unreachable error (type 3, code 3)	closed
Other ICMP unreachable errors (type 3, code 1, 2, 9, 10, or 13)	filtered

Table 2: How Nmap interprets responses to a UDP probe

The protocol scans have similar limitations in terms of performance as compared to the UDP scans, since the ICMP unreachable messages are often rate limited. We employ similar performance enhancement techniques for these scans as well. Protocol scans are requested by using the -sO Nmap option.

3.1.4 Service and Application Version Detection

Using the nmap-services database, which catalogs over 2,200 well-known services, Nmap can make educated guesses about the nature of the services associated with specific ports. However, relying solely on these port-to-service associations poses a risk, as users may either run services on unconventional ports. Variations in port assignments are common. Even if Nmap is right, and the port is running a particular service, that is not a lot of information. When doing vulnerability assessments, we want to know which exact versions are running as it helps dramatically in determining which exploits the target device is vulnerable to. Nmap service scans help reveal the exact service and version number of the running service on the target device. It obtains all of this data by connecting to open ports and interrogating them for further information using probes that the specific services understand. These scans are requested by adding the -sV option.

Nmap offers various 'intensity levels' from 0 to 9, which identify the running service with different degrees of accuracy, the higher the intensity the more likely that that service is running on that port. Initially, we started with a lighter intensity to gauge the performance of Nmap over large subnets. Using the default intensity of 7 did not add significant delays in scanning, and we went ahead with that for all our experiments.

3.1.5 OS Detection

As the name suggests, OS detection scans identify the operating system running on the target device. Nmap includes a huge database that helps in identifying thousands of different systems based on how they respond to a particular selection of TCP/IP probes. These probes are specially designed to exploit various ambiguities in the standard protocol RFCs. The attributes in these responses are combined to form a TCP/IP fingerprint which is in turn used to pinpoint the operating system of the device.

Nmap might return multiple possible operating systems in case a fingerprint match is not conclusive. These are comma separated and are usually from the same family (for example Linux or Windows), just different versions. We use the -O flag to request an Nmap OS scan.

3.2 Censys

We utilized the Censys database to specifically target and analyze certain IP ranges associated with Georgia Tech. Our main focus was to gather information about the host devices operating within these networks. This includes information about open ports, the services running on those ports, the types of operating systems in use and any additional information provided by Censys. This allows us to assess potential vulnerabilities from an external attacker's point of view, i.e, someone who does not have inherent access to the internal network. For this purpose, Georgia Tech's networks were queried via Censys Search [4].

3.3 Performance

As discussed in Section 3.1.2 and 3.1.3, Nmap scans often run into performance issues when scanning large networks. Since we were aiming to scan a /10 as well as multiple /16 subnets, a total of around 6 million IP addresses, Nmap's performance had to be optimized as much as possible. The aim was to reduce scanning times to reduce the load on the network, while maintaining a high degree of accuracy in determining the open ports, services and operating systems. We used multiple Nmap options in all our commands to achieve this, which are explained below.

- Fast mode (-F): When using this flag, Nmap only scans the 100 most popular ports in each protocol. Most of the 65,535 ports won't have any services running on them, and even lesser might be open. It is therefore reasonable to only scan the popular ports since those ports are the ones which a malicious actor might actually target.
- No DNS resolution (-n): Since we are not interested with the domain names associated with the IP addresses, we skip the reverse DNS resolution lookup on any active IP addresses.
- Maximum probe retransmissions (–max-retries): When Nmap receives no response to a port scan probe, that means the port is filtered or a packet was simply lost on the network. So it tries again by retransmitting the initial probe. While this benefits accuracy, it also lengthens scan times. We set this value to 5.
- Minimum rate of scanning (–min-rate): When specified, Nmap tries to send the probe packets as fast or faster than the specified rate. We set this value to 10000 packets per second.

These options helped reduce the scanning times considerably while also maintaining an acceptable level of accuracy.

3.4 Deployment Guidelines

Our experiments involved close collaboration with the Georgia Tech network team, ensuring a coordinated and transparent approach to our activities. The primary focus was on fingerprinting rather than active exploitation. Prior to initiating the scans, thorough guidelines was established which specified crucial parameters and the exact commands to be run. A document outlining these guidelines was shared with the network team. Before executing the scans, we were also required to send a timely email to the Office of Information Technology's network security team, ensuring that our scans were not blocked or marked as suspicious activity. Furthermore, the scans were permitted only outside of institute business hours, to minimize the potential impact of the Nmap probes on regular users.

Georgia Tech's Zone Protection Profile has implemented Flood Protection on every firewall interface. In case we hit these limits, the firewall starts dropping our packets. Adhering to the strict firewall policies, our experiments were designed not to trigger their alarms, with clear instructions on the maximum scanning rate to avoid disruption. Additionally, Reconnaissance Protection was enabled as well, that monitors for TCP, UDP and host sweep scans. For intra-campus traffic, this will trigger an alert but will not block the traffic. These alerts are expected as we will be intimating our scanning times to the firewall team beforehand.

The initial scans to test the feasibility of the project were done via a device connecting to the intra-campus network, eduroam. Conducting these initial scans via Georgia Tech's VPN service gave similar results to the former. Subsequently, we conducted the actual scans through the VPN itself.

Scan Type	Hosts Found
SYN	41667
UDP	41378
S/V Detection	41711
OS Detection	42135
Protocol	41422

Table 3: Hosts Detected by Scan Type

4 Results

4.1 Nmap

As mentioned in Section 3, we performed 5 different scans over each subnet. Table 3 tells us the consolidated number of hosts detected in each scan. An interesting point to note is that even though we probed over 6 million IP addresses, the maximum number of hosts we could detect was only 42,135. While it's not uncommon for network scans to detect only a small portion of the IP Address space being probed, 0.68% is a significantly low number. This can be explained by multiple factors:

- Low Subnet Utilization: There is a possibility that a substantial number of IP addresses are not currently allocated or actively in use. Academic institutions often have large IP blocks simply for historical reasons. These are either reserved for future use or sold off.
- Hosts configured to block probes: Administrators will often configure devices to block such scanning probes. In our experience, Windows 10/11 devices also never respond to nmap probes (as long as they use Windows Firewall).
- Scan Timing: As instructed, all of our scans were conducted during non-business hours. While this minimizes the effect of any disruptions, it also increases the chances of a large number of devices being offline.
- Network Segmentation: Firewalls and Access Control Lists could also cause us to miss hosts on other subnets. However, this does not seem to be the case here.

4.1.1 SYN Scans

SYN Scans by far resulted in the most number of services being identified/discovered, as can be witnessed in Table 4. For the sake of brevity, we only include top 50 results. Most are common services like HTTP, HTTPS, SSH etc. We compare these services with CVEs in Section 5.

We also see a service titled 'h323q931' running on Port 1720. Our scans captured 344 instances of this service being run. The most common usage for this port and service is for Microsoft's Netmeeting Client, which has long been discontinued. The likely explanation is that this port was opened by F5 software, which we know is being used at Georgia Tech.

4.1.2 UDP Scans

As is seen in Table 5, UDP Scans were able to identify 13 distinct services running on various ports. Out of the 41,378 hosts discovered, only 6872 services with open ports were found. As expected, we have very common services like Simple Network Management Protocol (SNMP @43.7%) and Network Time Protocol (NTP @38.4%) taking up a majority. We also observed some protocols like SLP (Service Location Protcol) being used. As such, the results here are expected and confidence-inspiring.

4.1.3 OS Detection

Operating system scans using Nmap gave us close to 100 different Operating systems/versions being run on various devices as seen in Table 6. Surprisingly, the highest number of detected OS were all from Cisco's routers/switches. Coming in second, we have various versions of Linux, making up about 3166 scanned OSes. Windows and Mac devices typically block probes in their default settings. The 21 Apple devices we captured are Airport Routers or some other Apple service; they do not represent consumer-grade Apple Devices like iPhones/Macbooks, etc. Similarly, most Windows devices out of 553 were Windows server machines. However, there were a few instances of Windows XP and Windows Vista being run. These could have been set up for research purposes and as such don't require any attention.

4.1.4 Service & Version Detection

Our Service and Version Detection (SaV) scans gave us over 700 distinct types of services and versions being run. Including all our results here is impossible, so we link our dataset in [5]. The most commonly running service was 'Microsoft Terminal Services at 5106 instances. We see many different versions of OpenSSH being run on various operating systems.

On the slightly concerning side, some instances of uTorrent and BitTorrent clients were being run. While there's nothing wrong with using these software, they're, more often than not, used for illicit purposes. We also see instances of older Apache services being run, known to have vulnerabilities, discussed in Section 5

4.1.5 Protocol Scans

The protocol scans yielded results that were notably less impressive than the others. Even though we detected a similar number of hosts (41,422), the only protocols identified were ICMP and SCTP. Consequently, this outcome did not justify further investigation into these scans.

Port	Service	Count	Percentage
80/8008	http	8649	25.417
443	https	7245	21.291
22	ssh	6180	18.161
3389	ms-wbt-server	3211	9.436
179	bgp	1687	4.958
139	netbios-ssn	1628	4.784
445	microsoft-ds	1013	2.977
135	msrpc	751	2.207
9100	jetdirect	394	1.158
5060	sip	357	1.049
23	telnet	347	1.020
1720	h323q931	344	1.011
515	printer	197	0.579
8080	http-proxy	174	0.511
631	ipp	174	0.511
5000	upnp	160	0.470
8443	https-alt	145	0.426
111	rpcbind	138	0.406
5900	vnc	130	0.382
2001	dc	118	0.347
88	kerberos-sec	93	0.273
21	ftp	79	0.232
53	domain	74	0.217
2049	nfs	61	0.179
5357	wsdapi	60	0.176
8000	http-alt	53	0.156
25	smtp	39	0.115
3306	mysql	30	0.088
7070	realserver	29	0.085
8081	blackice-icecap	27	0.079
389	ldap	26	0.076
514	shell	19	0.056
8888	sun-answerbook	17	0.050
10000	snet-sensor-mgmt	14	0.041
3000	ppp	13	0.038
427	svrloc	12	0.035
8009	ajp13	12	0.035
1433	ms-sql-s	11	0.032
587	submission	11	0.032
5432	postgresql	9	0.026
6000	X11	8	0.024
2000	cisco-sccp	8	0.024
873	rsync	6	0.018
5009	airport-admin	6	0.018
990	ftps	6	0.018
3128	squid-http	4	0.012
993	imaps	4	0.012
5051	ida-agent	4	0.012
548	afp	3	0.009
554	rtsp	3	0.009

Table 4: Services detected by SYN Scan

Port	Service	Count	Percentage
161	snmp	3004	43.714
123	ntp	2643	38.460
137	netbios-ns	847	12.325
111	rpcbind	135	1.964
53	domain	64	0.931
3283	netassistant	63	0.917
2049	nfs	54	0.786
5353	zeroconf	28	0.407
500	isakmp	13	0.189
427	svrloc	10	0.146
623	asf-rmcp	7	0.102
443	https	3	0.044
17185	wdbrpc	1	0.015

Table 5: Services Detected by UDP Scan

Category	Count
Android	26
Linksys Devices	4
Cisco Devices	3329
FreeNAS	165
Windows Operating Systems	553
FreeBSD	192
Linux Operating Systems	3166
HP Devices (Printers)	191
Avaya Devices	84
Juniper Devices	122
Apple Devices	21
Other Categories	49

Table 6: Broadly Categorized OS Counts

4.2 Censys

Searching the Censys database for all of Georgia Tech's managed networks, we found entries for only 3 of them, namely 143.215.0.0/16, 128.61.0.0/16 and 130.207.0.0/16. All the other networks are not publicly accessible and hence do not respond to Censys probes. Out of these 3 networks, we know for a fact that 143.215.0.0/16 is allocated to the VPN, and it is reasonable to expect it to be open to the internet. Secondly, when connected to the campus WiFi, eduroam, we were allocated IP addresses from 128.61.0.0/16, and we can safely assume that that network is reserved for these services.

It is unclear why 130.207.0.0/16 is accessible from the outside, however one of the reasons could be due to it hosting web servers for Georgia Tech. It has a higher number of HTTP service instances than the other networks. Additionally, this network has a significantly higher number of Apache and HTTPD product instances running on the network machines as compared to the other networks. This indicates a cluster of servers used to host websites, potentially Georgia Tech's .edu websites.

Service	143.215.0.0/16	128.61.0.0/16	130.207.0.0/16
http	424	297	594
ntp	297	167	376
ssh	171	128	43
snmp	72	9	6
bgp	31	-	12
smtp	16	4	15
sip	14	-	6

Table 7: Services detected for different networks by Censys

A few of the popular services running on the network machines are listed in Table 7. The results are similar to what we saw in the Nmap scans, with many devices running common services such as HTTP, NTP and SSH.

5 Discussion

During our analysis, we identified several critical Common Vulnerabilities and Exposures (CVEs) associated with key services running on open ports accessible by anyone on the network. These services include and are not limited to Session Initiation Protocol (SIP), Internet Printing Protocol (IPP), Service Location Protocol (SVRLOC) and even Apache HTTP servers (httpd). Addressing these CVEs is extremely important to maintain the security and integrity of the network, as they may pose several risks, from unauthorized access to DoS attacks. Discussing existing vulnerabilities for each and every service is beyond the scope of this paper, instead we will focus on a few key services.

Apache HTTP: Apache HTTP server or httpd, is a widely used open source web server, and we found multiple instances of this service in the network. Several vulnerabilities were discovered this year affecting Apache HTTP servers. For example, an attacker was able to block the handling of a particular HTTP/2 connection, which in turn could exhaust the server's worker resources. Another out-of-bounds read vulnerability was found affecting certain servers as well. Fortunately, these vulnerabilities have been patched with software updates. Our Nmap scans did not return the particular version number used by the Apache services, therefore we cannot say for certain whether a particular vulnerability can be exploited in practice. However, in case devices are not patched in a timely manner, it leaves them at risk. Malicious actors can regularly probe the network for any out-of-date devices and launch attacks against them.

SIP: F5 BIG-IP devices are used to handle SIP traffic for devices using real time communication. A vulnerability discovered in 2023 allows undisclosed traffic to cause the Traffic Management Microkernel (TMM) to terminate. This affects only particular BIG-IP versions, however as we discussed earlier, some devices may still not have been patched, leaving them open to attack.

IPP: We saw close to 200 instances of open ports running IPP, the device presumably being a printer. An older vulnerability, dating back 4 years, allows a buffer overflow attack via the IPP implemented in HP Laserjet printer (for which we found several instances present in the network).

The sheer number of different services discovered on the network prohibits us from discussing all of them in this paper. However, we can say that identifying services with vulnerabilities discovered recently indicates that a motivated malicious actor can scan the network to pinpoint these services and exploit vulnerabilities in older devices. All the devices managed by Georgia Tech such as servers, routers and printers must be regularly updated. Furthermore, services which should not be exposed to the network and be running on open ports, must be shut down or refuse any incoming unauthorized connections.

6 Related Work

There have been several papers assessing the security and existing vulnerabilities of university campus networks. Zheng et al. developed a tool named 'WebHunt' developed specifically to understand and identify the security risks associated with 7 university networks across China [6]. They use fuzzy matching techniques to find software vulnerabilities present in the network. Camacho et al. performed a comprehensive study of Dartmouth College over several years [7]. Their main focus was data collection and analysis, focusing more on the evolution of WiFi networks over time rather than trying to assimilate security vulnerabilities. They collected data on user behaviour and data usage patterns. Chillar and Shrivastava performed network scanning on 2 /24 subnets in their university's network using Nmap and Nexpose [8]. They only performed basic ping scans which gave them results for open ports and the potential services running. Our approach expands on theirs by adding protocol, service and application version, and OS detection scans.

7 Conclusion

With educational institutes such as Georgia Tech storing vast amounts of public and private data, it is imperative that any vulnerabilities be identified and fixed immediately. To assess the network health of Georgia Tech's network, we conducted Nmap scans across all their subnets and compared the findings with an external scanning dataset Censys.

We observed that most hosts were running common services such as HTTP, HTTPS, SSH etc. This behaviour is expected since devices running particular applications would require this port to be open to allow incoming connections. We also found a few services which should not have been running on open ports, however the rarity of these instances lead us to believe that these might be the student's personal machines instead of institute managed devices.

As observed via Censys, only absolutely necessary networks are publicly accessible such as the VPN service and Georgia Tech's website servers. Other networks can only be accessed internally. Attackers who do not have access to the internal campus network have only a few open services to target, thereby reducing the risk of security breaches. It must be noted that extra attention must be given to these networks since they are the ones that are most likely to be the first ingress point for any external attack, and all network devices must be constantly monitored and updated with the latest software patches.

References

[1] Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J. Alex Halderman. 2015. A Search Engine Backed by Internet-Wide Scanning. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15). Association for Computing Machinery, New York, NY, USA, 542–553. https://doi.org/10.1145/2810103.2813703

[2] CVE. December 12, 2023. https://cve.mitre.org

[3] Nmap. December 12, 2023. https://nmap.org

[4] Censys Search. December 12, 2023.

[5] Consolidated Scan Results. GT Vault Link

[6] Zheng R, Ma H, Wang Q, Fu J, Jiang Z. Assessing the Security of Campus Networks: The Case of Seven Universities. Sensors (Basel). 2021;21(1):306. Published 2021 Jan 5. doi:10.3390/s21010306

[7] José Camacho, Chris McDonald, Ron Peterson, Xia Zhou, and David Kotz. 2020. Longitudinal analysis of a campus Wi-Fi network. Comput. Netw. 170, C (Apr 2020). https://doi.org/10.1016/j.comnet.2020.107103

[8] K. Chhillar and S. Shrivastava, "Vulnerability Scanning and Management of University Computer Network," 2021 10th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON), Jaipur, India, 2021, pp. 01-06, doi: 10.1109/IEMECON53809.2021.9689207.