Incorporating Threat Intelligence into Incident Responses

Threat intelligence refers to the collection and analysis of information about current and emerging cyber threats, including attacker behavior, indicators of compromise (IOCs), and known tactics and techniques. It plays a critical role in how organizations respond to cyber incidents. Rather than responding without context, teams can use intelligence to understand what kind of threat they are dealing with, where it originated, and how to handle it effectively. By using threat intelligence throughout each phase of the incident response process, organizations can make faster, smarter decisions that reduce damage and help prevent similar attacks in the future. It turns a reactive process into a more proactive and informed approach.

In the **preparation phase**, threat intelligence helps organizations get ahead of potential attacks. This includes collecting information about recent threats, common attack methods, and known indicators such as suspicious IP addresses or malware signatures. These details are integrated into security tools like firewalls and monitoring systems to help detect abnormal activity. Preparation also involves using threat intelligence to build incident response playbooks, simulate realistic attack scenarios, and train staff based on actual adversary behavior (CISA, 2021).

During the **detection and analysis phase**, threat intelligence provides essential context for interpreting suspicious activity. Analysts use known indicators and adversary techniques to validate alerts and investigate abnormal behavior. This intelligence helps define the scope of an incident, identify attacker objectives, and associate the activity with

known threat actors. Activities such as log correlation, endpoint forensics, and MITRE ATT&CK mapping are informed by threat intelligence to build a complete picture of the intrusion (MITRE ATT&CK, 2024).

When an incident is confirmed, threat intelligence supports **containment, eradication, and recovery** efforts by identifying the methods the attacker may have used to maintain access. For example, knowledge of techniques like registry modification or scheduled tasks allows response teams to effectively remove persistence mechanisms. Intelligence also guides prioritization, helping determine which systems to isolate, which vulnerabilities to patch, and how to block malicious infrastructure to prevent further compromise.

In the **post-incident phase**, threat intelligence supports organizational learning and long term improvement. Any new indicators or tactics uncovered during the investigation are documented and fed back into detection systems. These findings may also be shared with trusted partners and government agencies to strengthen collective defenses. Most importantly, threat intelligence helps teams evaluate their response and make certain adjustments to ensure that they are better prepared for any future incidents.

Incorporating threat intelligence throughout each phase of the incident response lifecycle significantly strengthens an organization's ability to respond to and recover from cyber threats. Rather than relying solely on reactive measures, threat intelligence enables teams to make timely, informed decisions based on real world attacker behavior and indicators. This proactive approach not only improves the speed and accuracy of detection and containment but also supports continuous improvement through lessons learned and

shared insights. As the threat landscape continues to evolve, integrating intelligence into response efforts remains a key factor in maintaining a resilient cybersecurity posture.

Alien Vault OTX Threat Intelligence Analysis

AlienVault Open Threat Exchange (OTX) is a collaborative threat intelligence platform maintained by AT&T Cybersecurity. It enables security professionals to research, share, and monitor real time threat indicators such as IP addresses, domains, malware signatures, and vulnerabilities. OTX aggregates community-generated “pulses” that provide detailed information about active threats and campaigns. In this project, AlienVault OTX was used to investigate threat actors, extract Indicators of Compromise (IOCs), and examine the geographic distribution of malware activity (AT&T Cybersecurity, n.d.).

Based on the dashboard view, the malware with the largest circle is **Trojan: Win32/Zombie**. It belongs to the Trojan category and has a count of 163,820, which means it has been observed many times in the dataset. The feature count is 0, indicating that no specific behavioral or static features are currently associated with this malware in the system. The size of the circle visually confirms it has the highest count among all malware types shown in the dashboard (AT&T Cybersecurity, n.d.).

Trojan: Win32/Zombie, **Category**: Trojan , **Count**: 163820, **Feature Count**: 0

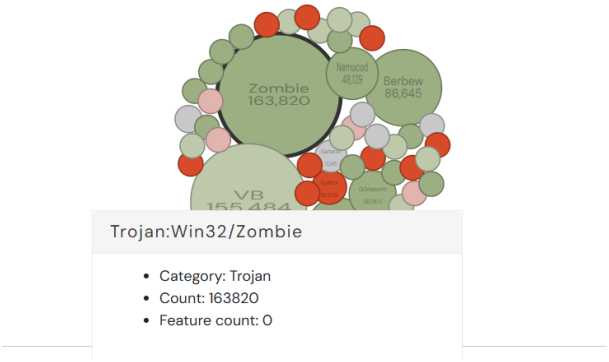


***Figure 1**:AlienVault OTX dashboard highlighting Trojan:Win32/Zombie as the most observed malware instance.*

***Source:** AlienVault OTX, https://otx.alienvault.com*

For the pulse with ID **687d74d0266b4805d1dfa9d2**, AlienVault OTX reports a total of **5,904 indicators of compromise (IOCs)**. These include multiple categories such as FileHash-MD5 (3), FileHash-SHA1 (3), IPv4 (310), Domain (1,521), FileHash-SHA256 (1,062), and a substantial number classified as Other (3,005). The dominance of the "Other" and "Domain" categories indicates that this malware is associated with a wide range of artifacts and malicious behaviors, underscoring its broad threat profile (AT&T Cybersecurity, n.d.).

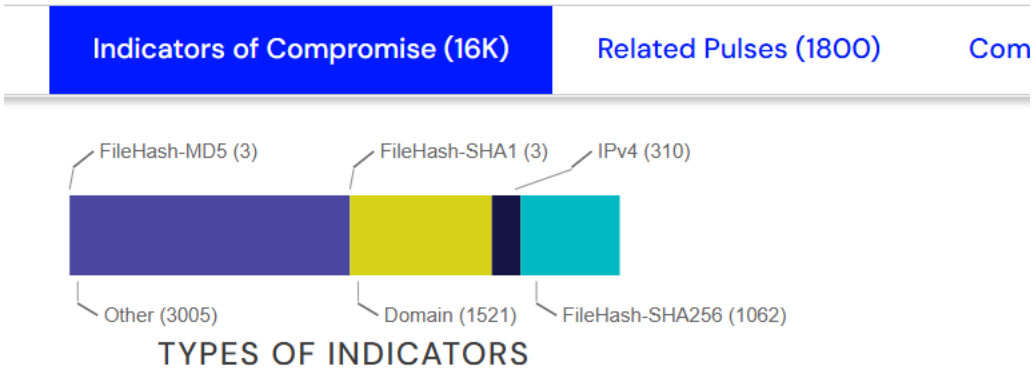


Figure 2: Pulse ID 687d74d0266b4805d1dfa9d2 showing IOC distribution by type in AlienVault OTX.

Source: AlienVault OTX, https://otx.alienvault.com

For the pulse ID **687d74d0266b4805d1dfa9d2**, the threat infrastructure section highlights the **geographic distribution** of associated malicious activity. The data shows that most of the infrastructure is hosted in the **United States**, with a total of **306 indicators**, while **Singapore** accounts for 2 indicators and **France** for 1. This distribution suggests that most of the infrastructure tied to this pulse leverages U.S.-based hosting services or compromised systems, reflecting both the prevalence of large-scale providers and the attractiveness of this region for adversaries (AT&T Cybersecurity, n.d.).

***Figure 3**: Geographic distribution of malicious infrastructure for Pulse ID 687d74d0266b4805d1dfa9d2.*

***Source:** AlienVault OTX, https://otx.alienvault.com*

Analysis of the indicators shows that the **IPv4 count reached 7,003,387**, whereas the **IPv6 count was only 18,534**. This significant gap reflects the long-standing dominance of IPv4 as the primary internet protocol. Most enterprise networks, malicious infrastructure, and security tools remain heavily dependent on IPv4, making it the primary focus for both attackers and defenders. In contrast, IPv6 adoption has progressed more slowly due to compatibility challenges and the persistence of legacy IPv4 environments, which limits both malicious activity and defensive visibility in IPv6 space (Cloudflare, 2022).

IPv4 count: 7,003,387

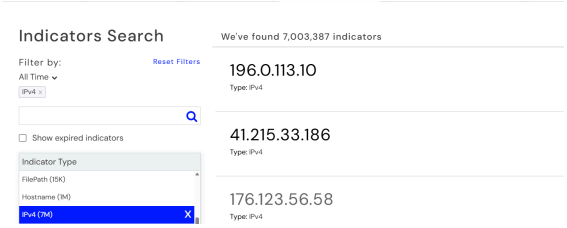


***Figure 4**: AlienVault OTX results showing IPv4 indicator count (7,003,387).*

***Source:** AlienVault OTX, https://otx.alienvault.com*

IPv6 count: 18,534

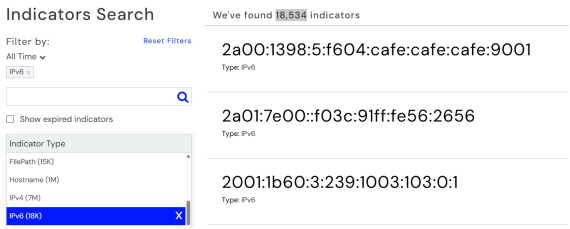


Figure 5: AlienVault OTX results showing IPv6 indicator count (18,534).

Source: AlienVault OTX, https://otx.alienvault.com

Within the Browse ⟶ Indicators tab for the pulse, filtering by the ransomware role revealed that the most common IOC type was FileHash-SHA256, with a total of 4,688 indicators. The high volume of file hash–based indicators reflect the file-centric nature of ransomware campaigns, which often involve deploying numerous malicious binaries. SHA-256 hashes serve as a reliable mechanism for tracking and detecting these files, enabling security researchers and defensive systems to identify and correlate ransomware variants across different environments (AT&T Cybersecurity, n.d.).

The most IOC for ransomware is **File Hash- SHA256 with 4,688 results**.

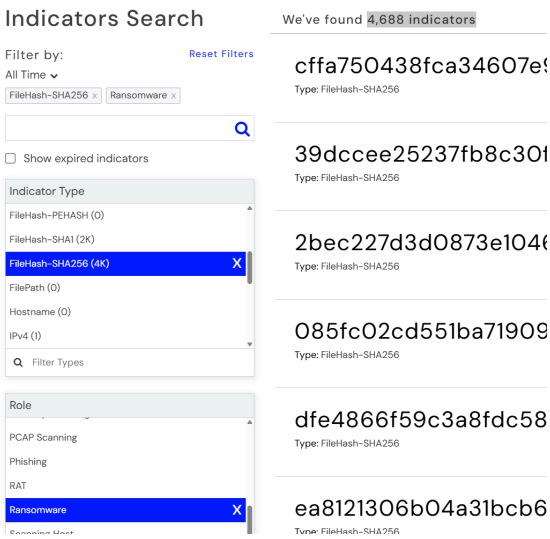


Figure 6: AlienVault OTX ransomware IOC results showing FileHash-SHA256 with 4,688 indicators.

Source: AlienVault OTX, https://otx.alienvault.com

To determine the number of pulses contributed by the user MetaDefender, the AlienVault OTX API was queried using a curl command. This level of contribution reflects the value of collaborative platforms such as OTX, where community-driven data enhances detection and response capabilities across organizations (AT&T Cybersecurity, n.d.).

Prompt: curl -H "X-OTX-API-KEY: b6d55885cf1914191da58eeb36db70e703796ca9cbcc7a8487f12e05988e03e2" https://otx.alienvault.com/api/v1/pulses/user/MetaDefender

This command queries the endpoint with my API key and the username Meta Defender. The result has a field count of 15221, which means the user **Meta Defender has contributed 15,221 pulses** to the OTX platform.

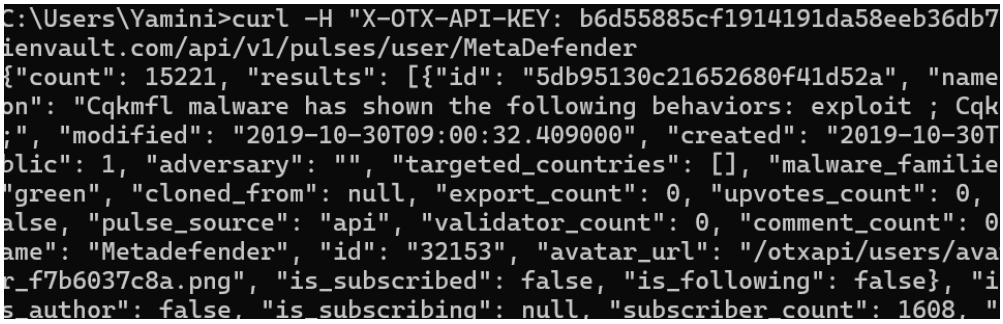


Figure 7*: Command-line output using curl and AlienVault OTX API showing MetaDefender contributions (15,221 pulses).*

Source: *Command-line output using curl and AlienVault OTX API, executed by the author.*

To determine the correct indicator type for Bitcoin addresses in **AlienVault OTX**, the API was queried to return the list of supported indicator types. The JSON response included the entry for Bitcoin addresses, which specifies the slug as **"bitcoin-address."**

This designation is critical for filtering or querying pulse data related to cryptocurrency addresses, ensuring accurate identification of Bitcoin-related indicators in threat intelligence workflows (AT&T Cybersecurity, n.d.).

curl -H "X-OTX-API-KEY:

b6d55885cf1914191da58eeb36db70e703796ca9cbcc7a8487f12e05988e03e2"

https://otx.alienvault.com/api/v1/pulses/indicators/types

The indicator type for Bitcoin Address in the AlienVault OTX API is:

Name: BitcoinAddress

Description: Bitcoin Address

Slug: **bitcoin-address**

***Figure 8**: Command-line output using curl and AlienVault OTX API showing supported indicator types, including Bitcoin address.*

***Source:** Command-line output using curl and AlienVault OTX*

The command below was used to query the AlienVault OTX API for any known malware samples that have been observed communicating with the domain microsoft.com.

curl -H "X-OTX-API-KEY:

b6d55885cf1914191da58eeb36db70e703796ca9cbcc7a8487f12e05988e03e2"

https://otx.alienvault.com/api/v1/indicators/domain/microsoft.com/malware

Yes, malware samples have been identified by AlienVault Labs, which attempted to connect to microsoft.com. One such detection is **Trojan:Win32/Emotet.YL**, observed on **2025-07-21 at 03:37:06**. Emotet is a notorious malware strain known for spreading through spam campaigns and stealing sensitive information. The sample was detected by Microsoft Defender and further classified by ClamAV as Win.Malware.Emotet-6993311-0.

C:\Users\Yamini>curl -H "X-OTX-API-KEY: b6d55885cf1914191da58eeb36db70e703796ca9cbcc7a8487f12e05988e03e2" https://otx.alienvault.com/api/v1/indicators/domain/microsoft.com/malware
{"data": [{"datetime_int": 1753093139, "hash": "7bc06281d12b1db6a67027087d94e80343e32634af4c6210ed87e644edd85dac", "detections": {"avast": null, "avg": null, "clamav": "Win.Dropper.Tofsee-9816235-0", "msdefender": "Trojan:Win32/Azorult.DSK!MTB"}, "date": "2025-07-21T10:18:59"}, {"datetime_int": 1753076110, "hash": "86f6dd910c252c770079d7db4287855ad2d0ed2108afb35a775705b5fe3f3703", "detections": {"avast": null, "avg": null, "clamav": "Win.Trojan.Fakeav-34492", "msdefender": "TrojanDownloader:Win32/Moure.gen!C"}, "date": "2025-07-21T05:35:10"}, {"datetime_int": 1753069086, "hash": "68272ad20598d8c605b11c1bc5ff02f0ff189106b7c0e34e70f3398fd8f3bc48", "detections": {"avast": null, "avg": null, "clamav": "Win.Trojan.Tofsee-7102058-0", "msdefender": "Backdoor:Win32/Tofsee.T"}, "date": "2025-07-21T03:38:06"}, {"datetime_int": 1753069026, "hash": "1aa10c09b94899a752130ff34e24e227bc4866c866db91b6c3fef82d666b479d", "detections": {"avast": null, "avg": null, "clamav": "Win.Malware.Emotet-6993311-0", "msdefender": "Trojan:Win32/Emotet.YL"}, "date": "2025-07-21T03:37:06"}, {"datetime_int": 1753068828, "hash": "acb61f61e9e241791498faa12ed4b836372768763adf662c481172d2b146ca14", "detections": {"avast": null, "avg": null, "clamav": "Win.Trojan.Tofsee-7102058-0", "msdefender": "Backdoor:Win32/Tofsee.T"}, "date": "2025-07-21T03:33:48"}, {"datetime_int": 1753051235, "hash": "4f54c39d1e6027ccc039cec3b897b2f6dc0c328cdcecdd855fc8243672836c63", "detections": {"avast": null, "avg": null, "clamav": "Win.Malware.Emotet-6993311-0", "msdefender": "Trojan:Win32/Emotet.YL"}, "date": "2025-07-20T22:40:35"}, {"datetime_int": 1753046308, "hash": "d69fee8385d8dd3e320cad9d7b763073e1d780d4e4ee0ae4a9c461684ec32a86", "detections": {"avast": null, "avg": null, "clamav": "Win.Dropper.Tofsee-7443490-0", "msdefender": "Backdoor:Win32/Tofsee.T"}, "date": "2025-07-20T21:18:28"}, {"datetime_int": 1753016474, "hash": "ea8cddd9fb6c54f505b64446032e266babbf6fdde330bf343d4beb58020964e2", "detections": {"avast": null, "avg": null, "clamav": "Win.Malware.Emotet-6993311-0", "msdefender": "Trojan:Win32/Emotet.YL"}, "date": "2025-07-20T13:01:14"}, {"datetime_int": 1753016365, "hash": "e99145141ca1442d5e895fb9557831f4ccd087afd423b6d3a6cd9c4e54f24a79", "detections": {"avast": null, "avg": null, "clamav": "Win.Malware.Unsafe-6979475-0", "msdefender": "Trojan:Win32/Emotet.YL"}, "date": "2025-07-20T12:59:25"}, {"datetime_int": 1753015797, "hash": "96bc9ea84f18fa9536d1b32515582a2d277c17991fa79318ec60749574421614", "detections": {"avast": null, "avg": null, "clamav": "Win.Malware.Emotet-6993311-0", "msdefender": "Trojan:Win32/Emotet.YL"}, "date": "2025-07-20T12:49:57"}], "size": 116877, "count": 116877}

Figure 9 *: Command-line output using curl and AlienVault OTX API showing detections for the microsoft.com domain, including Trojan:Win32/Emotet.YL.*

Source: *Command-line output using curl and AlienVault OTX API, executed by the author.*

Querying the HTTP scan data for the domain webapps.umgc.edu through the AlienVault OTX API revealed that the SSL certificate's expiration date is listed under the

key “443 certificate notAfter.” The certificate expired on **September 4, 2021, at 23:59:59 GMT**.

curl -H "X-OTX-API-KEY: b6d55885cf1914191da58eeb36db70e703796ca9cbcc7a8487f12e05988e03e2" https://otx.alienvault.com/api/v1/indicators/domain/webapps.umgc.edu/http_scans

```
C:\Users\Yamini>curl -H "X-OTX-API-KEY: b6d55885cf1914191da58eeb36db70e703796ca9cbcc7a8487f12e05988e03e2" https://otx.alienvault.com/api/v1/indicators/domain/webapps.umgc.edu/http_scans
{"data": [{"key": "80 title", "name": " 80 Title", "value": "WEBAPPS Redirect"}, {"key": "80 a_domains", "name": "80 A Domains", "value": "www.umuc.edu"}, {"key": "80 body", "name": "80 Body", "value": " html  head  title WEBAPPS Redirect /title  META http equiv= refresh  content= 0 URL=http://www.umuc.edu  /head  body bgcolor= ffffff  center The contents you are looking for have moved. You will be redirected to the new location automatically in 5 seconds. Please bookmark the correct page at  a href= http://www.umuc.edu  http://www.umuc.edu /a  /center /body /html "}, {"key": "80 header", "name": "80 Header", "value": "HTTP/1.1 200 OK Content Length: 416 Content Type: text/html Last Modified: Wed  17 Jun 2015 15:56:44 GMT Accept Ranges: bytes ETag:  b2d4a13516a9d01:0 Server: Microsoft IIS/7.5 X Powered By: ASP.NET Date: Tue  04 May 2021 03:41:17 GMT "}, {"key": "443 header", "name": "443 Header", "value": "HTTP/1.1 200 OK Content Length: 416 Content Type: text/html Last Modified: Wed  17 Jun 2015 15:56:44 GMT Accept Ranges: bytes ETag:  b2d4a13516a9d01:0 Server: Microsoft IIS/7.5 X Powered By: ASP.NET Date: Tue  04 May 2021 03:41:16 GMT "}, {"key": "443 certificate subject", "name": "443 Certificate Subject", "value": "US"}, {"key": "443 certificate subject ", "name": "443 Certificate Subject", "value": "20783"}, {"key": "443 certificate subject ", "name": "443 Certificate Subject", "value": "Maryland"}, {"key": "443 certificate subject ", "name": "443 Certificate Subject", "value": "Adelphi"}, {"key": "443 certificate subject ", "name": "443 Certificate Subject", "value": "3501 University Blvd. East"}, {"key": "443 certificate subject ", "name": "443 Certificate Subject", "value": "University of Maryland University College"}, {"key": "443 certificate subject ", "name": "443 Certificate Subject", "value": "Information Technology"}, {"key": "443 certificate subject ", "name": "443 Certificate Subject", "value": "webapps.umgc.edu"}, {"key": "443 certificate issuer ", "name": "443 Certificate Issuer", "value": "MI"}, {"key": "443 certificate issuer ", "name": "443 Certificate Issuer", "value": "Ann Arbor"}, {"key": "443 certificate issuer ", "name": "443 Certificate Issuer", "value": "Internet2"}, {"key": "443 certificate issuer ", "name": "443 Certificate Issuer", "value": "InCommon"}, {"key": "443 certificate issuer ", "name": "443 Certificate Issuer", "value": "InCommon RSA Server CA"}, {"key": "443 certificate version", "name": "443 Certificate Version", "value": 3}, {"key": "443 certificate serialNumber", "name": "443 Certificate Serialnumber", "value": "1A82BFCA6EACF05AB840C1E66B129B7F"}, {"key": "443 certificate notBefore", "name": "443 Certificate Notbefore", "value": "Sep  5 00:00:00 2019 GMT"}, {"key": "443 certificate notAfter", "name": "443 Certificate Notafter", "value": "Sep  4 23:59:59 2021 GMT"}, {"key": "443 certificate subjectAltName ", "name": "443 Certificate Subjectaltname", "value": "webapps.umuc.edu"}, {"key": "443 certificate OCSP", "name": "443 Certificate Ocsp", "value": "http://ocsp.usertrust.com"}, {"key": "443 certificate caIssuers", "name": "443 Certificate Caissuers", "value": "http://crt.usertrust.com/InCommonRSAServerCA_2.crt"}, {"key": "443 certificate crlDistributionPoints", "name": "443 Certificate Crldistributionpoints", "value": "http://crl.incommon-rsa.org/InCommonRSAServerCA.crl"}, {"key": "443 certificate_sha1", "name": "443 Certificate Sha1", "value": "5a74739176736f0b949943818ac525177592f410"}], "count": 27}
```


Figure 10 *: Command-line output using curl and AlienVault OTX API showing SSL certificate scan data for webapps.umgc.edu (expired September 4, 2021).*

Source: Command-line output using curl and AlienVault OTX API, executed by the author.

Summary of AlienVault OTX Usage in Cybersecurity Programs

If incorporated into a cybersecurity program, AlienVault OTX would serve primarily as a free and community-driven threat intelligence feed to enrich existing detection capabilities. Integration with platforms such as Microsoft Sentinel, Azure Defender, and Splunk allows for the scheduled ingestion of OTX pulses, enabling automated correlation of known indicators of compromise (IOCs) with internal security logs. This approach enhances the ability to proactively

identify malicious domains, IP addresses, file hashes, and URLs, thereby reducing dwell time and strengthening incident triage (AT&T Cybersecurity, n.d.).

From a strategic perspective, OTX can be leveraged to monitor trends in global threat campaigns and align them with an organization's internal risk profile. Comparing the latest OTX threat pulses with local telemetry supports prioritization of patching, proactive threat hunting, and risk communication. Operationally, the OTX API can be used to build automated workflows that enrich alerts in SIEM platforms with context such as malware families, tactics, techniques, and procedures (TTPs), and potential threat actor attribution. This additional intelligence enables Tier 1 and Tier 2 analysts to respond more efficiently and effectively (AT&T Cybersecurity, n.d.).

At the tactical level, OTX functions as a valuable lookup resource during investigations. For example, if a security platform generates an alert related to a suspicious domain, cross-referencing the domain in OTX determines whether it has been observed in recent global threat campaigns. This immediate context enhances situational awareness and guides decision-making on containment or deeper investigation. Overall, OTX complements existing security tooling by injecting community-shared threat intelligence into both automated pipelines and human-led analysis, ultimately improving detection and response outcomes (AT&T Cybersecurity, n.d.).

Comprehensive Threat Intelligence Tool Analysis

Cisco Talos

Cisco Talos Intelligence Group is one of the world's leading commercial threat intelligence teams, providing real-time information on vulnerabilities, malware campaigns, spam, and threat actor infrastructure. The Talos platform offers tools such as the Reputation Center, Email & Spam analysis, and Vulnerability Reports, which are widely used by security analysts to detect and mitigate risks across enterprise environments. For this project, Cisco Talos was used to identify high-severity vulnerabilities (CVSS 10), analyze global spam distribution, and gather actionable intelligence related to malicious email traffic (Cisco Talos Intelligence Group, n.d.).

Based on the global threat activity displayed on the **Cisco Talos Intelligence map**, **Australia** reported the lowest number of email-related events. At the time of observation, the map displayed only **one blue marker**, representing legitimate email traffic, with no significant malware or spam activity.

In contrast, regions such as **North America and Europe** showed multiple red and green markers, indicating higher volumes of spam and malware email traffic. This disparity illustrates that Australia had the lowest visible email activity during the observation period, while other regions experienced substantially greater volumes of malicious communications (Cisco Talos Intelligence Group, n.d.).

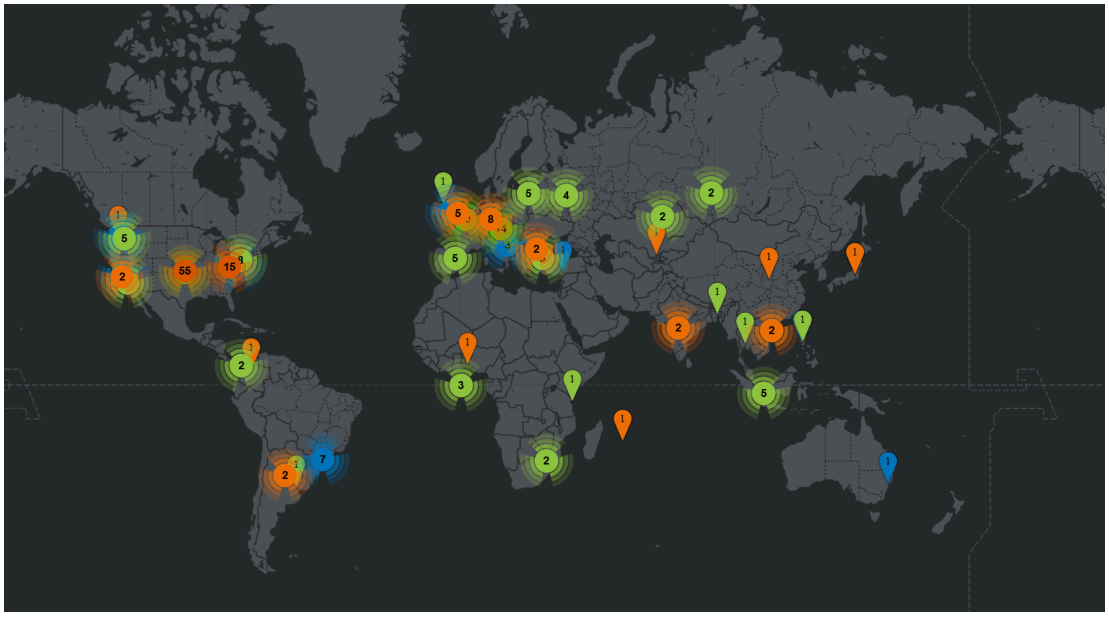


***Figure 11**: Cisco Talos Intelligence map showing global threat activity, with Australia reporting the lowest visible email traffic.*

***Source:** Cisco Talos, https://talosintelligence.com*

To provide insight into **regional email threat activity**, the Cisco Talos Intelligence map was examined with a focus on the Mid-Atlantic region of the United States. The closest malware-related email report was identified near **Columbus, Ohio**, represented by a green marker on the map. The threat details revealed an **IP address and hostname of 206.123.128.45**, categorized as **malware**, with a **last day email volume of 7.50**. This type of data enables analysts to track real-time threat sources and monitor emerging infection vectors within specific geographic areas (Cisco Talos Intelligence Group, n.d.).

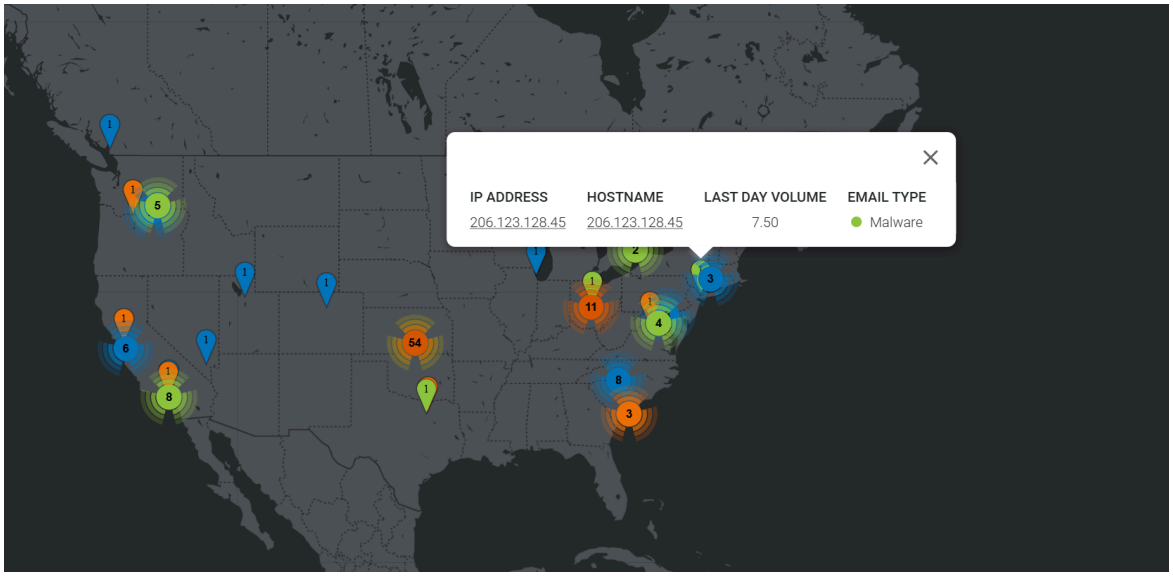


***Figure 12**: Cisco Talos Intelligence map showing a malware-related email report near Columbus, Ohio, with details including IP 206.123.128.45.*

***Source:** Cisco Talos, https://talosintelligence.com*

An evaluation of the domain **mail.umgc.edu** using the Cisco Talos Intelligence platform revealed several important attributes relevant to risk analysis. The lookup confirmed that the **network owner is Microsoft Corp**, which indicates that the University of Maryland Global Campus leverages Microsoft's infrastructure to deliver its email services. The domain was categorized under **Education** and assigned a **favorable web reputation**, reflecting that it is not associated with spam, malware, or other malicious activity. Additionally, the analysis showed no significant email volume during the observation period and no evidence of the domain being placed on Talos block lists. Collectively, these findings demonstrate that mail.umgc.edu maintains a powerful reputation and operational integrity, making it a trusted domain for academic communications (Cisco Talos Intelligence Group, n.d.).

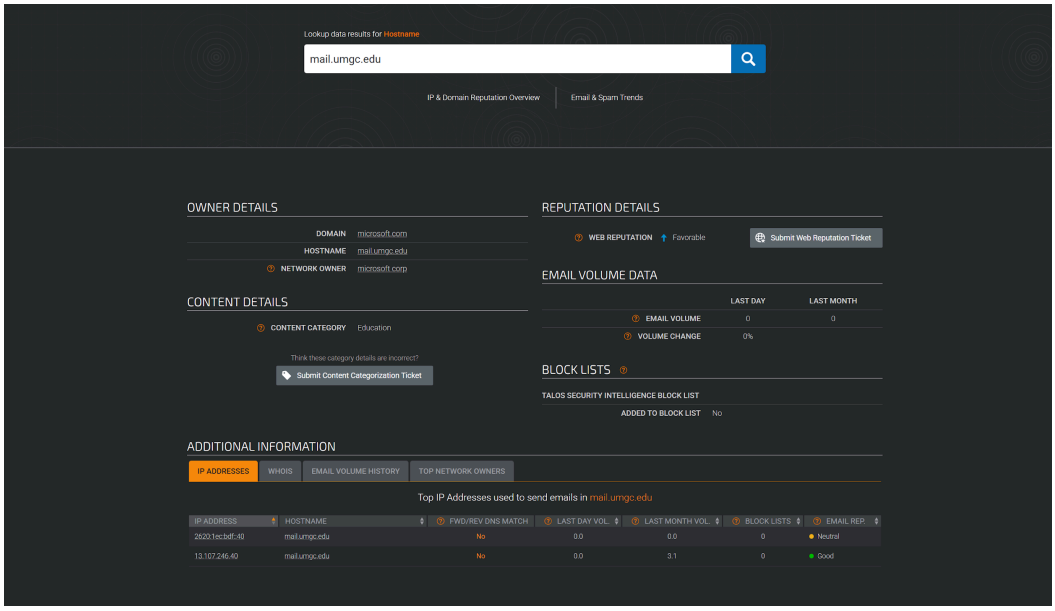


Figure 13*: Cisco Talos Intelligence lookup results for the domain mail.umgc.edu, showing ownership, reputation, and email activity details.*

Source: *Cisco Talos, https://talosintelligence.com*

A **WHOIS record lookup** for the domain **umgc.edu** provided details about ownership, technical contact, and registration information. The record showed that the domain was last updated on **May 10, 2025**, and is active through **July 31, 2027**. The domain was originally registered on **June 27, 2019**, and is managed by the DNS Administrator for the University of Maryland University College. The technical contact is listed in Adelphi, Maryland, with associated email and phone details, and the record also identifies multiple authoritative name servers hosted on Amazon's AWS infrastructure. These findings confirm that the domain is actively maintained and securely registered through a major cloud provider, ensuring operational continuity for university communications (Cisco Talos Intelligence Group, n.d.).

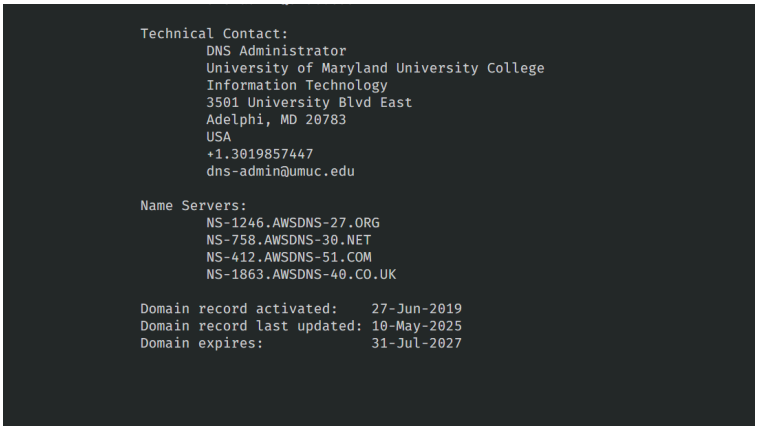


Figure 14: WHOIS record for umgc.edu showing registration details, name servers, and expiration date of July 31, 2027.

Source: Cisco Talos, https://talosintelligence.com

An analysis of global spam activity using the **Cisco Talos Intelligence Email & Spam Trends tool** revealed the top countries contributing to outbound spam volume. By applying the **"Spam" filter** and reviewing the most recent report, the data showed that the **United States (7.7)**, **China (6.9)**, and **Benin (6.9)** were the three leading sources of spam traffic. These figures represent the **last day volume** of spam originating from IP addresses registered in each country. Understanding these geographic trends provides valuable context for organizations, enabling the development of **geo-based filtering rules** and enhancing email security defenses through threat intelligence enrichment (Cisco Talos Intelligence Group, n.d.).

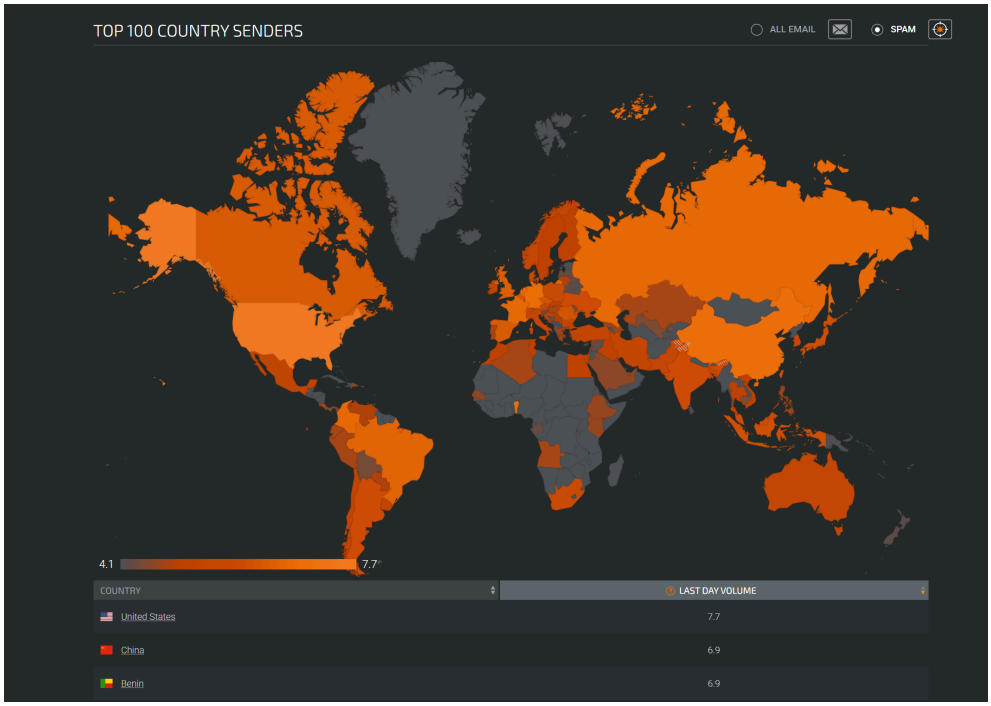
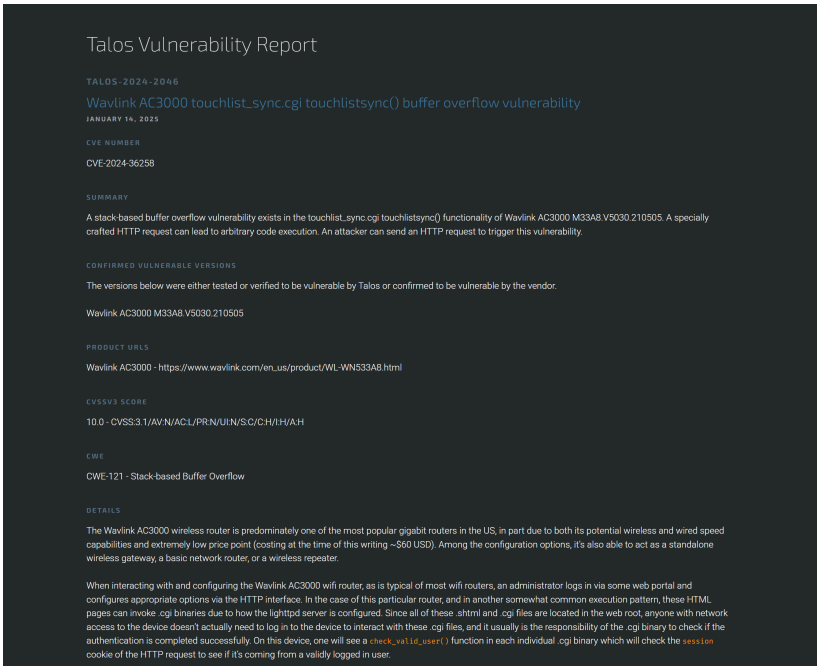


***Figure 15**: Cisco Talos Intelligence Email & Spam Trends tool showing top global spam-sending countries: United States, China, and Benin.*

***Source:** Cisco Talos, https://talosintelligence.com/reputation_center/email_rep*

To assess the potential impact of severe vulnerability, **Cisco Talos vulnerability reports** were reviewed. Among the findings, **CVE-2024-34166** was identified with a **CVSS score of 10.0**, representing the highest possible level of severity. This vulnerability, found in the **Wavlink AC3000 touchlist_sync.cgi functionality**, can allow an attacker to send crafted HTTP requests that lead to arbitrary code execution. The affected product, **Wavlink AC3000 routers**, is a widely deployed consumer networking device, making this vulnerability particularly impactful for home and small business environments (Cisco Talos Intelligence Group, n.d.).



Talos Vulnerability Report

TALOS-2024-2046

Wavlink AC3000 touchlist_sync.cgi touchlistsync() buffer overflow vulnerability

JANUARY 14, 2025

CVE NUMBER

CVE-2024-36258

SUMMARY

A stack-based buffer overflow vulnerability exists in the touchlist_sync.cgi touchlistsync() functionality of Wavlink AC3000 M33A8.V5030.210505. A specially crafted HTTP request can lead to arbitrary code execution. An attacker can send an HTTP request to trigger this vulnerability.

CONFIRMED VULNERABLE VERSIONS

The versions below were either tested or verified to be vulnerable by Talos or confirmed to be vulnerable by the vendor.

Wavlink AC3000 M33A8.V5030.210505

PRODUCT URLS

Wavlink AC3000 - https://www.wavlink.com/en_us/product/WL-WN533A8.html

CVSSV3 SCORE

10.0 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-121 - Stack-based Buffer Overflow

DETAILS

The Wavlink AC3000 wireless router is predominately one of the most popular gigabit routers in the US, in part due to both its potential wireless and wired speed capabilities and extremely low price point (costing at the time of this writing ~$60 USD). Among the configuration options, it's also able to act as a standalone wireless gateway, a basic network router, or a wireless repeater.

When interacting with and configuring the Wavlink AC3000 wifi router, as is typical of most wifi routers, an administrator logs in via some web portal and configures appropriate options via the HTTP interface. In the case of this particular router, and in another somewhat common execution pattern, these HTML pages can invoke .cgi binaries due to how the lighttpd server is configured. Since all of these .shtml and .cgi files are located in the web root, anyone with network access to the device doesn't actually need to log in to the device to interact with these .cgi files, and it usually is the responsibility of the .cgi binary to check if the authentication is completed successfully. On this device, one will see a `check_valid_user()` function in each individual .cgi binary which will check the `session` cookie of the HTTP request to see if it's coming from a validly logged in user.

Figure 16*: Cisco Talos Vulnerability Report for CVE-2024-34166, affecting Wavlink AC3000 routers with a critical CVSS score of 10.0.*

Source: *Cisco Talos, https://talosintelligence.com/vulnerability_reports*

Summary

This vulnerability exists in the Wavlink AC3000 router's web interface, specifically in the touchlist_sync.cgi endpoint. Due to insufficient input validation, remote attackers can inject arbitrary system commands into the web interface through crafted HTTP requests. The flaw does not require authentication, making it an elevated risk vector for unauthenticated remote command execution.

With a CVSS score of 10, this vulnerability affects the confidentiality, integrity, and availability of the target device, allowing full system compromise (Cisco Talos Intelligence Group, n.d.).

How an Attacker Could Exploit It:

If an organization had deployed this device and had not applied a firmware update or workaround, an attacker could:

- Exploit the router remotely by sending a malicious HTTP GET or POST request to the touchlist_sync.cgi page.
- Inject and execute shell commands like wget, rm, or chmod to download and install malware, create backdoors, hijack network traffic, shut down or wipe the device.
- Use the compromised router as a pivot point into the internal network for lateral movement or reconnaissance.

Nmap

Nmap (Network Mapper) is an open source security scanner widely used for network discovery and vulnerability assessment. It plays a critical role in threat intelligence gathering by identifying active devices, open ports, running services, and operating system details across networked assets. From a cybersecurity defense perspective, Nmap enables analysts to detect potential attack vectors, misconfigured services, and unauthorized access points. It is especially valuable for proactively monitoring enterprise environments, auditing firewall configurations, and validating patching efforts. When used regularly, Nmap contributes to a broader threat intelligence strategy by uncovering the network footprint and surface area that adversaries may exploit (Nmap, n.d.).

Nmap Host and Service Discovery:

IP Addresses: The Nmap scans revealed distinct IP addresses for each system. The host **umgc-tomcat9.azurewebsites.net** resolved to **10.13.246.13**, while both **umgc-juiceshop.azurewebsites.net** and **umgc-web-dvwa.azurewebsites.net** shared the IP address **10.13.246.5**. In addition, two internal desktop systems were identified with separate IPs: **10.11.11.117** for the Windows host and **10.11.11.116** for the Linux host. These results highlight a mix of shared and unique infrastructure across the scanned environments.

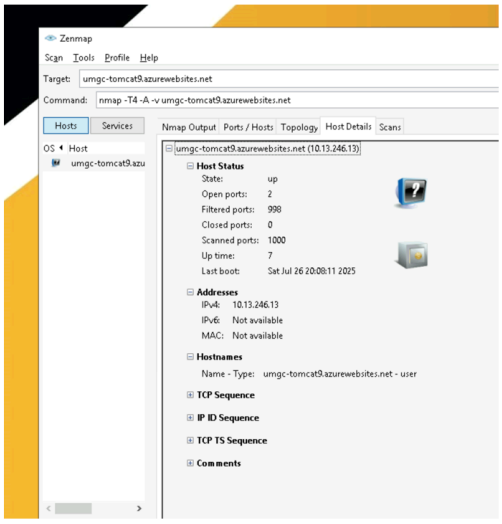
Ports Scanned: Each of the five systems underwent a scan of **1,000 ports**, ensuring comprehensive coverage of commonly used and potentially vulnerable network services. This uniform scanning approach provided a consistent basis for comparing the attack surfaces of the different hosts.

Open Ports: The scan results showed that the three web application hosts were limited to only **two open ports: 80 (HTTP)** and **443 (HTTPS)**, reflecting minimal service exposure. In contrast, the Windows host revealed **10 open ports**, including **22, 135, 139, 445, 1947, 2179, 3389, 5357, 8000, and 8089**, which indicates a broader service footprint. The Linux host presented a smaller surface, with just **two open ports: 22 (SSH)** and **3389 (RDP)**. These findings demonstrate the differences in exposure between web application servers and multi-service desktop systems.

Services Detected: The open ports corresponded to a range of services. These included **SSH (22), HTTP (80), Microsoft RPC (135), NetBIOS-SSN (139), HTTPS (443), SMB over TCP/IP (445), SafeNet HASP License Manager (1947), Microsoft RemoteFX (2179), RDP (3389), Microsoft HTTPAPI (5357), Splunkd (8000), and Splunkd – remote login**

disabled (8089). This mapping of ports to services provides insight into potential attack vectors and highlights the importance of monitoring and patching network services exposed to external traffic.

Operating Systems: Finally, the scans attempted to identify the operating systems of each host. No operating system fingerprints could be determined for the three web application hosts, which is common in hosted environments. The Windows host was successfully identified as **Microsoft Windows 10, version 1703**, with an accuracy of **92%**, while the Linux host was detected as **Linux 2.6.32**, with an accuracy of **95%**. This contrast underscores the differences in system-level visibility between cloud-based web applications and traditional desktop systems.



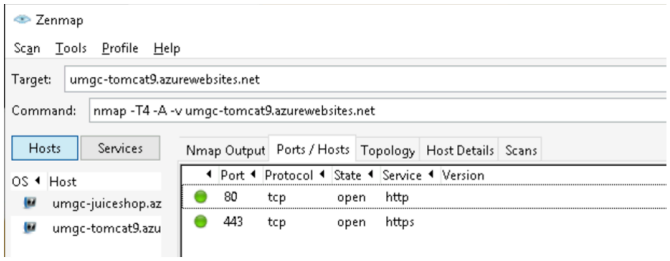


Figure 17. *Nmap scan results for umgc-tomcat9.azurewebsites.net*

Source: *Nmap scan results.*

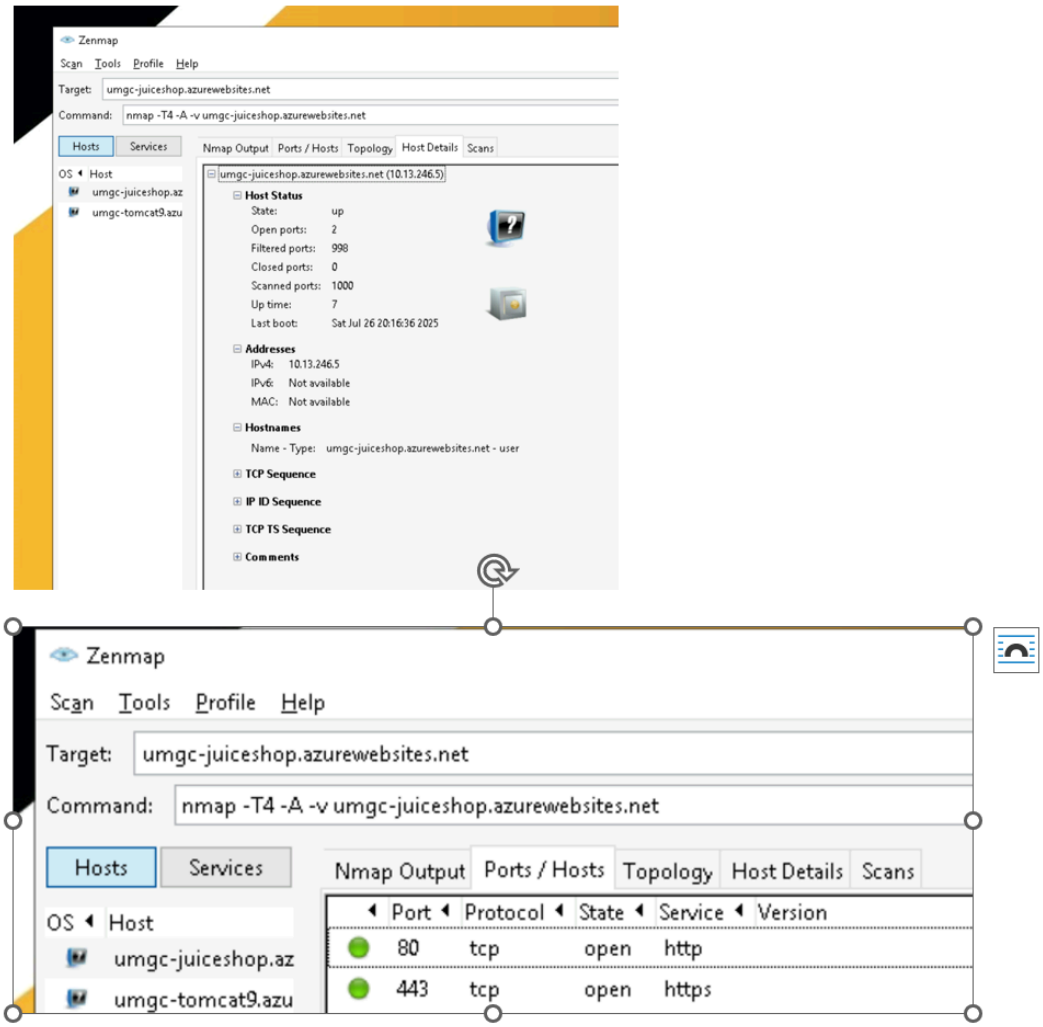


Figure 18. *Nmap scan results for umgc-juiceshop.azurewebsites.net*

Source: *Nmap scan results.*

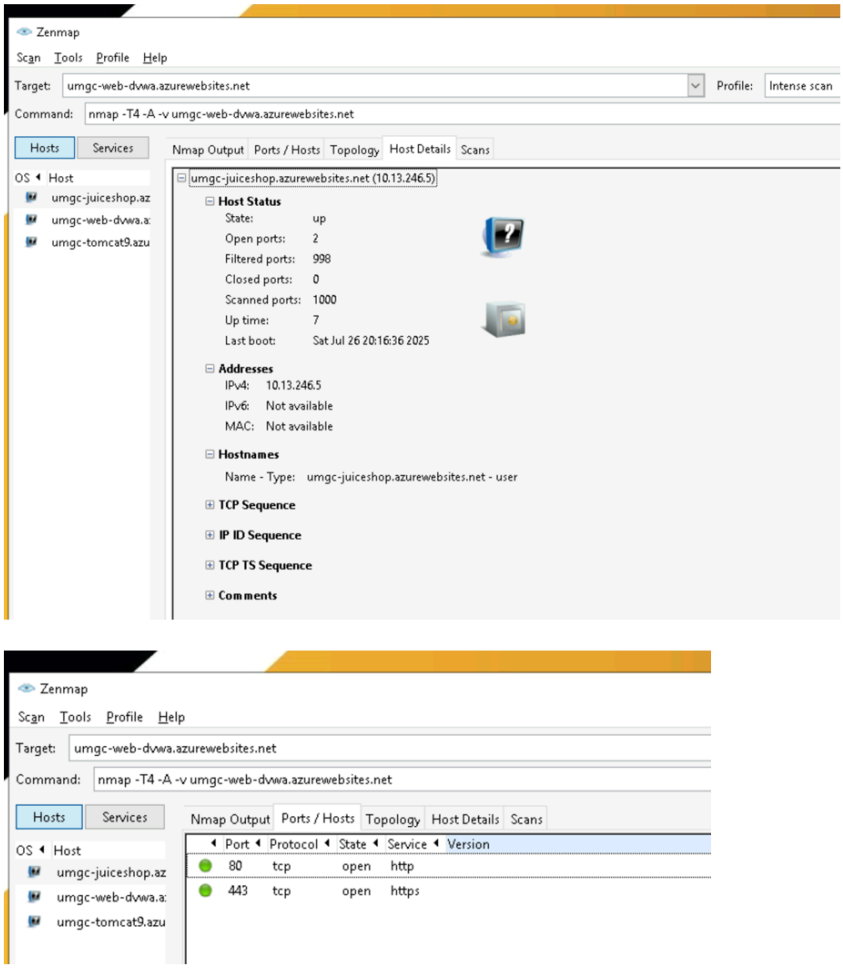


Figure 19. *Nmap scan results for umgc-web-dvwa.azurewebsites.net*

Source: *Nmap scan results.*

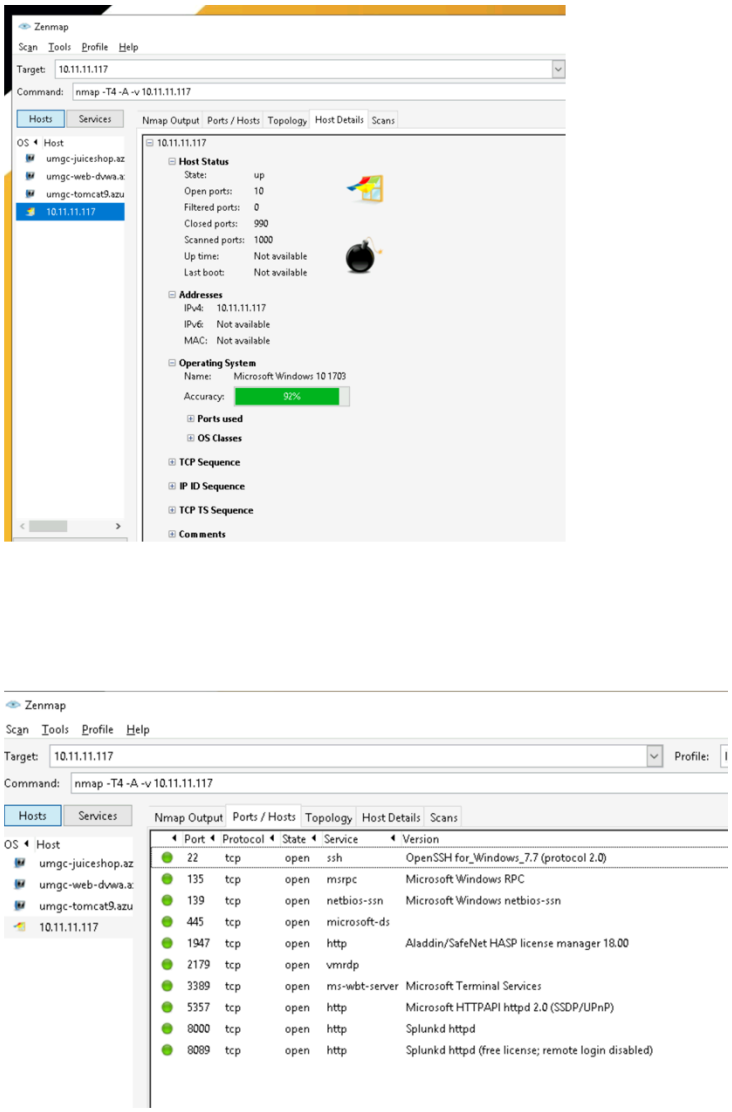


Figure 20: *Nmap scan results for Windows Desktop (10.11.11.117) showing multiple open ports and detected OS (Windows 10).*

Source: *Nmap scan results.*

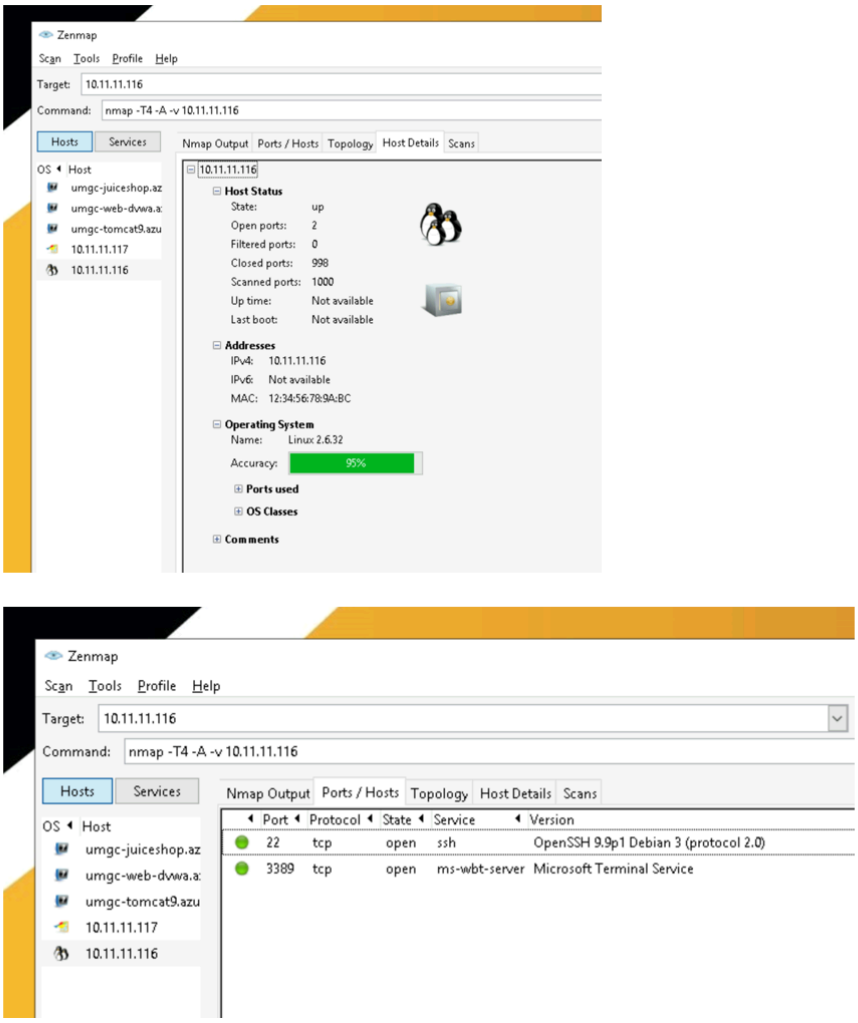


Figure 21. *Nmap scan results for Linux Desktop (10.11.11.116) showing two open ports and detected OS (Linux 2.6.32).*

Source: *Nmap scan results.*

This visual illustrates the extended network topology generated from the Zenmap scans using the fisheye display. The central scanning node, labeled *localhost*, is shown with direct connections to multiple target hosts. Each host is represented with a color-coded node to indicate status: **green nodes represent active and responsive systems**, while the **red node highlights a system with potential exposure or higher security risk**. This visualization provides a clear overview of the scanned environment, enabling analysts to quickly interpret host availability, connectivity, and areas requiring deeper investigation.

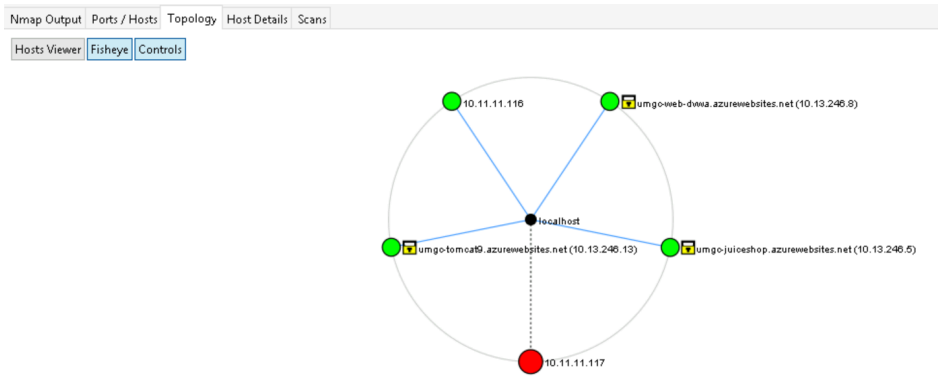


Figure 22: *Nmap Topology Map (Fisheye Display)*

Source: *Zenmap (Nmap GUI), umgc.edu*

From a cybersecurity defense perspective, running Nmap scans on networked assets is like regularly checking the doors and windows of a building to ensure nothing is left open. Nmap helps identify open ports, running services, and even potential vulnerabilities that attackers could exploit. By proactively scanning with tools like Nmap,

defenders can catch misconfigurations, unauthorized services, or exposed systems before a real threat actor does (Lyon, n.d.).

Regular scans are crucial because IT environments are dynamic, systems are updated, new assets come online, and services change constantly. What was secure last month might be vulnerable today. Continuous monitoring helps maintain visibility and security hygiene across the network (Scarfone & Mell, 2007). Especially in large or cloud connected environments, where assets may scale up or down quickly, scheduled scans become part of a strong vulnerability management process.

Kali Linux

Dnsenum:

The **dnsenum** tool is a widely used DNS enumeration script leveraged during the reconnaissance phase of cybersecurity assessments. It automates the collection of DNS-related data, including A records, NS records, MX records, subdomains, and IP ranges (Offensive Security, n.d.). By identifying publicly exposed infrastructure, dnsenum provides critical intelligence that supports vulnerability assessments and strengthens threat detection efforts.

To illustrate its capabilities, the command **dnsenum --enum umgc.edu** was executed against the *umgc.edu* domain, enabling a comprehensive discovery of domain-related components. This process revealed valuable insights into the network footprint and potential exposure points associated with the target domain.

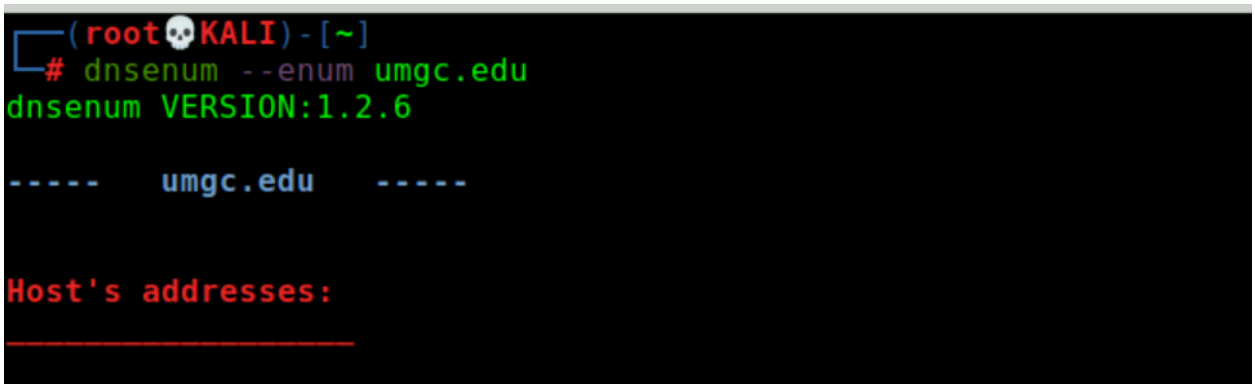


Figure 23: *Execution of dnsenum tool on the umgc.edu domain*

Source: *dnsenum command output in Kali Linux terminal*

The dnsenum scan revealed key DNS information for the *umgc.edu* domain, including mail exchange (MX) servers, which play a critical role in managing incoming email traffic. Analyzing MX records is a valuable practice in threat intelligence, as it helps identify the mail provider in use, assess potential risks associated with third-party services, and detect misconfigurations that could be exploited by attackers for phishing or spam campaigns.

In this case, **four MX servers** were discovered, all associated with the domain **umgc-edu.mail.protection.outlook.com**. The corresponding IPv4 addresses were **52.101.194.4**, **52.101.9.5**, **52.101.40.24**, and **52.101.11.15**. These results confirm that the institution relies on Microsoft Outlook's protection service to handle email communications, which provides additional layers of filtering and security controls.

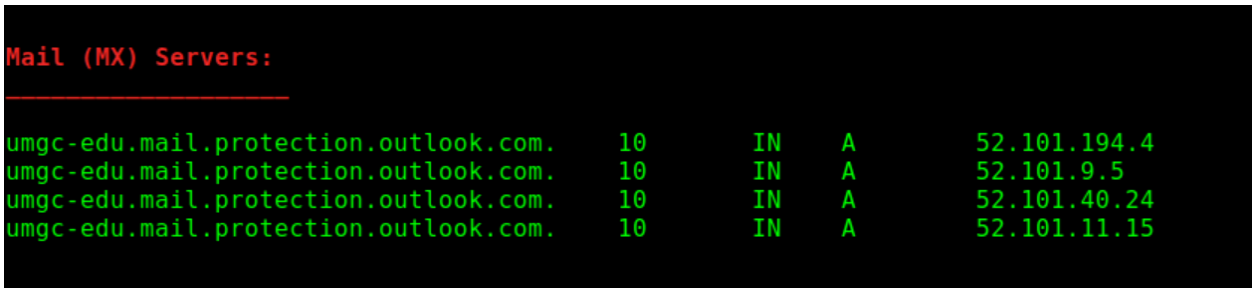


Figure 24: *MX Records Enumeration for umgc.edu using dnsenum*

Source: *dnsenum command output in Kali Linux terminal.*

The dnsenum scan of the *umgc.edu* domain also revealed four authoritative name servers (NS records), which play a critical role in directing DNS queries and managing domain traffic. Identifying name servers is a valuable step in threat intelligence, as it highlights the underlying infrastructure and can expose potential misconfigurations or third-party dependencies that might be exploited. The name servers discovered were **ns-758.awsdns-30.net (205.251.194.246)**, **ns-1246.awsdns-27.org (205.251.196.222)**, **ns-1863.awsdns-40.co.uk (205.251.199.71)**, and **ns-412.awsdns-51.com (205.251.193.156)**. Together, these findings confirm that UMGC's DNS infrastructure is managed through Amazon Web Services (AWS), reflecting the institution's reliance on a cloud-based provider for scalability and resilience.

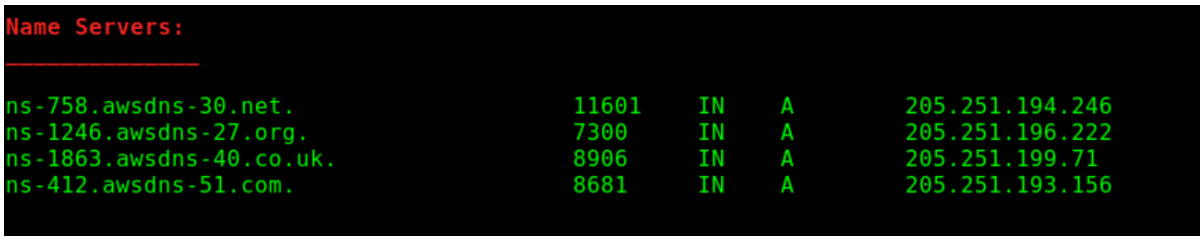


Figure 25: *Name Server Records for umgc.edu using dnsenum*

Source: *dnsenum command output in Kali Linux terminal.*

Name servers are responsible for resolving domain names into IP addresses, enabling devices to locate and communicate over the internet. They are a fundamental part of the DNS infrastructure and play a critical role in making web services accessible (Kinsta, 2024). In threat intelligence, analyzing name servers can help identify third-party DNS providers, detect misconfigurations, and map the digital footprint of an organization. Malicious actors often exploit vulnerable or poorly configured DNS systems to redirect traffic, exfiltrate data, or hide command-and-control (C2) domains.

An MX (Mail Exchange) server is responsible for receiving and routing email messages for a domain. It uses DNS records to direct incoming emails to the correct mail server based on priority settings (Cloudflare, n.d.).

From a threat intelligence perspective, examining MX records helps analysts identify the email service provider (e.g., Microsoft, Google), assess the organization's email security posture, and detect misconfigured or outdated mail systems. Attackers often exploit weak or exposed mail infrastructure for phishing, email spoofing, or business email compromise (BEC). Identifying MX server IPs also helps detect potential spam relays or track email-based attack vectors during investigations.

The dnsenum scan of the *umgc.edu* domain identified **three distinct IP address blocks** associated with the university’s infrastructure. These blocks are **131.171.0.0/16**, **151.101.0.0/16**, and **54.64.0.0/11**. The discovery of IP ranges is particularly valuable in cybersecurity analysis, as it reveals the broader allocation of network resources tied to the organization.

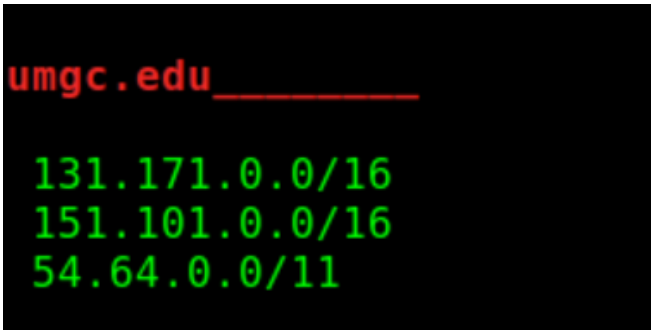


Figure 26: *IP Blocks Associated with umgc.edu Identified by dnsenum*

Source: *dnsenum command output in Kali Linux terminal.*

In the dnsenum output for the umgc.edu domain, the IP block discovered is listed as 131.171.0.0/16, which includes a significantly broad range of IPv4 addresses. A /16 CIDR block uses the first 16 bits for the network portion and leaves the remaining 16 bits for host addresses. This means a /16 block contains 65,536 possible IPv4 addresses. Although the question specifically asks 131.171.0.0/32 , which was not shown in the output , it is useful to know that a **/32 block refers to only one IP address**, typically used to represent a single device. Therefore, while the /16 range seen in the scan provides a large network of addresses, **the /32 range includes only one**.

DNS records help define how internet traffic is managed for a domain. An **A record** connects a domain name to its IPv4 address, allowing users to access websites by name instead of IP. An **NS record** points to the name servers that manage the DNS settings for the domain, telling other systems where to get authoritative DNS responses. An **MX record** identifies the mail servers responsible for receiving email for the domain, which is essential for directing email traffic properly. A **CNAME record** creates an alias from one domain to another, helping to simplify domain redirection and hosting setups.

Each of these records plays a significant role in how systems communicate and understanding them is key in both system administration and threat intelligence (Cloudflare, n.d.).

The **dnsenum** scan revealed that the subdomain *europe.umgc.edu* is publicly resolvable and associated with four IPv4 addresses: **151.101.195.10, 151.101.131.10, 151.101.67.10, and 151.101.3.10**.

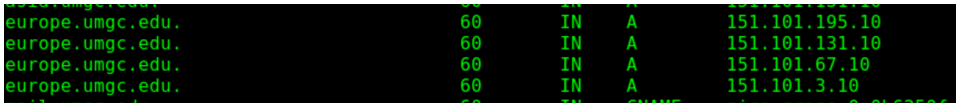


Figure 24: *dnsenum output showing records for europe.umgc.edu*

Source: *Output from dnsenum umgc.edu command executed in Kali Linux terminal.*

By contrast, attempts to resolve the subdomain *vpn.europe.umgc.edu* resulted in an **NXDOMAIN** response, meaning that no IP address was returned. This indicates that the subdomain does not exist in public DNS. The absence of resolution suggests that it may be inactive, restricted for internal use only, or not published via external name servers. While *europe.umgc.edu* is valid and accessible, the *vpn.europe.umgc.edu* subdomain could not be verified using either dnsenum or nslookup.

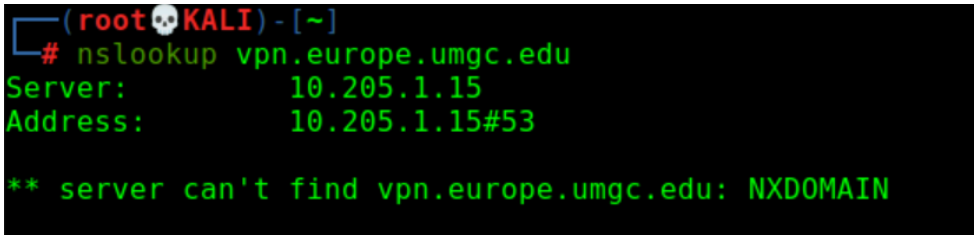


Figure 25: *nslookup vpn.europe.umgc.edu output showing NXDOMAIN*

Source: nslookup vpn.europe.umgc.edu command executed in Kali Linux terminal.

Dnsmap:

The **dnsmap** tool is designed to identify subdomains of a given domain using a dictionary-based brute-force approach. It is frequently applied in the reconnaissance phase of penetration testing to uncover public-facing subdomains that may expose additional infrastructure or services. Unlike **dnsenum**, which collects multiple DNS record types, dnsmap is focused specifically on detecting subdomains and resolving their corresponding IPv4 addresses.

For the domain *umgc.edu*, the command dnsmap umgc.edu was executed to enumerate subdomains. The tool systematically attempted to resolve entries from its built-in wordlist, producing a list of valid subdomains and their associated IP addresses. This process revealed subdomains such as **go.umgc.edu**, resolved to **52.72.49.79**, and **help.umgc.edu**, resolved to **151.101.67.10**.

The results provide valuable intelligence for both defensive and offensive security operations. From a defensive perspective, the discovery of subdomains helps organizations monitor misconfigured or forgotten services that could introduce risk. From an offensive perspective, such intelligence can reveal potential entry points into hidden services, development environments, or exposed internal systems.

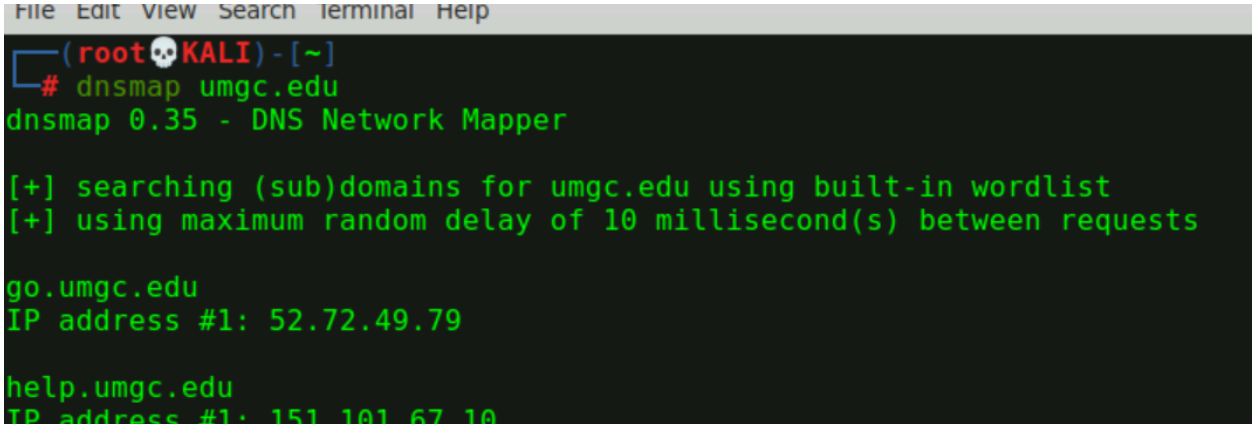


Figure 26: *dnsmap umgc.edu output showing discovered subdomains and associated IPv4 addresses*

Source: *dnsmap umgc.edu command executed in Kali Linux terminal.*

According to the **dnsmap** scan results, a total of **16 subdomains** were identified for the *umgc.edu* domain. These subdomains represent publicly resolvable hosts that may be associated with numerous services, applications, or environments tied to the institution. The scan also revealed **42 associated IP addresses**, along with **2 internal IP addresses**, highlighting the range of infrastructure linked to the domain.

Identifying subdomains is a crucial step in reconnaissance because they often uncover additional services, hidden environments, or potential entry points that may not be visible through the primary domain. This knowledge enhances threat intelligence by revealing possible misconfigurations, legacy systems, or overlooked assets that could be exploited if left unmonitored.

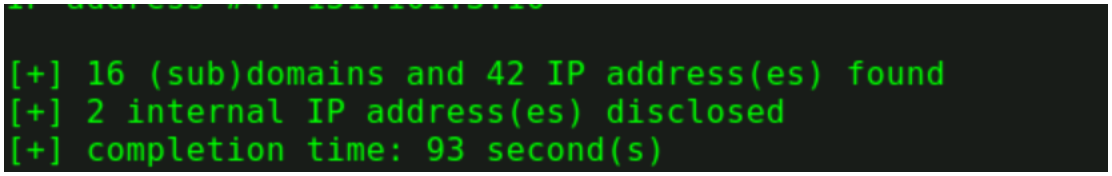
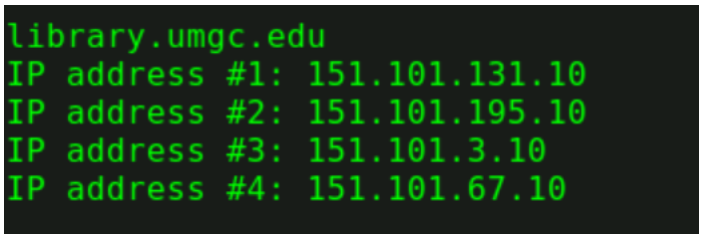


Figure 27: *dnsmap umgc.edu scan output showing 16 discovered subdomains and associated IP addresses.*

Source: *dnsmap umgc.edu command executed in Kali Linux terminal.*

The **dnsmap** scan identified the subdomain *library.umgc.edu* as being associated with four distinct IPv4 addresses. Specifically, the subdomain resolves to **151.101.131.10, 151.101.195.10, 151.101.3.10, and 151.101.67.10**. The presence of multiple IP addresses for a single subdomain indicates the use of load balancing or content delivery network (CDN) services, which are commonly implemented to improve reliability, distribute traffic efficiently, and enhance overall performance. From a cybersecurity perspective, recognizing these associated IP addresses is valuable for monitoring potential attack surfaces and ensuring that each endpoint is properly secured.



Source: Output from dnsmap umgc.edu command in Kali Linux showing resolved IP addresses for library.umgc.edu.

The dnsmap scan disclosed **two internal IP addresses** associated with the subdomain web.umgc.edu. The internal IPs are:

- **10.202.41.88**
- **10.202.40.163**

These addresses fall within the **private IP range 10.0.0.0/8**, which is reserved for internal use and is not routable on the public internet.

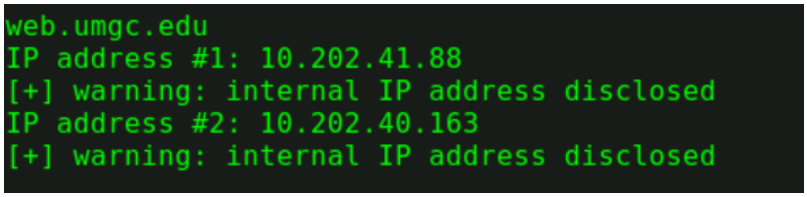


Figure 28: *dnsmap umgc.edu output showing resolved IP addresses for library.umgc.edu*

Source: *dnsmap umgc.edu command executed in Kali Linux terminal.*

In the context of an offensive cyber operation, the presence of internal IPs in public DNS records may indicate misconfiguration or poor network segmentation. This information could assist an attacker in **mapping the internal network structure**, identifying potential targets for lateral movement, or crafting targeted phishing or VPN attacks. If the attacker gains access to a connected system or VPN, these internal IPs could serve as direct targets for exploitation, especially if they expose administrative interfaces or legacy services.

The **dnsmap** scan identified that the subdomain *kb.umgc.edu* is associated with eight distinct IPv4 addresses. These include **52.217.81.67, 52.217.232.197, 16.182.97.213, 16.15.194.67, 16.15.177.129, 54.231.225.117, 16.15.177.206, and 54.231.130.205**. The presence of multiple IP associations for a single subdomain suggests reliance on distributed infrastructure, potentially involving cloud service

providers or content delivery networks. This configuration enhances performance and redundancy but also broadens the scope of potential attack surfaces.

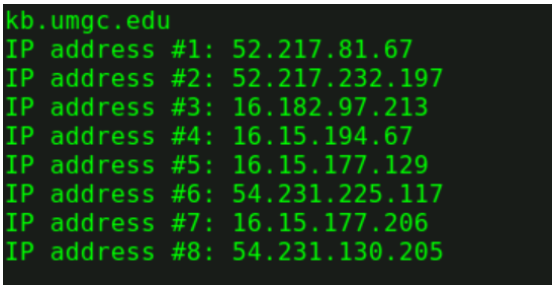


Figure 29: *dnsmap umgc.edu output showing IPv4 addresses assigned to kb.umgc.edu*

Source: *dnsmap umgc.edu command executed in Kali Linux terminal.*

IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6) are both protocols used for identifying devices on a network and routing traffic across the internet. IPv4 uses a 32-bit addressing scheme, which allows for approximately 4.3 billion unique IP addresses. These addresses are written in dotted decimal format, such as 192.168.0.1. Due to the explosive growth of internet connected devices, the available IPv4 address space has become exhausted, leading to the development of IPv6. IPv6, by contrast, uses a 128-bit addressing format, which supports approximately 340 undecillion unique addresses, an incomprehensibly considerable number. IPv6 addresses are written in colon-separated hexadecimal, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334. In addition to its expanded address capacity, IPv6 introduces several improvements over IPv4, including native support for IPsec, simplified packet headers, more efficient routing, and the elimination of NAT (Network Address Translation) in many use cases. From a security and performance

perspective, IPv6 enables end-to-end connectivity, making communication more direct and less reliant on intermediate devices. It also supports auto-configuration and better multicast routing, improving scalability in large and dynamic networks. While IPv4 is still widely used today, the transition to IPv6 is ongoing and critical for the future of the internet (Lifewire, 2020; AWS, n.d.).

Below are the repeated IPv4 addresses identified in the dnsmap scan of the umgc.edu domain. These addresses were observed across multiple subdomains, which suggest shared backend infrastructure or the use of a content delivery network (CDN). Identifying repeated IP addresses is useful in threat intelligence, as it may reveal centralized hosting platforms or single points of failure that attackers could exploit.

IPv4 Address	**Associated Subdomains**
151.101.131.10	help.umgc.edu, library.umgc.edu, m.umgc.edu, my.umgc.edu, support.umgc.edu, www.umgc.edu
151.101.195.10	help.umgc.edu, library.umgc.edu, m.umgc.edu, my.umgc.edu,

	support.umgc.edu, www.umgc.edu
151.101.3.10	help.umgc.edu, library.umgc.edu, m.umgc.edu, my.umgc.edu, support.umgc.edu, www.umgc.edu
151.101.67.10	help.umgc.edu, library.umgc.edu, m.umgc.edu, my.umgc.edu, support.umgc.edu, www.umgc.edu
13.107.246.40	mail.umgc.edu, sf.umgc.edu

The **dnsmap** scan identified the IPv4 address associated with the subdomain *sf.umgc.edu* as **13.107.246.40**. This mapping confirms that the subdomain is actively tied to a single public-facing IP address. From a threat intelligence perspective, such information is valuable for monitoring potential exposure, verifying infrastructure alignment with trusted service providers, and detecting malicious activity targeting this endpoint.

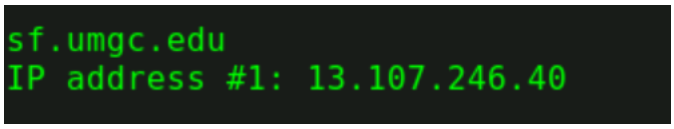


Figure 30*: dnsmap umgc.edu output showing IPv4 address assigned to sf.umgc.edu*

Source: *dnsmap umgc.edu command executed in Kali Linux terminal.*

To enhance subdomain discovery for *umgc.edu*, the **dnsmap** tool was executed with an extended wordlist to identify additional hosts not detected in the initial scan. The command utilized the SecLists project's DNS wordlist, a widely recognized resource for security testing:

dnsmap umgc.edu -w /usr/share/seclists/Discovery/DNS/namelist.txt

By leveraging this more comprehensive dataset, previously undetected subdomains such as *asia.umgc.edu* and *europe.umgc.edu* were successfully identified along with their associated IP addresses. Using larger and well-curated wordlists increases the effectiveness of reconnaissance by uncovering hidden or less common subdomains, thereby providing a more accurate picture of the organization's exposed infrastructure.

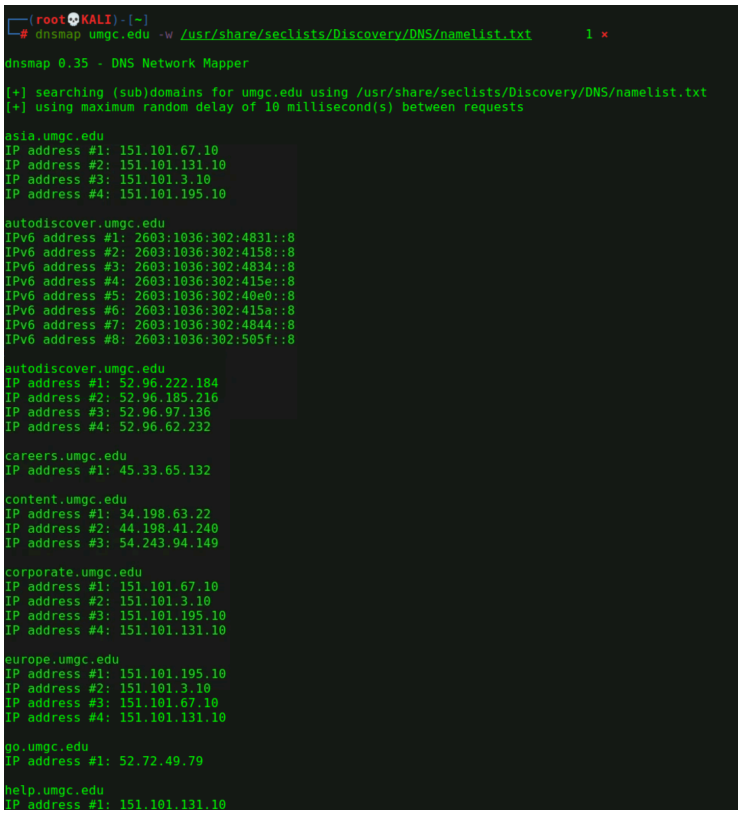


Figure 31: *dnsmap output with extended wordlist revealing additional subdomains for umgc.edu*

Source: *Output from Kali Linux terminal.*

Dnsrecon:

The **dnsrecon** tool is a powerful DNS enumeration utility commonly used in penetration testing and threat intelligence to collect DNS records, verify configurations, and identify misconfigurations. It supports multiple record types, including A, MX, NS, and TXT, and allows for reverse lookups and zone transfer attempts. For the *umgc.edu* domain, dnsrecon was executed with the command **dnsrecon -d umgc.edu** to enumerate DNS-related information.

The scan revealed that DNSSEC is not configured for the domain and identified authoritative name servers such as *ns-1246.awsdns-27.org* (205.251.196.222) and *ns-758.awsdns-30.net* (205.251.194.246). These results provide insight into the DNS infrastructure supporting the domain and highlight the importance of reviewing external DNS configurations in security assessments. Additional options, such as the **-t** flag, can be applied in follow-up scans to perform more advanced enumeration techniques.

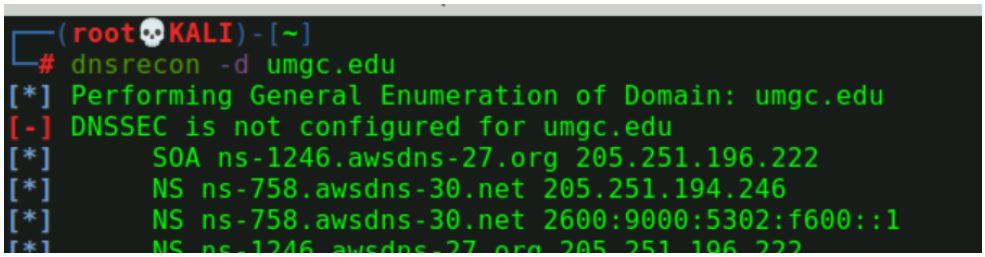
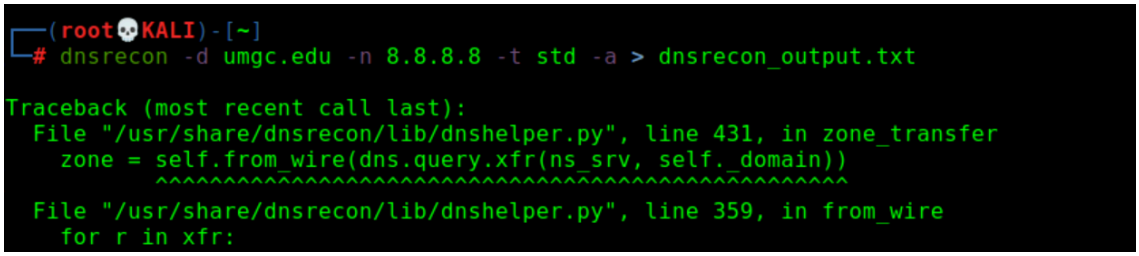


Figure 32: *dnsrecon output showing DNS records for umgc.edu*

Source*: Output from dnsrecon -d umgc.edu in Kali Linux*

To identify the Apple domain verification ID for **umgc.edu**, the dnsrecon tool was executed against Google's public DNS server (8.8.8.8) with output redirected to a file for analysis. The resulting records were then filtered to extract TXT entries associated with the domain. Among the TXT records returned, one contained the Apple domain verification ID: **8s4Ct8Vrn88hRtw9**. This value demonstrates that the domain has been registered and verified with Apple services, which is an important indicator of domain ownership validation.



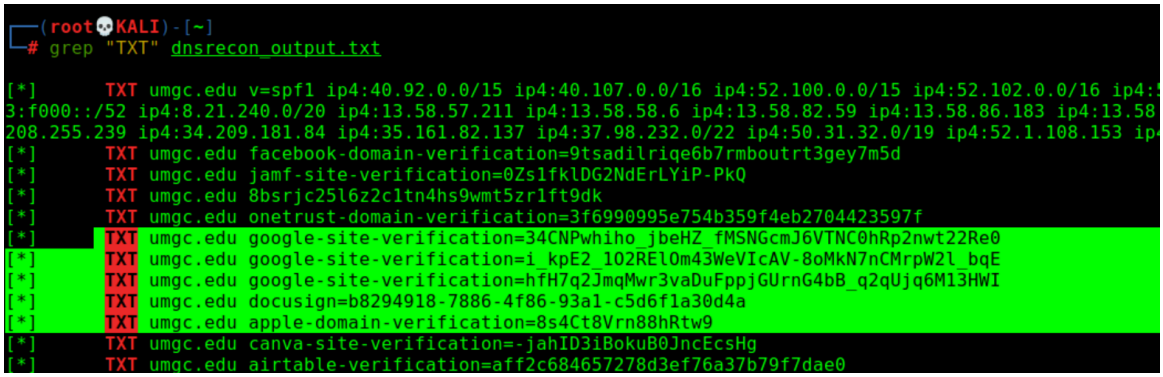


Figure 33: *dnsrecon TXT record output showing Apple domain verification ID for umgc.edu*

Source: *Output from dnsrecon command execution in Kali Linux terminal.*

Upon comparing the results of the dnsenum and dnsrecon tools for the domain umgc.edu, it is evident that the number and details of the MX (Mail Exchange) servers do not fully match. The dnsenum output shows four MX entries pointing to the mail server umgc-edu.mail.protection.outlook.com, each associated with an IPv4 address: **52.101.194.4, 52.101.9.5, 52.101.40.24, and 52.101.11.15**. In contrast, the dnsrecon output reveals a total of eight MX records for the same mail server, which include both IPv4 and IPv6 addresses. The IPv4 addresses listed in dnsrecon are **52.101.11.13, 52.101.41.183, 52.101.194.19, and 52.101.41.28,** while the IPv6 addresses are **2a01:111:f403:c946::2, 2a01:111:f403:c931::1, 2a01:111:f403:f901::1, and 2a01:111:f403:c902::.** Although both tools identify with the same mail domain, the

specific IP addresses vary and dnsrecon provides a more comprehensive set of results by including IPv6 information. Therefore, the number of MX servers and their corresponding values do not exactly match between the two tools.

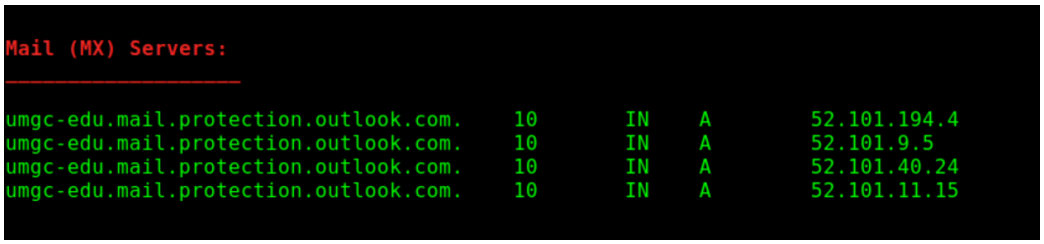


Figure 34: *dnsenum output showing MX servers for umgc.edu*

Source: *Output from dnsenum umgc.edu command executed in Kali Linux terminal.*

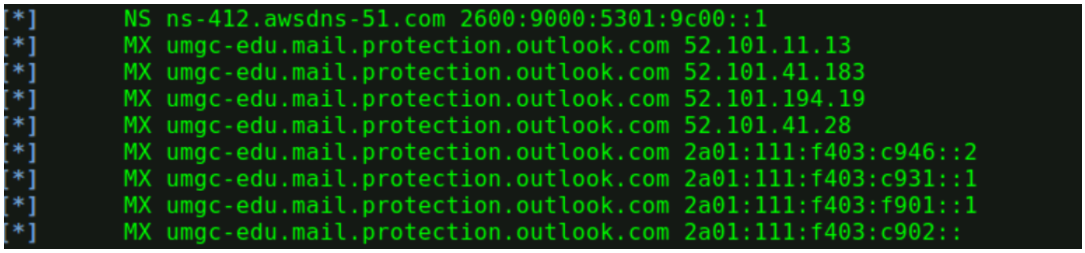


Figure 35: *dnsrecon output showing MX servers for umgc.edu*

Source: *Output from dnsrecon -d umgc.edu -t std command executed in Kali Linux terminal.*

To determine how many Google Site Verification IDs are associated with the **umgc.edu** domain, the grep command was applied to the TXT record output generated by dnsrecon. This search specifically targeted entries containing "google-site-verification." The results revealed **three distinct Google verification IDs** linked to the domain, suggesting that UMGC has validated its domain for multiple Google services or that different administrators have configured verification

independently. This information provides insight into domain ownership and third-party service integrations.

Figure 36: *dnsrecon output showing Google Site Verification IDs for umgc.edu*

Source: *Output from commands run in Kali Linux terminal.*

To determine how many Name Servers (NS) for the **umgc.edu** domain was configured with IPv4 addresses, the dnsrecon -d umgc.edu -t std command was executed in Kali Linux. The results were filtered with grep using a regular expression designed to capture IPv4 address patterns. This process revealed that **four valid name servers** are associated with the domain. The servers identified were: ns-412.awsdns-51.com (205.251.193.156), ns-1863.awsdns-40.co.uk (205.251.199.71), ns-758.awsdns-30.net (205.251.194.246), and ns-1246.awsdns-27.org (205.251.196.222). These findings highlight how DNS infrastructure for the domain is

distributed across multiple geographic and organizational zones, reducing risk by ensuring redundancy and resilience.

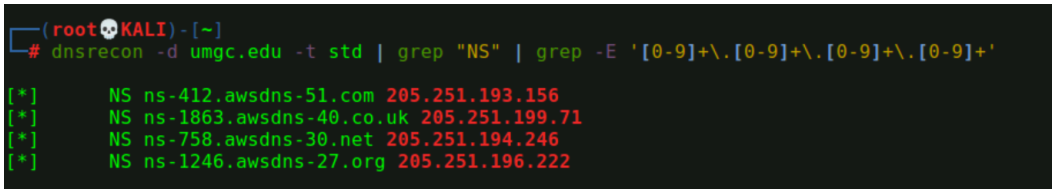


Figure 37: *dnsrecon output showing four IPv4-configured Name Servers for umgc.edu*

Source: *Output from dnsrecon -d umgc.edu -t std in Kali Linux filtered with grep.*

IPv6 addresses **cannot be directly converted to IPv4 addresses** because they are fundamentally different in structure and purpose. IPv4 uses 32-bit addressing, allowing for approximately 4.3 billion unique addresses, while IPv6 uses 128-bit addressing, offering a vastly larger address space of about 340 undecillion addresses. This means an IPv6 address can represent far more data and include several types of routing and identification information that IPv4 simply does not support. While some transitional mechanisms such as dual stack and tunneling exist to allow IPv4 and IPv6 to coexist, these do not convert addresses directly. Instead, they allow systems to handle both protocols separately. Any mapping between IPv6 and IPv4 is a workaround and only applicable in limited scenarios, for backward compatibility (GeeksforGeeks, n.d.; A10 Networks, n.d.; Wikipedia, n.d.).

Yes, IPv4 addresses can be represented in IPv6 format using special compatibility mechanisms, but **they cannot be truly converted** in a functional sense due to major architectural differences. IPv4 is a 32-bit addressing scheme, whereas IPv6 uses a 128-bit format, making their structures fundamentally incompatible (GeeksforGeeks,

n.d.). **IPv6 allows embedding IPv4 addresses inside IPv6 addresses using techniques like IPv4-mapped IPv6 addresses**, which help during transitions or dual-stack deployments. However, this does not mean the IPv4 address becomes a native IPv6 address. It is simply a transitional tool to facilitate communication between systems that support both protocols (A10 Networks, n.d.). Therefore, while there are ways to represent IPv4 within IPv6, they are not interchangeable or directly convertible.

To perform a reverse DNS lookup on the IP range 151.101.67.0/24 associated with the domain umgc.edu, the command dnsrecon -d umgc.edu -r 151.101.67.0/24 was executed in Kali Linux. This command initiates a reverse lookup process for all 256 IP addresses in the given CIDR block, attempting to resolve each IP to a corresponding domain name using PTR records. The output confirmed that the reverse lookup scan was conducted from 151.101.67.0 to 151.101.67.255. However, the results showed that zero PTR records were found within this range. This means none of the IP addresses in the specified block resolved to a hostname, indicating that reverse DNS records are either not configured or not publicly available for this subnet. This is a common scenario in many environments where reverse DNS is not implemented or intentionally restricted for security or administrative reasons.

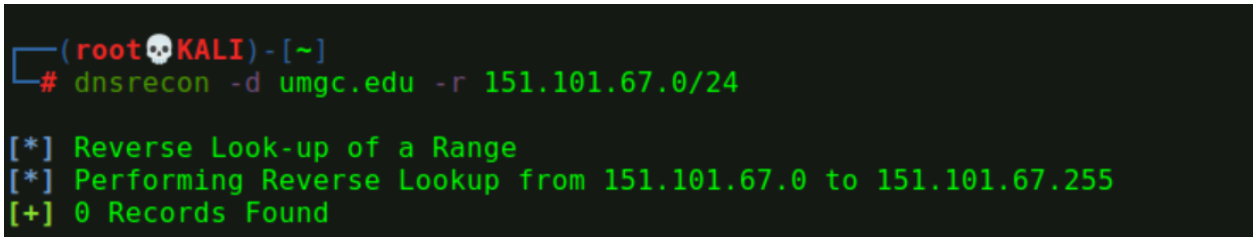


Figure 38: *dnsrecon reverse lookup results for IP range 151.101.67.0/24*

Source: *Output from dnsrecon -d umgc.edu -r 151.101.67.0/24 executed in Kali Linux terminal.*

The -t option in the dnsrecon tool specifies the type of enumeration technique to perform. When using -t std, the tool conducts standard DNS enumeration by collecting DNS records such as A, MX, NS, SOA, and SRV. In the screenshot of the command **dnsrecon -d umgc.edu -t std**, **the output revealed several DNS records, including IPv4 and IPv6 addresses associated with mail servers and name servers**. This output provides a comprehensive view of the domain's DNS configuration.

On the other hand, the -t zonewalk option attempts to perform an NSEC zone walk, which can enumerate DNS zone data by exploiting misconfigured DNSSEC implementations. The second screenshot demonstrates this with the command **dnsrecon -d umgc.edu -t zonewalk**, which retrieved **only a few A records** and noted a missing SOA record, indicating that the zone was misconfigured. The difference in output highlights that -t std is used for general enumeration, while -t zonewalk is a more specialized approach targeting DNSSEC-specific vulnerabilities (Offensive Security, n.d.).

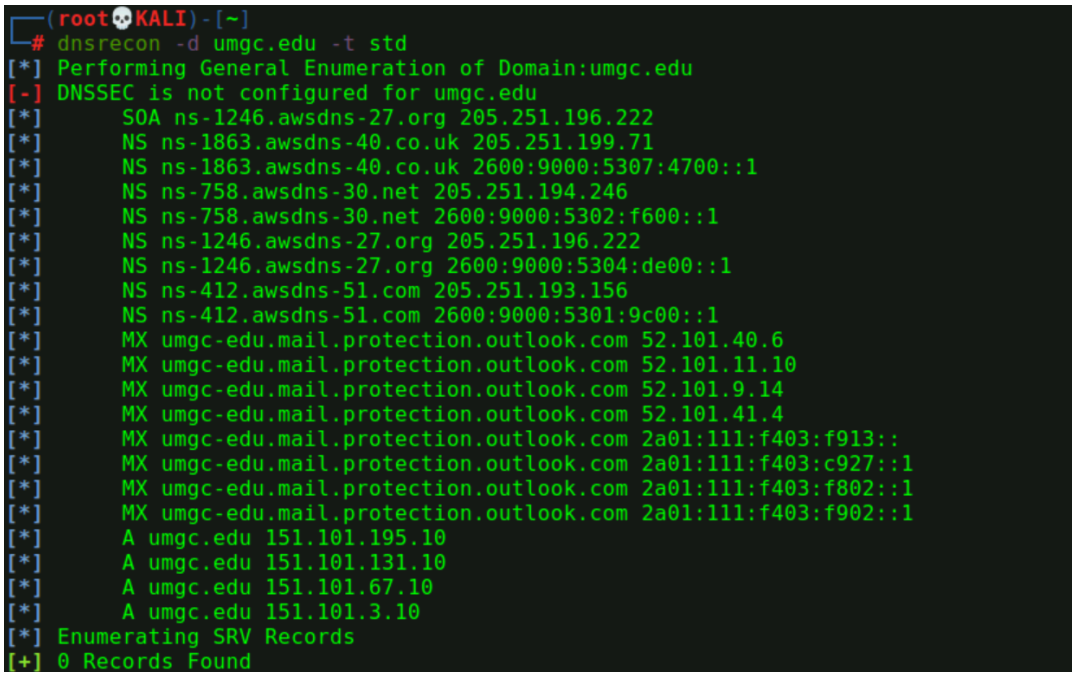


Figure 39: *dnsrecon standard enumeration results for umgc.edu*

Source: *Output from dnsrecon -d umgc.edu -t std command in Kali Linux.*

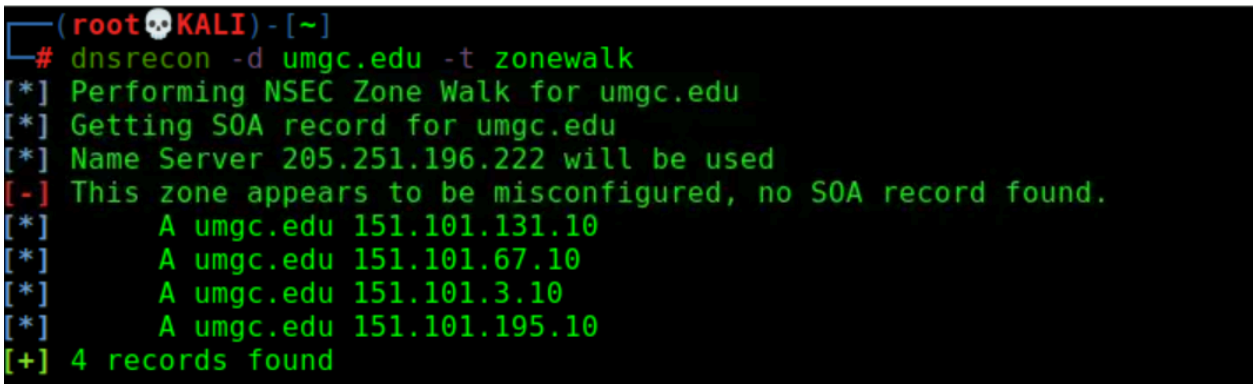


Figure 40: *dnsrecon zone walk results for umgc.edu*

Source: *Output from dnsrecon -d umgc.edu -t zonewalk command in Kali Linux.*

Fierce:

In threat intelligence and reconnaissance activities, identifying an organization's exposed digital assets is a critical first step. The Fierce tool plays a valuable role in this

process by conducting DNS enumeration to uncover subdomains, name servers, and potentially hidden infrastructure associated with a target domain. From a threat intelligence perspective, Fierce helps analysts map the external attack surface of an organization, providing insight into possible weak points or misconfigured services that adversaries might exploit. This kind of intelligence can be used to proactively harden security and detect early indicators of compromise (Kali Linux Tools, n.d.).

Using the command **fierce --domain umgc.edu | grep "mars.umgc.edu"**, the IPv4 address for **mars.umgc.edu** was identified as **151.101.131.10**. This helps in threat intelligence by revealing active subdomains that could be potential targets.

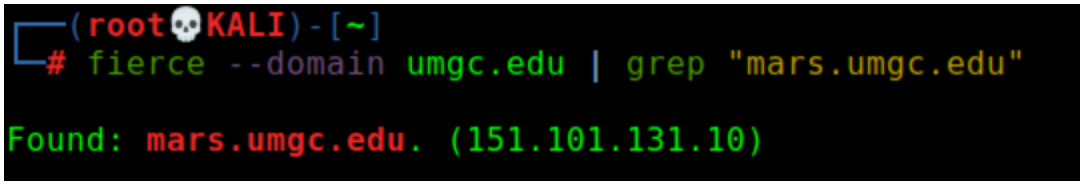


Figure 41: *fierce command output showing discovery of mars.umgc.edu subdomain*

Source: *Output from the fierce --domain umgc.edu | grep "mars.umgc.edu" command executed in Kali Linux terminal.*

The fierce tool was used to enumerate subdomains of the umgc.edu domain, leveraging a combination of filters to refine the results. By running the command fierce --domain umgc.edu | grep "Found:" | grep ".umgc.edu" | cut -d' ' -f2, a comprehensive list of subdomains was extracted. Identifying subdomains is a critical part of threat intelligence, as it highlights the organization's potential external attack surface and helps security teams detect misconfigurations, hidden services, or vulnerable entry points. The

results revealed several subdomains, including asia.umgc.edu, careers.umgc.edu, content.umgc.edu, corporate.umgc.edu, europe.umgc.edu, go.umgc.edu, help.umgc.edu, info.umgc.edu, kb.umgc.edu, labs.umgc.edu, library.umgc.edu, m.umgc.edu, mail.umgc.edu, mars.umgc.edu, my.umgc.edu, office.umgc.edu, peoplesoft.umgc.edu, phones.umgc.edu, and portal.umgc.edu. These findings provide valuable insights into the breadth of publicly accessible infrastructure tied to the umgc.edu domain.

Figure 42: *Output from fierce tool showing extracted subdomains of umgc.edu*

Source: *Output from the command fierce --domain umgc.edu | grep "Found:" | grep ".umgc.edu" | cut -d' ' -f2 executed in Kali Linux terminal.*

The fierce tool was used to enumerate the Name Servers (NS) for the umgc.edu domain. By executing the command fierce --domain umgc.edu | grep -i "NS:" | tr ' ' '\n' | grep "^ns", the results were filtered to extract only the NS records, ensuring clarity in the

output. This process revealed four authoritative name servers supporting the umgc.edu domain: ns-1863.awsdns-40.co.uk, ns-412.awsdns-51.com, ns-758.awsdns-30.net, and ns-1246.awsdns-27.org. Identifying these servers is important in security assessments, as they play a key role in managing DNS traffic and may highlight dependencies on third-party providers.

Figure 43: *Output from fierce tool showing NS records for umgc.edu*

Source: *Output from the command fierce --domain umgc.edu | grep -i "NS:" | tr ' ' '\n' | grep "^ns" executed in Kali Linux terminal.*

As part of the threat intelligence investigation targeting the subdomain **careers.umgc.edu**, the analysis began by resolving its IP address using the host command. This revealed that *careers.umgc.edu* is a CNAME alias for **umuccareers.buyerads.com**, which further resolved to the IP address **45.33.65.132** (Figure 44).

Once the IP address was confirmed, a **proximity scan** was performed using the **fierce** tool with the range **45.33.65.128/27** to identify other domain names mapped to IPs within the same subnet. This scan revealed a set of nearby domains and hostnames, providing visibility into additional infrastructure surrounding the target (Figure 45).