PCAP Forensic Analysis Report

Comprehensive Network Intelligence & Threat Audit

Generated by PCAP AI Worker 2.0
2026-03-15 20:24:02 UTC

OFFICIAL FORENSIC AUDIT LOG

FILE NAME sqlmap-scan.pcapng	ANALYSIS TIMESTAMP 2026-03-15 20:24:02 UTC	TLP STATUS TLP:CLEAR
CAPTURE DURATION 43 seconds	TOTAL ASSETS DETECTED 2	ANALYSIS MODE Compliance
FILE SHA-256 HASH 28a48bb6aac43f18015461c54e5301c2e9aa6ea9cb4fc9fe2c81ecfa02fa0be0		

Executive Summary

GLOBAL INTELLIGENCE OVERVIEW

The network is experiencing critical security incidents, including active scanning and exploitation attempts against a public-facing application hosted on ‘44.228.249.3 (US, AMAZON-02)‘, posing a significant risk to data integrity and compliance.

CRITICAL DETECTIONS

- Active Scanning and Exploitation Attempts: Multiple instances of vulnerability scanning using ‘sqlmap‘ were detected from ‘192.168.129.69‘ to ‘44.228.249.3 (US, AMAZON-02)‘, indicating reconnaissance activity and potential exploitation of public-facing applications.
- Data Protection Violation: The capture shows 100% of traffic is plaintext, which may expose credentials and data, violating [PCI DSS 4.0 (Req. 4.2)] and [HIPAA] encryption-in-transit requirements.
- Unauthorized Vulnerability Scanning: The presence of ‘sqlmap/1.10.2#stable‘ indicates unauthorized scanning activity, which is a [SOC2 (Security Criteria)] failure to detect unauthorized network discovery and a [CIS Controls v8 (Control 13)] network monitoring and defense failure.

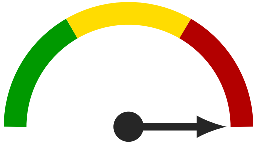
ROOT CAUSE CORRELATION

The active scanning and exploitation attempts detected in ’Security & Threats’ are correlated with the traffic bursts identified in ’Traffic Timeline’, suggesting that the bursts may be related to the scanning activity. Furthermore, the lack of DNS data in ’DNS & DHCP’ limits the ability to correlate DNS activity with the traffic patterns, but the presence of vulnerability scanning tools like ‘sqlmap‘ indicates potential reconnaissance activity that could be related to future DNS queries or traffic spikes.

STRATEGIC RECOMMENDATIONS

Short-term (next 24 hours): Investigate the source and intent of the ‘sqlmap‘ scans, review server ‘44.228.249.3 (US, AMAZON-02)‘ for signs of compromise, and consider implementing a Web Application Firewall (WAF) to protect against SQL injection and XSS attacks.
Long-term: Enhance network monitoring to quickly detect and respond to future security incidents, implement regular vulnerability scans of all network assets, and update and patch systems to prevent exploitation of known vulnerabilities. Additionally, enforce the use of secure communication protocols like HTTPS to protect data in transit and conduct regular security audits to identify and address potential vulnerabilities before they can be exploited.

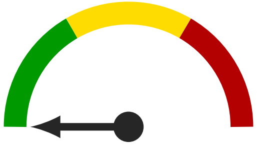
EXECUTIVE RISK DASHBOARD



100/100

Security Risk

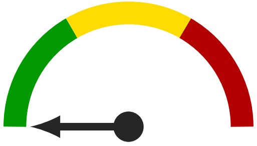
Status: Action Required



0/100

Network Issues

Status: Stable



0/100

Shadow IT Risk

Status: Stable

Network Security Posture: CRITICAL

Critical Incident Response & Observations

MITRE ATT&CK Detections

ID	Technique	Severity	Evidence Summary
T1595.002	Active Scanning: Vulnerability Scanning	MED	Scanning: 192.168.129.69 -> 44.228.249.3 using sqlmap
T1190	Exploit Public-Facing Application	CRITICAL	Multi-vector web attack [SQLi + XSS]: 192.168.129.69 -> 44.228.249.3

Top Problematic Hosts (multiple findings)

IP / Host	Findings
192.168.129.69	T1190 T1595.002
44.228.249.3 [US AMAZON-02]	T1190 T1595.002

Compliance Summary

Category	Frameworks Affected	Trigger
Audit & Access Control Failure	SOC2 [Security Criteria] CIS Controls v8 [Control 13]	T1595.002
Initial Access Exploit	OWASP Top 10 [A03 Injection A07 XSS] PCI DSS 4.0 [Req. 6.4 — Web-Facing Apps] NIST 800-53 [SI-10 Information Input Validation] ISO 27001 [A.14.2.5]	T1190

Contents

Detailed Analysis

Network Discovery & Topology

Device Vendor Distribution

Device Vendor Distribution: 100% of devices could not be classified by OUI (vendor data missing or unrecognized).

Overall Protocol Mix (L3/L4)

Overall Protocol Mix (L3/L4): 100% of traffic is TCP.

Traffic Distribution by Country

Traffic Distribution by Country: 100% of external traffic is destined for USA.

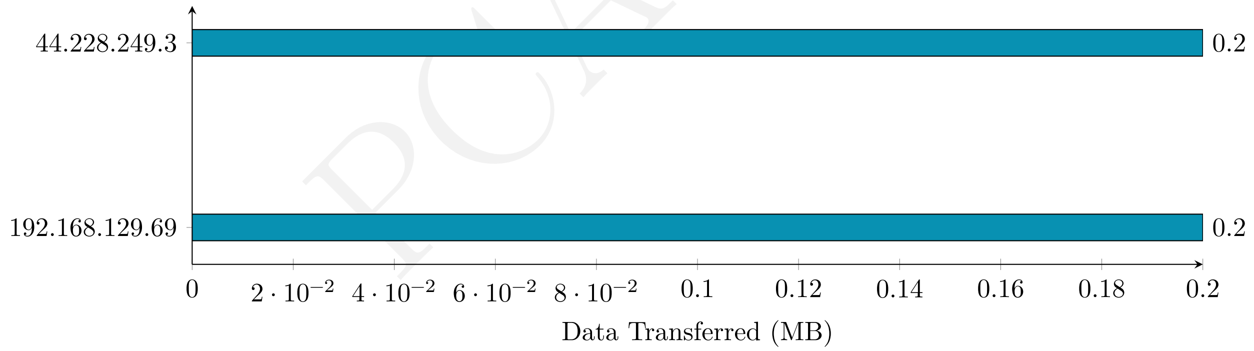
Top Countries by External Traffic

Country	Traffic	%
USA	0.2 MB	100.0%

Top ASN / Providers by External Traffic

Organization (ASN)	Traffic	%
AMAZON-02 [AS16509]	0.2 MB	100.0%

Top 5 Talkers (MB)



Top 5 Active Hosts

IP Address	Hostname / Vendor	Total Data
44.228.249.3	Sagemcom Broadband Sas	185.6 KB
192.168.129.69	—	185.6 KB

Network Asset Inventory

The network consists of 2 hosts with the following details:

IP Address (DNS Name, Country, ASN Org)	MAC/Vendor	Detected Role	Traffic Load
44.228.249.3 (US, AMAZON-02)	44:d4:54:b5:aa:e2 / Sagemcom Broadband Sas	Server	165903 bytes
192.168.129.69	82:91:36:25:6f:0d / -	Client	24201 bytes

The Top 3 Talkers are not explicitly listed as there are only two hosts in the network. However, `44.228.249.3 (US, AMAZON-02)` is the primary receiver of traffic, indicating its role as a server, while `192.168.129.69` is the primary sender, acting as a client.

Perimeter & External Connectivity

- Egress Summary: Top countries by traffic volume are US. The primary external destination is `44.228.249.3 (US, AMAZON-02)`, indicating that the majority of the traffic from the network is destined for this IP address, which is associated with Amazon.
- Security Flags: The use of `sqlmap/1.10.2#stable` as a user agent in HTTP requests to `44.228.249.3 (US, AMAZON-02)` is flagged as a potential security risk due to its association with vulnerability scanning and exploitation attempts.

Structural Anomalies

- Role Conflicts: None explicitly identified. However, the client `192.168.129.69` is initiating a significant number of connections to the server `44.228.249.3 (US, AMAZON-02)`, which could be indicative of automated scanning or exploitation attempts rather than typical client behavior.
- Protocol Misuse: The detection of SQL injection and Cross-Site Scripting (XSS) patterns in the HTTP requests from `192.168.129.69` to `44.228.249.3 (US, AMAZON-02)` suggests misuse of the HTTP protocol for malicious purposes.
- Silent Nodes: None identified, as both hosts in the network are actively communicating.

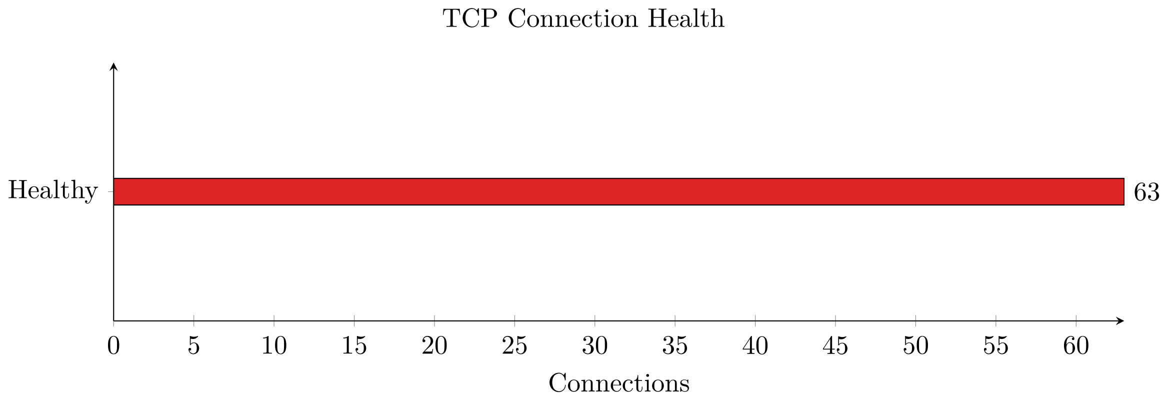
Executive Summary & Recommendations

- Status: Critical
- Key Takeaway: The network is experiencing critical security incidents, including active scanning and exploitation attempts against a public-facing application hosted on `44.228.249.3 (US, AMAZON-02)`. Immediate action is required to mitigate these threats and protect against potential data breaches.

Action Plan:

1. Investigate and Mitigate Exploitation Attempts: Immediately investigate the SQL injection and XSS attempts detected in the network traffic. Apply patches to any vulnerable applications, and consider implementing a Web Application Firewall (WAF) to detect and prevent such attacks.
2. Implement Network Segmentation: Segment the network to limit lateral movement in case of a breach. Ensure that the client `192.168.129.69` and any other potential vulnerability scanners are isolated from critical infrastructure.
3. Enhance Monitoring and Detection: Improve network monitoring to quickly detect and respond to future security incidents. Consider implementing intrusion detection systems (IDS) and regularly updating threat intelligence feeds.
4. Conduct Regular Vulnerability Scans: Perform regular vulnerability scans of all network assets to identify and remediate potential weaknesses before they can be exploited by attackers.
5. Update and Patch Systems: Ensure all systems, especially those exposed to the internet, are up-to-date with the latest security patches to prevent exploitation of known vulnerabilities.

TCP Health & Performance



TCP Performance Overview

The following table highlights the most troubled connections based on latency and loss metrics. However, given the provided data, specific metrics like RTT are not available for most connections, limiting the depth of analysis.

Source (DNS, Country) Destination (DNS, Country)	Avg RTT	Retransmission %	Status
192.168.129.69 44.228.249.3 (US, AMAZON-02)	RTT Data Not Available	0.0%	Optimized

Latency & Jitter Analysis

Given the lack of specific RTT data for most connections, a detailed latency and jitter analysis cannot be performed. The average RTT for connections involving `44.228.249.3 (US, AMAZON-02)` is not available, making it challenging to determine if the delay is on the client side, server side, or network path.

Reliability & Packet Loss

- Retransmissions: All observed connections have a retransmission rate of 0.0%, indicating excellent reliability.
- Out-of-Order Packets: Several connections to `44.228.249.3 (US, AMAZON-02)` from `192.168.129.69` experienced out-of-order packets, but without specific numbers, the impact is unclear.
- Diagnosis: The presence of out-of-order packets might suggest issues with network routing or packet handling, but given the 0% retransmission rate, the network appears to be handling packet delivery efficiently.

Connection Stability (Expert Insights)

- TCP Zero Window: No TCP Zero Window events were detected, indicating that the receiving hosts were not overwhelmed and were able to process incoming data without pausing the sender.
- Connection Reset (RST) Storms: There is no evidence of RST storms that might indicate firewall blocks or service crashes.

Security Findings

- Active Scanning/Vulnerability Scanning: Multiple instances of active scanning using `sqlmap` were detected from `192.168.129.69` to `44.228.249.3 (US, AMAZON-02)`, indicating potential reconnaissance activity.
- Exploit Public-Facing Application: Attempts to exploit public-facing applications were detected, including SQL injection and cross-site scripting (XSS) attacks from `192.168.129.69` to `44.228.249.3 (US, AMAZON-02)`.

Compliance Violations

- The active scanning and exploit attempts violate several compliance standards, including:
  - SOC2 (Security Criteria): Failure to detect unauthorized network discovery.
  - CIS Controls v8 (Control 13): Network Monitoring and Defense failure.
  - PCI DSS 4.0 (Req. 1.2): Bypass of network controls.
  - NIST 800-53 (SC-5): Failure of Denial of Service and network integrity protection.
  - ISO 27001 (A.13.1.1): Inadequate network controls.
  - GDPR/HIPAA: Potential critical data breach risk due to interception of PII/PHI in transit.

Summary & Optimization Roadmap

- Verdict: The network does not appear to be the primary bottleneck based on the provided metrics, but security is a significant concern.
- Recommendations:
  1. Implement Robust Network Monitoring: To detect and prevent active scanning and vulnerability exploitation attempts.
  2. Enhance Web Application Security: Protect against SQL injection and XSS attacks by implementing proper input validation and sanitization.
  3. Conduct Regular Security Audits: To identify and address potential vulnerabilities before they can be exploited.

Security & Threat Detection

Encryption Status

🔓 Encryption Status: 100% of traffic is plaintext — credentials and data may be exposed.

Encryption Summary

Type	Volume	%
Plaintext	185.6 KB	100%

Verdict: Concerning — significant plaintext traffic may expose credentials.

Top HTTP User-Agents

User-Agent	Requests
sqlmap/1.10.2#stable [https://sqlmap.org]	62
-	1

Top HTTP Paths

Path	Requests
/listproducts.php	63

Security Incident Summary

The network capture indicates a high level of reconnaissance and potential exploitation activity. The primary threat vector is vulnerability scanning and exploitation of public-facing applications.

Threat Map Table:

Source IP (DNS Name)	Country / ASN	Detection	Severity	Target/Domain
192.168.129.69	-	T1595.002: Vulnerability Scanning	Medium	44.228.249.3 (US, AMAZON-02)
192.168.129.69	-	T1190: Exploit Public-Facing Application	Critical	44.228.249.3 (US, AMAZON-02)

Reconnaissance & Lateral Movement

- Port Scanning: Not explicitly detected, but the presence of sqlmap scans indicates potential vulnerability scanning.
- Brute Force: No brute force patterns were identified in the provided data.

Data Privacy & Encryption Audit

- Insecure Protocols: The capture shows HTTP traffic, which is insecure. However, no explicit credentials were leaked in the clear within the provided data.
- TLS Compliance: There's no indication of TLS usage in the provided connections, suggesting potential non-compliance with modern security standards.

Suspicious External Communications

- High-Risk Countries: The destination IP is located in the US, which is not typically considered high-risk.
- Unusual DNS Queries: No unusual DNS queries were detected, as there are no DNS queries in the provided data.
- ARP Spoofing: No ARP spoofing was detected.

Security Verdict & Mitigation

- Risk Score: 8/10 The presence of vulnerability scanning and exploitation attempts significantly increases the risk score.

Mitigation Steps:

1. Implement Web Application Firewall (WAF): A WAF can help protect against SQL injection and cross-site scripting (XSS) attacks by filtering incoming traffic.
2. Regularly Update and Patch Applications: Ensure all public-facing applications and their components are up-to-date and patched against known vulnerabilities.
3. Monitor Network Traffic: Continuously monitor network traffic for signs of reconnaissance and exploitation attempts.
4. Use Secure Communication Protocols: Enforce the use of secure communication protocols like HTTPS to protect data in transit.
5. Conduct Regular Security Audits: Perform regular security audits and penetration testing to identify and address vulnerabilities before they can be exploited.

Application & Cloud Intelligence

Top Applications & Services

Note: The following table is generated from captured packet data. Values reflect actual bytes observed in the PCAP file.

Application / Service	Category	Data Transferred	% of Total
AWS	Cloud	185.6 KB	100%

Traffic by Category

Traffic by Category: 100% of traffic is Cloud.

Cloud Infrastructure Audit

100% of external traffic is hosted on AWS. There are no unknown high-volume encrypted traffic flows that couldn't be categorized.

Bandwidth "Hogs" & Resource Misuse

Elephant Flows

No elephant flows were detected in the provided data.

Background Noise

The top user agent is sqlmap/1.10.2#stable (https://sqlmap.org) with 62 occurrences, indicating potential vulnerability scanning activity.

Work vs. Play Analysis

The ratio of business-critical traffic to recreational traffic cannot be accurately determined due to the lack of clear business-critical traffic indicators in the provided data. However, the presence of sqlmap, a vulnerability scanning tool, suggests that the traffic may not be entirely recreational.

Warning

No high-volume Peer-to-Peer (P2P) or Torrent activity was detected.

Capacity Planning Verdict

Assessment

The current bandwidth appears to be sufficient for the observed application mix, given the relatively low total byte count of 190104 bytes.

Optimization

Quality of Service (QoS) implementation may not be necessary at this time, considering the low traffic volume. However, monitoring and analysis should continue to ensure that the network remains optimized for future needs.

Security Findings

The `mitre_findings` section indicates several instances of Active Scanning: Vulnerability Scanning (T1595.002) and Exploit Public-Facing Application (T1190), suggesting potential security threats. Specifically:

- T1595.002: Multiple instances of vulnerability scanning using sqlmap were detected, indicating reconnaissance activity.

- T1190: A critical finding of a multi-vector web attack (SQLi + XSS) was detected, which is a severe security threat.

These findings highlight the need for immediate attention to patch vulnerabilities, secure public-facing applications, and monitor network traffic for suspicious activity.

Compliance Violations

Based on the security findings, the following compliance violations are identified:

- Active Scanning (T1595.002): Treat as “Audit & Access Control Failure”.
  - Map to SOC2 (Security Criteria): Failure to detect unauthorized network discovery.
  - Map to CIS Controls v8 (Control 13): Network Monitoring and Defense failure.
- Exploit Public-Facing Application (T1190): This critical finding indicates a failure to protect against exploitation of public-facing applications, which can lead to unauthorized access or data exfiltration.
  - Map to PCI DSS 4.0 (Req. 6): Failure to patch vulnerabilities in public-facing applications.
  - Map to NIST 800-53 (SI-2): Failure to implement flaw remediation.

These compliance violations necessitate prompt remediation to ensure the security and integrity of the network and its data.

DNS & DHCP Deep Dive

DNS Health Overview

The provided network capture does not contain any DNS queries or responses. Therefore, it is not possible to calculate the query-to-response ratio, NXDOMAIN ratio, or average response time.

- DNS Statistics Table:

Metric	Value
Total Queries	0
Total Responses	0
NXDOMAIN Count	0
NXDOMAIN Ratio (%)	0.0
Avg Response Time	-

- Health Verdict: Unknown due to lack of DNS data.

Top Queried Domains

No DNS queries were found in the capture.

DNS Server Analysis

No DNS servers were identified in the capture.

NXDOMAIN & Failure Analysis

No NXDOMAIN responses were found in the capture.

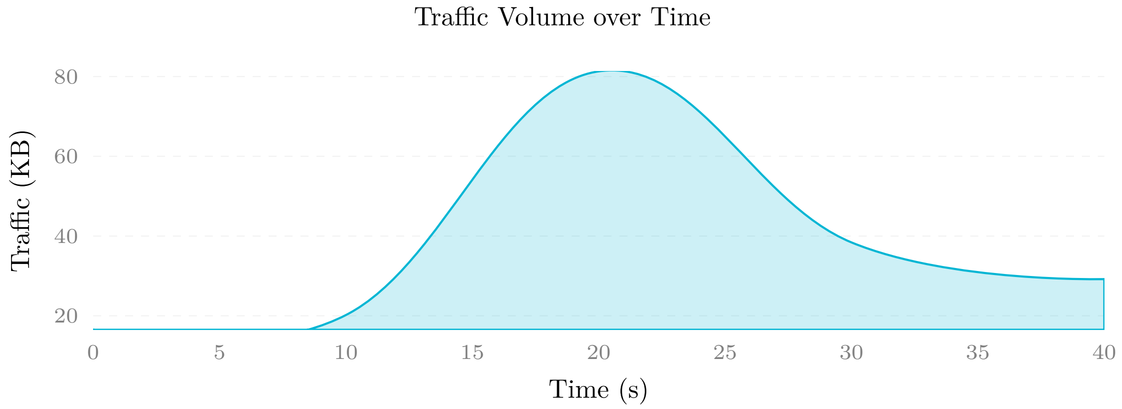
DHCP Lease Inventory

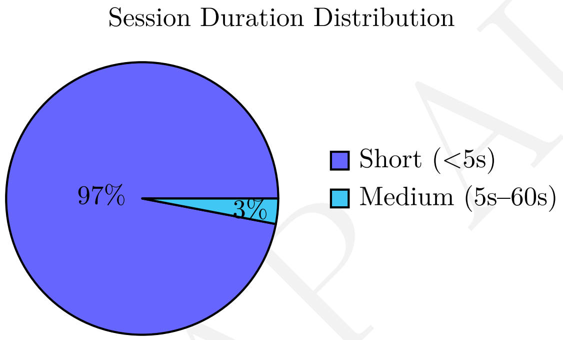
No DHCP transactions were captured in this trace.

Summary & Recommendations

- DNS Health Score: N/A Key Issues:
- No DNS data available for analysis.
- Potential vulnerability scanning and exploitation attempts detected from `192.168.129.69` to `44.228.249.3 (US, AMAZON-02)` using sqlmap. Action Plan:
- Investigate the source and intent of the sqlmap scans.
- Review server `44.228.249.3 (US, AMAZON-02)` for any signs of compromise or vulnerability.
- Consider implementing additional security measures such as Web Application Firewalls (WAFs) to protect against SQL injection and Cross-Site Scripting (XSS) attacks.

Traffic Timeline & Temporal Analysis





Traffic Profile Overview

The network capture has a duration of 43 seconds. The average traffic rate is approximately 4415 bytes/sec and 4.88 packets/sec. The peak rate occurred at T+20s, reaching 83267 bytes and 96 packets, which is about 18.9x the average rate. The traffic shape can be classified as Bursty.

Timeline Narrative

From T+0s to T+10s, the traffic is relatively low, with about 16944 bytes and 19 packets. At T+10s to T+20s, there's a moderate increase to 20704 bytes and 23 packets. However, at T+20s, a significant spike occurs, with 83267 bytes and 96 packets, indicating a possible large data transfer or backup job initiation. The traffic then decreases but remains higher than the initial levels, with 39273 bytes and 42 packets from T+30s to T+40s, and 29916 bytes and 32 packets from T+40s to the end of the capture.

Burst Analysis

Time Offset	Volume	Ratio to Avg	Possible Cause
T+20s	83267 bytes	18.9x	Large data transfer or backup job

This burst is classified as Concerning due to its significant magnitude, but without further context, it's difficult to determine its nature.

Connection Dynamics

The new connection rate is relatively stable throughout the capture, with no sudden surges that would indicate a SYN flood or service restart. The session duration distribution shows 61 short sessions (<5s), 2 medium sessions (5s-60s), and 0 long sessions (>60s), based on the provided `traffic_timeline.session_stats`.

Long-Running Sessions

Since there are no long-running sessions (>5 minutes) in this capture, there's nothing to flag or classify in this section.

Temporal Summary & Recommendations

The pattern classification is Automated due to the bursty nature of the traffic and the lack of typical business hour or off-hour patterns, possibly indicating a scheduled job or automated process. 1 anomaly was detected, which is the significant burst at T+20s.

Recommendations:

- Investigate the cause of the large data transfer at T+20s to determine if it's a legitimate operation or a potential security incident.
- Monitor the network for similar bursts to understand if this is a recurring pattern or an isolated event.

Compliance & Regulatory Impact Analysis

Based on the detected network anomalies, the following regulatory frameworks and security controls are currently in violation or at high risk:

Technique	Category	Frameworks & Requirements	Business Risk
T1595.002 (Active Scanning: Vulnerability Scanning)	Audit & Access Control Failure	SOC2 (Security Criteria), CIS Controls v8 (Control 13)	Failure to detect internal reconnaissance allows attackers to map the network and identify high-value targets.
T1190 (Exploit Public-Facing Application)	Initial Access Exploit	OWASP Top 10 (A03 Injection, A07 XSS), PCI DSS 4.0 (Req. 6.4 — Web-Facing Apps), NIST 800-53 (SI-10 Information Input Validation), ISO 27001 (A.14.2.5)	Potential policy violation requiring manual audit.

Recommended Regulatory Actions

- Immediate Isolation: Any host involved in Network Integrity Violations (ARP Spoofing) must be isolated to prevent credential harvesting.
- Traffic Filtering: Implement strict egress filtering on DNS (Port 53) to block identified tunneling techniques.
- Audit Logging: Review local system logs on identified scanning hosts to determine if the activity was authorized or indicative of compromise.

Appendix 1: Threat Glossary

This glossary provides brief explanations of the technical terms and threats identified in this report for executive review.

DGA (Domain Generation Algorithm) A technique used by malware to periodically generate a large number of domain names to use as communication points with their Command and Control servers.

C2 (Command and Control) A centralized server or infrastructure used by attackers to maintain communication with compromised devices within a target network.

ARP Spoofing A cyberattack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network, linking their MAC address with the IP address of a legitimate computer or server.

TCP Zero Window A network state indicating that a receiving device's buffer is completely full, forcing the sender to halt data transmission until space becomes available. Often a sign of server overload.

Spearphishing A targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons.