OSINT Reconnaissance Report – Acme Corp

Engagement ID: BBP-OSINT-2025-001
Primary domains: acme.com

---

1. Executive Summary

This OSINT assessment focused on identifying publicly visible assets, exposed services, and externally observable risks relating to **Acme Corp**.
The analysis combined passive and active reconnaissance using industry-standard tooling (Amass, Subfinder, Naabu, Httpx, Nuclei) in line with BlackBox Pentesters' methodology.

Key Findings Summary

- **Identified hostnames:** 32
- **Identified IPv4 addresses:** 0
- **Externally reachable services:** 0
- **HTTP(S) services discovered:** 0
- **Template-based vulnerabilities (Nuclei):** 0
- **Credential exposure hits:** 0
- **GitHub code references:** 0
- **Shodan-exposed hosts:** 0

At the time of testing, **no exposed services or high-risk vulnerabilities** were identified.
This significantly reduces the externally accessible attack surface.
However, organisations with a minimal perimeter remain susceptible to:

- credential-based attacks
- supply-chain compromise
- phishing and social engineering
- accidental infrastructure exposure following future DNS or hosting changes

---

2. OSINT-Driven Observations

Automated reconnaissance did **not** identify:

- public remote-access services (SSH, RDP, VPN)
- externally reachable administrative interfaces
- misconfigured cloud buckets
- vulnerable web services accessible from the internet

This result is positive and indicates that **Acme Corp's external exposure is currently low**.

Recommendations

1. **Continue perimeter monitoring** to detect new hosts, DNS changes, or unexpected exposures.
2. **Review credential hygiene**, as password reuse and historical breaches remain a leading attack vector.
3. **Conduct regular phishing and social-engineering assessments**, as human factors remain exploitable even with a minimal technical footprint.
4. **Re-run OSINT quarterly** or after major infrastructure updates.

---

3. External Attack Surface – Asset Inventory

A detailed breakdown of all identified externally visible assets is provided below.

3.1 Subdomain Inventory

Total Acme-owned hostnames identified: **32**

These hostnames represent the external footprint of acme.com during the assessment.

#	Hostname

| 1 | acme.com |

| 2 | auth.acme.com |

| 3 | chumaker.acme.com |

| 4 | gate.acme.com |

| 5 | groupr.acme.com |

| 6 | heartmaker.acme.com |

| 7 | labelmaker.acme.com |

| 8 | licensemaker.acme.com |

| 9 | mail.acme.com |

| 10 | mail.patton.acme.com |

| 11 | mail.rr.acme.com |

| 12 | mapper.acme.com |

| 13 | online.acme.com |

| 14 | patton.acme.com |

| 15 | photo.acme.com |

| 16 | pix.acme.com |

| 17 | root.acme.com |

| 18 | rr.acme.com |

| 19 | www.acme.com |

| 20 | www.auth.acme.com |

| 21 | www.chumaker.acme.com |

| 22 | www.groupr.acme.com |

| 23 | www.heartmaker.acme.com |

| 24 | www.labelmaker.acme.com |

| 25 | www.licensemaker.acme.com |

| 26 | www.mail.acme.com |

| 27 | www.mapper.acme.com |

| 28 | www.online.acme.com |

| 29 | www.patton.acme.com |

| 30 | www.photo.acme.com |

| 31 | www.pix.acme.com |

| 32 | www.rr.acme.com |

3.2 Open Ports (Naabu)

Externally reachable hosts with open ports: **0**

No open ports identified by automated scanning.

3.3 HTTP(S) Services (Httpx)

HTTP(S) services identified: **0**

No HTTP services identified.

---

4. Nuclei Findings (Template-Based Checks)

Total detections: **0**

No issues detected by Nuclei.

---

5. Credential Exposure (Public Breach Intelligence)

Total breach matches: **0**

No credential exposure identified or breach API disabled.

---

6. Public Code & Infrastructure Intelligence

6.1 GitHub Search

Matches identified: **0**

No GitHub references identified.

6.2 IP / ASN Intelligence

IP enrichment results: **0**

No IP intelligence available.

6.3 Shodan Exposure

Exposed hosts detected: **0**

No Shodan-indexed exposure detected.

---

7. Analyst Notes & Next Steps

- This report forms the OSINT / reconnaissance section of a full penetration test.
- Findings here should be used to validate scope and guide deeper testing.
- As Acme's infrastructure evolves (new cloud services, SaaS adoption, DNS changes), new exposures may appear that were not observable during this engagement.

For ongoing monitoring or deeper analysis, BlackBox Pentesters can integrate:

- Continuous DNS and attack-surface monitoring
- Dark web credential monitoring
- Code repository monitoring
- Scheduled Shodan/Censys exposure checks

Generated automatically using the BlackBox OSINT Automation Framework.
Report timestamp: 2025-12-02 15:03 UTC
