Le Bon Bon Croissant

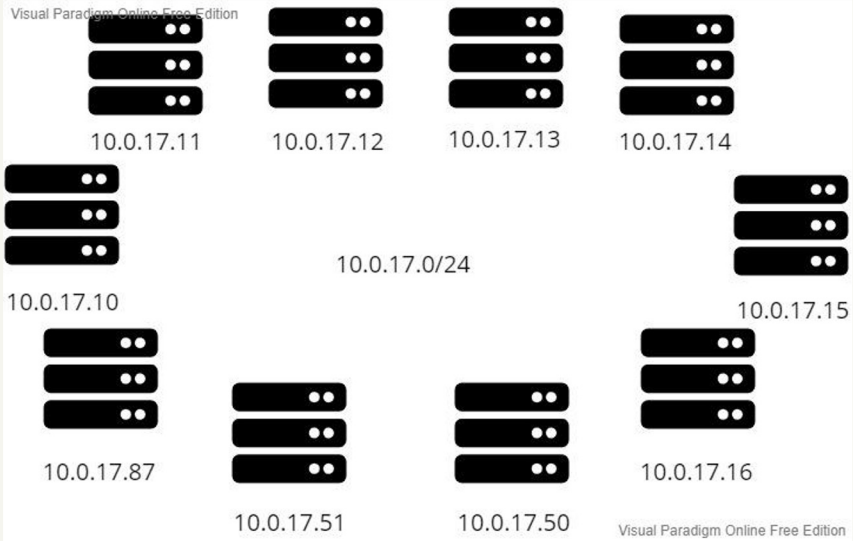
Executive Briefing | Finals
Team XX

We love croissants too!

Goal & Scope

Two-part pentest engagement to assess the security posture of Le Bonbon Croissant to validate security controls following a prior security breach.

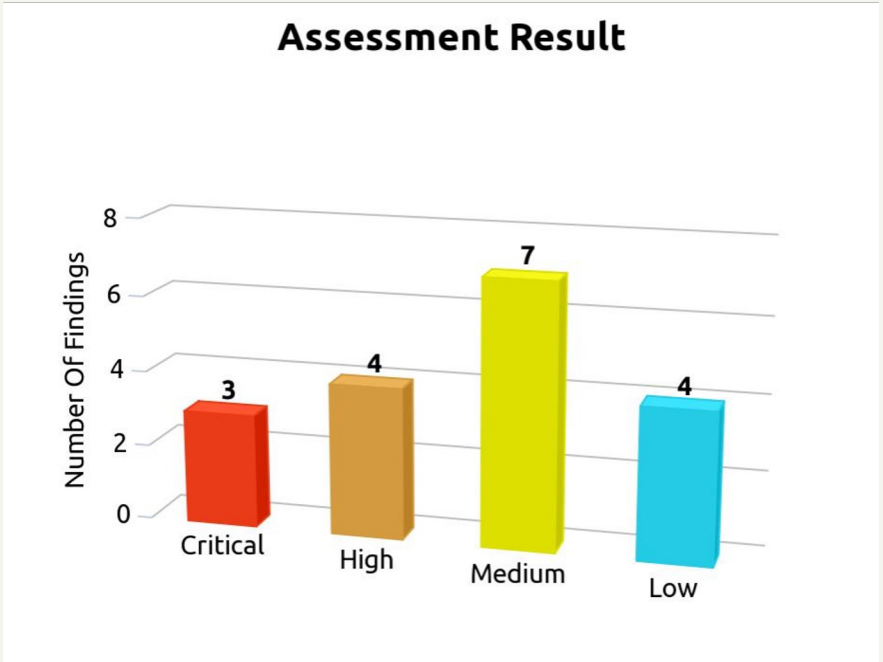
Scope: **10** discoverable hosts on the 10.0.17.0/24 subnet, including core distribution warehouse and customer systems.



Summary of Findings

Three Critical Findings

- Unauthenticated Administrator access to two critical databases storing sensitive customer and payment information
- Remote Code Execution
- Credit Card Data Unencrypted and accessible on Postgresql Jawbreaker database



Inherent & Residual Risks

Vuln ID	Description	Machine	CVSS Score	Inherent Risk	Residual Risk
C1	Unauthenticated Root Access to MySQL E-commerce Database	10.0.17.14	9.8	CRITICAL	MED
C2	Unauthenticated Root Access to Postgres Database	10.0.17.14	9.8	CRITICAL	MED
C3	Credit Card Data Unencrypted on Postgres Jawbreaker Database	10.0.17.14	9.0	CRITICAL	MED
H1	PostGres Authenticated RCE	10.0.17.14	8.5	HIGH	MED
H2	Unauthenticated Access to Administrative API Functions	10.0.17.11	7.8	HIGH	LOW
H3	System Denial of Service	10.0.17.13	7.5	HIGH	LOW
H4	Weak Encoding on MySQL Database	10.0.17.14	7.5	HIGH	LOW

Regulatory Requirements

PCI DSS

- Potential fines of up to **$5,000 to $100,000** per month
- **$50-$90** per cardholder info endangered

- **6,000+** credit cards were discovered
- In the event of a breach, using the median fine amount, the estimated fine for LBC is approximately **$270,000.**

- **6,000+** Users PII was discovered, potential breach of this size would have to be reported due to SEC enforcements

GDPR

- Requires consent of personal information collected of an EU resident.
- Fines are **4% of annual global revenue**

- **6,000+ users** were found.
- Testing team did not discover a method for users to opt out of collection or request to remove their data

Positive Observations

P1: PLC Security

P2: Limited Remote Access

P3: No SSL Variants Allowed

P4: Limited Service Footprint

Potential Improvements

- **Credit Card Information Hygiene**
  - 3rd Party for processing credit card information
  - Do not store user credit card information
  - Encrypt using strong ciphers if credit card information is required

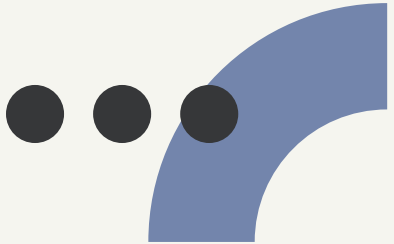
- **Implement Least Privilege Access Across the Network**
  - Network Segmentation to limit cardholder data environment scope for PCI requirements

- **Consider improving Defense-in-Depth Mechanisms by implementing common security controls such as:**
  - Firewalls, EDR, AV, DLP, MFA, and a WAF

Next Steps

- Consider a full PCI Assessment with a qualified security assessor (QSA)
- Recommended follow up within 6-months for PCI testing
- Evaluate current credit card processing mechanisms and consider alternatives

MITRE HEAT MATRIX



Reconnaissance	Initial Access	Execution	Credential Access	Discovery	Collection	Impact
Active scanning	Exploit internet facing application	Command and Scripting Interpreter	Unsecured credentials	File and Directory Discovery	Data from Information Repositories	Endpoint denial of service
Gather victim host information	Valid accounts		Exploitation for Credential Access	Account Discovery		
				Network Service Scanning		

Thank you