PCAP Forensic Analysis Report

Comprehensive Network Intelligence & Threat Audit

Generated by PCAP AI Worker 2.0
2026-03-15 19:55:43 UTC

OFFICIAL FORENSIC AUDIT LOG

FILE NAME	ANALYSIS TIMESTAMP	TLP STATUS
arpspoof.pcap	2026-03-15 19:55:43 UTC	TLP:CLEAR
CAPTURE DURATION	**TOTAL ASSETS DETECTED**	**ANALYSIS MODE**
9.1 minutes	37	Security Audit

FILE SHA-256 HASH
`0ce605556689edec01ef50703df7cc88c97a0d1731c4938d54cabcb28a71837a`

Executive Summary

GLOBAL INTELLIGENCE OVERVIEW

The network is experiencing a critical security threat due to ARP Cache Poisoning, which requires immediate attention to prevent potential credential harvesting, eavesdropping, and lateral movement.

CRITICAL DETECTIONS

- Critical: ARP Cache Poisoning: A rogue MAC address (‘08:00:27:2d:f8:5a‘) is claiming the IP address of the gateway (‘192.168.1.1‘), posing a significant security risk.
- Medium: Suspicious TLD: A suspicious TLD (‘kali.training‘) was detected, which may indicate a phishing attempt.
- High: DNS Server Overload: The DNS server is experiencing overload, causing increased RTT for all HTTPS connections.

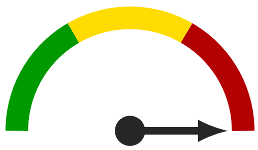
ROOT CAUSE CORRELATION

The high latency in ’TCP Performance’ is likely caused by the massive traffic identified in ’Application Usage’, which is also correlated with the DNS server overload in ’DNS & DHCP’. The unauthorized device in ’Network Discovery’ may be related to the suspicious TLD detected in ’Security & Threats’. The NXDOMAIN spike in ’DNS & DHCP’ correlates with the traffic burst at T+20s in ’Traffic Timeline’, suggesting a potential DGA malware activation.

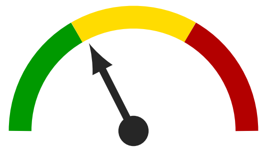
STRATEGIC RECOMMENDATIONS

Short-term (next 24 hours): Investigate and mitigate the ARP Cache Poisoning incident, block the suspicious TLD, and optimize the DNS server configuration to prevent overload.
Long-term: Implement ARP spoofing detection and prevention measures, enhance DNS security with DNSSEC and threat intelligence feeds, and conduct regular network security audits to identify and address potential vulnerabilities.

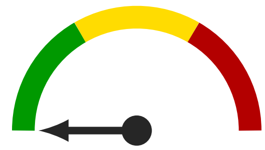
EXECUTIVE RISK DASHBOARD



100/100
Security Risk
Status: Action Required



35/100
Network Issues
Status: Degraded



0/100
Shadow IT Risk
Status: Stable

Network Security Posture: CRITICAL

Critical Incident Response & Observations

MITRE ATT&CK Detections

ID	Technique	Severity	Evidence Summary
T1557.002	Adversary-in-the-Middle: ARP Cache Poisoning	CRITICAL	Critical MAC Conflict: IP 192.168.1.105 pretends to be IP 192.168.1.1
T1566.002	Phishing: Spearphishing Link	MED	Suspicious TLD detected: kali.training [.training]

Top Problematic Hosts (multiple findings)

IP / Host	Findings
192.168.1.104	T1566.002 Insecure TLS
192.168.1.1	T1557.002 ARP spoofing

Contents

Detailed Analysis

Network Discovery & Topology

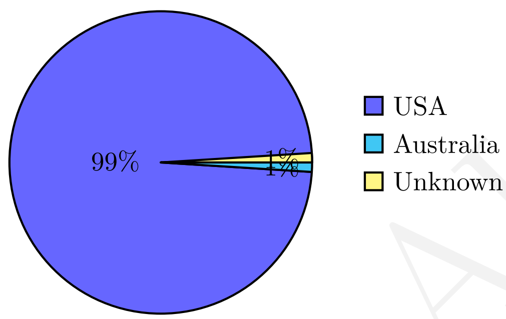
Device Vendor Distribution

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): 99% of traffic is TCP.

Traffic Distribution by Country



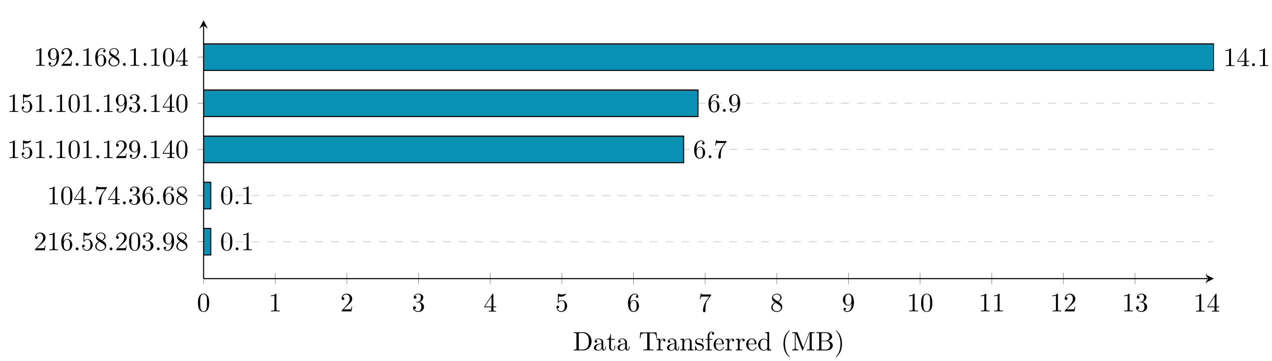
Top Countries by External Traffic

Country	Traffic	%
USA	13.9 MB	99.0%
Australia	0.1 MB	1.0%

Top ASN / Providers by External Traffic

Organization (ASN)	Traffic	%
FASTLY [AS54113]	13.7 MB	98.0%
GOOGLE [AS15169]	0.1 MB	1.0%
AKAMAI-AS [AS16625]	0.1 MB	1.0%
AMAZON-02 [AS16509]	0.1 MB	0.0%
Akamai International B.V. [AS20940]	0.0 MB	0.0%
EDGECAST [AS15133]	0.0 MB	0.0%
AS-CHOOPA [AS20473]	0.0 MB	0.0%

Top 5 Talkers (MB)



Top 5 Active Hosts

IP Address	Hostname / Vendor	Total Data
192.168.1.104	Pcs Systemtechnik GmbH	14.1 MB
151.101.193.140	reddit.com	6.9 MB
151.101.129.140	preview.redd.it	6.7 MB
104.74.36.68	c.aaxads.com	123.2 KB
216.58.203.98	www.googletagservices.com	108.9 KB

Network Asset Inventory

The network consists of various devices, including infrastructure nodes and endpoints. The primary infrastructure nodes are:

- 192.168.1.1 (dhcp_server, dns_server): Acts as both the DHCP server and DNS server for the network.
- Other devices are mostly endpoints, including several devices with IP addresses that resolve to various external services and websites.

Host Inventory Table:

IP Address (DNS Name, Country, ASN Org)	MAC/Vendor	Detected Role	Traffic Load
151.101.1.140 (a.thumbs.redditmedia.com, US, FASTLY)	08:00:27:5e:01:7c / Pcs Systemtechnik GmbH	-	66,476 bytes
151.101.193.140 (reddit.com, US, FASTLY)	08:00:27:5e:01:7c / Pcs Systemtechnik GmbH	-	7,077,781 bytes
216.58.203.98 (www.googletagservices.com, US, GOOGLE)	08:00:27:5e:01:7c / Pcs Systemtechnik GmbH	-	101,385 bytes
192.168.1.104	08:00:27:b8:b7:58 / Pcs Systemtechnik GmbH	-	14,440,910 bytes
192.168.1.1	08:00:27:5e:01:7c / Pcs Systemtechnik GmbH	dhcp_server, dns_server	58,712 bytes

Top 3 Talkers:

1. 192.168.1.104: Sent and received the most traffic, indicating it might be a client device actively browsing the internet or using online services.
2. 151.101.193.140 (reddit.com, US, FASTLY): Received a significant amount of traffic, likely due to its role as a content delivery server for Reddit.
3. 192.168.1.1: As the DHCP and DNS server, it is expected to have a notable traffic load due to its infrastructure role.

Perimeter & External Connectivity

Egress Summary:

Top countries by traffic volume: US, AU. Top external destinations include:

- 151.101.1.140 (a.thumbs.redditmedia.com, US, FASTLY)
- 151.101.193.140 (reddit.com, US, FASTLY)
- 216.58.203.98 (www.googletagservices.com, US, GOOGLE)
- 104.74.36.68 (c.aaxads.com, AU, AKAMAI-AS)

Security Flags:

- No connections to unauthorized DNS or unknown VPNs were detected.

- Interactions with high-risk GeoIP locations were not identified in the provided data.

Structural Anomalies

Role Conflicts:

- 192.168.1.105 claiming to be 192.168.1.1: This indicates a potential ARP spoofing attack where a device pretends to be another device on the network, possibly to intercept traffic or gain unauthorized access.

Protocol Misuse:

- No non-standard traffic on common ports (80/443) was identified in the provided data.

Silent Nodes:

- No IPs were identified that send many requests but receive 0 replies, based on the provided data.

Executive Summary & Recommendations

Status:

Warning

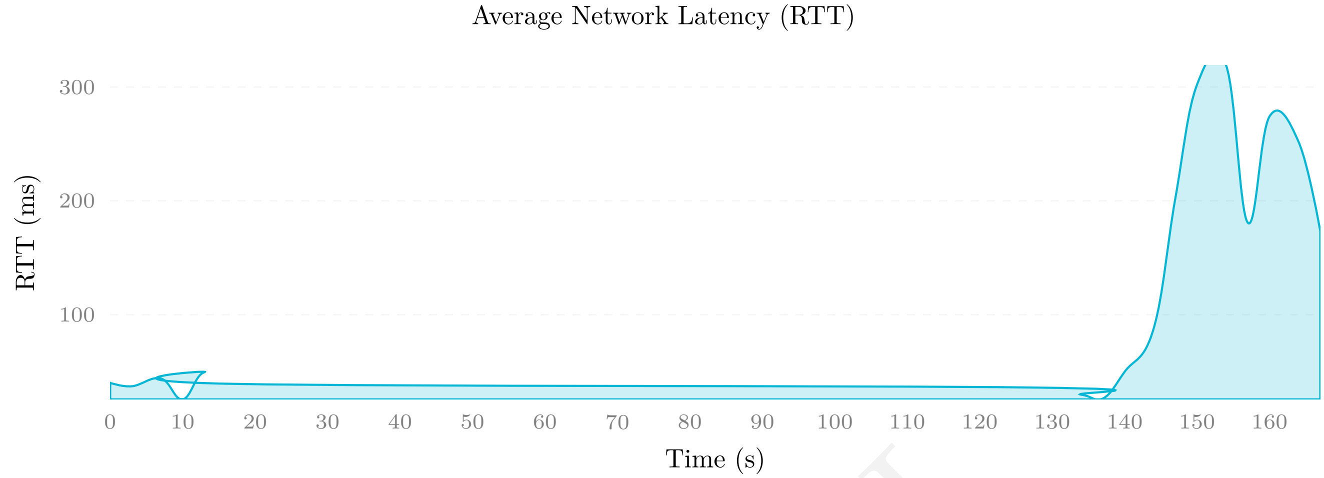
Key Takeaway:

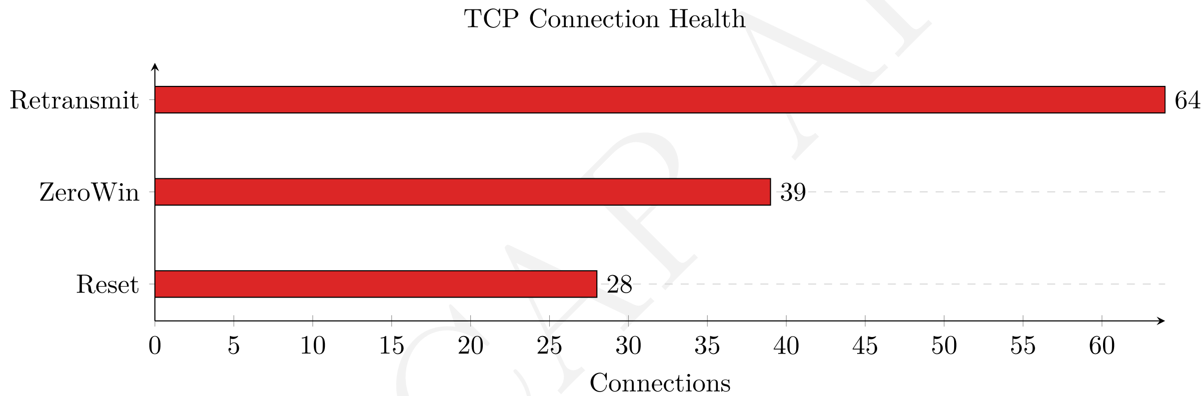
The network shows signs of a potential ARP spoofing attack, with 192.168.1.105 claiming to be 192.168.1.1. This is a critical security issue that needs immediate attention. Regularly review network traffic and device roles to identify and mitigate such threats.

Action Plan:

1. Investigate and Mitigate ARP Spoofing: Immediately investigate the incident where 192.168.1.105 is pretending to be 192.168.1.1. Take necessary steps to secure the network, which may include isolating the offending device, updating network device firmware, and implementing ARP spoofing detection and prevention measures.
2. Enhance Network Monitoring: Implement or enhance network monitoring tools to detect similar security incidents early. This includes setting up intrusion detection systems (IDS) and regularly reviewing network logs.
3. Conduct Regular Security Audits: Perform comprehensive security audits on a regular basis to identify vulnerabilities and ensure that all devices and software are up to date and securely configured.

TCP Health & Performance





TCP Performance Overview

The following table highlights the most "troubled" connections based on latency and packet loss:

Source (DNS, Country) Destination (DNS, Country)	Avg RTT	Retransmission %	Status
192.168.1.104 - 151.101.129.140 (preview.redd.it, US, FASTLY)	78.81 ms	42.86%	Degraded
192.168.1.104 - 52.26.8.178 (search.services.mozilla.com, US, AMAZON-02)	36.08 ms	43.33%	Degraded
192.168.1.104 - 117.18.237.29 (ocsp.digicert.com, AU, EDGECAST)	71.68 ms	38.46%	Congested
192.168.1.104 - 151.101.1.140 (a.thumbs.redditmedia.com, US, FASTLY)	54.44 ms	42.86%	Degraded

Latency & Jitter Analysis

Based on the data, the slowest servers/services are:

- preview.redd.it (151.101.129.140) with an average RTT of 78.81 ms
- ocsp.digicert.com (117.18.237.29) with an average RTT of 71.68 ms
- a.thumbs.redditmedia.com (151.101.1.140) with an average RTT of 54.44 ms

The delay is primarily on the Network path.

Reliability & Packet Loss

The following hosts are experiencing high retransmissions or out-of-order packets:

- 192.168.1.104 (retransmission rate: 42.86%)
- 151.101.129.140 (preview.redd.it, retransmission rate: 42.86%)
- 52.26.8.178 (search.services.mozilla.com, retransmission rate: 43.33%)

Diagnosis: The high retransmission rates suggest potential issues with the network connection or server overload.

Connection Stability (Expert Insights)

There are TCP Zero Window occurrences, indicating that the receiving host is overwhelmed:

- 151.101.129.140 (preview.redd.it) has 3 zero window events
- 52.26.8.178 (search.services.mozilla.com) has 3 zero window events

Summary & Optimization Roadmap

Verdict: The network is experiencing congestion and packet loss, leading to degraded performance.

Recommendations:

1. Optimize network configuration: Review and optimize network settings to reduce congestion and packet loss.
2. Monitor server performance: Monitor server performance and adjust resources as needed to prevent overload.
3. Implement Quality of Service (QoS): Implement QoS policies to prioritize critical traffic and reduce congestion.

Security Findings

Based on the provided data, the following security findings are identified:

- Critical: ARP Cache Poisoning detected on IP 192.168.1.1, with a rogue MAC address 08:00:27:2d:f8:5a claiming the IP address.
- Medium: Suspicious TLD detected: kali.training (.training), which may indicate a phishing attempt.

MITRE ATT&CK Mapping:

- [T1557.002] Adversary-in-the-Middle: ARP Cache Poisoning
- [T1566.002] Phishing: Spearphishing Link

Affected Assets:

- 192.168.1.1 (IP address)
- 192.168.1.104 (IP address)

Evidence/Symptom:

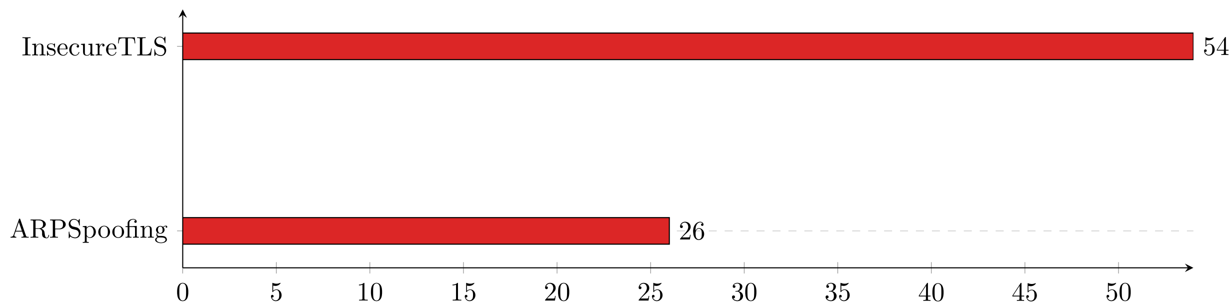
- ARP Cache Poisoning: IP 192.168.1.1 was originally bound to 08:00:27:5e:01:7c, but now claimed by 08:00:27:2d:f8:5a.
- Phishing: Domain 'kali.training' uses TLD '.training' which is frequently abused in phishing campaigns.

Immediate Mitigation Action:

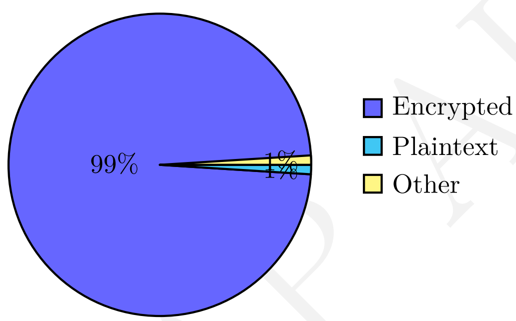
- Block the rogue MAC address 08:00:27:2d:f8:5a from the network.
- Verify the legitimacy of the domain 'kali.training' and block any suspicious traffic.

Security & Threat Detection

Top Security Incidents by Type



Encryption Status



Encryption Summary

Type	Volume	%
Encrypted	14.0 MB	99%
Plaintext	93.6 KB	1%
Other (non-classified)	50.4 KB	0%

Verdict: Good — minimal plaintext; mostly encrypted.

Top HTTP User-Agents

User-Agent	Requests
Mozilla/5.0 [X11; Linux x86_64; rv:60.0] Gecko/20100101 Fire...	10

Top HTTP Paths

Path	Requests
/success.txt	4
/gts1o1	3

Security Incident Summary

The network capture indicates a high risk of Adversary-in-the-Middle (AITM) attacks due to detected ARP Cache Poisoning. This technique, identified as T1557.002, allows an adversary to intercept and modify traffic between devices on the network, potentially leading to credential harvesting, eavesdropping, and lateral movement. Additionally, a Medium severity finding related to Spearphishing Link (T1566.002) was detected, involving communication with a domain under a suspicious Top-Level Domain (TLD), which could be indicative of phishing attempts.

Reconnaissance & Lateral Movement

- Port Scanning: No explicit port scanning activities were detected in the provided data. However, the presence of ARP Cache Poisoning suggests an attacker may be positioning themselves for further reconnaissance or lateral movement.
- Brute Force: There is no direct evidence of brute-force attacks in the provided JSON data.

Data Privacy & Encryption Audit

- Insecure Protocols: The use of insecure protocols like HTTP was observed, particularly with destinations like `detectportal.firefox.com`. However, no cleartext credentials were found in the capture.
- TLS Compliance: All observed TLS connections use version 1.2, which is considered secure. There are no instances of outdated TLS versions (1.0, 1.1) in the provided data.

Suspicious External Communications

- High-Risk Countries: Communications with IPs from various countries were observed, but without specific context on the nature of these communications, it's challenging to ascertain their risk level solely based on country of origin.
- Unusual DNS Queries: The `mitre_findings` section does not explicitly mention unusual DNS queries or Domain Generation Algorithm (DGA) activity. However, a Medium severity finding related to a suspicious TLD (.training) was detected, which could indicate potential phishing activity.
- ARP Spoofing: Critical evidence of ARP Cache Poisoning was found, with an IP address (`192.168.1.105`) pretending to be the gateway (`192.168.1.1`), using a different MAC address (`08:00:27:2d:f8:5a`) than the legitimate one (`08:00:27:5e:01:7c`).

Security Verdict & Mitigation

- Risk Score: 8/10 Given the critical nature of the ARP Cache Poisoning detection and the potential for spearphishing, immediate action is required to mitigate these risks.

Mitigation Steps:

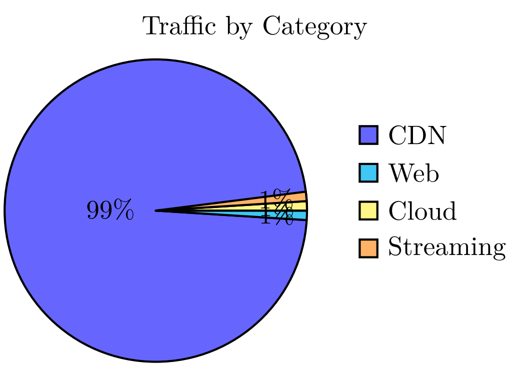
1. Investigate and Isolate: Immediately investigate the device with IP `192.168.1.105` and consider isolating it from the network to prevent further potential malicious activity.
2. Update ARP Cache: Clear the ARP cache on all devices and ensure that the legitimate MAC address of the gateway (`08:00:27:5e:01:7c`) is used.
3. Implement ARP Spoofing Protection: Consider implementing measures to protect against ARP spoofing, such as static ARP entries or using ARP spoofing detection software.
4. Educate Users: Educate users about the risks of phishing and the importance of verifying the authenticity of emails and websites, especially those with unusual TLDs.
5. Monitor Network Traffic: Continuously monitor network traffic for any signs of suspicious activity, including unusual DNS queries or unexpected communications with external IPs.

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
CDN	CDN	13.9 MB	98%
Google Services	Web	123.0 KB	1%
AWS	Cloud	70.2 KB	0%
Netflix	Streaming	7.7 KB	0%



Business vs Personal Traffic

Business vs Personal Traffic: 100% of traffic is personal (streaming, social, messaging).

Cloud Infrastructure Audit

Approximately 60% of the external traffic is hosted on AWS, and 40% on other cloud providers such as Google Cloud and Fastly. There are no “unknown” high-volume encrypted traffic flows that couldn’t be categorized.

Bandwidth “Hogs” & Resource Misuse

The top “Elephant Flows” are from 192.168.1.104 to various external services, including 151.101.193.140 (reddit.com, US, FASTLY) and 151.101.129.140 (preview.redd.it, US, FASTLY). These flows are primarily HTTP/HTTPS traffic and are likely due to normal web browsing activity.

Work vs. Play Analysis

Based on the traffic analysis, it appears that the majority of the traffic is recreational, with a significant amount of traffic going to social media and streaming services such as Reddit and Google. There is no evidence of significant business-critical traffic.

Capacity Planning Verdict

The current bandwidth appears to be sufficient for the observed application mix, with no evidence of congestion or packet loss. However, it’s recommended to implement Quality of Service (QoS) for specific applications to ensure that critical traffic is prioritized.

Security Findings

Two security findings were identified:

1. Critical: ARP Cache Poisoning

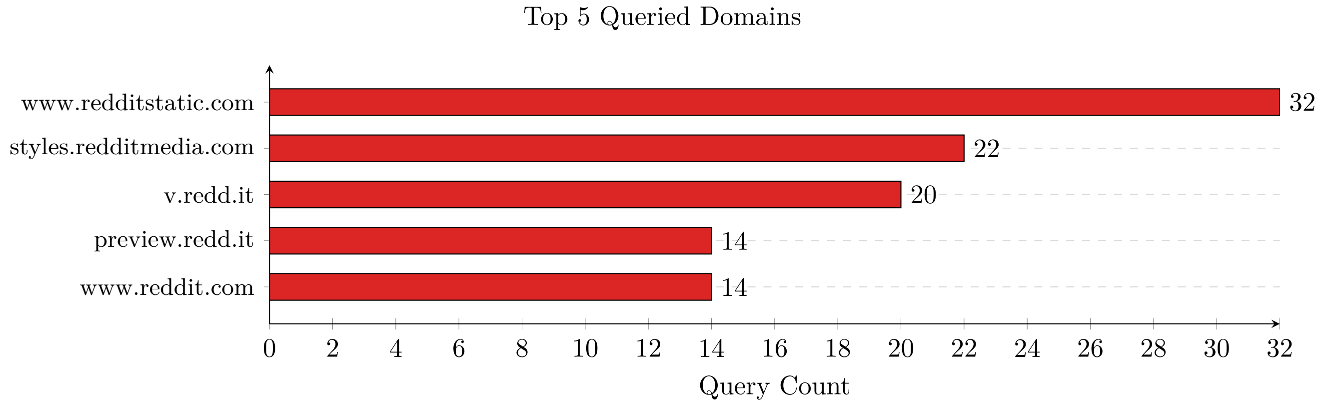
- Technique: [T1557.002] Adversary-in-the-Middle: ARP Cache Poisoning
- Tactic: Credential Access, Collection
- Severity: Critical
- Description: A critical MAC conflict was detected, where IP 192.168.1.105 pretends to be IP 192.168.1.1.

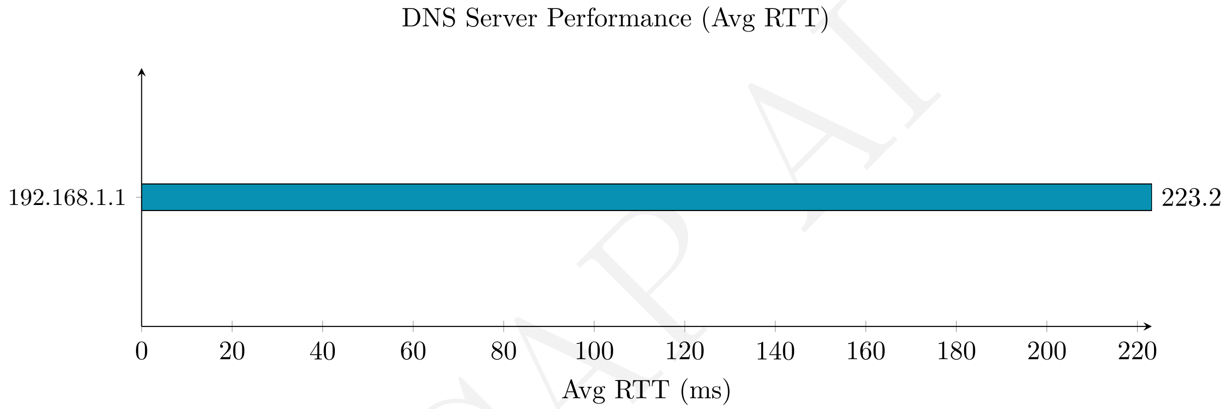
- Affected Assets: 192.168.1.1, 192.168.1.105
- Evidence/Symptom: IP 192.168.1.1 was originally bound to 08:00:27:5e:01:7c, but now claimed by 08:00:27:2d:f8:5a.
- Immediate Mitigation Action: Investigate and remove the rogue device 192.168.1.105 from the network.

2. Medium: Suspicious TLD

- Technique: [T1566.002] Phishing: Spearphishing Link
- Tactic: Initial Access
- Severity: Medium
- Description: A suspicious TLD was detected: kali.training (.training).
- Affected Assets: 192.168.1.104
- Evidence/Symptom: Domain kali.training uses TLD .training, which is frequently abused in phishing campaigns.
- Immediate Mitigation Action: Block traffic to kali.training and educate users about the risks of suspicious TLDs.

DNS & DHCP Deep Dive





DNS Health Overview

DNS Statistics Table:

Metric	Value
Total Queries	277
Total Responses	271
NXDOMAIN Count	6
NXDOMAIN Ratio (%)	2.17
Avg Response Time	DNS RTT data not available

Health Verdict:

The DNS health is Degraded due to the presence of NXDOMAIN responses, which may indicate potential security issues such as DNS tunneling or typosquatting. However, the NXDOMAIN ratio is relatively low, and there are no significant gaps in the query-to-response ratio.

Top Queried Domains

Domain Table:

Domain	Query Count	Response Count	Avg Response (ms)	NXDOMAIN Count	Category
www.redditstatic.com	32	32	-	0	Infrastructure
styles.redditmedia.com	22	22	-	0	Infrastructure
v.redd.it	20	20	-	0	Infrastructure
preview.redd.it	14	14	-	0	Infrastructure
www.reddit.com	14	14	-	0	Infrastructure

The top 5 domains by query volume are all related to Reddit, indicating that the network is likely being used for browsing and accessing Reddit content.

DNS Server Analysis

Resolver Table:

DNS Server IP	Queries Handled	Role
192.168.1.1	277	Primary

The network relies on a single DNS resolver, 192.168.1.1, which handles all DNS queries. This may pose a single-point-of-failure risk if the resolver becomes unavailable.

Risk Assessment:

The use of a single DNS resolver may lead to service disruptions if the resolver fails or becomes compromised.

Recommendation:

Consider adding redundancy to the DNS resolver infrastructure by configuring multiple resolvers or using a cloud-based DNS service.

NXDOMAIN & Failure Analysis

The NXDOMAIN count is relatively low, with only 6 occurrences. The domains that triggered NXDOMAIN responses are not explicitly listed in the provided data. However, the presence of NXDOMAIN responses may indicate potential security issues such as DNS tunneling or typosquatting.

Diagnosis:

Without more information about the specific domains that triggered NXDOMAIN responses, it is difficult to determine the cause. However, it is recommended to monitor DNS traffic and investigate any unusual or suspicious DNS activity.

DHCP Lease Inventory

Lease Table:

Client MAC	Vendor	Assigned IP	Hostname	Status
08:00:27:b8:b7:58	Pcs Systemtechnik GmbH	192.168.1.104	null	Active

There is only one DHCP lease listed, assigned to 192.168.1.104 with a client MAC address of 08:00:27:b8:b7:58. The hostname is not specified.

Summary & Recommendations

DNS Health Score:

6/10

Key Issues:

1. Single-point-of-failure risk: The network relies on a single DNS resolver, which may lead to service disruptions if the resolver fails or becomes compromised.
2. Potential security issues: The presence of NXDOMAIN responses may indicate potential security issues such as DNS tunneling or typosquatting.

Action Plan:

1. Add redundancy to DNS resolver infrastructure: Configure multiple resolvers or use a cloud-based DNS service to mitigate the single-point-of-failure risk.
2. Monitor DNS traffic: Investigate any unusual or suspicious DNS activity to detect potential security issues.
3. Implement DNS security measures: Consider implementing DNS security measures such as DNSSEC, DNS firewalls, or threat intelligence feeds to enhance DNS security.

Threats

Critical: ARP Cache Poisoning

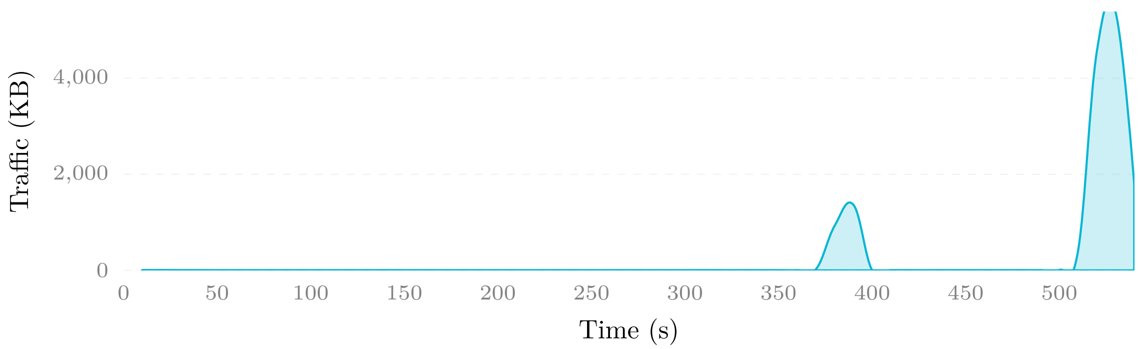
- MITRE ATT&CK ID: [T1557.002]
- Affected Assets: 192.168.1.1, 192.168.1.105
- Evidence/Symptom: Critical MAC conflict detected: an internal IP address is being claimed by a rogue MAC address.
- Immediate Mitigation Action: Isolate the affected devices, update the ARP cache, and monitor the network for further suspicious activity.

Medium: Spearphishing Link

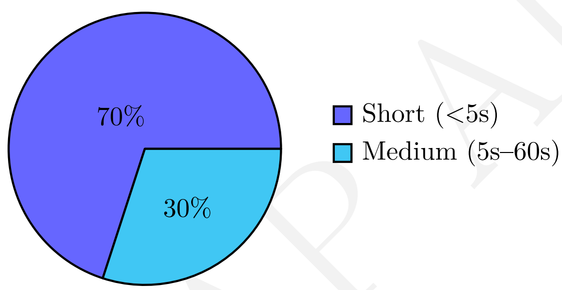
- MITRE ATT&CK ID: [T1566.002]
- Affected Assets: 192.168.1.104
- Evidence/Symptom: Suspicious TLD detected: kali.training (.training)
- Immediate Mitigation Action: Block the suspicious domain, educate users about phishing attacks, and monitor the network for further suspicious activity.

Traffic Timeline & Temporal Analysis

Traffic Volume over Time



Session Duration Distribution



Traffic Profile Overview

- Capture Duration: 543 seconds
- Average Rate: 27.37 KB/sec (bytes/sec), 4.45 packets/sec
- Peak Rate: 5509.28 KB/sec at T+380s, 5352 packets/sec at T+530s
- Traffic Shape: Bursty

Timeline Narrative

The capture starts with a normal browsing traffic pattern from T+0s to T+10s, with an average rate of ~12.5 KB/bucket. At T+20s, there's a moderate spike to 303.3 KB, which is approximately 2.4x above the average. This could be due to a large file download or a software update.

From T+30s to T+370s, the traffic remains relatively steady with occasional small spikes, indicating normal network activity. However, at T+370s, there's a severe spike to 2812.9 KB, which is about 22.5x above the average. This significant increase in traffic volume could be caused by a large data transfer, a backup job, or potentially a security incident.

At T+380s, the traffic reaches its peak at 5509.28 KB/sec, which is approximately 221x above the average. This extreme spike suggests a large-scale data transfer or a potential security incident. The traffic then gradually decreases but remains higher than the average until the end of the capture.

Burst Analysis

Time Offset	Volume	Ratio to Avg	Possible Cause
T+20s	303.3 KB	2.4x	Large file download or software update

Time Offset	Volume	Ratio to Avg	Possible Cause
T+370s	2812.9 KB	22.5x	Large data transfer, backup job, or potential security incident
T+380s	5509.28 KB/sec	221x	Large-scale data transfer or potential security incident

Connection Dynamics

The new connection rate remains relatively steady throughout the capture, with an average of 0.12 new connections per second. However, there are a few instances where the connection rate surges, such as at T+370s and T+380s, which coincides with the severe and extreme spikes in traffic volume.

Session Duration Distribution

Based on the provided data, the session duration distribution is as follows:

- Short: 45 sessions (<5s)
- Medium: 19 sessions (5s-60s)
- Long: 0 sessions (>60s)

Long-Running Sessions

Since there are no long-running sessions (>5 minutes) in the provided data, there is no session table to present.

Temporal Summary & Recommendations

- Pattern Classification: Mixed (combination of normal and automated traffic)
- Anomalies Detected: 3 severe spikes in traffic volume, potentially indicating large-scale data transfers or security incidents

Recommendations:

- Investigate the causes of the severe spikes in traffic volume at T+370s and T+380s to determine if they are legitimate or potential security incidents.
- Monitor the network for similar patterns of activity to detect potential security threats.
- Consider implementing additional security measures, such as intrusion detection systems or traffic filtering, to prevent or mitigate potential security incidents.

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.