

Passive Reconnaissance Report - Lenskart.com


Screenshot 1: Whois Information


| | |
|-----------|--|
| Registrar | GoDaddy.com, LLC IANA ID: 146 URL: https://www.godaddy.com,http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) +1.4806242505 |
|-----------|--|

Screenshot 2: IP Address Information

| | | |
|------------|--|---|
| IP Address | 104.17.2.118 is hosted on a dedicated server |  |
|------------|--|---|

Screenshot 3: MX Records (Email Servers)

mx:lenskart.com [Find Problems](#) [Solve Email Delivery Problems](#) 

 Outlook.com requires DMARC for Inbox Delivery!
Get ready with MxToolbox Delivery Center!


[Learn More](#)

| Pref | Hostname | IP Address | TTL | | |
|------|-------------------------|---|-------|-----------------|-----------|
| 60 | aspmx.l.google.com | 64.233.180.26 <small>Google LLC (AS15169)</small> | 5 min | Blacklist Check | SMTP Test |
| 60 | aspmx.l.google.com | 2607:f8b0:4004:c08::1b | 5 min | Blacklist Check | |
| 300 | alt1.aspmx.l.google.com | 172.253.116.27 <small>Google LLC (AS15169)</small> | 5 min | Blacklist Check | SMTP Test |
| 300 | alt1.aspmx.l.google.com | 2a00:1450:400b:c02::1a | 5 min | Blacklist Check | |
| 300 | alt2.aspmx.l.google.com | 173.194.76.26 <small>Google LLC (AS15169)</small> | 5 min | Blacklist Check | SMTP Test |
| 300 | alt2.aspmx.l.google.com | 2a00:1450:400c:c00::1b | 5 min | Blacklist Check | |
| 600 | alt3.aspmx.l.google.com | 142.250.102.27 <small>Google LLC (AS15169)</small> | 5 min | Blacklist Check | SMTP Test |
| 600 | alt3.aspmx.l.google.com | 2a00:1450:4025:402::1b | 5 min | Blacklist Check | |
| 600 | alt4.aspmx.l.google.com | 192.178.156.27 <small>Google LLC (AS15169)</small> | 5 min | Blacklist Check | SMTP Test |
| 600 | alt4.aspmx.l.google.com | 2a00:1450:4013:c1c::1a | 5 min | Blacklist Check | |


Screenshot 4: DNS Lookup

SuperTool Beta9

[DNS Lookup](#)

a:lenskart.com [Find Problems](#) 

| Type | Domain Name | IP Address | TTL |
|------|------------------------------|---|-------|
| A | lenskart.com | 104.17.2.118 <small>Cloudflare, Inc. (AS13335)</small> | 5 min |
| A | lenskart.com | 104.17.3.118 <small>Cloudflare, Inc. (AS13335)</small> | 5 min |

| | Test | Result |
|---|----------------------|------------------|
|  | DNS Record Published | DNS Record found |

Your DNS hosting provider is "Cloudflare" [Need Bulk Dns Provider Data?](#)

Threat Model Table

| Actor | Asset | Threat |
|----------|-----------------------------|---|
| Outsider | Registrar Info (GoDaddy) | Social engineering attack to hijack domain |
| Outsider | IP Address (Cloudflare) | DDoS attack or fingerprinting infrastructure |
| Attacker | MX Records (Google servers) | Email spoofing or phishing using MX info |
| Insider | DNS Configuration | Misconfigured DNS leading to subdomain takeover |

Summary of Findings

In this Week 1 project, we performed passive reconnaissance on the website lenskart.com using various online tools such as Whois Lookup, MXToolbox, DNS Lookup, and BuiltWith. The Whois data revealed that the domain is registered through GoDaddy.com, LLC, providing details like the registrar contact and Whois server. The site is hosted on a dedicated IP address (104.17.2.118), which is managed by Cloudflare, indicating some level of DDoS protection and CDN infrastructure.

Further DNS lookup using MXToolbox showed that Lenskart uses Google's email infrastructure (aspmx.l.google.com, altX.aspmx.l.google.com) for handling emails. The DNS records confirm that Cloudflare is the DNS hosting provider, which typically helps in hiding the actual server IP and provides protection against various network attacks. Multiple mail servers with different priorities also suggest good failover email configuration.

Based on the collected data, a threat model was created listing various actors and potential threats. For example, an outsider could attempt social engineering on the domain registrar to hijack the domain, or attackers might try phishing by spoofing the email setup identified in the MX records. The use of Cloudflare minimizes some direct server threats, but DNS misconfiguration or insider threats still pose risks. Overall, this exercise offered a practical understanding of what assets are exposed and how attackers might exploit them using only publicly available data.